APT1：揭秘一支中国网络间谍部队

----------MANDIANT

H3C测试中心安全小组 原文翻译制作

目　录Table of Contents

APT1：揭秘一支中国网络间谍部队

关键词：APT、PLA、IOCs

缩略语清单：

Abbreviations 缩略语	Full spelling 英文全名	中文
APT	Advanced Persistent Threat	高级持续攻击
PLA	People’s Liberation Army	中国人民解放军
CPC	Communist Party of China	中国共产党
GSD	General Staff Department	总参（部队）
IOCs	Indicators of Compromise	危险指标

“中国的商业间谍活动已经达到了令人无法忍受的程度，而且我认为美国和美国在欧洲和亚洲的盟友，必须直面北京的威胁，并且要求他们停止这种强盗活动。

北京正在对我们发动大规模贸易战，我们应该联合起来迫使北京停止战争。只有联合起来，才能对中国形成贸易优势，并且利用这种优势阻止灾难的发生。”

— U.S. Rep. Mike Rogers, 2011年10月

“在没有任何确凿证据的情况下，这是一份对中国发动网络战的业余的、无理的指责。”

— 中国国防部, 2013年1月

1 摘要

从2004年开始，Mandiant公司已经调查了全球数百个组织的计算机安全事件，这些事件中的大部分都属于“高级持续入侵”（Advanced Persistent Threat，简写为APT）攻击。我们第一次公布APT的细节，是在2010年1月份的“M-Trends”报告中。正如我们在报告中描述的：“中国政府可能参与了这些活动，但是我们无法确定参与的程度”。现在，三年过去了，我们有证据修正以前的结论。我们分析了几百起调查事件的细节，使我们相信发起这些攻击的组织主要位于中国，并且中国政府默认了他们的行为。

Mandiant持续跟踪了世界上很多能够发动APT攻击的组织，这份报告聚焦于这些组织中的大多数，我们称之为“APT1”。在APT1中，有超过20个组织都位于中国。最晚从2006年开始，APT1就成了计算机间谍活动参与者的唯一组织。根据我们的观察，APT1是众多成功窃取大量信息的组织的一个。APT1参与者的规模和影响，促使我们写了这份报告。

我们已经发现了APT1实施的部分计算机间谍活动。虽然只有部分，但是我们能够推断出，在过去七年中，有超过150名的受害者遭到入侵。根据受害者的反馈，我们从网络上逆向追踪APT1，发现了位于上海的发起攻击的四个网络，其中有两个位于浦东新区。我们揭示了APT1发起攻击的基础设施以及惯用方法（工具、手段和攻击过程）。为了突出每一名攻击者，Mandiant公司展示了其中三个人的画像。这三个人，也许是三名士兵，可能仅仅是按照别人的指令行动。

通过分析，我们推断APT1很可能受到政府的资助。因此，我们也相信APT1能够在大范围内发动长期的计算机间谍活动。在确认入侵者身份的过程中，我们的研究发现，中国人民解放军61398部队和APT1在任务、能力和资源上很相近。中国人民解放军61398部队和APT1也位于同样的区域。

关键发现

APT1被认为隶属于总参三部二局，更普遍的称呼是61398部队

- 61398部队的任务属于国家机密，尽管如此，我们认为它的主要任务是“计算机网络破坏”
- 61398部队的一部分位于上海浦东新区高桥镇大同路，一座2007年前的建筑中，其中心占地130663英尺，有12层楼
- 基于61398部队的建筑规模，我们估计它可能有几百名，甚至上千名的成员
- 中国电信集团以国家安全的名义，提供了专门的光纤接入通道
- 61398部队要求它的成员都接受计算机安全和计算机网络的培训，并且精通英语
- Mandiant追踪的位于上海的，APT1发起攻击的四个网络中，有两个位于61398部队的建筑内

APT1已经从至少141个组织，系统的窃取了几百个T的数据，并且展现出了从更多的组织同时窃取数据的能力和意图

- 从2006年开始，APT1已经入侵了20多个行业的141家公司
- APT1有明确的攻击方法以窃取大量数据
- 一旦APT1成功侵入，它会每隔几个月或者几年窃取一次各类数据，包括工业蓝皮书、专业制造流程、测试结果、商业计划、价格书、合作协定、电子邮件和受害组织领导的联系人列表
- APT1会使用其它APT组织未使用过的工具和技术，比如两种窃取电子邮件的技术-GETMAIL和MAPIGET
- APT1会长年接入受害者的网络，最长的达到1764天，即4年10个月
- APT1在10个月的时间中，从某个组织窃取了6.5T的压缩数据
- 在2011年初，APT1成功的新入侵了10个行业的至少17名受害者

APT1更倾向于入侵以英语为母语的国家的组织

- 在APT1的141名受害者中，87%的公司总部位于以英语为母语的国家
- APT1攻击目标所属的行业，和中国政府第12个5年规划中7大新兴产业中的4个，是一致的

APT1在全球范围内控制着大量计算机资源

- 为了展开攻击，APT1控制了成千的计算机资源
- 在过去的两年中，APT1在13个国家，使用了849个不同的IP地址，创建了937个C2（Command and Control）服务器。在849个IP地址中，有709个位于中国，109个位于美国
- 在过去两年中（2011年1月～2013年1月），我们确认APT1的1905个成员，使用远程桌面从832个不同的IP地址，入侵了受害者的计算机
- 我们确认在过去的几年中，有2551个FQDN（Fully Qualified Domain Name，完全合格域名）属于APT1

Mandiant观测到的APT1发起的1905次入侵中，超过97%发起者使用的是在上海注册的IP地址，并且使用的是简体中文系统

- 在我们的观测到的APT1实施的1905次攻击中，有1849次（占97%）其攻击者的键盘布局设置为“中国（简体）-美式键盘”。微软的远程桌面客户端配置会自动根据客户操作系统选择语言。因此，APT1攻击者极有可能是使用配置为显示简体中文的微软操作系统。
- APT1通过远程桌面控制的系统，根据IP地址，有98%（832个IP地址中的817个）都可以逆向追踪回中国
- 我们分析了使用“HUC Packet Transmit Tool”或“HTRAN”方式的767个独立的事件，共使用了614个不同的IP地址。这614个IP：
  - 100%位于中国
  - 99.8%位于前文提到的位于上海的4个攻击网络中的1个

APT1基础设施的规模意味着至少有几十个大型组织，更可能有潜在数百个操作员。

- 我们保守估计，APT1的当前攻击的基础设施包括超过1,000台服务器。
- 基于攻击量、持续时间和我们所观察到的攻击活动类型，APT1操作者需要有如下支持：有语言学家、开源研究人员、恶意软件作者、转换请求方的任务给操作员的业界专家，以及传送被盗信息给请求方的人。
- APT1也需要一个相当大的IT团队，致力于获取和维护计算机设备，理财专员，设施管理和物流（例如，运输）。

为了强调键盘背后实际的那个人，Mandiant揭示了与APT1活动相关的三个人物角色。

- 第一个角色，“UglyGorilla”，自2004年10月一直活跃在计算机网络作战。他的活动包括注册归属于APT1的域名和创作APT1活动中使用的恶意软件。“UglyGorilla”于2004年1月公开的表达了他对中国的“网络部队”的兴趣。
- 第二个角色，我们称之为“DOTA”的一个参与者，先后注册几十个电子邮件帐户，用来进行社会工程和鱼叉式网络钓鱼攻击，支持APT1活动。“DOTA”所使用过一个上海的电话号码来注册这些帐户。
- 我们观察到无论是“UglyGorilla”还是“DOTA”，均使用相同的共享基础设施，包括我们已经确认是属于APT1的FQDN和IP地址范围。
- 第三个角色，使用了绰号“SuperHard”，他是APT1及其APT组织所使用的AURIGA和BANGAT恶意软件家族的创始者和杰出贡献者。“SuperHard”披露了他的位置是上海的浦东新区。

Mandiant提供了3000多个证据来指证APT1的活动。

- 具体而言，Mandiant提供以下内容：
  - 超过3000个APT1指示灯的数字化交付，如域名，IP地址和MD5散列的恶意软件。
  - 妥协的样本指标（IOC）和超过40个家族的APT1数字武器兵工厂恶意软件的详细描述。
  - APT1使用的13个X.509加密证书。
  - 显示实际攻击者的会话和他们的入侵活动的视频搜集。
- Mandiant的企业级产品的现有客户，Mandiant管理国防和Mandiant智能响应，可以优先使用这些APT1证据，我们也让他们可以使用红线：我们的一个免费的基于主机的调查工具。

红线可以在http://www.mandiant.com/resources/download/redline.下载。

结论

庞大的规模、基于中国的奇异特定团体，发起如此大范围行业的持续、广泛攻击，组织背后是APT1毫无疑问。我们相信全部证据。本文档提供了APT1是61398部队的证据支撑，但是，我们承认还有另一个不太可能的可能性：

除61398部队外，还有另一个秘密、实力雄厚的中国组织，可直接通往上海的电信基础设施。多年从事企业规模的计算机间谍活动，执行类似61398部队的任务。

为什么我们要揭露APT1

公布我们关于61398部队情报的重要部分是一个艰苦的决定。这是开始于：我们传统的非公开政策关于一个“假设”的讨论很快就变成了现实，揭露APT1，所产生的正面影响盖过了我们收集这个特殊组织的情报能力的风险。现在是时候承认威胁源于中国了，我们希望进行我们的武装，并准备安全专业人员有效地打击这种威胁。属性问题，一直是公众了解APT网络间谍缺失的环节。如果没有建立与中国建立稳固的连接，总是会有空间，使得观察员对APT行动不协调、事实上纯粹的犯罪、或周边较大的国家安全和全球经济的担忧。我们希望这份报告增强更多的认识，以及对APT网络违规行为采取协调一致的打击行动。

与此同时，公开发布所有的信息也有不利的一面。许多本报告中所描述的更有效的方法和技术，攻击者还不知道他们。此外，出版某类证据将大大缩短其寿命。当61398部队阅读这份报告后，改变了他们的技术，无疑将迫使我们更加努力地工作，以继续准确地跟踪他们。然而我们真诚的希望，这份报告可以暂时增加61398部队的运营成本，并阻碍他们的发展。

我们深知这份报告对我们的风险。我们预计会收到来自中国的报复，以及批评的冲击。

2 中国 61398 部队的计算机网络作战任务

我们的研究和观察表明，中国共产党给中国解放军下发任务，让其进行系统性的网络间

Emblem of the People's Liberation Army

谍和对世界各地的企业数据盗窃。本节提供如下内容：照片和61398部队设施细节，文献讨论该部队的培训和课程要求的文献，记录部队的性质与至少一个国有企业有关联的内部通信。当我们讨论APT1的专业技术、人员、地点和那些与61398部队类似组织时，这些细节将是特别有意义的。

中国共产党

中国人民解放军的网络组织是完全社会化，可以借鉴中国国有企业的资源以支持其业务。中国共产党是中国大陆最高权威；不像在西方社会中，政党都隶属于政府，军方和政府在中国都从属于中国共产党。事实上，中国人民解放军直接向中共中央军事委员会报告（CMC，中央军事委员会）。这意味着中国解放军内的任何企业的网络间谍活动是发生在党的高级指挥下的。

我们相信，解放军的战略网络司令部坐落在解放军总参谋部，特别是其第3部（总参三部）。GSD是最高级中国解放军部门，类似于美国参谋长联席会议，GSD建立学说并为解放军提供业务指导。在GSD内，总参三部有一个联合组织专注于信号情报，外语水平和国防信息系统，据估计有130,0009人员分布在12个局、三个研究机构、16个区及功能局之间。我们认为，总参三部2局，是我们正在跟踪的APT1集团。图1示出了总参三部二局与最高级别的中国共产党有多接近。在这个层面上，第二局也位于大量从属办事机构之上。

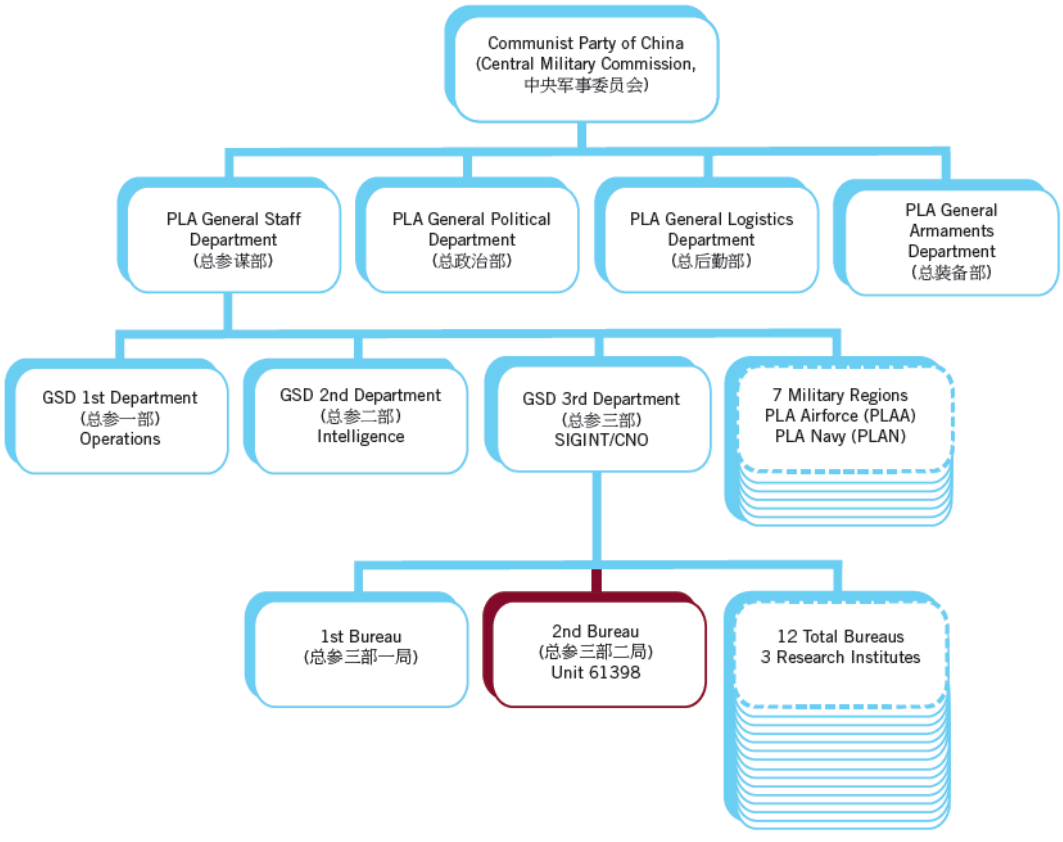


FIGURE 1: Unit 61398's position within the PLA[11]

推断61398部队的计算机网络操作任务和能力

公开的可用资料证实，人民解放军总参三部二局，部队番号为61398，通常被熟知为61398部队。资料明确指出61398部队被任命进行计算机网络运作。2049计划组织报告：在2011年，61398部队“作为总参三部的重要职能单位，聚焦于美国和加拿大的最可能在政治、经济、军事方面相关的情报工作”。我们的调查支持这一报告，且显示61398部队的计算机网络运作活动不限于美国和加拿大，似乎延伸到所有以英语为第一语言的组织。

什么是MUCD?

中国军事部队的军事部队代号（MUCD）——作为军事通信和操作时的标准编号，由五位数字序号编码，使部队在被提及时匿名。（例如，“81356部队正在向目标移动”，等同于“第十四军第三师第一百二十五团第一营正在向目标移动”）。军事部队代号还用于官方出版物和互联网上，用于谈论部队。该代号常显示在部队的营房、制服、旗帜上。

人民解放军总参三部二局即为61398部队

关于人民解放军维持总参三部二局与61398军事部队代号分离的想法，通过查询互联网或者中国政府的官方文档同时提到总参三部二局与61398部队的地方，可以得到部分的证实。图2显示出这样一些查询的结果。

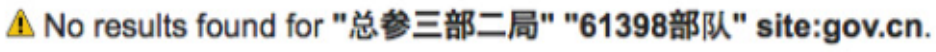


图2 未在中国任何政府网站找到“总参三部二局”和“61398部队”的搜索结果

尽管在线上找到中国政府与61398部队的联系难度很大，我们在调查中仍然找到了线上证据，证据指出总参三部二局就是61398部队。特别的，google索引到某些论坛与履历里提及61398部队，一旦中国共产党的检察官发现这些记录，他们就会修改或者从互联网移除这些记录或文档。图3显示了一些google关于61398部队的搜索结果和回应（当你读到这份报告时，搜索结果里显示的联系可能已经被移除）。

图3，google搜索结果显示出61398部队特征“泄密”

61398部队的成员要求

61398部队活跃在征求和培训英语人员——特别是各种信息技术领域的。该部队以前及现在的成员暗示了部队在这方面的着重。例如，李兵兵，一个专修信息隐藏的毕业生，公开的承认了其加入过61398部队，于2010年出版了一篇论文，讨论微软word文档的信息隐藏。另一个例子是，英语语言学家王卫忠的传记信息，发布在河北商会，描述了其在61398部队受到的英语语言培训。这些以及其他的展示61398部队的专业技能领域的例子，已列在下方的表1里。

TABLE 1: Chinese sources referring to the areas of expertise contained in Unit 61398.

Type of Expertise in Unit 61398 (部队)	Source Describing that Expertise in Unit 61398
Covert Communications	Article in Chinese academic journal. Second author Li Bingbing (李兵兵) references Unit 61398 as the source of his expertise on the topic.[15]
English Linguistics	Bio of Hebei Chamber of Commerce member Wang Weizhong (王卫忠). He describes that he received his training as an English linguist during his service in Unit 61398. (Hebei is a borough in Shanghai.)[16]
Operating System Internals	Article in Chinese academic journal. Second author Yu Yunxiang (虞云翔) references Unit 61398 as the source of his expertise on the topic.[17]
Digital Signal Processing	Article in Chinese academic journal. Second author Peng Fei (彭飞) references Unit 61398 as the source of his expertise on the topic.[18]
Network Security	Article in Chinese academic journal. Third author Chen Yiqun (陈依群) references Unit 61398 as the source of his expertise on the topic.[19]

此外，有证据显示，61398部队大量地从大学工科招聘新的人才，像哈尔滨工业大学和浙江大学计算机学院。61398部队的大部分职位描述里，寻求满足精通于计算机技术要求的人才。该组织似乎也常对是否精通英语有要求。表2展示了61398部队职位的两个例子，附各职位对大学所修课程的要求和精通程度的要求。

TABLE 2: Two profession codes and university recommended courses for students intending to apply for positions in Unit 61398

Profession Code	Required Proficiencies
080902 — Circuits and Systems	» 101 — Political » 201 — English » 301 — Mathematics » 842 — Signal and Digital Circuits (or) 840 - Circuits » Interview plus a small written test: – Circuits and Systems-based professional knowledge and comprehensive capacity – Team spirit and ability to work with others to coordinate – English proficiency
081000 — Information and Communications Engineering	» 101 - Political » 201 – British [English] » 301 - Mathematics » 844 - Signal Circuit Basis

61398部队人力设备的规模和地点

根据61398部队的基础设施的规模，我们推测，该部队雇佣了几百甚至上千人。这是基于中国有关于61398部队基地地点公开描述的推断。例如，公开的资料证实早在2007年，江苏龙海建工集团有限公司为61398部队完成的上海市浦东新区高桥镇大同路208号的大楼，被认为是61398部队中心大楼，12层高，130663平方英尺的面积，我们推断能容纳约2000人工作。图4到图7提供了建筑的鸟瞰图和街道区位图，显示了它的大小和位置。这只是该部队的数个建筑中的一个，其他的一些建筑甚至比它更大。

FIGURE 4: Datong circa 2006 (prior to Unit 61398 Center Building construction) Image Copyright 2013 DigitalGlobe

图4：大同路，2006年（61398部队中心大楼建设前）

FIGURE 5: Datong Circa 2008 (Unit 61398 Center Building visible at 208 Datong) Image Copyright 2013 DigitalGlobe

图5：大同路，2008年（61398部队中心大楼已经可见）

FIGURE 6: Unit 61398 Center Building (main gate, soldiers visible) Image Copyright 2013 city8.com

