A²PT与“准APT”事件中的攻击武器

安天实验室

2015-07-23

（中国互联网大会）

智者安天下

汇报提纲

Table of Contents

APT这个概念是何时产生的？是谁发明的？

APT概念的溯源和再说明

APT不是一个新概念了

“APT”一词最初起源于2005-2006年间在空军工作的网络安全工程师们对于一些安全事件的描述，他们创造了这个词以使公众不对此类安全事件小题大做……

——Peter Cap在Bruce Blog上的留言

Bruce Schneier

Schneier on Security

A blog covering security and security technology.

« Unlocking any iPad2 using a Smart Cover | Main | Commentary on Strong Passwords »

November 9, 2011

Advanced Persistent Threat (APT)

It's taken me a few years, but I've come around to this buzzword. It highlights an important characteristic of a particular sort of Internet attacker.

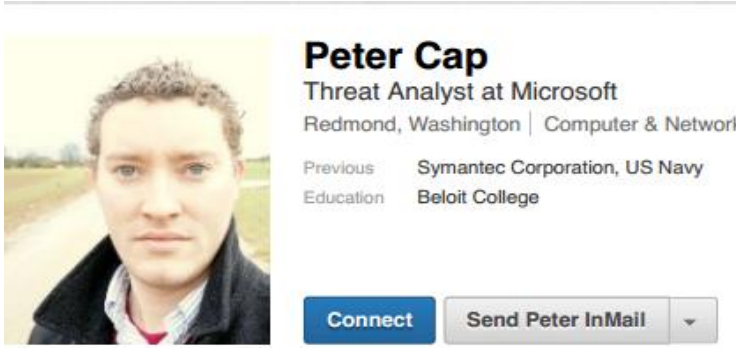
A conventional hacker or criminal isn't interested in any particular target. He wants a thousand credit card numbers for fraud, or to break into an account and turn it into a zombie, or whatever. Security against this sort of attacker is relative; as long as you're more secure than almost everyone else, the attackers will go after other people, not you. An APT is different; it's an attacker who -- for whatever reason -- wants to attack you. Against this sort of attacker, the absolute level of your security is what's important. It doesn't matter how secure you are compared to your peers; all that matters is whether you're secure enough to keep him out.

APT attackers are more highly motivated. They're likely to be better skilled, better funded, and more patient. They're likely to try several different avenues of attack. And they're much more likely to succeed.

This is why APT is a[illegible] buzzw[illegible]

Subscribe

Subscribe via Kindle



Peter Cap

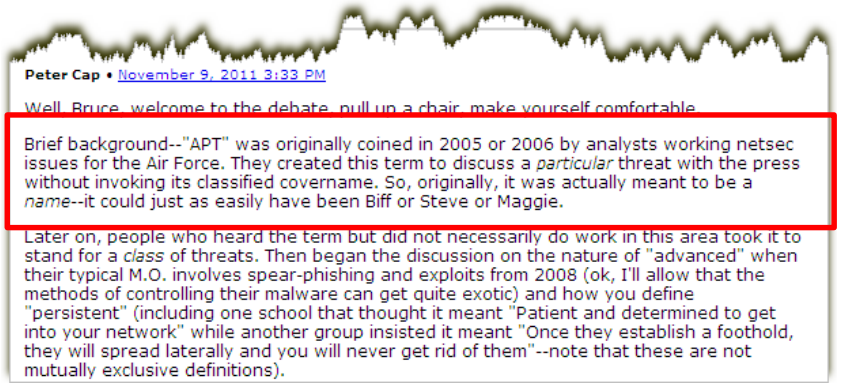
Threat Analyst at Microsoft

Redmond, Washington | Computer & Network Security

Previous Symantec Corporation, US Navy

Education Beloit College

Connect | Send Peter InMail



Peter Cap • November 9, 2011 3:33 PM

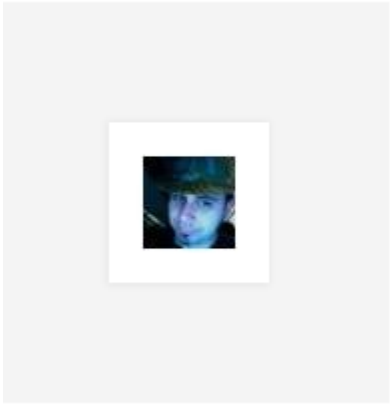
Well, Bruce, welcome to the debate, pull up a chair, make yourself comfortable.

Brief background--"APT" was originally coined in 2005 or 2006 by analysts working netsec issues for the Air Force. They created this term to discuss a *particular* threat with the press without invoking its classified covername. So, originally, it was actually meant to be a *name*--it could just as easily have been Biff or Steve or Maggie.

Later on, people who heard the term but did not necessarily do work in this area took it to stand for a *class* of threats. Then began the discussion on the nature of "advanced" when their typical M.O. involves spear-phishing and exploits from 2008 (ok, I'll allow that the methods of controlling their malware can get quite exotic) and how you define "persistent" (including one school that thought it meant "Patient and determined to get into your network" while another group insisted it meant "Once they establish a foothold, they will spread laterally and you will never get rid of them"--note that these are not mutually exclusive definitions).

参考资料：https://www.schneier.com/blog/archives/2011/11/advanced_persis.html

APT的起源



Michael Cloppert

CIRT Chief Research Analyst at DoD Contractor

美国 华盛顿都会区 | 计算机和网络安全

目前就职 DoD Contractor

曾经就职 US DoD Contractor, USAID, Fifth Third Bank

教育背景 The George Washington University

向Michael发送 InMail

286 位联系人

高级持续威胁一词的起源

美国空军被誉为*高级持续威胁*这一词汇的创造者。Mike Cloppert 告诉洛克希德马丁公司：“我第一次听到这个词是在 2006 年。美国空军第八航空队在一个小会议室使用了这个词汇。我认为他们将这一词汇用于任何从事信息战以支撑长期战略目标的复杂的对手。”

Origins of the Term

The US Air Force is generally credited with coining the phrase Advanced Persistent Threat. Mike Cloppert with Lockheed Martin said, “I first heard this term used by the USAF’s 8th Air Force in a small meeting room in 2006… I give them credit for coining this term, which is any sophisticated adversary engaged in information warfare in support of long-term strategic goals.”

APT的起源：谁最初创造了“APT”一词

Greg Rattray

Managing Director, JP Morgan Chase

New York, New York | 计算机和网络安全

目前就职	JP Morgan Chase
曾经就职	Delta Risk LLC, Finanical Services Roundtable, ICANN
教育背景	Fletcher School of Law and Diplomacy, Tufts University

工作经历：

Managing Director 摩根大通总经理
JP Morgan Chase
2014 年 6 月 – 至今 (1 年 2 个月) | 美国 大纽约地区

Founding Partner Delta Risk创始合伙人
Delta Risk LLC
2007 年 9 月 – 2014 年 6 月 (6 年 10 个月) | Washington DC and San Antonio

Senior Vice President for Security 金融服务圆桌会议安全高级副总裁
Finanical Services Roundtable
2010 年 9 月 – 2011 年 12 月 (1 年 4 个月) | Washington DC

Chief Security Advisor ICANN首席安全顾问
ICANN
2007 – 2010 (3 年)

Commander 美国空军信息战中心业务组指挥官
Operations Group USAF Information Warfare Center
2005 – 2007 (2 年)

Director for Cyber Security 白宫国家安全委员会网络安全主管
National Security Council White House
2002 – 2005 (3 年)

Commander 凯利空军基地23期信息作战中队指挥官
23d Information Operations Squadron, Kelly AFB, TX
2000 – 2003 (3 年)

起源追溯：

APT的第一个标志是来自于专为敏感信息泄露设计的有针对性的、社会工程的电子邮件投放木马，并于2005年被英国和美国组织判定。虽然没有使用 “APT” 这个名字，但是攻击者符合定性其为APT的标准。**2006年，“高级持续性威胁”被美国空军上校Greg Rattray引入。**

The first signs of APTs came from targeted, socially-engineered emails dropping Trojans designed for exfiltration of sensitive information. They were identified by UK and US CIRT organizations in 2005. Although the name "APT" was not used, the attackers met the criteria that determines an APT. **The term "advanced persistent threat" is cited as originating from the Air Force in 2006 with Colonel Greg Rattray.**

