AhnLab

安全月刊

Vol. 26

2014 年 APT 攻击手法解析

2014年安全威胁报告

APT攻击手法解析

如今高级持续性威胁(Advanced Persistent Threat)已不再是新种威胁，全世界大多数的安全入侵事件的中心总是会有APT攻击。AhnLab 曾在“2014年网络安全预测”中也提到了APT攻击将会越来越高级化，不仅针对特定目标的APT攻击将继续，而且攻击范围也不断扩大。实际在今年连续发生了APT攻击事件，尤其在发生了多起攻击金融机关窃取重要金融信息的事件频繁发生。
本刊通过实际发生的案例，解析攻击的流入路径、攻击手法，还有最近的APT攻击趋势。

高级持续性威胁通常被称为APT。APT攻击特征是，黑客针对特定对象采用多样的攻击手法发动持续的网络攻击和侵袭行为，最终目的是窃取重要信息。黑客首先收集对象的信息，然后入侵到内部，最终窃取机密情报。最近出现了利用目标组织使用的应用程序漏洞的APT攻击。除此之外，最近APT攻击主要特征如下所示：

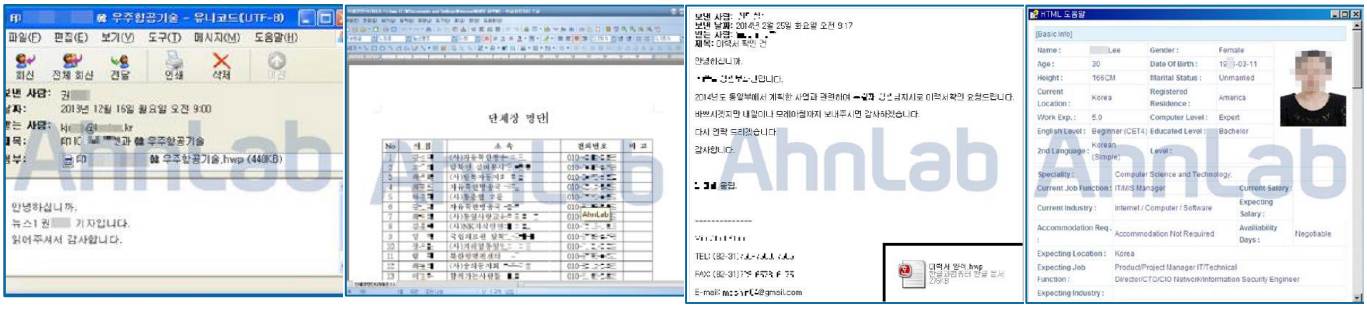
- 通过外部的更新服务器或第三方产品入侵到内部网络
- 利用鱼叉式网络钓鱼(Spear Phishing)和水坑式攻击(Watering-Hole)的入侵
- 为了持续感染以提高生存率，采用了高级的躲避技术和使安全软件失灵的技术
- 国际网络产业间谍组织的活动
- 运营可处理多国语言的攻击人力资源

APT Scene #1: 攻击点

1. 鱼叉式网络钓鱼(Spear Phishing)

鱼叉式网络钓鱼(spear phishing)是面向特定组织的欺诈行为，目的是不通过授权访问机密数据。和用于常规钓鱼(phishing)活动的电邮信息一样，鱼叉式网络钓鱼信息看上去来源可靠。钓鱼信息通常看上去是来自广泛群众基础的大型知名公司或网站，比如易趣或贝宝(PayPal)。但是在鱼叉式网络钓鱼事件中，电子邮件的显示来源可能是接收人公司内部的个人，且通常是地位比较高的人。[1]
发送欺诈性电子邮件的攻击方式不是新的方式，而是很传统的方式。问题是该攻击方式还是很有效。针对与此，安全专家们指出：“最大的安全漏洞是人”。

[1] http://www.searchsecurity.com.cn/whatis/word_5846.htm



【图 1】鱼叉式网络钓鱼的电子邮件中附上的恶意文件事例

应用程序	漏洞
Microsoft Word	CVE-2014-1761 CVE-2012-1856 CVE-2013-0633 CVE-2011-1980 CVE-2013-1331 CVE-2012-0158
Microsoft PowerPoint	CVE-2014-4114
Adobe PDF	CVE-2014-4148 CVE-2011-2462 CVE-2013-0640 CVE-2013-2729 CVE-2010-0118

