2015年安天应对的威胁与事件回顾

安天安全研究与应急处理中心
刘佳男

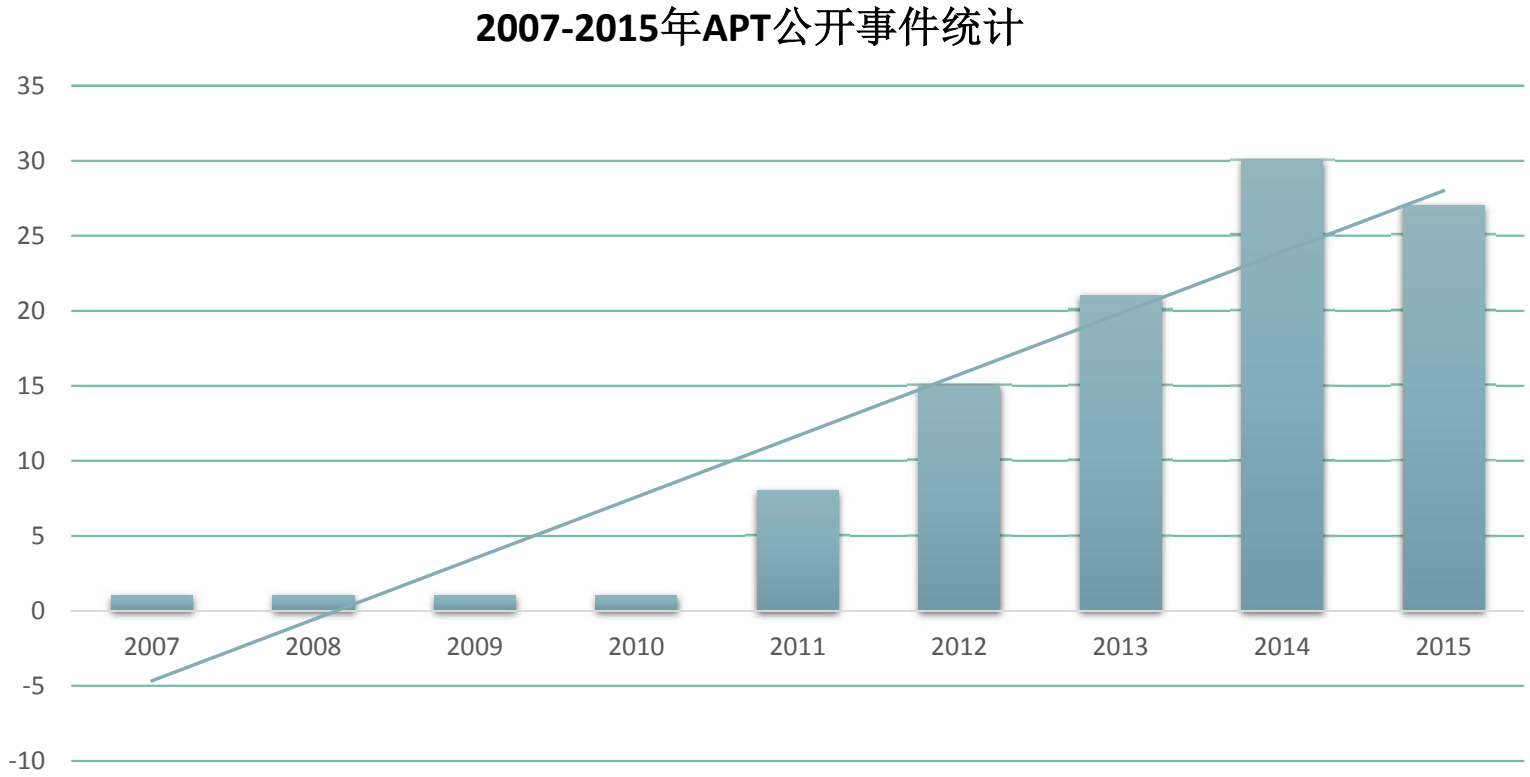
提纲

- 2015重大网络安全事件
- 典型安全事件回顾
- 2016网络安全展望

Part 01

2015重大网络安全事件

历年APT事件趋势


2007-2015年APT公开事件统计
35
30
25
20
15
10
5
0
-5
-10
2007
2008
2009
2010
2011
2012
2013
2014
2015