图6：61398部队中心大楼（大门，士兵可见）

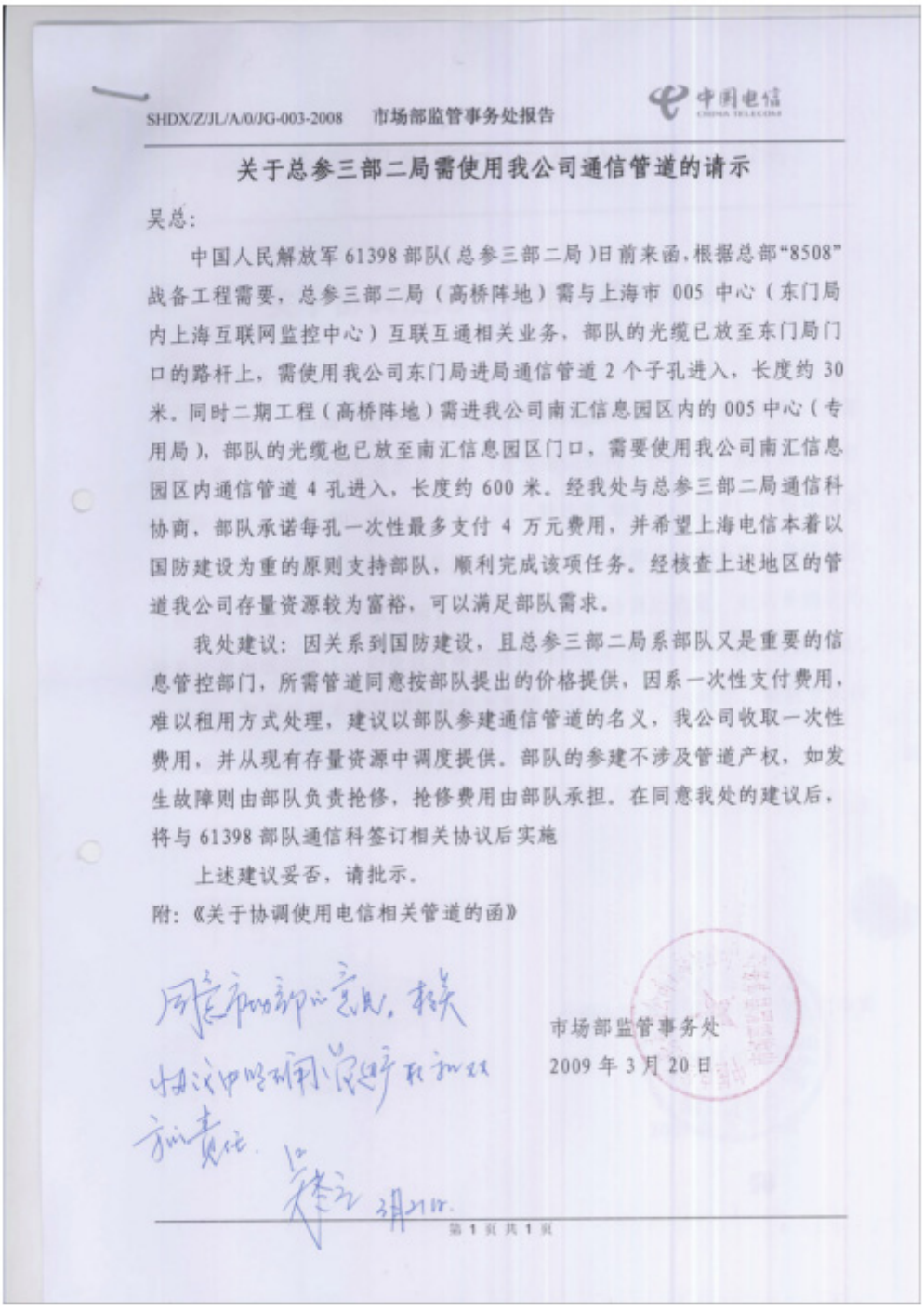
FIGURE 7: Unit 61398 Center Building 208 Datong (rear view, possible generator exhausts visible) Image Copyright 2013 city8.com

图7：大同路208号，61398部队中心大楼后视图

61398部队，同时还有一条龙的支持部队和联合的基础设施，大部分位于上海浦东新区高桥镇大同路方向，包括位于高桥镇及上海其他一些地方的后勤部队、门诊、幼儿园，以及宾馆。这些便利设施常与军事部队或高层单位相关。这些便利设施使得61398部队人民解放军高级的编制中占据重要的位置。（61398部队在人民解放军中的位置见图1。）

61398部队和国营的中国电信企业是计算机网络基础设施运营合作伙伴。

Mandiant在线找到一份中国电信内部文档，提供了关于提供给61398部队的基础设施的一些细节。该文档（图8中）揭示了中国电信决定与61398部队“共同”整理他们的光通信线路的使用清单——基于国防机构的重要原则。该信还指出这是中国电信对61398部队的特殊关照，出于中国电信的“正常租用方法”之外。此外，该文档将词语“61398部队”注释为“总参三部二局”。该文档不仅支持61398部队的身份即为总参三部二局的观点，而且揭示了“一个非常重要的通信和控制部门”（61398部队）与国营企业之间的关系。



SHDX/Z/JL/A/0/JG-003-2008　市场部监管事务处报告

中国电信 CHINA TELECOM

关于总参三部二局需使用我公司通信管道的请示

吴总：

中国人民解放军 61398 部队（总参三部二局）日前来函，根据总部“8508”战备工程需要，总参三部二局（高桥阵地）需与上海市 005 中心（东门局内上海互联网监控中心）互联互通相关业务，部队的光缆已放至东门局门口的路杆上，需使用我公司东门局进局通信管道 2 个子孔进入，长度约 30 米。同时二期工程（高桥阵地）需进我公司南汇信息园区内的 005 中心（专用局），部队的光缆也已放至南汇信息园区门口，需要使用我公司南汇信息园区内通信管道 4 孔进入，长度约 600 米。经我处与总参三部二局通信科协商，部队承诺每孔一次性最多支付 4 万元费用，并希望上海电信本着以国防建设为重的原则支持部队，顺利完成该项任务。经核查上述地区的管道我公司存量资源较为富裕，可以满足部队需求。

我处建议：因关系到国防建设，且总参三部二局系部队又是重要的信息管控部门，所需管道同意按部队提出的价格提供，因系一次性支付费用，难以租用方式处理，建议以部队参建通信管道的名义，我公司收取一次性费用，并从现有存量资源中调度提供。部队的参建不涉及管道产权，如发生故障则由部队负责抢修，抢修费用由部队承担。在同意我处的建议后，将与 61398 部队通信科签订相关协议后实施

上述建议妥否，请批示。

附：《关于协调使用电信相关管道的函》

市场部监管事务处

2009 年 3 月 20 日

第 1 页 共 1 页

FIGure 8: 中国电信为61398部队提供资源的纪要

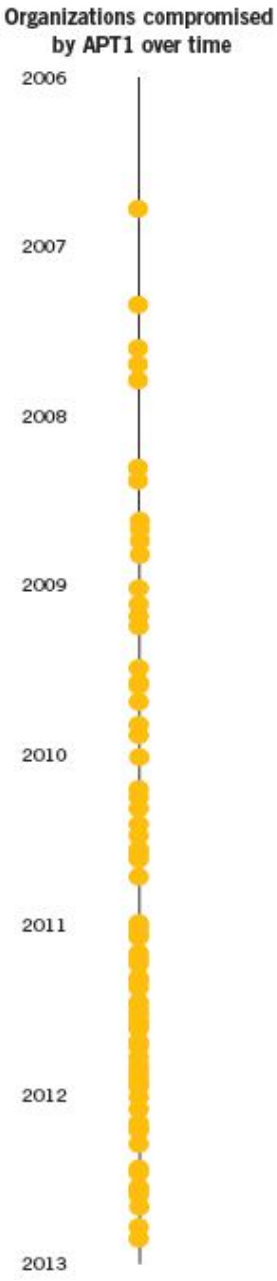
人民解放军61398部队总结

我们收集的证据显示人民解放军61398部队的任务和基础设置揭露了该组织：

- 雇佣几百，甚至可能上千的人员

- 要求人员受过计算机安全和计算机网络操作的培训
- 要求人员精通英语
- 在上海的浦东新区有大量的基础设施和便利设施
- 是国有企业中国电信以国防名义提供的光纤通信基础设施的受益者

本报告的后续章节详细介绍APT1的网络间谍和数据窃取操作。这些持续性的攻击的规模和周期无疑显示了其背后是有企业级规模的组织。我们将展示APT1的目标受害者的特点，该组织的架构，任务策略，以及人民解放军61398部队的架构。



3 APT1：多年的间谍活动

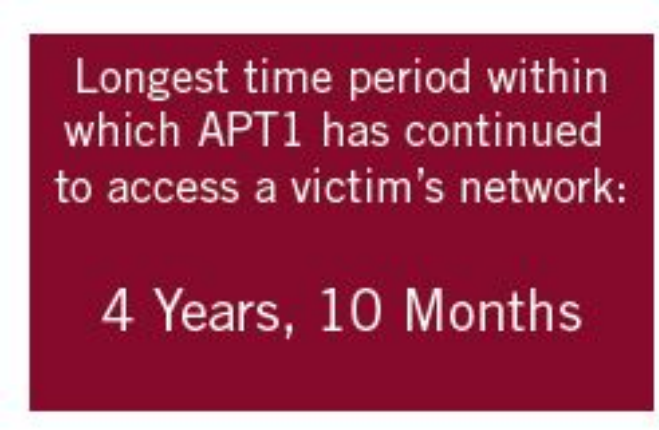
我们拥有的证据表明，APT1早在2006年开始，就从跨越了不同行业的至少141个组织中窃取了几百G字节数据。尤其是我们已经证实APT1同时将许多组织作为目标。一旦APT1能够访问受害者的网络，他们将持续在几个月或者几年里定期从受害组织的领导层，窃取大量有价值的知识产权信息，包括技术蓝皮书、制造工艺版权、测试结果、商业计划、定价文档、合作协议、电子信函和通讯录。我们相信，我们直接掌握的这些行为仅仅代表了APT1这类网络间谍活动的一小部分。

APT1致力于APT攻击的“持久性”

自2006年始我们就看到APT1疯狂扩展到新的受害者。图10显示了我们所了解的141个组织受到危险的时间轴；图表中每个标记都代表一个独立的受害者，并标明是在这个组织网络中APT1活动的最早确认时间。

由于电子证据的短暂性，许多APT1的早期活动的数据显示，我们低估了APT1在网页上表现的持久性。

图10：时间轴表示APT1在141个组织的网页上活动的早期数据，这141个组织是Mandiant观察到被APT1进行网络间谍的组织。



一旦APT1对一个网页进行网络间谍活动，他们会重复检测和窃取正确的数据，并和受害者通信数月甚至数年。对于图10中的组织，我们发现APT1持续进入受害者的网络平均为356天。APT1最长时间的持续进入一个受害者的网络至少有1764天，也就是四年零十个月。APT1在这个时间段不是进行持续入侵活动；然而，在我们观察的巨大的案例里，只要APT1进入网络就会不断地窃取数据。

APT1的地理及行业焦点

APT1主要对用英语的组织展开其网络间谍活动。然而，我们也看到一组小数量的非英语受害者。我们观察到87%的APT1受害者是把总部设立在以英语为本土语言的国家（见图11）。这包括了设立在美国的115个受害者和设立在加拿大和英国的7个受害者。剩下的19个受害者中，有17个受害者是以英语作为其主要的经营语言。这些包括国际合作发展机构，英语为多种外交语言之一的外国政府，和主要用英语进行生意往来的跨国联合大企业。只有两个受害者使用的不是英语。考虑到大多数PLA（中国人民解放军）61398部队的成员都要求精通英语，我们相信这两个非英语受害者是APT1正常执行任务活动外异常出现的个例。

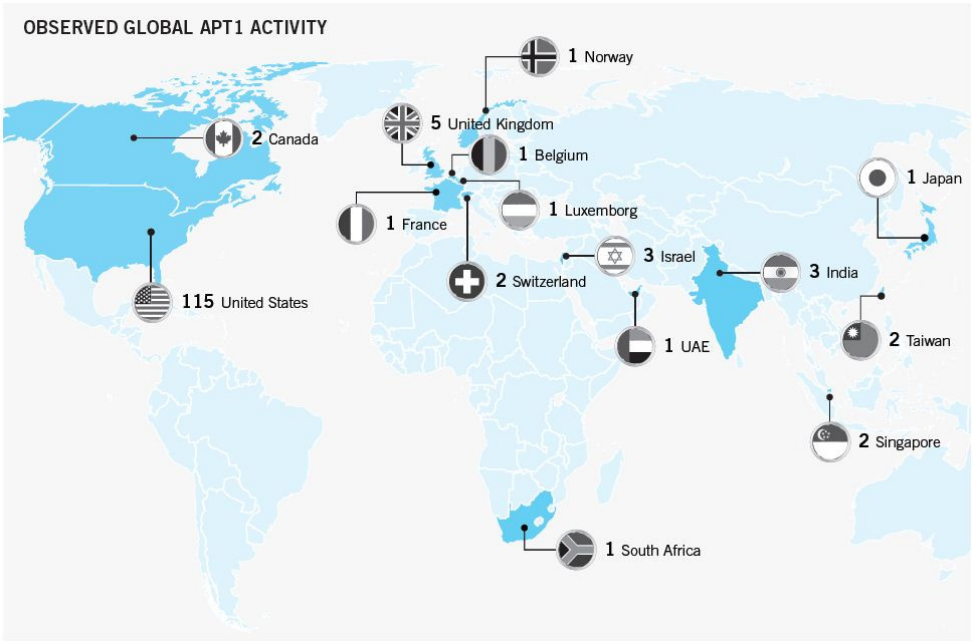


图11：APT1受害者的地理位置。在呈现的众多受害者案例中，这些位置反映了APT1进行网络间谍活动（后来发现的）不是在组织的分部，就是在组织的总部。

APT1展示了同时窃取多个组织和大范围行业的能力和意图。图12提供了一系列早期APT1针对我们确定的141个受害者进行活动的数据，这些数据是由他们呈现的20个主要行业组织形成的。这结果表明APT1的使命是非常广的；这个团体不是系统地以行业为目标，更像是在持续地从一个巨大的行业范围里窃取数据。数据中呈现出的组织仅仅是APT1受害者的一小部分，APT1的目标行业范围也许比我们调查显示的更广。

更近一步地说，APT1的类似活动范围暗示了这个团队拥有可支配的重要人员和技术资源。比如在2011年的第一个月，从图12可以看出，APT1成功地在10个不同的行业对17个新受害者进行网络间谍活动。我们看到这个团体在第一次进行网络间谍活动后，仍继续对每个受害者进行网络间谍活动，平均每个受害者持续一年，我们推断APT1在对这17个新受害者进行网络间谍活动的同时，仍继续进入之前许多受害者的网络，并从中窃取数据。

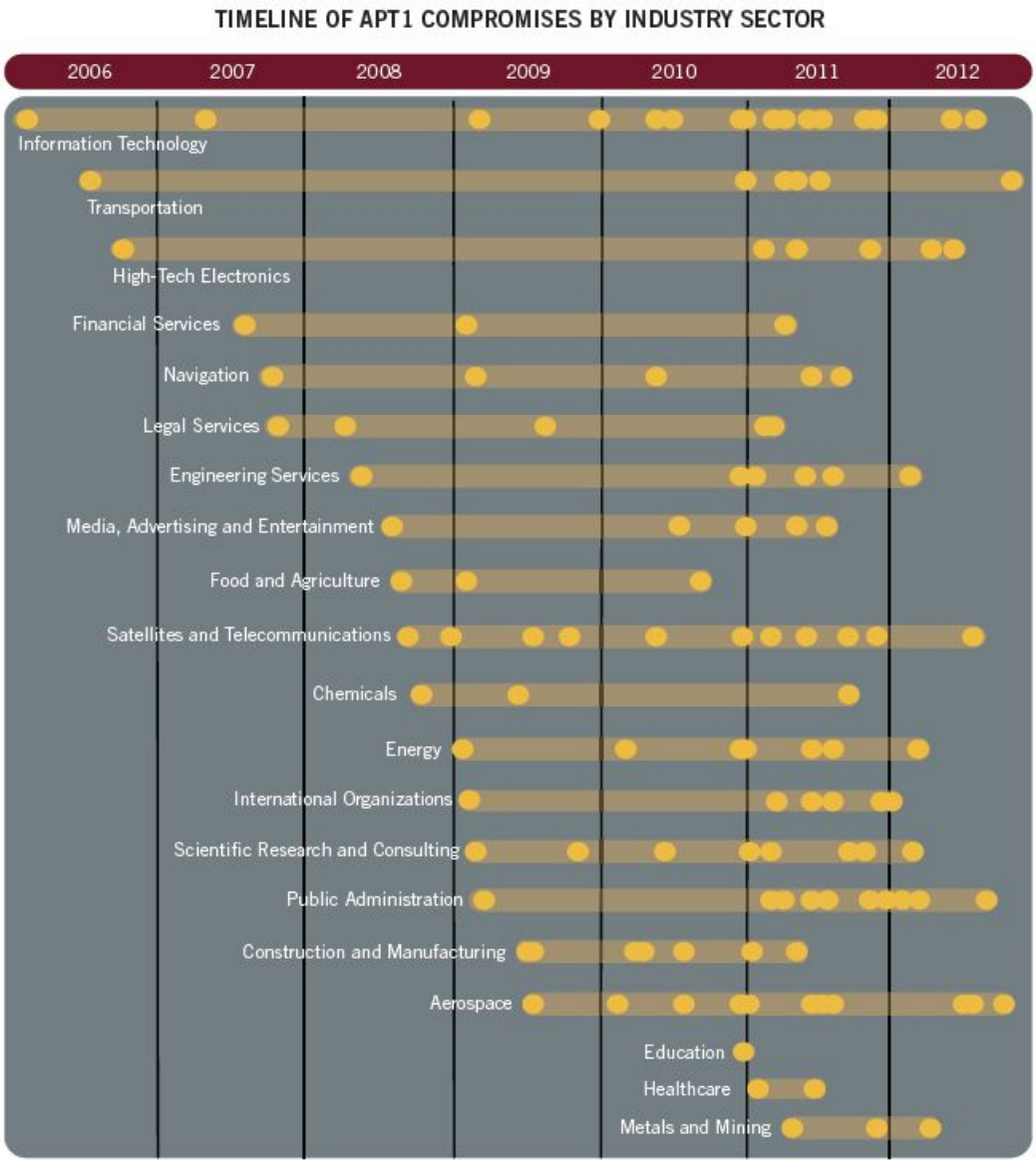


图12：APT1按照行业领域对组织进行网络间谍活动时间表。每一条里的点代表了APT1在行业领域里对一个新的组织进行网络间谍活动的早期数据。

我们相信与中国战略优先权有关系的所有行业领域的组织都是APT1综合网络间谍运动的潜在目标。我们可以明确地看出这个团体把某些行业领域当做重点目标（见图13），我们的观察报告证实了，在这出现的七个重要行业领域中至少有四个是在中国的第12个五年计划中确定的，这些都是APT1的目标。

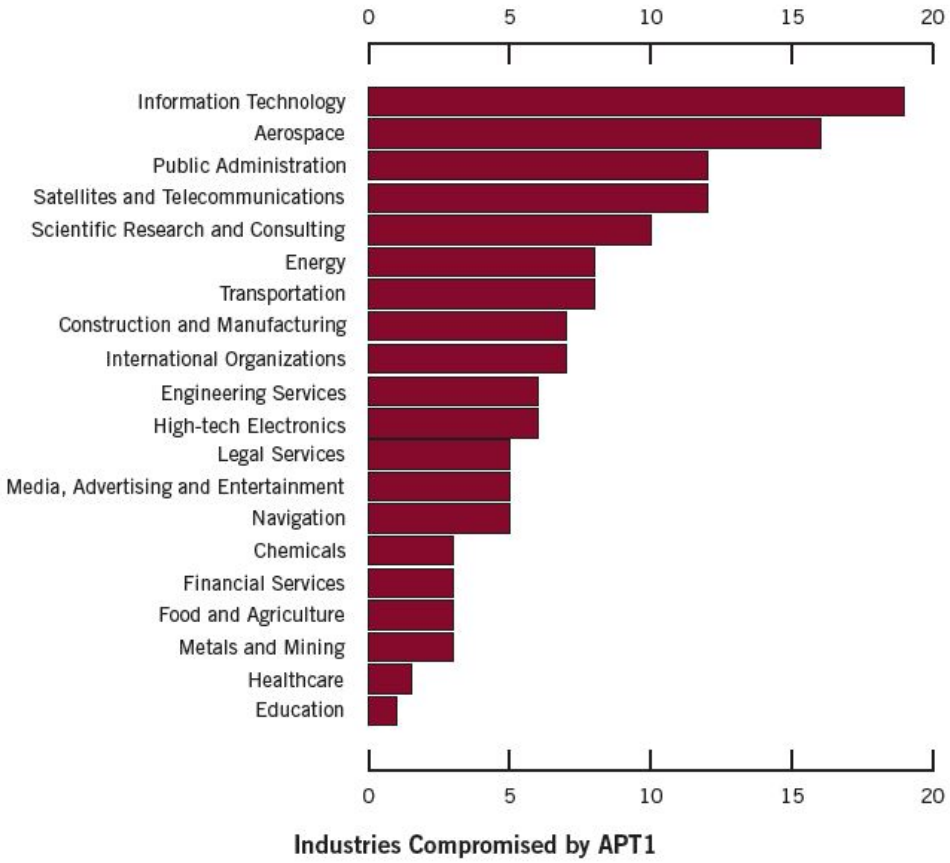


图13：按行业领域划分的APT1受害者的数字。我们决定每个组织所属的工业领域都以胡佛系统检查分类为基础划分。从信息可用性的程度来说，我们也会考虑APT1在每一个组织中所窃取的数据内容。

APT1 数据窃取

APT1 从其侵犯的组织中窃取了范围广泛的信息。这些信息种类与以下相关：

- 产品开发和使用，包括测试结果信息、系统设计、产品手册、部件清单、仿真技术；
- 制造程序，如对专有工艺、标准、垃圾管理过程的描述；
- 商业计划，如有关合同谈判立场、产品价格、法律事件、兼并、合资、收购等信息；
- 政策立场和分析，如白皮书、包括高层人员的会议议程和纪要；
- 高层雇员的邮件；
- 用户凭证和网络架构信息。

