**Muddy Waters, LLC**
www.muddywatersresearch.com
info@muddywatersresearch

Director of Research: Carson C. Block, Esq.

**Use of Muddy Waters reports is limited by the Terms of Service on its website, which are as follows. To be authorized to access such reports, you must agree to these terms, regardless of whether you have downloaded its reports directly from this website or someone else has supplied the report to you without authorization from Muddy Waters.**

**Terms of Service:**

By downloading from, or viewing material on, this website you agree to the following Terms of Service. You agree that use of Muddy Waters LLC's research is at your own risk. In no event will you hold Muddy Waters LLC or any affiliated party liable for any direct or indirect trading losses caused by any information on this site. You further agree to do your own research and due diligence before making any investment decision with respect to securities covered herein. You represent to Muddy Waters that you have sufficient investment sophistication to critically assess the information, analysis and opinion on this site. You further agree that you will not communicate the contents of this report to any other person unless that person has agreed to be bound by these same terms of service. If you download or receive the contents of this report as an agent for any other person, you are binding your principal to these same Terms of Service.

**You should assume that as of the publication date of our reports and research, Muddy Waters, LLC (possibly along with or through our members, partners, affiliates, employees, and/or consultants) along with our clients and/or investors and/or their clients and/or investors has a short position in all stocks (and/or options, swaps, and other derivatives related to the stock) and bonds covered herein, and therefore stands to realize significant gains in the event that the price of either declines. We intend to continue transacting in the securities of issuers covered on this site for an indefinite period after our first report, and we may be long, short, or neutral at any time hereafter regardless of our initial recommendation**.

This is not an offer to sell or a solicitation of an offer to buy any security, nor shall Muddy Waters offer, sell or buy any security to or from any person through this site or reports on this site. Muddy Waters, LLC is not registered as an investment advisor in any jurisdiction.

If you are in the United Kingdom, you confirm that you are accessing research and materials as or on behalf of: (a) an investment professional falling within Article 19 of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 (the "FPO"); or (b) high net worth entity falling within Article 49 of the FPO.

Our research and reports express our opinions, which we have based upon generally available information, field research, inferences and deductions through our due diligence and analytical process. To the best of our ability and belief, all information contained herein is accurate and reliable, and has been obtained from public sources we believe to be accurate and reliable, and who are not insiders or connected persons of the stock covered herein or who may otherwise owe any fiduciary duty or duty of confidentiality to the issuer. However, such information is presented "as is," without warranty of any kind, whether express or implied. Muddy Waters, LLC makes no representation, express or implied, as to the accuracy, timeliness, or completeness of any such information or with regard to the results to be obtained from its use. Further, any report on this site contains a very large measure of analysis and opinion. All expressions of opinion are subject to change without notice, and Muddy Waters, LLC does not undertake to update or supplement any reports or any of the information, analysis and opinion contained in them.

You agree that the information on this website is copyrighted, and you therefore agree not to distribute this information (whether the downloaded file, copies / images / reproductions, or the link to these files) in any manner other than by providing the following link: http://www.muddywatersresearch.com/research/. If you have obtained Muddy Waters research in any manner other than by download from that link, you may not read such research without going to that link and agreeing to the Terms of Service. You further agree that any dispute arising from your use of this report and / or the Muddy Waters Research website or viewing the material hereon shall be governed by the laws of the State of California, without regard to any conflict of law provisions. You knowingly and independently agree to submit to the personal and exclusive jurisdiction of the superior courts located within the State of California and waive your right to any other jurisdiction or applicable law, given that Muddy Waters, LLC has offices in California. The failure of Muddy Waters, LLC to exercise or enforce any right or provision of these Terms of Service shall not constitute a waiver of this right or provision. If any provision of these Terms of Service is found by a court of competent jurisdiction to be invalid, the parties nevertheless agree that the court should endeavor to give effect to the parties' intentions as reflected in the provision and rule that the other provisions of these Terms of Service remain in full force and effect, in particular as to this governing law and jurisdiction provision. You agree that regardless of any statute or law to the contrary, any claim or cause of action arising out of or related to use of this website or the material herein must be filed within one (1) year after such claim or cause of action arose or be forever barred.

**Company:** NQ Mobile Inc.

**Ticker:** NQ

**Industry:** Mobile Security

**Thesis:** Strong Sell

**Report Date:** October 24, 2013

**Target Price:** < $1

**Stock Price:** $22.88

**Market Cap:** $1.1 Billion

**Float:** 31.1 Million

**Avg Volume:** 4.9 Million

- NQ is a massive fraud. We believe it is a "Zero". At least 72% of NQ's purported 2012 China security revenue is fictitious. NQ's largest customer by far is really NQ. Our research estimates that NQ's real market share in China is only about 1.5%, versus the approximately 55% it reports. We estimate that its China paying user base is less than 250,000, versus the six million NQ claims.

- NQ's Antivirus 7.0 is unsafe for sale to consumers, and we consider it to be spyware that makes users' phones vulnerable to cyber attack. NQ makes a weak attempt to protect users' private data as it's uploaded through the Chinese government's firewall to NQ's server. Phones are vulnerable to MITM attacks because NQ fails to adhere to basic security protocols. MW engaged top-flight security software engineers to analyze this product.

- NQ's purported international revenue of $36.5 million is likely less real than its PRC revenue. NQ claims to generate international revenue in obscure markets, and through mysterious counterparties that seem to seldom pay.

- NQ's future is as bleak as its past. The recent pivot to advertising and gaming is merely an attempt to change to a fraud that NQ hopes will be less obvious. NQ cannot monetize users that it does not have.

- NQ's acquisitions are highly likely to be corrupt.

- NQ's cash balances are highly likely to not be real. In NQ's 2012 20-F, PwC classified all cash and term deposits as Level 2 assets (slightly hard to value), which is the first time we have seen this. NQ's purported movements of cash from its IPO almost certainly did not occur due to PRC FX controls. We therefore believe the term deposits are likely forgeries.

# NQ Mobile: China Fraud 2.0

NQ is a massive fraud. We believe it is a "Zero". At least 72% of NQ's purported China security revenue is fictitious. NQ's largest customer by far is really NQ. Its real business with carriers and SPs is a fraction of what NQ purports. NQ's online payment portal does not work – it is cosmetic only, designed to make investors think that NQ is a real company. NQ's prepaid card channel is a bad joke. We estimate that NQ's real market share in China is about 1.5%, versus the approximately 55% it purports. We estimate that NQ's paying China user base is less than 250,000, versus the approximately six million it purports. This fraud and the undisclosed related party transactions amount to securities fraud. We have already provided the SEC with information concerning NQ.

NQ's Antivirus 7.0 is unsafe for sale to consumers, and we consider it to be spyware. We engaged a group of top-tier specialized software engineers to dive deeply into the application's code. The engineers found that the application creates serious vulnerabilities, making users' phones prone to data compromise and cyber attack by hackers or the Chinese government. In other words, users phones are much more susceptible to compromise or attack with AV 7.0 than with nothing at all. NQ's applications send far more data than necessary to its server in China. This data includes information on all URLs a user visits and location information (among other sensitive items). The uploaded data is not sent securely (let alone in accordance with industry standards), despite passing through the Chinese government's firewall, which is believed to view and store all passing data. NQ sends this data to a third party analytics firm in China. Downloads are even less secure. The application does not require signature, making the phone highly vulnerable to third parties uploading malware. Our engineers successfully staged such an attack. After their analysis, the engineers speculated that these vulnerabilities could be deliberate because the techniques vary so widely from industry standards.

NQ's purported international revenue is even more questionable than its PRC revenue. A leading Android analytics provider estimates that NQ's global annual app revenue is well under $1.0 million. NQ generates de minimis revenue in the United States. The agreements NQ has announced with various US partners seem to have resulted in attachment rates of only 2% to 3%. NQ's purported days sales outstanding ("DSO") from are 198 days– much of which supposedly comes international revenue. Even in the most emerging of markets, NQ should be getting paid in 30 to 45 days. NQ's involvement with Telefónica is massively exaggerated. It is one of 3,000 developers on Telefonica's Blue Via platform. No developer has ever been expelled from the platform.

NQ's future is as bleak as its past. Its expansion into gaming and advertising is merely an attempt to prolong the fraud. NQ's lies about its security app market share have worn very thin, and the Company is trying to hide the ball by switching emphases. Co-CEO Omar Khan offers the clearest explanation of why NQ's expansion will fail. If NQ were really a "platform" that had the lowest user acquisition costs in the world, as Mr. Khan claims, then there could be a strategic basis for the expansion. In reality, NQ's acquisition costs are closer to being the highest in the world, and it should not be called a "platform" with a straight face. This is merely a way to claim to be in a business in which NQ hopes its fraud will be less obvious.

With one exception, NQ's real management (i.e., those perpetrating the fraud) are sloppy – to the point of being comical – fraudsters. They broke – with flying colors – the cardinal China fraud rule of not getting into trouble in China. NQ was caught red handed by China's largest television news organization, CCTV, installing malware on phones in order to sell them the cure. In addition to that incident, and the subsequent lies NQ tells about it, are illustrative of the type of people behind NQ. In addition to being greedy and willing to engage in illegal behavior, they are clearly undisciplined. That lack of discipline and desperation for real revenue leads them to do bizarre things, such as developing a knockoff Segway (we call it the "Family Guardian Emergency Response Vehicle"); selling anonymous phone cards in China to phone spammers (again, making the cure and the disease); trying to sell a "NQ for Men" app that enables philandering; engaging in black hat SEO by likely infringing trademarks of companies such as Samsung, Vodafone, and Apple; fabricating virus discovery announcements; and, claiming to have paid an outrageous amount ($1.55 million) for its domain.

The one intelligent move NQ made to further its fraud is putting in place the veneer of US management – particularly "Co-CEO" Omar Khan. Were Mr. Khan not fronting for NQ, we do not think that investors would have been so willing to overlook so many red flags. It is unclear what Mr. Khan does and does not know; however, he is not a member of the boards or management of any of NQ's China entities. It is clear that his stock package is worth close to $100 million, which is likely far more than he would have earned as a non-C level manager at Citigroup.

NQ's auditor has clearly done a sloppy job. The auditor failed to ensure that disclosures about cash balances by entity are correct. It classified all cash as a Level 2 asset, which we have never seen before. The auditor failed to ensure that share-based compensation is recorded at the correct entity. It permitted NQ to reclassify significant costs from Cost of Sales to R&D, substantially boosting NQ's gross margin. The auditor failed to notice that receivables from NQ's largest purported trade debtor, Yidatong, are aged well beyond what the contract permits. Having noticed this might have clued in the auditor that Yidatong is really NQ.

NQ's acquisitions are highly likely to be corrupt. Analysis of SAIC files of certain of NQ's acquisitions shows inconsequential businesses with very little capitalization. In some cases, we see shareholders of these purported technology companies who appear to be highly unlikely – villagers from remote parts of China who do not even have high school education. In some cases, the companies were operating at ghost addresses at the time NQ acquired them. "Ghost addresses" are a major theme in our due diligence on NQ. A ghost address is not only one where the subject company cannot be found, it is one where no business can physically be found – usually because the address does not exist.

NQ's cash balances are highly likely to not exist. Certain purported movements of IPO funds to one of NQ's onshore entities almost certainly could not have, and therefore did not, occur. The classification of all of NQ's cash and equivalents as Level 2 assets (meaning assets that are somewhat difficult to value) raises massive red flags about what evidence of cash balances NQ has given its auditor.

## Table of Contents

**THE VAST MAJORITY OF NQ'S CHINA REVENUE IS FRAUDULENT** .......... 6
YDT IS REALLY NQ. .......... 14
NQ'S THIRD PARTY PAYMENT CHANNEL IS NON-EXISTENT. .......... 17
NQ'S CHINA PREPAID CARD CHANNEL DOES NOT CONTRIBUTE MATERIALLY TO REVENUE. .......... 19
*Want to stump NQ customer service? Ask them where to buy prepaid cards in Beijing, Shanghai, or Guangzhou.* .......... 20
*Sellers report very few sales.* .......... 21
*NQ's online (lack of) card sales affirms our physical store checks that show the cards are obscure and immaterial to NQ revenue.* .......... 23
NQ IS AN OBSCURE COMPANY IN CHINA WITH MINIMAL BRAND RECOGNITION; OUR RESEARCH ESTIMATES THAT FEWER THAN 1.5% OF SMART PHONE OWNERS PRESENTLY HAVE A NQ SECURITY APP. .......... 25
*Retailer Visits Further Confirm that NQ has a Sliver of the Market Share it Claims.* .......... 29
*China App Store Download Data Confirm that NQ has a Sliver of the Market Share it Claims.* .......... 29

**NQ'S SAIC FINANCIALS ARE FRAUDULENT, LEADING TO FRAUDULENT SEC FINANCIALS** .......... 32

**NQ'S ANTIVIRUS 7.0 MAKES IT EASY FOR THE PRC GOVERNMENT AND HACKERS TO READ COPIOUS AMOUNTS OF SENSITIVE DATA, AND TO UPLOAD MALWARE TO USERS' PHONES** . 33

**NQ'S INTERNATIONAL REVENUE – HIGHLY LIKELY TO BE MASSIVELY OVERSTATED** .......... 37

**THE FARCICAL SIDE** .......... 41

**NQ'S 3-15 DNA – VIDEO AVAILABLE AT: HTTPS://VIMEO.COM/77704496** .......... 45

**US MANAGEMENT IS MERELY A FRONT** .......... 46

**NQ'S CASH BALANCE (A LEVEL 2 ASSET) IS HIGHLY LIKELY TO BE FRAUDULENT** .......... 48

**NQ'S LIKELY CORRUPT ACQUISITIONS** .......... 53

**NQ'S FUTURE IS AS BLEAK AS ITS PAST** .......... 55

**NQ'S FILINGS MAKE CLEAR THAT PWC'S AUDITS WERE SLOPPY** .......... 57
CASH .......... 58
LEVEL 2 CASH .......... 58
SHARE BASED COMPENSATION .......... 59
YIDATONG IS NOT PAYING PURSUANT TO THE TERMS OF THE CONTRACT OR IN LINE WITH NORMAL TRADE TERMS. .......... 59
REALLOCATION OF COSTS TO BOOST GROSS MARGIN. .......... 60

**APPENDIX A: U.S. STORE VISITS** .......... 61

**APPENDIX B: SAIC FINANCIAL FRAUD INDICIA** .......... 67

**APPENDIX C: SOFTWARE ENGINEER REPORT** .......... 71

## The Vast Majority of NQ's China Revenue is Fraudulent

We conclude that at least 72% of NQ's reported $32.2 million in 2012 China security software is fraudulent.[1] SAIC financials for Yidatong, its largest customer, NQ's enterprise and gaming companies, NationSky and FL Mobile, show indicia of fraud. It is therefore likely that very little of NQ's reported China revenue is real.

NQ reported $32.2 million in security software revenue in 2012 from China. We believe that NQ's real security revenue was $2.5 million to $7.7 million (7.8% to 23.9% of reported revenue). NQ purports to generate security revenue in China from three sources: carrier billing, which consists of receiving payments directly from mobile carriers and through "Service Providers" ("SPs"), direct payment through third party payment services, such as its purported partner Alipay; and prepaid cards (which encompass scratch off cards and purportedly also activation codes provided to retailers). (NQ might be preparing to fraudulently claim that carriers' prepaid cards are another payment channel.)

NQ's carrier billing channel revenue is inflated by at least 362% after eliminating NQ's fraudulent sales to the shell company it secretly controls, Yidatong.

NQ's largest customer is really NQ. NQ secretly controls a shell company called Yidatong ("YDT"). NQ claims that YDT is an independent company, and accounted for $20.2 million in 2012 revenue. In 2012, NQ's China carrier billing channel revenue totaled $27.9 million, meaning that without YDT's revenue, the carrier billing channel generated at most revenue of only $7.7 million, 72.1% lower than NQ purports. (This is generous, as we believe that China carrier billing was likely no more than $2.5 million.) After conducting extensive due diligence on YDT, we conclude that YDT is an empty shell with no discernable operation whatsoever. Further, YDT is really NQ. Our due diligence process included visiting 10 sites purportedly occupied by YDT, all of which were empty or did not exist; studying YDT's SAIC files and financial statements; searching for current and former employees; and reviewing various other records.

YDT's financial statements show that it generated a fraction of the business NQ claims YDT does. YDT's purported role is a SP (i.e., transaction processor), facilitating NQ's billing of mobile carriers in China.[2] For NQ to have generated $20.2 million in revenue from YDT, YDT would have to have generated at least that much itself because NQ receives its revenue from YDT net of YDT's margin. PRC accounting standards mandate that YDT book all funds it receives from the carriers as its revenue, and then book the payments to NQ and other clients as costs of sales.[3]

[1] NQ March 2013 investor presentation.

[2] Wireless Value-Added Application Service Channel Cooperation Agreement (Domestic) Between Beijing NetQin Technology Co. Ltd. and Tianjin Yidatong Technology Development Co. Ltd. Exhibit 10.11 to 2012 20-F.

[3] Accounting Standards for Enterprises No. 14 – Revenues.
http://209.200.107.14/english/law2_disp.asp?sublawcode=SUB57585711610141610&lawcode=LAW3544911991291514&country=China

According to SAIC financials, YDT only generated $2.9 million in 2012 revenue, which is 14% of what NQ purports to have generated in revenue from YDT. YDT would have had to generate at least the $20.2 million NQ purports to have generated from YDT…to say nothing of the 40% of YDT revenue purportedly attributable to other clients.[4] YDT's Cost of Sales account would include any amounts YDT paid to NQ and its other customers. Instead, YDT generated only $2.9 million in revenue, and had Cost of Sales of only $1.8 million. NQ reported accounts receivable from YDT of $9.3 million as of FY 2012,[5] but YDT's financials show total accounts payable of $3.7 million, once again showing the fraudulent nature of NQ's financials.

PRC GAAP requires that YDT's financial statements book revenue gross of payments to NQ and other customers.[6] The Business Tax (sales tax) of $97,000 YDT paid was a fraction of the more than $4.0 million it would have paid if it were generating the volumes NQ claims. The lack of Business Tax payments confirms that YDT's revenue is shown in its SAIC file on a gross basis. Under the PRC tax regime, YDT pays Business Tax on the gross amount of revenue it collects from carriers.[7] If NQ tries to argue that YDT is just your upstanding tax cheat,[8] the argument would not hold water. The parties that purportedly pay YDT – China Mobile, China Telecom, and China Unicom – would require Business Tax invoices in order to avoid being taxed on monies paid out. For YDT to generate a Business Tax invoice, it would need to pay the tax to the Tax Bureau, which would cause it to show up in YDT's financials.

YDT's income statement is below. It generated far less revenue, and paid far less in Business Tax than it would have were NQ's claims not fraudulent.

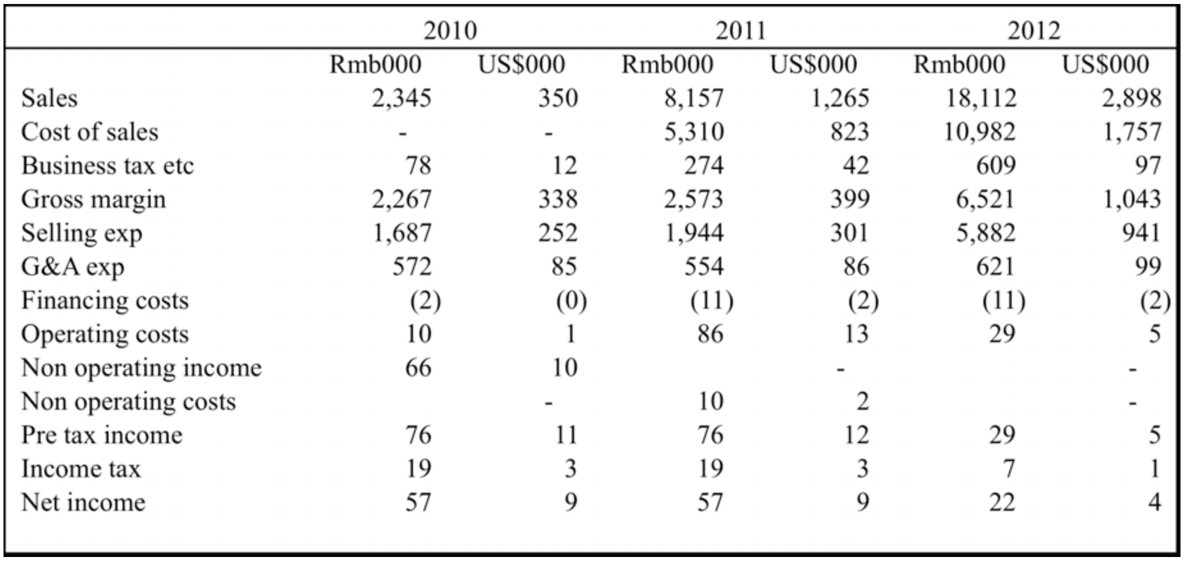
[4] NQ claims that YDT derives roughly 60% of its revenues from NQ. Assuming YDT only has a 10% gross margin on NQ business, YDT would generate about $35 million. See NQ "Response to J Capital Report, NQ: Not at Any Price," August, 2013.

[5] NQ 2012 20-F, p. F-17.

[6] Accounting Standards for Enterprises No. 14 – Revenues: http://209.200.107.14/english/law2_disp.asp?sublawcode=SUB5758571161014161O&lawcode=LAW3544911991291514&country=China

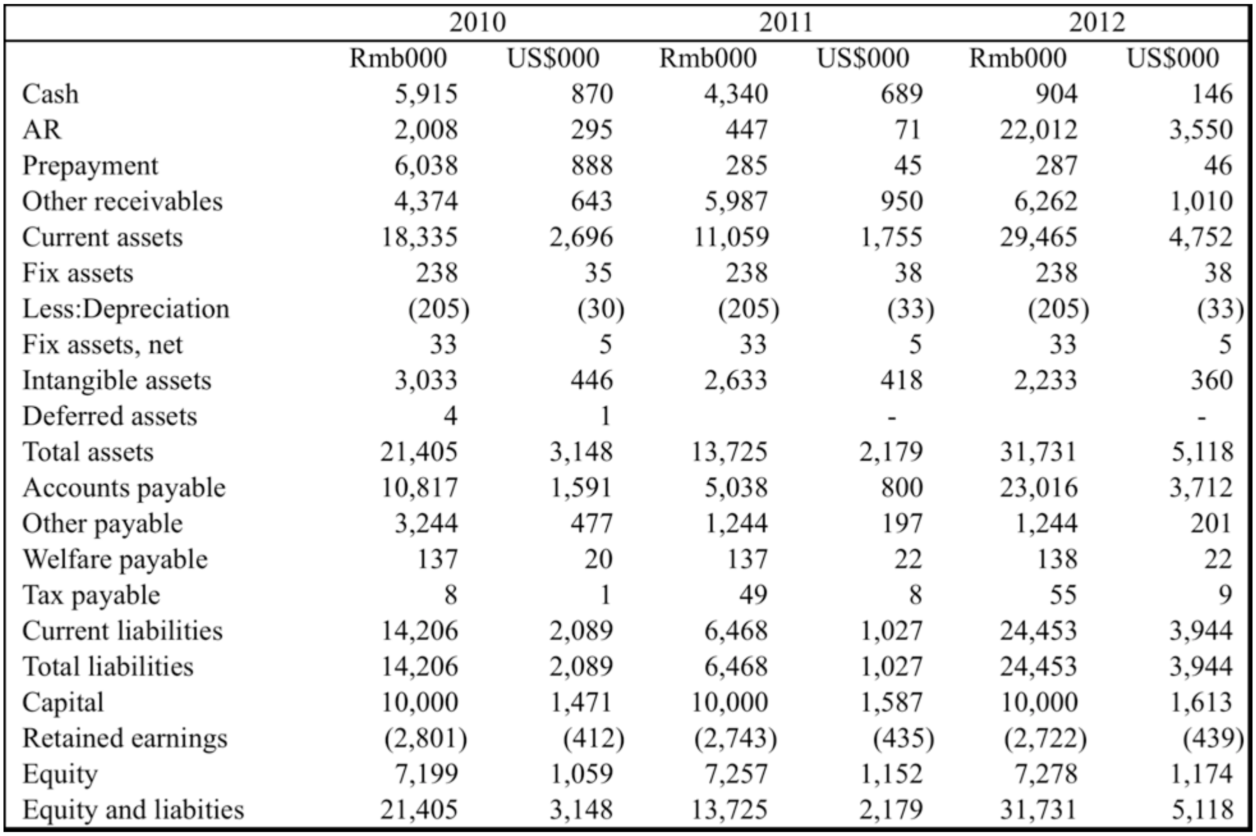
[7] https://www.bj.10086.cn/Portals/0/revision/images/mwsphzglssdxywfc.pdf

[8] "Upstanding tax cheat" is meant to illustrate the cognitive dissonance many investors in China companies exhibit when they argue that a given company is not a fraud – it merely cheats on taxes, resulting in understated revenues on SAIC financials.



| | 2010 | | 2011 | | 2012 | |
|---|---|---|---|---|---|---|
| | Rmb000 | US$000 | Rmb000 | US$000 | Rmb000 | US$000 |
| Sales | 2,345 | 350 | 8,157 | 1,265 | 18,112 | 2,898 |
| Cost of sales | - | - | 5,310 | 823 | 10,982 | 1,757 |
| Business tax etc | 78 | 12 | 274 | 42 | 609 | 97 |
| Gross margin | 2,267 | 338 | 2,573 | 399 | 6,521 | 1,043 |
| Selling exp | 1,687 | 252 | 1,944 | 301 | 5,882 | 941 |
| G&A exp | 572 | 85 | 554 | 86 | 621 | 99 |
| Financing costs | (2) | (0) | (11) | (2) | (11) | (2) |
| Operating costs | 10 | 1 | 86 | 13 | 29 | 5 |
| Non operating income | 66 | 10 | | - | | - |
| Non operating costs | | - | 10 | 2 | | - |
| Pre tax income | 76 | 11 | 76 | 12 | 29 | 5 |
| Income tax | 19 | 3 | 19 | 3 | 7 | 1 |
| Net income | 57 | 9 | 57 | 9 | 22 | 4 |

YDT's balance sheet below shows total payables that are a fraction of what NQ claims its AR from YDT were at the end of 2012. NQ purports that its AR from YDT was $9.3 million.



| | 2010 | | 2011 | | 2012 | |
|---|---|---|---|---|---|---|
| | Rmb000 | US$000 | Rmb000 | US$000 | Rmb000 | US$000 |
| Cash | 5,915 | 870 | 4,340 | 689 | 904 | 146 |
| AR | 2,008 | 295 | 447 | 71 | 22,012 | 3,550 |
| Prepayment | 6,038 | 888 | 285 | 45 | 287 | 46 |
| Other receivables | 4,374 | 643 | 5,987 | 950 | 6,262 | 1,010 |
| Current assets | 18,335 | 2,696 | 11,059 | 1,755 | 29,465 | 4,752 |
| Fix assets | 238 | 35 | 238 | 38 | 238 | 38 |
| Less:Depreciation | (205) | (30) | (205) | (33) | (205) | (33) |
| Fix assets, net | 33 | 5 | 33 | 5 | 33 | 5 |
| Intangible assets | 3,033 | 446 | 2,633 | 418 | 2,233 | 360 |
| Deferred assets | 4 | 1 | | - | | - |
| Total assets | 21,405 | 3,148 | 13,725 | 2,179 | 31,731 | 5,118 |
| Accounts payable | 10,817 | 1,591 | 5,038 | 800 | 23,016 | 3,712 |
| Other payable | 3,244 | 477 | 1,244 | 197 | 1,244 | 201 |
| Welfare payable | 137 | 20 | 137 | 22 | 138 | 22 |
| Tax payable | 8 | 1 | 49 | 8 | 55 | 9 |
| Current liabilities | 14,206 | 2,089 | 6,468 | 1,027 | 24,453 | 3,944 |
| Total liabilities | 14,206 | 2,089 | 6,468 | 1,027 | 24,453 | 3,944 |
| Capital | 10,000 | 1,471 | 10,000 | 1,587 | 10,000 | 1,613 |
| Retained earnings | (2,801) | (412) | (2,743) | (435) | (2,722) | (439) |
| Equity | 7,199 | 1,059 | 7,257 | 1,152 | 7,278 | 1,174 |
| Equity and liabities | 21,405 | 3,148 | 13,725 | 2,179 | 31,731 | 5,118 |

YDT is a ghost company (because it is really NQ). We tried extremely hard to find its operations, but were unsuccessful, despite visiting ten different office addresses throughout China. We obtained these addresses from YDT's SAIC filings, its website, NQ's SEC filings, and other sources. Five of the addresses were ghost addresses – i.e., it would have been impossible for YDT to ever be there because the addresses did not exist. (Ghost addresses are a theme that runs throughout our due diligence on NQ.) YDT's offices are either non-existent or completely empty. NQ claims that YDT accounted for roughly 15% of NQ's Q1 2013 revenue;[9] yet, YDT is clearly incapable of processing meaningful amounts of payments on behalf of NQ because it does not have even one employee regularly present to:

- turn on the lights,
- answer phones,
- reconcile billing issues with carriers,
- order office supplies,
- pay vendors,
- develop and implement marketing programs,
- sell services to new and existing customers,
- handle inquiries from existing customers, and
- (duties from NQ's purported contract with YDT): maintain the value-added technology platform, technology platform interface; provide verification codes for related products and technology support to customers; coordinate with telecom operators to ensure the testing and activation of client business; negotiate and communicate with telecom operators; maintain the revenue and flow search pages for customers; delete non-existent or discontinued users; review customers' marketing methods; oversee customers' compliance; develop, maintain, ensure stability and responsiveness of the information platform.

(On the positive side, it appears as though YDT's business model does not call for any human resource employees, which is an innovative approach to cost saving.)

We explored several permutations of the address for YDT's headquarters in Tianjin, before finding it in the Tianjin Haosheng Building. Because the lobby directory still had the prior tenant's name plate posted for room 502-2, and the office door located off a narrow, dingy hallway was unmarked, we thought it was another dead end. However, when queried, the building's management office confirmed that YDT did indeed rent room 502-2.

The manager of the building in which YDT has its headquarters said "this is just the registered address, but nobody works here…They all work in Beijing it seems, all of them, this is just the registered address, this is not their workplace, it's in Beijing". However, the YDT employees do not work in Beijing…or Shanghai…or Xi'an…or any of the nine purported YDT addresses we found. YDT is clearly a company trying not to be found. Below is a summary of our site visit attempts and findings. Actually, it is not really a company – we suspect that the meager revenue and expenses it did show were run through its books for reasons unconnected to its purported operations.

[9] NQ "Response to J Capital Report, NQ: Not at Any Price," August, 2013.

| | Address | Note | Source |
|---|---|---|---|
| Yidatong (Tianjin)<br>Headquarters | 天津市天津经济技术开发区第 3 大街 8 号豪威大厦 1 门 502-2<br>1-502-2, Haowei Tower, No. 8, Third Street, TEDA, Tianjin<br>Source: SAIC address | Visited. Confirmed with building management that this is Yidatong's registered address. Was told Yidatong has no operation there, no employees work at this location. The lobby directory also shows the company name of the former resident of the office space. Found 502-2 located down a narrow hallway, sharing the 502 number with two other small businesses. There was no sign posted on the door and the door was locked. Neighboring business were not familiar with them either. | YDT SAIC file |
| Yidatong - Beijing | 北京海淀区清华园三才堂 42 号 9 栋二层 4590<br>4590, Second floor, Ninth Building, No. 42, Sancaitang, Qinghuayuan, Haidian District, Beijing<br>Source: SAIC address | Ghost address. **Building 9 does not exist.** At No. 42 there are only two buildings. Furthermore, in the Qinghuayuan area, no community is composed of more than 7 buildings. | YDT Beijing office SAIC file |
| Yidatong - Beijing | 北京雅宝大厦 032 室<br>Suite 032, Yaobao Building, Beijing | In Suite 032 of the Yaobao Building, there is only a wholesale store selling gloves. The Yaobao Building management office confirmed Yidatong was not a tenant; additionally they explained they have no corporate tenants, and only are renting to individuals who are operating small businesses. | Online research[10], |
| Yidatong - Beijing | 北京市首体南路 22 号 11 层 11A<br>Suite 11A, Floor 11, No. 22, Shoutinan Road, Beijing | No 22, Shoutinan Road is a single building. The 11th floor is occupied by another company. Building management never heard Yidatong. | YDT Beijing office SAIC file,<br>Online Research,[11] |
| Yidatong – Beijing | 北京东城区和平里东街 4 号院 4 楼.<br>Building 4, No. 4 Yard, Hepingli East Street, Dongcheng, Beijing | Ghost address. Yard 4 does not exist. | YDT-NQ agreement, NQ, Exhibit 4-13. |

[10] http://www.xizhi.com/COMDAEKVQEBAAk4M69/, http://beijing.youbian.com/huangye/info592868/

[11] http://bj.gsdpw.com/%E5%A4%A9%E6%B4%A5%E5%B8%82%E6%98%93%E8%BE%BE%E9%80%9A%E7%A7%91%E6%8A%80%E5%8F%91%E5%B1%95%E6%9C%89%E9%99%90%E5%85%AC%E5%8F%B8%E5%8C%97%E4%BA%AC%E5%88%86%E5%85%AC%E5%8F%B8

| | | | |
|---|---|---|---|
| Yidatong-Xi’an | 西安市碑林区红缨路9号豪盛大厦C座30 801室<br>Suite, 30801 Haosheng Building, No. 9, Hongying Road, Beilin District, Xi’an City | Ghost address. It appears the address was a combination of two others. No.9 Hongying Road is a pharmacy. The Haosheng Building is adjacent to it, but it’s address is No. 78, Zhuque Ave. There is no suite 30801 in Haosheng Building. The management office never heard of Yidatong and confirmed the company does not have an office in the Haosheng Building. | Online research[12], SAIC address |
| Yidatong-Guiyang | 贵阳市南明区新华路242号2栋2单元7层12号<br>2-7-12, Building 2, No. 242, Xinhua Road, Nanming District, Guiyang | This is a residential community and no companies are located within it. Community residents never heard of Yidatong. The community is also older, disorderly, and down market. | SAIC address<br>Online research[13] |
| Yidatong-Guangzhou | 广州市天河区中山大道棠下村儒林路大街东三巷27号。<br>No. 27, Dongsanxiang, Rulinlu Ave. Tangxia Village, Zhongshan Ave. Tianhe District, Guangzhou City | Ghost address. There is only No. 18-26. There is no 27. Furthermore, there is no Yidatong in this area. Talked with locals and management office. | Online research[14], |
| Yidatong-Guangzhou | 广州经济技术开发区青年路511号上层202室。<br>202, Upper Level, No. 511, Qingnian Road, Guangzhou EDA, Guangzhou | Visited No. 511 Qingnian Rd, which is a sanitation company. The building’s upper level is a residential apartment. Based on conversations with local residents, no company operates at upper level. | SAIC source, Online Research[15], Company website[16] |
| Yidatong-Shanghai | 上海市奉贤区现代农业园区大庆路3号房D区3号 | Ghost address. Within the Fengxian District, there is no Daqing Rd. only a Daxing West Road. However Google maps displays this as Daqing Rd. The buildings were re-numbered. | SAIC address, Online research |

[12] http://company.ch.gongchang.com/info/51510557_886a/

[13] http://www.xizhi.com/COMDwEIUwIOCQAXHW3/

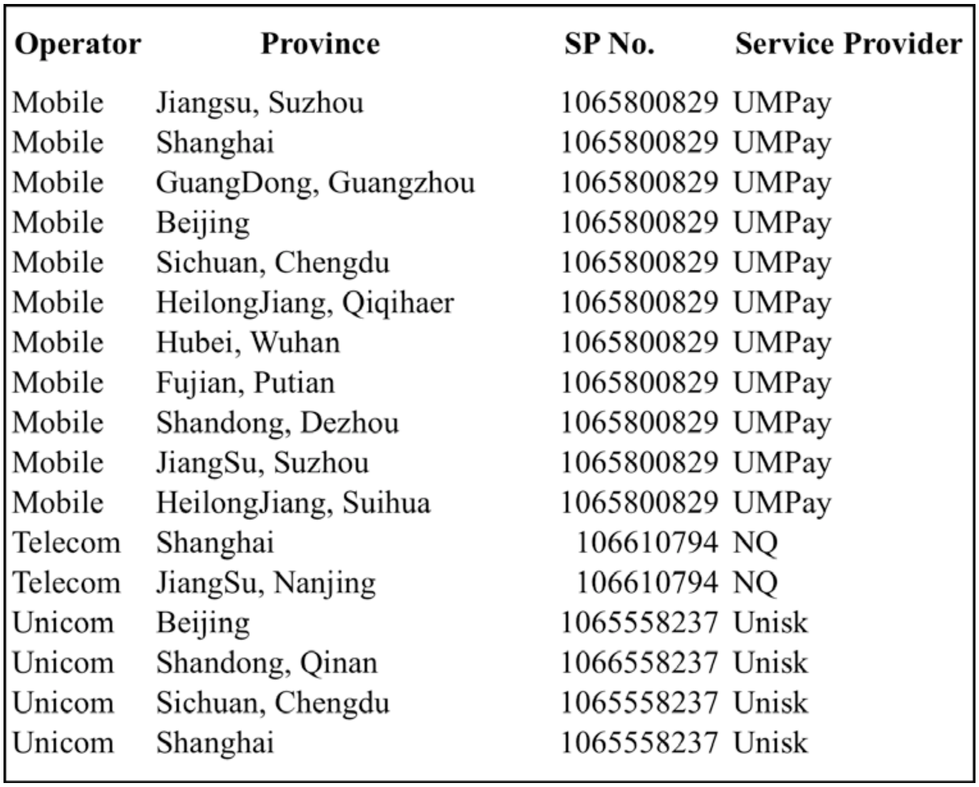
[14] http://www.ems185.com/corp_125662.html , http://www.ems185.com/corp_125662.html

[15] http://www.11467.com/shanghai/co/179331.htm

[16] http://www.yidatone.com/contact.jsp

|  |  |  |  |
|---|---|---|---|
|  | No. 3, Block D, Suite 3, Daqing Road, Modern Agriculture Park, Fengxian District, Shanghai | Previously the address for No. 41 was No. 3. No. 41 is now a kindergarten; prior to that it was a technical school and a middle school. The office of the Community Residents' Committee located nearby never heard of the company Yidatong and one member became borderline irate by the suggestion that Yidatong could be located at the same address as the school. |  |

We subscribed to NQ's paid mobile apps via carrier billing on 17 different prepaid SIMs in order to see whether YDT shows up as the SP. Unsurprisingly, it did not. The results of our attempts are below.



| Operator | Province | SP No. | Service Provider |
|---|---|---|---|
| Mobile | Jiangsu, Suzhou | 1065800829 | UMPay |
| Mobile | Shanghai | 1065800829 | UMPay |
| Mobile | GuangDong, Guangzhou | 1065800829 | UMPay |
| Mobile | Beijing | 1065800829 | UMPay |
| Mobile | Sichuan, Chengdu | 1065800829 | UMPay |
| Mobile | HeilongJiang, Qiqihaer | 1065800829 | UMPay |
| Mobile | Hubei, Wuhan | 1065800829 | UMPay |
| Mobile | Fujian, Putian | 1065800829 | UMPay |
| Mobile | Shandong, Dezhou | 1065800829 | UMPay |
| Mobile | JiangSu, Suzhou | 1065800829 | UMPay |
| Mobile | HeilongJiang, Suihua | 1065800829 | UMPay |
| Telecom | Shanghai | 106610794 | NQ |
| Telecom | JiangSu, Nanjing | 106610794 | NQ |
| Unicom | Beijing | 1065558237 | Unisk |
| Unicom | Shandong, Qinan | 1066558237 | Unisk |
| Unicom | Sichuan, Chengdu | 1065558237 | Unisk |
| Unicom | Shanghai | 1065558237 | Unisk |

We understand that the same SP generally handles billing for both prepaid and postpaid accounts for a given carrier and city or province.