【表 1】通过电子邮件传播恶意代码时主要利用的漏洞

2. 水坑式攻击(Watering-Hole)

这种攻击行为类似《动物世界》纪录片中的一种情节：捕食者埋伏在水里或者水坑(Watering-Hole)周围，等其他动物前来喝水时发起攻击猎取食物，也是一个“针对性攻击”的一种。攻击者通过分析被攻击者的网络活动规律，寻找被攻击者经常访问的网站的漏洞，先攻下该网站并植入攻击代码，等待被攻击者来访时实施攻击。

应用程序	漏洞
Internet Explorer(IE)	CVE-2012-4792 CVE-2013-3163 CVE-2012-4969 CVE-2013-3897 CVE-2013-1347 CVE-2014-0322
Java	CVE-2012-0507 CVE-2013-2460 CVE-2013-1488 CVE-2013-2465 CVE-2013-2423 CVE-2010-0118
SWF (Flash Player)	CVE-2011-2110 CVE-2014-0497 CVE-2012-1535 CVE-2014-0515 CVE-2013-0634
PDF (Acrobat Reader)	CVE-2013-3346
Silverlight	CVE-2013-0074

【表 2】通过Web传播恶意代码时主要利用的漏洞

【表 2】所示的是通过网站漏洞传播恶意代码的攻击，与此相关的主要网络自动化攻击工具(Web Exploit Kit)事例如下：

- 利用IE零日漏洞(CVE-2014-0322)传播恶意代码
- 利用IE漏洞(CVE-2012-1889)传播恶意代码

- 2014年4月出现新的网络自动化攻击工具“RIG漏洞利用工具(RIG Exploit Kit)” : 利用CVE-2012-0507、CVE-2013-2465、CVE-2013-0634、CVE-2013-0074等Java、SilverLight、Flash Play等多样的应用程序漏洞攻击代码
- 在“GongDa漏洞利用工具(GongDa Exploit Kit)”中增加了新的IE漏洞(CVE-2014-6332)攻击代码

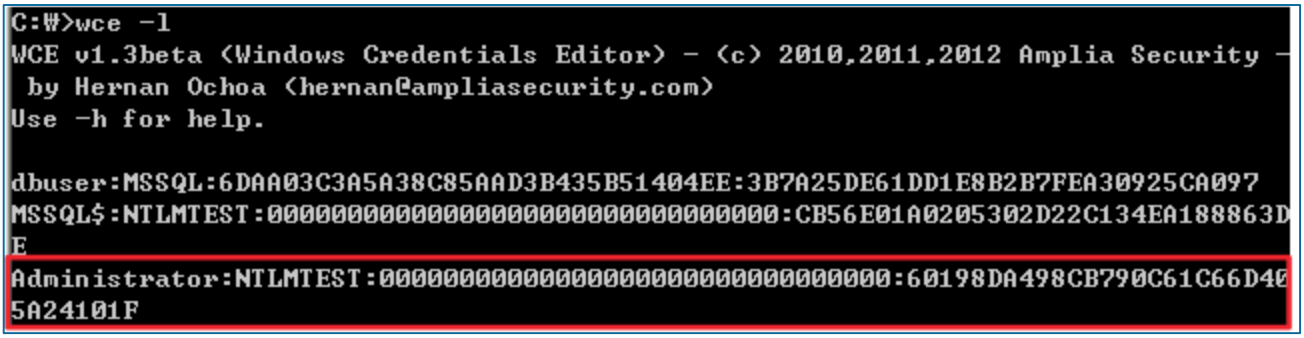
另外，还有利用如下多样的网络自动化攻击工具(Web Exploit Kit)入侵企业内部的事例：

- Red Kit (利用CVE-2010-0188, CVE-2012-0422, CVE-2012-1723, CVE-2013-2423等漏洞)
- Chinese Kit (利用CVE-2013-3897, CVE-2012-4681, CVE-2013-0422等漏洞)
- Sweet Orange Exploit Kit
- Angler Exploit Kit (利用CVE-2013-7331等漏洞)
- Fiesta Exploit Kit (利用CVE-2013-2729, CVE-2010-0188等漏洞)