我们很难评估APT1在入侵活动中到底窃取了多少数据，原因如下：

- APT1 在窃取数据后将删除压缩档案，留下的痕迹通常被日常业务活动覆盖；
- 预先存在的网络安全监控很少记录或识别出被窃取的数据；
- 从数据遭窃到Mandiant着手调查的时间间隔太长，窃取数据的痕迹证据往往已经被日常业务活动覆盖；
- 一些被侵犯组织更愿意分配资源来恢复其网络的安全，而不是调查并理解安全泄露的影响。

尽管面对这些挑战，我们还是观察到APT1在10个月内从一个受侵犯组织中窃取了6.5TB压缩数据。根据APT1的活动范围，基于我们所看到其所侵犯组织的数量和行业领域及他们很明显能够从任何单一组织中窃取的数据数量，我们认为APT1很可能已经从其侵犯的组织中窃取了数百TB数据。

尽管我们没有直接的证据说明谁接收了APT1窃取的信息，以及接收者如何处理这样大量的数据，我们相信这些被窃取的信息能够被中国和其国有企业使用以获得发展。例如，2008 年，APT1 侵犯了一个批发业的公司。APT1 安装了工具来产生压缩文件档案并提取邮件及其附件。在后边的两年半中，APT1从这个公司窃取了未知数量的文件，并重复访问几个高层管理者的邮件账号，包括CEO 和董事会。在同一个时间段，主要新闻机构报道称，在与被侵犯企业的谈判中，针对其主要商品之一的单价，中国成功地取得了两位数的价格跌幅。这可能是巧合；然而，如果说APT1 能够持续实施这样广泛领域的网络间谍和数据窃取活动，而不能

将其活动成果交给那些能够使用这些成果的组织手中，结果将是让人吃惊的。

新闻中的APT1

公开报道证实并拓展了我们对APT1网络间谍活动的观察。然而，几个因素使得我们汇总公开报道的过程变得复杂。其一，信息安全研究者和期刊将APT1称作不同的名称。另外，很多网络安全侧重于去写多个中国APT团组分享的工具，而没有区分不同的使用者。

为了帮助研究者识别那些公开报道的入侵组织是我们所识别的APT1，表3提供了一系列经常出现在媒体上的APT组织的昵称名单，并按照是否属于APT1进行了区分。另外，下边是有关中国入侵组织的公开报道，我们确认与APT1相关。

- 最早知道的关于APT1基础设施的报道，是2006年Symantec 日本分部发布的。这个报告指出了主机名sb.hugesoft.org，这是注册给一个被称为Ugly Gorilla 的APT1成员的（本报告后边会讨论）。
- 2012 年9 月，"Krebs on Security" 网络犯罪博客的Brian Krebs报道一起施耐德电气的安全泄露事故，根据黑客用于探索并获得系统访问权所使用的工具和基础设施，我们认为是APT1 所为。

TABLE 3: Identifying APT1 Nicknames in the News

Nickname	Verdict
Comment Crew	Confirmed APT1
Comment Group	Confirmed APT1
Shady Rat	*Possibly APT1 (not confirmed)*
Nitro Attacks	Not APT1; Attributed to another tracked APT group
Elderwood	Not APT1; Attributed to another tracked APT group
Sykipot	Not APT1; Attributed to another tracked APT group
Aurora	Not APT1; Attributed to another tracked APT group
Night Dragon	Not APT1; Attributed to another tracked APT group

表 3：识别新闻中的 APT1 别名

- 名为Digital Bond 的SCADA 安全公司，在2012 年6 月发布了一个有关针对其公司进行鱼叉钓鱼攻击的报告。AlienVault 对相关恶意软件提供了分析。报告中证据被归于APT1基础设施的一部分。
- 2012 年11 月，Bloomberg's Choloe Thiteaker 就中国威胁组织“CommentGroup”写了文章，其中描述了APT1成员Ugly Gorilla 所使用的不同工具和域名。

4 APT1：攻击生命周期

APT1有一个定义良好的攻击方法，经过多年磨练、设计用于窃取大量知识产权。他们从积极的鱼叉式网络钓鱼攻击开始，进而部署定制的数字武器，向中国输出大量压缩文件，

以此作为一个循环。他们熟练运用英语——能使用可接受的俚语——在他们的社会工程邮件中。他们在七年多的时间内完善了数字武器，并在软件生命周期内持续升级是。他们适应环境和跨系统扩散的能力使得他们对于具有信任关系的企业环境非常有效。

这些攻击符合本章描述的在Mandiant攻击生命周期模型框架下的一个循环行为模式。在每一个阶段我们将讨论APT1 的具体技术来说明他们操作的顽强及规模。（参见附件B:“APT和攻击生命周期”，大多数APT 团组在攻击生命周期的每个阶段使用步骤的总括。）

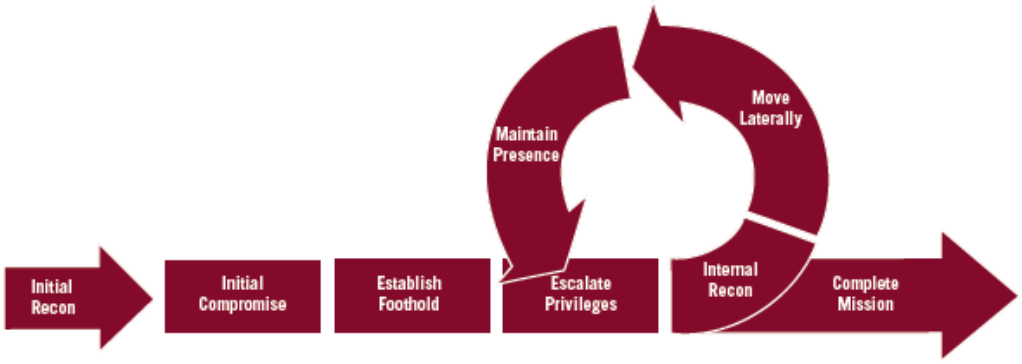


FIGURE 14: Mandiant's Attack Lifecycle Model

图14：Mandiant的攻击生命周期模型

初始攻陷

初始攻陷代表入侵者所使用的方法来第一次渗透进某目标组织的网络。与大多数其他APT团组一样，鱼叉式钓鱼是APT1 最常使用的技术。钓鱼攻击邮件包括恶意的附件或者连接到恶意文件夹的链接。主题行和邮件文本通常与接收者相关。APT1 也使用真正的人名建立web 邮件账号——接收者熟悉的名字，如同事，公司领导，IT 部门员工，或公司顾问，并使用这些账号来发送邮件。作为一个现实世界的例子，下面是一封APT1 发送给Mandiant员工的邮件：

```
Date: Wed, 18 Apr 2012 06:31:41 -0700
From: Kevin Mandia <kevin.mandia@rocketmail.com>
Subject: Internal Discussion on the Press
Release

Hello,
Shall we schedule a time to meet next week?
We need to finalize the press release.
Details click here.

Kevin Mandia
```

FIGURE 15: APT1 Spear Phishing Email

图15：APT1 鱼叉式钓鱼邮件

第一眼看去，这封邮件好像来自Mandiant 的CEO，Kevin Mandia。但是，进一步的审查就会发现这封邮件不是从Mandiant 的公司邮件账号中发出的，而是从“kevin.mandia@rockertmail.com"中发出的。Rocketmail 是一个免费的web 邮件服务。这个邮箱“kevin.mandia@rockertmail.com"也不属于Kevin Mandia。相较而言，这个邮箱很可能是APT1攻击者专门为此次钓鱼事件注册的。如果任何人在那天点击了连接（幸亏没人点击），他们的计算机将会下载一个恶意ZIP 文件。这个文件包含恶意执行代码，会安装APT1 专用的叫做WEBC2-TABLE的后门。

尽管APT1成员使用的鱼叉式网络钓鱼邮件附件并不一定是ZIP格式，但据我们在过去几年的观察，ZIP格式依然是主要趋势。下面列举了一些APT1曾使用过的ZIP格式的恶意文件名：

2012ChinaUSAviationSymposium.zip

Employee-Benefit-and-Overhead-Adjustment-Keys.zip

MARKET-COMMENT-Europe-Ends-Sharply-Lower-On-Data-Yields-Jump.zip

Negative_Reports_Of_Turkey.zip

New_Technology_For_FPGA_And_Its_Developing_Trend.zip

North_Korean_launch.zip

Oil-Field-Services-Analysis-And-Outlook.zip

POWER_GEN_2012.zip

Proactive_Investors_One2One_Energy_Investor_Forum.zip

Social-Security-Reform.zip

South_China_Sea_Security_Assessment_Report.zip

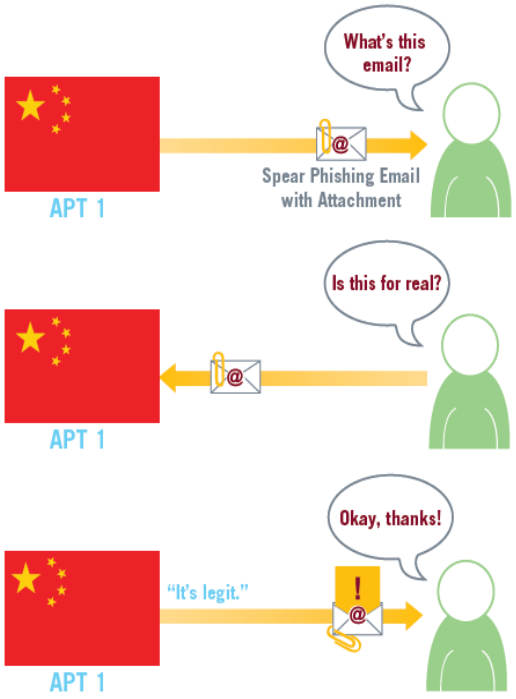
Telephonics_Supplier_Manual_v3.zip

The_Latest_Syria_Security_Assessment_Report.zip

Updated_Office_Contact_v1.zip

Updated_Office_Contact_v2.zip

Welfare_Reform_and_Benefits_Development_Plan.zip



如上列举的文件名包括军事，经济和外交的主题，这表明APT1的目标涉及各行业领域。

有些名字也是通用的（如“updated_office_contact_v1.zip”），可以用于任何工业目标。

在某些情况下，不知情的收件人回复了这些鱼叉式钓鱼邮件，并相信他们是在与熟人沟通。 在一个案例中收件人说：“我不知道这封邮件是否合法，所以我没有打开它。”然后在20分钟后，APT1中就有人回复了一个简洁的邮件证明“这是合法的。”

图16：APT1的鱼叉式网络钓鱼邮件与收件人互动

你是否会点击这个件？

许多APT1成员都会将恶意软件隐藏在ZIP格式文件内并将其伪造成一个Adobe PDF文件。下面是一个例子：

这并不是一个PDF文件。它的文件扩展名看起来像是PDF格式，实际上在“.pdf” 之后有119的空格，然后是“.exe”，这才是真正的文件扩展名。 APT1甚至还会将这个可执行文件的图标伪造成Adobe的样式来完成的他们的入侵目的。然而，这个文件其实是一个自定义APT1后门，我们称之为WEBC2-QBP。

建立一个据点

建立据点是为了确保可以从外网来进行目标网络控制。一旦电子邮件被收件人打开，那么恶意文件以及后门就会随之安装，这样APT1就成功建立了一个据点。后门程序是一种软件，安装后允许入侵者使用远程命令入侵内部系统。通常，APT后门程序启动后会主动外联

入侵者的“命令&控制”（C2）服务器。 APT入侵者使用这种战术策略是因为网络防火墙针对处理外网的恶意软件向内部网络系统通信能力很强，而对于已经存在于内部系统中的恶意软件向外通信就显得无能为力了。

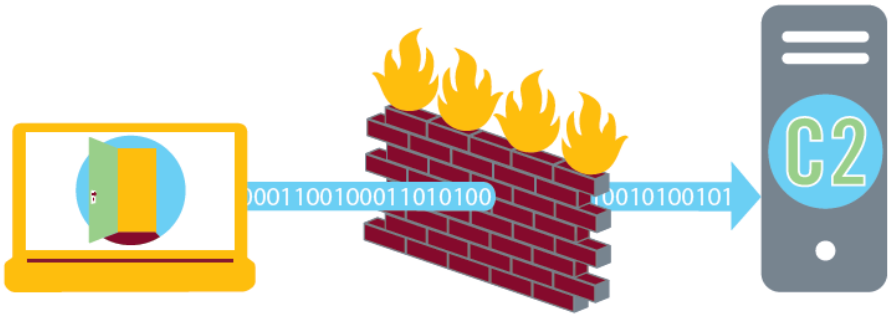


图17：安装在内部系统的后门程序发起与C2服务器的外网连接

APT1入侵者偶尔会使用一些知名的后门程序，如Poison Ivy和GH0ST RAT。在过去很长一段时间内，他们入侵所使用的后门程序通常都是自定义的。我们已记录了42种APT1已使用但未公开的后门程序在“附录C：恶意软件库”中。此外，我们还提供1007个APT1所使用的恶意软件MD5哈希校验值在附录E中。我们将APT1使用的后门程序区分为两大类：“据点后门”和“标准后门。”

据点后门

据点后门可提供入侵最低功能需求。它们为入侵者提供一个小的据点用于执行简单的任务，如检索文件，收集系统基本信息，并触发执行其他更显著的功能，比如一个标准后门。APT1的据点后门就是我们所说的WEBC2后门，是APT1后门中最知名的一种，因此也令一些安全公司将APT1作为“Comment Crew.”。WEBC2后门被设计为网页检索连接C2服务器。该网页包含特殊的HTML标记；该后门程序会将该标记间的数据解析为命令。初期版本的WEBC2后门会解析包含在HTML标记的数据，随着时间的流逝，WEBC2后门变种已经发展到可以解析其他类型标记的数据。很明显，早在2006年7月我们就可以确认APT1已采用WEBC2后门进行入侵。但是，WEBC2 - KT3的第一次编译时间是在2004-01-23 ，这表明APT1自2004年初以来已经开始设计WEBC2后门，基于我们收集的400多个WEBC2变种样品，表明APT1有超过6年的时间都直接从开发者手中获取最新的WEBC2后门变种。

什么是恶意软件家族？

恶意软件家族是恶意软件的集合，其成员都有共同的代码特征。为了说明这一点，用现实世界进行举例，。现在有一个庞大平板电脑销售平台。其中包括苹果的iPad，三星的Galaxy Tab，以及微软的Surface。虽然这些都是平板电脑，但是内在他们是完全不同的。显然对于iPad1与iPad2共同点更多，而对于iPad1与Surface就可以归属于iPad家族以及Surface家族。

对于计算机程序，如果代码相似部分达到80%以上我们就考虑将其分到同一类别。当然也有例外，例如有些文件包含相同的公共或者标准lib代码，这种我们是不考虑划分为一类的。

例如，在WEBC2样本表中如下两个构建路径，有效的说明了APT1长期持续的更新WEBC2后门变种的一个发展过程：

例子 A

MD5: d7aa32b7465f55c368230bb52d52d885

编译日期: 2012-02-23

\work\code\2008-7-8muma\mywork\winInet_winApplication2009-8-7\mywork\aaaaaaa2012-2-23\Release\aaaaaaa.pdb

例子 B

WEBC2家谱

WEBC2-AUSOV	WEBC2-KT3
WEBC2-ADSPACE	WEBC2-QBP
WEBC2-BOLID	WEBC2-RAVE
WEBC2-CLOVER	WEBC2-TABLE
WEBC2-CSON	WEBC2-TOCK
WEBC2-DIV	WEBC2-UGX
WEBC2-GREENCAT	WEBC2-YAHOO
WEBC2-HEAD	WEBC2-Y21K

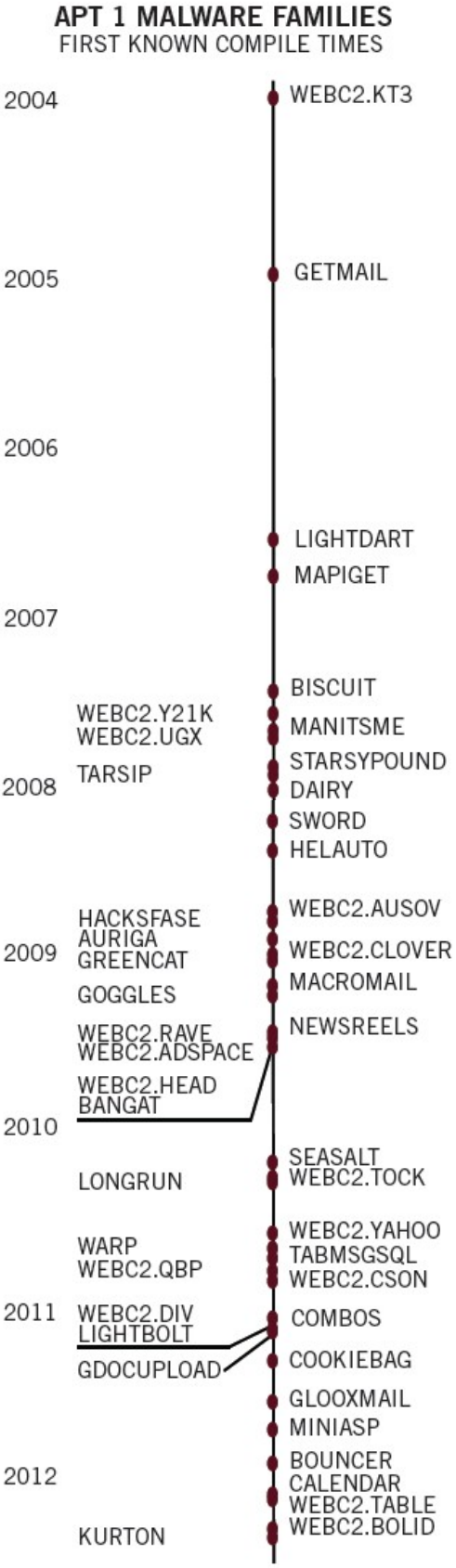
...仍有许多尚未分类

MD5: c1393e77773a48b1eea117a302138554

编译日期: 2009-08-07

D:\work\code\2008-7-8muma\mywork\winInet_winApplication2009-8-7\mywork\aaaaaaa\Release\aaaaaaa.pdb

“编译路径”暴露了开发者所建立的目录和他所编译的源代码。这些WEBC2的样本，2.5年前编译完成，被编译在目录“工作\代码\...\文件夹中编译MYWORK”下。这些事例显示出，在WEBC2上进行工作是某些人的日常工作，而不是隐藏的项目或业余爱好。此外，该样本A生成的字符串包含“2012-2-23” - 匹配样本A的编译完成日期。虽然样本B生成字符串缺少“2012-2-23”，但包括“2009-8-7” - 这也同样匹配样品B的编译完成日期。 这表明，用来编译样本A的代码是从2.5年以前已经编译的样品B的代码演变而来。而存在的字符串“2008-7-8”表明两个样本的代码是为从2008年7存在的一个版本演变而来，这个时间正好是样本B产生的一年前。这一系列的日期表明，发展和改进WEBC2后门是一个长期反复的过程。



WEBC2后门通常是APT1袭击者通过一系列短而基本的命令发送到受害者的系统，包括：

»»打开一个交互式外壳程序（通常是Windows的CMD.EXE）

»»下载并执行文件

»»睡眠（即保持不活动状态）在指定的时间内

WEBC2后门通常通过打包鱼叉式钓鱼邮件进行安装。一旦安装完毕，APT1入侵者可以选择受害者系统下载并执行自己选择的额外恶意软件。WEBC2后门可以达到预期的目的，但它们比下面描述的“标准后门”功能少。

标准后门

其中的标准，指非WEBC2 APT1后门通常使用HTTP协议进行通信（以融入合法的网络

流量）或该恶意软件作者自己设计的自定义协议。这些后门给APT入侵者提供了一系列的方法来控制受害人的系统，包括：

»»创建/修改/删除/执行程序

»»上传/下载文件

»»创建/删除目录

»»显示/启动/停止进程

»»修改系统注册表

»»以用户的桌面截图

»»捕获击键

»»捕捉鼠标的动作

»»启动交互式shell命令

»»创建远程桌面（即图形）接口

»»获取密码

»»枚举用户

»»在网络上列举其他的系统

»»睡眠（即变为无效），在指定的时间内

»»注销当前用户

»»关闭系统

BISCUIT后门（因命令“bdkzt”命名）就是APT1构造的“标准”后门命令中一个比较典型的例子。APT1从2007年就开始使用并且有规律的修改BISCUIT，而且到目前仍然在使用。

表四：一些BISCUIT命令

Command	Description
bdkzt	Launch a command shell
ckzjqk	Get system information
download <file>	Transfer a file from the C2 server
exe <file> <user>	Launch a program as a specific user
exit	Close the connection and sleep
lists <type>	List servers on a Windows network.
ljc	Enumerate running processes and identify their owners.
sjc <PID>|<NAME>	Terminate a process, either by process ID or by process name.
upload <file>	Send a file to the C2 server
zxdosml <input>	Send input to the command shell process (launched with “bdkzt”).