The days sales outstanding from YDT stood at 167 days at December 31, 2012, despite the purported contract between NQ and YDT requiring settlement within 30 days.[17] This contradiction affirms our conclusion that YDT is a sham counterparty. The DSO mismatch with

[17] NQ 2012 20-F, Exhibit 10.11, p. 6. In addition, an Agreement between NQ and China Mobile also has terms of 45 days. NQ 2012 20-F, Exhibit 10.13, p. 8.

the contractual requirement is one of several data points we identified evidencing that NQ's audit is materially deficient. (See *NQ's Filings Make Clear that PwC's Audits Were Sloppy* for the discussion of the myriad audit failures.)

The high DSO from YDT does not relate to international (i.e., non-PRC) business, and therefore is not subject to payment terms greater than 30 days. NQ executed an agreement with YDT for international business in April 1, 2010 "that provides for up to one calendar month" to pay; however, that agreement expired on March 31, 2012.[18] Aside from the issue of YDT not having an international department, NQ investor relations informs investors that all of YDT's purported revenue is from PRC revenues.

The contracts between NQ and YDT are sham contracts. NQ has executed two contracts for domestic business with YDT – one on April 1, 2010 and the other on June 1, 2012. In addition to YDT's failure to remotely adhere to the payment terms of the contract or provide a staff to carry out its purported duties, the following sloppy errors in the contracts exist because the contracts were never intended to govern a real business relationship.

- China Telecom was not included in the original contract, it was included in the second
- In the first contract, there was no mention of who owned the registered users. In the second contract, the registered users information and database were owned by both parties.
- The arbitration clause was drafted in a way that could make any arbitration award unenforceable because it lacked necessary (and standard) language regarding the execution of awards.

YDT's purported application lineup shows that even if someone were trying to operate it as a business, it would fall far short of generating the approximately $35 million total revenue NQ claims YDT generates as a SP. YDT does not appear to represent any remotely in-demand products or provide any service of economic substance. A review of YDT's website shows an unimpressive portfolio of 12 products: three e-book readers, two video game simulators, two products from NQ, Microsoft's Mobile MSN, and the ever essential "Network Clock" application.

NQ and YDT have a history of suspect financial dealings. YDT received "advances" from NQ each year between and including 2007 to 2011 in amounts totaling approximately $5.0 million.[19] It is stunning that NQ's auditor has not looked closely at YDT.

The claim that NQ would have needed to work with YDT does not hold water. YDT is supposed to be a "Service Provider" ("SP"), which is a company that the Ministry of Industry and Information Technology ("MIIT") licenses to provide "value added telecommunication services" through mobile phone carrier billing. In the past, SPs aggregated content from mobile "Content Providers" ("CP"), and provided it to carriers. The content was 2G content, such as ringtones and SMS alerts. At the time, CPs had no way beside carrier billing to charge users, and carriers did not yet have their own app stores. Around 2006, China's SPs began to die out as content

[18] NQ 2012 20-F, Exhibit 10.10.

[19] 2011 IPO prospectus, pp. F-25,F-26, Notes 5 and 8

costs went up because the content was more data-rich, and carriers launched their own content platforms. The late 2000s became even tougher for SPs because of the proliferation of direct-to-CP payment options, such as Alipay. Alipay generally allows CPs to keep about 95% of the revenue, versus 60% to 80% for carrier billing through SPs. In order to determine how relevant the SP model is, we called approximately 300 SPs from a list of 1,800 SPs provided by MIIT. Approximately 50% of the SPs are out of business.

All of these facts beg the question "Why would NQ rely on SPs when SPs are dying businesses, and NQ could keep more money billing users directly?" Two more facts make this question even more important. NQ received its own SP license from MIIT in 2007, and thus would have no reason to deal through a tiny SP that is in perpetual need of interest-free loans from NQ.[20,21] NQ's investee company, and as of 2012, wholly-owned subsidiary, FL Mobile, received its Beijing SP license in 2010.[22] The answer to the question posed is that YDT is not a real company. Its purpose is to assist NQ in defrauding investors.

## YDT is really NQ.

In August, 2013, NQ blatantly lied to investors about the nature of its relationship to YDT. NQ was responding to a limited circulation research report that raised a number of questions about the Company, including its relationship with YDT.[23] YDT is one of the worst disguised related parties we have encountered in our years of trawling the sewers of US-listed China companies. The key is YDT's 75% owner, Ms. Rong Xu. Ms. Xu also previously worked at NQ.

YDT is clearly not a separate business from NQ. Undisclosed related parties are essential elements of China fraud.

- As of December 2011, the Guangdong branch of China Mobile showed YDT and NQ both as being based at NQ's Beijing office, with the same phone numbers, and the same contact person (Chen An An). [24]

- A list of service providers that China Mobile publishes for Fujian province listing of Service Providers show that YDT's telephone and fax numbers are (tel) 010-8565-5555 and (fax) 010-8565-5518. NQ's Chinese webpage lists those very same numbers as it main numbers on its Contact page.[25,26]

- YDT's email server is the exact same server as NQ's.

[20] https://tsm.miit.gov.cn/pages/EnterpriseSearchList_Portal.aspx?type=1&keyword=北京网秦天下科技&pageNo=1

[21] NQ 2011 IPO prospectus, p. 123, reads "Net revenues generated directly from China Mobile, as a percentage of our total net revenues, were 28% in 2008, 48% in 2009 and 10% in 2010."

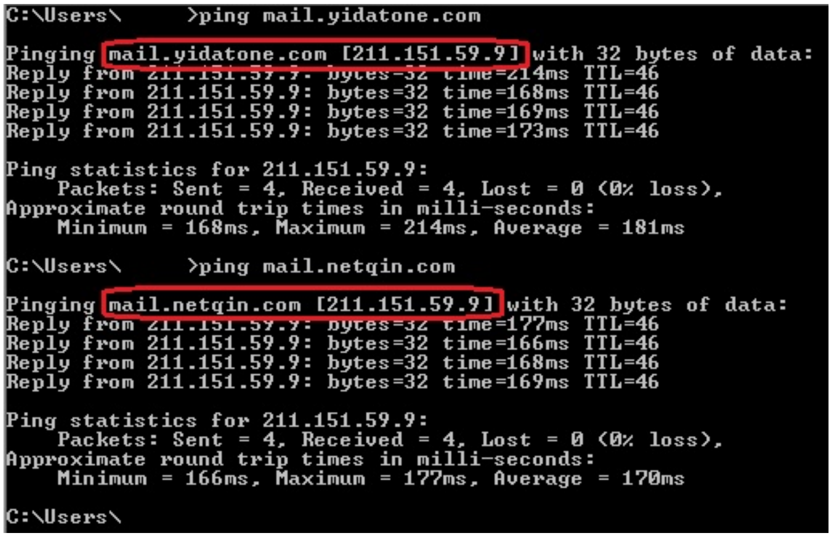
[22] http://www.miit.cc/verifyseal/105264.

[23] J Capital Research, "NQ Not At Any Price," July 31, 2013.

[24] Available as a downloadable spreadsheet at: http://gd.10086.cn/mwin/attachFileServlet?attachid=601100101410

[25] http://www.fj.monternet.com/image/fj/ad/splist/sms12.htm

[26] http://cn.nq.com/about/#tab5



```
C:\Users\      >ping mail.yidatone.com

Pinging mail.yidatone.com [211.151.59.9] with 32 bytes of data:
Reply from 211.151.59.9: bytes=32 time=214ms TTL=46
Reply from 211.151.59.9: bytes=32 time=168ms TTL=46
Reply from 211.151.59.9: bytes=32 time=169ms TTL=46
Reply from 211.151.59.9: bytes=32 time=173ms TTL=46

Ping statistics for 211.151.59.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 168ms, Maximum = 214ms, Average = 181ms

C:\Users\      >ping mail.netqin.com

Pinging mail.netqin.com [211.151.59.9] with 32 bytes of data:
Reply from 211.151.59.9: bytes=32 time=177ms TTL=46
Reply from 211.151.59.9: bytes=32 time=166ms TTL=46
Reply from 211.151.59.9: bytes=32 time=168ms TTL=46
Reply from 211.151.59.9: bytes=32 time=169ms TTL=46

Ping statistics for 211.151.59.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 166ms, Maximum = 177ms, Average = 170ms

C:\Users\
```

- The landline customer service number YDT provided to the Ministry of Information Industry and Telecommunications ("MIIT") is NQ's customer service number – NQ customer service representatives answer this phone when dialed.[27]

- Yidatong and NQ gave a Zhejiang government registry the same employee, Wang Qiu, as the official contact person. Wang Qiu must be a NQ employee, as both entities once again used NQ's phone number as the contact number.[28]

- The company information sheet in YDT's Shanghai SAIC files gives a NQ email address as the email contact: xuying@netqin.com. (Net Qin is NQ's former name, and netqin.com is one of NQ's domains.)

- NQ has repeatedly provided interest free loans to YDT totaling approximately $5.0 million, despite YDT purportedly collecting money from carriers before sending a portion onward to NQ.

NQ also blatantly lied about the extent of YDT's majority owner, Ms. Rong Xu's, involvement with NQ, including the dates on which she became involved with NQ, and when she left. NQ's response stated the following: [29]

- Ms. Xu worked at NQ for less than six months, as marketing director, and then left NQ in 2007 in order to buy her stake in YDT;
- YDT is a separate and completely independent business from NQ; and
- NQ accounts for only 60% of YDT's revenue.

NQ has taken pains to convince investors that there was no overlap between Ms. Xu's time at NQ and YDT. In reality, Ms. Xu's involvement with NQ is not just overlap – it is entanglement.

[27] http://bzxx.miit.gov.cn:8080/datainfo/miit/miit10079Details.jsp?affairl1=18
[28] Source: Website of Zhejiang Communications Administration: http://www.zca.gov.cn
[29] NQ "Response to J Capital Report, 'NQ Not At Any Price,'" August, 2013.

- Ms. Xu became involved with YDT far earlier than when NQ claims she left. In February 2006, Ms. Xu is shown as YDT's Executive Director – over one year before NQ claims she left in order to join YDT.[30] (Executive Director is the title commonly used when a company is small and only has one director.)

- Ms. Xu was director of a company that came to own 25% of NQ in 2006. In November 2006, a company of which Ms. Xu was (and still is) a director, Yiteng Beijing Technology Co. Ltd. came to own 25% of NQ.[31] One of the other Yiteng directors and shareholders is Ma Jun. Ma Jun is Ms. Xu's co-shareholder at YDT.

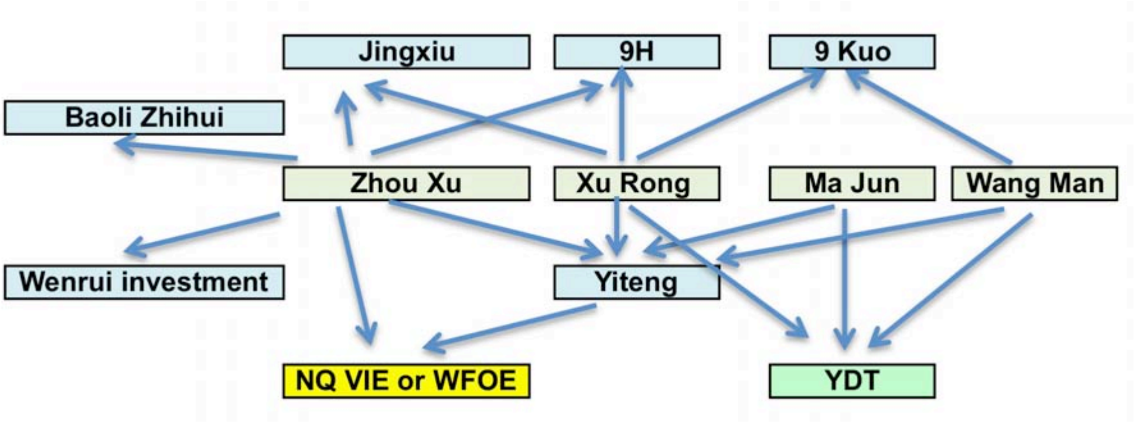
  It is important to note that one of the present Yiteng shareholders is NQ co-founder Mr. Xu Zhou.[32] Mr. Zhou and Ms. Xu appear to have an exceptionally close relationship, which is essential to understanding her ongoing entanglement with NQ. Strangely, the month after Yiteng became a shareholder, Yiteng transferred its ownership to Mr. Zhou and three other individuals. We do not know how to interpret these actions, but it is clear that Ms. Xu is part of the inner circle of NQ, and not just the marketing advisor NQ claimed. One theory we have is that these people were figuring out how to structure the NQ fraud, and had a number of fits and starts.

- Ms. Xu became YDT's Legal Representative in February 2007; however, NQ awarded her stock options for her "services" in a company that was not established until March 14, 2007.[33,34]

- Ms. Xu was still a Senior Vice President at NQ well into 2008, approximately one year after NQ claims she left. A May 20, 2008 Sina.com news article about Red Cross benefit for earthquake victims shows a picture of NQ Senior Vice President Ms. Rong Xu. She was holding up a NQ sign as presented a donation.

The following is a relationship graph showing part of the web of NQ inner circle members:

[30] It is likely that she was a shareholder of YDT at this time, but our SAIC files do not show when she became a shareholder.
[31] It owned 25% of Beijing NQ Technology Co. Ltd.
[32] http://ir.nq.com/phoenix.zhtml?c=243152&p=irol-govboard
[33] NQ 2011 20-F, p. 10.
[34] e424b4, p. F-7



As shown in the graph above, Ms. Xu is involved in three companies with NQ co-founder and director Zhou Xu. It appears that Mr. Zhou and Ms. Xu presently share office space – we found an employment ad 9H placed in August 2013 in which the workplace address is the same as Mr. Zhou's office at Jingxiu. The two had an endearing microblog exchange just prior to NQ's IPO:

> Mr. Xu Zhou, 5/3/2011:
>
> Dear brothers and sisters, after sharpening our blade for ten years, today we entered NYC, my heart is pounding, awash in emotion, the great dream in my heart, friends fighting together shoulder by shoulder, there glorious future is before us, and in '13 you will see 9H.
>
> > Ms. Rong Xu reply, 5/4/2010:
> >
> > 5/5, IPO day in New York, overflowing with excitement, the red five-starred banner waving in the wind, and the traders are grinning. Family and dear friends lend support, keep the price up throughout the night, keep the numbers across screen continuously flashing green. We are rejoicing. We are moving down the path to success, a brilliant future is dawning - -- 9H is next, go go go!

In reality, NQ's carrier billing channel generated $2.5 million to $7.7 million in 2012, versus the $27.9 NQ purports.

## NQ's Third Party Payment Channel is Non-Existent.

NQ's third party payment channel is non-existent and its China payment portal is purely cosmetic. We therefore extrapolate that this channel provides no revenue to NQ. We tried 59 times to make payments to NQ through third party payment services via NQ's payment portal (http://pay.nq.com), such as Alipay, TenPay, and banks between September 26th and October 18th. We were unsuccessful each time. (Note that Alipay and Tenpay are China's two largest third party payment services.)

We called Alipay and TenPay customer service twice for assistance, and none of them were able to make NQ's payment portal work. They all confirmed that the problem is with NQ, not their service. Alipay customer service stated that NQ is not a partnering merchant, which contradicts NQ's claim that it partners with Alipay.[35] NQ also claims that Yeepay, which is not shown on NQ's site, is a payment partner. Yeepay confirmed that NQ is not a partner either. It is easy for businesses in China to open accounts with Alipay and Yeepay, and we are left to conclude that NQ deliberately avoids doing so.

The NQ payment portal's lack of functionality is clear affirmation that NQ is a fraud. The cosmetic portal calls to mind John Hempton of Bronte Capital's exposé of Universal Travel Group (de-listed, formerly UTA). UTA had claimed to be one of the largest online travel booking sites in China. In reality, it was a Zero. Hempton attempted to use the slick-looking website to book travel, but was unable to complete his purchase because the website had no functionality. It was also purely cosmetic, and designed to fool US investors into thinking the business was real. NQ's portal appears to serve the same purpose – to provide legitimacy at a glance to investors and to its auditor. It does not process payments, and NQ's customers have not noticed because, by and large, they do not exist.

In committing fraud, it can be almost as important to avoid legitimate transactions as to record fake ones. We theorize that the reason NQ's payment portal does not work is that it would make it more difficult to fool its auditor if NQ were receiving legitimate payments from these payment processors, but in the trifling amounts that NQ would generate. If NQ is showing its auditor forged transaction documents from these payment processors, tiny monthly payments from the same payers hitting NQ's account might get the auditor's attention. Bernard Madoff claims to have executed no real trades in his fraud – likely for this reason.[36]

Alexa data evidencing minimal traffic to the payment portal shows that nobody besides short sellers noticed the problem, despite NQ claiming to have approximately six million paying customers in China. We did not find any versions of NQ apps that allow for payment through third party payment processors. It is extremely unlikely that NQ has partnered directly with banks for payments because that would put NQ further ahead of most of China's third party payment processors.

We therefore extrapolate that the third party payment channel generates an immaterial amount of revenue for NQ.

NQ's claims that its security apps are on approximately 55% of smart phones in China is patently false.[37] Two independent market research firms have pegged NQ's market share as less than 35% - often much less.[38] Our own surveys conducted in three Tier 1 cities, one Tier 3 city, and one Tier 4 city, yield market share of only 1%. We estimate that NQ has no more than 250,000 (300 million smart phones times 1.4% times 50% active user ratio times 10% paying user ratio paying users in China, versus the approximately six million it purports to have.

[35] NQ Mobile Investor Presentation 20130528, p. 13.

[36] http://en.wikipedia.org/wiki/Madoff_investment_scandal

[37] 2012 20F.

[38] iiMedia (Q2 2013) and RedTech (January 2011).

## NQ's China prepaid card channel does not contribute materially to revenue.

The purported combined amount of third party processor and prepaid card revenue in 2012 was somewhere between US$4 million to $10 million.[39] NQ does not break out how much was attributable to cards, versus third party channels. (Transparency is the enemy of fraud.) We concluded that third party payment channels contribute immaterial amounts of revenue. We conclude the same for NQ's prepaid card channel.

Prepaid cards consisted of scratch off cards and activation codes. Based on NQ customer service's difficulty in directing us to prepaid vendors in major cities, and our pre-installation channel checks, which show minimal penetration for NQ, we are skeptical that many (if any) retailers in China have access to NQ's access codes via automated systems or DVDs. Moreover, after we found the cards, we discovered that NQ only allows an account holder to use a prepaid card one time before being converted to carrier billing. That fact alone ensures that prepaid card revenue is insignificant.

[39] Senior management comment.

### Want to stump NQ customer service? Ask them where to buy prepaid cards in Beijing, Shanghai, or Guangzhou.

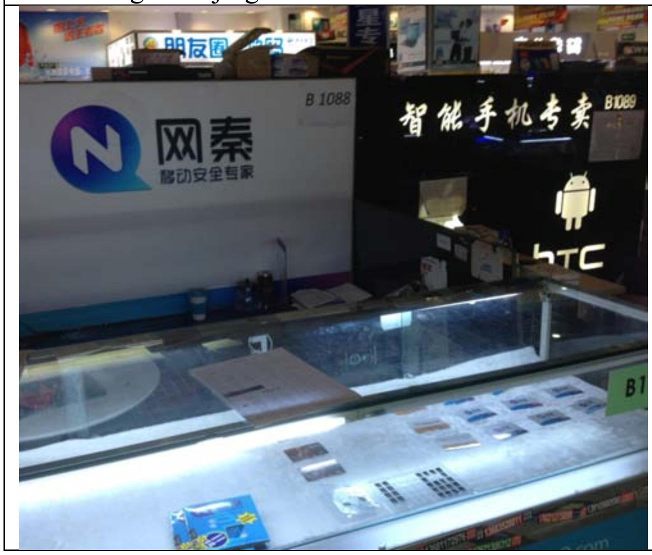
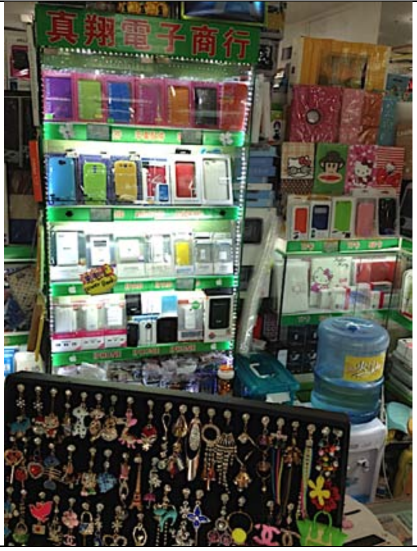
WHEEL OF EXCUSES
"I'm Not Supposed to talk about that."
DENIED
"Please try a different prepaid card."
NO SERVICE
"Try again tomorrow

We made four calls to customer service to inquire about where to buy prepaid cards in Beijing, Shanghai, Shijiazhuang (a large city near Beijing), and Guangzhou. In every case, including for Beijing (NQ's headquarters), customer service was unaware of whether there were sellers in those cities, and if so, who they are or where they were located. Prior to October 14, 2013, customer service was willing to go the extra mile to help find them, in two instances we received follow up calls/texts from customer service with more information. On October 10th, we received a text back from NQ customer service advising us of the location where we could buy the cards in Guangzhou. We received a separate call back from NQ's customer service regarding the Beijing distributor's retail location. We were told that the Beijing vendor is the only seller in the city, and that no distributors were operating in Shanghai or Suzhou. Additionally, their text message informed us that the Company was just in discussions with a distributor in Shijiazhuang (Hebei province) but that they were not able to sell cards at this time.

Despite apparently being NQ's exclusive vendor in Beijing, the seller is located in a spartan kiosk (B 1088) in the basement of a computer mall in the Zhongguancun section of Haidian

District, Beijing. (Of note, NQ's registered addresses for the WFOE and VIE are also in Zhongguancun.) This seller sells no products or services except for NQ cards, although the stand appears to be under common ownership with the kiosk on its right, which sells HTC, Android, Samsung, Sony, and Apple products.

Whereas the Beijing seller's kiosk embraced a minimalist aesthetic, the Guangzhou seller looks like a Costco, featuring a virtual cornucopia of products available for sale. The Guangzhou seller occupies a roughly 100 square foot stall in a computer mall on the first floor of the Haiyin Center in Guangzhou's Dongshan district, but every square inch is packed with merchandise, most of which is jewelry, scarves and cell phone accessories staffed by a father/daughter team.

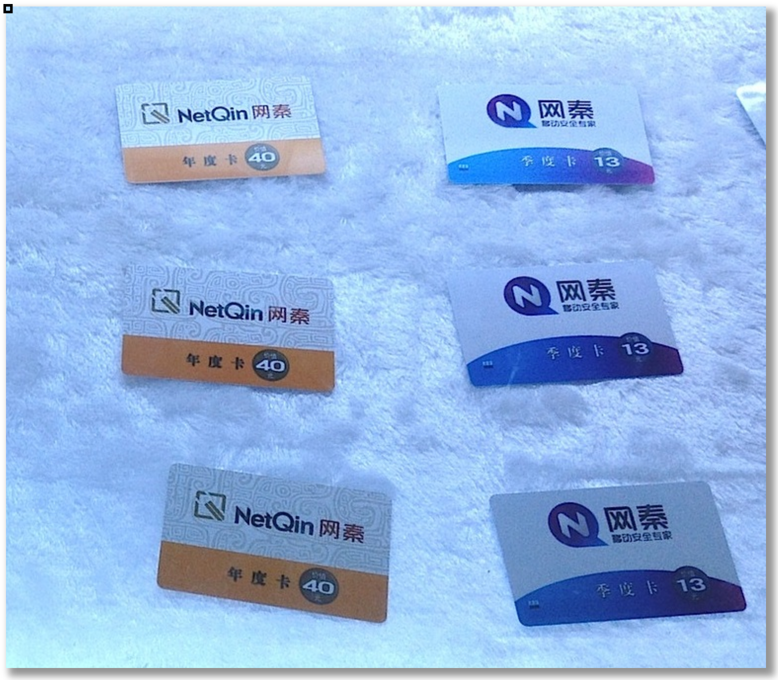
| NQ's China Prepaid Card Distributors in Beijing and Guangzhou | |
|---|---|
| Mr. Zhang's Beijing kiosk at B1088 | Zhen Xiang Electronics Store in Guangzhou |
|  |  |

### Sellers report very few sales.

We interviewed both vendors about the prepaid cards and learned that neither sells very many cards, and neither thought there were other vendors nearby.[40] The Guangzhou seller said she was not sure whether there were other distributors nearby, but did not think that many other retailers would be interested in selling these cards because the profit margin is low.

The Beijing seller echoed the Guangzhou seller, stating that while there were some sales, they do not sell a lot, and not for much profit. Mr. Zhang, the vendor, indicated people who do buy tend to be customers who already knew the product. Potential customers look and leave, apparently because they do not seem to understand the product. When asked how they came to sell NQ's prepaid cards, Mr. Zhang explained that they are old friends of the family, and they do it to "help them out".

[40] In China vendors of a specific product type typically group together and a popular product will quickly spread throughout a marketplace and to other similar markets as well.



The one-year prepaid NQ card (above, left) is a dead giveaway that hardly anybody ever buys these cards. The sell thru rate of these cards appears to be very low as the cards on the left still bear the old logo. NQ announced its new logo on June 11, 2011; therefore, these cards are well over two years old.[41]

The RMB 13 cards contain an interesting clue. The bottom left corner (difficult to see in the photo) contains the logo for the company that owns the kiosk, Beijing Huahui Yunzhen. Huahui appears to be a tiny company, yet NQ printed up numerous cards with that logo. That indicates that as insignificant as Huahui is, it occupies a rarified place in the pantheon of NQ's business partners.

While conducting this research we learned that NQ produces prepaid phone cards for China Mobile that enable anonymous calling – these are most likely to be used by telephone spammers. (See *The Farcical Side*.) On the right of Mr. Zhang's display case are branded prepaid NQ app cards, and in the middle are the unbranded anonymous calling cards.

NQ's lack of physical presence and virtually non-existent effort to update its merchandise, or build out its retail distribution are a clear sign their fraud is not focused on Chinese consumers, but rather US investors.

We proverbially poked NQ with a stick in the prepaid card area in order to observe how it reacts. As we expected, the reaction was interesting. An investor recently asked NQ investor relations (on our behalf) for names and addresses of some card and code resellers to secretly shop. At the same time, we were regularly calling customer service asking for card vendor information. Our

[41] http://www.chinascopefinancial.com/en/news/post/12668.html

impression is that customer service gets few calls overall, and that calls about prepaid cards are far rarer. Investor relations had seemed willing to arrange appointments with purported vendors, but as any investor who was burned in companies such as China Biotics and China MediaExpress will attest, such prearranged meetings can easily be frauds as well. The investor responded by asking for names and contact information so that we could secretly shop the vendors. Investor relations has not responded.

After asking investor relations for information on China prepaid card sales and sellers, customer service began refusing to discuss prepaid cards. October 14, 2013, we called customer service again to inquire about card sellers in other cities. The service representative said to us that they only provide technical support for the products and do not engage in sales, instead kept referring the customer to other sales channels. While on the surface this response appears relatively benign, their prior willingness to help check, identify, and contact us through follow-up communication was noticeably absent. We believe this was a result of a corporate directive to forbid further disclosure of details on the Company's prepaid card distribution (or lack thereof). This lasted for a few days. Then customer service changed its tune again, urging callers to buy prepaid cards for China Mobile, China Unicom, and China Telecom to pay for NQ apps. We believe that NQ was preparing for being exposed as having no real prepaid card sales by being able to retort "You do not understand our business; prepaid cards also include carriers' cards". To the extent this is true, it is a payment method only a few days old.

## NQ's online (lack of) card sales affirms our physical store checks that show the cards are obscure and immaterial to NQ revenue.

Taobao Marketplace is owned by Alibaba, and is a very large, reputable website in China similar to both Ebay and Amazon.[42] It dominates China's online B2C and C2C markets. We found only three sellers of NQ prepaid cards listed on Taobao Marketplace, and we believe two of these sites belong to the Beijing NQ Card Distributor. All three sites show meager sales at best. (Consistent with our view that the anonymous phone cards are not a Kosher business in China, there seem to be no NQ anonymous card sellers on Taobao.) One of the sellers, "NQ Card Agent" prominently displays a card with the old logo.

Taobao also provides seller data analytics. Below is the sales data for the three sellers. Beijing Huahui Yunzhen is the kiosk we visited in Beijing. The Beijing NQ card distributor sells not just NQ products but also cell phone recharge cards. Of the prior six months' 48 reported sales, only 11 sales were for NQ cards. NQ Card Agent's Taobao year-to-date sales are only 348.5 RMB, approximately $57.13 (fifty seven dollars and thirteen cents). Performance at their sister company was equally dismal. The Guangzhou kiosk has not made a single sale on Taobao since April of this year.

[42] http://en.wikipedia.org/wiki/Taobao

|  | NQ Card Agent<br>NQ点卡代理<br>(花辉云臻) |  | Beijing Huahui Yunzhen<br>北京华辉云臻 |  | Guangzhou Lixingjing<br>广州利行景 |  |
|---|---|---|---|---|---|---|
|  | NQ Card Sales (#) | NQ Card Sale Value (RMB) | NQ Card Sales (#) | NQ Card Sale Value (RMB) | NQ Card Sales (#) | NQ Card Sale Value (RMB) |
| Oct. | 0 | 0.0 | 0 | 0.0 | 0.0 | 0.0 |
| Sept. | 0 | 0.0 | 0 | 0.0 | 0.0 | 0.0 |
| Aug. | 1 | 32.0 | 0 | 0.0 | 0.0 | 0.0 |
| July | 2 | 42.5 | 1 | 18.5 | 0.0 | 0.0 |
| June | 2 | 64.0 | 7 | 154.0 | 0.0 | 0.0 |
| May | 6 | 103.5 | 2 | 50.5 | 0.0 | 0.0 |
| April | 0 | 0.0 | 2 | 59.8 | 0.0 | 0.0 |
| March | 1 | 10.5 | Data checked back to 4/23/2013 |  | 1.0 | 32.0 |
| Feb. | 1 | 32.0 |  |  | 0.0 | 0.0 |
| Jan. | 2 | 64.0 |  |  | 1.0 | 32.0 |
| Dec. | 0 | 0.0 |  |  | 0.0 | 0.0 |
| Nov. | Data checked back to 12/18/2012 |  |  |  | 3.0 | 978.5 |
| Oct. |  |  |  |  | 0.0 | 0.0 |
| Sept. |  |  |  |  | 6.0 | 1078.9 |
| Aug. |  |  |  |  | 12.0 | 3038.0 |
| July |  |  |  |  | 5.0 | 146.5 |
| June |  |  |  |  | 0.0 | 0.0 |
| May |  |  |  |  | 12.0 | 3141.9 |
| April |  |  |  |  | Data checked back to 5/14/2012 |  |
|  |  |  |  |  |  |  |
| Total | 15 | ¥348.50 | 12 | ¥282.80 | 40 | ¥8,447.80 |

A review of rough comparables on Taobao further suggests that the online market for premium or even moderately priced mobile phone software for Chinese consumers is very small, and pricing is competitive. (Free-ware remains by far and away the most popular choice.) Over the past month, the number one and number two leading sellers were retailing their paid software for just RMB 5 (US$0.82). Kasperski's RMB 1.3 (US$0.21) security software managed only three sales. All others posted numbers in low single digits or sold nothing at all.

NQ's physical and online presence in China is at best anemic. NQ's inability to cultivate a sales ecosystem suggests that neither retailers nor consumers are interested in selling or buying NQ products.

## NQ is an Obscure Company in China with Minimal Brand Recognition; Our Research Estimates that Fewer than 1.5% of Smart Phone Owners Presently have a NQ Security App.

Muddy Waters's survey-based market research estimates that NQ's actual share of the China security app market is 1.4%, versus NQ's purported approximate share of approximately 55%. Based on our research, we estimate that NQ has fewer than 250,000 paying customers in China, versus its claim of six million. (This yields revenue of approximately $2.5 million, versus the $32.2 million NQ purports to generate.) NQ, its competitor QIHU, and some market research firms have cited various market share studies that have very different results. NQ's latest claims are that its share of the China security app market is approximately 55%. On the other hand, QIHU claims that its market share is 70%.[43] We came across research by iiMedia that shows NQ's market share is only 7.2%.[44] We set out to settle the question of which research (if any) is likely to be accurate by conducting surveys of smart phone owners.

Our research shows that NQ's China market share claims of approximately 55% are ludicrous, as are its claims of having approximately six million paying users. Our surveys of over 800 respondents from five cities show that NQ's share of the China mobile security app market is only 1.4%. In contrast, Qihoo 360 Technology Co. Ltd. (NASDAQ: QIHU) has 73.5% market share in our survey, followed by Tencent Holding Ltd. (HK: 700) at 15.7%, Kingsoft Corp. Ltd. (HK: 3888) at 4.9%, and "other" at 3.8%.

As we show in the pie charts on the next page, NQ's (lack of) market share was remarkably consistent across the Tier 1, Tier 3, and Tier 4 cities. QIHU is dominant across all cities we surveyed, but has given more ground to Tencent in Tier 1 cities than in the Tier 3 and 4 cities we surveyed. Overall, 58.8% of respondents had some form of security, antivirus, or data protection software on their phones.

NQ might criticize our survey sample as being too small to be significant; however, this sample size is large enough to reject with 95% confidence a null hypothesis of NQ's market share being far, far lower than NQ claims. The key is the massive delta between what NQ claims and what we found. There is no way to bridge that gap.

NQ might criticize our survey sample as being geographically flawed – in other words, we did not conduct surveys in the markets in which NQ is strongest. This criticism would not hold water though. The product at issue is distributed over the mobile Internet. There are likely some variations in NQ's market share from city to city, but given the roughly 60 percentage point delta, rejecting our findings for geographical reasons would be a de facto argument that there are special places in China that are connected to a very different mobile internet. Moreover, NQ has refused to disclose any information on where in China it actually has market share. A long-oriented recently investor asked NQ investor relations director Matt Mathison for some – any – detail on where NQ's market presence is strongest. Mr. Mathison replied that NQ does not disclose this information. (Transparency is the enemy of fraud.)

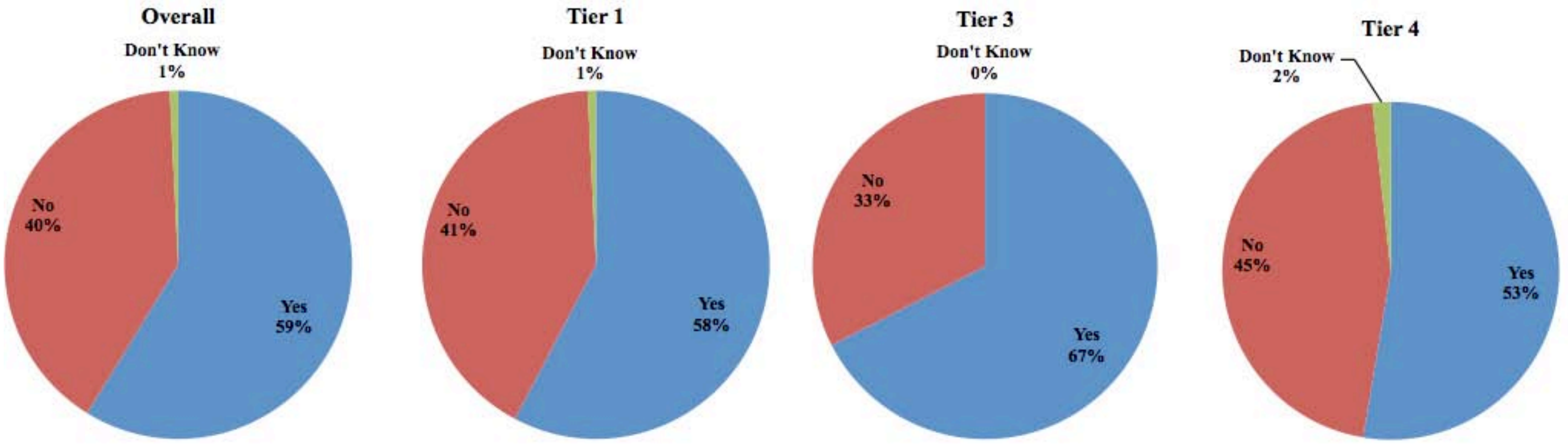
[43] QIHU 2012 20-F, p. 27.
[44] Q2 2013.