关于APT背景的再探讨

APT**不是一个新概念**

（since2006->9年）

A

B

与APT同期的一些**关联概念**：

- AET(Advanced Evasion Techniques)，技术方法
- Specialized Threat，有沿革性的领域

APT热度有深厚的

政经背景

C

为什么有人，震网不是APT，说我们所熟悉的APT

APT->A²PT中的装备与能量

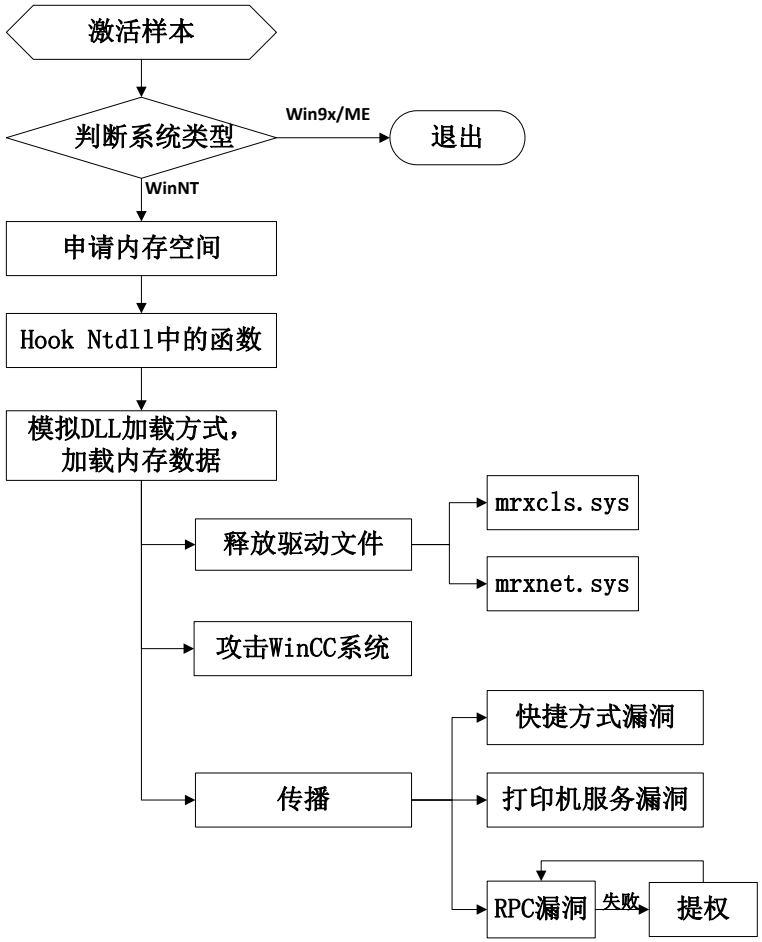
Michael 观点：Stuxnet不是APT

原文: The level of sophistication of Stuxnet is by every account very high. The code is relatively difficult to reverse engineer, contains a PLC rootkit, multiple zero-day exploits, and code that can run on processors with different chipsets. More often than not, the binaries in APT intrusions are relatively straightforward, and exploit a single vulnerability most often in client applications. This enables the adversary to "hide in plain sight" without triggering any heuristic attention through various code obfuscation and file hiding techniques that tend to leave unusual artifacts. After all, with a small target space, the likelihood of discovery is low, and analytical economies of scale will not apply for APT intrusions, meaning survivability against RE efforts is less important to build in. ↵

译文： Stuxnet 蠕虫的复杂程度非常之高。其代码难以进行逆向工程，包含一个 PLC（可编程逻辑控制器）rootkit 和多个零日漏洞，而且代码可以在具备不同芯片组的处理器上运行。很多时候，APT 攻击中的二进制文件相对简单，在客户端应用程序中通常利用单个漏洞。这使得攻击者利用不同的代码混淆和文件隐藏技术，能够“隐藏在众目睽睽下”，而不会触发任何启发式的关注。毕竟，目标空间很小，被发现的可能性也很小，而且规模分析经济体将不适用于 APT 攻击，这意味着针对 RE 响应的生存能力并不那么重要。↵

来源：摘自<Why Stuxnet Isn‘t APT>，http://digital-forensics.sans.org/blog/2011/03/24/digital-forensics-stuxnet-apt