在众多后门中这些功能是比较有特点的，ATP1甚至是APT都在使用。例如，任何人想远程控制一个系统都很可能把“上传/下载文件”放到后门中。

隐蔽通信

除了HTTP协议，一些APT后门试图去伪造合法的网络通信。APT1创建了少数的协议，包括：

表五：伪造合法通信协议的后门程序

Backdoor	Mimicked protocol
MACROMAIL	MSN Messenger
GLOOXMAIL	Jabber/XMPP
CALENDAR	Gmail Calendar

当网络守卫者看到这些后门和C2服务器之间的通信，可能会简单的当做是合法的网络流量进行处理。此外，许多APT1的后门程序使用SSL加密，使通信都隐藏在一个加密的SSL通道。我们在附录F中提供了APT1的公共SSL证书，使人们可以将它们纳入自己的网络签名中。

权限提升

提升特权包括获得的信息（通常是用户名和密码）可以接入到更多资源的网络。在现在及未来，APT1和其它的APT入侵者（或一般入侵者）差不多，主要使用公开可用的工具，从受害者的系统获得hash密码，以获取合法用户的信息。

APT1利用这些权限提升工具：

表6：已经公开的APT1已使用的权限提升工具

Tool	Description	Website
cachedump	This program extracts cached password hashes from a system's registry	Currently packaged with fgdump (below)
fgdump	Windows password hash dumper	http://www.foofus.net/fizzgig/fgdump/
gsecdump	Obtains password hashes from the Windows registry, including the SAM file, cached domain credentials, and LSA secrets	http://www.truesec.se
lslsass	Dump active logon session password hashes from the lsass process	http://www.truesec.se
mimikatz	A utility primarily used for dumping password hashes	http://blog.gentilkiwi.com/mimikatz
pass-the-hash toolkit	Allows an intruder to “pass” a password hash (without knowing the original password) to log in to systems	http://oss.coresecurity.com/projects/pshtoolkit.htm
pwdump7	Dumps password hashes from the Windows registry	http://www.tarasco.org/security/pwdump_7/
pwdumpX	Dumps password hashes from the Windows registry	The tool claims its origin as http://reedarvin.thearvins.com/, but the site is not offering this software as of the date of this report

●

哈希密码是什么？

当一个人登录到计算机，网站，电子邮件服务器，或任何网络资源时，需要提供密码，该密码需要进行验证。验证的一种方法是，在系统上存储个人实际的密码，在用户登录时比较输入的密码与存储的密码。虽然简单，但这种方法很不安全，可以访问这些系统的人都能够看到用户的密码。取而代之的是，验证密码系统通常存储密码哈希值。简单而言，hash密码是用数学的方法来进行加密的数字。使用数学方法（算法）创建的hash密码都是唯一的值。当一个人提供他们的密码，计算机将生成hash密码并比较其存储的哈希值。如果它们匹配，密码则是对的，且用户允许登录。

哈希后的值是不可能“反向”的散列来得到原来的密码。然而，有可能用足够的计算资源，以“破解”密码哈希值，发现原来的密码。（“破解”一般由猜测大量的密码，哈希它们，并比较所产生的hash值，并与现有的hash值进行比较，看是否匹配。）。入侵者希望从受害者系统窃取密码hash值的原样（即“传递hash值”），或破解他们来发现用户密码。

内部侦察

在内部侦察阶段，入侵者收集有关受害人的环境信息。像大多数的APT（和非APT）的入侵者，APT1主要使用内置的操作系统命令来探索一个受损系统和它的网络环境。虽然他们通常只需要输入这些命令，有时入侵者可以使用批处理脚本来加快这一进程。下面的图18显示了APT1在至少四个受害者网络上使用的脚本。

```
@echo off
ipconfig /all>>"C:\WINNT\Debug\1.txt"
net start>>"C:\WINNT\Debug\1.txt"
tasklist /v>>"C:\WINNT\Debug\1.txt"
net user >>"C:\WINNT\Debug\1.txt"
net localgroup administrators>>"C:\WINNT\Debug\1.txt"
netstat -ano>>"C:\WINNT\Debug\1.txt"
net use>>"C:\WINNT\Debug\1.txt"
net view>>"C:\WINNT\Debug\1.txt"
net view /domain>>"C:\WINNT\Debug\1.txt"
net group /domain>>"C:\WINNT\Debug\1.txt"
net group "domain users" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain admins" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain controllers" /domain>>"C:\WINNT\Debug\1.txt"
net group "exchange domain servers" /domain>>"C:\WINNT\Debug\1.txt"
net group "exchange servers" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain computers" /domain>>"C:\WINNT\Debug\1.txt"
```

图18：可自动侦察的APT1批处理脚本

这个脚本执行如下功能并将结果记录到文本文件中：

»»显示被攻击网络的配置信息

»»列出被攻击网络系统上启动的服务

»»列出当前运行的进程

»»列出系统上的账号

»»列出系统管理员账号

»»列出当前网络节点

»»列出当前共享的网络节点

»»列出网络中其他的系统

»»列出计算机网络和账户所属的组（“域控制器”，“域用户”，“域管理员”等）

横向移动

一旦APT入侵者在网络内部有合法的立足点和合法的证书凭证时，那侵入者在网络内部活动就不会被察觉：

- 他们可以和连接的其他系统共享资源
- 他们从微软Sysinternals或者微软内部的任务调度程序，并使用公开的工具“psexec”，在其他系统上执行命令。

这些动作是很难发现的，因为合法的系统管理员也可以使用这些技术对网络进行操作。

保持存在

在这个阶段时，攻击者为了确保从网络外部长时间持续的控制网络环境中的重要系统，会采取一下措施。ATP1通常是采取三种方式。

1 在多操作系统安装新的后门程序

在他们存在网络期间内(可能是以年计)，APT1通常安装新的后门程序以便他们能够在环境中获得更多的系统。那么，如果一个后门被发现和删除，他们仍然有其他的后门可以使用。我们经常在被攻击网络周边散落的多个软件族中检查到ATP1后门程序，而此时APT1已经存在几周了。

2 使用合法的VPN证书

一般情况下，APT攻击者和黑客一直在寻找有效的证据，以便于能够冒充合法的用户。我们经常观察到APT偷取用户名和密码登录到被攻击者网络的VPN中，由于VPN只是单一的认证。从那里他们可以访问到只有内网用户才可以访问的任何资源。

3 登录到门户网站

一旦凭证被偷取，APT1入侵者也会尝试登录到门户网站的的网络提供商。这不仅包括受限制的门户网站，而且还包括基于WEB的电子邮件系统，如Outlook web access等。

完成任务

类似于我们跟踪其他APT组织，一旦APT1发现他们感兴趣的文件，他们会在偷取之前将文件压缩打包。ATP入侵者经常使用RAR压缩工具来完成这个任务，并且确保压缩文件时密码保护的。有时候APT1入侵者使用批处理脚本，来协助他们完成这个任务。如图19所示（”XXXXXXXX”是实际批处理脚本中的文本）

```
@echo off
cd /d c:\windows\tasks
rar.log a XXXXXXXX.rar -v200m "C:\Documents and Settings\Place\My
Documents\XXXXXXXX" -hpsmy123!@#
del *.vbs
del %0
```

图19 捆绑被盗文件转换成RAR压缩包文件的APT1批处理脚本

通过创建RAR压缩文件，APT1攻击者和其他APT组织在网络外通过这种方式传输文件。包括使用FTP或者其他已经存在的后门程序。很多时候传输的RAR文件是很大的，在传输前需要将其分成小块。上图19中显示了1个RAR命令和选项，意思是将RAR文件分成200MB大小的部分。

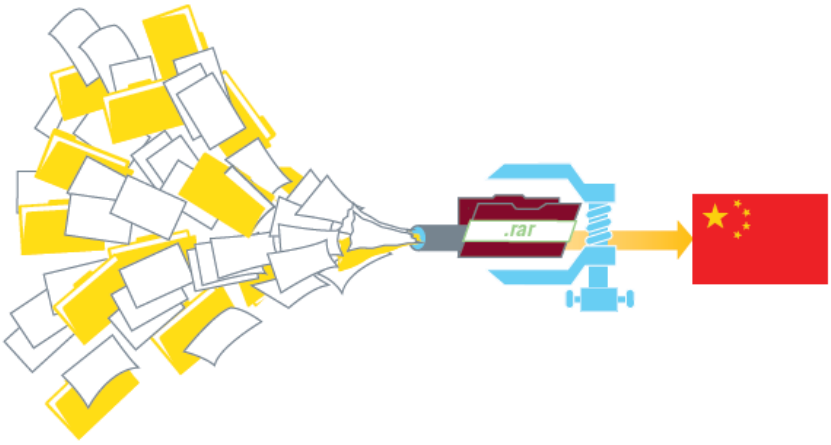


图20 APT1将盗窃的数据在传输到中国前转换成RAR压缩包

不像我们跟踪的其他APT组织，APT1使用两个邮件盗窃应用，我们相信是APT1独有的。首先是GETMAIL，是专门从微软Outlook存档中获取电子邮件、附件和文件夹。

微软Outlook的存档很大，经常存储的多年积累的电子邮件。他们可能很大，从网络转出很快，同时入侵者不会关心他们偷取的每一封邮件。GETMAIL程序允许入侵者灵活的只根据日期进行他们的选择。在之前的案例中，APT1攻击者每周一次进入受攻击的网络，连续四周仅偷取过去一周的邮件。

鉴于GETMAIL盗取Outlook存档邮件，第二个工具是MAPIGET,是专门盗取尚未存档和仍然存放在微软Exchange服务器上的邮件。为了操作成功，MAPIGET需要用户名/密码组合，Exchange服务器才会接受。MAPIGET会从指定的账户中提取电子邮件正文生成文本文件并分离附件。

英语作为第二种语言

APT1所说的英语“这是合法的”电子邮件，不应该被认为APT1人员都精通英语，尽管有些人是。他们的数字化工具显示他们编写程序的人员第一语言不是英语。下面是多年来APT1使用的工具中的一些不正确语法的例子。

表7：APT1恶意软件实例中语法不正确的短语

Phrase	Tool	Compile date
If use it, key is the KEY.	GETMAIL	2005-08-18
Wether encrypt or not,Default is NOT.	GETMAIL	2005-08-18
ToolHelp API isn't support on NT versions prior to Windows 2000!	LIGHTDART	2006-08-03
No Doubt to Hack You, Writed by UglyGorilla	MANITSME	2007-09-06
Type command disable.Go on!	HELAUTO	2008-06-16
File no exist.	Simple Downloader (not profiled)	2008-11-26
you specify service name not in Svchost\netsvcs, must be one of following	BISCUIT	2009-06-02
Can not found the PID	WEBC2 (Uncat)	2009-08-11
Doesn't started!	GREENCAT	2009-08-18
Exception Catched	MACROMAIL	2010-03-15
Are you sure to FORMAT Disk C With NTFS?(Y/N)	TABMSGSQL	2010-11-04
Shell is not exist or stopped!	TARSIP	2011-03-24
Reqfile not exist!	COOKIEBAG	2011-10-12
the url no respon!	COOKIEBAG	2011-10-12
Fail To Execute The Command	WEBC2-TABLE	2012-02-23

5 APT1：基础设施

APT1在全世界维护着一个庞大的计算机基础设施。我们有证据表明APT1控制着成千上万的系统，用来支持他们的攻击行为，并且直接监视和控制着这些系统。虽然他们控制着许多国家的系统，但他们的攻击源于上海的四个大的网络中心-其中两个直属于浦东地区，属于61398部队。APT1的IP地址集中在上海地区，再加上APT1的攻击系统都有简化的中式键盘布局设计，暴露了工作人员的真实位置和使用的语言。为了帮助管理他们控制着大量的系统，APT1已经注册了很多域名，其中大部分的域名都是指向了上海本地。这些域名名称和IP地址都包含了APT1的指令和控制框架以便他们统一管理并且伪装他们的真实来源。

APT1 网络起源

我们经常会问为什么在中国一个无效的安全措施可以正确阻拦连接你网络的所有的IP地址。简单来说，APT1攻击者通过反弹或者“跳”的方式穿过中间系统但是他们几乎从来不直接通过在上海的系统连接被侵入的网络。基于强大的网络组织架构，他们可以选择任何国家发起攻击进行入侵。这种类型的网络重定向的系统被叫做“跳跃点”或者“跳”。跳跃点大部分是APT1可以使用“沦陷”的系统，为了隐蔽他们的攻击，系统的拥有者不会知道系统已经被攻击，这些系统属于第三方的受害者。

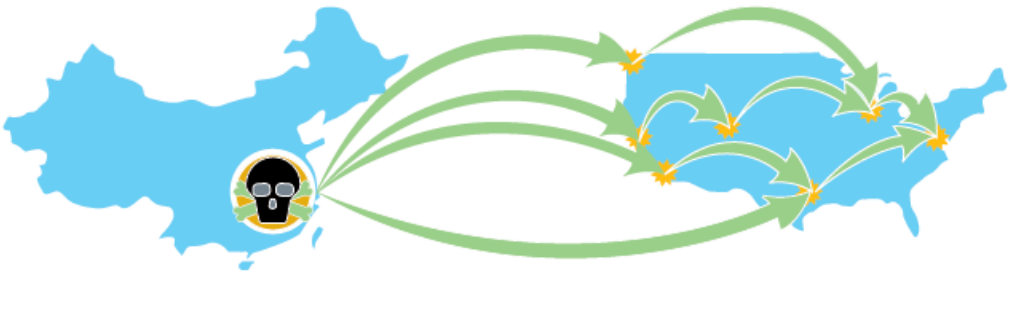


FIGURE 21: APT1 bounces through “hop point” systems before accessing victim systems

图21：APT1通过跳点访问受害者系统

我们已经发现一些APT1的活动，尤其当他们穿过美国领域之后。他们使用不同的技术登录跳跃点，大部分是远程桌面和FTP。在两年时间中（2011年1月到2013年1月）我们确认APT1操作者使用832个不同的IP地址通过远程桌面方式登录过1095次他们的跳跃点。远程桌面提供一个可视化的接口。这个体验就类似用户可以真实的使用系统并且可以直接操控桌面、鼠标和键盘。832个IP地址，有817(98.2%)属于中国并且这些地址受控于APT1的网络，属于上海的四个大的网络块。

表8：APT1用来访问跳点的IP地址块

Number	Net block	Registered Owner
445	223.166.0.0 - 223.167.255.255	China Unicom Shanghai Network
217	58.246.0.0 - 58.247.255.255	China Unicom Shanghai Network
114	112.64.0.0 - 112.65.255.255	China Unicom Shanghai Network
12	139.226.0.0 - 139.227.255.255	China Unicom Shanghai Network
1	114.80.0.0 - 114.95.255.255	China Telecom Shanghai Network
1	101.80.0.0 - 101.95.255.255	China Telecom Shanghai Network
27	Other (non-Shanghai) Chinese IPs	

需要指出的是，上面的第二和第三个网段的注册信息中包括了如下信息：

person: yanling ruan

nic-hdl: YR194-AP

e-mail: sh-ipmaster@chinaunicom.cn

address: No.900,Pudong Avenue,ShangHai,China

phone: +086-021-61201616

fax-no: +086-021-61201616

country: cn

这两个网络网段的注册信息表明他们是服务于上海浦东新区解放军61398总部。

另外832个地址中的15个地址被注册到美国、台湾、日本和韩国的组织。我们已经证实，其中一些系统是APT1跳跃点系统，并且被APT1非法控制-换句话说APT1是从一个跳跃点访问到另一个跳跃点，而不是从上海直接去访问。

为了有更好的用户体验，远程桌面协议要求客户端应用向服务器端发送一些重要细节，包括他们的客户端的主机名和键盘布局。在过去的两年中我们从1849个APT1远程桌面的会话观察中发现键盘设置都为”简体中文-美式键盘”。微软系统的远程桌面客户端自动根据客户端系统上所选择的语音进行配置，这样会确定APT1操作者管理的下一跳的基础设施都有简体中文(zh-cn)的输入设置。”简体中文”是自20世纪50年代已在使用传统的中国文字，发源于中国大陆。台湾和直辖市例如香港仍然使用”传统中文”(zh-tw)字符集。

与后门程序的互动

正如我们刚才提到的，APT1攻击者通常利用跳跃点来连接并且控制受害者的系统。受害者后门程序定期连接到跳跃点，时刻等待着攻击者给他们下达指令。但是这样的工作往往需要使用特定的工具。

手工WEBC2更新

由于已经在前面的”攻击生命周期”一节中覆盖了，WEBC2后门把不同的下载和翻译数据存储在HTML页面的tag之间，如同命令行一样。ATP1通常是从系统内的跳跃点下载HTML页面。我们观察APT1入侵者登录到WEBC2服务器并且手工编辑HTML页面，该后门程序就会下载。因为这些命令通常是编码，难以从内存中读取，APT1入侵者通常不输入这些字符串，而是将他们复制并且粘贴到HTML文件。他们很可能在自己的系统中已经创建好这些编码命令然后在粘贴到跳跃点的HTML文件中。例如，我们观察到一个APT攻击者粘贴字符串”czolNA==”到HTML页面中。这些字符串使用base64进行编码为”s:54”，意思为”休眠54分钟”(或者小时，取决于不同的后门工具)。除了手动编辑跳跃点的HTML文件，我们也观察到ATP1入侵者可以上传已经编辑好的HTML文件。

HTRAN

当APT1攻击者不使用WEBC2，他们需要一个”命令控制”(C2)的用户界面，这样他们就

可以对后门程序发出命令。这个接口有时运行于他们的个人攻击系统中，它通常是在上海。在这些情况下，当受害者后门程序与跳跃点进行连接时，这个通讯连接需要从跳跃点转到上海的入侵系统，使后门可以跟C2服务器软件进行沟通。我们观察到有767个单独的实例中APT1入侵者在跳跃点使用的公开的”HUC报文转换工具”或者HTRAN。与往常一样，这些工具的使用只是APT1活动的一小部分。

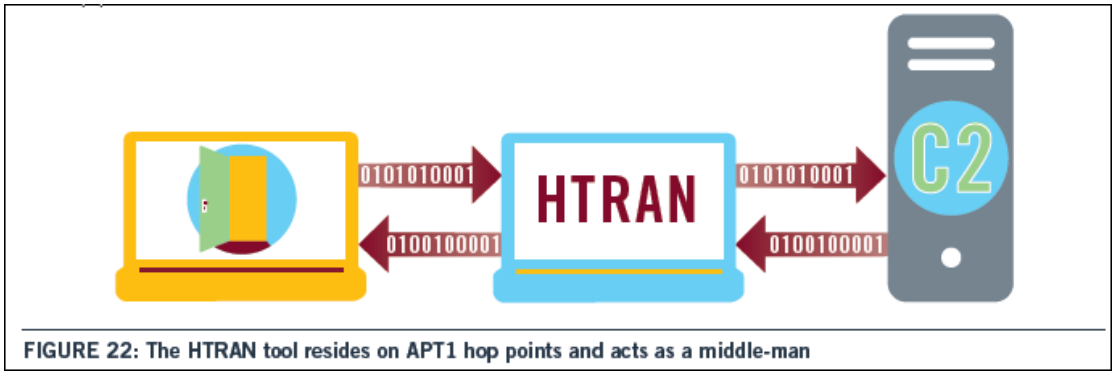


FIGURE 22: The HTRAN tool resides on APT1 hop points and acts as a middle-man

图22：HTRAN工具存在存在于APT1的跳跃点上，类似于中间人

HTRAN的典型应用很简单：攻击者必须指定起源的IP地址（他或者她在上海的工作站），还有一个可以接受连接的端口。例如，如下是由APT1操作者下发的命令，将监听跳跃点的443端口上的接入连接，并且自动代理他们到上海的IP地址58.247.242.254端口443：

Htran –tran 443 58.247.242.254 443

在HTRAN的767个观察对象中，APT1入侵者提供614不同的可以路由的IP地址。换句话说，他们用跳跃点充当受害系统和614个不同地址的中间人的功能。这些地址614个中有613个是APT1的内部地址:

Number	Net block	Registered Owner
340	223.166.0.0 - 223.167.255.255	China Unicom Shanghai Network
160	58.246.0.0 - 58.247.255.255	China Unicom Shanghai Network
102	112.64.0.0 - 112.65.255.255	China Unicom Shanghai Network
11	139.226.0.0 - 139.227.255.255	China Unicom Shanghai Network
1	143.89.0.0 - 143.89.255.255	Hong Kong University of Science and Technology

C2服务器软件

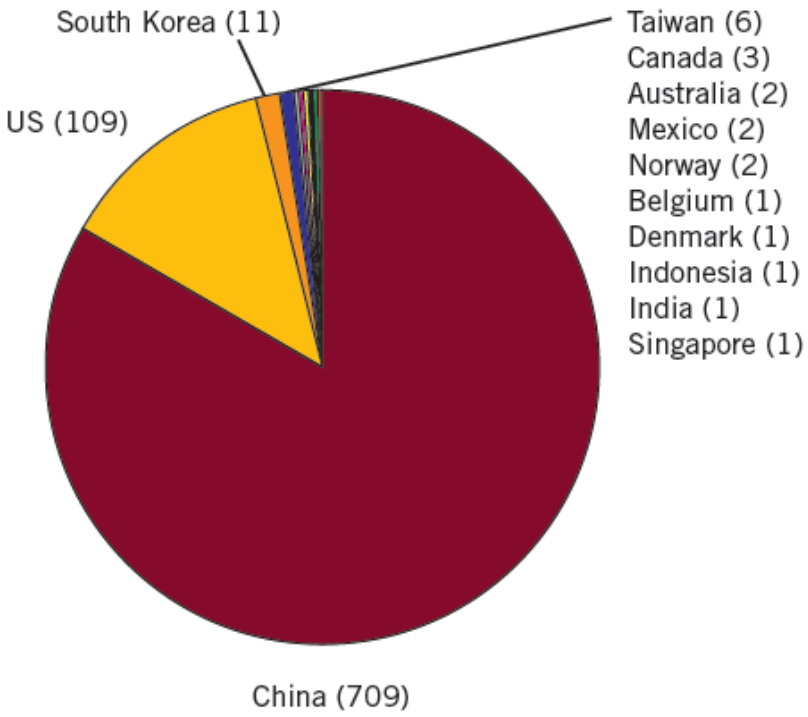
有时候，APT1攻击者已经在他们的基础设施系统中安装了C2服务器组件。在这种情况下，他们并不需要使用代理工具如HTRAN与受害者系统进行交互，然而，这并不意味着入侵者必须能够在跳跃点引用C2软件系统界面连接。我们观察APT1入侵者在他们的跳跃点登录，启动C2服务器，等待接入连接，然后进入到受害者系统下达指令。