最近除了利用常用的应用程序漏洞的攻击，还出现了利用企业系统中运行的特定应用程序漏洞的攻击。尤其出现了分析企业使用的应用程序更新体系和完整性检查过程的漏洞后，将恶意代码替换成更新文件的攻击方式。这种攻击方式非常智能，并且可以迅速感染企业内部的所有系统。

APT Scene #2: 攻击的内部扩散(Lateral Movement)

攻击者一旦成功入侵企业内部网络，便企图进入目标系统。此过程被称作“横向移动(Lateral Movement)”，这种移动需要授权帐户的验证信息，如“管理员ID”、“密码”和“NTLM哈希(Hash)”等。这些帐户验证信息可在系统注册表和内存中获得。此时，大部分的攻击者主要使用“gsecdump”，“WCE(Windows Credential Editor)”，“mimikatz”等攻击工具，或者将“wceaux.dll”，“sekuralsa.dll”等DLL植入到恶意代码。另外，还有使用后门程序(Backdoor)本身的键盘记录功能获得ID和密码。

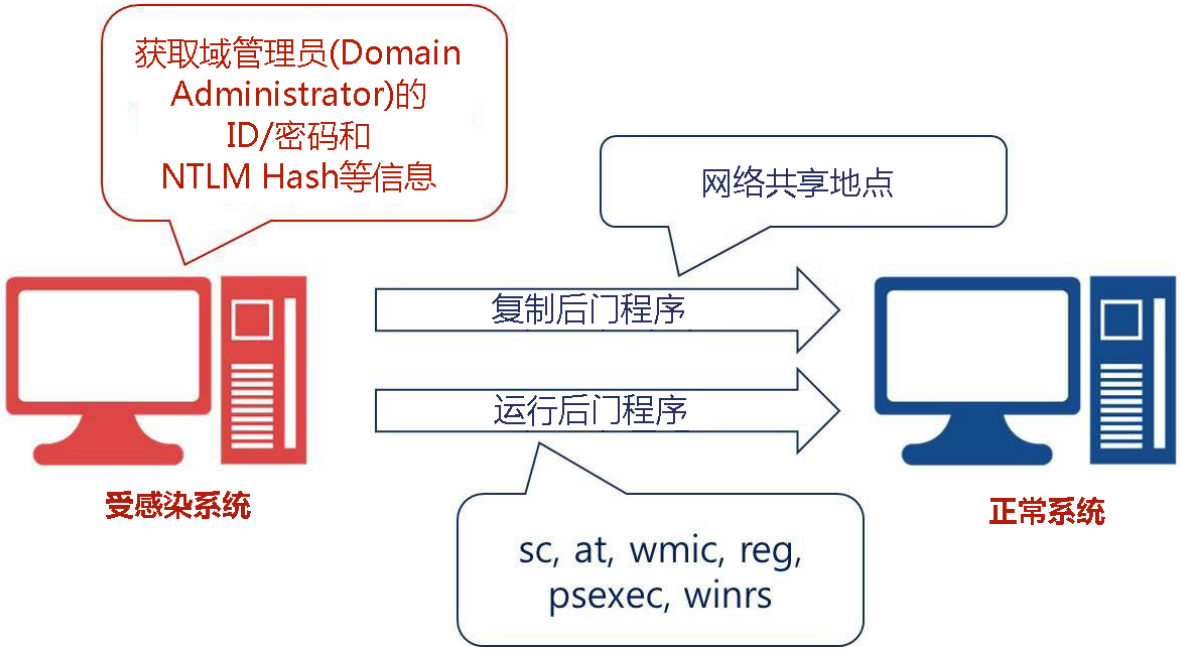


【图 2】通过WCE获取域管理员的NTLM哈希值

这种攻击可行的原因在于大部分的企业为了管理方便，企业内系统的管理员都使用相同的ID和密码。另外，在活动目录(Active Directory)环境下，如果使用域管理员帐户ID和密码访问多个系统的话，内存的域管理员帐户ID和密码的哈希值将被记录。

如此获得管理员帐户认证信息后，攻击者利用该信息入侵系统及安装后门程序。如果此时获得的帐户是域管理员帐户的话，不仅在该域的所有系统，还可在与该域依靠关系的所有域的系统安装后门程序。安装后门程序的过程如下：
首先利用获得的ID和密码或者NTLM哈希值与目标系统建立网络共享后复制后门程序。接着，登记远程服务或者任务计划运行复制的后门程序，然后以系统权限操作。运行的后门程序通过代理中继与C&C(Command and Control)服务器的连接，使攻击者可以访问该系统。