2015年重大APT事件

02

APT-TOCS（海莲花）

最低成本的APT攻击。随着商用攻击平台平民化和黑色产业链的发展攻击成本日益降低，APT攻击受害者将会越来越多。

01

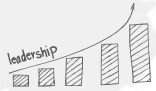
方程式（Equation）

安天独立发现并分析的APT事件，攻击手段隐蔽，技术已经突破网络深入到硬件。

03

Duqu2.0

该恶意软件平台是由沉寂三年的Duqu组织研发的，所以命名为Duqu2.0。对卡巴斯基及伊核六方会谈等发起针对性攻击。



06

蓝白蚁

一起针对日本的APT攻击，攻击日本养老金系统，还有日本政府、国防工业、重要基础设施、航空航天、财政金融、制造业和学术界。 主要攻击手法是利用钓鱼邮件，并通过C2C回传信息。怀疑emdivi家族所为。

04

HAMMERTOSS（APT29）

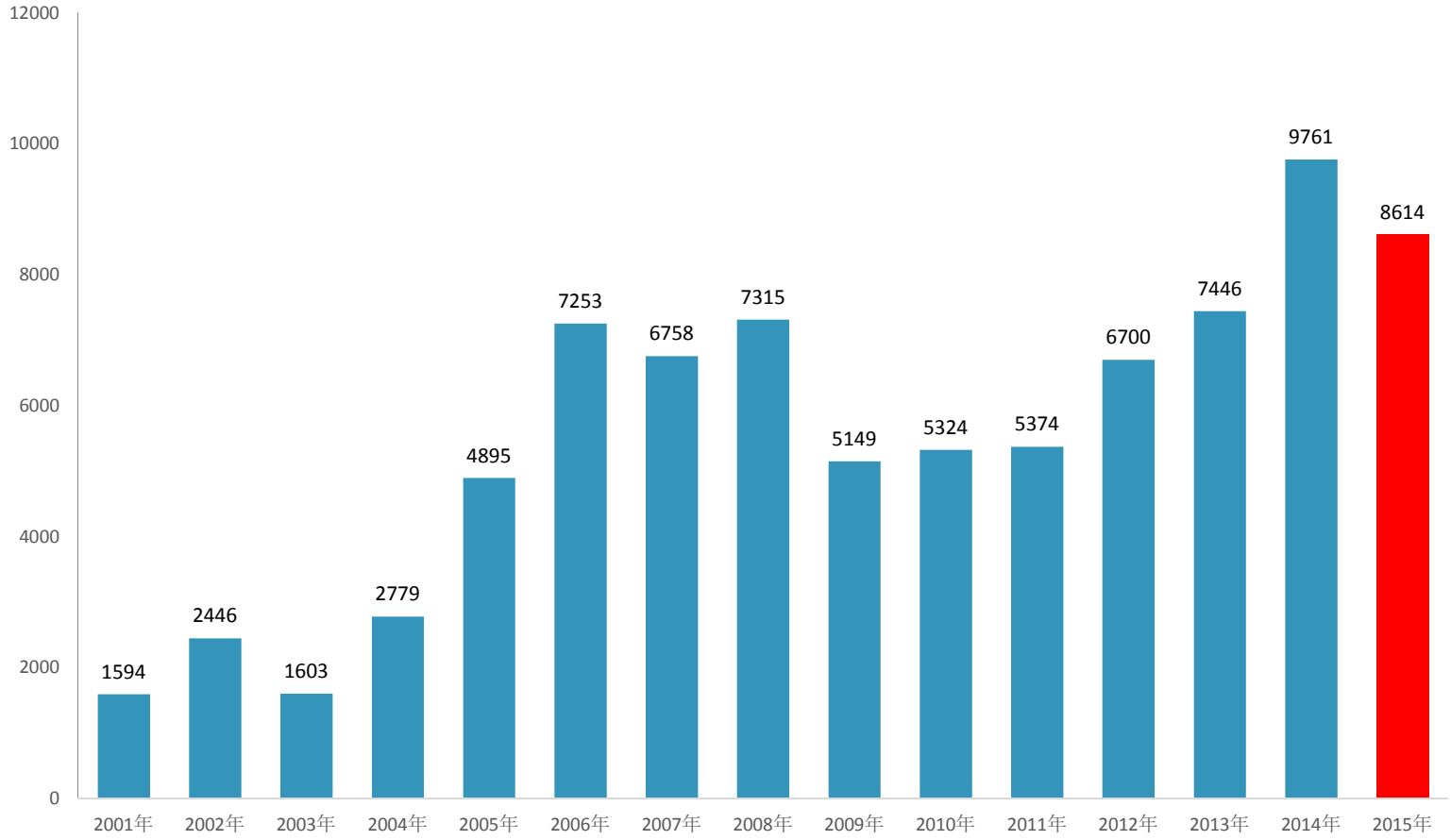
HAMMERTOSS是一款强大的后门工具，利用Twitter、GitHub和云存储服务回放指令并从被攻陷的网络提取数据，并通过多层代码混淆和模仿合法用户的行为，躲避安全防护产品的检测。