With NQ refusing to provide any detail on its China markets, we chose three of the four Tier 1 cities: Beijing (NQ's hometown), Shanghai, and Shenzhen. We then chose two cities in Zhejiang province as the respective representative Tier 3 and Tier 4 cities: Ningbo and Huzhou. We chose Zhejiang because it was the most pro-NQ means we could think of doing the survey. NQ previously announced its first major nationwide sales promotion and established an agreement with the Zhejiang-branch of China National Postal and Telecommunications (PTAC) to pair up NQ software with 3G cell phones PTAC was distributing.[45] Ningbo (about 2.5 hours drive from Shanghai) has a population of 7.6 million, 3.5 million of whom reside in the urban areas.[46] Ningbo's 2011 per capita GDP was RMB 79,500 (Shanghai's was RMB 82,600).[47] Huzhou (about one hour drive from Shanghai) population is 2.6 million, with an urban population of 1.1 million.[48] Huzhou's 2011 per capita GDP was RMB 58,500.[49]

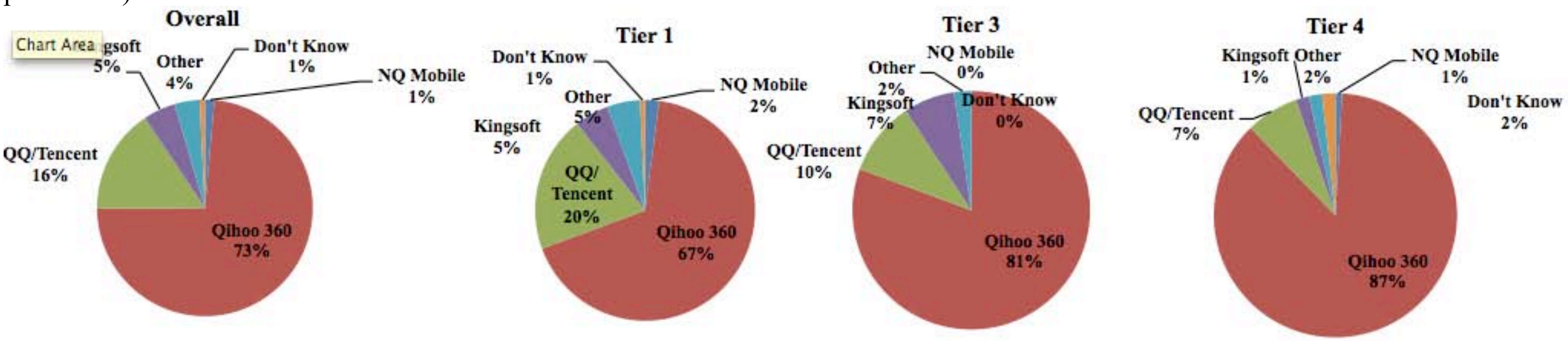
If NQ wants to dispute our conclusion that it has laughably low penetration rates in China, actions speak louder than words. Investor relations should refrain from hemming and hawing about the samples we have taken, and tell us exactly where in China NQ has high penetration rates. Anything else NQ says to try to refute this point is a waste of toner.

[45] "3G leads to an explosion in the security market! Cell phone security software suites are on fire!," July 22, 2009, http://www.enet.com.cn/article/2009/0722/A20090722505055.shtml.
[46] http://en.wikipedia.org/wiki/Ningbo
[47] http://en.wikipedia.org/wiki/List_of_prefecture-level_cities_by_GDP_per_capita
[48] http://www.at0086.com/Huzhou/
[49] http://en.wikipedia.org/wiki/List_of_prefecture-level_cities_by_GDP

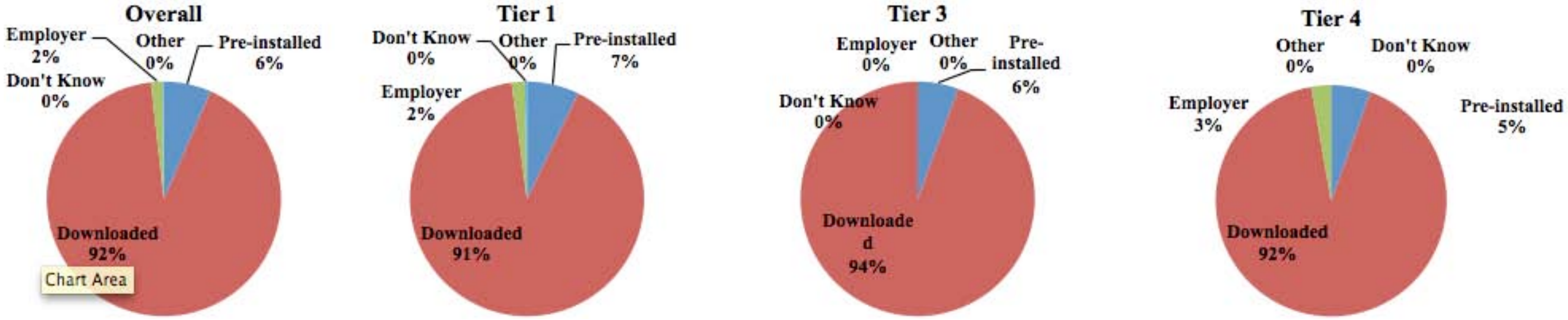
Q: Does your mobile phone have any security, antivirus, or data protection software? (Multiple choice.)



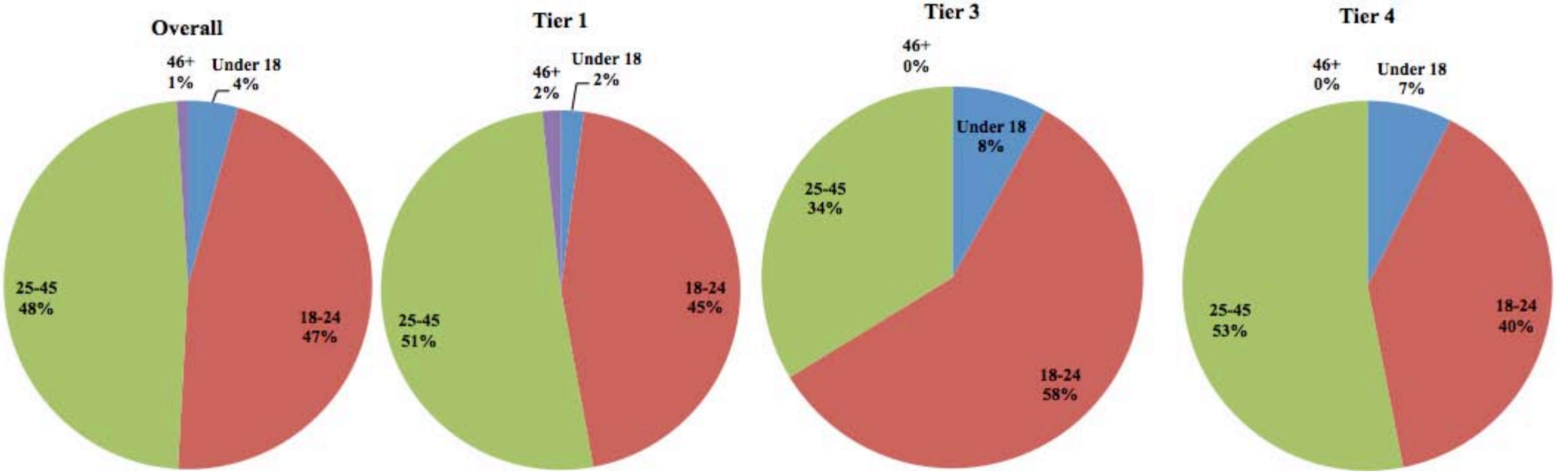
Q: Which company's security, AV, data protection app is on your mobile phone? (Multiple choice, more than one selection permitted.)



Q: How was the app installed on your phone?  (Multiple choice.)



Q: What is your age?  (Multiple choice.)



Note that pre-installations account for only 6.5% of the apps on phones. On one hand, this suggests that pre-installations are irrelevant to market share. Another interpretation is that NQ's claims about its pre-installations are exaggerated. Based on our retail channel checks (infra), NQ is just as obscure at retail as on users' smartphones.

NQ's massively exaggerated claims about its market share started with a Frost & Sullivan report from late 2010 or early 2011 (the period during which NQ was in late stage preparations for its IPO).[50] The Frost report estimated that NQ had 67.7% market share in 2010. We believe that NQ paid for this report, and that the research methodology did not involve collecting data from users. We believe that the methodology instead was a combination of accepting NQ's data at face value, and speaking with industry parties friendly to NQ. Since then, NQ has primarily relied on research from a firm called Sino MR to support its market share claims. We do not believe the Sino MR research is remotely credible, as we are skeptical of Sino MR's ability to manage the conflict of interest – let alone keep a straight face when discussing conflict management.

## Retailer Visits Further Confirm that NQ has a Sliver of the Market Share it Claims.

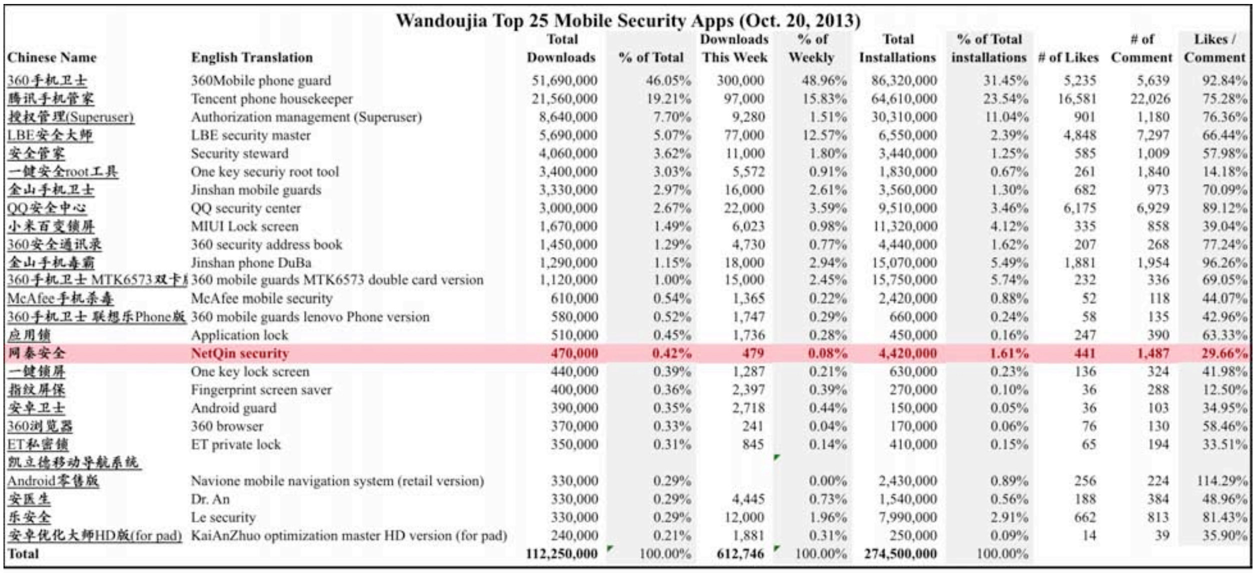
Our examination of 113 phones at various stores across five cities in China concluded that NQ's pre-installation or bundled software channel is close to being non-existent as of Q3 2013 in Beijing, Guangzhou, Shanghai, Shenzhen, and Shijiazhuang (Hebei province). This does not mean that this channel did not exist before, but it is actually the behavior of software providers such as NQ (the 315 incident) that has resulted in less software being bundled because handset manufacturers and operators have realized bundling can damage their businesses. It is also easier than ever before to download apps, and some handset manufacturers have their own branded apps.

54.0% of the phones we checked had no anti-virus software on them, and only four out of 113 phones had NQ installed. Two of the phones (Samsung) were bought in Beijing and had originally been display phones. All other phones of the same model in that store had no NQ software bundled with it. All of the NQ bundled phones with the exception of one had also had additional antivirus software on it from Tencent. We therefore theorize that NQ employees paid store employees to install the software.

## China App Store Download Data Confirm that NQ has a Sliver of the Market Share it Claims.

The below download numbers come from two of China's largest independent app stores, Wandoujia and 91 Zhu Shou, and show that NQ has miniscule market share. NQ's "Likes" as a percentage of comments (29.66%) is among the lowest on the list, and compares unfavorably to QIHU's 360 Mobile Phone Guard at 92.84%.

[50] http://www.netqin.com/upLoad/File/en/China%20Mobile%20Security%20Market%20Research%20Report_final.pdf



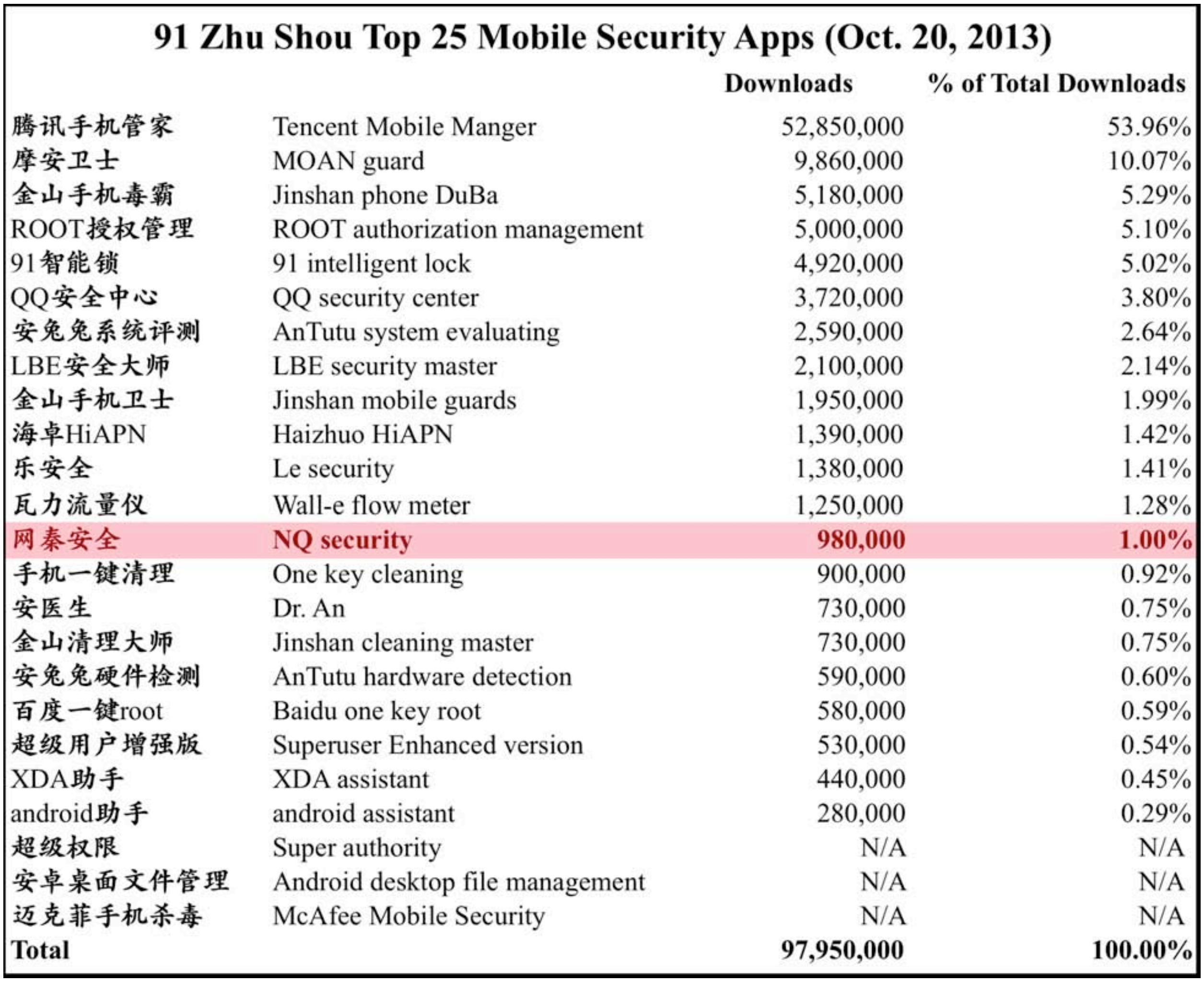
Wandoujia Top 25 Mobile Security Apps (Oct. 20, 2013)

| Chinese Name | English Translation | Total Downloads | % of Total | Downloads This Week | % of Weekly | Total Installations | % of Total installations | # of Likes | # of Comment | Likes / Comment |
|---|---|---|---|---|---|---|---|---|---|---|
| 360手机卫士 | 360Mobile phone guard | 51,690,000 | 46.05% | 300,000 | 48.96% | 86,320,000 | 31.45% | 5,235 | 5,639 | 92.84% |
| 腾讯手机管家 | Tencent phone housekeeper | 21,560,000 | 19.21% | 97,000 | 15.83% | 64,610,000 | 23.54% | 16,581 | 22,026 | 75.28% |
| 授权管理(Superuser) | Authorization management (Superuser) | 8,640,000 | 7.70% | 9,280 | 1.51% | 30,310,000 | 11.04% | 901 | 1,180 | 76.36% |
| LBE安全大师 | LBE security master | 5,690,000 | 5.07% | 77,000 | 12.57% | 6,550,000 | 2.39% | 4,848 | 7,297 | 66.44% |
| 安全管家 | Security steward | 4,060,000 | 3.62% | 11,000 | 1.80% | 3,440,000 | 1.25% | 585 | 1,009 | 57.98% |
| 一键安全root工具 | One key securiy root tool | 3,400,000 | 3.03% | 5,572 | 0.91% | 1,830,000 | 0.67% | 261 | 1,840 | 14.18% |
| 金山手机卫士 | Jinshan mobile guards | 3,330,000 | 2.97% | 16,000 | 2.61% | 3,560,000 | 1.30% | 682 | 973 | 70.09% |
| QQ安全中心 | QQ security center | 3,000,000 | 2.67% | 22,000 | 3.59% | 9,510,000 | 3.46% | 6,175 | 6,929 | 89.12% |
| 小米百变锁屏 | MIUI Lock screen | 1,670,000 | 1.49% | 6,023 | 0.98% | 11,320,000 | 4.12% | 335 | 858 | 39.04% |
| 360安全通讯录 | 360 security address book | 1,450,000 | 1.29% | 4,730 | 0.77% | 4,440,000 | 1.62% | 207 | 268 | 77.24% |
| 金山手机毒霸 | Jinshan phone DuBa | 1,290,000 | 1.15% | 18,000 | 2.94% | 15,070,000 | 5.49% | 1,881 | 1,954 | 96.26% |
| 360手机卫士 MTK6573双卡 | 360 mobile guards MTK6573 double card version | 1,120,000 | 1.00% | 15,000 | 2.45% | 15,750,000 | 5.74% | 232 | 336 | 69.05% |
| McAfee手机杀毒 | McAfee mobile security | 610,000 | 0.54% | 1,365 | 0.22% | 2,420,000 | 0.88% | 52 | 118 | 44.07% |
| 360手机卫士 联想乐Phone版 | 360 mobile guards lenovo Phone version | 580,000 | 0.52% | 1,747 | 0.29% | 660,000 | 0.24% | 58 | 135 | 42.96% |
| 应用锁 | Application lock | 510,000 | 0.45% | 1,736 | 0.28% | 450,000 | 0.16% | 247 | 390 | 63.33% |
| 网秦安全 | NetQin security | 470,000 | 0.42% | 479 | 0.08% | 4,420,000 | 1.61% | 441 | 1,487 | 29.66% |
| 一键锁屏 | One key lock screen | 440,000 | 0.39% | 1,287 | 0.21% | 630,000 | 0.23% | 136 | 324 | 41.98% |
| 指纹屏保 | Fingerprint screen saver | 400,000 | 0.36% | 2,397 | 0.39% | 270,000 | 0.10% | 36 | 288 | 12.50% |
| 安卓卫士 | Android guard | 390,000 | 0.35% | 2,718 | 0.44% | 150,000 | 0.05% | 36 | 103 | 34.95% |
| 360浏览器 | 360 browser | 370,000 | 0.33% | 241 | 0.04% | 170,000 | 0.06% | 76 | 130 | 58.46% |
| ET私密锁 | ET private lock | 350,000 | 0.31% | 845 | 0.14% | 410,000 | 0.15% | 65 | 194 | 33.51% |
| 凯立德移动导航系统 Android零售版 | Navione mobile navigation system (retail version) | 330,000 | 0.29% |  | 0.00% | 2,430,000 | 0.89% | 256 | 224 | 114.29% |
| 安医生 | Dr. An | 330,000 | 0.29% | 4,445 | 0.73% | 1,540,000 | 0.56% | 188 | 384 | 48.96% |
| 乐安全 | Le security | 330,000 | 0.29% | 12,000 | 1.96% | 7,990,000 | 2.91% | 662 | 813 | 81.43% |
| 安卓优化大师HD版(for pad) | KaiAnZhuo optimization master HD version (for pad) | 240,000 | 0.21% | 1,881 | 0.31% | 250,000 | 0.09% | 14 | 39 | 35.90% |
| Total |  | 112,250,000 | 100.00% | 612,746 | 100.00% | 274,500,000 | 100.00% |  |  |  |

We estimate that about 80% of the comments on Wandoujia regarding NQ are negative.  Some of the more commonly used adjectives are "gangster (流氓)", "brute (禽兽)", "garbage (垃圾)".[51]  A number of commenters wondered how NQ has been able to survive.  Here are some of the ones that we found more pertinent to show users' opinion of the product.

Note that 91 Zhu Shou is owned by BIDU, which has an acrimonious relationship with QIHU, which is likely the reason that QIHU is not offered in the store.

[51] One of our native Chinese speakers learned some new unflattering English adjectives by reading the reviews, and having to translate them.



91 Zhu Shou Top 25 Mobile Security Apps (Oct. 20, 2013)

| | | Downloads | % of Total Downloads |
|---|---|---|---|
| 腾讯手机管家 | Tencent Mobile Manger | 52,850,000 | 53.96% |
| 摩安卫士 | MOAN guard | 9,860,000 | 10.07% |
| 金山手机毒霸 | Jinshan phone DuBa | 5,180,000 | 5.29% |
| ROOT授权管理 | ROOT authorization management | 5,000,000 | 5.10% |
| 91智能锁 | 91 intelligent lock | 4,920,000 | 5.02% |
| QQ安全中心 | QQ security center | 3,720,000 | 3.80% |
| 安兔兔系统评测 | AnTutu system evaluating | 2,590,000 | 2.64% |
| LBE安全大师 | LBE security master | 2,100,000 | 2.14% |
| 金山手机卫士 | Jinshan mobile guards | 1,950,000 | 1.99% |
| 海卓HiAPN | Haizhuo HiAPN | 1,390,000 | 1.42% |
| 乐安全 | Le security | 1,380,000 | 1.41% |
| 瓦力流量仪 | Wall-e flow meter | 1,250,000 | 1.28% |
| **网秦安全** | **NQ security** | **980,000** | **1.00%** |
| 手机一键清理 | One key cleaning | 900,000 | 0.92% |
| 安医生 | Dr. An | 730,000 | 0.75% |
| 金山清理大师 | Jinshan cleaning master | 730,000 | 0.75% |
| 安兔兔硬件检测 | AnTutu hardware detection | 590,000 | 0.60% |
| 百度一键root | Baidu one key root | 580,000 | 0.59% |
| 超级用户增强版 | Superuser Enhanced version | 530,000 | 0.54% |
| XDA助手 | XDA assistant | 440,000 | 0.45% |
| android助手 | android assistant | 280,000 | 0.29% |
| 超级权限 | Super authority | N/A | N/A |
| 安卓桌面文件管理 | Android desktop file management | N/A | N/A |
| 迈克菲手机杀毒 | McAfee Mobile Security | N/A | N/A |
| **Total** | | **97,950,000** | **100.00%** |

NQ recently addressed the paucity of downloads in these stores with a non sequitur:

> "For example, if an analyst tried to verify market share data for handsets in China and surveyed 1000's of people in the streets of Beijing or Shanghai, they might find results that would show 65% of users have Samsung-branded phones while 35% have Apple's iPhone. One might conclude from this faulty sampling methodology that there is no way that Huawei, ZTE, Lenovo, or Xiaomi would have the kind of market share that actually exists." [52]

These two stores represent over 200 million downloads of security apps, including significant downloads of apps produced by the clear market leaders, QIHU and Tencent. Again, it seems NQ wants investors to accept that there are places in China with their own very special mobile internet, and users who are super motivated to seek out NQ.

[52] NQ "Response to J Capital Report Titled, 'NQ: Not At Any Price,'" August, 2013, p.2.

## NQ's SAIC Financials are Fraudulent, Leading to Fraudulent SEC Financials

NQ's SAIC financial statements largely match those in its SEC filings; however, NQ's SAIC financials are fraudulent. This means that NQ's SEC filing financials are also fraudulent. A company prepares its GAAP and tax financials from the same set of books. In the PRC, companies are required to file PRC GAAP financial statements to SAIC. If the SAIC financials are fraudulent, then the books from which they are drawn are as well. In the case of a US-listed public company, the fraudulent books form the basis for the SEC financials. Therefore, fraudulent SAIC financials tell us that SEC financials are also fraudulent.

Of course we know that NQ's financials are fraudulent from having observed the Yidatong fraud, customers' inability to pay through NQ's payment portal, NQ's miniscule prepaid card sales, and the barely-existent position NQ occupies in the China market. Putting those elements aside and assuming no pre-existing knowledge of NQ's fraud, NQ's SAIC financials contain significant indicia of fraud.

Chinese media called NQ's SAIC financials into question the day before NQ's IPO. The 21st Century Business Herald (often referred to as "The Wall Street Journal of China") published an article titled "Netqin investigation, the night prior to public listing - inflated sales proceeds".[53] The article noted that while NQ's 2009 SAIC financials matched its prospectus, its 2008 SAIC financials showed revenue that was only a fraction of what the prospectus claimed. (We presume that in the chaotic pre-IPO environment, the parties responsible for executing the fraud overlooked 2008 SAICs.)

Certain of NQ's tax disclosures and accounting are significant indicia of fraud and fraudulent SAIC financials. (These misses also evidence a sloppy audit – see *NQ's Filings Make Clear that PwC's Audits Were Sloppy*.)

Bungled tax treatment is common in China frauds. Accounting for a fraud is much harder than accounting for a legitimate business.[54] Business accounting is a largely rote exercise – accountants are merely documenting historical facts. On the other hand, fraud accounting requires imagination and the ability to organize a complex web of lies, on top of business accounting skills. Few book cookers are perfect, and one of the most common areas in which they make mistakes is in accounting for taxes on revenue and income. China's tax laws and regulations are complex and rapidly changing. There is a constant stream of national, provincial, and local preferences coming into effect and expiring. We noted significant tax accounting problems in frauds perpetrated by CCME, DGW, RINO, and TRE.

China frauds tend to claim tax preferences for which they are not eligible. One staple of audits in China is tax payment documentation. Frauds can forge payment documentation, but motivated auditors can spot forged tax payment docs if they diligently seek to confirm their

[53] "Netqin investigation, the night prior to public listing - inflated sales proceeds," *21st Century Business Herald*, March 26, 2011.
[54] Conversely, building a successful fraud is much easier than building a successful business.

authenticity. (Many China auditors are neither motivated nor diligent.) Another option frauds have is to actually pay taxes commensurate with their fraudulent financials. This method is obviously costly, and is often not worthwhile. The best method we have observed so far is to claim tax treatment that precludes the need to pay much in the way of tax. Many China auditors seem either to miss that the claimed preferences do not apply to their clients, or believe in a Guanxi Fairy that bestows extralegal tax treatment on the company from the local tax bureau.

After analyzing NQ's SEC filings and SAIC files, we believe that NQ made a number of tax errors in the filings for its Wholly Foreign-Owned Enterprise ("WFOE") NQ Beijing, FL Mobile, and NationSky because NQ's internal and SAIC financials are fraudulent. We explain those errors in Appendix B.

## NQ's Antivirus 7.0 Makes it Easy for the PRC Government and Hackers to Read Copious Amounts of Sensitive Data, and to Upload Malware to Users' Phones

MW engaged a team of top-flight specialized software engineers to analyze potential vulnerabilities in NQ's Antivirus 7.0. Both they and we were shocked a) at the amount of sensitive data (including location data) the app collects, b) by the fact that it sends much of this sensitive data to its server in China, c) by the fact that it also sends this data onward to a Chinese analytics company, d) that the uploaded data is extremely poorly protected (the engineers opined that the lack of protection could be deliberate), and e) that due to the lack of basic safeguards on downloaded data, users' phones can easily be loaded with malware by third parties. The elephant in this room of course is the Chinese government and "The Great Firewall of China" that reads and records all data going into and out of the country. The encryption AV 7.0 uses is pointless because it includes the key with the data it is encrypting, which is akin to leaving the key hanging out of a safe.

All mobile apps need to secure the transmission of information and the information being transmitted in order to provide basic protection to the user. This is typically accomplished by using standard technologies and techniques, some of which include HTTPS, SSL/TLS, and digitally signing the payload being transmitted. These techniques authenticate the server and the payload to the user, and prevent hackers from inserting themselves between the company and the users by using Man in The Middle attacks (MITM).

NQ Antivirus 7.0 does not adhere to these technologies, techniques or any other best practices. For some uploads, NQ "Gzips" the data and relies on an encoding technique using XOR (0x6e) instead of encryption. Without encryption, all of the data NQ admits to gathering in their privacy policy is uploaded to servers in China as near plain text. Other data is encrypted; however, it includes the key used to encrypt the data as a simple encoded string broadcast along with the payload, making the encryption nearly worthless. The data so "protected" includes:

> "SMS, MMS, Email, Contacts, call log, call conversation, location information, phone number, the IMSI, the IMEI, the ICCID, the ESN and the model of the phone, the

software that is installed and apps that are running in the phone, and information about analytics on your operation, your favorites, network connection and downloading."[55]

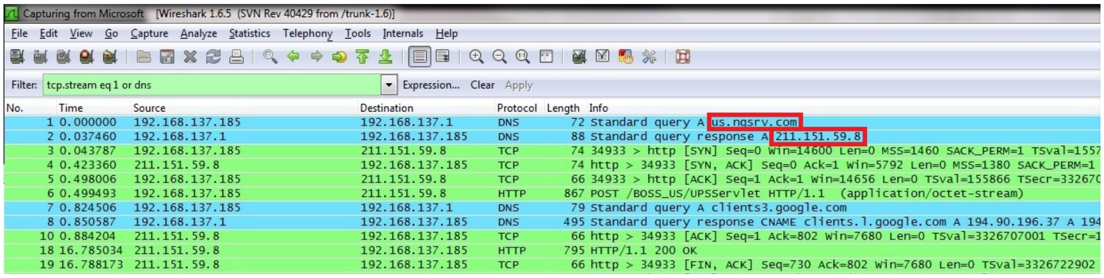
This means that all of the above user details are vulnerable to hackers sniffing the network between the user and NQ's Chinese servers, and the Chinese government.  NQ sends the data as well to TalkingData.net, which is a Chinese data analytics service.

When downloading data from the server, NQ does not use HTTPS or SSL. The result is that NQ users are vulnerable to Man in the Middle ("MITM") attack, a technique wherein a hacker impersonates the NQ server and intercepts all of the above listed data the app broadcasts. NQ does encrypt the data transmission from server to app, however it includes the key used to encrypt the data as a simple encoded string broadcast along with the payload, making the encryption nearly worthless.

By modifying their host file, our engineers were able to perform a MITM attack against themselves and discovered an additional special command that directs the application to download and execute any file from any server on the device.

Rounding out our analysis of the app / server communication protocol failures, we note that NQ does not sign its downloads. Without a digital signature, the user app has no way of authenticating the download or ensuring that it came from anyone other than NQ.

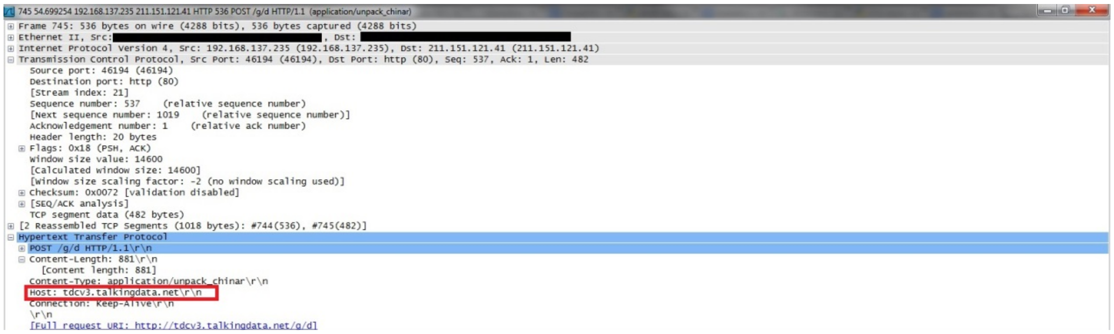
The engineers' report with details on the app, server and payload failures of NQ Antivirus 7.0 are available in Appendix C.



Filter: tcp.stream eq 1 or dns

```
No.    Time        Source            Destination       Protocol Length Info
     1 0.000000    192.168.137.185   192.168.137.1     DNS          72 Standard query A us.nqsrv.com
     2 0.037460    192.168.137.1     192.168.137.185   DNS          88 Standard query response A 211.151.59.8
     3 0.043787    192.168.137.185   211.151.59.8      TCP          74 34933 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1557
     4 0.423360    211.151.59.8      192.168.137.185   TCP          74 http > 34933 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1380 SACK_PERM=1
     5 0.498006    192.168.137.185   211.151.59.8      TCP          66 34933 > http [ACK] Seq=1 Ack=1 Win=14656 Len=0 TSval=155866 TSecr=33267
     6 0.499493    192.168.137.185   211.151.59.8      HTTP        867 POST /BOSS_US/UPSServlet HTTP/1.1  (application/octet-stream)
     7 0.824506    192.168.137.185   192.168.137.1     DNS          79 Standard query A clients3.google.com
     8 0.850587    192.168.137.1     192.168.137.185   DNS         495 Standard query response CNAME clients.l.google.com A 194.90.196.37 A 194
    10 0.884204    211.151.59.8      192.168.137.185   TCP          66 http > 34933 [ACK] Seq=1 Ack=802 Win=7680 Len=0 TSval=3326707001 TSecr=1
    18 16.785034   211.151.59.8      192.168.137.185   HTTP        795 HTTP/1.1 200 OK
    19 16.788173   211.151.59.8      192.168.137.185   TCP          66 http > 34933 [FIN, ACK] Seq=730 Ack=802 Win=7680 Len=0 TSval=3326722902
```

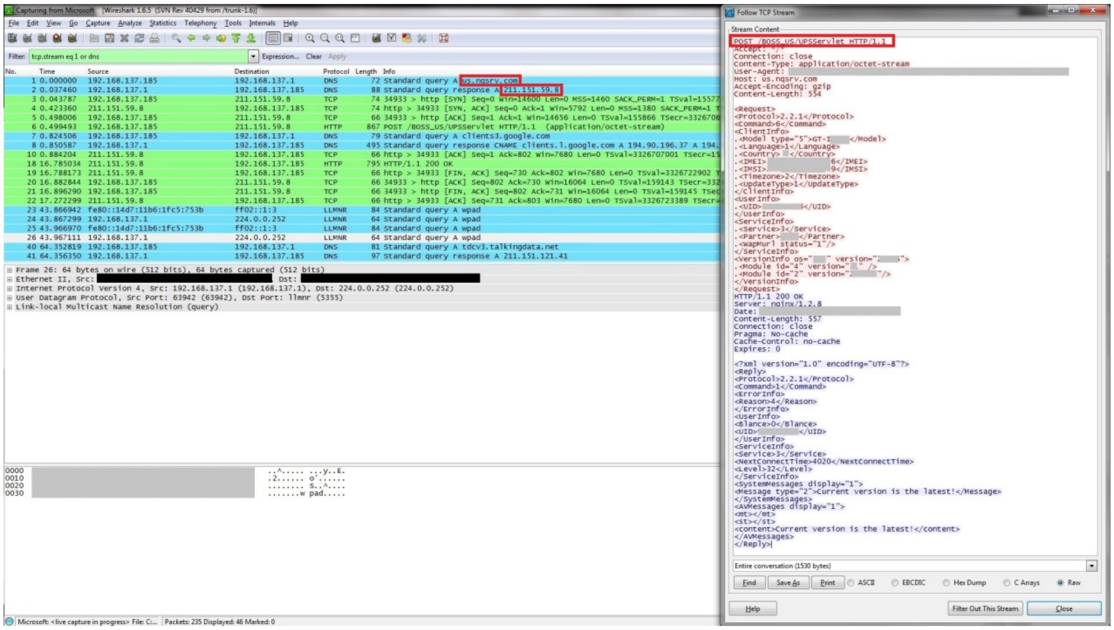
Data being sent to NQ's server in China



```
745 54.699254 192.168.137.235 211.151.121.41 HTTP 536 POST /g/d HTTP/1.1  (application/unpack_chinar)
⊞ Frame 745: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits)
⊞ Ethernet II, Src: [redacted], Dst: [redacted]
⊞ Internet Protocol Version 4, Src: 192.168.137.235 (192.168.137.235), Dst: 211.151.121.41 (211.151.121.41)
⊟ Transmission Control Protocol, Src Port: 46194 (46194), Dst Port: http (80), Seq: 537, Ack: 1, Len: 482
    Source port: 46194 (46194)
    Destination port: http (80)
    [Stream index: 21]
    Sequence number: 537    (relative sequence number)
    [Next sequence number: 1019    (relative sequence number)]
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x18 (PSH, ACK)
    Window size value: 14600
    [Calculated window size: 14600]
    [Window size scaling factor: -2 (no window scaling used)]
  ⊞ Checksum: 0x0072 [validation disabled]
  ⊞ [SEQ/ACK analysis]
    TCP segment data (482 bytes)
⊞ [2 Reassembled TCP Segments (1018 bytes): #744(536), #745(482)]
⊟ Hypertext Transfer Protocol
  ⊞ POST /g/d HTTP/1.1\r\n
  ⊟ Content-Length: 881\r\n
      [Content length: 881]
    Content-Type: application/unpack_chinar\r\n
    Host: tdcv3.talkingdata.net\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://tdcv3.talkingdata.net/g/d]
```