攻击者反复这种行为来寻找自己想要的数据库等系统。通常是在业务网络寻找管理员的系统，通过该系统访问网关服务器，然后入侵到服务器网络带宽。此后，如前面所述，在服务器网络带宽里的所有服务器中安装后门程序。



【图 3】攻击内部扩散过程

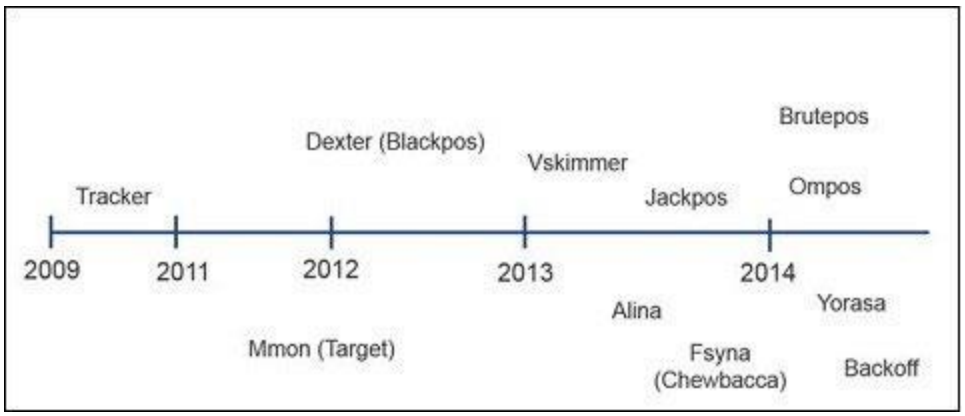
APT Scene #3: 攻击零售产业

今年1月17日，美国联邦调查局(FBI)向多家零售企业发布了报告，题目为《最近指向零售企业的网络入侵事件(Recent Cyber Intrusion Events Directed Toward Retail Firms)》。FBI警告美国零售业者做好迎接更多网络攻击的准备。FBI发现，2013年有大约20起网络攻击事件发生，均涉及相同类型的恶意软件。报告描述了这种恶意软件感染POS机系统所造成的风险。报告称，尽管执法部门和网络安全公司采取措施减少其影响，但相信针对POS系统的网络攻击事件近期内将持续增长。这种恶意软件可以在地下经济市场中获得，而且该软件价格不高，而从美国零售业POS系统所能获得的潜在收益却很大，这使得这种基于经济目的的网络犯罪对很多人都颇具吸引力。

最近美国连续发生了针对主要零售企业的网络攻击。利用恶意软件感染POS系统的具有代表性的入侵事件如下：

- 尼曼马库斯百货公司(Neiman Marcus Group)110万个信用卡数据被盗
- 塔吉特公司(Target)4000万个信用卡与借记卡数据外泄
- 家得宝(Home Depot)5600万个信用卡数据被盗

以2009年的塔吉特公司的信用卡数据被盗事件为首，大局发生针对POS系统的多样的恶意软件是从2013年起。有关针对POS系统的多样的恶意软件，我们曾在今年的9月号中详细说明。