WEBC2变种可能包括一个服务器组件，它提供了一个简单的C2接口给入侵者。这样入侵者就不必要进行手工编辑WEB页面。也就是说，这个服务器组件接收来自受害者后门程序的连接，将信息显示给入侵者，然后转换入侵者的命令为到HTML页面中以便受害者后门程序读取。

APT1 服务器

仅在过去的两年，我们已经确认了937个APT1 C2服务端，这些服务器处于激活状态的监听或通信程序，运行在849个独立的IP地址上。不过，我们有证据让人想象到APT1运行着成百上千的其它服务器(看以下的域名分布)。这些程序作为APT1服务器主要用于：1、作为传输文件的FTP；2、主要用于WEBC2的WEB；3、作为远程控制系统的RDP；4、作为代理的HTRAN；5、同各种后门联系的C2服务器。

已确认的APT1服务器在全球的分布



已确认的APT1服务端在中国的分布

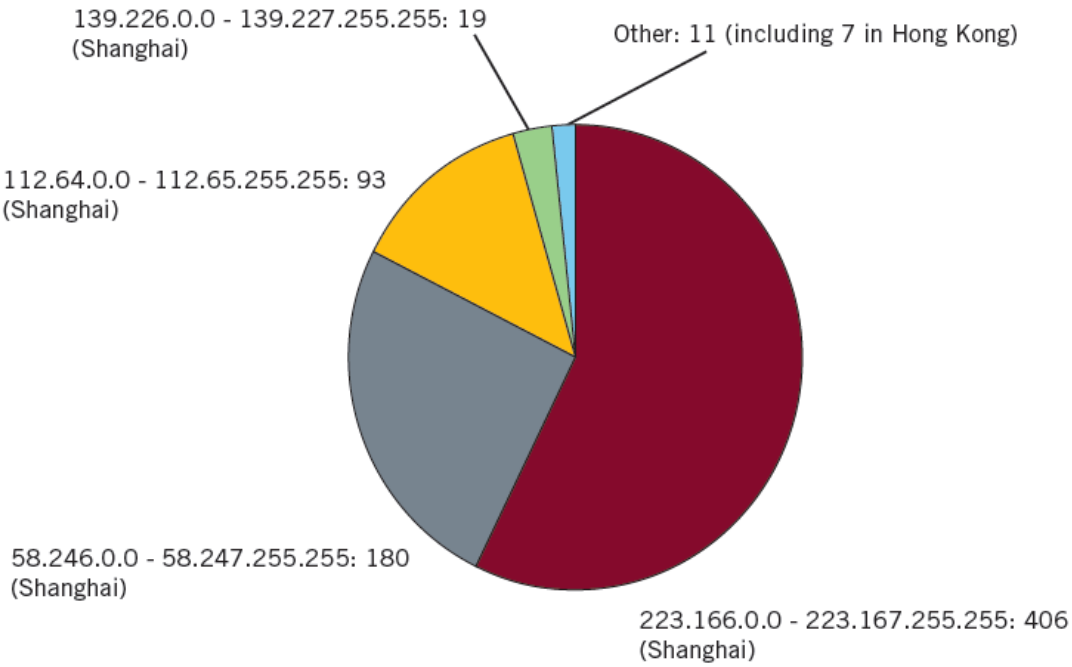


图23：已确认的ATP1服务端的全球分布

域名

域名系统（DNS）就是万维网的电话簿，就像人们将联系人以不同的名字存于手机中，不需要记住电话号码一样，DNS允许人们仅记住像“google.com”这样的名字而非IP地址。当人们在浏览器中输入“google.com”，DNS会将之转成一个IP地址，这样个人计算机就能够访问Google。能够被DNS解析成IP地址的名字被称为完全合格域名（FQDN）。

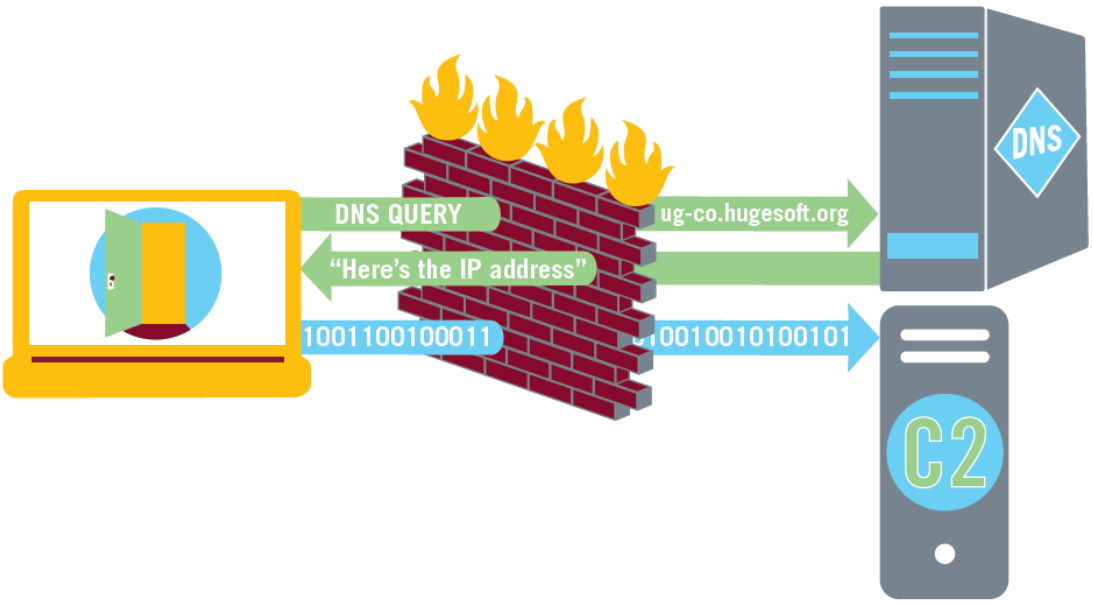
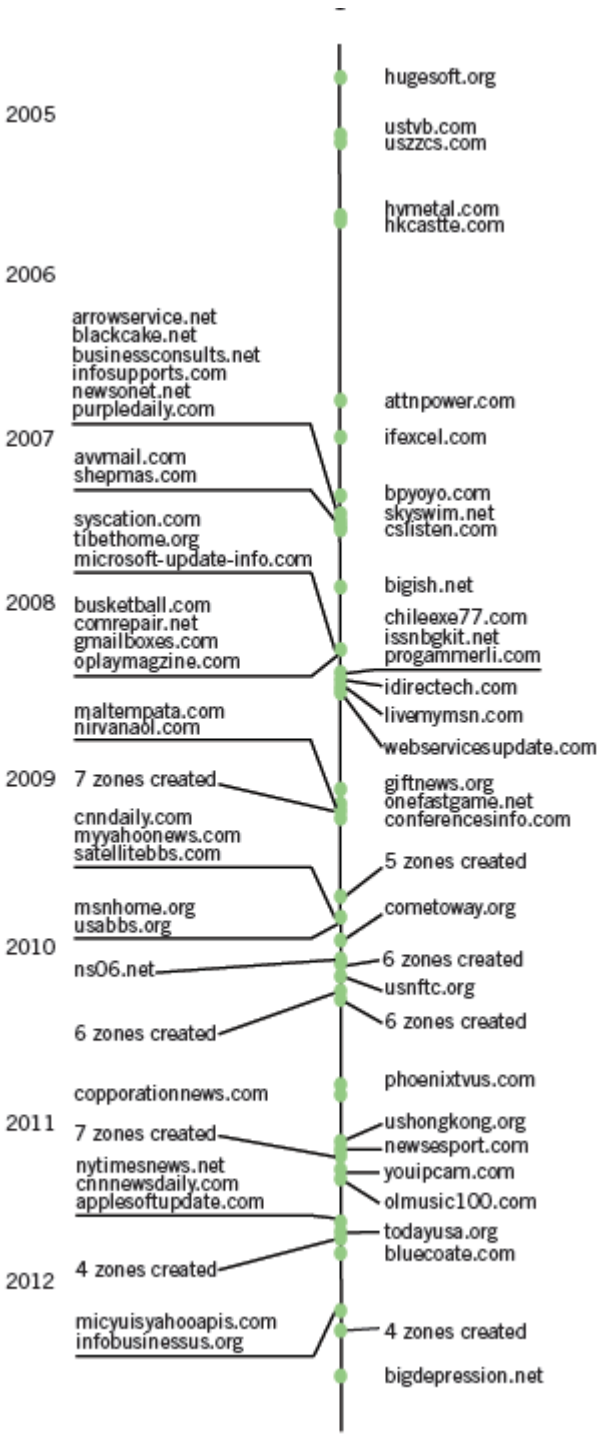


图24：使用DNS请求把APT1 FQDN解析成C2服务端的IP地址

APT1注册区



APT1的基础设施包括FQDN及对应的IP地址，ATP1将FQDN作为C2地址嵌入到他们的后门中，FQDN在他们的入侵活动中起了重要的作用。在过去的几年中，我们已经确认2552个FQDN属于APT1。另外，我们编辑整理了跟受害者相关联的FQDN，并在附录D中提供了2046个FQDN。通过使用FQDN而非固定的IP地址作为C2地址，攻击者可以动态的决定来自后门的主动连接指向哪里的C2。这样的话，如果他们失去一个具体跳点（IP地址）的控制，他们还能将C2 FQDN地址指向另外一个地址，并且重新取得被害者后门的控制。这种灵活性方便攻击者将被害者的系统连接到大量的C2服务端，保证连接畅通。

APT1 FQDN可以归为以下三类：1、注册区；2、第三方区；3、劫持域。

注册区

一个DNS区代表了一个含有不同FQDN名字的集合，这些FQDN通常通过域名注册公司来注册，并被单一的拥有者控制。例如，“hugesoft.org”既是一个FQDN，同时也代表了一个区。“ug-co.hugesoft.org” 和“7cback.hugesoft.org”这两个FQDN是“hugesoft.org”这个区的一部分，被称为这个区的子域。注册“hugesoft.org”的人可以添加任意多的子域，并且控制这些FQDN的IP解析。从2004年，APT1已经注册了至少107个区。在这些区里，我们知道数以千计的FQDN被解析成几百个IP地址（我们怀疑这

些是不同的跳点），且一些APT1源地址在上海。

我们知道的第一个区是“hugesoft.org”，它于2004年10月被eNom公司注册。注册人提供的邮件地址为uglygorilla@163.com。其提供的注册信息截至2013年2月3日在公共数据库“whois”仍然可以查看到，注册信息如下：

域名：HUGESOFT.ORG

创建时间：2004年10月25日 09:46:18

注册人：huge soft

注册机构：hugesoft

注册街道：上海

注册城市：上海

注册邦/省：S

注册邮编：200001

注册国家：中国大陆

注册电话：+85.21000021

注册邮箱：uglygorilla@163.com

这些提供的注册信息不一定精确。例如，“上海“并不是一个街道的名字。不过值的注意的是，上海出现在我们知道的第一个APT1注册域名中，而且其电话号码是以中国的国际代码”+86“开头的。事实上，在107个注册域名中，至少有24个（22%）的注册城市为上海。

在APT1的注册域名信息中出现的其他城市如下：

表10：除中国上海外，注册域名信息中出现的其他地点

Number	City	State	Country
7	Beijing	-	China
5	Calgary		Canada
4	Guizhou	-	China
4	Pasadena	CA	US
4	Houston	TX	US
3	Sydney		Australia
3	Salt Lake	UT	US
3	Washington, DC		US
2	Homewood	AL	US
2	Kalkaska	MI	US
2	Shallotte	NC	US
2	Yellow Spring	OH	US
2	New York	NY	US
2	Provo	UT	US
2	Shenzhen	-	China
1	Birmingham	AL	US
1	Scottsdale	AZ	US
1	Sunnyvale	CA	US
1	Albany	NY	US
1	Pearl River	NY	US
1	Chicago	-	US
1	Moscow	-	Guatemala
1	Nanning	-	China
1	Wuhua	-	China
27	Registration information blocked or not available		

部分注册信息明显存在错误。例如，2005年为域“uszzcs.com”代理的注册信息如下：

Victor etejedaa@yahoo.com +86.8005439436

Michael Murphy

795 Livermore St.

Yellow Spring,Ohio,UNITED STATES 45387

此处，注册信息中的电话号码带有中国的前缀（“+86”），然而地址却在美国。既然美国使用的前缀是“+1”，那么一个人住在Ohio就几乎不可能使用一个开头是“+86”的号码。另外，城市的名称也未拼写正确，应该是“Yellow Springs”而不是“Yellow Spring”。这本应该是一次性的拼写错误，但该注册者却把城市名称拼错数次，在“uszzcs.com”和“attnpower.com”中都存在。该注册者真的认为“Yellow Spring”是正确的拼写，实际上，那些生活或工作在Yellow Springs的Ohio居民却不这么认为。

总体而言，一个相对数量的“上海”注册登记但信息错误的域名注册活动从2004一直持

续到现在，其中一些人试图捏造非上海的位置，但其他人没有。这被互联网上的电子邮件地址“lfengg@163.com”的语境信息所支持（由注册信息的107区中的第7区提供）。在网站“www.china-one.org,“电子邮件地址”lfengg@163.com”与上海Kai光信息技术有限公司有关联，一个位于上海某处的网站出品公司，与其隔河相望的居然是中国人民解放军61398部队。

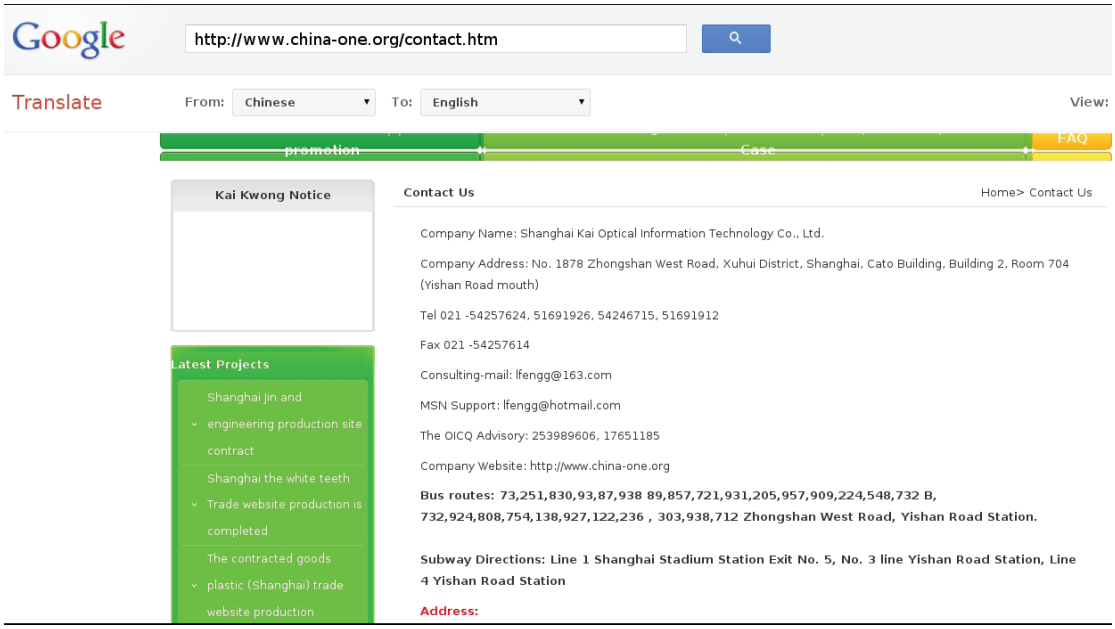


图25：一个用于注册APT1域的电子邮件地址，同时也与一个上海的公司有关联

命名主题

大约一半的APT1区根据三个主题命名：新闻，技术和业务。这些主题使APT1指挥和控制地址第一眼就能认出。然而，我们相信在这些区域的数百个FQDN是为APT1入侵的目的而设立的。（注：通常这些主题对于APT1，甚至APT都不是独有的）

新闻主题区，包括著名的新闻媒体如CNN，Yahoo和Reuters。

然而，它们也包括引用说英文的国家的名称，如“aunewsonline.com”（澳大利亚），“canadatvsite.com”（加拿大），和“todayusa.org”（美国）。下面是一个由APT1用新闻命名而注册的清单：

aoldaily.com	issnbgkit.net	purpledaily.com
aunewsonline.com	mediaxsds.net	reutersnewsonline.com
canadatvsite.com	myyahoonews.com	rssadvanced.org
canoedaily.com	newsesport.com	saltlakenews.org
cnndaily.com	newsonet.net	sportreadok.net
cnndaily.net	newsonlinesite.com	todayusa.org
cnnnewsdaily.com	newspappers.org	usapappers.com
defenceonline.net	nytimesnews.net	usnewssite.com
freshreaders.net	oplaymagzine.com	yahoodaily.com
giftnews.org	phoenixtvus.com	

技术的主题域名参考知名科技公司（AOL，Apple，Google，Microsoft），反病毒厂商（McAfee，Symantec），和产品（Blackberry，Bluecoat）。APT1也使用更通用名称引用主题软件：

aolonline.com	globalowa.com	microsoft-update-info.com
applesoftupdate.com	gmailboxes.com	micyuisyahooapis.com
blackberrycluter.com	hugesoft.org	msnhome.org
bluecoate.com	idirectech.com	pcclubddk.net
comrepair.net	ifexcel.com	progammerli.com
dnsweb.org	infosupports.com	softsolutionbox.net
downloadsite.me	livemymsn.com	symanteconline.net
firefoxupdata.com	mcafeepaying.com	webservicesupdate.com

最后，一些由APT1使用的域名表现了一个企业主题。这类名字提供了专业人士可能会访问网站：

advanbusiness.com	companyinfosite.com	infobusinessus.org
businessconsults.net	conferencesinfo.com	jobsadvanced.com
businessformars.com	copporationnews.com	

不是每一个域名都被APT1永远控制。在持续这么多年的攻击里，APT1并没有总是对它们攻击基础设施的每一个域进行更新。此外，有些已经完全终止。剩余的已经转移到试图去模仿域名的组织里。例如，2011年9月，Yahoo向法院提起诉讼，“Arizona, USA”的”zheng youjun”，他注册了APT1区”myyahoonews.com”。Yahoo宣称的<myyahoonews.com>域名与被投诉人的YAHOO!标记相似以及[zheng youjun]注册并恶意使用< myyahoonews.com >域名。对此，国家仲裁法庭发现“myyahoonews.com”网站在当时指向一个钓鱼网页：一个致力于收集登录凭据的诈骗网站。毫不奇怪，”zheng youjun”没有响应。随后，“myyahoonews.com”的控制权由APT1转给雅虎。

第三方服务

APT1使用得最多的第三方服务被称为“动态DNS”。这是一种服务，允许人们向其他人已经注册并提供服务的子区进行注册。多年来，APT1已经使用这种方式注册了数百个FQDN。当他们需要改变一个FQDN的IP解析时，他们只需简单地通过网络接口登录到这些

服务器并更新他们的FQDN IP解析。除了动态DNS，最近我们发现APT1已经开始创建后缀为“appspot.com”的FQDN，这表明他们正在使用谷歌应用引擎服务。

被劫持的FQDN

APT1入侵者经常使用他们的跳点FQDN。我们将这些领域称为“劫持”是因为它们被一些拥有正当的理由的人注册，却为了恶意的目的被APT1利用。APT1使用劫持的FQDN主要有两个目的。首先，他们把恶意软件（通常在ZIP文件中）放在的合法网站主办的跳点，然后把发送鱼叉式网络钓鱼电子邮件的链接放在合法的FQDN中。第二，在他们的后门嵌入劫持FQDN做为C2的地址。

海量基础设施的证据

正如上面提到的，我们已经证实了937台服务器的存在（监听应用），托管在849个不同的IP地址，IP地址注册的大多数组织在中国（709），其次是美国（109）。在过去的三年里，我们已经观察到了APT1 FQDN解析988个独特的IP地址，我们认为不是“sinkhole”或“domain parking”IP地址：

≈54 United States: 559

≈54 China: 263

≈54 Taiwan: 25

≈54 Korea: 22

≈54 United Kingdom: 14

≈54 Canada: 12

≈54 Other: 83

中国的IP地址又绝大多数属于APT1的母网络，这意味着在某些情况下，入侵者可能绕过他们的基础设施跳点，直接与受害者系统进行联系：

表格11：APT1 FQDNs 解析的中国地址块中的地址

Number	Net block	Registered Owner
150	223.166.0.0 - 223.167.255.255	China Unicom Shanghai Network
68	58.246.0.0 - 58.247.255.255	China Unicom Shanghai Network
10	112.64.0.0 - 112.65.255.255	China Unicom Shanghai Network
7	114.80.0.0 - 114.95.255.255	China Telecom Shanghai Network
5	139.226.0.0 - 139.227.255.255	China Unicom Shanghai Network
4	222.64.0.0 - 222.73.255.25	China Telecom Shanghai Network
3	116.224.0.0 – 116.239.255.255	China Telecom Shanghai Network
16	Other (Non-Shanghai)	