[55] http://www.nq.com/privacy

Data being sent to China-based analytics company Talking Data



Capturing from Microsoft   [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.stream eq 1 or dns
Expression... Clear Apply

```
No.  Time       Source                     Destination      Protocol Length Info
   1 0.000000   192.168.137.185            192.168.137.1    DNS       72 Standard query A us.nqsrv.com
   2 0.037460   192.168.137.1              192.168.137.185  DNS       88 Standard query response A 211.151.59.8
   3 0.043787   192.168.137.185            211.151.59.8     TCP       74 34933 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=15577
   4 0.423360   211.151.59.8               192.168.137.185  TCP       74 http > 34933 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1380 SACK_PERM=1 T
   5 0.498006   192.168.137.185            211.151.59.8     TCP       66 34933 > http [ACK] Seq=1 Ack=1 Win=14656 Len=0 TSval=155866 TSecr=3326706
   6 0.499493   192.168.137.185            211.151.59.8     HTTP     867 POST /BOSS_US/UPSServlet HTTP/1.1  (application/octet-stream)
   7 0.824506   192.168.137.185            192.168.137.1    DNS       79 Standard query A clients3.google.com
   8 0.850587   192.168.137.1              192.168.137.185  DNS      495 Standard query response CNAME clients.l.google.com A 194.90.196.37 A 194.
  10 0.884204   211.151.59.8               192.168.137.185  TCP       66 http > 34933 [ACK] Seq=1 Ack=802 Win=7680 Len=0 TSval=3326707001 TSecr=15
  18 16.785034  211.151.59.8               192.168.137.185  HTTP     795 HTTP/1.1 200 OK
  19 16.788173  211.151.59.8               192.168.137.185  TCP       66 http > 34933 [FIN, ACK] Seq=730 Ack=802 Win=7680 Len=0 TSval=3326722902 T
  20 16.882844  192.168.137.185            211.151.59.8     TCP       66 34933 > http [ACK] Seq=802 Ack=730 Win=16064 Len=0 TSval=159143 TSecr=332
  21 16.896290  192.168.137.185            211.151.59.8     TCP       66 34933 > http [FIN, ACK] Seq=802 Ack=731 Win=16064 Len=0 TSval=159145 TSec
  22 17.272299  211.151.59.8               192.168.137.185  TCP       66 http > 34933 [ACK] Seq=731 Ack=803 Win=7680 Len=0 TSval=3326723389 TSecr=
  23 43.866942  fe80::14d7:11b6:1fc5:753b  ff02::1:3        LLMNR     84 Standard query A wpad
  24 43.867299  192.168.137.1              224.0.0.252      LLMNR     64 Standard query A wpad
  25 43.966970  fe80::14d7:11b6:1fc5:753b  ff02::1:3        LLMNR     84 Standard query A wpad
  26 43.967111  192.168.137.1              224.0.0.252      LLMNR     64 Standard query A wpad
  40 64.352819  192.168.137.185            192.168.137.1    DNS       81 Standard query A tdcv3.talkingdata.net
  41 64.356350  192.168.137.1              192.168.137.185  DNS       97 Standard query response A 211.151.121.41
```

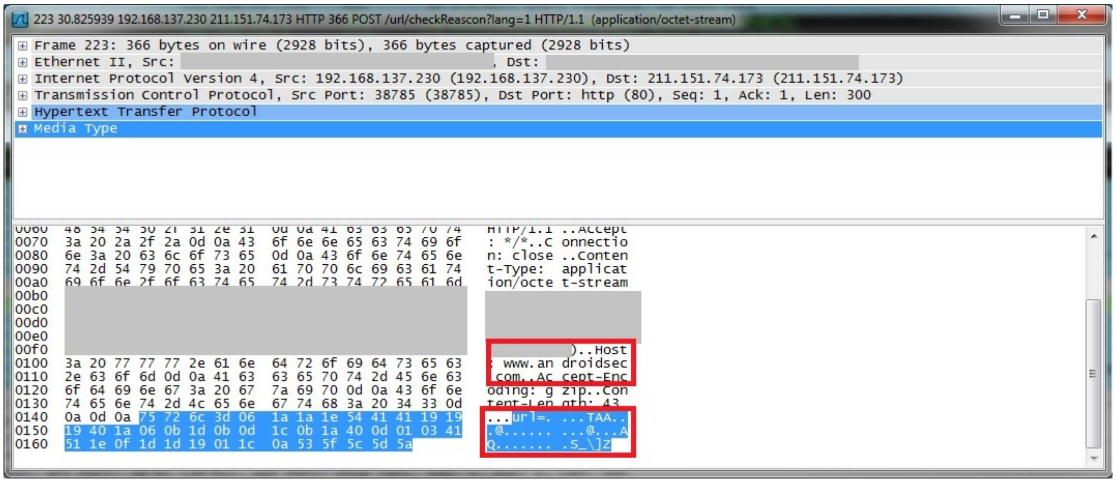
```
⊞ Frame 26: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
⊞ Ethernet II, Src: [redacted] Dst: [redacted]
⊞ Internet Protocol Version 4, Src: 192.168.137.1 (192.168.137.1), Dst: 224.0.0.252 (224.0.0.252)
⊞ User Datagram Protocol, Src Port: 63942 (63942), Dst Port: llmnr (5355)
⊞ Link-local Multicast Name Resolution (query)
```

```
0000  [redacted]  ..^..... ...y..E.
0010              .2...... o'......
0020              ........ s..^....
0030              .......w pad.....
```

Microsoft: <live capture in progress> File: C:...
Packets: 235 Displayed: 46 Marked: 0
Follow TCP Stream
Stream Content

```
POST /BOSS_US/UPSServlet HTTP/1.1
Accept: */*
Connection: close
Content-Type: application/octet-stream
User-Agent: [redacted]
Host: us.nqsrv.com
Accept-Encoding: gzip
Content-Length: 554

<Request>
<Protocol>2.2.1</Protocol>
<Command>6</Command>
<ClientInfo>
.<Model type="5">GT-I[redacted]</Model>
.<Language>1</Language>
.<Country>[redacted]</Country>
.<IMEI>[redacted]6</IMEI>
.<IMSI>[redacted]9</IMSI>
.<Timezone>2</Timezone>
.<UpdateType>1</UpdateType>
</ClientInfo>
<UserInfo>
.<UID>[redacted]</UID>
</UserInfo>
<ServiceInfo>
.<Service>3</Service>
.<Partner>[redacted]</Partner>
.<WapMurl status="1"/>
</ServiceInfo>
<VersionInfo os="[redacted]" version="[redacted]">
.<Module id="4" version="[redacted]" />
.<Module id="2" version="[redacted]"/>
</VersionInfo>
</Request>
HTTP/1.1 200 OK
Server: nginx/1.2.8
Date: [redacted]
Content-Length: 557
Connection: close
Pragma: No-cache
Cache-Control: no-cache
Expires: 0

<?xml version="1.0" encoding="UTF-8"?>
<Reply>
<Protocol>2.2.1</Protocol>
<Command>1</Command>
<ErrorInfo>
<Reason>4</Reason>
</ErrorInfo>
<UserInfo>
<Blance>0</Blance>
<UID>[redacted]</UID>
</UserInfo>
<ServiceInfo>
<Service>3</Service>
<NextConnectTime>4020</NextConnectTime>
<Level>32</Level>
</ServiceInfo>
<SystemMessages display="1">
<Message type="2">Current version is the latest!</Message>
</SystemMessages>
<AVMessages display="1">
<mt></mt>
<st></st>
<content>Current version is the latest!</content>
</AVMessages>
</Reply>
```

The app sending the phone’s IMEI and IMSI to China in plain text, readable XML format.

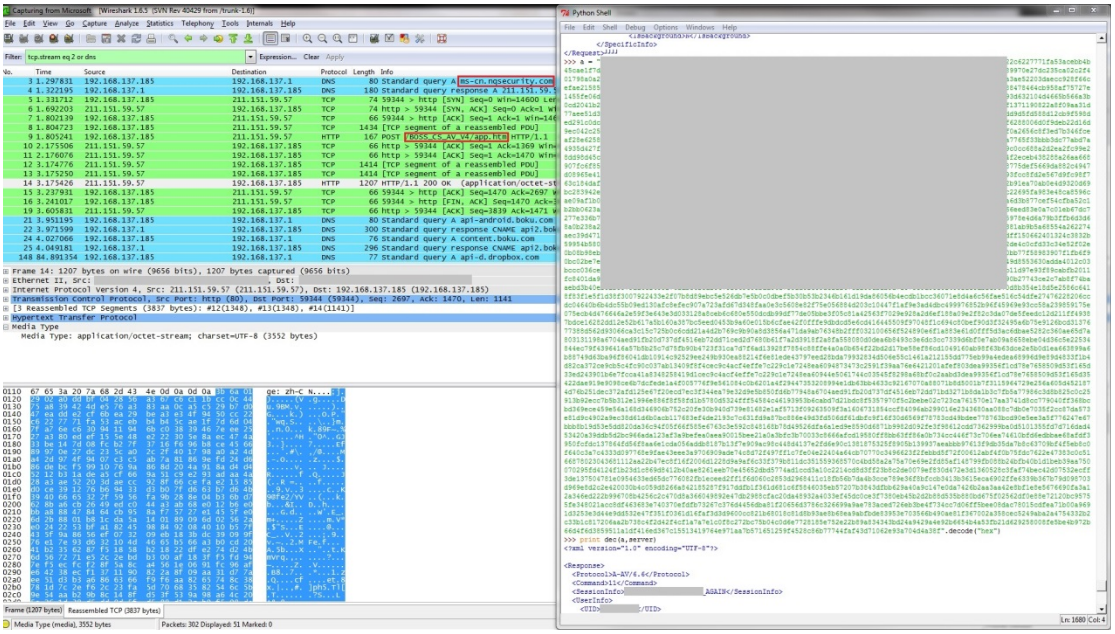


223 30.825939 192.168.137.230 211.151.74.173 HTTP 366 POST /url/checkReascon?lang=1 HTTP/1.1 (application/octet-stream)

```
⊞ Frame 223: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits)
⊞ Ethernet II, Src: [redacted], Dst: [redacted]
⊞ Internet Protocol Version 4, Src: 192.168.137.230 (192.168.137.230), Dst: 211.151.74.173 (211.151.74.173)
⊞ Transmission Control Protocol, Src Port: 38785 (38785), Dst Port: http (80), Seq: 1, Ack: 1, Len: 300
⊞ Hypertext Transfer Protocol
⊞ Media Type
```

```
0060  48 54 54 50 2f 31 2e 31  0d 0a 41 63 63 65 70 74   HTTP/1.1 ..Accept
0070  3a 20 2a 2f 2a 0d 0a 43  6f 6e 6e 65 63 74 69 6f   : */*..C onnectio
0080  6e 3a 20 63 6c 6f 73 65  0d 0a 43 6f 6e 74 65 6e   n: close ..Conten
0090  74 2d 54 79 70 65 3a 20  61 70 70 6c 69 63 61 74   t-Type:  applicat
00a0  69 6f 6e 2f 6f 63 74 65  74 2d 73 74 72 65 61 6d   ion/octe t-stream
00b0  [redacted]                                         [redacted]
00c0
00d0
00e0
00f0                                                     [redacted])..Host
0100  3a 20 77 77 77 2e 61 6e  64 72 6f 69 64 73 65 63   : www.an droidsec
0110  2e 63 6f 6d 0d 0a 41 63  63 65 70 74 2d 45 6e 63   .com..Ac cept-Enc
0120  6f 64 69 6e 67 3a 20 67  7a 69 70 0d 0a 43 6f 6e   oding: g zip..Con
0130  74 65 6e 74 2d 4c 65 6e  67 74 68 3a 20 34 33 0d   tent-Len gth: 43.
0140  0a 0d 0a 75 72 6c 3d 06  1a 1a 1e 54 41 41 19 19   ...url=. ...TAA..
0150  19 40 1a 06 0b 1d 0b 0d  1c 0b 1a 40 0d 01 03 41   .@...... ...@...A
0160  51 1e 0f 1d 1d 19 01 1c  0a 53 5f 5c 5d 5a         Q....... .S_\]Z
```

All user URL and browsing history is sent to China unencrypted, and easily decoded.

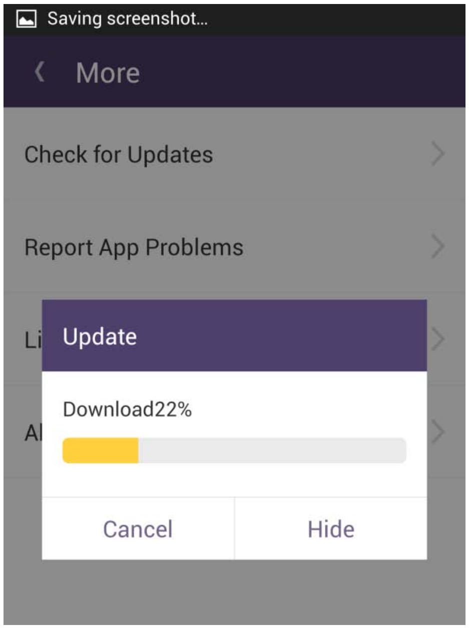


Capturing from Microsoft [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.stream eq 2 or dns
Expression... Clear Apply
Python Shell
File Edit Shell Debug Options Windows Help
Frame (1207 bytes) Reassembled TCP (3837 bytes)
Media Type (media), 3552 bytes
Packets: 302 Displayed: 51 Marked: 0
Ln: 1680 Col: 4

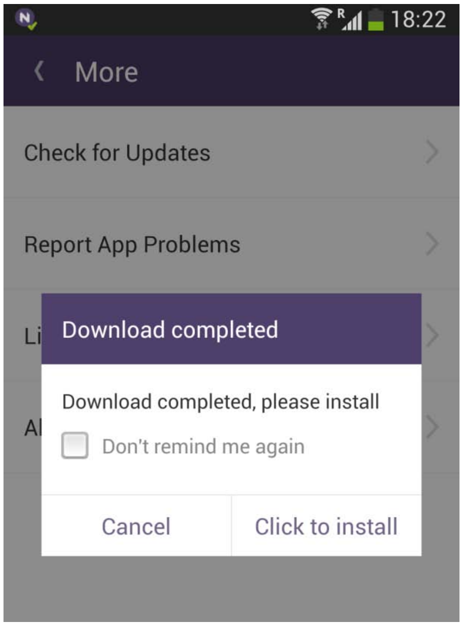
```
No.   Time        Source            Destination       Protocol Length Info
    3 1.297831    192.168.137.185   192.168.137.1     DNS        80 Standard query A ms-cn.nqsecurity.com
    4 1.322195    192.168.137.1     192.168.137.185   DNS       180 Standard query response A 211.151.59.5
    5 1.331712    192.168.137.185   211.151.59.57     TCP        74 59344 > http [SYN] Seq=0 Win=14600 Len
    6 1.692203    211.151.59.57     192.168.137.185   TCP        74 http > 59344 [SYN, ACK] Seq=0 Ack=1 Wi
    7 1.802139    192.168.137.185   211.151.59.57     TCP        66 59344 > http [ACK] Seq=1 Ack=1 Win=146
    8 1.804723    192.168.137.185   211.151.59.57     TCP      1434 [TCP segment of a reassembled PDU]
    9 1.805241    192.168.137.185   211.151.59.57     HTTP      167 POST /BOSS_CS_AV_V4/app.htm HTTP/1.1
   10 2.175506    211.151.59.57     192.168.137.185   TCP        66 http > 59344 [ACK] Seq=1 Ack=1369 Win=
   11 2.176076    211.151.59.57     192.168.137.185   TCP        66 http > 59344 [ACK] Seq=1 Ack=1470 Win=
   12 3.174776    211.151.59.57     192.168.137.185   TCP      1414 [TCP segment of a reassembled PDU]
   13 3.175250    211.151.59.57     192.168.137.185   TCP      1414 [TCP segment of a reassembled PDU]
   14 3.175426    211.151.59.57     192.168.137.185   HTTP     1207 HTTP/1.1 200 OK  (application/octet-st
   15 3.237931    192.168.137.185   211.151.59.57     TCP        66 59344 > http [ACK] Seq=1470 Ack=2697 W
   16 3.241017    192.168.137.185   211.151.59.57     TCP        66 59344 > http [FIN, ACK] Seq=1470 Ack=3
   19 3.605831    211.151.59.57     192.168.137.185   TCP        66 http > 59344 [ACK] Seq=3839 Ack=1471 W
   21 3.951195    192.168.137.185   192.168.137.1     DNS        80 Standard query A api-android.boku.com
   22 3.971599    192.168.137.1     192.168.137.185   DNS       300 Standard query response CNAME api2.bok
   24 4.027066    192.168.137.185   192.168.137.1     DNS        76 Standard query A content.boku.com
   25 4.049181    192.168.137.1     192.168.137.185   DNS       296 Standard query response CNAME api2.bok
  148 84.891354   192.168.137.185   192.168.137.1     DNS        77 Standard query A api-d.dropbox.com

⊞ Frame 14: 1207 bytes on wire (9656 bits), 1207 bytes captured (9656 bits)
⊞ Ethernet II, Src: [redacted], Dst: [redacted]
⊞ Internet Protocol Version 4, Src: 211.151.59.57 (211.151.59.57), Dst: 192.168.137.185 (192.168.137.185)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 59344 (59344), Seq: 2697, Ack: 1470, Len: 1141
⊞ [3 Reassembled TCP Segments (3837 bytes): #12(1348), #13(1348), #14(1141)]
⊞ Hypertext Transfer Protocol
⊟ Media Type
    Media Type: application/octet-stream; charset=UTF-8 (3552 bytes)

0110   67 65 3a 20 7a 68 2d 43  4e 0d 0a 0d 0a 3b 6a 01   ge: zh-C N....;j.
0120   29 02 a0 dd bf 04 28 56  a3 67 c6 c1 1b cc 0c 44   )......(V .g.....D
0130   75 a8 39 42 4d e5 76 a3  83 aa 0c a5 c5 29 b7 d0   u.9BM.v. .....)..
0140   47 ea dd e2 cf 6b ea 29  be a3 e3 4f 94 50 cc 22   G....k.) ...O.P."
0150   c6 22 77 71 fa 53 ac eb  b4 b4 5c ae 1f 7d 6d 04   ."wq.S.. ..\..}m.
0160   7f a7 6e c6 30 94 11 94  6b c0 38 39 46 7e ee 25   ..n.0... k.89F~.%
0170   27 a3 80 ed ef 15 5e 48  e2 22 30 5e 8a ec 47 4a   '.....^H ."0^..GJ
0180   33 be 14 7d 08 fc b2 7f  37 16 f6 96 b8 ce 45 66   3..}.... 7.....Ef
0190   89 97 0e 27 dc 23 5c a0  2c 2f 40 17 98 a0 a2 4d   ...'.#\. ,/@....M
```

```
              <IsBackground>N</IsBackground>
        </SpecificInfo>
</Request>JJJJ
>>> a = "[redacted]
...
66d4f6d3859511a1df416ed367c15513419764e971aa7b571651259f4528c86b77744faf43d71062e93a704d4a38f".decode("hex")
>>> print dec(a,server)
<?xml version="1.0" encoding="UTF-8"?>

<Response>
  <Protocol>A-AV/6.6</Protocol>
  <Command>11</Command>
  <SessionInfo>[redacted]AGAIN</SessionInfo>
  <UserInfo>
    <UID>[redacted]</UID>
```

Encoded data that is easily hacked


Saving screenshot...

Download22%


Download completed, please install

☐ Don't remind me again

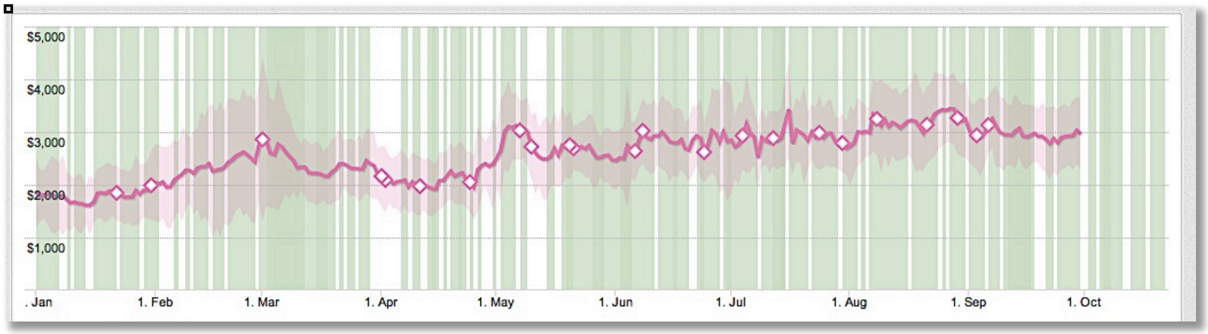
Software engineers simulated a Man in the Middle Attack disguised as a software update to the user’s phone.

NQ's Chief Security Architect testing NQ's encryption.

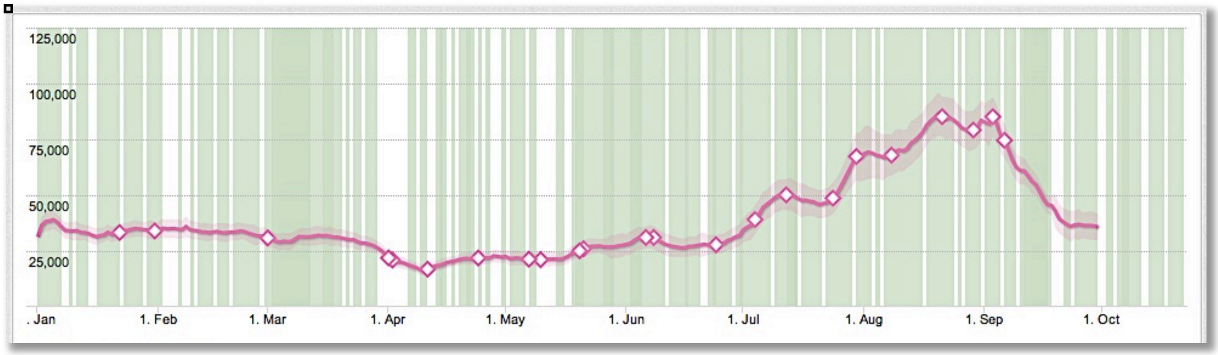
## NQ's International Revenue – Highly Likely to be Massively Overstated

NQ's purported $36.5 million on 2012 international revenue is absurd, and to be almost entirely fabricated. Our conclusion is based on analyses of app downloads, retail site visits, calls with an international carrier, discussions with NQ management, and discussions with industry consultants and NQ competitors.

NQ claims that its ex-China revenue in 2012 was $36.5 million. However, Distimo analytics estimates NQ's year-to-day worldwide revenue at less than $800,000. Distimo is a web analytics company that tracks over 3.2 billion downloads per quarter, and is widely used by web and mobile companies. Distimo tracks downloads from Google Play, the world's largest Android app store; and, Distimo develops estimates for app and developer revenue. The year-to-date chart below shows daily revenue on Google Play for 35 countries. Distimo tracks the following NQ products: Android Booster, Easy Battery Saver, Family Guardian, Easy Finder, Mobile Security, Mobile Security for Retail, Mobile Security 6.0 and Antivirus 7.0, Security Multi-Language, Vulnerability Killer, Super Task Killer and Vault (the Dataset):



The Year-To-Date chart below shows daily downloads on Google Play for the Dataset above:

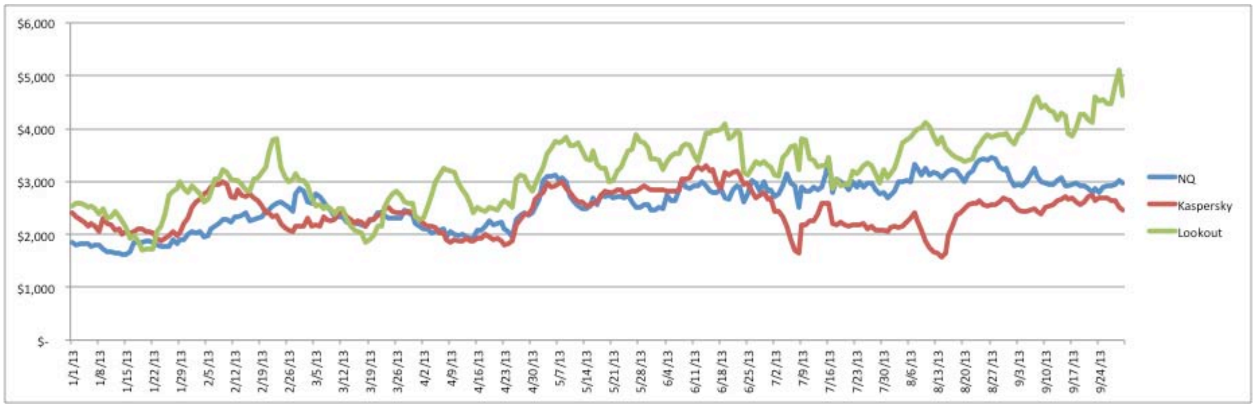


NQ tells investors that its strongest markets are in Southeast Asia and the Middle East – particularly Malaysia, Thailand, Indonesia, and Dubai. It claims an annual ARPU in these markets of $15. The monthly blended ARPU in Thailand is $7.13, with 60% of Thais using a mobile device to access the Internet.[56]

NQ has its co-headquarters in the US, spends significant sums of money on PR, and yet does not generate meaningful revenue in this market. (It is not a coincidence that revenue from the US would be much easier to audit than that from developing countries.) Our site visits to 84 retail locations in the US that are supposed to sell NQ products, and conversations with management of some of NQ's US distribution partners yields attachment rates generally of only 2% to 3%. The average ARPU in the US is $46.50.[57]

The graph below from Distimo data compares the average daily revenue of Lookout, Kaspersky, and NQ, across all mobile security products. We understand that Lookout's worldwide mobile security app revenue is less than $10 million annually.

[56] http://www.slideshare.net/yozzo1/2013-thailand-mobile-market-information
[57] http://www.totaltele.com/view.aspx?ID=472089



Source: Distimo

Our conversations with former mobile security employees of NQ competitors, such as Lookout, Kaspersky, and AVG makes clear that the best markets for mobile security are North America and Western Europe. Developed world consumers are far less price sensitive than developing world consumers, and are more willing to spend money on mobile security, despite not facing as many malware threats as in the developing world. Developed world conversion rates from download to paying user are around 2%. Developing world conversion rates are lower.

The primary reason malware is so much more prevalent in the developing world is precisely because people are unwilling to pay for apps – they often download pirated versions of apps for free, and these apps often are malware.

At the end of Q2 2013, NQ's DSOs were 198 days. The Company states that much of the high AR balance is due to its international revenue, and that its processors often have 180 days to settle. The industry people with whom we spoke all said that in their experience, their companies received payment in 30 to 45 days – even in emerging markets. The companies for which they worked utilize carrier billing, direct payment, and Google and app store payment mechanisms. Direct carrier billing is the most costly and time consuming of these methods. None of these industry experts could understand why NQ takes so long to receive payment.

NQ reveals nothing about its partners in its key overseas markets. Yet, it seems that every time a US-based executive signs up for a new loyalty program, NQ issues a press release about a "partnership".

It seems that most of NQ's high revenue international partners are not carriers, but rather are some type of intermediary. However, NQ claims to have the lowest user acquisition costs in the world, at approximately $0.07. Given that NQ is dealing through multiple layers to get to customers, it is highly unlikely its acquisition costs would be the lowest in the world. Given that NQ has a fraction of the user base it claims to, its user acquisition costs are probably in reality close to being the highest in the world.

We previously noted NQ's penchant for turning the most mundane event into a headline. It is somewhat ironic that it did so with Telefonica. NQ signed an agreement with Telefonica in connection with their Blue Via platform on February 27, 2012. Blue Via is a payment service created to foster development of new apps by facilitating payment integration. Telefonica offers this service free to any developer willing to adhere to its ethical policy. There are approximately 3,000 developers using Blue Via, and we understand that Telefonica has never terminated any relationship. There is no minimum sales requirement to be on the platform. Telefonica provides no marketing support, other than the Blue Via portal. In short, being an app developer on the Blue Via platform is as special as having the last name Smith. The irony though is that one of Blue Via's nicest features is that it processes payments quickly – developers generally receive payment within 15 days of the end of the month.

One of our consultants with knowledge of Blue Via said, "There have not been many downloads of NQ software. Just a few. It's not a big business." Telefonica's mobile security vendor of choice in Brazil is F-Secure, not NQ. Consumers download F-Secure from the Vivo app store. The attach rate for F-Secure was 6% after a two week trial period in June 2011, and was considered a success by Vivo. Vivo pays F-Secure within 30-45 days after the customer is billed, as is customary for mobile app payments.

*The mobile security app market is much harder than NQ makes it appear*

The mobile antivirus and security revenue constitutes a negligible segment of the overall antivirus software market. Desktop antivirus companies offer a mobile product for competitive reasons, often at a loss, to lock their customers into a multi-device solution and reduce the opportunity for competitors to poach their customers. Because it does not have a desktop app with which to create a bundle, this opportunity is not present for NQ.

The US retail channel is not well-suited to mobile security app developers. Android smartphone industry has grown and created opportunities for antivirus and security companies that can demonstrate their value and have strong brand recognition. However, retail is a difficult sales channel to penetrate considering stores want 30% to 40% of gross revenue. Stores require collateral and sales person training in order to effectively pitch the product.

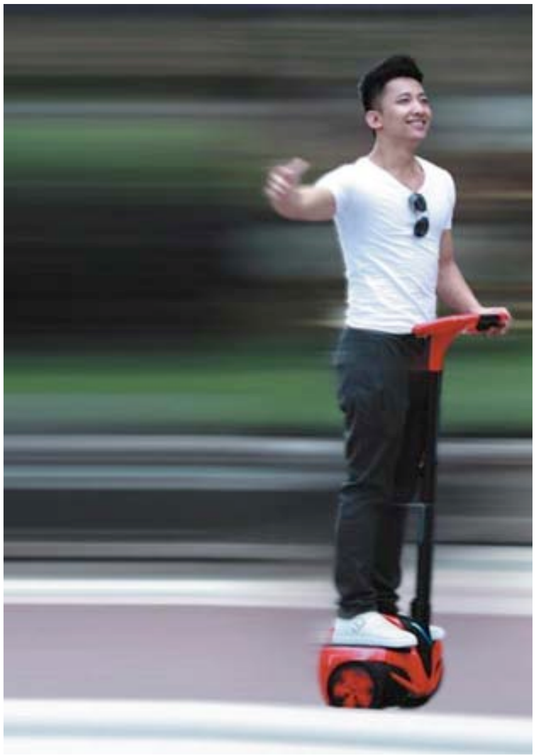
Retail salespeople are seldom motivated to sell security apps. Selling mobile antivirus at the retail level is a lot of work for a little money, and without a catalyst to drive mobile antivirus sales such as the CodeRed and Nimda viruses consumers do not feel the pain enough to motivate the purchase an antivirus solution. The goal of antivirus companies is to get consumers to accept desktop pricing for mobile solutions, however that has not yet occurred.

NQ's lack of a desktop product creates a disadvantage when it comes to retail sales and the sales person upon whom they must rely has a store full of products to sell, most of which can be sold quickly, require little sales training, are more popular and provide a greater economic incentive to sell than NQ products. After selling the NQ product the salesperson must physically install it on the consumer handset and register the consumer with NQ, a time consuming process with little upside for the salesperson. Salespeople tend to view NQ as a product to sell as a last resort if they can't upsell any of the other easier products they traditionally sell.

## The Farcical Side

The farcical facts we uncovered about NQ sometimes made it easy to forget that the Company is committing a very serious fraud. Such chicanery is not unusual in the China fraud context – it usually seems to result from a fraudulent company desperately trying to find ways to generate real revenue in order to relieve some of the pressure of having to constantly cook books. Some of the stranger things we came across when looking at NQ were its knockoff Segway (MW internally dubbed it the "Family Guardian Emergency Response Vehicle"); the anonymous calling cards; black hat SEO that is likely infringing trademarks belonging to Samsung, Apple, and other large companies; claiming to pay $1.55 million to a middleman for a 10-year lease on its URL; having a "NQ for Men" philandering tool app, and falsely claiming to have just discovered viruses.

Below are pictures of NQ's knockoff Segway (http://inmotion.nq.com).



NQ should produce *Breakin' 3 Don't Crash Into a Tree* and do product placement.

NQ's anonymous calling card business is silly. China now requires an ID to buy prepaid cards. Anonymous calling cards are relatively rare in China, and are not condoned by the authorities. (This is why we believe NQ's brand is not on the card.) The main market for anonymous cards is likely telephone / SMS spammers and scammers. Investors might find it ironic that a company that makes anti-spam software also enables spam. However, as we explain in *NQ's 3-15 DNA*, NQ was exposed by China's state television news for infecting phones with malware in order to sell users the cure.

Card buyers need to download software to operate the anonymous card. The two vendors told us that the URL on the anonymous card, http.KD.tl (.tl is an East Timor domain.), is the site from which to download the software. (NQ has an affinity for two-letter domains – as we highlight infra, it claims to have paid $1.55 million to an anonymous party for 10-year rights to www.nq.com.) Similar to how NQ has responded to our prepaid card inquiries, it suddenly removed all content from the website on October 18th. The Beijing vendor also changed his story about the cards on October 18th – as we discussed supra, we rattled NQ's cage with our prepaid card queries.

NQ is behind the anonymous calling cards. The software used references NQ, and a website through which the software operates http://secretclothes.com, lists NQ's webmaster, Zhang Guobao, as the contact.

NQ's is likely infringing the trademarks of Samsung, Nokia, HTC, NTT, Vodaphone, and Apple. NQ is engaged in "black hat SEO" by registering URLs with these trademarks in them, and pointing them toward NQ's US website. On October 21, 2013 we ran a Reverse IP lookup on NQ's website, www.netqin.com, located at 211.151.59.30. These servers host domains that include expected regional variations of the NQ brand such as NQ.fr, NQ.jp. However, these servers also host domains with the following trademarks in the URL:

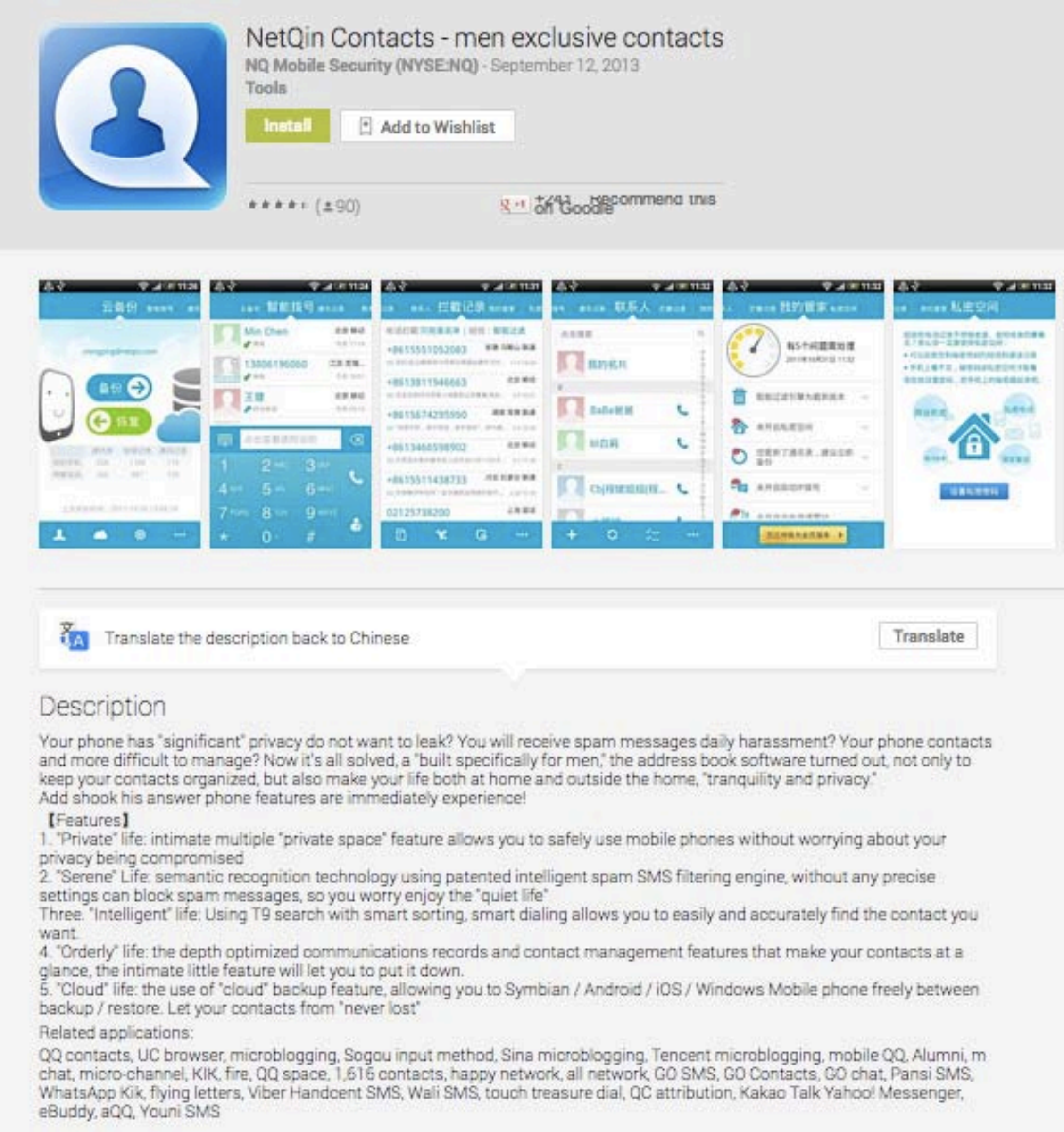
1. NOKIAsecure.com
2. NTTsecurity.com
3. SAMSUNGsecure.com
4. securityHTC.com
5. securityIPHONE.com
6. VODAFONEsecurity.com

All of these domains redirect to en.NQ.com.

We would be surprised if these companies licensed their trademarks to NQ for this purpose – particularly in the case of Samsung, which has a similar URL for its security equipment division (www.samsungsecurity.com). We have already sent letters to the general counsel for each of these companies. This black hat stunt would be far less likely to happen at a real company.

Pimpin' sure gets a lot easier with NQ for Men.[58] NQ for Men appears to be a mobile phone app that keeps significant others from being able to see the "black book" part of the contacts, call / SMS history to black book contacts, and blocks calls and SMSes from these contacts during inconvenient times. MW acknowledges that there is likely a niche market for this product, but we are not sure it is something with which a global leader in mobile security would be involved. Note to Anthony Weiner: read the section titled *NQ's Antivirus Makes it Easy for the PRC Government and Hackers…* before using.

[58] "Pimpin' Ain't Easy", Big Daddy Kane, It's a Big Daddy Thing (1989).



NetQin Contacts - men exclusive contacts

NQ Mobile Security (NYSE:NQ) - September 12, 2013

Tools

Translate the description back to Chinese

Description

Your phone has "significant" privacy do not want to leak? You will receive spam messages daily harassment? Your phone contacts and more difficult to manage? Now it's all solved, a "built specifically for men," the address book software turned out, not only to keep your contacts organized, but also make your life both at home and outside the home, "tranquility and privacy."
Add shook his answer phone features are immediately experience!