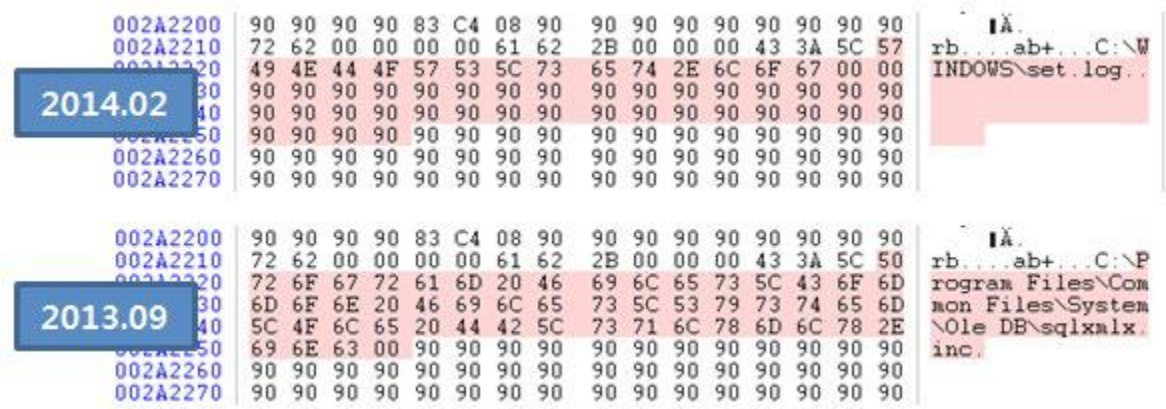


【图 4】2009年~2014年发现的主要针对POS系统的恶意软件

APT Scene #4: 不会消失的威胁

■ Kimsuky

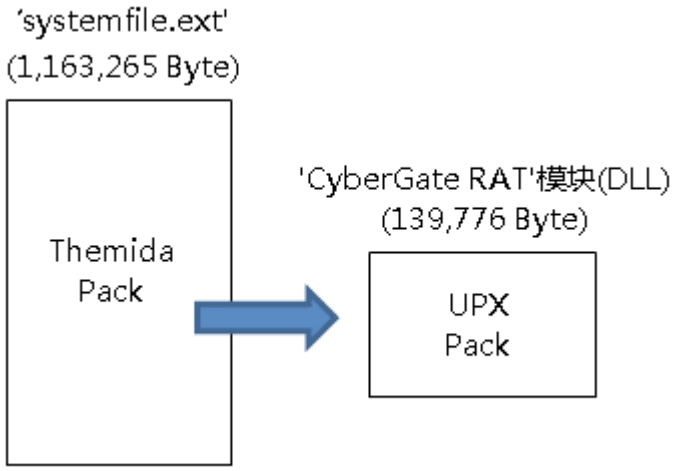
2013年针对政府及主要机关的被称为“Kimsuky Operation”的APT攻击中使用的恶意软件在2014年2月25日再次登场。2月25日和3月19日发现的这种恶意软件这次也不例外，首先通过存在漏洞的Hangul[2]文档（HWP格式）感染。



【图 5】比较2014年和2013年Kimsuky恶意软件“Team Viewer”

■ CyberGate RAT

2014年3月，再次发生了由“CyberGate RAT”恶意软件引起的感染事件。2013年6月发现的恶意软件是利用Hcell[3]文档存在的漏洞来安装的，但是这次发现的恶意软件利用了广告软件伪装成多样的正常文件的后安装。尤其此次发现的攻击不是针对特定机关的APT攻击形式，而是针对不特定多数的普通网民对象传播。由此可以推测，这可能是企图寻找新的攻击目标。