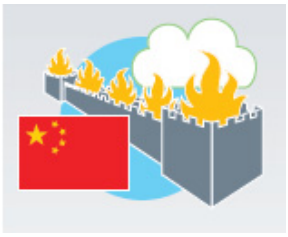
这些统计数字表明，仅在美国就有超过400个IP地址是活动的APT1服务器，这些服务器都是未经Mandiant证实的。此外，虽然我们知道有超过2500个APT1 FQDN，但还有许多我们还不能归于APT1。我们估计（保守地），APT1目前的跳点基础设施中有将超过1000台服务器。

6 APT1：身份

在网络数字世界中APT1并不是象幽灵一样无处可寻，为了说明解放军是APT1幕后的操纵者，我们决定有选择性的揭露APT1的一些人的身份。这些参与者都进行低级的操作安全选择，这利于我们的研究，并允许我们跟踪他们的活动。他们是一些APT1的数字武器的作者和APT1 FQDN和电子邮件帐户的注册人。这些参与者都表示在中国的网络战的兴趣，透露出他们的位置是浦东新区上海，并且甚至使用了上海的手机号码注册鱼叉式网络钓鱼中的电子邮件帐户。

识别APT人员往往需要汇集很多小块的信息做全面的了解。通常这种归一的方法，我们不仅能够揭露不仅该组织的属性，甚至我们能够推导出小团队和个人之间的关联性。APT1人员掌握中技术资源，如跳点和FQDN，他们知道怎么样合理的使用这些网络攻击的资源，把自己融入到工作环境中。

中国的“伟大防火墙”是我们威胁跟踪的额外的元素。像中国许多黑客一样，APT1的攻击者不喜欢被中国共产党所布置的伟大防火墙所限制，他们不喜欢那些严格的条款及审查措施，入WEB访问限制，如不能访问谷歌.COM ， facebook.com ，和twitter.com。黑客的工作要求他们能够控制“伟大防火墙”外的基础设施。这就创造了一种场景：黑客需要从他们的攻击机构采用简单的方式登录到Facebook和Twitter。一旦这种情况被发现，将是揭露他们身份的有效的机会。



什么是中国伟大的防火墙？

“伟大的防火墙”常被中国政府用来描述各种技术手段，通过这些方法，隔断对他们认为是敏感或者不适宜网络服务的访问。所谓的“不适宜”包括色情、政治分歧，也包括社会媒体及对中国及官员的不光彩的描述。“伟大的防火墙”通过地址阻断、域名重定向、阻断特定IP地址;阻断或重定向特定的域名;过滤或阻止任何含有URL目标关键字;和限速或重置TCP连接等方式进行隔离。中国的审查者也例行监视中国网站，博客以及其他 “不适当”的内容，一旦发现就删除。其结果是，中国公民谁希望访问删减的内容必须求助于变通方法，如使用加密手段。中国将继续完善和进一步限制互联网接入，最近（2012年12月）通过阻断额外的服务和限制或阻止使用加密技术，如虚拟专用网络。

APT1黑客简介：丑陋的大猩猩（王东/汪东）

“丑陋的大猩猩” （ UG ）的故事追溯到2004年。当时的教授张召忠，现在退休海军少将，是在这个过程中帮助塑造了中国未来信息战策略。张教授已经是一个军事的“信息化”大力倡导者，并发表了一系列关于军事策略方面的著作，包括《网络战争》和《打赢信息化战争》。国防科技大学（国防大学）军事科技与装备系的指导员，2004年1月，张教授应邀参加题为“展望2004：国际战略形势”的项目。

图26张召忠教授 16 Jan 2004,来源http://www.chinamil.com.cn/site1/gflt/2004-09/30/content_705216.htm

在中国军网解放军日报主办的网上答问环节，一个年轻的男子，绰号“绿地”的人提了一个特别有先见之明问题

“张教授，我看你的书《网络战争》，书中的观点和论据给我留下深刻印象，据说，美国军方已成立专用网络力量被称为“网军”。中国是否也有类似的军用力量？中国是否有网络部队？”

– 2004年UglyGorilla1月16日

像中国军网论坛的其他用户一样，“绿地”被要求填写电子邮件及其他自己的一些相关信息。互联网永远记录所有信息的特性让我们获取了这些数据。

图 27: 丑陋的大猩猩，中国军网简介，来源: http://bbs.chinamil.com.cn/forum/bbsui.jsp?id=(o)5681

因此，我们称之为“ UglyGorilla ” （ UG）的人物首次有记载。除了他的电子邮件地址， UG列出了他的“真正的命名为JackWang。

在一年之内，我们看到了UG所打造工具的第一个证据。2004年10月25日，UG注册了现在臭名昭著的“hugesoft.org ”域名。在“hugesoft.org ”域内，它的许多APT1主机仍然活动并在UG的控制中。注册信息最近更新于2012年9月10日，延长该域名的注册期限到2013年。作为本报告的结果，我们可能会看到UG放弃这个域名和其他域名。

2007年， UG撰写的第一个已知的恶意软件MANITSME，像一个很好的艺术家一样，留下了他清晰可辨的签名，代码为：“1.0版，黑你没商量，UglyGorilla所写，06/29/2007”。UG有为他的作品前面的嗜好。甚至在他的主机名及后门程序的通信协议里面也有体现。例如

例如，包含其他高级持续攻击全称域名（FQDN）的主机名，如“arrowservice.net”和较新的“msnhome.org”都留有UG的印记（注意域中的“UG”）：

ug-opm.hugesoft.org

ug-rj.arrowservice.net

ug-hst.msnhome.org

虽然这类明显的纰漏因为UG的经验越来越丰富而变得逐渐减少，但他用来作为高级持续攻击者的工具如MANITSME和WEBC2 - UGX仍然出自于上海。

UG一直在各种网络帐号使用的用户名“UglyGorilla”通过许多在线交流留下了很少但有用的线索。在大多数情况下，如黑客工具，信息安全主题，和与上海当地交互的内容都使用了合理方法清除。例如，在2011年2月，由匿名泄露的所有注册“rootkit.com”的账户中包含了用户“uglygorilla”注册的电子邮件地址uglygorilla@163.com。同样的电子邮件用于注册2004年解放军论坛和域名hugesoft.org 。包括rootkit.com泄露帐户信息的IP地址58.246.255.28，明确的指向了前面讨论的高级持续攻击专家用来注册UG的帐户：58.246.0.0/15 。

在其中的几个账户，UG已经列出了比“JackWang”更适合作为他真实姓名的东西。 2006年2月2日，用户名为“uglygorilla”的用户向中国开发者网站PUDN（www.pudn.com）上传了一个名为“mailbomb_1.08.zip”（批量电子邮件工具）的文件。从他PUDN帐户的详细资料中包含了真实姓名“Wang Dong”（汪东）。

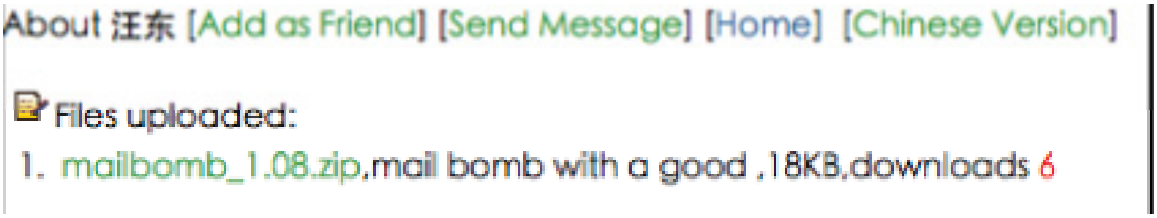


图29：汪东上传到pudn.com的文件

需要注意两个很重要的事情。首先，中国的名字以姓氏开始。所以，“Wang”在汪东名字的最后面。第二，它是中国一个相当普遍的做法，即使在中国，选择一个英文名作为首名。因此，“JackWang”可能完全不会有另一个别名。

高级持续攻击黑客（APT1）简介：DOTA

另一个APT1人物是“dota”（DOTA），他的命名表现了强烈的倾向，几乎他创建的所有用户都使用了该变体名称并且用于他攻击基础设施。DOTA可能从简称为DotA的视频游戏“远

祖防御”命名了他的名字，虽然我们还没有观察到有关此游戏的任何直接链接或其他关联。

我们监测他创建的几十个帐户，包括d0ta010@hotmail.com和dota.d013 @ gmail.com的，并且经常看到DOTA基于Web电子邮件服务创建几个连续的帐户（例如，dota.d001到dota.d015 ）。大多数情况下，这些帐户用于社会工程并在电子邮件地址订阅其他服务时进行钓鱼攻击或接触。例如，DOTA（使用APT1的IP地址58.247.26.59）在他的美国跳点使用中国简体键盘设置的电子邮件地址“d0ta001@hotmail.com”注册Facebook的用户“do.ta.5011”（Facebook的用户ID：100002184628208）。

某些服务，如谷歌的Gmail ，要求用户在注册过程中提供电话号码，用以他们发送包含验证码的验证“短信”。然后，用户必须输入验证码完成网站上的注册。在一个中间设备上观察到的会话显示DOTA使用手机号码“159-2193-7229”，以接收来自谷歌验证短信，然后他在几秒钟内提交网页。

在中国的电话号码被组织成包含一个区号，前缀，以及类似美国电话号码的行号，通过添加的区号用来分配给移动手机供应商。电话“159-2193-7229”分解成“159”区号，这表明了这个移动电话号码为中国移动，和前缀“2193”表明了上海移动号码。这意味着最起码这个号码最初是由中国移动分配给上海使用。 DOTA的应答速度也预示着他在那个时间拥有这个手机号码。

DOTA： 哈利波特的粉丝？

从特征上看DOTA可能是哈利波特的粉丝。他经常在账户的秘密问题中，如谁是你最喜欢的老师，谁是你最喜欢的童年朋友中填写“哈利”和“波特”，这些创建的账户包括：poter.spol@gmail.com,或者改变邮件地址为dota.sb005@gmail.com

我们还观察到DOTA使用的名字罗德尼和拉茨以流利的英语通过电子邮件与包括在马来西亚和菲律宾的东南亚军事组织的各种目标联系。如果这个Gmail帐户专门用于海军作战部长赋予他的使命，那这个使命还不清楚，但大部分的流量，表明其既在使用简单网络钓鱼攻击，也用以基于社会工程的更复杂的电子邮件。

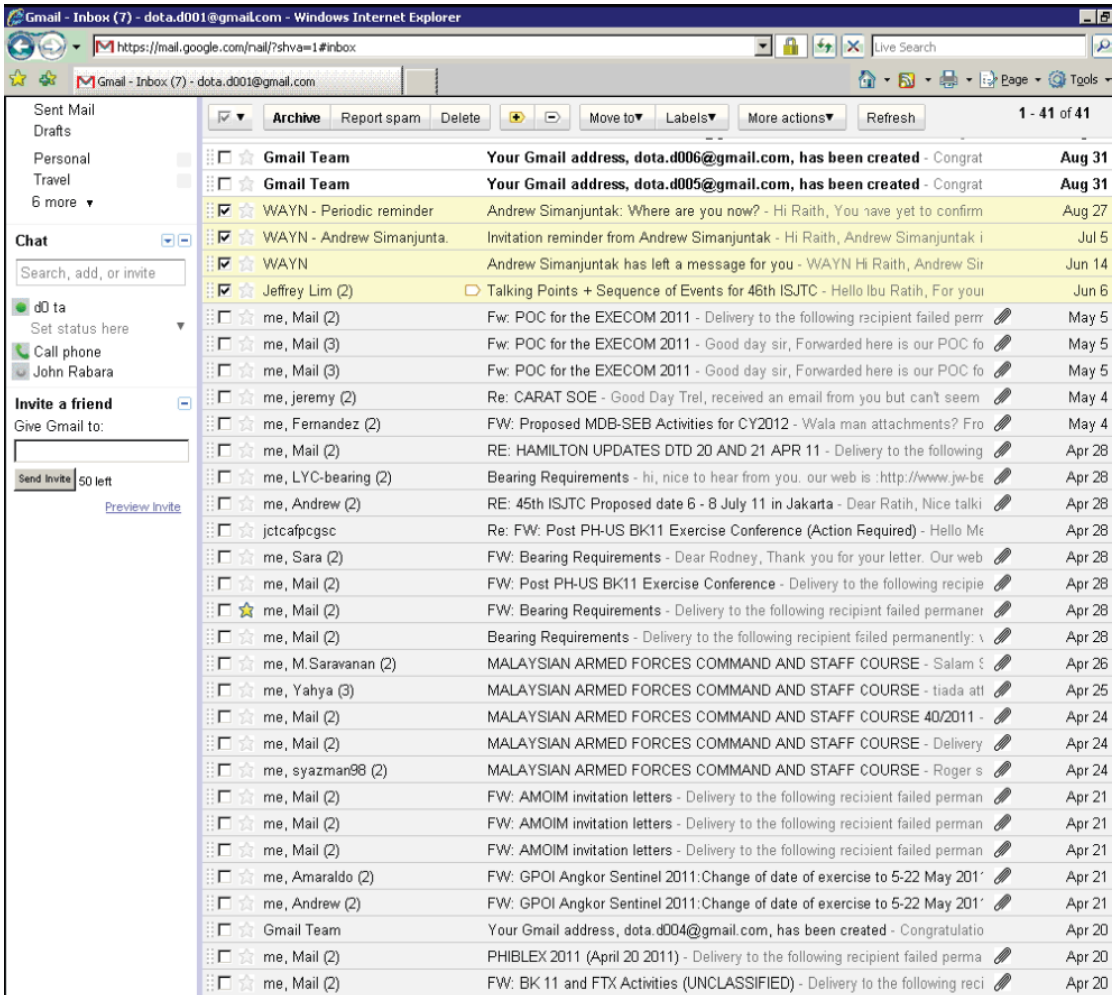


图30 ： dota.d001 @ gmail.com（收件箱视图）[41]

当在交流社区和受害者系统上创建数十个，或者数百个账户时，密码管理就成为一个重要的任务。因此，大多数APT1攻击者使用的密码，要么是基于模式的，如键盘模式“1qaz2wsx”或非常难忘的，如使用“rootkit”作为网站rootkit.com信息安全研究的密码 。像许多APT1攻击者，DOTA频繁的使用基于键盘模式作为密码，如“1qaz@WSX＃EDC”。然而，有一口令“2j3c1k” 不是基于键盘的模式被DOTA广泛使用，显然他可能不是唯一使用它的APT1执行者。编号“j”，其次是编号为“c”，然后一个编号为“k”可能缩写为（“j”/“c”/“k”）为ju/chu/ke（局/处/科）组织结构（翻译为局/处/科）被解放军总参谋部广泛使用。2049项目描述了典型的解放军的组织结构，“局级首长...监督6至14个下属点或办事处...局以下的站点/办事处进一步分成几个部分。由于这种模式，密码“2j3c1k”很可能代表一部三师二局[61398部队]，那些使用这些密码模式工作的人员隶属于第二局。

试图跟踪DOTA并追溯现实中的某一个人是困难的；他的活动线索联系不到一个现实世界的身份。然而，Mandiant已经能够建立UG和DOTA之间有明显的联系。特别是，我们观察到两个使用共享APT1基础设施，FQDNs，IP地址范围和出口。这种共享的基础设施的协调，结合他们与61398部队密切接触变得很有可能，至少，UG和DOTA互相认识，甚至可能一起工作。

APT1黑客介绍：SuperHard（Mei Qiang/梅强）

我们揭示第三个也是最后的角色称为SuperHard（SH）。SH第一次被观察到是作为一名工具作者，并且是AURIGA和BANGAT恶意软件（见附录C：恶意软件库）的创造者或者一个有效的贡献者。同样类似于UG，SH在他的很多作品中使用工具嵌入他的名字。特别是，该可执行元件（PE）文件VS_VERSIONINFO结构经常被设置为SuperHard，或者cmd.exe副本被从“Microsoft corp.”修改为“superhard corp.”。

此外，许多包含驱动模块的SH工具被设计用来装入Windows内核以颠覆系统要素。虽然不是唯一APT1编码人员，但是其经验把SH编入一个非常有能力的较小的APT1开发组。经常的，SH的工具被使用在其他APT1人物和观察到的几个实例及其他APT组织。鉴于SH的工具是由其他APT1成员们用的，并没有迹象表明SH是一个全职的操作员，我们认为SH主要为APT1进行研究和开发。

有一次，在跟踪SH时，我们幸运的可以访问公开帐户rootkit.com。该rootkit.com“SuperHard_M”帐户最初是从IP地址58.247.237.4注册，在一个已知的APT1出口范围，并使用电子邮件地址“mei_qiang_82@sohu.com”。我们观察到DOTA正在与mei_qiang_82@sohu.com用电子邮件往来。“Mei Qiang”（梅强）这个名字是一个相当常见的中文名字组合。此外，中国网民的普遍做法是在最后两位数字增加他们的出生年份，这表明SuperHard其实是梅强，出生于1982年。不幸的是，有一些1982年出生身份是“Mei Qiang”的人，让定位变得困难。

幸运的是，我们可以用SH的电子邮件地址连接一些他所注册的网站。许多这些帐户透露出细节再次证实SH和mei_qiang_82@sohu.com及APT1联系，例如SH通过写木马程序赚钱，他参与微软内核破坏研究（顺便说一句，greenfeld的评论，可能是UG），最近，他在上海的

浦东新区。

7 结论

在一个严格监控互联网使用的国家，中国政府不知道攻击来自上海浦东新区是不可能的。对APT1攻击的规模和持续性，我们都记录在本报告中。因此，最有可能的结论是，APT1能够发动这样一个长期和广泛的网络间谍活动，拥有大量技术储备，必须和政府合作才行。根据既定的任务、资源和中国人民解放军61398部队的位置，我们得出这样的结论：中国人民解放军61398部队就是APT1。

表12 APT1和解放军61398部队之间的映射。

特征	APT1（直接观察）	61398部队（据报道）
任务区	>>从英语组织窃取知识产权 >>中国十二五规划新兴产业战略性行业为目标	>>以说英语组织作为计算机网络操作的目标
工具，战术和程序（TTPs）	>>有组织的，资助的，训练有素的运营商特定靶向目标和道德规范（例如，我们没有目睹APT1破坏财产或窃取金钱，类比“黑客”及最复杂的组织犯罪集团）	>>进行军事级别的计算机网络操作
经营操作	>>至少从2006年从141个组织不断偷盗了数百百万兆字节信息；同时存在的受害者在至少20大产业 >>大量的跳点基础设施和连续的恶意软件更新表明至少有几十个操作员与上百的支持人员。	>>作为中国人民解放军的一部分，资源（人力，资金，影响）达到APT1的规模 >>根据PLA的设施及位置有上百甚至上千的人员
专业技术人员	>>英语语言水平 >>恶意软件编写 >>电脑黑客 >>确定20大产业数据值得偷的能力	>>英语语言要求 >>操作系统内核，数字信号处理，信息隐藏 >>中国科技大学招聘
位置	>> APT1职员使用上海的电话号码注册电子邮件帐户	>>总部和其他设施分布于中国上

	>>上海两到四个网块被分配到浦东新区 >>由APT1入侵者使用的系统有简体中文语言设置 >>APT1角色的身份地点是浦东新区	海浦东新区
基础设施	>>中国联通经营的四个主干网在上海（一到两个1级的互联网服务供应商） >>也有使用中国电信的IP地址（其他1级互联网服务供应商）	>>已国家安全的名义与电信公司共建的网络基础设施

根据我们直接观察和仔细的研究，我们相信事实只有两种可能性：

或者

一个秘密的、资源丰富的、其成员为讲汉语的组织，坐落在61398部队周围，能够直接访问上海的电信基础设施，多年从事企业规模的计算机间谍活动执行的任务与61398部队的相似。

或者

APT1是61398部队。

附录A　Mandiant如何辨别黑客组织

Mandiant(一家美国网络安全公司)使用“黑客组织”描述那些一起攻击和渗入到网络的入侵者。一些独立个体可能会承担同样的任务，协作并共享工具和方法。他们一起操作以获取目标并窃取数据。因此，这个群体不是由方法而是由人来定义的。

然而，仅基于已发现的攻击活动去确定一个‘黑客组织’并不是一件简单的事。在没有见到坐在键盘前的人前去决定不同入侵事件是否由同一个人指挥或是一起协作的两个人或是两个互无联系的两个人是困难的。不同组织可能会使用相同或类似的攻击方法和广泛存在于互联网上的工具(比如pwdump，HTRAN，ghost rat等)。还有这样一种可能，这些入侵事件是由两个组织使用同样的恶意程序或漏洞甚至同样的人员。那些独立行动的入侵者也许会短暂或永久的隶属于不同组织。一个入侵者也会被多个组织雇佣。最终，多个组织为达成一

致目标而协同工作。

尽管如此，通过足够的信息、分析经验及技术手段区分开不同攻击组织是有可能的。举一个现实世界的例子:比如小偷在不同作案现场留下的痕迹。不同的案件在很多细节上都是不同的：