05

黑色藤蔓

针对医疗保险服务商的针对性攻击，并且怀疑该组织与“隐秘山猫”有一定的关系。

历年来漏洞数量

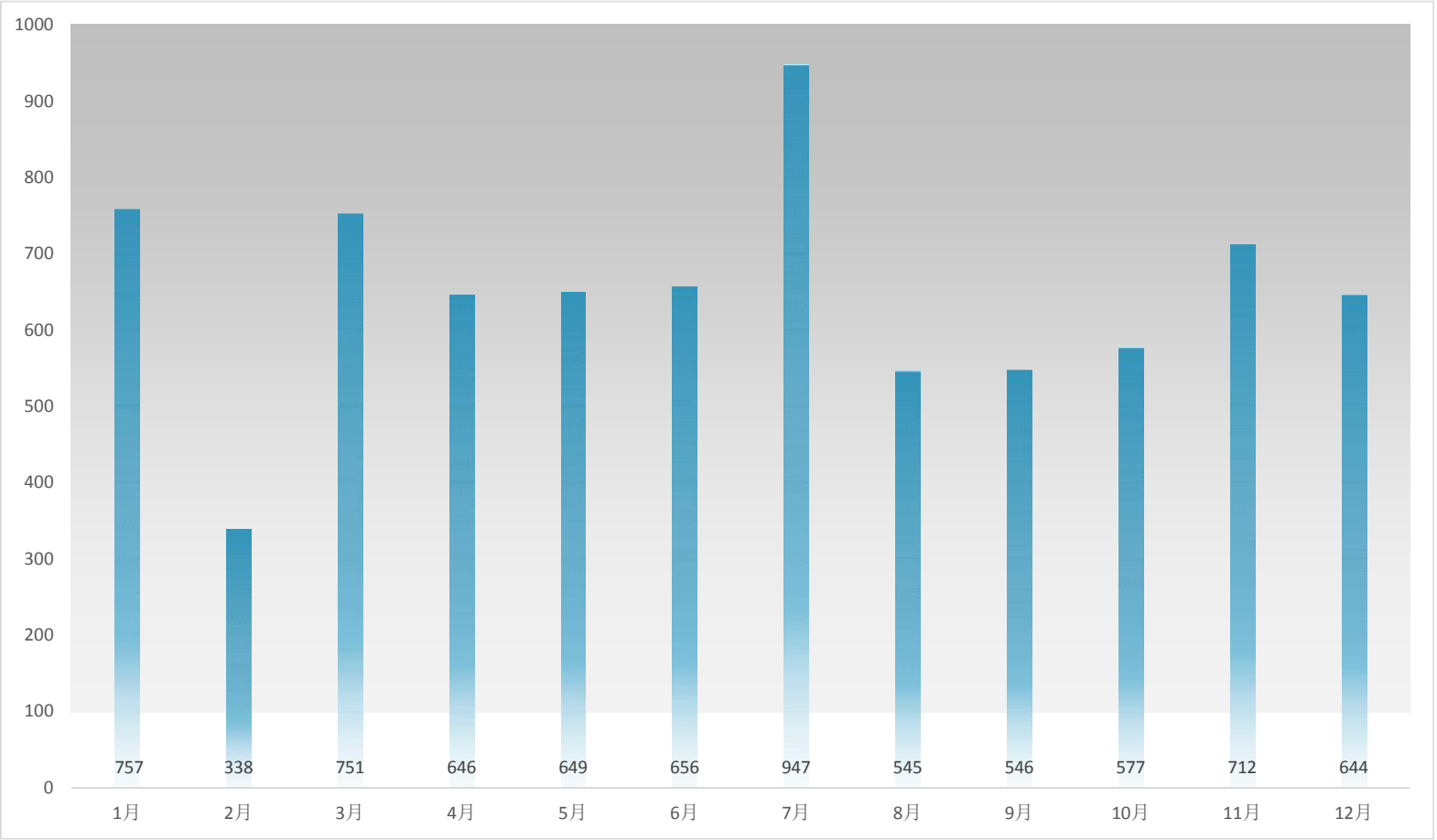


数据来源：www.cnvd.org.cn

漏洞影响对象类型和产生原因统计

数据来源：www.cnvd.org.cn

2015年安天报送漏洞月数量趋势



2015年都有哪些重大漏洞？

2015年初的一个漏洞（CVE-2015-0002）引发了业内对于漏洞披露方式的探讨。起因是Google的安全小组发现了一个Windows8.1的漏洞，在微软尚未对漏洞做出修补的情况下将漏洞细节公之于众。