A²PT：近乎挥霍的0day资源



MS08-067

- RPC远程执行漏洞

MS10-046

- 快捷方式文件解析漏洞

MS10-061

- 打印机后台程序服务漏洞

MS10-073

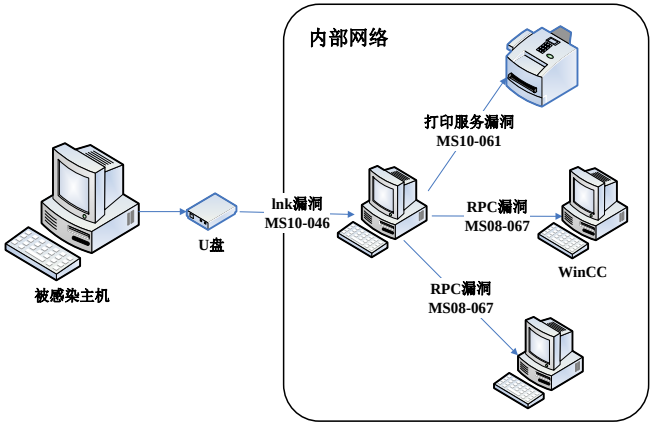
- 内核模式驱动程序漏洞

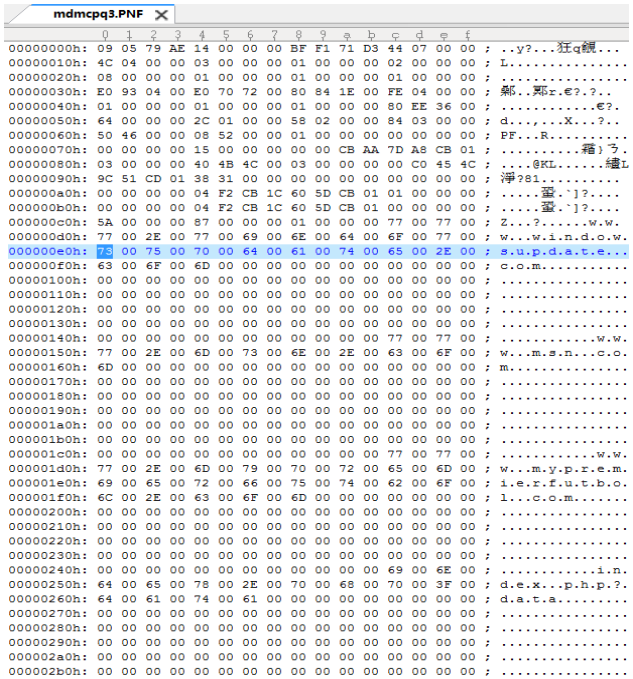
MS10-092

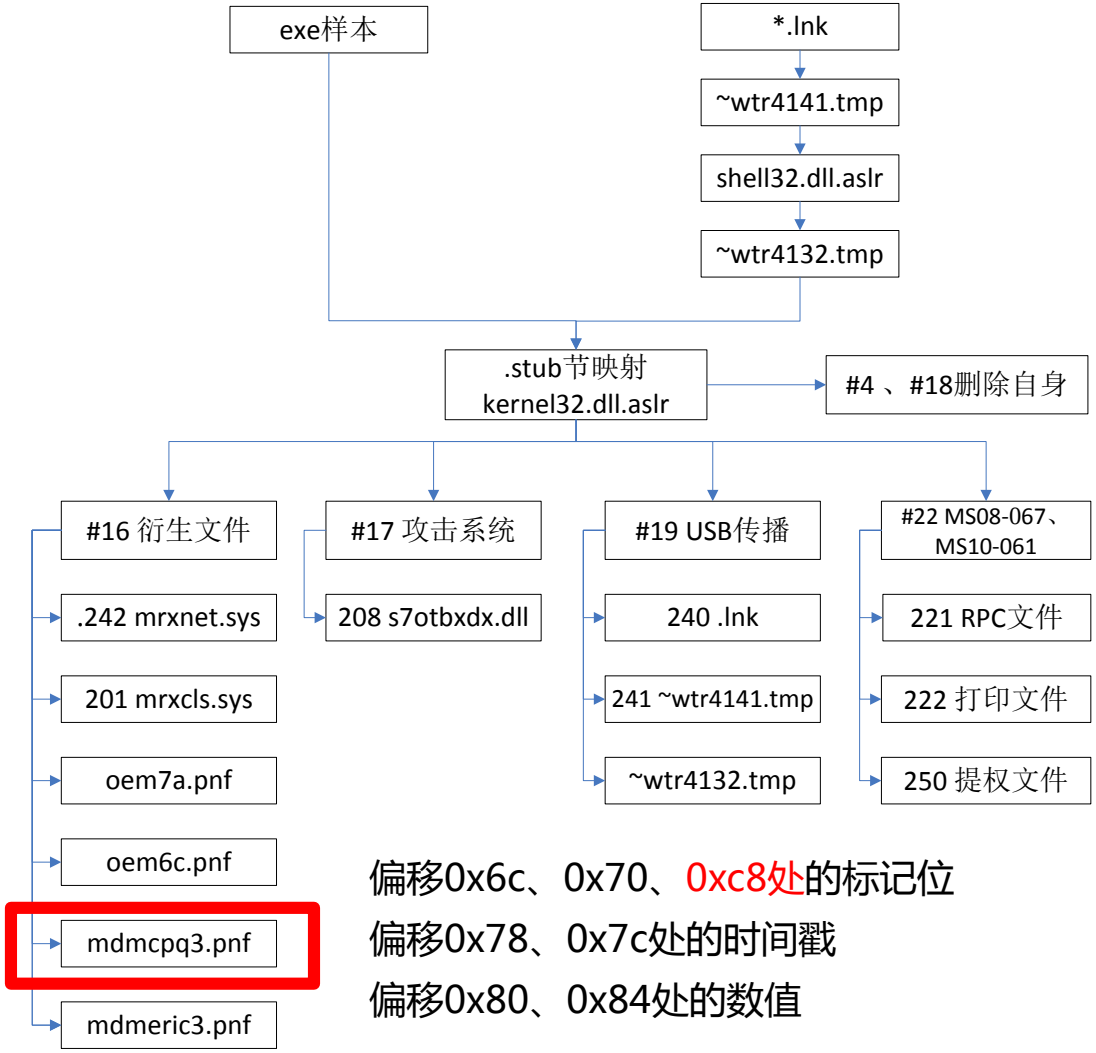
- 任务计划程序程序漏洞

来源： 安天《对Stuxnet蠕虫攻击工业控制系统事件的综合报告》

A²PT：复杂的条件逻辑







偏移0x6c、0x70、0xc8处的标记位

偏移0x78、0x7c处的时间戳

偏移0x80、0x84处的数值

来源： 安天《对Stuxnet蠕虫攻击工业控制系统事件的综合报告》

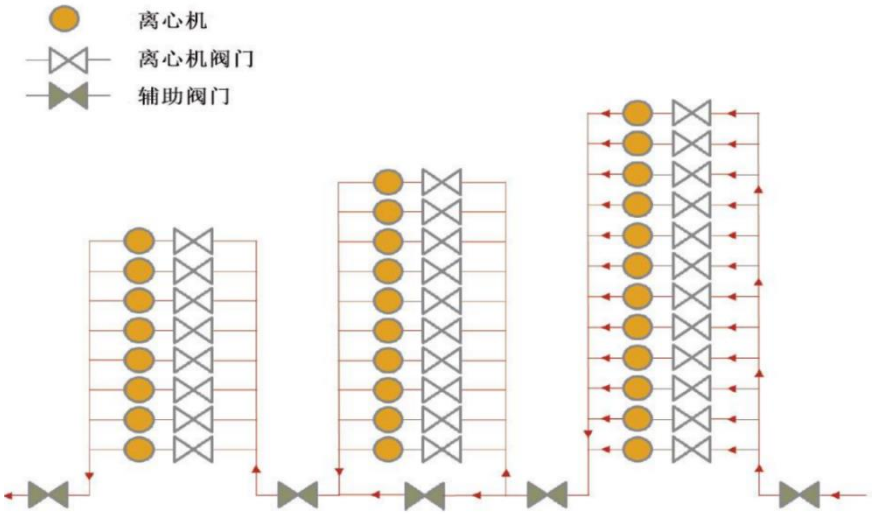
A²PT：场景纵深

漏洞	0.500	1.001	1.100	1.101	描述
CVE-2010-3888			X	X	任务调度程序 EOP
CVE-2010-2743			X	X	加载键盘布局 EOP
CVE-2010-2729		X	X	X	PrintSpooler RCE
CVE-2008-4520		X	X	X	Windows 服务器服务 RPC RCE
CVE-2012-3015	X	X	X	X	Step7 Insecure Library Loading
CVE-2010-2772		X	X	X	WinCC 缺省密码
CVE-2010-2568			X	X	Shortcut.lnk RCE
MS09-025		X			NtUserRegisterClassExWow /NtUserMessagerCall EOP

表 2. Stuxnet 漏洞利用的演变

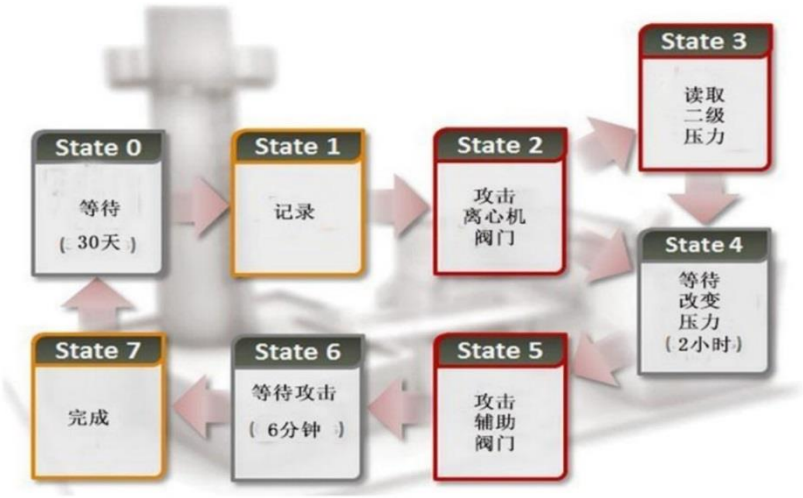
复制技术	0.500	1.001	1.100	1.101
Step 7 项目文件	X	X	X	X
利用 Step 7 项目文件的 USB	X			
利用自动运行的 USB		X		
利用 CVE-2010-2568 的 USB			X	X
网络共享		X	X	X
Windows 服务器 RPC		X	X	X
Printer Spooler		X	X	X
WinCC 服务器		X	X	X
利用 mailslots 进行 P to P 更新	X			
利用 RPC 进行 P to P 更新		X	X	X