》小偷闯入的方式；

》打开保险柜的工具；

》小偷选择窃取的东西，或者是带走所有东西希望能够得到一些有价值的东西；

》小偷也可能会很谨慎地选择他们的目标，绕过警报，试图毁灭证据(比如指纹)；或者只是小心到不被抓住。

侦探们能够分析多种犯罪现场，并通过现场留下的证据判断是这个小偷而不是另外的其他人。

同样的方法，网络入侵者也会留下数据“指纹”。他们会留下ip地址或者邮件地址。邮件中可能会包含某些线索。文件会有特定的名字，MD5值，时间戳，常用的功能和加密算法。后门会有植入的口令和控制IP或者域名。这些只是计算机侦探认为区分不同网络黑客组织的无数线索的一小部分。

数字指纹并不决定归属。他们的有效期和值只是黑客组织所填写数据的唯一性。例如像HTRAN这个被广泛使用的工具--就工具本身而言--在确定一个特定黑客组织时并不是独特的和有用的。相对而言，一个特定的常用的后门是更好的标识工具，尽管并不充分但至少有比较积极地作用。

当收集到足够充分的证据 会有合理的怀疑两起入侵事件是否是同一人或者同一组织所为。

附录B　高级持续入侵和攻击的生命周期

大部分的电脑入侵在攻击的生命周期里都会伴随着常见的、高水平的一系列的阶段，中国的APT的生命周期却有点不同，原因是他们独特的长期的目标。下面这部分对应了Mandiant的攻击生命周期模型的阶段，同时给予了关于在每个阶段中APT都应该是什么样的简单概括。在‘创建据点’和‘完成任务’之间的阶段中，不需要每次都以这样的顺序出现。实际上，一旦在进入了网络，APT组织将会持续重复不间断的控制观测，识别感兴趣的数据，通过其他方法去访问那些数据，然后已‘完成任务‘的形式最终盗取这些数据。这将会无期限的持续着，直到他们彻底离开网络。

最初的受害

最初的受害阶段就是入侵者过去常常渗入一个目标组织网络所用的一些方法。APT入侵者常常瞄准那些个人的有着上当可能性的用户。例如，大部分常见的最初的受害方式就是网络诈骗。这些网络诈骗短信可能包含了恶意的攻击，一个带有恶意文件或者网站的链接。还有少部分的情况，APT入侵者可能尝试联系潜在的受骗者，然后通过社交网站或紧急短信发送恶意的内容。另一种常用的手段就是重要的网络受害，攻击者会放置一些恶意代码在网站上，这些网站是被攻击的人经常访问的网站。当他们以往常的流程访问这些网站时，如果他们的电脑是容易被攻击者编写的代码所攻击的，那他们将会受到损害。APT组织也可能寻找易受攻击的网络和上传服务器来获得访问内部网络的入口，或者寻找有技术性漏洞的公共设施。

创建据点

创建一个据点可确保APT入侵组织能访问和控制一个或多个外部网络中受到攻击的电脑。APT组织会利用公众的后门（GHOST RAT和Poison等常见的例子），黑客网上提供的或者通过个人获得的‘潜在的’后门和他们自己发现的‘容易找到的’后门。这些后门常常能建立一个从受害网络到攻击者控制的电脑的外部连接。这种通讯方式从清晰的明文或简单的加密到更高级的加密。这些后门使得APT组织能够通过命令行界面或者图形界面来访问系统。

提升权限

提升权限可以访问更多在受害者环境中的资源。这些大部分都包含了用户名和密码，但是它也可能包含获得访问的PKI证书，VPN用户软件，授权电脑，或其他需要访问感兴趣的数据和系统的资源。APT入侵者更喜欢尽可能地越级获取特权账户，例如域管理员，有域权限的服务账户，本地管理员账户，授权用户账户。一般地通过从电脑，服务器或域控制器中输出密码hash值来完成的特权获取。攻击者可能有能力获取合法账户密码通过破解密码hash值。换句话说，在‘翻译hash值’攻击中，攻击者可以利用hash值本身，来获取到可能用于认证的密码，来替代实际的密码。许多公共的可用的工具能够轻易的被用于破解hash密码值和这种类型的攻击。

内部监测

在内部监测阶段，攻击者搜集关于受害者的信息。APT入侵者们使用嵌入式的操作系统命令（例如windows的net命名）来获取关于内部网络的信息，包括电脑、信任关系、用户和团队。为了识别感兴趣的数据，他们可能会查询目录或网络共享列表、或者通过文件扩展名、关键词或最新已修改的数据来寻找数据。感兴趣数据多以多种形式存在，但大多由文档，email账号及数据库组成。因此文件服务器，email服务器和域控制器就成了内部监测的目标。一些APT组织利用定制的脚本来自动操作监测程序和识别感兴趣数据。

横向迁移

大部分情况，入侵者最初破坏的系统并没有他们想要的数据。因此他们必须在网络里迁移到其他的既有数据又允许他们访问的电脑上。APT组织利用用户信息或使用hash翻译工具来访问受害网络的其余的电脑和设备。他们通常使用PsExec/或windows任务管理器来执行命令和在远端系统上安装恶意软件。

维持伪装

在这个阶段，入侵者要采取行动来确保从外部网络持续控制受害网络环境内的关键系统。在整个入侵期间，APT组织常常会安装新的后门程序（例如，不同于创建据点章节提到的后门程序）在网络环境中。他们可能会安装不同种类的木马在多台电脑上，使用各种各样的命令和控制地址，最大可能的冗余来使它不被轻易的识别和移除出所有访问的节点。此外，

APT组织可以建立多种网络访问的方法来避免隔离后门程序，以至于他们能维持自己的伪装，即使网络管理员发现并移除了他们的木马。这些方式可能包括使用有效的PKI或VPN认证，允许入侵者伪装为一个合法的用户来获取并访问公司网络和内部资源。在一些实例中，APT入侵者能够实现一个认证被两个人使用的情况来维持并继续访问受害网络和它的资源。

任务完成

APT攻击者最大的目标就是盗取数据，包括劳动者的财产，商业契约或协商，政策文件或内部书信。一旦APT组织在受害的电脑上找到了感兴趣的文件，他们常常会在盗取前先打包这些文件。他们大部分使用RAR工具来压缩文件，但也会使用其他公共可用的软件，例如ZIP或7-ZIP。APT参与者不仅压缩文件，而且还经常设置密码进行保护。最后他们会使用各种方法把这些文件传送出受害网络，这些方法包括FTP，用户文件传送工具或者现存的后门。

附录C　恶意软件库

此附录是电子版的，能够在http://www.mandiant.com/apt1中找到。它包括ATT1已经使用过的恶意软件的扼要介绍。

附录D　FQDNS

这附录是电子版的，和此报告一起。它包括ATP1在他们攻击中使用FQDNs

附录E　MD5 哈希

此附录是电子版的，能够在http://www.mandiant.com/apt1.找到。它包括ATP1在攻击中使用的恶意程序MD5 Hashes。在附录G:IOCs中，命名为8dd23e0a-a659-45b4-a168-67e4b00944fb.IOC包括所有的在附录中提供的MD5 Hashes，和Redline™配合使用，Mandiant免费的基于主机的调查工具，或者Mandiant的智能回复，Mandiant商业的基于主机的调查工具。

附录F　SSL认证

此附录是电子版的，能够在http://www.mandiant.com/apt1.找到。它包括APT1使用在服务器上的SSL证书，那是他们控制和管理基础设施的一部分。

附录G　IOCs

此附录中有关IOCs的部分是电子版的，能够在 http://www.mandiant.com/apt1.中找到。

APT1 指标及Redline™使用。

随着Mandiant报告的发布，APT1：解密一支中国网络间谍部队，我们在附录G中提供一系列APT1 IOCs来帮助侦查在附录C中涉及的恶意软件。Malware Arsenal.IOCs被用作侦查手段来查找未知的入侵行为或者检查已知的威胁，附录G中涉及的IOCs适合后者。无论如何，记住APT1一直在升级他们的工具，因此必定有我们用这套IOCs无法监测的变种恶意软件和新的恶意攻击族。为了找到更多的报告或者数据附录（包括下载的在附录G中提到的一系列IOCs）可以去http://www.mandiant.com/apt1。

IOCs能够结合Redline使用，它是Mandiant公司免费的基于主机的监测工具，或者和MIR一起使用，它是Mandiant公司商业的基于主机的监测工具。拥有MIR licence的Mandiant的客户可以方便将压缩的IOCs文件导入到他们的控制中心。对于那些没有MIR的，可以从Mandiant的网站http://www.mandiant.com/resources/download/redline.下载Redline。

谨记在生产的环境使用这些新的IOCs之前要先经常检测.

什么是IOCs？

为了定义和共享威胁信息，Mandiant已经通过机器码形式开发出一款开放的，可扩展的标准。基于静态特征分析，IOCs汇集了超过500种通过归类的法庭证据及逻辑分析人员，从而提供高端的入侵检测能力。

如果你对IOCs不熟悉，去公开的IOCs网站http://openioc.org.这有详细的描述。

什么是Redline

Redline是Mandiant公司的一个免费工具，它通过分析内存及文件来监测主机上的恶意行为迹象，并出具威胁评估图表。Redline有以下优势：

快速分类判别

遇到一个潜在的弱保护主机，响应者必须首先评估系统中是否有活跃的恶意程序。为了快速分析，Redline全面审计系统中所有当前运行的进程及驱动程序，而不会安装软件或破坏系统的当前状态；为了详细的分析，它也收集全部的文件结构、网络状态及系统内存。Redline会将收集到的任何MD5值与一个MD5白名单进行比较、分析。用户可以通过Redline

的时间轴功能进一步分析和查看导入的审计数据，时间轴功能包括TimeWrinkles™和TimeCrunches™功能模块，能依据给定的时间来缩小和过滤出结果。

暴露隐藏的恶意程序

Redline Portable Agent能收集并分析完整的内存映像，其工作在内核态及其他恶意程序隐藏技术操作层级之下。在物理内存级别检测时，很多隐藏技术变得非常明显，使得内存分析是一个有效地找出恶意程序的工具。它也能暴露出不保存在磁盘上的“内存模式”恶意程序。

引导分析

Mandiant公司的Redline通过提供一个成熟的基于相对优先级的恶意程序分析流程来简化内存分析。这需要猜测出任务和时间分配，允许检测人员集中处理最严重的威胁。

Redline计算出一个像知名进程更可能值得检测那样的“恶意软件风险指数”，并鼓励用户参照进行。随着用户阅读从纯净和遭入侵系统审计，他们将建立起丰富的快速识别恶意活动经验。

如果你监测一个系统，这里介绍Redline如何帮助你集中注意力在易输出问题的数据上：

审查步骤

Redline可以收集巨大的原始信息。它的审查步骤帮助提供一个起始位置，这些地方就是高亮指标的数据，可以有效的引导你辨认恶意进程。除非你有一个特别的目标，否则我们建议你沿用这些步骤，来检查不符合你预期的信息。

这个一个高效的审查者的关键在于从各种的干净及受攻击的系统产出的检查Redline数据。多次之后，随着你审查越来越多的数据，你对数据的识别力会提高的很快。

恶意软件风险指数的增长

Redline利用各种规则和技术分析了每个进程和内存部分，用于计算每个进程的“恶意软件风险指数”。该数据是一个很有帮助的指导，用于识别那些看似更值得去审查的进程。被恶意软件入侵的处于最高危险级的程序被标记为红色记号，那些有一定风险因素的标为灰色记号，低风险的进程没有颜色标记。

MRI对于恶意软件不是觉对的。在调查期间，能够通过调节每个进程的具体的点数来调整恶意软件指标的记分，通过增加自己的点数，来调整输出结果。

IOCs

Redline除了提供MRI scoring之外，还提供了IOC分析。基于提供的IOCs，Redline便携式代理自动设定去采集数据，这些数据是执行后期IOC分析所需要的；该分析运行之后，IOC的命中结果将用于进一步调查研究。

此外，redline提供了创建IOC采集器的功能。这个功能特性授予了匹配一系列IOCs的数据类型的采集方法。

使用MIR

结合使用MIR，redline成为在线应答（live response）的强大工具。一个典型的例子如下：

1. IDS或者其他系统检测到主机上的可疑活动
2. 通过MIR，侦查员启动一个远程的在线应答脚本
3. 运行在主机上的MIR代理捕捉并分析本地的内存，将XML审计信息在几分钟内传回
4. 用户能够通过MIR在redline上直接打开该审计
5. 使用redline，侦查员迅速的识别出恶意程序，并且记录下在redline上发现的IOC的法理属性
6. 采用MIR和MCIC，侦查员能够快速彻底搜索IOC，发现网络中运行的含有相同恶意软件所有其他系统。

MIR用户之前能够访问那些IOCs吗？

这些IOCs是新的！然而，这一系列指标的检测能力都已经可以供我们MIR用户使用了。虽然作为创建和测试的改进结果，IOCs可能看起来有所不同。Mandiant创建于2013年，并一直注重于充分利用入侵情报。我们计划持续完善我们入侵情报和我们IOCs的合成，这个计划是通过提高我们的知识面，完善IOC创建程序，IOC管理程序以及IOC测试来实施的。大多数的指示器，或者修改后的版本，将被集成到下一代IOC发布。

这系列IOCs的家庭代号是什么？

在这些IOCs中，我们正在使用一个新的IOC代号，称为“（FAMILY）”。Mandiant的智能入侵单元通过在二进制组中特性来追踪恶意软件（malware）。我们把那些二进制组称为“familys”。包含在这个附录中的IOCs是APT1使用的恶意软件家族成员中的代表。新的代号FAMILY暗示了IOC适用于这个整个族，而不仅仅是一个样板。

为什么这些IOCs在某种程度上和我在Mandiant见到过的其他IOCs不同？

很多情况下，我们将原本应该放在数个指标中的信息结合起来放在一个单独的指标中。此外，我们就已经删除了某一类型的IOC，因为它们在不同的附录中发布(例如FQDNs和IPs)。

此外，一些IOCs在这个场景下使用文件排序块捕捉那些不能用别的方式识别出来的变型的恶意软件。

文件排序块是什么？

通过列举文件属性查找一到两个恶意病毒是另一种侦查攻击的方法。 关于该话题的更

多信息或者更多有关其他IOC的问题见https://forums.mandiant.com.

你会更新这些IOCs吗？

如果我们收到反馈，我们将有可能对附录G中的IOCs做一些更改。如果更新这些IOCs，这些更新将在和报告相同的位置http://www.mandiant.com/apt1.

你会发布更多像这样的IOCs吗？

目前，还没有这种规模的公开发布的计划。

附录H　视频

该附录的数据，能够在http://www.mandiant.com/apt1.中找到。它包括了一个编辑过的视频，该视频演示了真实黑客会话（sessions）以及他们的入侵活动。

《美国全球监听行动纪录》全文 2014 年 05 月 26 日 17:23　新华社

新华社北京5月26日电美国全球监听行动纪录

互联网新闻研究中心　　2014年5月26日

目录

导言

2013年6月，英国、美国和中国香港媒体相继根据美国国家安全局前雇员爱德华·斯诺登提供的文件，报道了美国国家安全局代号为“棱镜”的秘密项目，内容触目惊心。中国有关部门经过了几个月的查证，发现针对中国的窃密行为的内容基本属实。

作为超级大国，美国利用自己在政治、经济、军事和技术等领域的霸权，肆无忌惮地对包括盟友在内的其他国家进行监听，这种行为的实质早已超出了“反恐”的需要，显示出其为了利益完全不讲道义的丑陋一面。这种行为悍然违反国际法，严重侵犯人权，危害全球网络安全，应当受到全世界的共同抵制和谴责。

美国对全球和中国进行秘密监听的行径包括：

——每天收集全球各地近50亿条移动电话纪录。

——窥探德国现任总理默克尔手机长达十多年。

——秘密侵入雅虎、谷歌在各国数据中心之间的主要通信网络，窃取了数以亿计的用户信息。

——多年来一直监控手机应用程序，抓取个人数据。

——针对中国进行大规模网络进攻，并把中国领导人和华为公司列为目标。

美国的监听行动，涉及到中国政府和领导人、中资企业、科研机构、普通网民、广大手机用户等等。中国坚持走和平发展道路，没有任何理由成为美国打着“反恐”旗号进行的秘

密监听的目标。

美国必须就其监听行动作出解释，必须停止这种严重侵犯人权的行为，停止在全球网络空间制造紧张和敌意。

一、美国在全球范围广泛从事秘密监听

1.美国监听世界政要

2013年底，英国《卫报》报道，包含联合国秘书长潘基文、德国总理默克尔、巴西总统罗塞夫等多达35国领导人都出现在美国国家安全局的监听名单上。

德国《明镜》周刊今年3月29日援引斯诺登提供的文件披露，美国国家安全局2009年针对122名外国领导人实施监控，并建有一个专门存放外国领导人信息的数据库，其中关于德国总理默克尔的报告就有300份。名单从“A”开始，按每人名字的首字母顺序排列，第一位是时任马来西亚总理阿卜杜拉·巴达维，默克尔排在“A”区的第九位。122人名单的最后一位是尤利娅·季莫申科，时任乌克兰总理。

德国“明镜在线”报道，联合国总部、欧盟常驻联合国代表团都在美国国家安全局的监听范围之内，监听内容涉及政治、经济、商业等领域。

美国国家安全局2012年夏季成功侵入了联合国总部的内部视频电话会议设备，并破解了加密系统。被曝光的秘密文件说，“数据传输给我们送来了联合国内部视频电话会议。”

美国《纽约时报》报道，2010年5月，当联合国安理会考虑是否要因为伊朗的核计划而制裁该国的时候，数个理事国的投票意向悬而未决。当时的美国驻联合国大使苏珊·赖斯请求美国国家安全局的协助，“以便她制定应对策略”。美国国家安全局很快起草出了监控四个理事国外交官所需的法律文件。

根据斯诺登曝光的文件，美国国家安全局已经渗透的使馆与使团名单包括巴西、保加利亚、哥伦比亚、欧盟、法国、格鲁吉亚、希腊、印度、意大利、日本、墨西哥、斯洛文尼亚、南非、韩国、委内瑞拉和越南。

除了联合国总部，欧盟和国际原子能机构的IT基础设施和服务器信息已被美国掌握。欧盟驻联合国机构变换了办公地点，搬进新的办公室后，美国仍在继续其窃听行为。

斯诺登提供给英国《卫报》的一份文件显示，美方设于英国北约克郡一处情报分支机构在2009年的20国集团峰会上监听俄罗斯时任总统梅德韦杰夫与国内的卫星通话。这次监听的时间是梅德韦杰夫与美国总统奥巴马举行会谈后数小时，两人在会谈中刚刚就建立互信达成共识。

一份日期标注为2012年6月的机密文件显示，当时还是墨西哥总统候选人的培尼亚的电子邮件曾被美国国家安全局秘密窃取，其内容包括了培尼亚准备提名的部分内阁成员等。美

国国家安全局在窃取巴西总统罗塞夫的通讯资料时，使用了一种特殊的电脑程序，可以拦截电子邮件及网络聊天的内容。

在2007年联合国气候变化大会上，澳大利亚情报机构国防情报局同美国国家安全局对印尼开展了大规模的监听活动。

2010年6月G20峰会在多伦多召开时，美国国家安全局进行了为期六天的间谍活动，美国驻加拿大使馆当时则变身为安全指挥部。

曝光文件还显示，日本与巴西、伊拉克被共同列为美国“经济稳定与影响”领域的重点监控国。此外，“最新战略科学技术”领域的重点监控对象包括俄罗斯、印度、德国、法国、韩国、以色列、新加坡、瑞典及日本；“外交政策”领域包括中国、德国、法国、俄罗斯、伊朗、朝鲜及日本等17国及联合国。

《纽约时报》总结说，美国国家安全局之所以“敌友不分地进行日常监控”，是为达成“对法德等同盟国的外交优先地位”和“对日本及巴西的经济优先地位”。

2.美国监控全球民众

美国专门监控互联网的项目非常庞大，可以监控某个目标网民的几乎所有互联网活动。英国《卫报》披露，美国情报人员利用名为“XKeyscore”的项目监控互联网活动。该项目在全球多处配备500个服务器。这家报纸评价其是美国国家安全局“最庞大”监控项目，称情报人员“可以监控某个目标网民的几乎所有互联网活动”。

斯诺登曝光的文件显示，美国国家安全局通过接入全球移动网络，每天收集全球高达近50亿份手机通话的位置纪录，并汇聚成庞大数据库。美国国家安全局大规模搜集全球手机短信息，每天收集大约20亿条。

一些美国媒体认为，美情报机构对嫌疑人相关电话进行窃听以掌握情报并非新闻，但涉及国外如此海量信息的收集相当不可思议。

据《华盛顿邮报》报道，美国国家安全局曾秘密侵入雅虎、谷歌在各国数据中心之间的主要通信网络，窃取了数以亿计的用户信息，并且保留了大量数据。通过分析这些数据，美国国家安全局可以获悉这些通讯纪录的发出者、接受者以及双方通讯的时间、地点等信息。

巴西网站Fantastico报道称，美国国家安全局采用MITM攻击方式，通过虚假的安全认证伪装成合法网站，以绕过浏览器的安全防护并截取用户数据。美国国家安全局曾通过这一方式伪装成谷歌网站成功获取用户数据。