Google严格按照自身的标准，在第90天公布了漏洞详情，然而这一行为引发了业内对漏洞披露方式的探讨，一些漏洞披露方因此形成了一套自己的评价标准，比如一些漏洞平台在今年的漏洞信息中屏蔽掉了一些敏感的IP地址、域名等信息，这使得出现漏洞的厂商避免了微软遭遇的尴尬。

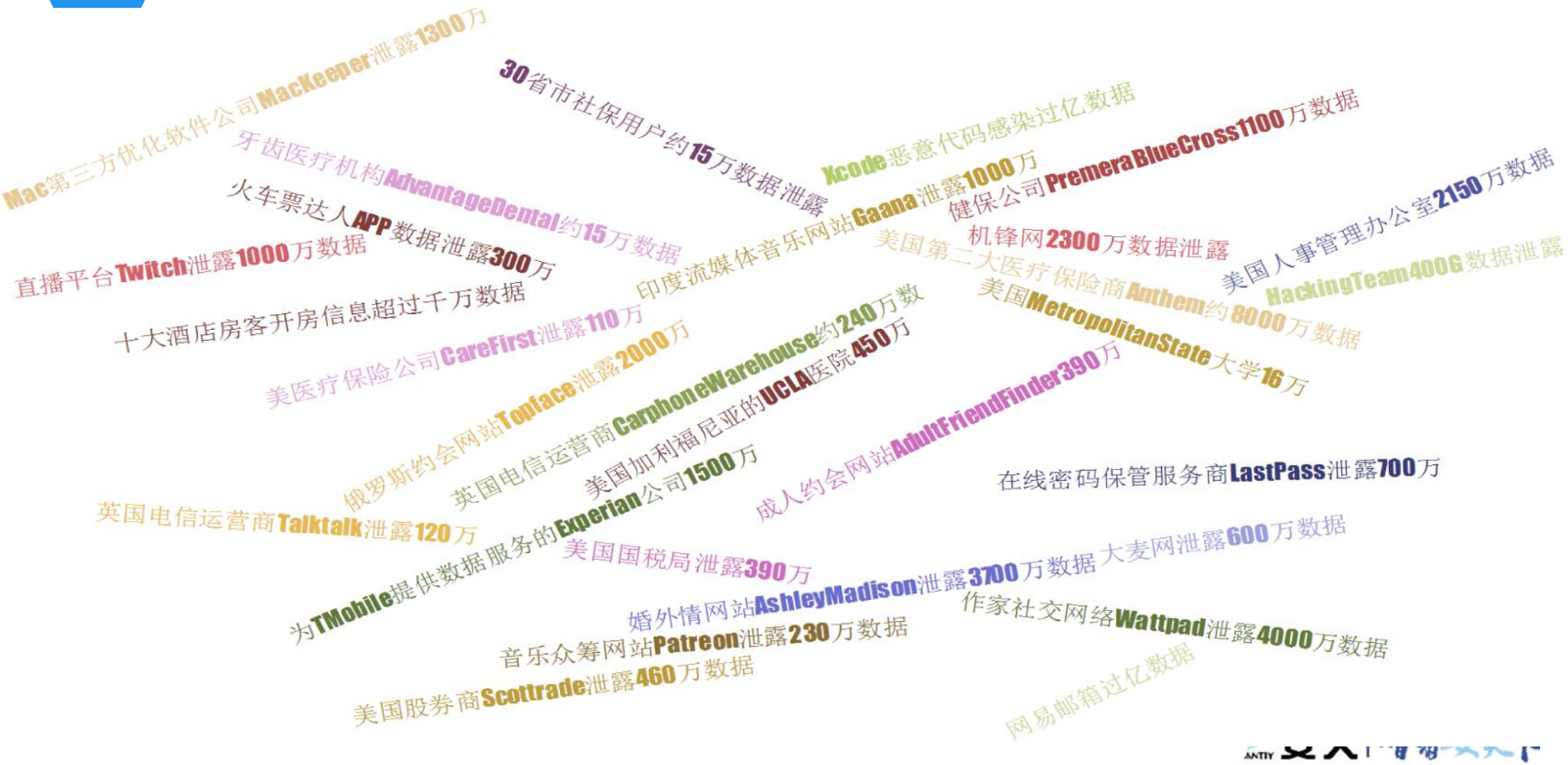
“幽灵”（Ghost）漏洞在2015年年初被发现，glibc是GNU发布的libc库，即c运行库。glibc是Linux系统中最底层的API，几乎其它任何运行库都会依赖于glibc。由于glibc除了封装Linux操作系统所提供的系统服务外，它本身也提供了许多其它一些必要功能服务的实现，所以“幽灵”漏洞几乎影响了所有linux操作系统，其影响力堪比“破壳”漏洞。