【图 6】恶意代码内部的远程控制‘Cyber RAT’模块

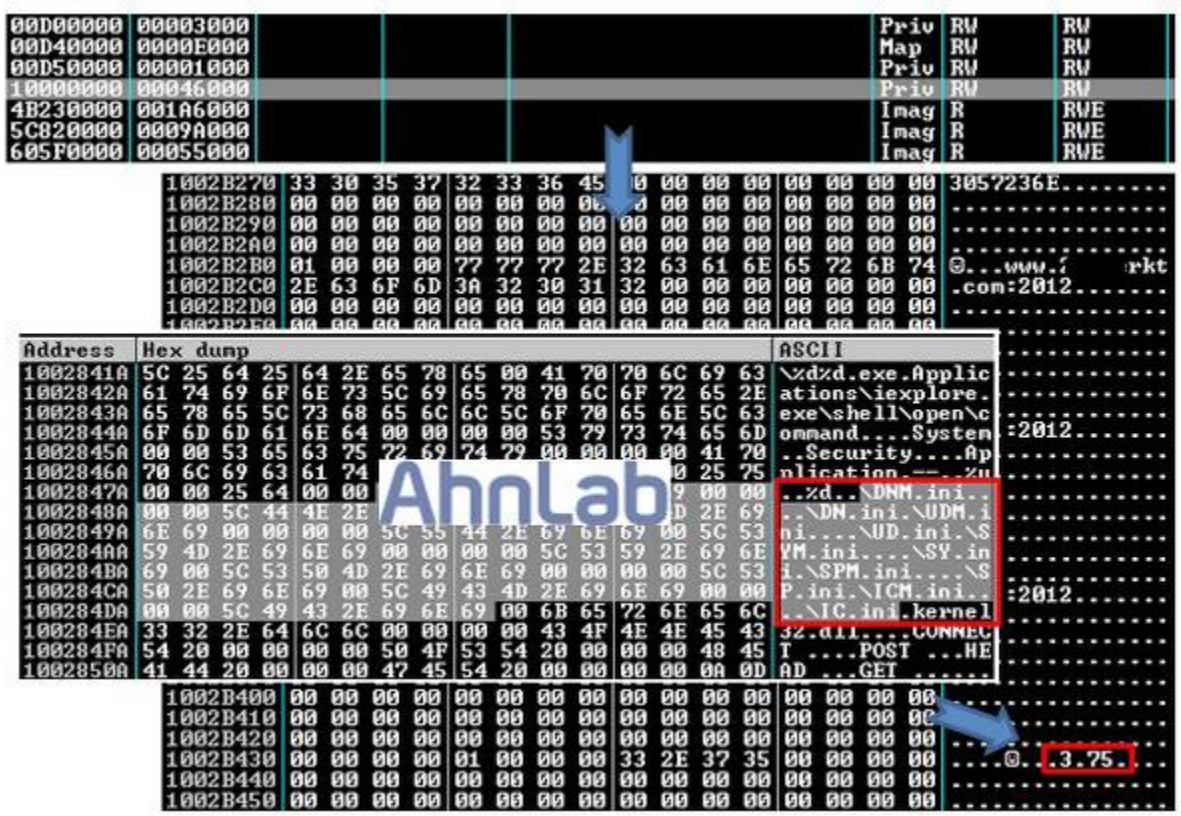
■ Gh0st

当用户利用网上银行时，黑客通常利用恶意软件篡改用户系统的主机文件。但最近发现这种恶意软件中植入了可以执行DDoS攻击的“Gh0st”远程控制工具。可以推测，黑客除了盗取用户的金融信息的目的之外，企图形成僵尸网络进行网络攻击。如此，以往在APT攻击主要利用的恶意软件，以不特定的多数的个人用户为对象发起攻击的事件持续发生。这就更加需要用户提高警惕。