表 3. Stuxnet 复制机制的演变



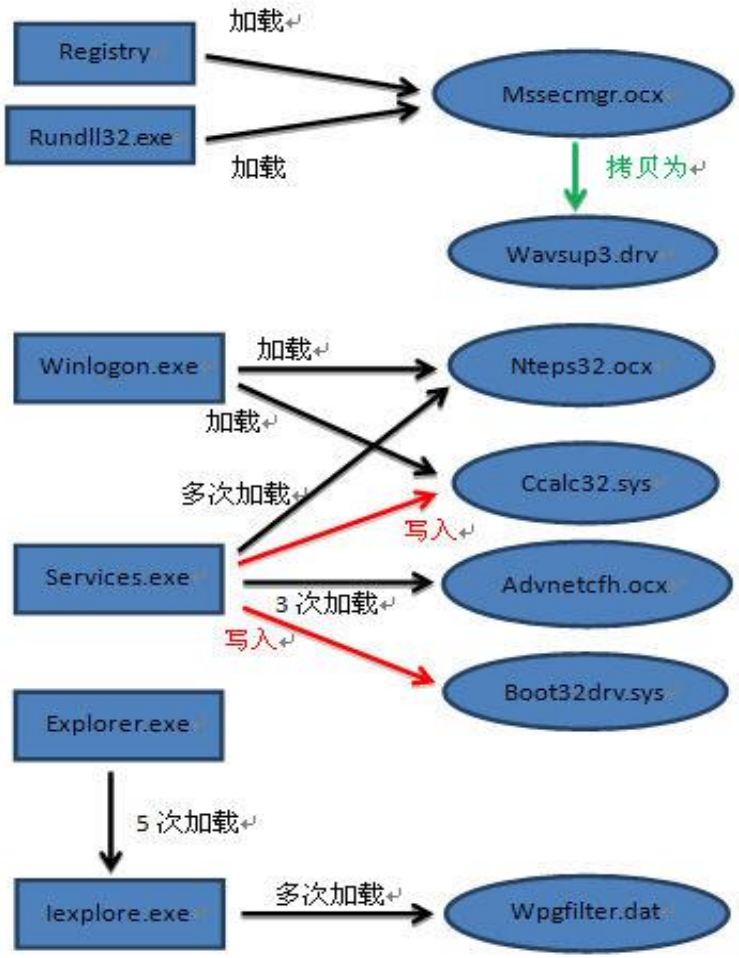
《Symantec： Stuxnet 0.5 How It Evolved》

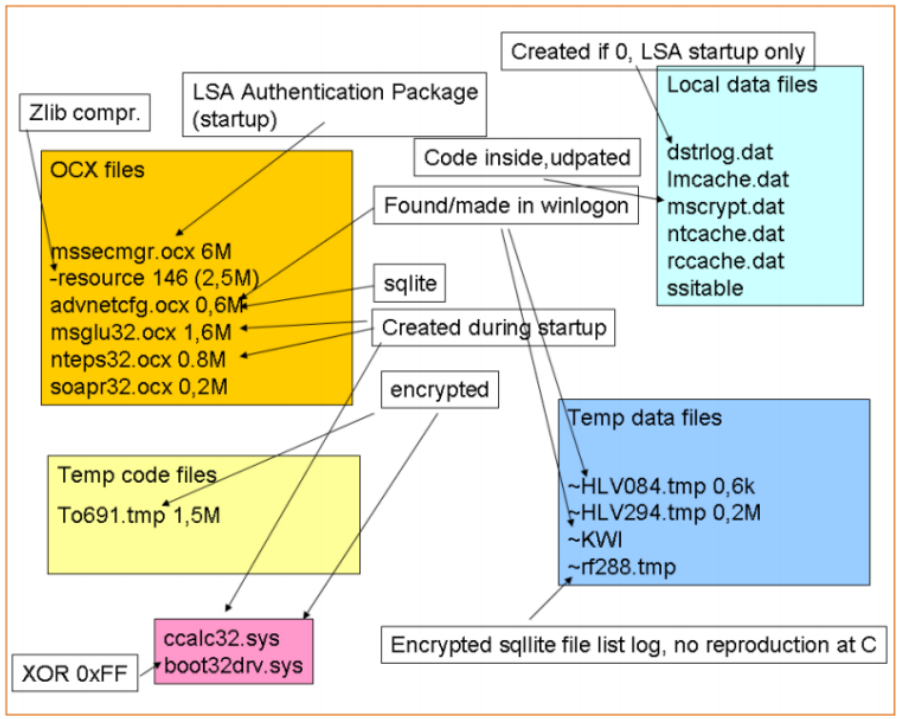
417PLC攻击代码状态流程图



《Symantec： Stuxnet 0.5 The Missing Link》

A²PT的近亲：火焰（Flame）



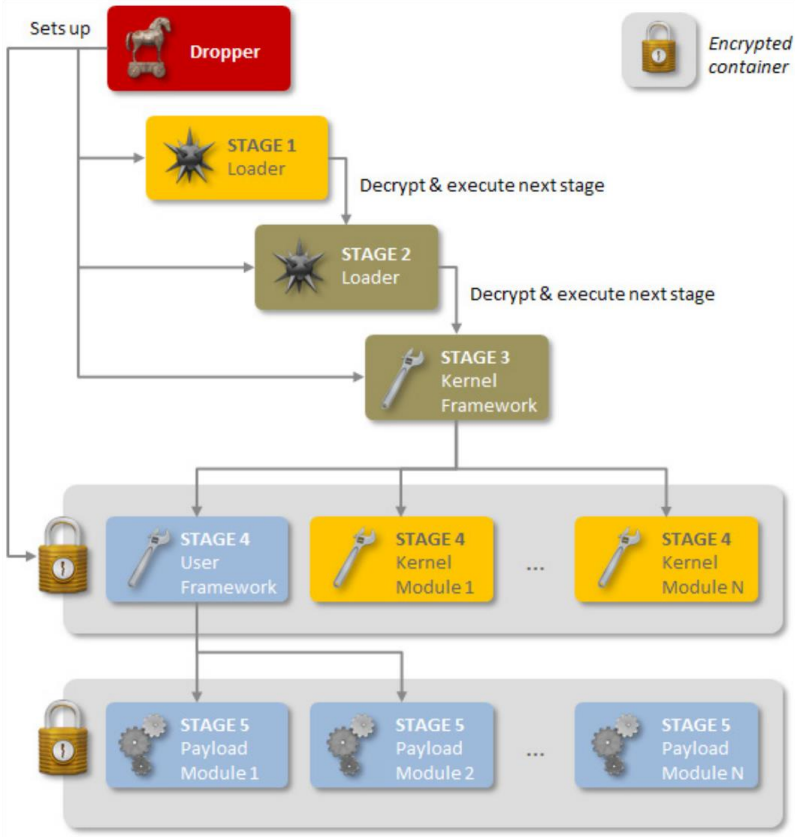


mssecmgr.ocx (6 M) 主模块
-- resource 146 (2.5 M) 类似 zlib 的压缩资源文件
advnetcfg.ocx (0.6 M) 感染部分，可能是窃取信息（类似于屏幕截图）
msglu32.ocx (1.6 M) 由主模块创建的文件
nteps32.ocx (0.8 M) 由主模块创建的文件
soapr32.ocx (0.2 M) 基于网络传播的模块
~rf<number>.tmp 包含完整的被感染计算机的文件列表，以 SQLite3 数据库格式

来源： 安天《Flame蠕虫样本集分析报告》

来源： http://www.crysys.hu/skywiper/skywiper.pdf

A²PT的演进：Rootkit-无文件实体瑞晶(Regin)



Regin的六个阶段	
阶段	组件
阶段 0	投放器。安装Regin 至目标计算机
阶段 1	加载驱动程序，初始阶段1驱动程序是计算机上唯一明显可见的代码。所有其他阶段都以加密数据的形式存储.....
阶段 2	加载驱动程序
阶段 3	加载压缩、解密、联网及处理加密的EVFS程序。
阶段 4	利用EVFS并加载额外的内核模式驱动程序，包括有效载荷。
阶段 5	主要的有效载荷和数据文件

更强的Rookit特性，无文件实体，难以提取完整载荷

来源： http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf

A²PT的演进：模块化 (Regin)

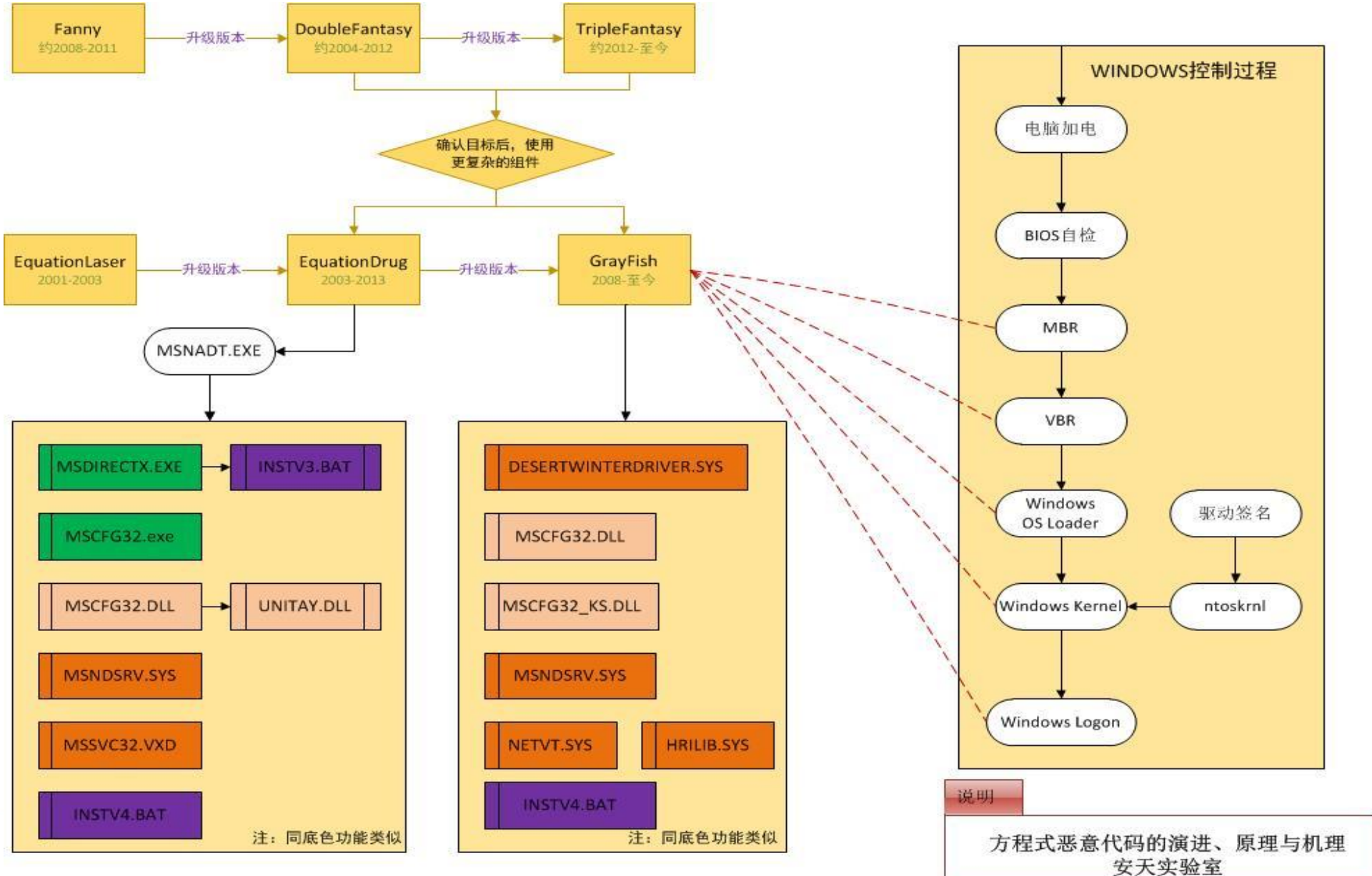
文件类型	编号	描述
SYS	0003	驱动程序
SYS	C433	Rootkit
SYS	C42B	PE加载程序
SYS	C42D	DLL注入
SYS	C3C3	类似WinPcap的网络数据包过滤器驱动程序（协议过滤器版本3.5 用于设置TCP和UDP穿透过滤器和绕过防火墙。 执行BPF（Berkeley包过滤器）字节码，存储在阶段5的数据文件里。
SYS	CE69	网络端口屏蔽器
DLL	C363	网络数据包捕获
DLL	4E3B	通过注册表或配置文件（如prefs.js, refs.js等）检索网页浏览器（IE浏览器，网景，火狐等）的代理信息。枚举会话和用户账户。
DLL	290B	密码窃取器： • Windows资源管理器凭据 • Windows资源管理器受保护存储记录 • IE合法设置 • 名为“cryptpp”登陆通知数据包的数据
DLL	C375	C&C HTTP/cookies
DLL	C383	SSL通信
DLL	C361	支持加密功能
DLL	001B	ICMP反向信道
DLL	C399	ApplicationLog.Evt记录创建程序
DLL	C39F	进程文件：%Temp%\~b3y7f.tmp