英国《卫报》披露美国国家安全局与以色列共享原始监听数据，且可能包括美国公民的邮件和其他数据，而此前美国总统奥巴马坚称不会把监听目标锁定在美国公民身上。

2013年12月31日，德国《明镜》周刊消息称，美国国家安全局非法获取欧洲和亚洲之间

最大的海底通讯电缆网络——SEA－ME－WE－4的数据，取得大量敏感资料，并计划继续监听其他海底通讯电缆。

法国《世界报》报道称，美国国家安全局曾在2012年12月10日至2013年1月8日期间，监听法国民众7030万通电话交谈。

苹果和安卓手机操作系统在美国国家安全局内部被称作“数据资源的金矿”，美英情报部门2007年就已合作监控手机应用程序，美国国家安全局一度将这方面的预算从2.04亿美元追加到7.67亿美元。

据英国《卫报》、美国《纽约时报》报道，美国国家安全局多年来一直从移动设备应用程序(App)中抓取个人数据，包括个人用户的位置数据(基于GPS)、种族、年龄和其他个人资料。这些应用程序包括手机游戏“愤怒的小鸟”、应用程序“谷歌地图”以及“脸谱”、推特和网络相册Flickr的手机客户端。

美国国家安全局至少于2008年起，向全球近10万台计算机植入专门软件，旨在时刻监控或攻击目标计算机，即使计算机没有连接上网，美国国家安全局仍可通过无线电波入侵。

自2010年起，美国国家安全局用收集到的资料，分析部分美国公民的“社交连结，辨识他们来往对象、某个特定时间的所在地点、与谁出游等私人信息”。

美国国家安全局所有的监控行为都是暗中操作，而政府也是秘密决定放开对监控的限制，并未通过国家情报法院的审定或者公开的讨论。根据2006年美国司法部的备忘录，该部曾对滥用情报监控进行过警告。

通过一项名为“共同旅行分析”的项目，美国国家安全局在收集“目标人物”相关信息纪录基础上，通过已知“目标人物”的活动发现其未知社会联系，并在一小时内在海量信息中得出“目标人物”活动时间、地点等完整情报。与“目标人物”有过联系的人将可能成为美国国家安全局新的“目标人物”。

美国官员辩称，这一大规模监听活动是合法的，不针对美国国内民众，但事实上，被窃听者包括许多到国外旅行的美国人。美国媒体报道说，美国国家安全局于2010年和2011年进行了一项有关大规模收集美国国内移动电话位置的试验项目。

2013年4月，联合国人权理事会言论自由问题特别报告员拉卢在向联合国人权理事会提交的报告中指出，美国修订“外国情报监控修正案法”，扩大美国政府对境外非美籍人士进行监控的权力，监控内容包括任何利用美国的云服务主机进行的通信。

曝光文件显示德国、韩国、日本等多国被大规模监听，美欧国家的情报机构正在联手对互联网和电话通信展开大规模监控，严重威胁世界各国网络安全。

挪威媒体报道说，挪威也是美国“监控门”的受害者，美国国家安全局曾在2012年12月10日至2013年1月8日间监听了3300多万次在挪威本土登记注册的移动电话通话。

根据意大利《快讯》周刊的报道，英国和美国情报机构大规模窃听意大利的电话和拦截网络数据。

3.监控外国企业

美国政府攻击的商业网络不仅包括互联网，还涉及金融、交通、电力、教育等诸多关系国计民生的关键行业。

斯诺登披露的文件显示，美国国家安全局开展的大规模监听行动不仅包括世界各国领导人，还包括众多国际组织和商业领袖。

据德国《明镜》周刊报道，美国国家安全局的监视项目包括国际间的金融交易，尤其是信用卡交易。全球知名的信用卡品牌维萨公司和总部设在布鲁塞尔的环球银行金融电信协会均在其监视范围之内。

一项名为“追踪金钱”的监视项目专门关注国际上银行金融交易往来。按照美国国家安全局的事先设想，通过追踪所谓的金融往来线索，可以追查到更多的恐怖分子。其为此专门建立一个名为Tracfin的金融数据库，用以存储从各个金融机构得到的信息。2011年，这一数据库的信息量达到1.8亿条，其中84%的数据是信用卡信息，涉及用户主要分布在欧洲、中东和非洲。

此外，该数据库中还有部分信息来自欧洲的环球银行金融电信协会。美国“9·11”恐怖袭击之后，环球银行金融电信协会开始秘密向美国提供金融交易数据。2006年这一事件被媒体曝光后，欧盟要求与美国展开谈判，以保证欧洲银行数据的安全和公民隐私权。在多轮谈判后，欧盟和美国于2010年达成一项协议，允许美国通过环球银行金融电信协会系统获取欧洲银行的交易信息，用于打击恐怖主义，但美国在使用和存储这些金融信息方面必须遵守欧盟数据保护法律之下的严格规定。然而，根据斯诺登的最新爆料，美国从来没有停止过监视环球银行金融电信协会的金融交易往来信息。这意味着，在此期间美欧之间所有的谈判都只是表面功夫，没有实际作用。

2013年12月29日，德国《明镜》周刊称，美国国家安全局多年前就已攻破了主要公司开发的几乎所有安全架构，其中包括来自思科、华为、瞻博和戴尔的产品。

据媒体报道，美国还侵入了巴西国家石油公司的电脑网络。

二、美国把中国当成秘密监听的主要目标

斯诺登曝光的证据证明：中国是美国非法窃听的主要目标之一，窃听范围涵盖国家领导人、科研机构、大学、企业等等。

斯诺登向德国《明镜》周刊提供的文件表明：美国针对中国进行大规模网络进攻，并把中国领导人和华为公司列为目标。攻击的目标包括商务部、外交部、银行和电信公司等。《明

镜》周刊称，美国的监控目标还包括数位中国前任国家领导人和多个政府部门及银行。

中国的政府机构是美国窃听的重点关照对象。白宫的一位外交政策助理也曾透露，美国曾在1990年8月落成的中国驻澳大利亚新使馆的每间办公室的混凝土墙里埋设了光纤窃听器，这种细细的玻璃丝在全面安全检查中没有被发现。直到这件事在前些时候被泄露给《悉尼先驱晨报》和其他新闻媒体后，才引起中国的警觉。

美国《外交政策》杂志报道，美国国家安全局旗下设有一个“获取特定情报行动办公室”，1997年以来通过网络攻击行动获得包括有关中国情报在内的多项重要情报。

据德国《明镜》周刊报道，已被曝光的一份美国2010年的“监听世界地图”包含了世界90个国家的监控点，中国作为美国在东亚的首要监听对象，北京、上海、成都、香港及台北等城市，均在美国国家安全局重点监控目录之下。从2009年开始，美国国家安全局就开始入侵中国大陆和香港的电脑和网络系统，中国大陆和香港已有数百个目标受到监视。在香港的目标中，多数是大学、政府官员、商人和学生。

《南华早报》援引斯诺登的话说：“美国国家安全局无所不用其极，利用非法侵入中国主要电信公司等手段，窃取用户的手机数据。”

《南华早报》称斯诺登爆料：美国国家安全局还对中国顶尖高等学府清华大学的主干网络发起大规模的黑客攻击。其中2013年1月的一次攻击中，至少63部电脑和服务器被黑。报道指出，中国六大骨干网之一的“中国教育和科研计算机网”就设在清华大学，“清华的主干网络被黑，意味着数百万中国公民的网络数据可能失窃”。

《南华早报》公布的对斯诺登的采访说，美国政府正大规模入侵中国的主要电信公司，以获取数以百万计短信内容。斯诺登表示，美国监控远不止这些，“美国国家安全局做各种事情，诸如入侵中国移动电话公司，以窃取你们所有的短信数据。”

据路透社报道，美国国家安全局曾与加密技术公司美国安全服务商RSA达成了1000万美元的协议，联合在加密算法中加入漏洞后门，旨在削弱软件加密标准，辅助相关机构RSA开展大规模监控程序。RSA的中国客户包括三大电信运营商中国电信、中国移动、中国联通，中国银行、中国工商银行、中国建设银行等，以及电信设备商华为和家电制造商海尔等。

美国《华盛顿邮报》依据斯诺登提供的多份机密文件爆料说，在2012年5月之前的一年间，美国国家安全局未经授权收集、存储、获取或分发受法律保护的通信信息多达2776次。其中2012年第一季度的非法操作次数增加尤其明显。报告说，原因可能在于2012年农历春节期间美国国家安全局非法监听访美的中国公民大量通话信息。

连网络游戏都成为了美国获取情报的渠道，英国《卫报》和《纽约时报》公布了美国著名新闻调查机构“为了人民”的文件，名为“对恐怖分子利用游戏和虚拟环境的研究”。该文件显示，美英两国的情报人员假扮“玩家”，曾渗透入网络游戏《魔兽世界》、《第二生命》中，收集真正电脑游戏玩家的纪录，监视游戏玩家。而实际上，这两款游戏的中国玩家最多。

针对中国的监控无孔不入：据媒体报道，斯诺登披露了一批机密文件，这些文件显示，腾讯聊天软件QQ和中国移动的移动即时通讯应用飞信竟然也在美国国家安全局的监视范围之内。

美国《外交杂志》说，美国一直就网络攻击问题施压中国之时，却从不提及美方大范围攻击中国网络的情况。而在中方指出美方动作时，面对媒体的求证，美国政府始终拒绝公开置评。

据德国《明镜》周刊网站、《纽约时报》网站报道，美国国家安全局尤其花大力气监控全球第二大通信设备供应商华为公司。2009年初，该局启动了一项针对华为的大规模行动。华为被视为美国思科公司最大的竞争对手之一。美国国家安全局的一个特别小组成功渗透进了华为公司的计算机网络，并复制了超过1400个客户的资料和工程师使用的内部培训文件。

报道称，该局人员不但窃取了华为的电子邮件存档，还获得了个别华为产品的源代码。美国国家安全局渗入华为的深圳总部，因为该公司通过总部处理每个员工的邮件往来，所以美国人从2009年1月起就读取了该公司很大一部分员工的电子邮件——包括公司高管的邮件。

美国情报部门说，如果了解了该公司如何运行，那么未来将会得到回报。迄今为止，网络结构由西方主宰，但中国人将努力使西方的公司变得“更不重要”。那样的话，迄今由美国公司主导的互联网技术标准将被打破，中国将逐步控制网络中的信息流。

美国《纽约时报》网站3月22日称，长期以来，美国官员一直将中国电信巨头华为公司视为安全威胁，竭力阻挠该公司在美国达成商业协议，担心它会在自己的设备中植入“后门”以便让中国军方或北京支持的黑客窃取企业和政府机密。不过，机密文件表明，美国国家安全局正直接向华为的网络植入自己的“后门”。

《纽约时报》报道指出，美国国家安全局对中国的情报活动并不仅仅局限于华为。根据2013年4月斯诺登曝光的文件，去年，美国国家安全局入侵了中国两家大型移动通信网络，从而得以追踪具有战略重要性的中国军方部门。

三、美国秘密监听不择手段

“棱镜”等项目的披露，凸现了美国在互联网时代监听项目多、投入大、范围广、时间长，情报机构、政府和私营企业间在监控上“无缝合作”，其大数据处理能力使得网络监听的广度和深度极大拓展。

1.项目之多、投入之大、范围之广、时间之长，无不是世界之最。

美国情报机构设立的与互联网监控直接相关的项目近十个，涵盖互联网、电信网，不仅有语音电话，也包括各种互联网信息，主要的互联网服务商都囊括在内。

由美国国家安全局兴建的犹他州大数据中心，是目前世界上最大的数据中心，投入20

亿美元，其主要任务是通过秘密监控系统收集数据，然后由密码破译专家、数据挖掘人员、情报分析员进行深度处理后分析运用，以获取有价值的情报。

2013年8月30日《华盛顿邮报》披露的《2013财年国会预算论证》卷1——《国家情报项目摘要》显示：2013年美国情报预算翻番，高达 526亿美元；网络行动预算占43亿美元，约占8%，任务显著侧重。自2007年9月11日开始从微软搜集信息算起，直到2012年10月开始从苹果搜集 信息，此类美国情报机构与私营机构尤其是主要互联网服务提供商的监控合作，从来没有中断过，迄今已持续6年多时间。

德国《明镜》周刊报道了代号为“特等舱”的情报项目：美国、英国、澳大利亚和加拿大的驻外大使馆秘密安装了监控设备，用于截听电子通讯信息。这四个国家和新西兰共同签署了一份情报共享协议。

2.情报机构、政府、私营企业之间的秘密合作极其深入且愈演愈烈。

美国互联网主要的九大软硬件供应商都提供了很核心的技术支持，特别是微软最早与美国国家安全局合作，开放outlook、hotmail内部接 口，甚至在outlook.com的加密系统正式发布之间就已将其提供给美国情报部门。曾声称其加密技术和P2P架构无法被政府“搭线接听”的 Skype，在被微软收购后，主动为“搭线窃听”打开“后门”。微软还与情报部门合作，帮助其破解大公司编码，以便能够监控用户；微软经常在漏洞发布前告 知情报机构，使他们能够利用时间差发起远程漏洞攻击。

3.利用强大的大数据处理和运用能力大幅提升监控范围和深度。

2012年3月，奥巴马政府将大数据战略上升为最高国策，认为大数据是“未来的新石油”，将对数据的占有和控制，作为陆权、海权、空权之外的另 一种国家核心能力。而“棱镜”项目与美国大数据战略有着必然联系。美国国家安全局拥有一种名为“无边界情报员”系统，这套系统以30天为周期，可以从全球 网络系统中接收到970亿条信息，再通过比对信用卡或通讯纪录等方式，能几近真实地还原个人的实时状况。

4.美国情报机构一直致力于或明或暗地寻找其国内法律漏洞，突破法律限制，谋求从源头和根本上控制网络信息。

“9·11”事件后，美国为了弥补通信情报收集的不足，开始建立监控项目的总统授权。2001年10月4日，布什总统颁布授权备忘录，“在一定 时期内开展特定电子监控行动”。此后，总统授权中的“国内收集”甚至一度被解释为允许对国内信息包括美国境内和美国人的通信信息进行收集。其后数年间，美 国国内就这类行政命令的效力、范围和法律依据产生争议。但总体上，美国总统与国家安全局、联邦调查局、司法部等机构就针对外国目标收集信息的法律说明逐渐 趋于一致。

2006年5月24日，国外情报监视委员会彻底改变了对《爱国者法案》第215条内容的解读方式，允许联邦调查局与国家安全局分享与恐怖事件调查相关的“商业纪录”，包括电话公司的电话纪录。自此，美国政府每3个月向大型电话公司下达数据索取命令。

2012年10月，奥巴马签署一项名为《美国网络作战政策》的总统指令，要求美国国家安全和情报官员制定一份美国可以进行网络攻击的目标名单。 同时，指令规定，为实现美国在全世界的国家安全目标，美国可以动用独特的和非常规的武力，在事先不进行任何警告的情况下发动攻击。

荷兰《新鹿特丹商报》称，斯诺登披露的文件显示，美国国家安全局利用五种收集方式，在全球范围内开展情报收集行动。一份2012年的档案文件显 示，五类情报收集方式包括：第三方/联络，即由美国国家安全局国际合作伙伴提供数据，其合作伙伴包括约30多个国家；区域获取，即以80多个区域为基础的 专门收集服务行动，该行动是由美国国家安全局和中央情报局在黑色预算支持下开展的；网络入侵，该活动由美国国家安全局下属的获取特定情报行动办公室执行， 已经在全球超过5万台计算机中植入了窃取敏感信息的恶意软件，主要目标为中国、俄罗斯、巴西、埃及、印度、墨西哥、沙特阿拉伯及东欧部分地区；大型电缆，即通过20个大型电缆主要节点获取信息，这些节点大多数位于美国境内；外国卫星情报收集，即拦截外国卫星处理的数据，如英国、挪威和日本。

“棱镜”事件反映出美国以国家安全局为主的情报机构，实施互联网信息监控和信息获取的主要手段和方法有以下三种：

——从光缆获取世界范围内的数据。全球的通信流量大部分经过美国，目标数据流可以很容易流入或流经美国。美国国家安全局与国防部等机构在 2003年与美国环球电讯公司签署《网络安全协议》，此后的10年间，又与更多的电讯公司签署了类似协议。这些协议规定，电讯企业要在美国本土建立“网络 运行中心”，美国政府官员可以在发出警告半小时内进入查访。与此同时，美国的盟友英国、加拿大等也为其提供光缆监听情报。

——直接进入互联网公司的服务器和数据库获取。“棱镜”项目相继与微软、雅虎、谷歌、脸谱、PalTalk、YouTube、Skype、 AOL和苹果等9家互联网公司合作，大多数情况下，数据会通过这些公司的服务器以电子方式传输给政府，有时一些公司的服务器还会建立独立安全入口，以便于 政府由此调取信息。情报人员可以直接进入上述公司的服务器和数据库获取数据，内容包括电子邮件、即时消息、视频、照片、存储数据、语音聊天、文件传输、视 频会议、登录时间和社交网络资料等10类信息，甚至可以直接监控用户网络搜索内容。

——美国国家安全局的特别机构主动、秘密、远程入侵获取。美国国家安全局早在1997年就下设“获取特定情报行动办公室”，其主要任务是通过秘 密入侵目标计算机和电信系统、破译密码、攻破受保护目标计算机的安全系统等，窃取存储在目标计算机中的数据，然后复制目标邮件系统中的所有信息和通过的数 据流量，来获取境外目标的情报。美国国家安全局描述这一系列行动的技术术语是“计算机网络漏洞利用侦察”，其实质就是网络攻击窃密。

四、美国全球监听受到广泛批评

“棱镜”计划曝光后，引发了包括美国盟友在内的全球范围对美国的批评。德国总理默克尔表示：“我们必须信任我们的盟友和伙伴，而这种信任如今需要重新建立。”

美国国家安全局监控巴西总统罗塞夫和时为墨西哥总统候选人培尼亚·涅托的通信纪录，引发巴墨两国政府强烈不满。罗塞夫说：“巴西政府坚决要求美 国方面澄清……要求采取具体行动，彻底消除监视的可能性。”由于美方未在巴方要求时间内对监视行为作出解释，罗塞夫推迟对美国的国事访问。

巴西总统罗塞夫还谴责，美国出于“经济和战略”而非国家安全动机侵入巴西国家石油公司电脑网络。她说，美国的监视活动不是为安保或打击恐怖主义，而是为攫取经济和战略利益，“毫无疑问，巴西国家石油公司不对任何国家的安全构成威胁。”

为了绕开美国的网络监控，巴西将与欧洲之间铺设一条海底光缆。巴西政府还下令邮政局和联邦数据处理中心开发一套新的电子邮件系统，旨在防范他国的间谍行为，保障本国经济与政治安全。

2014年4月底在巴西圣保罗举行的互联网管理大会，焦点就是如何建立新的国际互联网治理秩序。一向标榜网络自由的美国尽管尽量低调，但仍不断 被“呛声”。巴西总统罗塞夫在会议上不点名地批评美国说，“(在互联网治理中)多边参与是非常重要的。所有参与国家的政府都应该得到平等的、一视同仁的对 待，而不是某一个国家比其他国家具有更大的话语权”，矛头直指美国政府对互联网监管机构的控制以及对其他国家的网络监控行为。俄罗斯尖锐地对美国进行了抨 击，指责美“一国政府独掌”国际互联网名称和编号分配公司。俄方代表说，“这一现状令国际社会十分担忧”。

美国在马来西亚进行监听的消息曝光后，马来西亚外交部致函美国驻马大使表示抗议。马来西亚总理纳吉布说，监听涉及国家主权及原则问题，马来西亚政府坚决反对美国对马来西亚进行任何形式的监听行动。

九大主要国际公民自由联盟发表联合声明，认为美国联邦政府开展的秘密情报监视项目“棱镜计划”违反国际人权公约。联合声明指出“如此庞大而无孔不入的监视行为违反了隐私权和言论自由权两项最基本的人权。”

在美国本土，批评和抗议的声音此起彼伏。美国民权联盟官员严责美国国家安全局称，该局越权监控私人讯息，侵犯“美国人民生活的每个层面”。

有美国民权组织发表声明，对美国国家安全局如此大规模收集移动电话纪录表示抗议，对如此众多美国人的行踪遭到政府跟踪表示不安。美国公民自由联合会首席技术官克里斯·索格恩说：“在这种情形下，保护隐私权的唯一办法是切断所有现代通信手段，生活在一个山洞中。”

针对美国的全球监听行动，第68届联合国大会通过“数字时代的隐私权”决议，强调非法或任意监控、截取通信、非法搜集个人数据是对隐私权和言论 自由的侵犯。一些国家在决议通过前发言，指责美国不仅侵犯隐私权等基本人权，也违背了尊重国家主权和领土完整、不干涉内政等《联合国宪章》宗旨和原则。

美国国家安全局监控华为的行动曝光后，华为在美国的一位高管威廉·普卢默说，华为不知道自己成为美国国家安全局的目标，“讽刺的是，他们对我们所做的，恰恰是他们一直指控中国方面通过我们所做的。”

“华盛顿正在失去其道德”，德国《焦点》周刊引述外交政策专家的评论称，“多年来美国一直以‘中国间谍和黑客攻击’为由向中国施压。而实际上， 美国自己才是窃听者。”德国新闻电视台称，美国几乎在全方位监听“整个中国”，“说到底，这是因为美国害怕中国超越自己成为世界超级大国。”

斯诺登表示，美国政府“宣称(监视行动)不会针对民间设施”。“棱镜”项目曝光，目的就是揭露美国政府的“伪善”。(完)