【Features】
1. "Private" life: intimate multiple "private space" feature allows you to safely use mobile phones without worrying about your privacy being compromised
2. "Serene" Life: semantic recognition technology using patented intelligent spam SMS filtering engine, without any precise settings can block spam messages, so you worry enjoy the "quiet life"
Three. "Intelligent" life: Using T9 search with smart sorting, smart dialing allows you to easily and accurately find the contact you want.
4. "Orderly" life: the depth optimized communications records and contact management features that make your contacts at a glance, the intimate little feature will let you to put it down.
5. "Cloud" life: the use of "cloud" backup feature, allowing you to Symbian / Android / iOS / Windows Mobile phone freely between backup / restore. Let your contacts from "never lost"

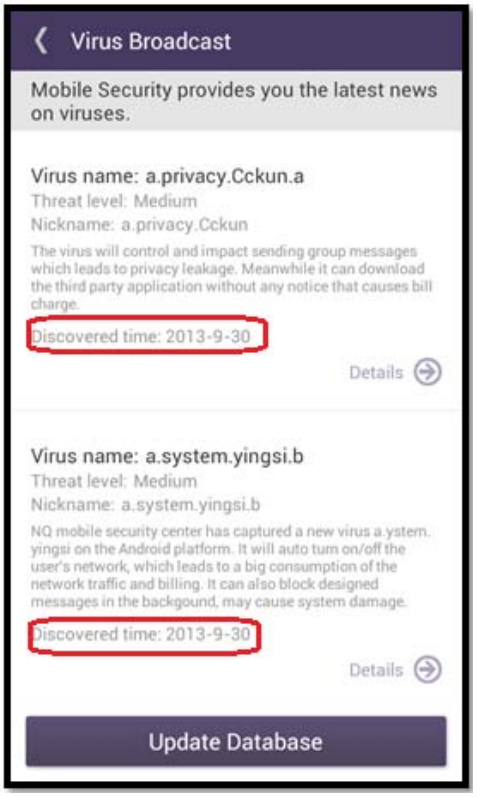
Related applications:

QQ contacts, UC browser, microblogging, Sogou input method, Sina microblogging, Tencent microblogging, mobile QQ, Alumni, m chat, micro-channel, KIK, fire, QQ space, 1,616 contacts, happy network, all network, GO SMS, GO Contacts, GO chat, Pansi SMS, WhatsApp Kik, flying letters, Viber Handcent SMS, Wali SMS, touch treasure dial, QC attribution, Kakao Talk Yahoo! Messenger, eBuddy, aQQ, Youni SMS

App store page for NQ for Men.

NQ's claim to have paid $1.55 million for the domain www.nq.com is outrageous. NQ claims to have paid the money in July 2011, but the curious thing is that the domain was transferred to an anonymous registrant in 2011, and then subsequently transferred to NQ in October 2011. The seller of the domain in July 2011 was a company called Conexus Software. It appears to have been very small – there was no physical address or phone number on the website as of June 2011. Google searches reveal little online information about it. Two possibilities strongly suggest themselves: a) NQ had a related party purchase the domain from Conexus for far less than $1.55 million, and then sell it to NQ for an inflated price, or b) NQ had a related party purchase the domain from Conexus for far less than $1.55 million, and then claimed to buy it for $1.55 million when in fact the price was much lower – this would have helped NQ burn off some "fake cash". Of course it is always possible that Conexus was able to command such a windfall price for the domain, but we would bet against it. Another interesting fact is that we called the original seller and he told us he was not at liberty to discuss the transaction without speaking to counsel first – it sounds as though he had a NDA. What is so secretive about selling your domain unless there is more to it than just “www.nq.com was sold for $1.55 million”?

NQ is “scare ware” – NQ Antivirus 7.0 is hardcoded to tell the user the NQ discovered two viruses the same day the user installs the app.  Upon installing NQ antivirus 7.0 and running an initial scan, the user receives a scare-ware message indicating that certain viruses have been recently discovered. This message is presented to all users, and the discovery date is always the same as the date the app was installed.

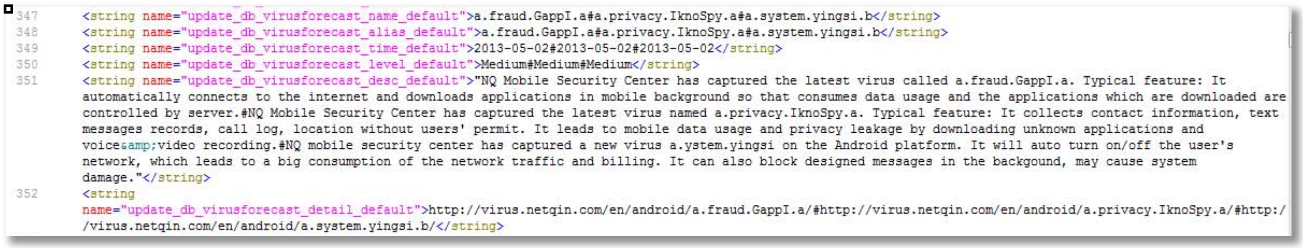


Mobile Security provides you the latest news on viruses.

Virus name: a.privacy.Cckun.a
Threat level: Medium
Nickname: a.privacy.Cckun
The virus will control and impact sending group messages which leads to privacy leakage. Meanwhile it can download the third party application without any notice that causes bill charge.
Discovered time: 2013-9-30

Virus name: a.system.yingsi.b
Threat level: Medium
Nickname: a.system.yingsi.b
NQ mobile security center has captured a new virus a.ystem.yingsi on the Android platform. It will auto turn on/off the user's network, which leads to a big consumption of the network traffic and billing. It can also block designed messages in the backgound, may cause system damage.
Discovered time: 2013-9-30

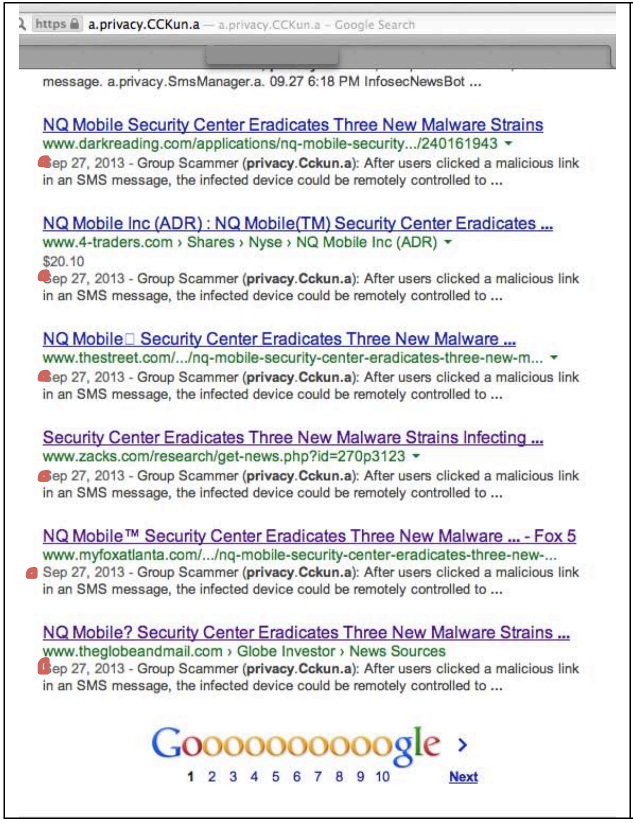
When we examine the code, we can see that these virus alerts are actually hardcoded into the application, and are presented to the user by default:



```
<string name="update_db_virusforecast_name_default">a.fraud.GappI.a#a.privacy.IknoSpy.a#a.system.yingsi.b</string>
<string name="update_db_virusforecast_alias_default">a.fraud.GappI.a#a.privacy.IknoSpy.a#a.system.yingsi.b</string>
<string name="update_db_virusforecast_time_default">2013-05-02#2013-05-02#2013-05-02</string>
<string name="update_db_virusforecast_level_default">Medium#Medium#Medium</string>
<string name="update_db_virusforecast_desc_default">"NQ Mobile Security Center has captured the latest virus called a.fraud.GappI.a. Typical feature: It
automatically connects to the internet and downloads applications in mobile background so that consumes data usage and the applications which are downloaded are
controlled by server.#NQ Mobile Security Center has captured the latest virus named a.privacy.IknoSpy.a. Typical feature: It collects contact information, text
messages records, call log, location without users' permit. It leads to mobile data usage and privacy leakage by downloading unknown applications and
voice&amp;video recording.#NQ mobile security center has captured a new virus a.ystem.yingsi on the Android platform. It will auto turn on/off the user's
network, which leads to a big consumption of the network traffic and billing. It can also block designed messages in the backgound, may cause system
damage."</string>
<string
name="update_db_virusforecast_detail_default">http://virus.netqin.com/en/android/a.fraud.GappI.a/#http://virus.netqin.com/en/android/a.privacy.IknoSpy.a/#http:/
/virus.netqin.com/en/android/a.system.yingsi.b/</string>
```

We searched the Internet hoping to find an actual user who has been infected with these viruses. We scoured user support groups, competing antivirus company websites, carrier websites, etc.

We did not find anyone who has been infected. What we did find were multiple websites that mindlessly regurgitate NQ press releases put out through PR Newswire service:



https a.privacy.CCKun.a — a.privacy.CCKun.a - Google Search

message. a.privacy.SmsManager.a. 09.27 6:18 PM InfosecNewsBot ...

NQ Mobile Security Center Eradicates Three New Malware Strains
www.darkreading.com/applications/nq-mobile-security.../240161943
Sep 27, 2013 - Group Scammer (**privacy.Cckun.a**): After users clicked a malicious link in an SMS message, the infected device could be remotely controlled to ...

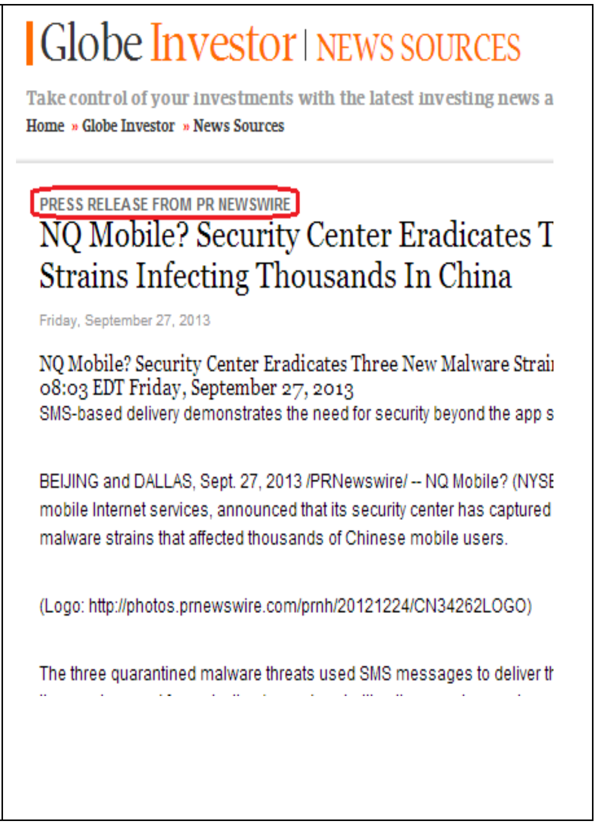
NQ Mobile Inc (ADR) : NQ Mobile(TM) Security Center Eradicates ...
www.4-traders.com › Shares › Nyse › NQ Mobile Inc (ADR)
$20.10
Sep 27, 2013 - Group Scammer (**privacy.Cckun.a**): After users clicked a malicious link in an SMS message, the infected device could be remotely controlled to ...

NQ Mobile□ Security Center Eradicates Three New Malware ...
www.thestreet.com/.../nq-mobile-security-center-eradicates-three-new-m...
Sep 27, 2013 - Group Scammer (**privacy.Cckun.a**): After users clicked a malicious link in an SMS message, the infected device could be remotely controlled to ...

Security Center Eradicates Three New Malware Strains Infecting ...
www.zacks.com/research/get-news.php?id=270p3123
Sep 27, 2013 - Group Scammer (**privacy.Cckun.a**): After users clicked a malicious link in an SMS message, the infected device could be remotely controlled to ...

NQ Mobile™ Security Center Eradicates Three New Malware ... - Fox 5
www.myfoxatlanta.com/.../nq-mobile-security-center-eradicates-three-new-...
Sep 27, 2013 - Group Scammer (**privacy.Cckun.a**): After users clicked a malicious link in an SMS message, the infected device could be remotely controlled to ...

NQ Mobile? Security Center Eradicates Three New Malware Strains ...
www.theglobeandmail.com › Globe Investor › News Sources
Sep 27, 2013 - Group Scammer (**privacy.Cckun.a**): After users clicked a malicious link in an SMS message, the infected device could be remotely controlled to ...



Globe Investor | NEWS SOURCES

Take control of your investments with the latest investing news a

Home » Globe Investor » News Sources

PRESS RELEASE FROM PR NEWSWIRE

NQ Mobile? Security Center Eradicates T
Strains Infecting Thousands In China

Friday, September 27, 2013

NQ Mobile? Security Center Eradicates Three New Malware Strai
08:03 EDT Friday, September 27, 2013
SMS-based delivery demonstrates the need for security beyond the app s

BEIJING and DALLAS, Sept. 27, 2013 /PRNewswire/ -- NQ Mobile? (NYSE
mobile Internet services, announced that its security center has captured
malware strains that affected thousands of Chinese mobile users.

(Logo: http://photos.prnewswire.com/prnh/20121224/CN34262LOGO)

The three quarantined malware threats used SMS messages to deliver th

## NQ's 3-15 DNA – Video Available at: https://vimeo.com/77704496

NQ broke the cardinal rule of China fraud: Do not get into trouble in China. State-owned CCTV, the most influential television news network in China, exposed some of NQ's dishonest practices in what is known as the "3-15 incident". Every March 15th in China is Consumer Day, and CCTV airs investigative reports on companies that are among the more egregious in their business practices. NQ was exposed during the March 15, 2011 program.

CCTV revealed that NQ and its subsidiary, FL Mobile, were paying phone refurbishers in China to install both NQ and FL software. However, the FL software was really a trojan, and about six hours after the user put a new SIM in, the phone would go haywire. The performance would slow down, and users would see their phones uploading and downloading data without being commanded. Non-NQ security apps were suddenly deleted. However, users could obtain salvation by running NQ, which informed them that they would need to become paying subscribers in order to eradicate the virus.

The exposure was a massive problem, and threatened to derail NQ's fraud dreams. Its IPO was postponed by a few months while it tried to paper over the bad publicity. We spoke with a former NQ employee who joined the Company after the 3-15 incident. She informed us that NQ tells employees that CCTV the following year aired a retraction. We viewed the 2012 program, and there was no retraction of any sort. This appears to be a lie.

NQ tells investors that CCTV privately retracted its reporting. We see no evidence of the sort. We did come across an interview with the director of that episode in which the director reiterated that NQ and FL were culpable:

> China Times: The day after the report exposing NetQin and Feiliu Jiu Tian of jointly harming consumers, they declared there were serious discrepancies with your facts.
>
> Yin Wen: the content of Feiliu JiuTian's statement really has no substance, they did not state what specific points were mistaken.
>
> The issue addressed in their statement was primarily that of the "version problem" followed by the "key" problems, and even went so far as to claim that they were framed by their competitors. All so-called "great" companies claim they were framed by competitors when they are exposed. Would CCTV's 3-15 Gala show do such a thing? Now the two companies have removed their statements, both having already admitted their mistakes.
>
> In fact, the purpose of this program is to provide consumers with a clue. Although the program was only a few minutes long, in fact, we started the investigation of these two companies in October of last year and spent a total of four months of time investigating. In total we spent four months tracking them, determining how they did the downloads, assessing how they control users, all of this have been investigated very clearly.

NQ tried to paper over its wrongdoing by submitting code to be certified as clean. Obviously NQ submitted the OTHER code – i.e., the code without the malware.

We have posted the 3-15 video on our website with subtitles. We believe that investors will find it illuminating. The video is at: https://vimeo.com/77704496.

3-15 is important for investors to understand NQ's management. First, they obviously lack an ethical compass – that is the obvious. More subtly though, this is evidence that they just cannot help themselves. Scamming consumers for RMB 2 a pop was clearly a stupid risk given the hundreds of millions of dollars they could pocket through a successful stock fraud. These are people who will steal the shirts off investors' backs – without hesitating.

## US Management is Merely a Front

NQ would have viewed Omar Khan as the perfect front for its fraud. That is why it offered him a pay package worth over approximately $20 million during the first three years, even though Mr. Khan had never been a C-level executive or a business operator. This is by far the smartest thing the perpetrators of the fraud have done – everything else we have seen from NQ is average to poor tradecraft.

By the second half of 2011, NQ was public, but it had barely pulled it off. The originally planned March 2011 IPO date was scuttled because of the CCTV exposure of its malware installation operation. (See NQ's 3-15 DNA.) Shortly after NQ went public, several high profile China fraud blowups caused investors to flee US-listed China stocks. Because NQ was among the more poorly disguised frauds, its stock price lingered in the gutter.

NQ's true management had a previously successful blueprint upon which they called for inspiration. China Fraud 1.0 generally involved having a smooth "CFO" who was usually based in the US. The CFOs usually had enough professional background to talk numbers intelligently, but they were not involved in any real management, budgeting, or CFO-ing. Their job was to market the stock. This model worked extremely well for several years.

NQ thus conceived China Fraud 2.0. China Fraud 2.0 is about making the US "management" presence appear more substantive than it did with 1.0, i.e. have a Co-CEO, rather than just a CFO. In addition, make the Co-CEO someone who really understands promotion and buzz – ideally, someone who would see opportunities to generate legitimacy for the Company by signing deals with US companies that lead to press releases. Lots and lots of press releases. Give the Co-CEO a staff and latitude to make as many arrangements – no matter how small or unprofitable – with US companies as possible. Finally, pair him with a former hedge fund manager to relentlessly market the stock.

Omar Khan is a top-flight pitchman. He had been the face of many of Samsung Mobile's biggest product launches in the US, and for good reason. He is smart, knows mobile, and connects extremely well with his audience. Because he had never been an operator though, he would be much less likely to figure out NQ is a fraud. In Mr. Khan, NQ got exactly what it needed – credibility, charisma, and naivete.

For Mr. Khan, the approximately $20 million stock package NQ offered him was likely far more money than he had ever seen, given his career trajectory as a sub-C level executive at large corporations, such as Motorola, Samsung, and then Citibank. NQ hired Mr. Khan out of Citibank in Dallas, TX.

Mr. Khan is not a board member or executive of any of NQ's China entities.[59]

So far, this has seemed to work out extremely well for Mr. Khan. His stock package is now worth approximately $100 million.

It is possible that Mr. Khan has been defrauded every bit as much as NQ's investors. This certainly is not without precedent though. When Longtop Financial Technologies Ltd. (formerly

[59] SAIC files.

LFT) was confirmed as a fraud, numerous very China savvy investors were stunned. We recall conversations with some of these investors, and their shock was due to their faith in LFT CFO Derek Palaschuk. Mr. Palaschuk was not the typical China Fraud 1.0 CFO – he knew his way around China companies, had long been based in China, and believed he had a substantive role in managing LFT. Apparently LFT built a fake online banking environment just in order to defraud Mr. Palaschuk, all the while causing him to unwittingly defraud thousands of investors. LFT and Mr. Palaschuk offer two lessons for NQ investors. First, the only people whose integrity matters are China-side management and their cabal of advisors and enablers. In NQ's case, no such integrity exists. Second, even the most sophisticated and deeply embedded executives are no match for the unfathomably large amount of tools and willingness to commit fraud available in China.

NQ's current and former CFO are old hands in the China Fraud world. We do not suspect that they were ever culpable in the frauds with which they have been involved, and we are not suggesting that either knows that NQ is a fraud or is culpable; but, once somebody is tainted with a public company fraud, it is hard to get work at a non-fraud. Prior to NQ, Suhai Ji, the recently departed CFO, headed business development for the New York Stock Exchange's Beijing office. During his tenure, the NYSE listed several frauds, including Ambow Education Holding Ltd. (AMBO), China Intelligent Lighting and Electronics Inc. (formerly CILE), alleged fraud China New Borun (BORN), Duoyuan Printing (formerly DYP), Duoyuan Global Water (formerly DGW), and Universal Travel Group (formerly UTA). NQ's current CFO comes was a managing director for Asia investment banking at Piper Jaffrey. During his time at Piper, Piper helped to underwrite BORN, DYP, DGW, and Gushan Environmental Energy (formerly GU).

## NQ's Cash Balance (a Level 2 Asset) is Highly Likely to be Fraudulent

We strongly suspect that the vast majority of the $127.9 million cash and investments NQ reported having as of December 31, 2012 is not actually in the Company's accounts; rather, that some to all of NQ's IPO proceeds have been diverted in order to further the accounting fraud. NQ's disclosures about its cash and term deposits being Level 2 assets raise significant red flags.[60] Its claim to have transferred approximately $47 million in IPO proceeds directly to its VIE contravenes China's capital controls, and in our view, never really happened – we believe that the money was instead diverted.

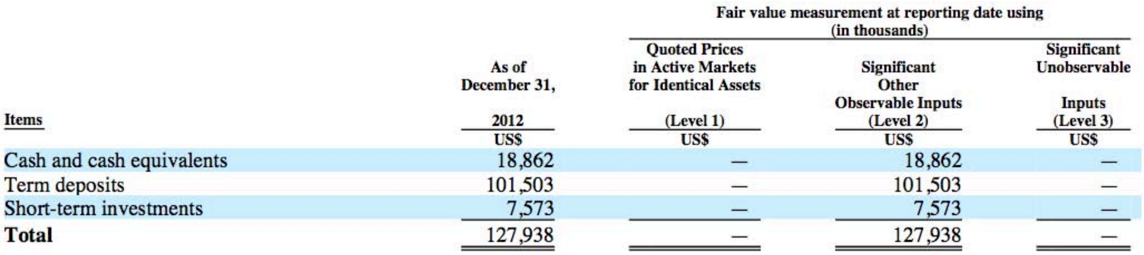
Forging cash balances in China is shockingly common and easy. Unfortunately, cash balance confirmation is the only anti-fraud procedure most public company audits incorporate. In other words, if a company can fake its cash balance, its auditor will generally conduct the audit with little to no skepticism. China's banks have very poor controls at the branch level, and branch employees have been co-opted in frauds countless times. The auditor resignation letter for Longtop Financial Technologies Ltd. makes clear that branch level employees were complicit in the fraud.[61] (The auditor only resigned after Bronte Capital and Citron Research scathingly exposed it as a fraud.) China Auditors now sometimes take steps to improve the quality of cash

[60] 2012 20F, p. F-23.
[61] See Longtop 6-K filed May 23, 2011.

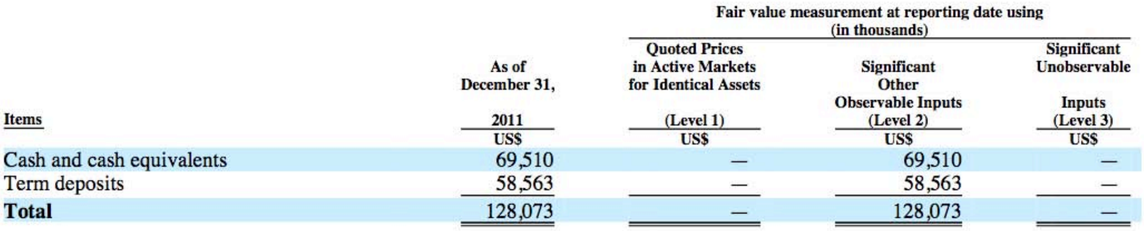
confirmations, including depositing a small amount of money in the client's account and immediately requesting the client's bank account statement to ensure the deposit shows up.

The first warning sign about NQ's purported cash balance being fraudulent is that in the 2012 20-F, NQ classified *all* cash and equivalents, and term deposits, as Level 2 assets for 2011 and 2012. This raises questions about how NQ is claiming to hold its cash, and how NQ's auditor confirmed the balances. We cannot recall having ever seen cash classified as a Level 2 asset. Even more troublesome, the 2011 20-F classified all of NQ's cash and term deposits as Level 1 assets, but in the 2012 20-F, the 2011 balances were reclassified as Level 2 without any explanation. The Level 2 reclassification raises worrying issues because the default assumption is that cash and term deposits of less than 12 months in safe banks are not Level 2 assets – that is, you should be able to derive their fair value without having to look at other assets for pricing. This default assumption was obviously the basis for the original 2011 classifications.

NQ's 2012 20-F makes the below disclosure about its cash and term deposits for 2011 and 2012. The 2012 20-F retroactively reclassified them as Level 2, but without explanation. [62]

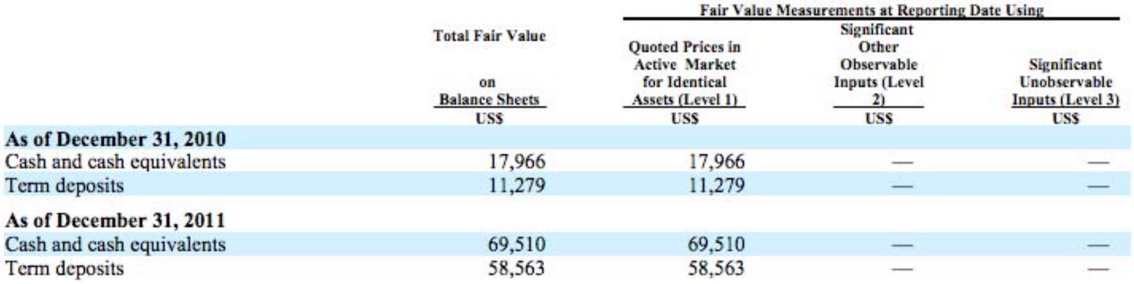


| | | Fair value measurement at reporting date using (in thousands) | | |
|---|---|---|---|---|
| Items | As of December 31, 2012 | Quoted Prices in Active Markets for Identical Assets (Level 1) | Significant Other Observable Inputs (Level 2) | Significant Unobservable Inputs (Level 3) |
| | US$ | US$ | US$ | US$ |
| Cash and cash equivalents | 18,862 | — | 18,862 | — |
| Term deposits | 101,503 | — | 101,503 | — |
| Short-term investments | 7,573 | — | 7,573 | — |
| **Total** | 127,938 | — | 127,938 | — |



| | | Fair value measurement at reporting date using (in thousands) | | |
|---|---|---|---|---|
| Items | As of December 31, 2011 | Quoted Prices in Active Markets for Identical Assets (Level 1) | Significant Other Observable Inputs (Level 2) | Significant Unobservable Inputs (Level 3) |
| | US$ | US$ | US$ | US$ |
| Cash and cash equivalents | 69,510 | — | 69,510 | — |
| Term deposits | 58,563 | — | 58,563 | — |
| **Total** | 128,073 | — | 128,073 | — |

Below is the 2011 20-F schedule. [63]



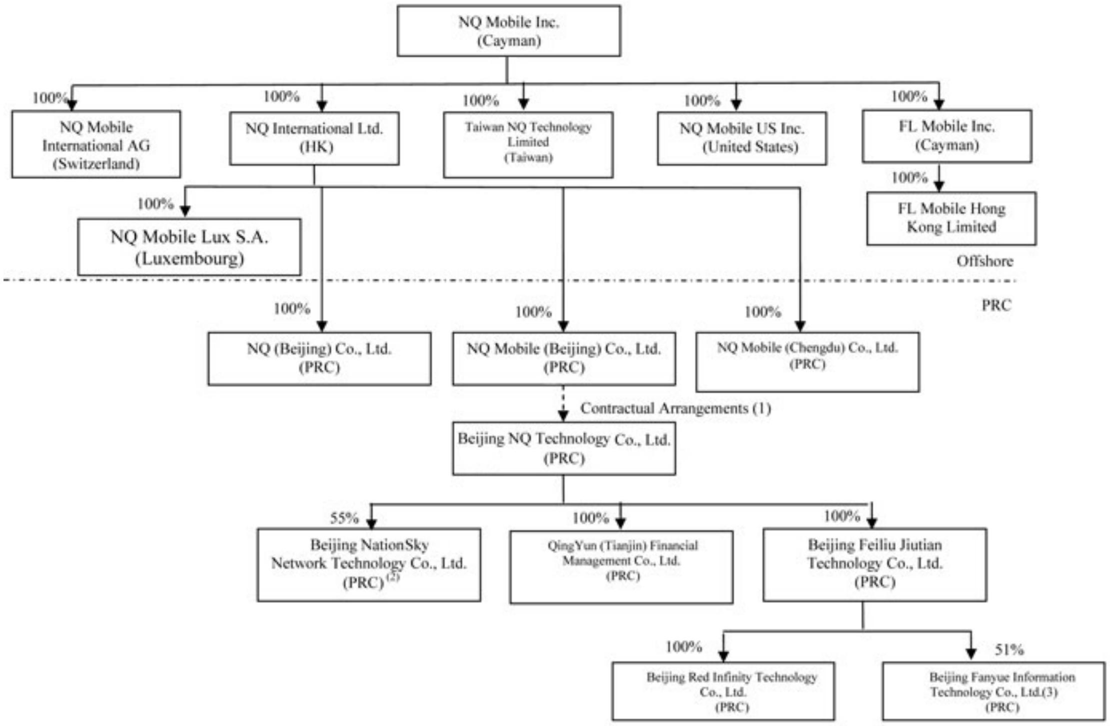
| | | Fair Value Measurements at Reporting Date Using | | |
|---|---|---|---|---|
| | Total Fair Value on Balance Sheets | Quoted Prices in Active Market for Identical Assets (Level 1) | Significant Other Observable Inputs (Level 2) | Significant Unobservable Inputs (Level 3) |
| | US$ | US$ | US$ | US$ |
| **As of December 31, 2010** | | | | |
| Cash and cash equivalents | 17,966 | 17,966 | — | — |
| Term deposits | 11,279 | 11,279 | — | — |
| **As of December 31, 2011** | | | | |
| Cash and cash equivalents | 69,510 | 69,510 | — | — |
| Term deposits | 58,563 | 58,563 | — | — |

[62] 2012 20F, p. F-23.
[63] 2011 20F, p. F-18.

One therefore wonders what NQ is showing its auditors as evidence of the existence of the cash and the term deposits, and why the auditor deemed it necessary to reclassify 2011 cash and term deposits.  These facts raise real concerns about whether NQ's purported cash is really there, and if it were, whether NQ is holding any of China's infamous "wealth management products".

NQ's purported implausible movement of funds makes it easier to divert funds without detection. When analyzing NQ's SEC filings alongside its (fraudulent) SAIC financials, it becomes clear that NQ purports to have moved about $47 million of IPO proceeds to its VIE in a way that almost certainly would not have been permitted, and would therefore not have been possible. This claim is reminiscent of Sino-Forest, which also purported to have moved cash in ways that contravened China's exchange controls.  Sino-Forest's similar claims were essential to its having obtained unqualified audit opinions for 16 years, most recently from Ernst & Young.

About $47 million of IPO proceeds purportedly ended up as a "term deposit" in the PRC belonging to the VIE.  This purported movement represents worst practices for managing risks of theft and other misconduct inherent in VIE structures.  Our view is that most to all of the cash transfer never happened, and that by purporting to have somehow circumvented China's capital controls in order to transfer the money directly to the VIE, it makes it easier for NQ to carry out its fraud by forging its cash balances.  In order to understand these points, it is necessary to consider NQ's corporate structure.  Below is a diagram of the relevant entities.

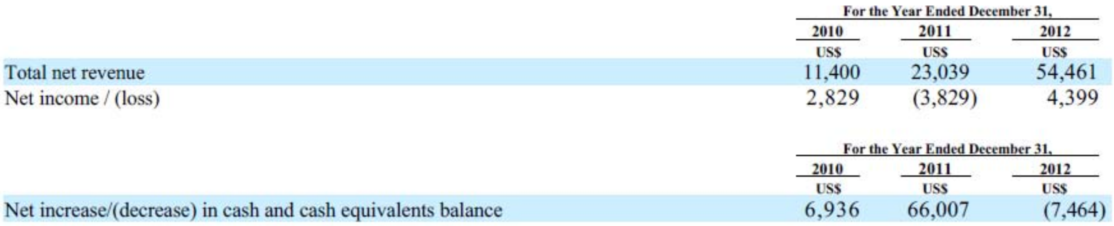

NQ Mobile Inc. (Cayman)
100%
NQ Mobile International AG (Switzerland)
100%
NQ International Ltd. (HK)
100%
Taiwan NQ Technology Limited (Taiwan)
100%
NQ Mobile US Inc. (United States)
100%
FL Mobile Inc. (Cayman)
100%
FL Mobile Hong Kong Limited
100%
NQ Mobile Lux S.A. (Luxembourg)
Offshore
PRC
100%
NQ (Beijing) Co., Ltd. (PRC)
100%
NQ Mobile (Beijing) Co., Ltd. (PRC)
100%
NQ Mobile (Chengdu) Co., Ltd. (PRC)
Contractual Arrangements (1)
Beijing NQ Technology Co., Ltd. (PRC)
55%
Beijing NationSky Network Technology Co., Ltd. (PRC)(2)
100%
QingYun (Tianjin) Financial Management Co., Ltd. (PRC)
100%
Beijing Feiliu Jiutian Technology Co., Ltd. (PRC)
100%
Beijing Red Infinity Technology Co., Ltd. (PRC)
51%
Beijing Fanyue Information Technology Co., Ltd.(3) (PRC)

The proper way to move money into the PRC is by downstreaming cash from NQ Hong Kong to NQ Beijing.  This may be in either the form of registered capital increase (i.e., equity subscription) or a loan from the parent (i.e., NQ Hong Kong).  This is neither a complicated nor lengthy process, and in fact, NQ did this with $20 million in January 2012 that it injected into

NQ Beijing via a registered capital increase.[64] NQ Beijing may then lend money without interest to the VIE, or to shareholders of the VIE. In May 2012, NQ Beijing did just that – it loaned the VIE shareholders RMB 40 million,[65] which was used to increase the registered capital of the VIE. The problem for NQ is that moving money into NQ Beijing is easily tracked and verified because it is a WFOE – there are records in the SAIC files of registered capital increases. In other words, there is a real paper trail when NQ moves money into NQ Beijing. By claiming to have moved money in a way the auditor likely has rarely (or never) seen, NQ would have a much greater ability to commit fraud.

NQ's SEC disclosures and SAIC financials make clear that it is purporting to have loaned IPO dollars directly to the VIE, at some point the funds were somehow converted into RMB, and then the VIE placed the money in a (Level 2) term deposit.

As you can see below, the VIE entities lost $3.8 million in 2011. Yet, cash at the VIE increased by $66 million. Because the Company only generated roughly $12 million in free cash flow, the only source for such an increase in VIE cash is from the parent Company IPO proceeds. At the end of 2010, the Company had cash of $18 million and term deposits of $11.2 million. By the end of 2011, cash was $69.5 million and term deposits were $58.5 million largely as a result of the 2011 IPO that raised $82.9 million. Much of the cash was therefore downstreamed as an intercompany transaction to the VIE from the parent. SAIC financials confirm that NQ purports to have moved money directly to the VIE because they show the VIE as having Other Payables of $78 million as of December 31, 2011; however, the WFOE has no matching receivable.



| | For the Year Ended December 31, | | |
|---|---|---|---|
| | 2010 | 2011 | 2012 |
| | US$ | US$ | US$ |
| Total net revenue | 11,400 | 23,039 | 54,461 |
| Net income / (loss) | 2,829 | (3,829) | 4,399 |

| | For the Year Ended December 31, | | |
|---|---|---|---|
| | 2010 | 2011 | 2012 |
| | US$ | US$ | US$ |
| Net increase/(decrease) in cash and cash equivalents balance | 6,936 | 66,007 | (7,464) |

It is almost inconceivable that NQ would have been able to execute the purported transaction. Because the VIE is owned by PRC nationals, it is considered a "domestically-funded enterprise". It is extremely difficult and rare for a domestic company to get approval to borrow money from offshore. The VIE would have to apply to the National Development and Reform Commission ("NDRC") to borrow from offshore for one year or more. Such approvals are given only to fund loan projects that "are in line with national industrial policies and economic development planning".[66] Loans up to one year would have to be approved by the State Administration of Foreign Exchange ("SAFE").[67] An attorney from a leading PRC law firm that is highly experienced in working with VIEs said that he and his partners had never seen any private

[64] NQ Beijing SAIC files

[65] NQ 2012 20-F, p. 97.

[66] "Provisional Measures Regarding Management of Debt" (National Planning Commission, Ministry of Finance, State Administration of Foreign Exchange Order No. 28) Articles 15 and 16" (《外债管理暂行办法》（国家计划委员会、财政部、国家外汇管理局令第 28 号）第 15 条和第 16 条).

[67] *Id.*

domestic company borrow from off-shore, and that the few instances of which they are aware all involve state-owned enterprise borrowers.

**VIE cash movement, excluding NQ Fujian**

| | 2011 |
|---|---|
| | US$000 |
| OCF excluding other payables | (7,407) |
| ICF | (1,131) |
| Changes in other payables - primary intercompany payables | 72,556 |
| Others | 1,969 |
| Net changes in cash + term deposit | 65,987 |

Note: Others mainly consist of currency translation differences ~$1.5mm.

Transferring cash directly to the VIE would represent worst practices for managing risks of theft and other misconduct inherent in VIE structures, and would make no legitimate business sense. Note that in the corporate structure supra, NQ shareholders do not own the VIE – rather, Chairman Lin and two associates do. In practice, the various agreements constituting the VIE package give public company shareholders little protection against thieving VIE owners. One of the basic tenants of VIE best practices is that as much of the company's value (cash, operating assets, customer agreements, and employees) as possible be kept in the WFOEs (i.e., the entities the public company shareholders own via offshore entities.) The notion that NQ successfully went through the complicated and uncertain offshore borrowing approval procedure in order to manage its cash in a way that contravenes acceptable practices, with no upside (i.e., just to dump into a purported term deposit), does not hold water.

We believe that the onshore cash is far less than what NQ claims, and that it uses a portion of the excess to commit its fraud. We believe that most of the IPO proceeds were diverted, and that portion was funneled into fake counterparties (such as Yidatong) to pay in as revenue. We believe that NQ then uses some of its acquisitions to spit this cash back out to other fake counterparties who will send it back in for more fraudulent sales.