DLL	C36B	UI manipulation • 截屏 • 记录键盘操作 • 锁定工作站/输入Ctrl-Alt-Del • 点击功能 (通过三条指令：去、点击并释放、返回原始位置) • 结束进程
DLL	C351	文件系统探索元和包括原始NTFS解析器的取证水平探索： • 获取其他文件信息和属性 • 浏览记录 • 读写文件 • 移动和复制文件 • 读取并修复部分或全部被删除的文件 • 计算文件哈希
DLL	2B5D	进程和模块操作： • 读取进程和模块 • 进程运行的时间、限制和权限 • 扫描时，跳过俄语或英语的微软文件 • 检测过去两天里新引进的PE文件
DLL	C3CD	枚举 %System%\CurrentControlSet\Services\Tcpip\Linkage\bind里的TCP/IP接口
DLL	C38F	TCPDump 功能
DLL	C3C5	Libnet 二进制文件
DLL	27E9	IIS 网页浏览器日志窃取 通过COM对象枚举发现IIS日志。检索部分或全部日志信息。 • 部分：日志类型、上一个日志、较早日志的时间戳 • 全部：被发掘的全部日志记录

来源： http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf

安天论坛技术公益翻译版本已公开译文

A²PT的演进：持久化（Equation）



A²PT的特点

神一样的对手

1 有充足的0day储备

2 载荷部分高度复杂，高度模块化

3 本地加密抗分析，网络严格加密通讯和伪装

4 不一定通过网络植入，可能为人工植入和物流链劫持

5 基本上完整普及了无文件载体技术，内存分段抗分析

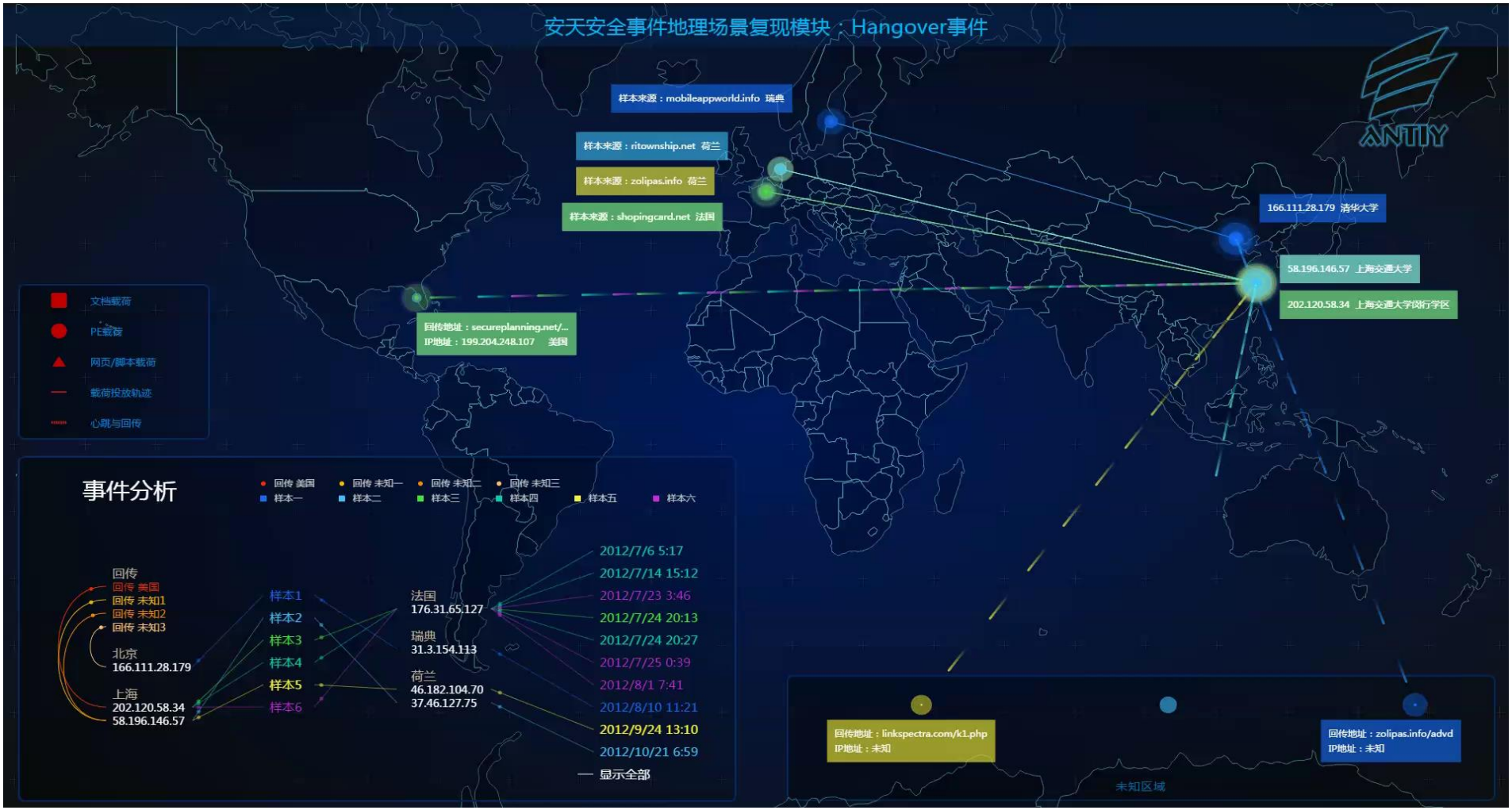
6 持久化向深度扩展（固件），向广度扩展（防火墙、邮件网关、局网内横向移动）

7 完整的覆盖所有操作系统平台（含移动）

不是所有高级持续性威胁都显得“高级”，不是所有“高级”都是攻击者的“自身能力”.....