---

[2] Hangul是类似MS word的办公软件，也是韩国应用最广泛的办公软件，在日常生活中的使用率要远远超过韩文版的Office。

[3] Hcell是类似MS Excel的韩国办公软件。



【图 7】Gh0st 3.75 版本的远程控制模块

APT Scene #5: CME共同作战以消灭恶意代码

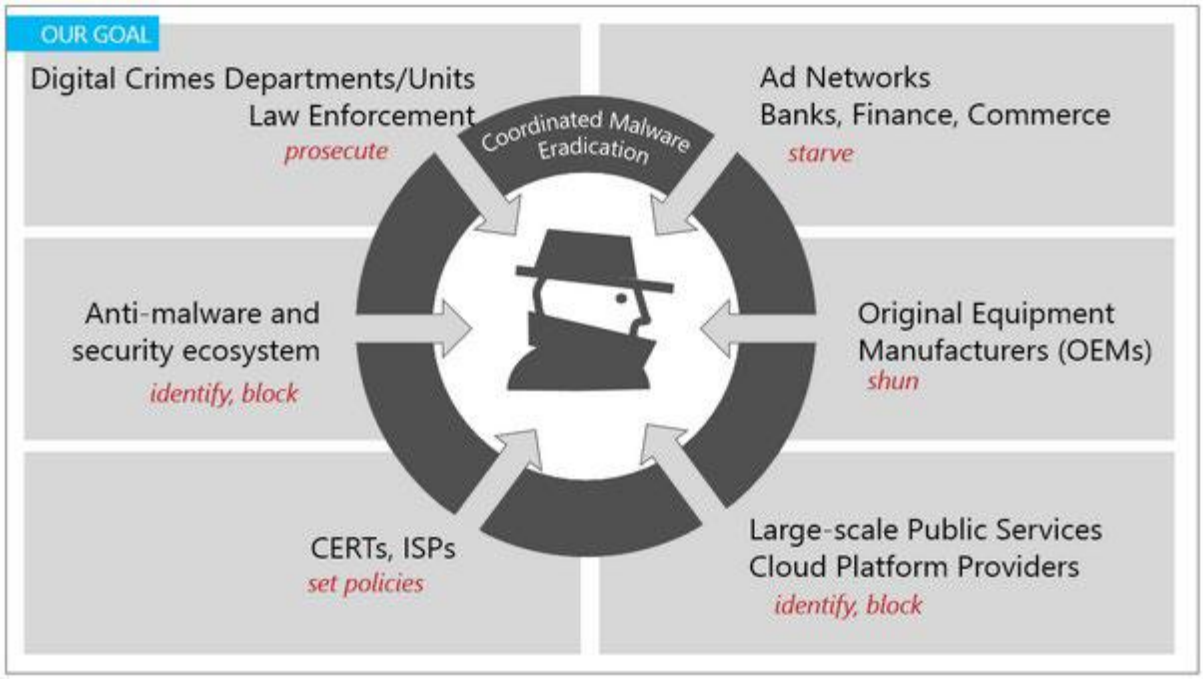
通过APT攻击事例，可以整理如下的最近APT攻击特征：

- 国际大型网络犯罪•产业间谍集团
- 国家之间的网络间谍(Cyber espionage)局面深化
- 针对主要国家的政府机关、国防部、研究机关、通信公司和能源公司的攻击
- 为了网络间谍之战，开发和利用严格受训的集团和攻击工具
- 鱼叉式网络钓鱼(Spear Phising)、水坑式攻击(Watering-Hole)和Rootkit, Bootkit等善于隐身，还拥有对通用操作系统(Windows、Mac、Unix、Linux等)的高级攻击技术
- 为了减少C&C服务器的曝光，将服务器位于内部网络，或者不直接连接通过代理控制恶意软件等周密的网络技术
- 经过长时间进出目标的网络，隐秘地掌握网络，持续盗取主要机密数据

如此，我们面对的网络攻击主犯已不再是单纯的窃贼水准。这不仅关系到个人和企业的安全，这也是与国家安保直接相关的问题。随着网络攻击组发展成国际规模，只有通过有机协同合作的响应才是唯一防御APT攻击的战略。

最近由网络安全提供商组成的“国际安全联盟”的响应APT攻击的事件引发关注。该事件又叫SMN作战(SMN Operation)，参与CME(Coordinated Malware Eradication)活动的主要网络安全提供商通过高效协作，在全世界4万3000多台的计算机中除去了Axiom[4]威胁组织植入的恶意软件。

[4] Axiom小组，根据美国网络安全联盟2014年10月28日发布报告称：它如今代表中国黑客顶尖水平，是一个更大网络间谍组织的分支机构，诺沃塔公司甚至认为，中国情报机构是“Axiom”小组的幕后主使。(来自：百度百科)



【图 8】CME 概念图

APT Scene #6: APT之战，永无止日！

在技术日新月异的今天，网络攻防永无止日。技术的发展使得APT攻击形态不断变化，并衍生出不少新的攻击方法。面对有组织、有计划、周密且持续、时而跨国的APT攻击，企业应该如何应对才有效防御APT攻击？
尽管很多全球化企业在安全控管上投入了庞大的资源，但是APT攻击仍然渗透到这些企业，并使一些企业遭遇了重大损失。这些事件向我们警示了APT攻击的高级化与复杂性，仅仅依靠个别的解决方案难以有效防御这些新型的威胁。并且，企业业务环境也越来越复杂多变不亚于IT技术，这就需要企业根据所属产业群的特性为基础，设定安全的优先级然后联系有效的安全技术和解决方案。

AhnLab基于世界领先的网络安全技术提供专门检测和响应APT攻击的下一代安全威胁响应解决方案-AhnLab MDS。AhnLab MDS具备了动态分析技术(Dynamic Content Analysis)和Anti-exploit技术，可以预防利用文件漏洞的攻击和迂回安全解决方案检测的最新的安全威胁。此外，AhnLab还结合多数客户经验的安全威胁和响应时积累的数据•信息，提供优化于每个产业群的特性和要求的安全，即安全情报(Security Intelligence)。 具体努力实现如下的威胁响应体系：▲通过与客户的双向交换数据，实时收集和分析威胁信息并再传送有意义的“信息”； ▲通过端点和解决方案的联系，实现了实际的响应；▲通过企业内部各部门和网络安全部门之间的有机联系，提示响应模型。

http:// cn.ahnlab.com

http://global.ahnlab.com

http://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。

AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室

电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | v3site@ahn.com.cn

© 2014 AhnLab, Inc. All rights reserved.