## NQ's Likely Corrupt Acquisitions

There are reasons to believe (apart from the fact that NQ is involved) that NQ's recent acquisitions are likely corrupt transactions. NQ has completed or announced acquisitions totaling $25 million of cash and 15 million ADSes (worth about $350 million at the present stock price).[68]

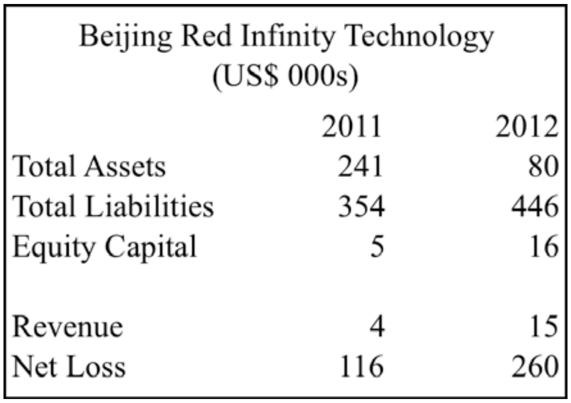
- NQ's acquisition of the remaining 73.4% of Feiliu (aka FL Mobile) for a total of $62.7 million is likely corrupt. Feiliu was of course exposed by CCTV as a co-conspirator in

[68] NQ usually / always makes its acquisitions with common shares. The ADSes are based on the 5:1 conversion ratio.

installing malware onto mobile phones so that NQ could charge users to fix their phones. Just before NQ acquired the remainder of Feiliu, Feiliu added six new shareholders. These shareholders were literally given their equity – NQ decreased its ownership percentage by 4.2% when it handed its shares over to these individuals.

The two new shareholders for whom we have been able to obtain background records are unlikely recipients of shares in the rapidly-growing, dynamic Feiliu. One of the new shareholders, Xie Yuteng, is from a small city in Guangxi province, and is a middle school graduate. Zhong Liang lives in a small city in Jiangxi province, which is not normally considered to be a technology center. In other words, both appear to be villagers. It is a common tactic in China Fraud to use villagers as fake shareholders – sometimes they are paid small sums for their cooperation, other times their identities are used without their knowledge or consent.

- Feiliu's November 2012 acquisition of Beijing Red Infinity Technology Co. Ltd. ("Red") is likely corrupt, as there is a strong chance Red was a tiny company. Red's four shareholders became Feiliu shareholders at the same time as the two (likely) villagers discussed supra. When NQ acquired their Feiliu shares one year late, they received compensation of up to $25.2 million. According to Red's SAIC files, Red was founded in January 2011, and when Feiliu acquired it, Red had received equity capital subscriptions totaling only $16,000 (RMB 100,000). The below are Red's summary financial statements from its SAIC files.



Beijing Red Infinity Technology
(US$ 000s)

| | 2011 | 2012 |
|---|---|---|
| Total Assets | 241 | 80 |
| Total Liabilities | 354 | 446 |
| Equity Capital | 5 | 16 |
| | | |
| Revenue | 4 | 15 |
| Net Loss | 116 | 260 |

- NQ's acquisition, via Feiliu, in January 2013 of 51% of Beijing Fanyue Information Technology Co. Ltd. ("Fanyue) for $0.089 million and 10.5 million shares, is likely corrupt because Fanyue appeared to have been on its way out of business at the time of the acquisition. It was "operating" at a ghost address. According to SAIC files, Fanyue changed its office three months before NQ acquired it. It moved from a real office building to room 1313 of the Jingshui hotel.[69] When our investigator went to the hotel, he found that there is no room 1313. The hotel staff had never heard of Fanyue, but speculated that the room to which 1313 refers is a conference room. A mining company presently rents it. Even at present, Fanyue's website lists no contact phone number or

[69] Room 1313, Jingshui Hotel, No. 10, Puhui Beili, Haidian District, Beijing (北京市海淀区普惠北里10号北京市京水宾馆)

address – just two QQ handles and email addresses. It appears to be another company that does not want to be found.

- NQ's acquisition of 31.71% of Hesine for $0.5 million and 3.5 million shares is likely corrupt, because Hesine moved into a 160 square foot office one year after NQ acquired it, and Hesine's business fell off a cliff.

- NQ's 30% acquisition of Pansi for up to $2.9 million is likely corrupt because Pansi appears to have been on its way out of business at the time of the acquisition. Pansi was "operating" at a ghost address

- NQ's $38 million of acquisition of NationSky could be a corrupt acquisition because its SAIC financial statements, which show 2012 revenue of $15.2 million, appear to be fraudulent. For analysis of the fraud indicia in its financial statements, see Appendix B.

We theorize that the real purposes of these acquisitions are 1) to generate cash that will be recycled into NQ as fake revenue, and 2) line the pockets of the perpetrators. NQ is paying substantial amounts of shares for these companies, and because the monetization occurs outside of China, it would be quite easy to book this cash as international revenue.

## NQ's Future is as Bleak as its Past

NQ is attempting to pivot to a fraud that it hopes will be less obvious – gaming and advertising revenue. NQ's focus on gaming and advertising will not allow it to "grow into the fraud" by generating real numbers approaching its fraudulent ones. NQ's new purported strategy is predicated on NQ having the lowest user acquisition costs in the world – otherwise one would not expect to see a mobile security company go into gaming and advertising. Because NQ has a fraction of the users it claims, and in reality possibly the highest user acquisition cost in the world, this strategy will inevitably fail to produce real profits. Before Chairman Lin realized that there was a good fraud reason to push the myth of generating advertising revenue, he explained why advertising is incompatible with being a mobile security company, which is a logical argument (for a real company).

NQ's gaming strategy is being executed through its now wholly-owned subsidiary Feiliu. (Feiliu was responsible for the malware installs exposed by CCTV.) NQ has likely fraudulently inflated the value of Feiliu by many times (see NQ's SAIC Financials are Fraudulent, Leading to Fraudulent SEC Financials). In speaking with a recently departed NQ gaming employee, we learned that the revenue of NQ's top games is a fraction of what NQ leads investors to believe. We also learned that many of the managers and employees responsible for leading NQ's overseas gaming charge have also recently left.

NQ's purported pivot into gaming is predicated on the fraudulent assertion that its user acquisition costs are the lowest in the world. Co-CEO Omar Khan made this clear during a May, 2013 interview:[70]

> Q: So how did you get from mobile to security to in app advertising and mobile gaming? I'm not necessarily seeing a direct correlation between the IP there.
>
> A: "It's really about the platform. The fact that we built a platform where we can acquire users in over 150 countries, or have billing integrated in local currencies in over 60 countries, our ability to do that in an economical fashion. Today we can acquire users in between, at about seven cents per registered user on a blended basis. That's a very advantageous economic scenario. So the question we then asked ourselves is 'What additional content types can we then run through that engine?' I think it's a similar evolution if you 12 years ago, or whenever it was, you had Jeff onstage at any of your conferences at Amazon and said 'Ok, how are you going to run your business?'

NQ's consumer monetization platform is a myth, and that reality voids any legitimate rationale for focusing on gaming. NQ has far fewer users than it claims, and generates a fraction of its purported revenue – its user acquisition costs are therefore far higher than seven cents per registered user.

Chairman Yu Lin explained in January 2013 why NQ would not look to advertising to monetize users:

> "Why don't we take ads? I think the format of ads on mobile phones is not mature yet. Furthermore, there is a fundamental conflict between our safety service, by its very nature, and the advertising model. If you want to target ads accurately, there will be privacy issues."[71]

Yet, here is Chairman Lin discussing NQ's exciting progress in generating advertising revenue in August 2013:

> "I am pleased to report that we again achieved record revenues in the second quarter of 2013," commented Dr. Henry Lin, Chairman and Co-Chief Executive Officer of NQ Mobile. "We are excited about the progress of our expanded monetization efforts across our platform. As a leading mobile Internet platform, we will continue to grow our user base around the world and broaden our monetization capabilities. We are now not only generating security subscription revenues but significant gaming and advertising revenues as well. This is only the beginning of our exciting journey forward."[72]

We learned from a recently departed gaming division employee that NQ's three best selling games are: Dragon Summons, War Fire, and Fight of the Three Kingdoms. According to the

[70] http://allthingsd.com/20130524/omar-khan-on-security-china-and-the-state-of-the-mobile-industry-video/ at 7:15

[71] http://knowledge.wharton.upenn.edu/article/nq-mobiles-henry-lin-we-have-been-a-global-company-from-day-one/

[72] http://ir.nq.com/phoenix.zhtml?c=243152&p=irol-presentations

former employee, Dragon Summons generated about $1.6 million in gross revenue in its first six months; and, that the gross margin is only about 40%. (The former employee said the gross margin is low in part because of payment processing costs.) NQ tells investors that Feiliu's gross margin is similar to that of NQ's (ex-NationSky), which is about 75%.[73] The former employee also believes that Fight of the Three Kingdoms is generating about $1,650 per day ($600,000 annually); and, War Fire is generating about $1,300 per day ($500,000 annually). If the former employee is correct, it is likely that Feiliu's real revenue, profit margin, and profit are far lower than NQ claims. (NQ recently advised that Feiliu is at a run rate of $40 million.[74] Considering that Feiliu only started to generate mobile gaming revenue in 2012,[75] the purported run rate would be truly amazing if true.)

NQ has stopped putting resources into international gaming and a number of the China side employees hired for international gaming have left, according to the former employee. If true, this would contradict NQ's Q2 2013 statement that Feiliu would expand into North America in September 2013.[76] NQ changed Feiliu's name to "FL Mobile" in Q1 2013 in anticipation of taking the rest of the world by storm.[77]

## NQ's Filings Make Clear that PwC's Audits Were Sloppy

There are clear signs that PwC's audits of NQ were sloppy. It is very difficult to know from the outside how diligently an auditor performed its audit of a given company. Knowing that an auditor is Big Four means little because the quality of the work within the same firm can range widely. The experience of a former junior auditor with a Big Four firm in the UK is instructive in this regard. At one of the UK offices to which he was assigned, junior auditors received bonuses for finding issues during the audit. Yet at a different UK office at which he worked, juniors were evaluated in large part based on how quickly they worked. Fraudulent companies often force their auditors to do sloppy jobs by creating delays during the audit process. (To learn how important the audit slowdown tactic is to furthering fraud, see: www.whitecollarfraud.com.)

The tells that NQ's audits were sloppy are:

- Failure to ensure that disclosures about cash balances by entity are correct. (As we explain in *NQ's Cash Balance (a Level 2 Asset) is Highly Likely to be Fraudulent*, we suspect that much of the cash on NQ's balance sheet is not really there.)
- Classifying Cash and Equivalents as a Level 2 asset in 2012, and reclassifying 2011 Cash and Equivalents as Level 2. We cannot conceive of a circumstance under which Cash and Equivalents could be Level 2 assets. If this was not a sloppy mistake, then PwC should require NQ to disclose the special circumstances surrounding its Cash balance.
- Not booking restricted share issuance related to performance issuance.
- Failure to ensure that share-based compensation is recorded at the correct entity.

[73] NQ Q4 2012 earnings conference call.
[74] NQ Q2 2013 earnings conference call.
[75] NQ 2012 20-F, pp. 7-8.
[76] NQ Q2 2013 earnings conference call.
[77] *id*.

- Failure to validate that receivables from NQ's largest purported trade debtor, Yidatong ("YDT"), are aged over four months beyond what the contracts permits.
- Permitting NQ to reclassify significant costs from Cost of Sales to R&D, which substantially boosted NQ's gross margin.

## Cash

At December 31, 2011, the Company reported consolidated cash and cash equivalents of $69 million and parent company cash of $49 million. That means that $20 million of cash was at the VIE and/or subsidiaries of the Parent. However, the VIE reported a net increase/(decrease) in cash and cash equivalents of $66 million. With the amount of consolidated cash and cash held at the parent, and since the VIE lost money and the WFOE did not generate much cash, it is not possible for the VIE cash to increase by $66 million. Therefore, the auditor failed to properly audit the change in cash and cash equivalents.

The consolidated term deposit balance was $58.5 million and the parent co term deposit was $0. Our view is that for the numbers to balance, the VIE would have to have invested in term deposits and that the increase in cash and cash equivalents would be lower by such amount. Our view is also that only source of cash to the VIE was from the IPO proceeds at the parent. Recall, our view is that the cash probably is no there at all and this is just a book keeping/balancing exercise.

Our analysis of the SAIC filings for 2011 confirm that the Company booked everything as cash and cash equivalents. However, this accounting is not correct under Chinese GAAP. Term deposits should be accounted for as an investment and not treated as cash and cash equivalents. Therefore, we can reasonably assume that the auditors did not check the bank account statements and have relied on the Company's internal reports for cash and cash equivalent disclosures. We question the audit procedures and if PWC has qualified accounting staff working on this audit. A basic back of the envelope calculation would show that it was not possible for cash and cash equivalents to have increased by the amount disclosed given the amount of cash and cash equivalents on a consolidated basis and at the parent level.

## Level 2 Cash

It's hard to imagine a scenario where cash and cash equivalents would be a level 2 asset. But, surprisingly, the auditor classified 2012 cash and cash equivalents as a level 2 asset and also reclassified 2011 cash and cash equivalents to level 2 from level 1. According to a PwC FAS 157 information memorandum

Level 1 inputs – observable, quoted prices for identical assets or liabilities in active markets. Examples include US government and agency securities, foreign government debt, listed equities and money market securities.

Level 2 inputs – quoted prices for similar assets or liabilities in active markets; quoted prices for identical or similar assets in markets that are not active; and inputs other than quoted prices e.g.

interest rates and yield curves. Examples include corporate bonds (investment grade, high yield), mortgage-backed securities, bank loans, loan commitments, less liquid listed equities, municipal bonds and certain OTC derivatives.

Based on the definition of cash and cash equivalents, our view is that the auditor was either not able to verify the cash or it's just another sign of a sloppy audit.  The reclassification of the 2011 cash is a concern since that would imply that the auditor did see something since none of the cash and cash equivalents was put into level 1 assets as one would expect.

As you can see from the level 2 definition, level 2 assets are much more risky and more difficult to value (compared to level 1 assets).  The combination of cash at the VIE and the reclassification to Level 2 from Level 1 is a red flag.  Especially, since we believe it was not transferred to the VIE in accordance with Chinese regulations.

## Share Based Compensation

The Company is underreporting and misallocating share based compensation at the parent company.  For 2012, the Company expensed $24.5 million in share based compensation and disclosed $1.84 million cash compensation to executive officers and directors.  Over the same timeframe, the Company booked $5.6mm of total G&A expenses (or 9% of total operating expenses) at the parent of which we believe no share based compensation was allocated.  We believe that share based compensation was also not allocated to the parent operations in 2011 and 2010.  First, the Company footnotes that share based compensation was included in the consolidated financial statements while no such footnote was included in the parent company footnotes.  Second, our analysis of the VIE and WFOE 2011 financial data shows that a nominal amount, if any, share based compensation was accounted for at these operating entities.  With the parent generating $20 million in sales (approximately 22% of total sales) and the VIE and WFOE generating the majority of the remaining revenues, the accounting and allocation of share based compensation appears to be another sign of a sloppy audit.  A substantial amount of the share based compensation was from US management and therefore should have been allocated to the parent in a much higher amount than shown.

## Yidatong is not paying pursuant to the terms of the contract or in line with normal trade terms.

The contract between Yidatong and NQ calls for settlement in one calendar month with payment on the 15th of the next calendar month.  One calendar month settlement terms are normal trade terms and consistent with the contract between NQ and China Mobile which also call for one month settlement with payment being done on the 15th of each month[78].  One month settlement is what other carriers have told us as well as retailers that sell NQ apps, including Telefónica and Verizon resellers.

[78] https://www.bj.10086.cn/Portals/0/revision/images/mwsphzglssdxywfc.pdf

Yidatong has DSO of more than 4 months. The actual realized payment terms are far beyond industry norms. This combined with the annual advances that NQ makes to Yidatong, and SAIC files that show much lower sales and amounts due to NQ, is a clear sign that something is wrong with this picture. What are the auditors looking at (or are they doing more listening that looking)?

## Reallocation of Costs to Boost Gross Margin.

In order to give the appearance of high gross margins, the Company has reclassified a material amount of expenses from cost of goods sold to R&D. Based on our analysis of 2011 SAIC files, R&D expenses increased by 10x (or $4.5mm) during consolidation as a result of a shift in costs.

| | 2011 | | | | | |
|---|---|---|---|---|---|---|
| | **Paren t** | **VIE** | **WFOE** | **Combined** | **Consolidation adj and other entities** | **Consolidated** |
| US$000 | | | | | | |
| Revenues, net | 17,858 | 25,503 | 17,781 | 61,142 | (20,471) | 40,671 |
| Cost of revenues | 791 | 20,983 | 1,659 | 23,433 | (15,376) | 8,057 |
| **Gross profit** | **17,067** | **4,520** | **16,122** | **37,710** | **(5,096)** | **32,614** |
| Operating expenses | | | | | | |
| Selling and marketing expenses | 1,575 | 2,259 | 5,547 | 9,381 | (1,426) | 7,955 |
| General and administrative expenses* | 1,083 | 2,056 | 2,055 | 5,195 | 8,829 | 14,024 |
| Research and development expenses* | 156 | 381 | - | 537 | 4,558 | 5,095 |
| **Total operating expenses** | **2,814** | **4,696** | **7,602** | **15,112** | **11,962** | **27,074** |

The Company discloses that most of the R&D is done in China. Therefore, it is surprising to see such a large increase in R&D and a related decrease in cost of goods sold. Also, there are incentives for Chinese companies to book as much to R&D as possible as a result of tax incentives.

## Appendix A: U.S. Store Visits

| MSA | Store | Address | City | Carry NQ? | What % of new phone buying customers buy any NQ product or app? | Promotional Materials? |
|---|---|---|---|---|---|---|
| Atlanta | Diamond Wireless | 3393 Peachtree Road NE, #19 | Atlanta | Yes | Haven't started integrating NQ products yet | Not sure what happened to display |
| Atlanta | Go Wireless | 3927 Buford Hwy NE, Suite D | Atlanta | Yes | 2%-3% | Yes |
| Atlanta | Target | 1275 Caroline Street NE | Atlanta | Yes | Hasn't sold one product in three weeks. | Yes |
| Atlanta | Target | 2539 Piedmont Rd NE | Atlanta | Yes | 10% | Yes |
| Atlanta | Target | 5570 Roswell Road | Sandy Springs | Yes | 5% | Yes |
| Atlanta | Target | 2535 Dallas Hwy SW | Marrietta | Refused to Answer | N/A | None |
| Atlanta | Target | 2600 Holcomb Bridge Drive | Alpharetta | Yes | None | No |
| Atlanta | Target | 3935 Venture Dr | Duluth | Yes | None | Yes |
| Atlanta | Target | 1405 Johnson Ferry Rd | Marrietta | Yes | None in the last month | Yes |
| Boston | Go Wireless | 34 Whiting St Rt 53 | Hingham | Yes | Sells 3-4 products per week on average, with a 20 per week maximum | Yes |
| Boston | Target | 250 Granit St, Ste 21 | Braintree | Yes | Around 1-2 products per month | No |
| Boston | Target | 1167 Washington St | Hanover | Yes | None | Yes, but not on display. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Boston | Target | 385 Centre Avenue | Abington | Yes | None | Yes, but had to retrieve from lower cabinet; brochures were still sealed in plastic wrap. |
| Boston | Target | 1 Hawes Way | Stoughton | Yes | Around 3 products per month | None |
| Boston | Target | 400 Cochituate Road | Framingham | Yes | None | None |
| Boston | TCC Wireless | 373 Centre Avenue | Abington | Yes | 25% of Android phones sold. | Yes |
| Boston | TCC Wireless | 307 Boston Road | North Billerica | Yes | Around 50% of Android phones sold | Yes |
| Chicago | Target | 2241 Willow Road | Glenview | Yes | 5%-10% | No - they get brochures form the office on inquiry. |
| Chicago | Target | 401 W Irving Park Road | Wood Dale | No, and they didn't know what the product was | N/A | N/A |
| Chicago | Target | 60 Yorktown Shopping Ctr | Lombard | No, and they didn't know what the product was | N/A | N/A |
| Chicago | Target | 1154 S Clark St | Chicago | Yes | None | None |

| | | | | | | |
|---|---|---|---|---|---|---|
| Chicago | Target | 1101 W Jackson Blvd | Chicago | No | N/A | N/A |
| Chicago | Target | 2939 W Addison St | Chicago | No | N/A | N/A |
| Chicago | Target | 2112 W Peterson Ave | Chicago | No | N/A | N/A |
| Chicago | TCC Wireless | 13041 LaGrange Road | Palos Park | Refused to Answer | N/A | N/A |
| Chicago | TCC Wireless | 2518 Greenbay Road | Evanston | Yes | 50%-60% | Yes |
| Chicago | TCC Wireless | 7261 W. Lake Street | River Forest | Yes | 50% | Yes |
| Dallas | Diamond Wireless | 6121 West Park Boulevard, #B 102 | Plano | No, and had never heard of the product | N/A | N/A |
| Dallas | Target | 2200 Dallas Pkway | Plano | Yes | Around 1-2 products per month | Yes |
| Dallas | Target | 120 W Parker Rd | Plano | Yes | Around 1-2 products per month | Yes |
| Dallas | Target | 4701 Lakeview Pkwy | Rowlett | Yes | None | Yes |
| Dallas | Target | 16731 Coit Rd | Dallas | Yes | None | Yes |
| Dallas | Target | 212 Medallion Shp Ctr | Dallas | Yes | None | Yes |
| Dallas | Target | 2417 N Haskell Ave | Dallas | Yes | None | Yes |
| Dallas | Target | 9440 Marsh Lane | Dallas | Yes | None | Yes, but difficult to find |
| LA | 4G Wireless | 8342 Lincoln Blvd | LA | Yes | None | Yes |
| LA | 4G Wireless | 1751 Artesia Blvd, Suite B | Manhattan Beach | No | N/A | N/A |
| LA | 4G Wireless | 8726 S Sepulveda Blvd, Suite C | LA | Yes | One product in three months | Yes |

| | | | | | | |
|---|---|---|---|---|---|---|
| LA | Diamond Wireless | 8014 Los Cerritos Center, #9014 | Cerritos | No | N/A | N/A |
| LA | Target | 1601 Kingsdale Ave | Redondo Beach | Yes | Only sold one so far | Yes |
| LA | Target | 11525 South St | Cerritos | Yes | Approximately 15% | Yes |
| LA | Target | 1200 N Sepulveda Blvd | Manhattan Beach | Yes | None | Yes |
| Miami | Target | 300 Hollywood Mall | Hollywood | Yes | None | Yes, but brochures were in cabinet |
| Miami | Target | 1750 W 37th St | Hialeah | Yes | Less than 1% | One flyer they were able to find after searching |
| Miami | Target | 5601 NW 183rd St | Miami Gardens | Yes | Around two products per month | Store recently reorganized displays; NQ displays still in storage; ran out of brochures, and hasn't been able to get more |
| Miami | Target | 5800 S University Dr | Davie | Yes | None | None |
| Miami | Target | 20500 SW 112th Ave | Miami | Yes | 1-2 products per month | None |
| Miami | Target | 11253 Pines Blvd | Pembroke Pines | Yes | Very few, if any | None |
| Miami | Target | 16901 Miramar Pkwy | Miramar | Yes | 6-7 products in the last three months | Yes |
| Miami | Wireless | 3331 Hollywood Blvd | Hollywood | Yes | 0-1% | Yes |
| NYC | A Wireless | 235 Propect Ave | West Orange | Yes | 10% | None |
| NYC | Target | 1598 Flatbush Ave | Brooklyn | Yes | Zero | None |

| | | | | | | |
|---|---|---|---|---|---|---|
| NYC | Target | 139 Flatbush Ave | Brooklyn | Yes | 20% | Yes |
| NYC | Target | 900 Bergen Town Ctr | Paramus | Yes | None | Yes, but in locked drawers, not displayed for customers |
| NYC | Target | 100 14th St | Jersey City | No | None | None |
| NYC | Target | 45 Central ave | Clark | No | None | None |
| NYC | Target | 632 Route 46E | Fairfield | No | N/A | N/A |
| NYC | Target | 100 Parsonage Road | Edison | Yes | Approximately 5% | Yes |
| Riverside | 4G Wireless | 2002 N Riverside Ave, Ste 103 | Rialto | Had not received the products yet | N/A | Had materials, hadn't put them on display yet |
| Riverside | 4G Wireless | 12761 Moreno Beach Dr., Ste 102 | Moreno Valley | Yes | Only a small percentage | Yes |
| Riverside | 4G Wireless | 497 E Alessandro Blvd, Suite C-1 | Riverside | No | Used to offer NQ products, but discontinued because there were no sales | None |
| Riverside | Diamond Wireless | 1299 Galleria At Tyler, #5549 | Riverside | No | N/A | N/A |
| Riverside | Go Wireless | 3782 Tyler Street, Suite A | Riverside | Yes | Only a few | Yes |
| Riverside | Go Wireless | 1180 Hamner Ave, Suite A | Norco | Yes | Only a few | Yes |
| Riverside | Target | 3333 Arlington Ave | Riverside | Yes | Only sold a few | Yes |
| Riverside | Target | 2615 Tuscanny | Corona | Yes | Not sure | None |
| Riverside | Target | 1290 Hamner Ave | Norco | Yes | None | Yes, but in locked cabinet not displayed for customers |
| San Francisco | 4G Wireless | 775 La Playa Dr | Hayward | Yes | None | Yes |
| San Francisco | 4G Wireless | 1398 Fitzgerald Dr | Pinole | Yes | None | None |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| San Francisco | 4G Wireless | 3631 Mount Diablo Blvd, Ste A | Lafayette | Yes | 10% | Yes |
| San Francisco | 4G Wireless | 1513 Sloat Blvd | San Francisco | No | No | No |
| San Francisco | 4G Wireless | 2041 Ralston Drive | Belmont | Yes | Only 2 products so far | Yes |
| San Francisco | Diamond Wireless | 1150 El Camino Real, K21 | San Bruno | No | N/A | N/A |
| San Francisco | Target | 1400 Fitzgerald Drive | Pinole | Yes | 10% | Yes |
| San Francisco | Target | 789 Mission Street | San Francisco | Yes | Only 1 product so far | Yes |
| San Francisco | Target | 133 Serramonte Center | Daly City | Yes | None | Yes |
| San Francisco | Target | 2220 Bridgepoint Pkwy | San Mateo | Yes | Don't know | Yes |
| Washington, DC | Target | 25 Grand Corner Ave | Gaithersburg | Yes | 10% | Yes |
| Washington, DC | Target | 5700 Bou Ave | Rockville | Yes | 20% | Yes |
| Washington, DC | Target | 10301 New Guinea Rd | Fairfax | No | 25%-30% | Yes |
| Washington, DC | Target | 6600 Springfield Mall | Springfield | Yes | 20% | Yes |
| Washington, DC | Target | 2905 District Ave | Fairfax | Yes | 15% | Yes, but not easy to find |
| Washington, DC | Target | 3100 14th Street NW Ste 201 | Washington | No | None | None |
| Washington, DC | TCC Wireless | 6230-X Rolling Road | Springfield | No | None | No |

## Appendix B: SAIC Financial Fraud Indicia

NQ's book cookers made the following tax-related errors in producing fraudulent financials for its various entities.

- Claiming that in 2011, NQ Beijing paid a sales tax called "Business Tax", rather than VAT. NQ claims that NQ Beijing began paying VAT in lieu of Business Tax in 2012 due to the expansion of a VAT pilot program to Beijing.[79] Software sales have been subject to VAT since 2001.[80] The VIE and WFOE obtained their software developer VAT certificates in 2006 and 2008, respectively. In order to maintain the VAT certificates, the companies would have needed to pay VAT on prior years software sales. The expansion of the pilot program to Beijing applied to industries other than software sales,[81] and thus would not have necessitated a sudden shift to VAT in 2012. The likely explanation is that the book cooker realized that because VAT is administered more closely than Business Tax, it was advantageous to claim NQ is a Business Tax payer; however, the 2012 VAT reform gave NQ less room to maneuver with its auditor.

- NQ Beijing's 2011 SAIC financials show that the company essentially paid no Business Tax, despite claiming that NQ Beijing was subject at the time to Business Tax of 3% to 5%.[82] NQ Beijing's 2011 income statement shows NQ Beijing's purported 2011 domestic revenue as being RMB 113.6 million. (Business Tax only applies to domestic revenue.) However, the income statement shows that NQ Beijing paid only RMB 8,000 (eight thousand) in Business Tax and surcharges in 2011. NQ Beijing should have paid at least RMB 3.4 million (340K, or 0.3% of revenue) in 2011 Business Tax.[83]

- In 2012, NQ Beijing's book cooker had the opposite problem. While the SEC filings claim that NQ Beijing began paying VAT in 2012, the SAIC income statement shows that NQ Beijing paid RMB 6.3 million in business tax on RMB 154.7 million in domestic sales. NQ Beijing should have paid far less in Business Tax and surcharges because at least 35% of the revenue should be taxed with VAT, in addition to the revenue being taxed with VAT under the pilot reform. Under PRC GAAP, VAT payments are not recorded in income statement accounts – they are only shown only as taxes payable on the balance sheet. Therefore, the RMB 6.3 million is not mislabeled VAT. It is just another mistake NQ made because its financials are fraudulent.

- NQ Beijing's SAIC financials fail to recognize as Non-Operating Income any VAT credits or refunds received. Once again, NQ's book cooker struggled with the taxes relevant to revenues. To understand the VAT problem, one first needs to understand NQ's claim about NQ Beijing's income tax treatment. NQ claims that NQ Beijing receives a corporate income tax preference for qualified software companies. In order to

[79] 2012 20F, p. F-29.

[80] http://www.xm-n-tax.gov.cn/gswz/jsp/fgkcx/xl.jsp?bm=200506031617445742

[81] http://www.chinatax.gov.cn/n8136506/n8136593/n8137537/n8138502/11735466.html

[82] 2012 20F, p. F-29.

[83] VAT for qualified software companies would be 3% of sales after refund. If all sales are VAT sales, the business tax and surcharge will be at least sales*3%*10% (10% surcharge rate)

qualify for this income tax preference, at least 35% of NQ Beijing's revenue would have to come from software sales. At least half of the software sold must be developed in-house.

The effective VAT for in-house developed software is 3% of sales, which consists of the 17% statutory VAT NQ pays on its software sales, netted against a) VAT it paid on its inputs, which are generally very low for software companies, and b) a credit or refund from the tax bureau sufficient to ensure the effective VAT is 3%. Again, NQ Beijing's SAIC financials show that its domestic revenue was RMB 113.6 million and RMB 154.7 million in 2011 and 2012, respectively.

PRC GAAP mandates that the VAT credit or refund be recognized as Non-Operating Income.[84] However, NQ Beijing had no such income in either 2011 or 2012. If NQ Beijing's SAIC financials were not fraudulent, they would show at least a few million RMB in Non-Operating Income in each year. Per a newsletter posted by the Haidian Tax Bureau (the tax bureau that receives taxes from NQ Beijing), cumulative VAT refunds to approximately 2,000 Haidian software companies in 2011 exceeded RMB 380 million (an average of about RMB 200,000 per company).[85]

- Omitting from NQ's 2011 prospectus a purported income tax preference for NQ Beijing. In the prospectus, NQ stated that NQ Beijing "was subject to the prevailing income tax rate of 25% on taxable income for the years ended 2008, 2009, and 2010."[86] However, in the 2011 20-F filed only 10 months later, NQ stated that NQ Beijing "was qualified as a software enterprise under the New CIT Law, which was entitled to enjoy preferential income tax treatment of income tax exemption for the first two years when it became profitable, followed by three years of preferential income tax rate of 12.5% up to 2015…Therefore, NetQin Beijing was not required pay any income tax for the years ended December 31, 2009, 2010, and 2011."[87] Omitting a tax preference from the prospectus is much less likely when the company's financials are genuine.

- NQ's SEC disclosures and SAIC financials show that NQ is shifting impermissibly high amounts of income from NQ's variable interest entity ("VIE") to NQ Beijing in order to avoid paying income tax. NQ claims that NQ Beijing was exempt from corporate income tax in 2011, while the VIE paid corporate income tax at 15%.[88] Under NQ's onshore corporate structure, the vast majority of NQ Beijing's 2011 revenue consisted of sales to the VIE. The year before (2010), NQ Beijing only booked RMB 1.5 million in revenue, so the VIE would not have been shifting revenue to it until 2011.

  By purporting to shift about two-thirds of the VIE's revenue to NQ Beijing in 2011, NQ lowered the VIE's gross margin from 62% in 2010 to 17% in 2011. Purportedly as a result of this shift, the VIE paid only RMB 106,000 in income taxes in 2011, which was

[84] http://www.tjsat.gov.cn/bd/0200/020002/20120508172346812.html
[85] http://www.bjsat.gov.cn/BJSAT/qxfj/hd/sy/zfxxgk/zfxxgkml/gzdt/201112/t20111209_74408.html
[86] 2012 20F, p. F-30.
[87] 2011 F0F, p. F-28.
[88] 2011 20F, p. F-28.

only 27.7% of the VIE's 2010 income taxes, while the VIE's purported revenue grew 193.2% in 2011.

NQ Beijing and the VIE are located in the same building and pay taxes to the same district tax office. PRC tax law requires business between related entities to be conducted at prices equivalent to those for arms length transactions.[89] It is implausible that the VIE would be permitted to shift this much profit from an entity that pays income taxes to one that does not.

The reason NQ's SAIC financials show this revenue shift is because the Company pays minimal PRC taxes because it has far less profit than it claims. The Company's SAIC and SEC financials are fraudulent.

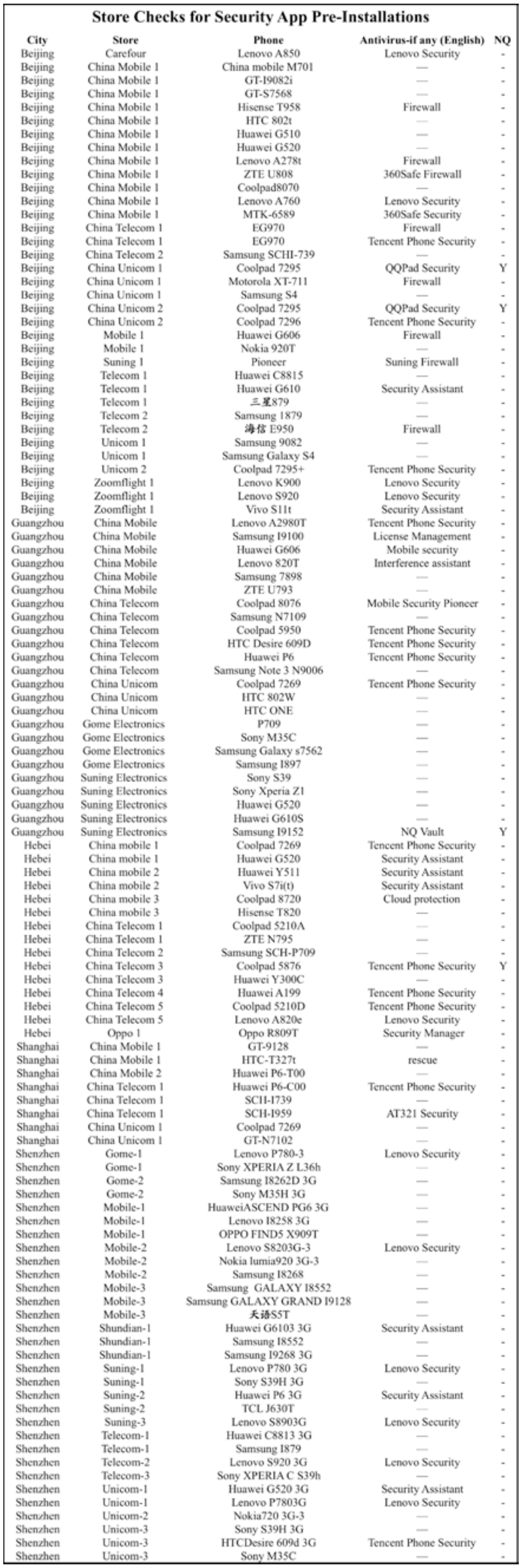
- NQ claims that Beijing Feiliu ("FL Mobile" or "FL") pays no income tax in 2012 and 2013, and a reduced rate thereafter because it was approved for a software enterprise tax preference under the new tax law.[90] This is not true. The preference is only available for newly-established software companies. FL was established in 2009, but obtained qualified software company status only in 2011.[91] (FL would have gone through the qualification process after establishment in order to be eligible for VAT refunds.) In order to enjoy the tax holiday, FL would need to have obtained its qualification in 2010.

  FL's tax preference (forgetting the qualification timing issue) would only be valid for two years from and including its first profitable year. NQ reported in its 20-F a US GAAP profit of $119,000 in 2011 on sales of $2.1 million (from SAIC). [92] It is unlikely that FL was unprofitable in 2011 for PRC tax accounting purposes. The claim that FL would not have to pay tax in 2013 seems to be another example of bungled tax treatment resulting from fraudulent accounting.

- NationSky's balance sheet shows too few taxes due as of December 31, 2012. NQ purports that Nation Sky generated $12.6 million of revenue in 2012, although NationSky's SAIC financials actually show $15.2 million of revenue. (The profit numbers are essentially the same though.) Chinese companies file monthly tax returns for VAT and Business Tax, while they file income tax returns on a quarterly basis. The yearend taxes payable balance should be at least approximately RMB 600,000. The balance sheet shows only RMB 38,000 payable.

  Another suspicious element of NationSky's income statement is that its 2012 sales and marketing expenses of only $479,000 seem too low to support a sales, presales, and marketing staff of over 80 people in 10 offices.