Adobe Flash的安全性一直被人诟病，被誉为“黑产军团的军火库”，向APT28等APT攻击中都利用了Adobe Flash的0day漏洞进行攻击，2015年全年Flash的漏洞更是多达300多条。Hacking Team的数据泄露事件，将Flash漏洞的危害性和影响力推到顶点，暴露出的三个漏洞几乎能够影响所有平台、所有版本的Flash。其中被发现的第二个漏洞（CVE-2015-5122）甚至被黑客团队戏称为“过去四年里最漂亮的Flash漏洞”。

年底，被称为“破坏之王”的Java反序列化漏洞爆发。早在2015年的1月28号，就有报告介绍了Java反序列化漏洞可以利用Apache Commons Collections这个常用的Java库来实现任意代码执行，可惜当时并没有引起太大的关注。其在WebLogic、WebSphere、JBoss、Jenkins、OpenNMS中均能实现远程代码执行，获取权限后将泄漏数据库。该漏洞被曝出9个月后依然没有发布有效的补丁，使其危害影响时间更加长。目前，根据安天CERT的安全服务来看，大量政府门户网站和信息管理系统受反序列化漏洞的影响十分严重，目前受影响最大的是WebLogic和Jboss两个应用服务器。

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Mac Os X	Apple	OS	384
2	Iphone Os	Apple	OS	375
3	Flash Player	Adobe	Application	314
4	Air Sdk	Adobe	Application	246
5	AIR	Adobe	Application	246
6	Air Sdk & Compiler	Adobe	Application	246
7	Internet Explorer	Microsoft	Application	231
8	Chrome	Google	Application	187
9	Firefox	Mozilla	Application	178
10	Windows Server 2012	Microsoft	OS	155
11	Ubuntu Linux	Canonical	OS	152
12	Windows 8.1	Microsoft	OS	151
13	Windows Server 2008	Microsoft	OS	149
14	Windows 7	Microsoft	OS	147
15	Windows 8	Microsoft	OS	146
16	Windows Rt 8.1	Microsoft	OS	139
17	Windows Rt	Microsoft	OS	138
18	Windows Vista	Microsoft	OS	135
19	Safari	Apple	Application	135
20	Android	Google	OS	130