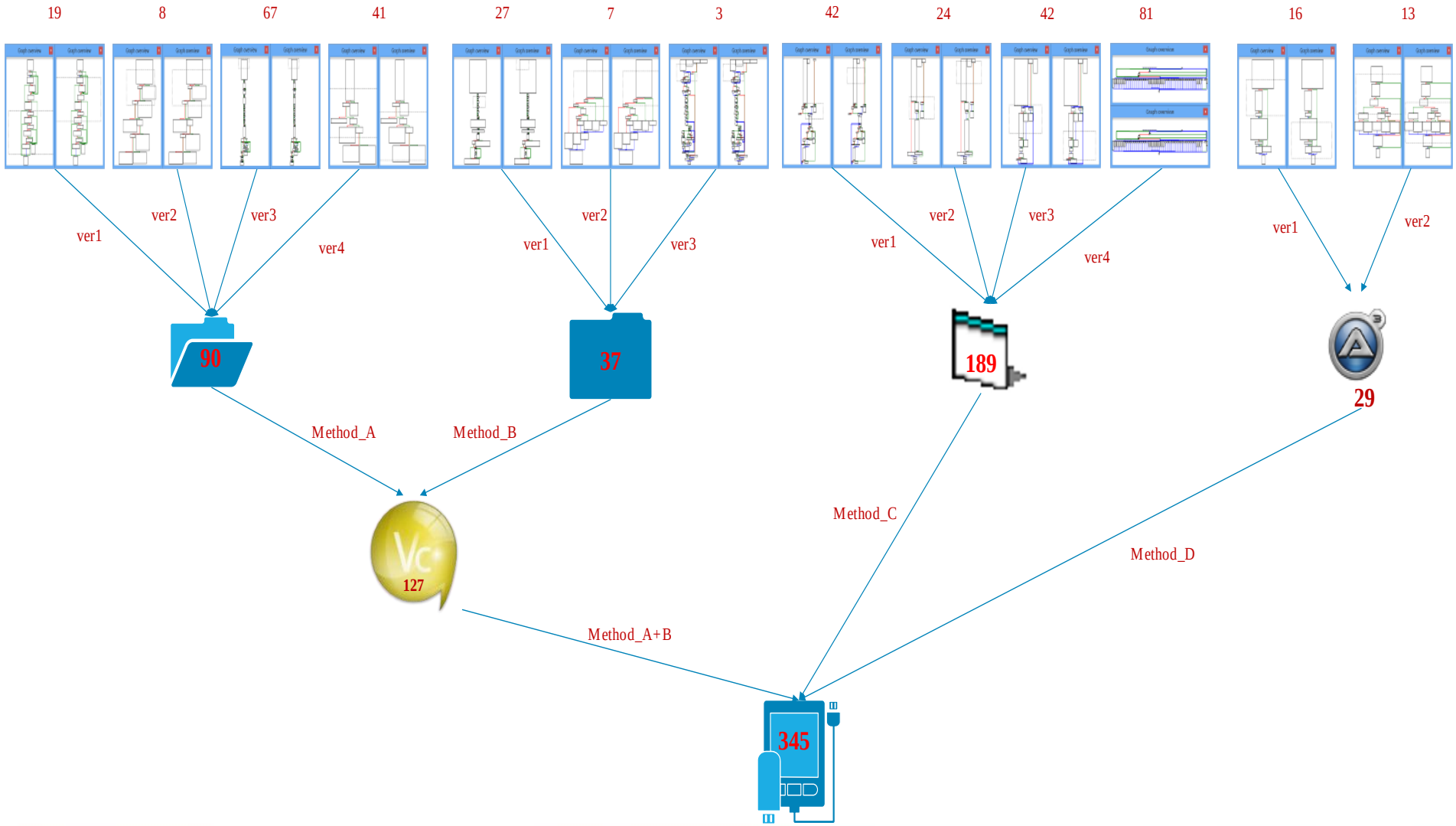
“轻量级”的APT、准APT以及其中的恶意代码

“不够A”的APT:从Hangover说起



没有使用0day；没有盗用大厂商证书；没有复杂的加密体系；没有必要的Rootkit手段

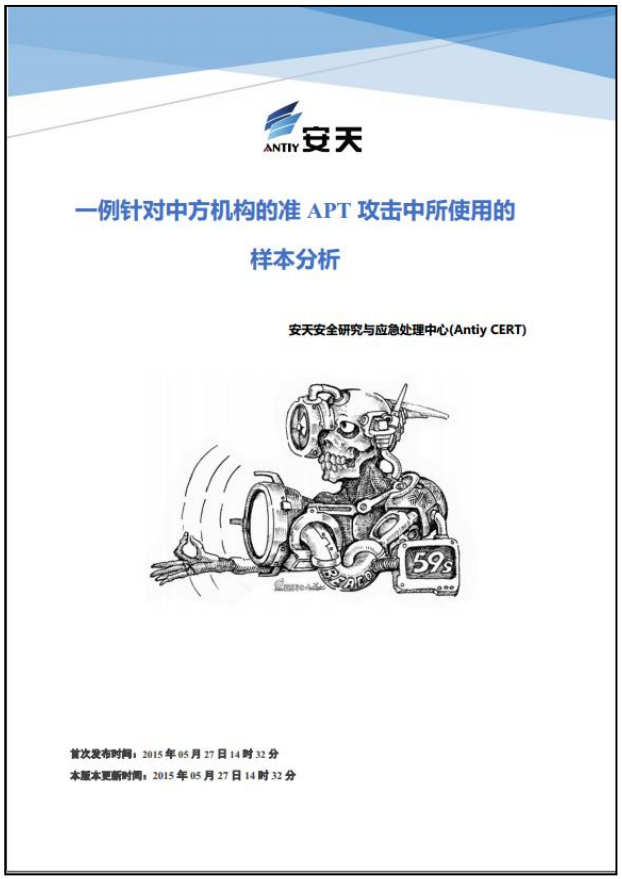
“不够A”的APT: hangover中的人海战术

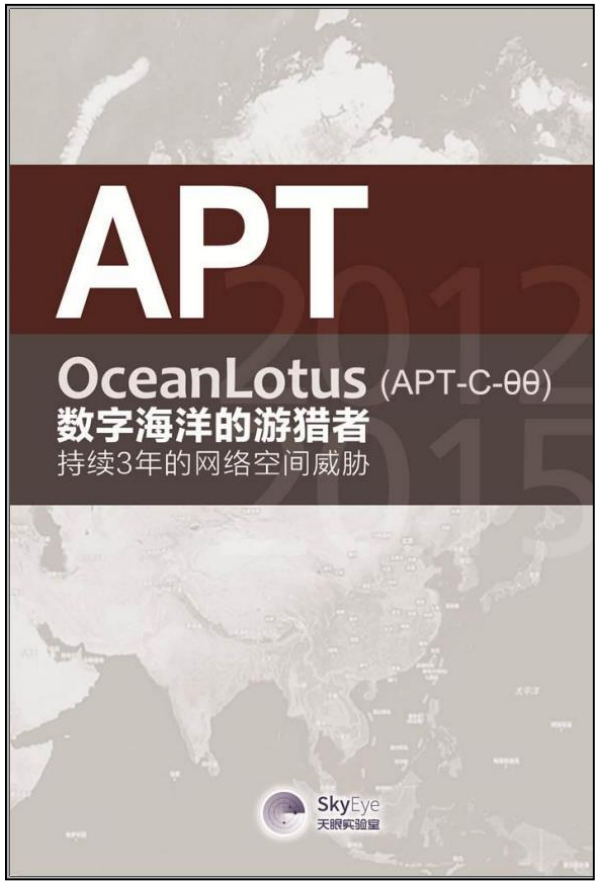


“轻量级”APT攻击的特点

1. 缺乏0day储备，很少使用0day
2. 载荷编写质量低下
3. 严重依赖网络投放
4. 没有采用必要的Rootkit手段
5. 缺少必要的持久化能力
6. 主要针对Windows系统平台作业