[89] http://www.chinatax.gov.cn/n8136506/n8136593/n8137681/n8817331/n8817348/8820018.html.
[90] NQ 2012 20F, p.F-37
[91] http://www.chinasoftware.com.cn/GGDetail3.asp?sID=5897&ssID=233990#233990
[92] NETC, FY 2011, 20F, F-35



## Store Checks for Security App Pre-Installations

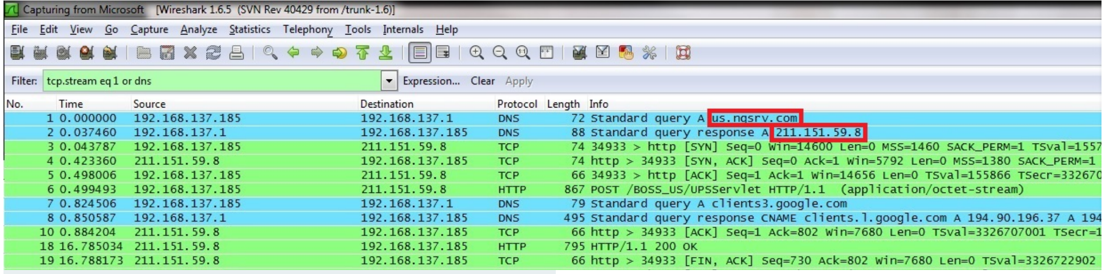
| City | Store | Phone | Antivirus-if any (English) | NQ |
|---|---|---|---|---|
| Beijing | Carefour | Lenovo A850 | Lenovo Security | - |
| Beijing | China Mobile 1 | China mobile M701 | — | - |
| Beijing | China Mobile 1 | GT-I9082i | — | - |
| Beijing | China Mobile 1 | GT-S7568 | — | - |
| Beijing | China Mobile 1 | Hisense T958 | Firewall | - |
| Beijing | China Mobile 1 | HTC 802t | — | - |
| Beijing | China Mobile 1 | Huawei G510 | — | - |
| Beijing | China Mobile 1 | Huawei G520 | — | - |
| Beijing | China Mobile 1 | Lenovo A278t | Firewall | - |
| Beijing | China Mobile 1 | ZTE U808 | 360Safe Firewall | - |
| Beijing | China Mobile 1 | Coolpad8070 | — | - |
| Beijing | China Mobile 1 | Lenovo A760 | Lenovo Security | - |
| Beijing | China Mobile 1 | MTK-6589 | 360Safe Security | - |
| Beijing | China Telecom 1 | EG970 | Firewall | - |
| Beijing | China Telecom 1 | EG970 | Tencent Phone Security | - |
| Beijing | China Telecom 2 | Samsung SCHI-739 | — | - |
| Beijing | China Unicom 1 | Coolpad 7295 | QQPad Security | Y |
| Beijing | China Unicom 1 | Motorola XT-711 | Firewall | - |
| Beijing | China Unicom 1 | Samsung S4 | — | - |
| Beijing | China Unicom 2 | Coolpad 7295 | QQPad Security | Y |
| Beijing | China Unicom 2 | Coolpad 7296 | Tencent Phone Security | - |
| Beijing | Mobile 1 | Huawei G606 | Firewall | - |
| Beijing | Mobile 1 | Nokia 920T | — | - |
| Beijing | Suning 1 | Pioneer | Suning Firewall | - |
| Beijing | Telecom 1 | Huawei C8815 | — | - |
| Beijing | Telecom 1 | Huawei G610 | Security Assistant | - |
| Beijing | Telecom 1 | 三星879 | — | - |
| Beijing | Telecom 2 | Samsung 1879 | — | - |
| Beijing | Telecom 2 | 海信 E950 | Firewall | - |
| Beijing | Unicom 1 | Samsung 9082 | — | - |
| Beijing | Unicom 1 | Samsung Galaxy S4 | — | - |
| Beijing | Unicom 2 | Coolpad 7295+ | Tencent Phone Security | - |
| Beijing | Zoomflight 1 | Lenovo K900 | Lenovo Security | - |
| Beijing | Zoomflight 1 | Lenovo S920 | Lenovo Security | - |
| Beijing | Zoomflight 1 | Vivo S11t | Security Assistant | - |
| Guangzhou | China Mobile | Lenovo A2980T | Tencent Phone Security | - |
| Guangzhou | China Mobile | Samsung I9100 | License Management | - |
| Guangzhou | China Mobile | Huawei G606 | Mobile security | - |
| Guangzhou | China Mobile | Lenovo 820T | Interference assistant | - |
| Guangzhou | China Mobile | Samsung 7898 | — | - |
| Guangzhou | China Mobile | ZTE U793 | — | - |
| Guangzhou | China Telecom | Coolpad 8076 | Mobile Security Pioneer | - |
| Guangzhou | China Telecom | Samsung N7109 | — | - |
| Guangzhou | China Telecom | Coolpad 5950 | Tencent Phone Security | - |
| Guangzhou | China Telecom | HTC Desire 609D | Tencent Phone Security | - |
| Guangzhou | China Telecom | Huawei P6 | Tencent Phone Security | - |
| Guangzhou | China Telecom | Samsung Note 3 N9006 | — | - |
| Guangzhou | China Unicom | Coolpad 7269 | Tencent Phone Security | - |
| Guangzhou | China Unicom | HTC 802W | — | - |
| Guangzhou | China Unicom | HTC ONE | — | - |
| Guangzhou | Gome Electronics | P709 | — | - |
| Guangzhou | Gome Electronics | Sony M35C | — | - |
| Guangzhou | Gome Electronics | Samsung Galaxy s7562 | — | - |
| Guangzhou | Gome Electronics | Samsung I897 | — | - |
| Guangzhou | Suning Electronics | Sony S39 | — | - |
| Guangzhou | Suning Electronics | Sony Xperia Z1 | — | - |
| Guangzhou | Suning Electronics | Huawei G520 | — | - |
| Guangzhou | Suning Electronics | Huawei G610S | — | - |
| Guangzhou | Suning Electronics | Samsung I9152 | NQ Vault | Y |
| Hebei | China mobile 1 | Coolpad 7269 | Tencent Phone Security | - |
| Hebei | China mobile 1 | Huawei G520 | Security Assistant | - |
| Hebei | China mobile 2 | Huawei Y511 | Security Assistant | - |
| Hebei | China mobile 2 | Vivo S7i(t) | Security Assistant | - |
| Hebei | China mobile 3 | Coolpad 8720 | Cloud protection | - |
| Hebei | China mobile 3 | Hisense T820 | — | - |
| Hebei | China Telecom 1 | Coolpad 5210A | — | - |
| Hebei | China Telecom 1 | ZTE N795 | — | - |
| Hebei | China Telecom 2 | Samsung SCH-P709 | — | - |
| Hebei | China Telecom 3 | Coolpad 5876 | Tencent Phone Security | Y |
| Hebei | China Telecom 3 | Huawei Y300C | — | - |
| Hebei | China Telecom 4 | Huawei A199 | Tencent Phone Security | - |
| Hebei | China Telecom 5 | Coolpad 5210D | Tencent Phone Security | - |
| Hebei | China Telecom 5 | Lenovo A820e | Lenovo Security | - |
| Hebei | Oppo 1 | Oppo R809T | Security Manager | - |
| Shanghai | China Mobile 1 | GT-9128 | — | - |
| Shanghai | China Mobile 1 | HTC-T327t | rescue | - |
| Shanghai | China Mobile 2 | Huawei P6-T00 | — | - |
| Shanghai | China Telecom 1 | Huawei P6-C00 | Tencent Phone Security | - |
| Shanghai | China Telecom 1 | SCH-I739 | — | - |
| Shanghai | China Telecom 1 | SCH-I959 | AT321 Security | - |
| Shanghai | China Unicom 1 | Coolpad 7269 | — | - |
| Shanghai | China Unicom 1 | GT-N7102 | — | - |
| Shenzhen | Gome-1 | Lenovo P780-3 | Lenovo Security | - |
| Shenzhen | Gome-1 | Sony XPERIA Z L36h | — | - |
| Shenzhen | Gome-2 | Samsung I8262D 3G | — | - |
| Shenzhen | Gome-2 | Sony M35H 3G | — | - |
| Shenzhen | Mobile-1 | HuaweiASCEND PG6 3G | — | - |
| Shenzhen | Mobile-1 | Lenovo I8258 3G | — | - |
| Shenzhen | Mobile-1 | OPPO FIND5 X909T | — | - |
| Shenzhen | Mobile-2 | Lenovo S8203G-3 | Lenovo Security | - |
| Shenzhen | Mobile-2 | Nokia lumia920 3G-3 | — | - |
| Shenzhen | Mobile-2 | Samsung I8268 | — | - |
| Shenzhen | Mobile-3 | Samsung  GALAXY I8552 | — | - |
| Shenzhen | Mobile-3 | Samsung GALAXY GRAND I9128 | — | - |
| Shenzhen | Mobile-3 | 天语S5T | — | - |
| Shenzhen | Shundian-1 | Huawei G6103 3G | Security Assistant | - |
| Shenzhen | Shundian-1 | Samsung I8552 | — | - |
| Shenzhen | Shundian-1 | Samsung I9268 3G | — | - |
| Shenzhen | Suning-1 | Lenovo P780 3G | Lenovo Security | - |
| Shenzhen | Suning-1 | Sony S39H 3G | — | - |
| Shenzhen | Suning-2 | Huawei P6 3G | Security Assistant | - |
| Shenzhen | Suning-2 | TCL J630T | — | - |
| Shenzhen | Suning-3 | Lenovo S8903G | Lenovo Security | - |
| Shenzhen | Telecom-1 | Huawei C8813 3G | — | - |
| Shenzhen | Telecom-1 | Samsung I879 | — | - |
| Shenzhen | Telecom-2 | Lenovo S920 3G | Lenovo Security | - |
| Shenzhen | Telecom-3 | Sony XPERIA C S39h | — | - |
| Shenzhen | Unicom-1 | Huawei G520 3G | Security Assistant | - |
| Shenzhen | Unicom-1 | Lenovo P7803G | Lenovo Security | - |
| Shenzhen | Unicom-2 | Nokia720 3G-3 | — | - |
| Shenzhen | Unicom-3 | Sony S39H 3G | — | - |
| Shenzhen | Unicom-3 | HTCDesire 609d 3G | Tencent Phone Security | - |
| Shenzhen | Unicom-3 | Sony M35C | — | - |

# Appendix C: Software Engineer Report

## Data is sent from the App to NQ servers located in China

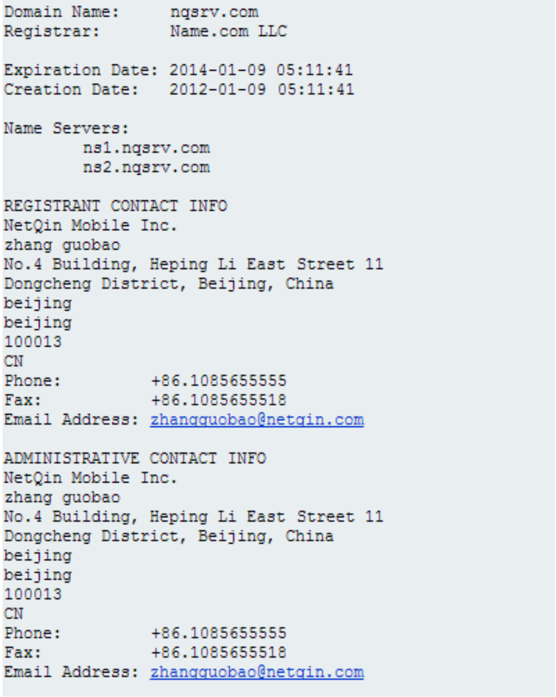
During our investigation we discovered that that app is communicates with remote servers.
We extracted the domains and IP that the app reaches and researched the IP using open source tools and services such as "WhoIs". We were able to show that the sites are located and hosted in china, and are owned by NQ.

http://us.nqsrv.com - 211.151.59.8

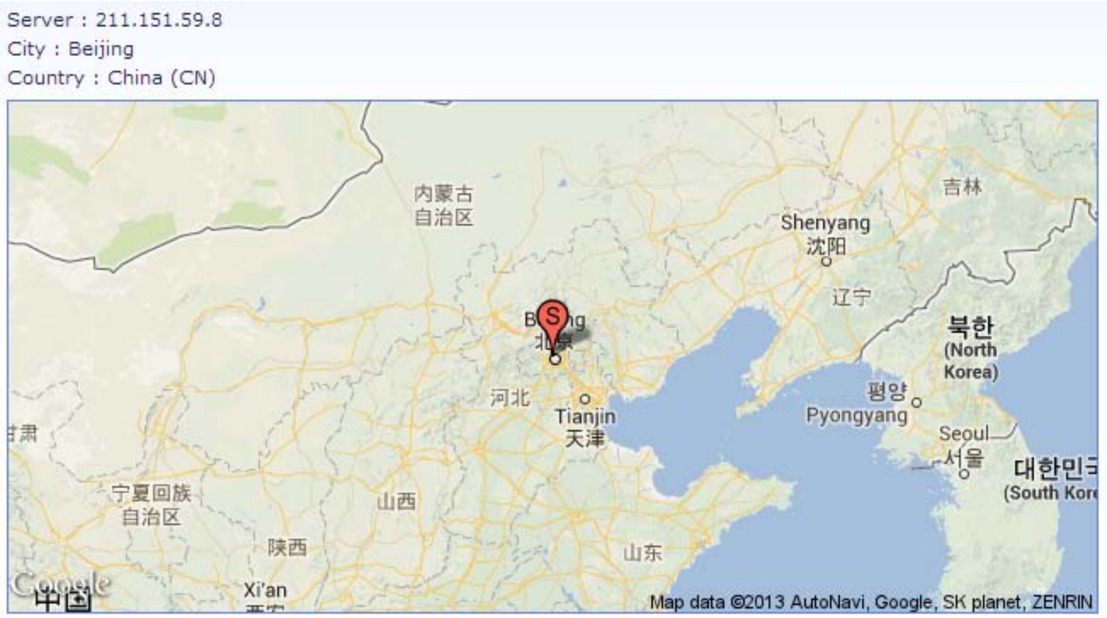

Capturing from Microsoft [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply

Filter: tcp.stream eq 1 or dns

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 192.168.137.185 | 192.168.137.1 | DNS | 72 | Standard query A us.nqsrv.com |
| 2 | 0.037460 | 192.168.137.1 | 192.168.137.185 | DNS | 88 | Standard query response A 211.151.59.8 |
| 3 | 0.043787 | 192.168.137.185 | 211.151.59.8 | TCP | 74 | 34933 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=1557 |
| 4 | 0.423360 | 211.151.59.8 | 192.168.137.185 | TCP | 74 | http > 34933 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1380 SACK_PERM=1 |
| 5 | 0.498006 | 192.168.137.185 | 211.151.59.8 | TCP | 66 | 34933 > http [ACK] Seq=1 Ack=1 Win=14656 Len=0 TSval=155866 TSecr=332670 |
| 6 | 0.499493 | 192.168.137.185 | 211.151.59.8 | HTTP | 867 | POST /BOSS_US/UPSServlet HTTP/1.1 (application/octet-stream) |
| 7 | 0.824506 | 192.168.137.185 | 192.168.137.1 | DNS | 79 | Standard query A clients3.google.com |
| 8 | 0.850587 | 192.168.137.1 | 192.168.137.185 | DNS | 495 | Standard query response CNAME clients.l.google.com A 194.90.196.37 A 194 |
| 10 | 0.884204 | 211.151.59.8 | 192.168.137.185 | TCP | 66 | http > 34933 [ACK] Seq=1 Ack=802 Win=7680 Len=0 TSval=332707001 TSecr=1 |
| 18 | 16.785034 | 211.151.59.8 | 192.168.137.185 | HTTP | 795 | HTTP/1.1 200 OK |
| 19 | 16.788173 | 211.151.59.8 | 192.168.137.185 | TCP | 66 | http > 34933 [FIN, ACK] Seq=730 Ack=802 Win=7680 Len=0 TSval=332672290 |



```
Domain Name:     nqsrv.com
Registrar:       Name.com LLC

Expiration Date: 2014-01-09 05:11:41
Creation Date:   2012-01-09 05:11:41

Name Servers:
        ns1.nqsrv.com
        ns2.nqsrv.com

REGISTRANT CONTACT INFO
NetQin Mobile Inc.
zhang guobao
No.4 Building, Heping Li East Street 11
Dongcheng District, Beijing, China
beijing
beijing
100013
CN
Phone:         +86.1085655555
Fax:           +86.1085655518
Email Address: zhangguobao@netqin.com

ADMINISTRATIVE CONTACT INFO
NetQin Mobile Inc.
zhang guobao
No.4 Building, Heping Li East Street 11
Dongcheng District, Beijing, China
beijing
beijing
100013
CN
Phone:         +86.1085655555
Fax:           +86.1085655518
Email Address: zhangguobao@netqin.com
```

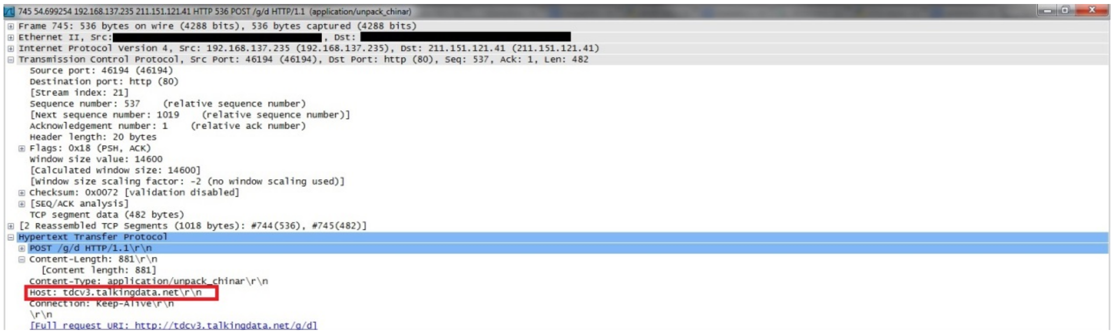


Server : 211.151.59.8
City : Beijing
Country : China (CN)

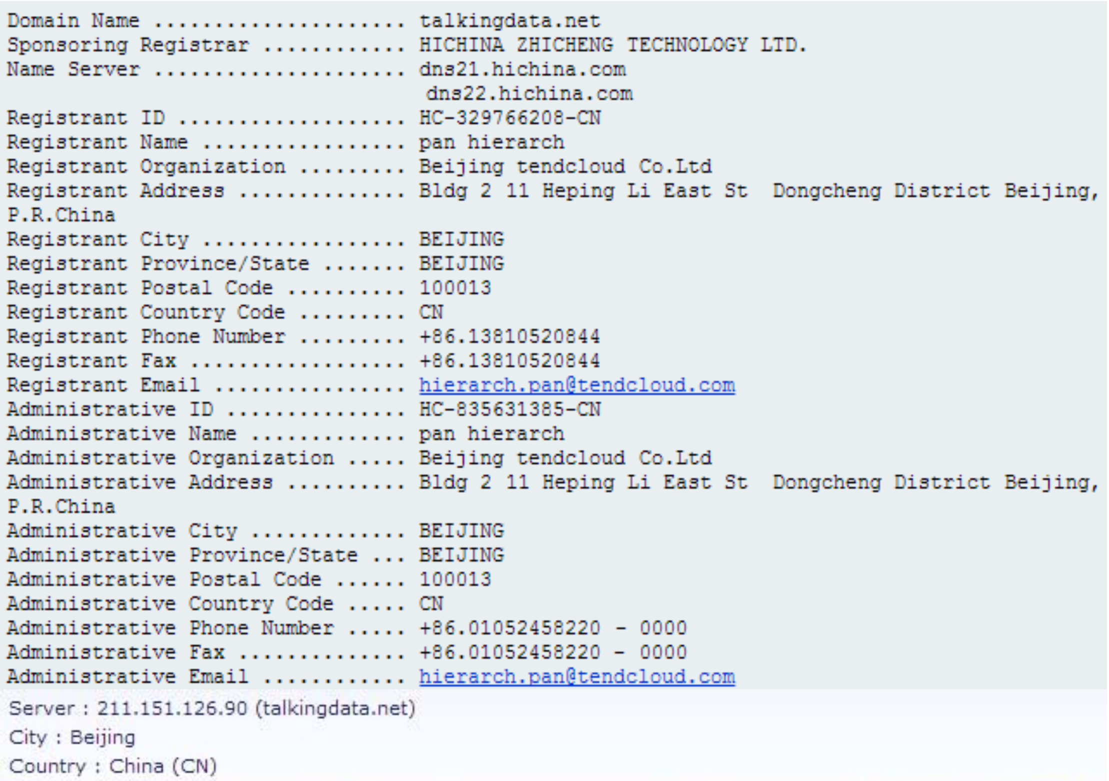
We have also encountered requests to servers, which were not owned by NQ, but rather a 3rd party company named TalkingData, especially to:

http://tdcv3.talkingdata.net - 211.151.121.41

TalkingData is a company providing mobile data collection and statistical analysis platform, located in China.



```
745 54.699254 192.168.137.235 211.151.121.41 HTTP 536 POST /g/d HTTP/1.1  (application/unpack_chinar)
⊞ Frame 745: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits)
⊞ Ethernet II, Src: [redacted], Dst: [redacted]
⊞ Internet Protocol Version 4, Src: 192.168.137.235 (192.168.137.235), Dst: 211.151.121.41 (211.151.121.41)
⊟ Transmission Control Protocol, Src Port: 46194 (46194), Dst Port: http (80), Seq: 537, Ack: 1, Len: 482
    Source port: 46194 (46194)
    Destination port: http (80)
    [Stream index: 21]
    Sequence number: 537    (relative sequence number)
    [Next sequence number: 1019    (relative sequence number)]
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x18 (PSH, ACK)
    Window size value: 14600
    [Calculated window size: 14600]
    [Window size scaling factor: -2 (no window scaling used)]
  ⊞ Checksum: 0x0072 [validation disabled]
  ⊞ [SEQ/ACK analysis]
    TCP segment data (482 bytes)
⊞ [2 Reassembled TCP Segments (1018 bytes): #744(536), #745(482)]
⊟ Hypertext Transfer Protocol
  ⊞ POST /g/d HTTP/1.1\r\n
  ⊟ Content-Length: 881\r\n
      [Content length: 881]
    Content-Type: application/unpack_chinar\r\n
    Host: tdcv3.talkingdata.net\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://tdcv3.talkingdata.net/g/d]
```



```
Domain Name ..................... talkingdata.net
Sponsoring Registrar ............ HICHINA ZHICHENG TECHNOLOGY LTD.
Name Server ..................... dns21.hichina.com
                                   dns22.hichina.com
Registrant ID ................... HC-329766208-CN
Registrant Name ................. pan hierarch
Registrant Organization ......... Beijing tendcloud Co.Ltd
Registrant Address .............. Bldg 2 11 Heping Li East St  Dongcheng District Beijing,
P.R.China
Registrant City ................. BEIJING
Registrant Province/State ....... BEIJING
Registrant Postal Code .......... 100013
Registrant Country Code ......... CN
Registrant Phone Number ......... +86.13810520844
Registrant Fax .................. +86.13810520844
Registrant Email ................ hierarch.pan@tendcloud.com
Administrative ID ............... HC-835631385-CN
Administrative Name ............. pan hierarch
Administrative Organization ..... Beijing tendcloud Co.Ltd
Administrative Address .......... Bldg 2 11 Heping Li East St  Dongcheng District Beijing,
P.R.China
Administrative City ............. BEIJING
Administrative Province/State ... BEIJING
Administrative Postal Code ...... 100013
Administrative Country Code ..... CN
Administrative Phone Number ..... +86.01052458220 - 0000
Administrative Fax .............. +86.01052458220 - 0000
Administrative Email ............ hierarch.pan@tendcloud.com
```

Server : 211.151.126.90 (talkingdata.net)

City : Beijing

Country : China (CN)

内蒙古
自治区
吉林
Shenyang
沈阳
辽宁
Beijing
北京
S
북한
(North
Korea)
河北
Tianjin
天津
평양
Pyongyang
Seoul
서울
대한민국
(South Korea)
甘肃
宁夏回族
自治区
山西
陕西
山东
Xi'an
Google
中国
Map data ©2013 AutoNavi, Google, SK planet, ZENRIN

**Captured Data Communications**

In the limited amount of time we were able to detect the following communications:

| Destination \ Trigger | Request | Response |
|---|---|---|
| Upon app loading, and periodically while using the App - TalkingData – 3$^{ed}$ party | Http unencrypted communication – Data encoded with GZip | Http unencrypted communication – Data encoded with GZip |
| System Update (update of the App) - NetQin | Http unencrypted communication – Data in plain text | Http unencrypted communication – Data in plain text |
| Virus DB Update – NetQin | Http unencrypted communication – Data encrypted with AES, and containing the XOR'ed AES key. | Http unencrypted communication – Data encrypted with AES, and containing the XOR'ed AES key. |
| Maliciose URL Protection, upon browsing to a website – NetQin | Http unencrypted communication – Data (URL address) XOR'ed | Http unencrypted communication – Data in plain text |

**TalkingData.net – 3rd party Chinese service provider**

Communication with Talking-Data's Servers is made throughout their app.

The sent data is delivered to their servers at - tdcv3.talkingdata.net (211.151.121.41)

The Request is an HTTP POST request to '/g/d'.

All packets are sent compressed with GZIP.

The packet that we have decoded contained potentially private information such as:

- Device Model
- Carrier
- GSM Cell information
- Wi-Fi SSIDs + percentage of reception

This information packet is sent periodically, and upon app loading.

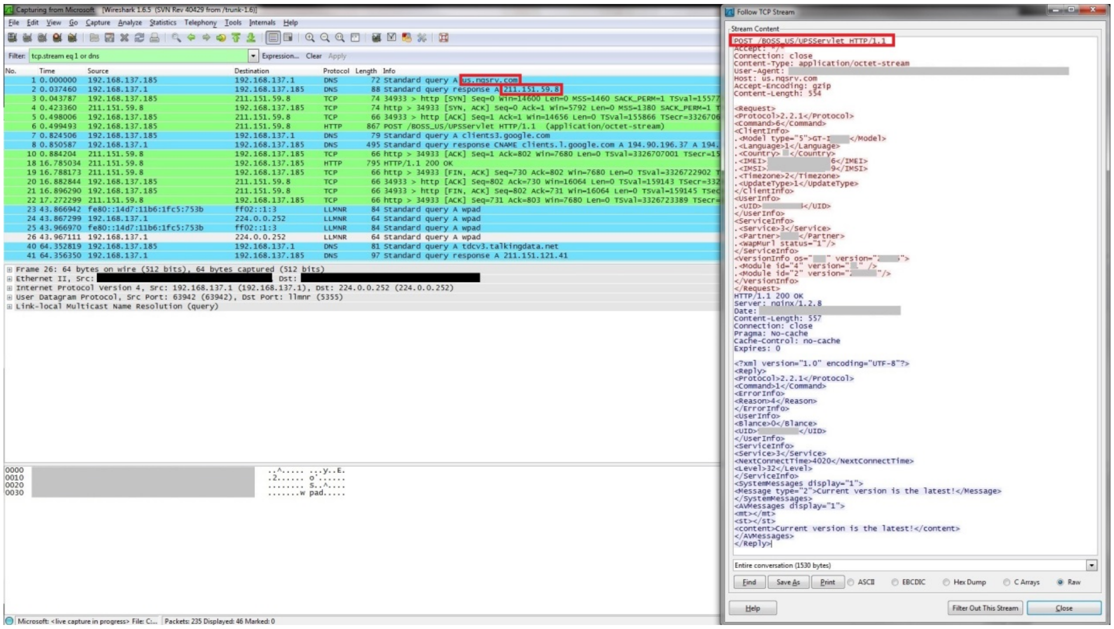
Such information shouldn't be shared with NQ or any other 3rd party.

The leaked information could lead to targeted attacks and reveal sensitive details about the user\device such as current location using Wi-Fi signals triangulation, device model\version for targeting specific exploitation methods etc.

**Software Update**

On the main screen of the application, there is a menu button on the top right corner. Clicking the "More" button of that menu, opened a new screen with a 'Check for updates' button. Clicking this button, the app sends a plain-text request which contains among other things the IMSI and IMEI inside a readable XML format.

This communication is delivered to NQ's servers - us.nqserv.com (211.151.59.8)



Capturing from Microsoft [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]

Filter: tcp.stream eq 1 or dns

```
No.  Time       Source                    Destination      Protocol Length Info
  1 0.000000   192.168.137.185           192.168.137.1    DNS       72 Standard query A us.nqsrv.com
  2 0.037460   192.168.137.1             192.168.137.185  DNS       88 Standard query response A 211.151.59.8
  3 0.043787   192.168.137.185           211.151.59.8     TCP       74 34933 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=15577
  4 0.423360   211.151.59.8              192.168.137.185  TCP       74 http > 34933 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1380 SACK_PERM=1 T
  5 0.498006   192.168.137.185           211.151.59.8     TCP       66 34933 > http [ACK] Seq=1 Ack=1 Win=14656 Len=0 TSval=155866 TSecr=3326706
  6 0.499493   192.168.137.185           211.151.59.8     HTTP     867 POST /BOSS_US/UPSServlet HTTP/1.1  (application/octet-stream)
  7 0.824506   192.168.137.185           192.168.137.1    DNS       79 Standard query A clients3.google.com
  8 0.850587   192.168.137.1             192.168.137.185  DNS      495 Standard query response CNAME clients.l.google.com A 194.90.196.37 A 194.
 10 0.884204   211.151.59.8              192.168.137.185  TCP       66 http > 34933 [ACK] Seq=1 Ack=802 Win=7680 Len=0 TSval=3326707001 TSecr=15
 18 16.785034  211.151.59.8              192.168.137.185  HTTP     795 HTTP/1.1 200 OK
 19 16.788173  211.151.59.8              192.168.137.185  TCP       66 http > 34933 [FIN, ACK] Seq=730 Ack=802 Win=7680 Len=0 TSval=3326722902 T
 20 16.882844  192.168.137.185           211.151.59.8     TCP       66 34933 > http [ACK] Seq=802 Ack=730 Win=16064 Len=0 TSval=159143 TSecr=332
 21 16.896290  192.168.137.185           211.151.59.8     TCP       66 34933 > http [FIN, ACK] Seq=802 Ack=731 Win=16064 Len=0 TSval=159145 TSec
 22 17.272299  211.151.59.8              192.168.137.185  TCP       66 http > 34933 [ACK] Seq=731 Ack=803 Win=7680 Len=0 TSval=3326723389 TSecr=
 23 43.866942  fe80::14d7:11b6:1fc5:753b ff02::1:3        LLMNR     84 Standard query A wpad
 24 43.867299  192.168.137.1             224.0.0.252      LLMNR     64 Standard query A wpad
 25 43.966970  fe80::14d7:11b6:1fc5:753b ff02::1:3        LLMNR     84 Standard query A wpad
 26 43.967111  192.168.137.1             224.0.0.252      LLMNR     64 Standard query A wpad
 40 64.352819  192.168.137.185           192.168.137.1    DNS       81 Standard query A tdcv3.talkingdata.net
 41 64.356350  192.168.137.1             192.168.137.185  DNS       97 Standard query response A 211.151.121.41

⊞ Frame 26: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
⊞ Ethernet II, Src: [redacted] Dst: [redacted]
⊞ Internet Protocol Version 4, Src: 192.168.137.1 (192.168.137.1), Dst: 224.0.0.252 (224.0.0.252)
⊞ User Datagram Protocol, Src Port: 63942 (63942), Dst Port: llmnr (5355)
⊞ Link-local Multicast Name Resolution (query)

0000  [redacted]  ..^..... ...y..E.
0010              .2...... o'......
0020              ........ S..^....
0030              .......w pad.....
```

Microsoft: <live capture in progress> File: C:... Packets: 235 Displayed: 46 Marked: 0

Follow TCP Stream

Stream Content

```
POST /BOSS_US/UPSServlet HTTP/1.1
Accept: */*
Connection: close
Content-Type: application/octet-stream
User-Agent: [redacted]
Host: us.nqsrv.com
Accept-Encoding: gzip
Content-Length: 554

<Request>
<Protocol>2.2.1</Protocol>
<Command>6</Command>
<ClientInfo>
.<Model type="5">GT-I[redacted]</Model>
.<Language>1</Language>
.<Country>[redacted]</Country>
.<IMEI>[redacted]6</IMEI>
.<IMSI>[redacted]9</IMSI>
.<Timezone>2</Timezone>
.<UpdateType>1</UpdateType>
</ClientInfo>
<UserInfo>
.<UID>[redacted]</UID>
</UserInfo>
<ServiceInfo>
.<Service>3</Service>
.<Partner>[redacted]</Partner>
.<WapMurl status="1"/>
</ServiceInfo>
<VersionInfo os="[redacted]" version="[redacted]">
.<Module id="4" version="[redacted]" />
.<Module id="2" version="[redacted]"/>
</VersionInfo>
</Request>
HTTP/1.1 200 OK
Server: nginx/1.2.8
Date: [redacted]
Content-Length: 557
Connection: close
Pragma: No-cache
Cache-Control: no-cache
Expires: 0

<?xml version="1.0" encoding="UTF-8"?>
<Reply>
<Protocol>2.2.1</Protocol>
<Command>1</Command>
<ErrorInfo>
<Reason>4</Reason>
</ErrorInfo>
<UserInfo>
<Blance>0</Blance>
<UID>[redacted]</UID>
</UserInfo>
<ServiceInfo>
<Service>3</Service>
<NextConnectTime>4020</NextConnectTime>
<Level>32</Level>
</ServiceInfo>
<SystemMessages display="1">
<Message type="2">Current version is the latest!</Message>
</SystemMessages>
<AVMessages display="1">
<mt></mt>
<st></st>
<content>Current version is the latest!</content>
</AVMessages>
</Reply>
```

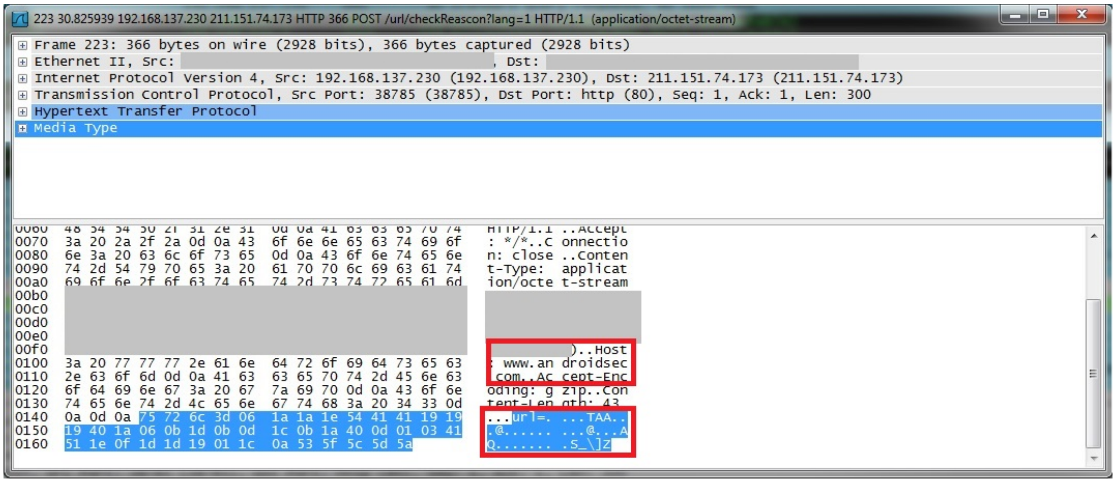
Entire conversation (1530 bytes) ○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply
Find
Save As
Print
Help
Filter Out This Stream
Close

## App leaks all the web browsing activities of the user:

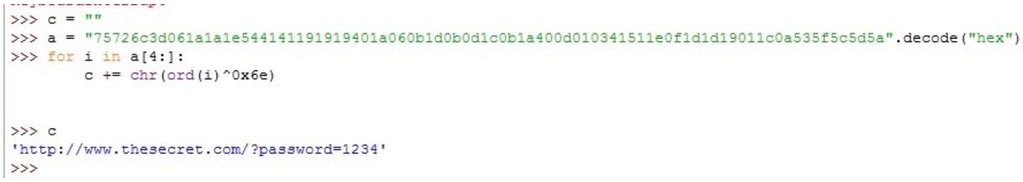
It was discovered that the app sends every URL that is browsed in the device to a remote server located in China (211.151.74.173). The connection through which the data is sent is not encrypted, but rather obfuscated with an easily reversible method of XOR the URL with 0x6e. It means that the provider, and anyone that is "sniffing" the network has the ability to track the users and obtain all browsing habits of the user, and even in some cases get information that is much more critical such as usernames and password and session ids if they are transferred in the URL.

We have tested the effectiveness of the URL tester and it indeed detects malicious pages, and blocks it.



223 30.825939 192.168.137.230 211.151.74.173 HTTP 366 POST /url/checkReascon?lang=1 HTTP/1.1 (application/octet-stream)

```
⊞ Frame 223: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits)
⊞ Ethernet II, Src: [redacted], Dst: [redacted]
⊞ Internet Protocol Version 4, Src: 192.168.137.230 (192.168.137.230), Dst: 211.151.74.173 (211.151.74.173)
⊞ Transmission Control Protocol, Src Port: 38785 (38785), Dst Port: http (80), Seq: 1, Ack: 1, Len: 300
⊞ Hypertext Transfer Protocol
⊞ Media Type

0060  48 54 54 50 2f 31 2e 31  0d 0a 41 63 63 65 70 74   HTTP/1.1 ..Accept
0070  3a 20 2a 2f 2a 0d 0a 43  6f 6e 6e 65 63 74 69 6f   : */*..C onnectio
0080  6e 3a 20 63 6c 6f 73 65  0d 0a 43 6f 6e 74 65 6e   n: close ..Conten
0090  74 2d 54 79 70 65 3a 20  61 70 70 6c 69 63 61 74   t-Type:  applicat
00a0  69 6f 6e 2f 6f 63 74 65  74 2d 73 74 72 65 61 6d   ion/octe t-stream
00b0  [redacted]                                         [redacted]
00c0
00d0
00e0
00f0                                                     [redacted])..Host
0100  3a 20 77 77 77 2e 61 6e  64 72 6f 69 64 73 65 63   : www.an droidsec
0110  2e 63 6f 6d 0d 0a 41 63  63 65 70 74 2d 45 6e 63   .com..Ac cept-Enc
0120  6f 64 69 6e 67 3a 20 67  7a 69 70 0d 0a 43 6f 6e   oding: g zip..Con
0130  74 65 6e 74 2d 4c 65 6e  67 74 68 3a 20 34 33 0d   tent-Len gth: 43.
0140  0a 0d 0a 75 72 6c 3d 06  1a 1a 1e 54 41 41 19 19   ...url=. ...TAA..
0150  19 40 1a 06 0b 1d 0b 0d  1c 0b 1a 40 0d 01 03 41   .@...... ...@...A
0160  51 1e 0f 1d 1d 19 01 1c  0a 53 5f 5c 5d 5a         Q....... .S_\]Z
```



```
>>> c = ""
>>> a = "75726c3d061a1a1e544141191919401a060b1d0b0d1c0b1a400d010341511e0f1d1d19011c0a535f5c5d5a".decode("hex")
>>> for i in a[4:]:
        c += chr(ord(i)^0x6e)


>>> c
'http://www.thesecret.com/?password=1234'
>>>
```

<u>**Update virus database**</u>

The most visible part of the app is the ‘Update virus database’ button, this button is in charge of asking the user for a payment. When clicked it makes the application communicate with a server owned by NQ at ms-cm.nqsecurity.com (211.151.59.57) and sends encrypted data.

The request is an HTTP POST request to ‘boss-cs-av-v4/app.htm.’