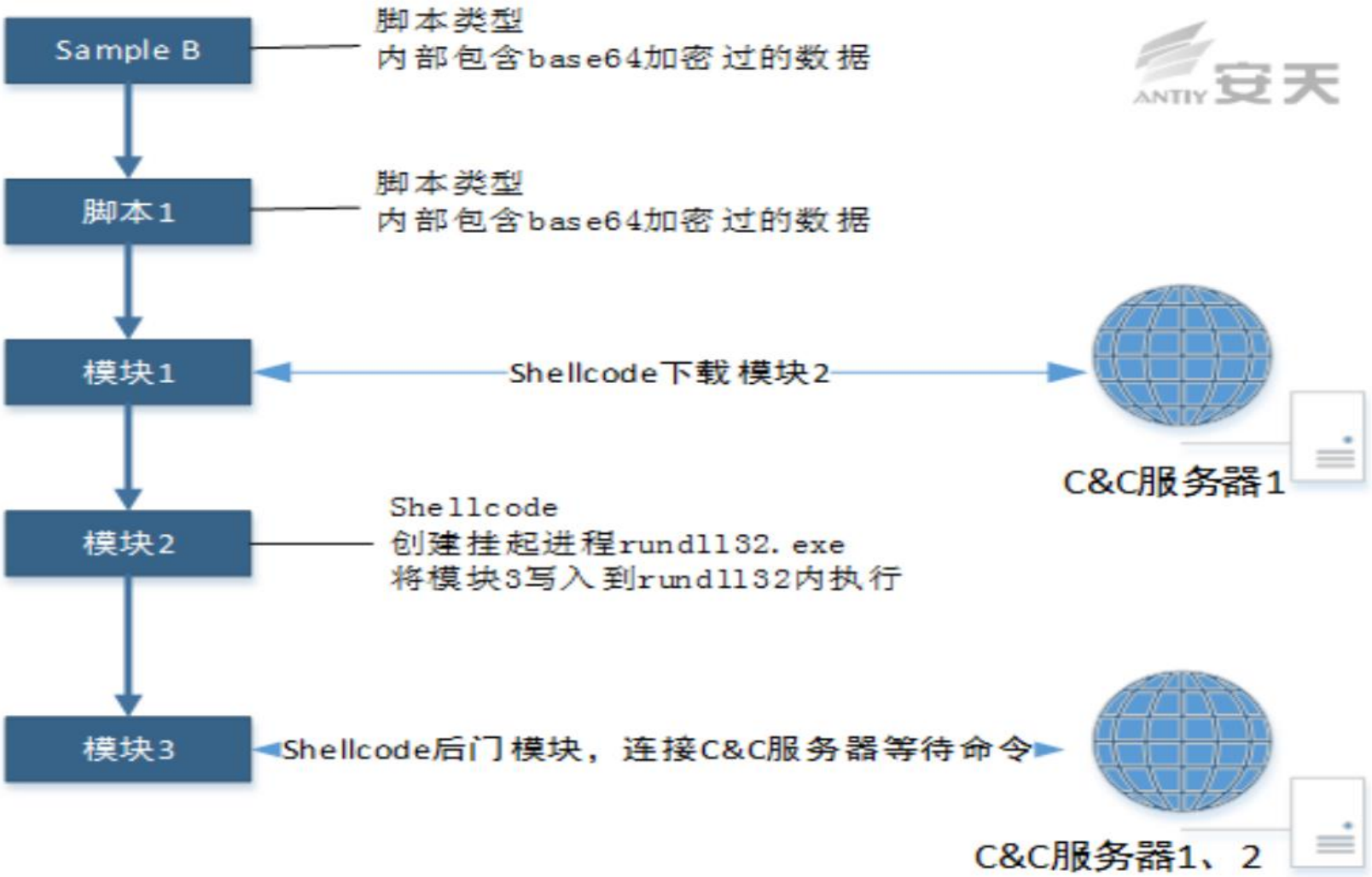
准APT的变化：从最近的热点事件说起





中国厂商自2015年5月27日起连续曝光境外APT，以上三篇文章是针对同一个对手的不同角度解读

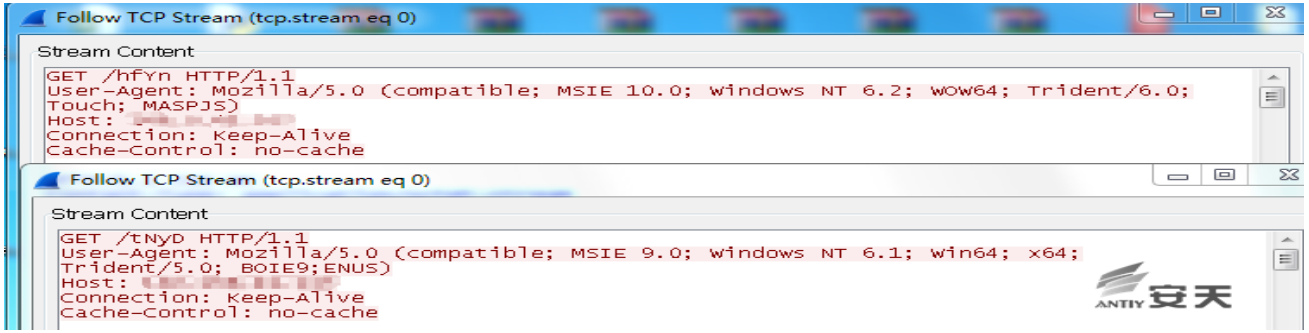
一个场景下的作业手段



来源： 2015.05.28 安天《一例针对中国官方机构的准APT攻击分析》

具有“艺术水准的攻击”从何而来？

攻击样本与Cobalt Strike攻击平台生成的样本比较



模块1与Cobalt Strike攻击平台生成样本的数据比较

来源： 2015.05.28 安天《一例针对中国官方机构的准APT攻击分析》

Cobalt Strike平台的情况

- Cobalt Strike是Armitage的商业版本。
- Armitage是一款Java写的Metasploit图形界面的渗透测试软件，可以用它结合Metasploit已知的exploit来针对存在的漏洞自动化攻击。
- bt5、kali linux 下集成的免费版本Armitage，最强大的功能是多了个beacon的payload。

Cobalt Strike首次发布时间：2012年6月

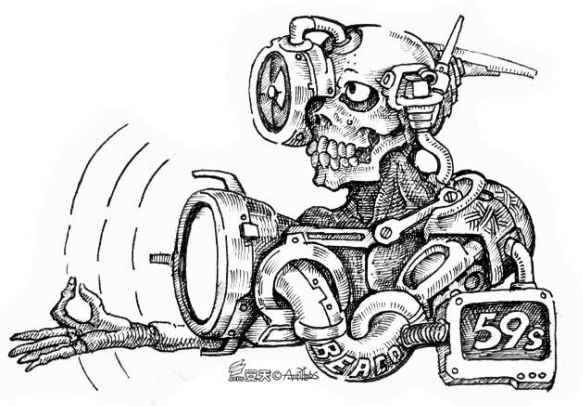
版本	描述
Cobalt Strike1.45及以前版本	可以连接本机windows的metasploit的，在后来就不被支持了，必须要求连接远程linux的metasploit。
Cobalt Strike1.46	系统分析器使用退回措施检查java报告版本信息，修复了密钥生成漏洞。
Cobalt Strike1.47	缓解了beacon多重信息积压；开启侦听器时进行全面检查。
Cobalt Strike1.48	beacon增加了timestomp命令；bypassuac特权文件复制完成等待至10秒。
Cobalt Strike1.49	修复了Windows XP的beacon HTTP Stager 负载生成器。
Cobalt Strike2.0	可塑性的命令和控制，增加了“veil”选项到负载生成器。
Cobalt Strike2.1	powershell命令启动本地主要的powershell；更新了build.sh工具。
Cobalt Strike2.2	重建过程注入和连接到目标系统上的VNC服务器，新过程由于基于主机的防火墙更容易被忽略；漏洞报告显示来自ZDI,MSB,US-CERT-VU 和WPVDB的URL引用。
Cobalt Strike2.3	用定制的编码器编码beacon的DNS阶段；beacon增加了runas命令、pwd命令。
Cobalt Strike2.4	增加时间戳到view - >web日志项；用不同参数重新生成默认beacon HTTPS证书；现在使用不同参数生成可塑的C2 HTTPS证书；更新了可执行文件和DLLS的默认工具包。

CS平台作者信息

- **Cobalt Strike作者**：Raphael Mudge（美国）
  - LLC创始人（the creator of Armitage and founder of Strategic Cyber LLC, develops Cobalt Strike）；
  - 基于华盛顿的公司为RED TEAM开发软件，为Metaslpoit创造了Armitage、sleep程序语言和IRC客户端jIRCii；
  - 曾是美国空军的安全研究员，渗透实验的测试者；
  - 他设置发明了一个语法检测器卖给了Automattic；
  - 发表多篇文章，定期进行安全话题演讲，给许多网络防御竞赛提供RED TEAM，曾参加2012-2014年黑客大会；
- **教育背景**：Syracuse University 美国雪城大学，密歇根科技大学
- **目前就职**：Strategic Cyber LLC（战略网络有限责任公司），特拉华州空军国民警卫队

公司/项目/机构	职位	时间
Strategic cyber LLC	创始者和负责人	2012.1-至今
特拉华州空军国民警卫队	领导，传统预备役	2009-至今
Cobalt strike	项目负责人	2011.11-2012.5
TDI	高级安全工程师	2010.8-2011.6
Automattic	代码Wrangler	2009.7-2010.8
Feedback Army, After the Deadline	创始人	2008.7-2009.11
美国空军研究实验室	系统工程师	2006.4-2008.3
美国空军	通信与信息 军官	2004.3-2008-3

为什么安天称之为“准”APT攻击



安天 CERT 分析小组之所以将 APT-TOCS 事件定位为准 APT 事件，是因为该攻击事件一方面符合 APT 攻击针对高度定向目标作业的特点，同时隐蔽性较强、具有多种反侦测手段。但同时,与我们过去所熟悉的很多 APT 事件中，进攻方具备极高的成本承担能力与巨大的能力储备不同，其成本门槛并不高，事件的恶意代码并非由攻击者自身进行编写构造，商业攻击平台使事件的攻击者不再需要高昂的恶意代码的开发成本，相关攻击平台亦为攻击者提供了大量可选注入手段，为恶意代码的加载和持久化提供了配套方法，这种方式降低了攻击的成本，使得**缺少雄厚资金、也缺少精英黑客的国家和组织**依托现即有商业攻击平台提供的服务即可进行接近 APT 级攻击水准，而这种高度“模式化”攻击也会让攻击缺少鲜明的基因特点，从而更难追溯。

来源：2015.05.28 安天《一例针对中国官方机构的准APT攻击分析》

移动平台的新情况

我们判断商业间谍移动工具间谍工具已经被应用到对中国目标的攻击当中。

BiiGe 比歌

- 功能齐全商业间谍
- 版本齐全，Android、iOS、BlackBerry
- 短信、监控端、C&C远控

服务	描述
15天完整高级功能!	比歌手机定位服务 + 短信记录备份 + WhatsApp Line Facebook + 通话记录备份 + 彩信记录备份 + 联系人备份管理 + 上网历史记录 + 软件远程管理 在你的手机或Web上直接查阅 支持系统: Android 4+

VS

PhoneBeagle

- 功能齐全商业间谍
- 版本相对较少，Android、BlackBerry
- 短信、监控端、C&C远控

How It Works

Locate & Watch Your Child

- Hidden Icon / Uninstall Protection
- SMS Text Messages
- Facebook Chat & Messages
- Skype WhatsApp LINE Messages
- GPS & Network Phone Location
- Remotely Block Calls / Text Messages
- Remotely Block Violent / Sexual Apps
- Spyware / Malicious App Alerts
- Call, App & Website Usage History
- Phone Address Book
- MMS Multi-Media Messages
- System & SIM Change Notifications