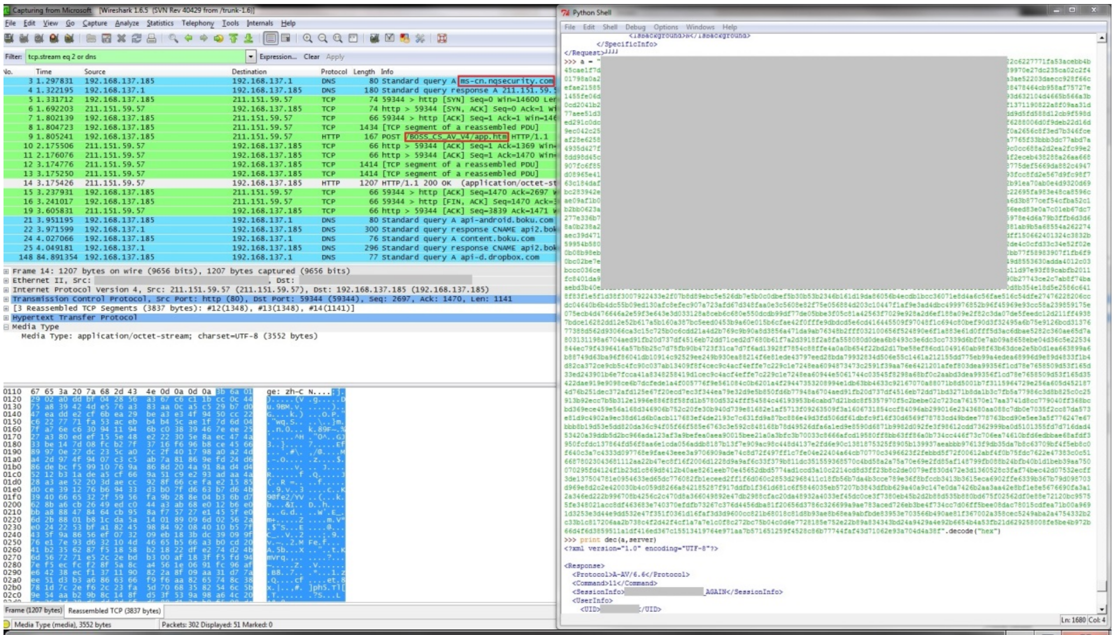
The data sent from the App to server:

- 10bytes ‘newversion’ XORed with 0x6e.
- 16bytes of encryption key XORed with 0x6e.
- Data encrypted with AES using the key just before it.

The data sent from the server to App:

- 16bytes of encryption key XORed with 0x6e.
- AES data following.

The content of the encrypted data is in XML format. It contains commands that look similar to the previously described XML in the plain-text communications. The command is an integer value that indicates the indicator "type" of command rather than a "exec-command".



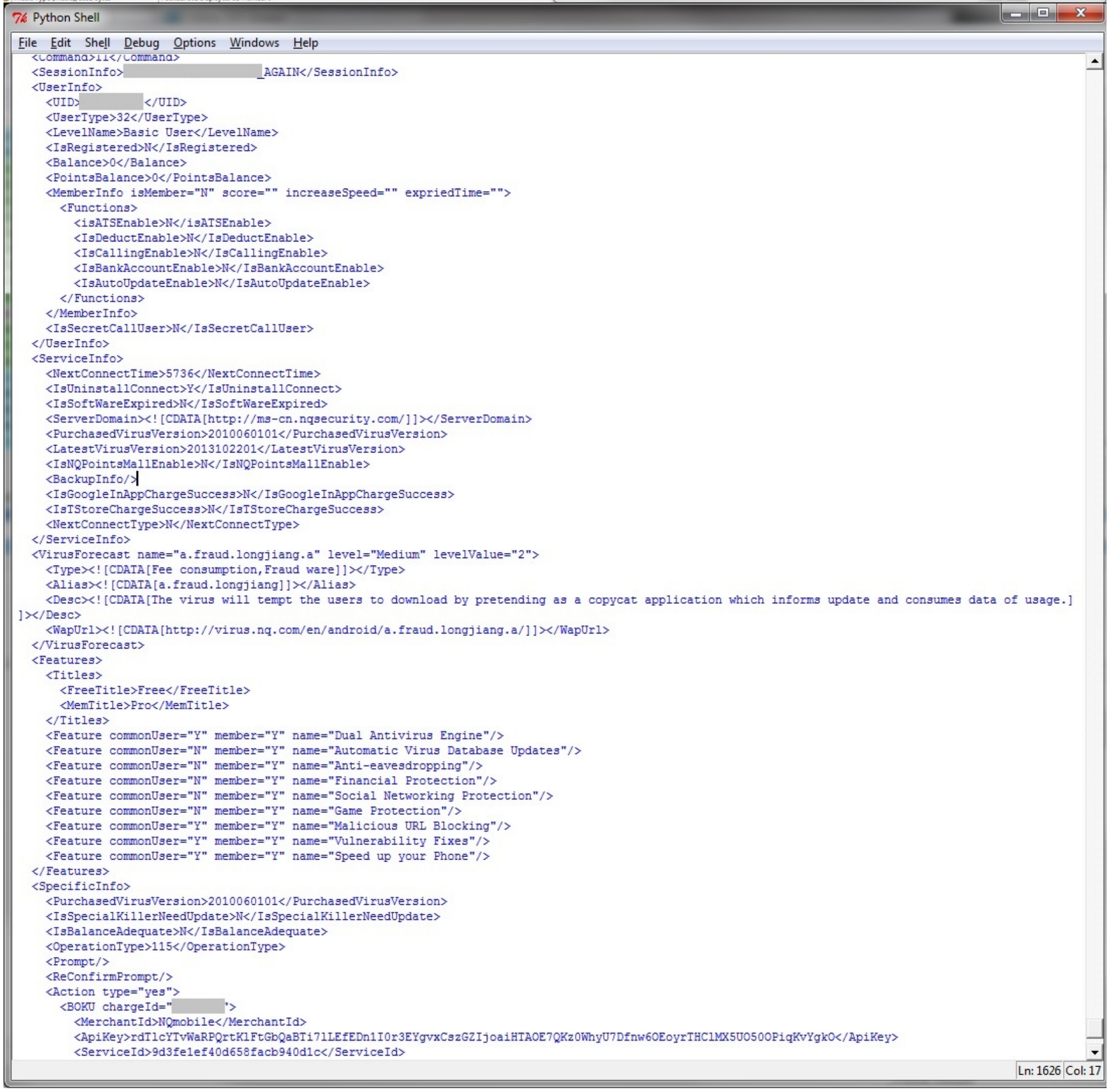
Capturing from Microsoft [Wireshark 1.6.5 (SVN Rev 40429 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.stream eq 2 or dns
Expression... Clear Apply

```
No.   Time       Source            Destination      Protocol Length Info
    3 1.297831   192.168.137.185   192.168.137.1    DNS       80 Standard query A ms-cn.nqsecurity.com
    4 1.322195   192.168.137.1     192.168.137.185  DNS      180 Standard query response A 211.151.59.
    5 1.331712   192.168.137.185   211.151.59.57    TCP       74 59344 > http [SYN] Seq=0 Win=14600 Len
    6 1.692203   211.151.59.57     192.168.137.185  TCP       74 http > 59344 [SYN, ACK] Seq=0 Ack=1 Wi
    7 1.802139   192.168.137.185   211.151.59.57    TCP       66 59344 > http [ACK] Seq=1 Ack=1 Win=146
    8 1.804723   192.168.137.185   211.151.59.57    TCP     1434 [TCP segment of a reassembled PDU]
    9 1.805241   192.168.137.185   211.151.59.57    HTTP     167 POST /BOSS_CS_AV_V4/app.htm HTTP/1.1
   10 2.175506   211.151.59.57     192.168.137.185  TCP       66 http > 59344 [ACK] Seq=1 Ack=1369 Win=
   11 2.176076   211.151.59.57     192.168.137.185  TCP       66 http > 59344 [ACK] Seq=1 Ack=1470 Win=
   12 3.174776   211.151.59.57     192.168.137.185  TCP     1414 [TCP segment of a reassembled PDU]
   13 3.175250   211.151.59.57     192.168.137.185  TCP     1414 [TCP segment of a reassembled PDU]
   14 3.175426   211.151.59.57     192.168.137.185  HTTP    1207 HTTP/1.1 200 OK  (application/octet-st
   15 3.237931   192.168.137.185   211.151.59.57    TCP       66 59344 > http [ACK] Seq=1470 Ack=2697 W
   16 3.241017   192.168.137.185   211.151.59.57    TCP       66 59344 > http [FIN, ACK] Seq=1470 Ack=3
   19 3.605831   211.151.59.57     192.168.137.185  TCP       66 http > 59344 [ACK] Seq=3839 Ack=1471 W
   21 3.951195   192.168.137.185   192.168.137.1    DNS       80 Standard query A api-android.boku.com
   22 3.971599   192.168.137.1     192.168.137.185  DNS      300 Standard query response CNAME api2.bok
   24 4.027066   192.168.137.185   192.168.137.1    DNS       76 Standard query A content.boku.com
   25 4.049181   192.168.137.1     192.168.137.185  DNS      296 Standard query response CNAME api2.bok
  148 84.891354  192.168.137.185   192.168.137.1    DNS       77 Standard query A api-d.dropbox.com

⊞ Frame 14: 1207 bytes on wire (9656 bits), 1207 bytes captured (9656 bits)
⊞ Ethernet II, Src: [redacted], Dst: [redacted]
⊞ Internet Protocol Version 4, Src: 211.151.59.57 (211.151.59.57), Dst: 192.168.137.185 (192.168.137.185)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 59344 (59344), Seq: 2697, Ack: 1470, Len: 1141
⊞ [3 Reassembled TCP Segments (3837 bytes): #12(1348), #13(1348), #14(1141)]
⊞ Hypertext Transfer Protocol
⊟ Media Type
    Media Type: application/octet-stream; charset=UTF-8 (3552 bytes)
```

```
0110  67 65 3a 20 7a 68 2d 43  4e 0d 0a 0d 0a 3b 6a 01   ge: zh-C N....;j.
0120  29 02 a0 dd bf 04 28 56  a3 67 c6 c1 1b cc 0c 44   ).....(V .g.....D
0130  75 a8 39 42 4d e5 76 a3  83 aa 0c a5 c5 29 b7 d0   u.9BM.v. .....)..
0140  47 ea dd e2 cf 6b ea 29  be a3 e3 4f 94 50 cc 22   G....k.) ...O.P."
0150  c6 22 77 71 fa 53 ac eb  b4 b4 5c ae 1f 7d 6d 04   ."wq.S.. ..\..}m.
0160  7f a7 6e c6 30 94 11 94  6b c0 38 39 46 7e ee 25   ..n.0... k.89F~.%
0170  27 a3 80 ed ef 15 5e 48  e2 22 30 5e 8a ec 47 4a   '.....^H ."0^..GJ
0180  33 be 14 7d 08 fc b2 7f  37 16 f6 96 b8 ce 45 66   3..}.... 7.....Ef
0190  89 97 0e 27 dc 23 5c a0  2c 2f 40 17 98 a0 a2 4d   ...'.#\. ,/@....M
01a0  a4 2d 97 4f 94 07 c3 c5  ab 7a 81 86 9e fd 24 d6   .-.O.... .z....$.
01b0  86 de bc f5 99 10 76 9a  86 8d 20 4a 91 8a d4 d4   ......v. .. J....
01c0  52 12 b3 1a de a5 cf 66  9a 51 c9 e2 93 ad aa 4a   R......f .Q.....J
01d0  28 a3 ae 52 20 3d ae cc  92 8f 66 ce fa e2 15 85   (..R =.. ..f.....
01e0  d0 ce 39 12 76 b6 94 33  d3 b0 7f d6 63 b7 d6 4b   ..9.v..3 ....c..K
01f0  39 40 66 65 32 2f 59 56  fa 9b 28 8e 04 b3 6b d7   9@fe2/YV ..(...k.
0200  62 8b a6 cb 26 49 ed c0  44 a3 ab 68 e0 12 b6 e0   b...&I.. D..h....
0210  bb a8 88 47 84 64 cb 95  8a f7 57 27 e1 45 5f e0   ...G.d.. ..W'.E_.
0220  6d 2b 88 01 b8 1c da 5a  14 01 89 09 6d 02 56 2a   m+.....Z ....m.V*
0230  e0 24 22 53 bf a1 82 45  98 84 92 08 40 10 b5 7f   .$"S...E ....@...
0240  43 5f 9a 86 56 ef 07 32  09 eb 18 3b dc 39 09 9f   C_..V..2 ...;.9..
0250  76 e1 7e 93 d6 32 10 4d  46 65 b5 66 a3 b0 cd 20   v.~..2.M Fe.f...
0260  41 b2 35 62 87 f5 18 58  b2 18 22 df e2 74 d2 4b   A.5b...X .."..t.K
0270  6d 56 72 71 e5 2c 2e bd  b3 00 af 18 3f f5 fd 94   mVrq.,.. ....?...
0280  7e f5 ec fc f2 8f 5a 8c  a4 56 1e 06 91 fc 96 af   ~.....Z. .V......
0290  e6 42 38 ec f1 37 11 90  82 2a 8f 09 aa 31 d7 7a   .B8..7.. .*...1.z
02a0  ee 51 d3 b3 a6 86 63 66  f9 f6 aa 82 65 74 8c 38   .Q....cf ....et.8
02b0  78 1d 7c 2e f6 2c 23 fa  5d 70 68 35 82 54 6c 5b   x.|..,#. ]ph5.Tl[
02c0  9e 54 aa b2 9b 8c 14 8f  d5 3f 53 9a 98 a6 4c 20   .T...... .?S...L
```

Frame (1207 bytes)
Reassembled TCP (3837 bytes)
Media Type (media), 3552 bytes
Packets: 302 Displayed: 51 Marked: 0
Python Shell
File Edit Shell Debug Options Windows Help
Ln: 1680 Col: 4

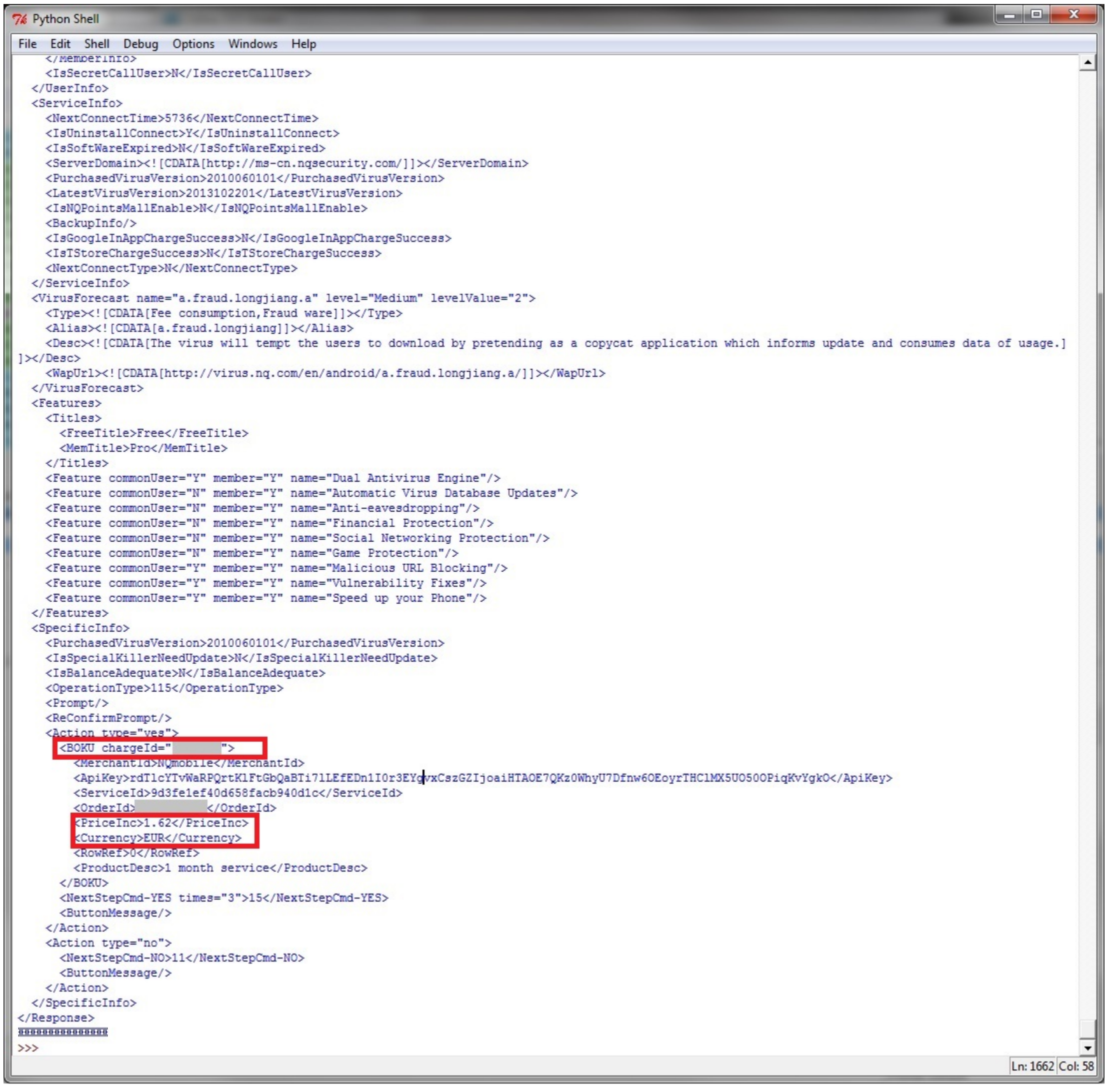
```
                <IsBackground>N</IsBackground>
        </SpecificInfo>
</Request>JJJJ
>>> a = "[redacted]22c6227771fa53acebb4b
45cae1f7d[redacted]89970e27dc235ca02c2f4
01798a0a2[redacted]a3ae52203daecc928f66c
efae21585[redacted]88478464cb958af75727e
1455fe06d[redacted]93d632104d4665b566a3b
0cd2041b2[redacted]f1371190822a8f09aa31d
77aee51d3[redacted]dd9d5fd588d12cb9f598d
ed291c0dc[redacted]f6288006d0f9deb22d16d
9ec042c25[redacted]f0a2656c8f3ed7b346fce
af28e6258[redacted]a7765f33bbb3dc77abd7a
4935d427f[redacted]9c0cc688a2d2ea2fc99e2
8dd98d45c[redacted]1f2eceb438288a26aa668
907fc6f85[redacted]3775def5669da882c4947
d08965e41[redacted]93fcc8fd2e567d9fc98f7
63c184daf[redacted]2b91ea70ab0e4d9320d69
bc283942e[redacted]c22695fa983e48ca8596c
ae09af1b0[redacted]a6d3b877cef54cfba52c1
b2bb0623a[redacted]56eed83e0a7c01eb67dc7
277e336b7[redacted]5978e4d6a79b3ffb6d3d6
8a0b238a2[redacted]881ab9b5a68554a262274
aec39d471[redacted]dff150662401324c3832b
59954b580[redacted]2de4c0cfd33c34e52f02e
0b08b98eb[redacted]0bb77f58983907f1fb6f9
0bc02be7e[redacted]19d8553630adda4012c03
bccc036ce[redacted]b11d97e93f89cabfb2011
fc8401da9[redacted]90b27743ce2c7ab8f74ba
aebd3b40e[redacted]0d8b354e18d5e2586c641
8f83f1e5f1d38f3007922433e2f07b8d89ebc5e526db7e5b0c0dbef5b30b53b2346b161d19da86056b4ecdb1bcc36071e8d4a6c56fae516c54dfe2747622820 6cc
dc04640b6b4dc55b09ed130afc8efec907a723afd67d348faa0e3c5608e82f75e056884d203c10447f1af9e3ad4dbc499976852b96f45969e93cc58a239859175e
075ecb4d476646a2e59f3e643e3d033128a8ceb6c680e550dcdb99df77de05bbe3f05c81a42563f7029e928a2d6ef188a09e2f82c3da07de5feedc12d211ff4938
7bdce16282dd12e52b617a5b160a387bc5eed0453b9a60e015b6cfae42f0fffe9dbdcd5e6cd416445509f97048f1c694c80bef90d3f32495a6b75e9126bcd31376
77388d562d93066ca3c15c725b0c6cdd21a4d2b769c9b90a8d3856a471da9ab76348b2fff032100656f524890e6f1a883e61d0fff5d3ac6dbae5282c360ae65d7a
803131198a6704aed91fb20d737df4516eb72dd71ced2d7680b61f7a2d3918f2a8fa558080d0dea6b8493c3e6dc3cc7339d6bf0e7ab09a8658ebe04d36c5e22534
844ec79f4396416a57b5b25c7d75fb90b4723f31ca7d7f6ad13928f7854c88ffe4a0a0b654f22bd2d17be58ef86cd1049160ab98f63b63dce2e5b0d1ea663899a6
b88749d63ba96f86041db10914c92529ee249b930ea88214f6e81ede43797eed28bda79932834d506e55c1461a212155dd775eb99a4edea68996d9e89d4833f1b4
d82ca372ce9cb5c4fc90c037ab13409f8f4cec9c4acf4effe7c229c1e7248ea6094873473c2591f39aa76e6421201afef803dea99356f1cd78e7658509d53f165d
33ed243901b6e7fcca41a8348258419d1cec9c4acf4effe7c229c1e7248ea60944e5061744c03545f8298a68bf0c2aabd3dea99356f1cd78e7658509d53f165d35
422dae919e9098ce6b7dcfede1a4f005776f9e561084c0b6201a4f29447353208994e1db63bb4633c92167070a88071b8d5001b7f3115964729e256a605d452187
4d76b251dec372afd125e67f20ecd7ec3f344ea79e32d9e5b850fd6b77948a6704aed91fb20d737df4516eb72dd71bd3271b8da1b3c7fb5a77986c3d8b825c0c25
913b92ecc7b5b312e1996e886f8f58fd1b5780d5324fff54584c46193953b6cabd7d21bdc8f5357970f5c2bebe02c723ca761570e17aa3741d8cc779040ff368bc
bd369ece459e56a168d346906b752c20fe30b940d739e81682e1af5713f09263509f3a1606731854ccf84096ab299016e2343680aa088c7db0e7035f2cc87da573
e81d9c4902a9ec38d61d6b0acb117683ef4de2193c7c631fd9a87bc886e49d3fd506df61dbfc9f16f30d6569f78783cd49bdee778763bcd90e5ee3a5f776247e67
bbb8b19d53e5dd820da36c94f05f66f585e6763c3e592c848168b78d49526dfa6a1ed9e8590d6871b9982d092fe3f98612cdd7362999ba0d5101355fd7d716dad4
53420a39ddb5d2bc966ada123af3a9befea0aea90015bee21a0a3bfc3b70033c8666afcd19580ff8bb63ff86a0b734cc446f73c706ea74610bfd6edbbae68afdf3
950fcfdc137864fd56f8aa6e1cda056addb8187b13f7e909ac98c448d4137e2fd6e90c1381875325f8905b139937aeabbb97613f9db35da7b8c63709bf4f5eb8c0
f640c3a7c4333d097768e9fae43eee3a9706909ade74c8d72f497ff1c7fe04e22404a64cb70770c3496623f2febbd5f72f00612abf4f0b75fdc7622e47383c0c51
6687802304368l112aa22b47ec8f16f2006d1228d9a9af6c33f379b811dc351559368570c4bd58a2a75a70e69e2fd85af148799fb088b24bfb40b1d1beb39aa750
070295fd4124f1b23d1c869d8412b40ae8261eeb70e45652dbd5774ad1ccd3a10c2214cd8d3ff23b8c2de0079ef830d472e3d1360528c3faf74bec42d07532ecff
3de137504781e0954633ed65dc776082fb1eceed2ff1f6d060c2853d2968411c18fb56b7da4b3cce789e36f8bfccb3413b3615eca6902ffe6339b367b79d098703
d969e8d2c2e420030b4c059d8266a842185287f917ddfb1f361d681c6f5846035eb57207b3843dfbb629a40a9c147e0da7426b2aa3aa42e8bf1e8e5676690fa3a1
2a346ed222b996708b4256c2c470d8a366049892e47db2988cfac20da48932a4033ef45dc0ce3f7380eb45b2d2b88d535b880bd675f02562df0e88e72120bc9575
5fe348021acc8df463683e740370efdfb73267c376d4456dba81f20656d3786c326699a9ae783aced726eb3be4f734cc7d06ff5bee08dac78015cdfea71b00a969
1d3253e3d44e9dd532e47f351f0361d16faf3d3d9600cc821b68018c81d8b93ae8b68ea9abfbde83953e703566b490ae81f367002a358cec5249aba2a4754332b2
c33b1c817206aa2b738c4f2d42f4cf1a7a7e1c0f8c272bc75b04c0d6e7728185e752e22b89a834343bd24a9429a4e92b6654b4a53fb21d629258008fe5be4b972b
66d4f6d385951la1df416ed367c15513419764e971aa7b571651259f4528c86b77744faf43d71062e93a704d4a38f".decode("hex")
>>> print dec(a,server)
<?xml version="1.0" encoding="UTF-8"?>

<Response>
  <Protocol>A-AV/6.6</Protocol>
  <Command>11</Command>
  <SessionInfo>[redacted]_AGAIN</SessionInfo>
  <UserInfo>
    <UID>[redacted]</UID>
```



```
  <Command>11</Command>
  <SessionInfo>[redacted]_AGAIN</SessionInfo>
  <UserInfo>
    <UID>[redacted]</UID>
    <UserType>32</UserType>
    <LevelName>Basic User</LevelName>
    <IsRegistered>N</IsRegistered>
    <Balance>0</Balance>
    <PointsBalance>0</PointsBalance>
    <MemberInfo isMember="N" score="" increaseSpeed="" expriedTime="">
      <Functions>
        <isATSEnable>N</isATSEnable>
        <IsDeductEnable>N</IsDeductEnable>
        <IsCallingEnable>N</IsCallingEnable>
        <IsBankAccountEnable>N</IsBankAccountEnable>
        <IsAutoUpdateEnable>N</IsAutoUpdateEnable>
      </Functions>
    </MemberInfo>
    <IsSecretCallUser>N</IsSecretCallUser>
  </UserInfo>
  <ServiceInfo>
    <NextConnectTime>5736</NextConnectTime>
    <IsUninstallConnect>Y</IsUninstallConnect>
    <IsSoftWareExpired>N</IsSoftWareExpired>
    <ServerDomain><![CDATA[http://ms-cn.nqsecurity.com/]]></ServerDomain>
    <PurchasedVirusVersion>2010060101</PurchasedVirusVersion>
    <LatestVirusVersion>2013102201</LatestVirusVersion>
    <IsNQPointsMallEnable>N</IsNQPointsMallEnable>
    <BackupInfo/>
    <IsGoogleInAppChargeSuccess>N</IsGoogleInAppChargeSuccess>
    <IsTStoreChargeSuccess>N</IsTStoreChargeSuccess>
    <NextConnectType>N</NextConnectType>
  </ServiceInfo>
  <VirusForecast name="a.fraud.longjiang.a" level="Medium" levelValue="2">
    <Type><![CDATA[Fee consumption,Fraud ware]]></Type>
    <Alias><![CDATA[a.fraud.longjiang]]></Alias>
    <Desc><![CDATA[The virus will tempt the users to download by pretending as a copycat application which informs update and consumes data of usage.
]]></Desc>
    <WapUrl><![CDATA[http://virus.nq.com/en/android/a.fraud.longjiang.a/]]></WapUrl>
  </VirusForecast>
  <Features>
    <Titles>
      <FreeTitle>Free</FreeTitle>
      <MemTitle>Pro</MemTitle>
    </Titles>
    <Feature commonUser="Y" member="Y" name="Dual Antivirus Engine"/>
    <Feature commonUser="N" member="Y" name="Automatic Virus Database Updates"/>
    <Feature commonUser="N" member="Y" name="Anti-eavesdropping"/>
    <Feature commonUser="N" member="Y" name="Financial Protection"/>
    <Feature commonUser="N" member="Y" name="Social Networking Protection"/>
    <Feature commonUser="N" member="Y" name="Game Protection"/>
    <Feature commonUser="Y" member="Y" name="Malicious URL Blocking"/>
    <Feature commonUser="Y" member="Y" name="Vulnerability Fixes"/>
    <Feature commonUser="Y" member="Y" name="Speed up your Phone"/>
  </Features>
  <SpecificInfo>
    <PurchasedVirusVersion>2010060101</PurchasedVirusVersion>
    <IsSpecialKillerNeedUpdate>N</IsSpecialKillerNeedUpdate>
    <IsBalanceAdequate>N</IsBalanceAdequate>
    <OperationType>115</OperationType>
    <Prompt/>
    <ReConfirmPrompt/>
    <Action type="yes">
      <BOKU chargeId="[redacted]">
        <MerchantId>NQmobile</MerchantId>
        <ApiKey>rdTlcYTvWaRPQrtKlFtGbQaBTi7lLEfEDn1I0r3EYgvxCszGZIjoaiHTAOE7QKz0WhyU7Dfnw60EoyrTHC1MX5UO50OPiqKvYgkO</ApiKey>
        <ServiceId>9d3fe1ef40d658facb940d1c</ServiceId>
```

In response to this request, the server returns a response indicating the applications payment state. It indicates whether the user paid already for enabling some features.

It also specifies with which payment provider it should request payment from, and the amount of money. We saw Boku and Google wallet as providers.



```
    </MemberInfo>
    <IsSecretCallUser>N</IsSecretCallUser>
  </UserInfo>
  <ServiceInfo>
    <NextConnectTime>5736</NextConnectTime>
    <IsUninstallConnect>Y</IsUninstallConnect>
    <IsSoftWareExpired>N</IsSoftWareExpired>
    <ServerDomain><![CDATA[http://ms-cn.nqsecurity.com/]]></ServerDomain>
    <PurchasedVirusVersion>2010060101</PurchasedVirusVersion>
    <LatestVirusVersion>2013102201</LatestVirusVersion>
    <IsNQPointsMallEnable>N</IsNQPointsMallEnable>
    <BackupInfo/>
    <IsGoogleInAppChargeSuccess>N</IsGoogleInAppChargeSuccess>
    <IsTStoreChargeSuccess>N</IsTStoreChargeSuccess>
    <NextConnectType>N</NextConnectType>
  </ServiceInfo>
  <VirusForecast name="a.fraud.longjiang.a" level="Medium" levelValue="2">
    <Type><![CDATA[Fee consumption,Fraud ware]]></Type>
    <Alias><![CDATA[a.fraud.longjiang]]></Alias>
    <Desc><![CDATA[The virus will tempt the users to download by pretending as a copycat application which informs update and consumes data of usage.]
]></Desc>
    <WapUrl><![CDATA[http://virus.nq.com/en/android/a.fraud.longjiang.a/]]></WapUrl>
  </VirusForecast>
  <Features>
    <Titles>
      <FreeTitle>Free</FreeTitle>
      <MemTitle>Pro</MemTitle>
    </Titles>
    <Feature commonUser="Y" member="Y" name="Dual Antivirus Engine"/>
    <Feature commonUser="N" member="Y" name="Automatic Virus Database Updates"/>
    <Feature commonUser="N" member="Y" name="Anti-eavesdropping"/>
    <Feature commonUser="N" member="Y" name="Financial Protection"/>
    <Feature commonUser="N" member="Y" name="Social Networking Protection"/>
    <Feature commonUser="N" member="Y" name="Game Protection"/>
    <Feature commonUser="Y" member="Y" name="Malicious URL Blocking"/>
    <Feature commonUser="Y" member="Y" name="Vulnerability Fixes"/>
    <Feature commonUser="Y" member="Y" name="Speed up your Phone"/>
  </Features>
  <SpecificInfo>
    <PurchasedVirusVersion>2010060101</PurchasedVirusVersion>
    <IsSpecialKillerNeedUpdate>N</IsSpecialKillerNeedUpdate>
    <IsBalanceAdequate>N</IsBalanceAdequate>
    <OperationType>115</OperationType>
    <Prompt/>
    <ReConfirmPrompt/>
    <Action type="yes">
      <BOKU chargeId="[redacted]">
        <MerchantId>NQmobile</MerchantId>
        <ApiKey>rdTlcYTvWaRPQrtKlFtGbQaBTi7lLEfEDn1I0r3EYgvxCszGZIjoaiHTAOE7QKz0WhyU7Dfnw6OEoyrTHClMX5UO50OPiqKvYgkO</ApiKey>
        <ServiceId>9d3fe1ef40d658facb940d1c</ServiceId>
        <OrderId>[redacted]</OrderId>
        <PriceInc>1.62</PriceInc>
        <Currency>EUR</Currency>
        <RowRef>0</RowRef>
        <ProductDesc>1 month service</ProductDesc>
      </BOKU>
      <NextStepCmd-YES times="3">15</NextStepCmd-YES>
      <ButtonMessage/>
    </Action>
    <Action type="no">
      <NextStepCmd-NO>11</NextStepCmd-NO>
      <ButtonMessage/>
    </Action>
  </SpecificInfo>
</Response>
################
>>>
```

## Remote Code Execution

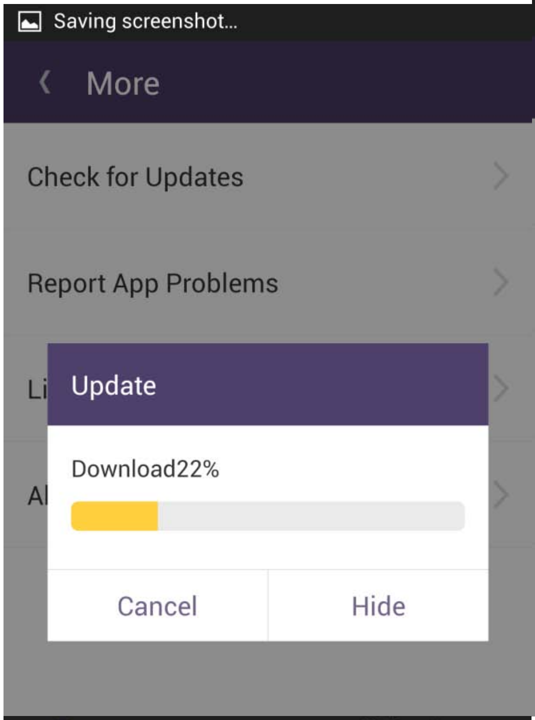
Goal: Determine if app allows remote code execution.

Process:  Research the software update, request update from the server, and get a response.
In this response, we saw there’s a command value. We looked in the code and saw that there’s another special command that is being processed which directs the application to download a file from the server or any address!

At that point of the research we set up an experiment where we did man-in-the-middle attack on the device, technically we edited the hosts file so the NQ server so that they will point to our HTTP server instead of NQ’s one. The idea is to show that we got code execution on the device and so does NQ.

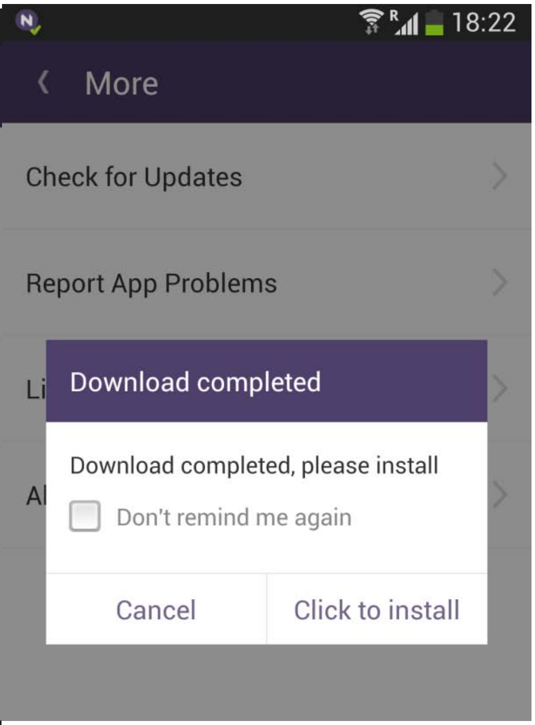
On our HTTP server we set up a response according to what we saw that the application expects. The response contains a different command value, which indicates to the client that it should download a file, and the URL of the file to download. Basically the file the protocol describes is supposed to be an .APK file. This file is later chmod’ed to become r+x so it could be executed later.

The application was properly installed but requires approval by user intervention.



Update

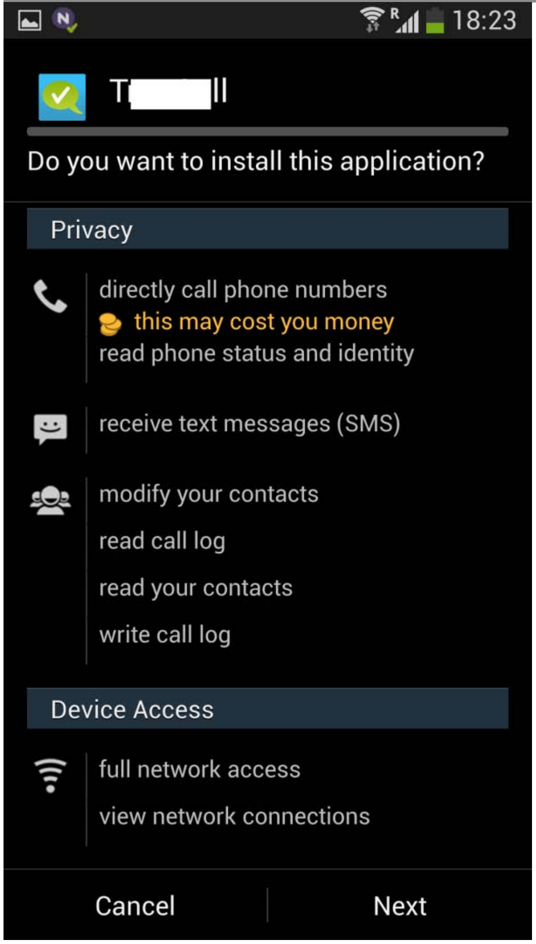
Download22%



Download completed

Download completed, please install

□ Don't remind me again



T[redacted]ll

Do you want to install this application?

Privacy

directly call phone numbers
this may cost you money
read phone status and identity

receive text messages (SMS)

modify your contacts
read call log
read your contacts
write call log

Device Access

full network access
view network connections

Later on, we decided to go further and see whether we could override existing files and bypass the user intervention to get rid of the message box. We found out that if we change the returned XML without the message related fields, then no message box is displayed for the user.

This technically leads to remote code execution on the device. We have to emphasis that this is not a vulnerability in the code, in contrary, this is part of a normal flow control of the code and can be easily exploited to push files to the device which are controlled by the server and could be malicious!

The fact that the app is not using standard encryption is very odd especially when dealing with a company that is providing security products. Using standard SSL encryption could have prevented (or at least make it fairly impractical) this risk and others.