版本对比

Biige - 内陆版

- 安装无图标
- 浏览器scheme url启动
- biige://open

- 所有数据上传C&C服务器
- 监控端从服务器读取数据
- 基于BeanShell技术后门
- 功能丰富
- 可透明地访问任何Java对象和API
- 可执行任意指令脚本

VS

PhoneBeagle - 海外版

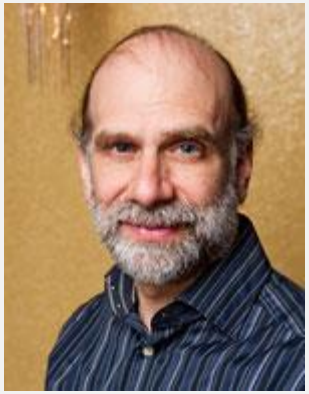
- 有/无图标版本-图标可隐藏
- 浏览器scheme url启动
- phonebeagle://opne
- 拨号盘“*#*#”＋call启动
- 所有数据上传C&C服务器
- 监控端从服务器读取数据
- 基于BeanShell技术后门
- 功能丰富
- 可透明地访问任何Java对象和API
- 可执行任意指令脚本

商业木马-在线销售


在线购买比歌
帮助
退出
My Demo Kid
短信
通话
地点
彩信
网页记录
软件
系统
控制面板
显示高级控制指令
常规 - 行车免干扰
常规 - 行车模式
通讯网络 - 漫游
常规 - 控制时间表
常规 - 发送手机数据
事件 - 删除事件
事件 - 上传通话记录
事件 - 立刻上传通话记录
事件 - 上传所有数据
事件 - 立刻上传所有数据
事件 - 立刻上传所有数据
事件 - 立刻上传所有数据(互联网/无线网络)
事件 - 上传方位
事件 - 立刻上传方位
事件 - 上传彩信或多媒体文件
事件 - 立刻上传彩信
事件 - 上传时间表
事件 - 上传短信
事件 - 立刻上传短信
事件 - 上传系统数据
事件 - 立刻上传系统数据
常规 - 应用程序启动
启动该指令
常规 - 行车免干扰
没有可用选项
这个指令指示目标手机是否开启或关闭行车免干扰模式。
当行车免干扰模式开启目标手机上的应用程序将使手机上的GPS功能持续开启并记录每次目标手机接收发送短信，电话和浏览网页时车辆方位和行驶速度。
初始状态为禁用此功能以保护手机电池耗电量。
短信指令
除了可以直接从互连网控制界面上发送指令之外，远程控制指令也可以短信形式用手机发送。
开启行车免干扰模式
关闭行车免干扰模式
开启车辆监控模式
禁用车辆监控模式
获取方位并上传数据
获取方位并通过短信发送数据
现在查看是否有新的指令
帐户详情
密匙 DEMODEMODEMODEMO
电子邮件
姓名 My Demo Kid
改变昵称
状态 激活
创建 2010 七月 01 6:00:00 [当地时间]
开启 2010 七月 01 6:00:00 [当地时间]
激活 2010 七月 01 6:00:00 [当地时间]
产品 momo biige_1
安装 版本 1 安装在 Android
改变电子邮件
改变密码


Buy PhoneBeagle Online
Help
Exit
My Demo Kid
Text
Facebook
WhatsApp
LINE
Calls
Location
Media
Web
Contacts & Blocks
Apps
App Blocks
App Alerts
System
Control
Show Advanced Commands
General - Distracted Driving Mode
General - Tracking Mode
Comms - Set Roaming
General - Set Control Schedule
General - Send Diagnostic Data
Events - Delete Events
Events - Set Upload Calls
Events - Set Upload Calls Immediately
Events - Set Upload All Types
Events - Set Upload All Types Immediately
Events - Upload Immediately
Events - Upload Immediately (WLAN/WiFi)
Events - Set Upload Location
Events - Set Upload Location Immediately
Events - Set Upload Multi-Media Messages
Events - Set Upload Multi-Media Messages
Events - Set Upload Schedule
Events - Set Upload Text Messages
Events - Set Upload Text Messages Immed
Set Command Active
General - Distracted Driving Mode
No Options Available
This command tells the App on the phone whether distracted driving mode should be enabled or disabled.
When distracted driving mode is enabled the App on the phone will keep GPS activated at all times and record location and speed every time Text Message, Call, Multi-Media Message and Web functionalities are used.
By default distracted driving mode is disabled in order to protect the phone from excessive battery drain.
Text Message Commands
In addition to commands sent directly from this Web App, commands can also be sent to the App on the phone using Text Messages.
Enable Distracted Driving Mode
Disable Distracted Driving Mode
Enable Tracking Mode
Disable Tracking Mode
Acquire Location & Send Via Text Message
Acquire Location, Send Via Text Message & Upload
Check For New Commands Now
Remote Activation
Account Details
Refresh Account Details
Key DEMODEMODEMODEMO
Email
Friendly Name My Demo Kid
Change
Status Activated
Enabled Thu Jul 01 2010 6:00 AM [Local Time]
Activated Thu Jul 01 2010 6:00 AM [Local Time]
Last Upload Sun Jan 00 NaN 12:00 AM [Local Time]
Product momo beagle_1
Uninstall Alert Phone Number Not Set
Change
Recorder Installation Version 1 Installed On Android
Protector Installation Not Installed
Change Email
Change Password

穷国的新“原子弹”



我认为目前正在发生而且真正重要的趋势是：越来越多战争中的战术行为扩散到更广泛的网络空间环境中。这一点非常重要。通过技术可以实现能力的传播，特别是计算机技术可以使攻击行为和攻击能力变得自动化。

——Bruce Schneier

安天认为同样存在另外一种倾向，就是商业化的工具和样本会更多的出现在国家与政经集团的相互的APT攻击当中。一种有趣的现象是，被先进者淘汰的滑膛枪，同样可以用于屠杀使用弓箭的原始部落（或平民）。

我们如何再认识APT？

如何重新认识A、如何重新认识P

小结

再谈如何定性APT？

APT不是一个严格的技术概念，必须关联其政经背景

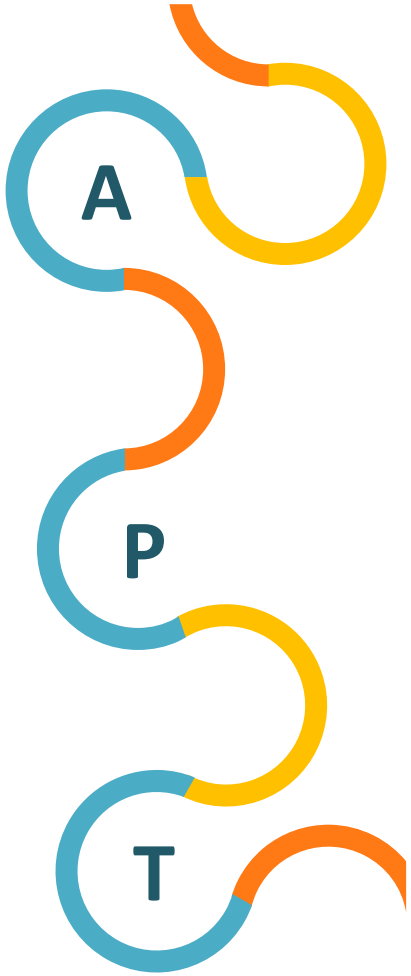
- 发起方与动机
- 受害方与后果
- 作业过程与手段

A的再认识，A具有相对性

- 相对攻击背景体系的能力层次
- 相对被攻击者的势能落差

P是具象的、也是宏观的

- 具象：其可能是连接能力、也可能是持久化的能力、或者反复进入的能力
- 宏观：取决于攻击方的作业意志的持续和成本支撑能力



防御、制高点、纵深、运动战

- *基于纵深防御的思想，黄晟提出的塔防思路是好模型。*
- *我们面对的不是一个能力维度层次的对手，我们既面对A^2PT、也有准APT，因此只有烧火棍不行，但“只能屠龙”的屠龙刀是未必好用的。*

安天拥有一些制高点，如静态检测的能力（AVL SDK）、动态的能力（追影）等，但我们不迷信制高点。

不论在防御和进攻中制高点都能产生一定的有利效果,这种效果是必须考虑的.....就便于运动这一点来说,高处的军队并不是绝对有利的,也不是在任何场合都是有利的。

——克劳塞维茨

安天提供在多个环节上削弱对手能力、呈现对手行为的产品，并在过去若干年一直在刀锋上与对手PK。

ANTIY 安天

谢谢聆听

www.antiy.com

seak@antiy.cn

weibo.com/seak

智者安天下