数据泄露事件


Mac第三方优化软件公司MacKeeper泄露1300万
30省市社保用户约15万数据泄露
牙齿医疗机构AdvantageDental约15万数据
Xcode恶意代码感染过亿数据
健保公司PremeraBlueCross1100万数据
火车票达人APP数据泄露300万
直播平台Twitch泄露1000万数据
印度流媒体音乐网站Gaana泄露1000万
美国第二大医疗保险商Anthem约8000万数据
机锋网2300万数据泄露
美国人事管理办公室2150万数据
十大酒店房客开房信息超过千万数据
美医疗保险公司CareFirst泄露110万
HackingTeam400G数据泄露
俄罗斯约会网站Topface泄露2000万
英国电信运营商CarphoneWarehouse约240万数
美国加利福尼亚的UCLA医院450万
美国MetropolitanState大学16万
成人约会网站AdultFriendFinder390万
英国电信运营商Talktalk泄露120万
为TMobile提供数据服务的Experian公司1500万
在线密码保管服务商LastPass泄露700万
美国国税局泄露390万
婚外情网站AshleyMadison泄露3700万数据
大麦网泄露600万数据
音乐众筹网站Patreon泄露230万数据
作家社交网络Wattpad泄露4000万数据
美国股券商Scottrade泄露460万数据
网易邮箱过亿数据

安天2015对外公开报告

DDoS攻击组织肉鸡美眉分析

方程式（EQUATION）部分组件中的加密技巧分析

- ✓ IIS再出远程执行漏洞：警惕新红色代码
- ✓ "攻击WPS样本"实为敲诈者

•部分利用社工技巧的群发邮件样本关联分析

- ✓ 利用路由器传播的DYREZA家族变种分析
- ✓ 黑客用HFS搭建服务器来传播恶意代码
- ✓ Xcode非官方版本恶意代码污染事件（XcodeGhost）的分析与综述
- ✓ 疯狂的窃密者——TEPFER

ROVNIX攻击平台分析-利用WordPress平台传播的多插件攻击平台

修改硬盘固件的木马 探索方程式（EQUATION）组织的攻击组件

- ■ 短信拦截马"相册"综合分析报告
- ■ 一例针对中方机构的准APT攻击中所使用的样本分析

- ◆ 揭开勒索软件的真面目
- ◆ 采用多种沙箱识别技术的Kasidet家族分析
- ◆ VBA病毒"制造机"正在流行

- ◆ 邮件发送js脚本传播敲诈者木马的分析报告
- ◆ 一例以"采访"为社工手段的定向木马攻击分析

Part 02

典型安全事件回顾

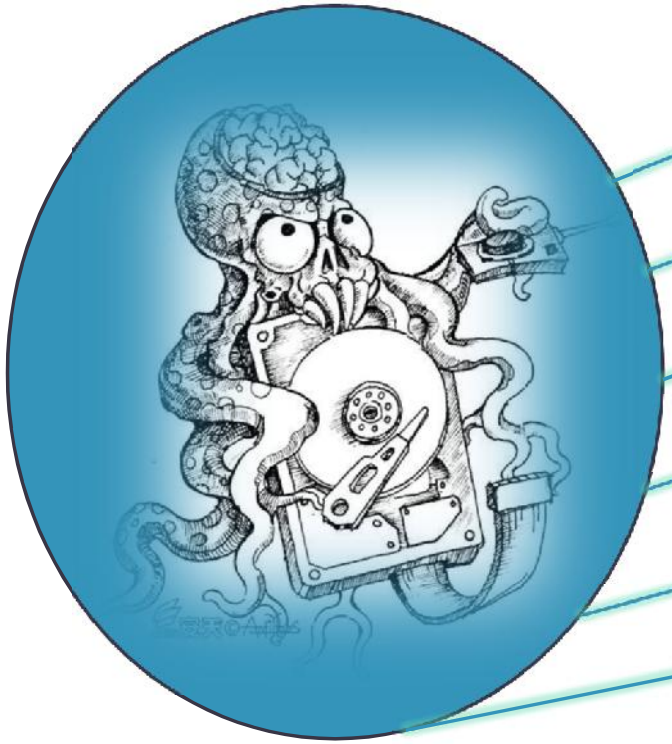
- 最复杂的攻击组织回顾
- 一例准APT事件回顾
- “谁”绑架了文件回顾
- 供应链污染事件回顾

Part 02

最复杂的攻击组织回顾

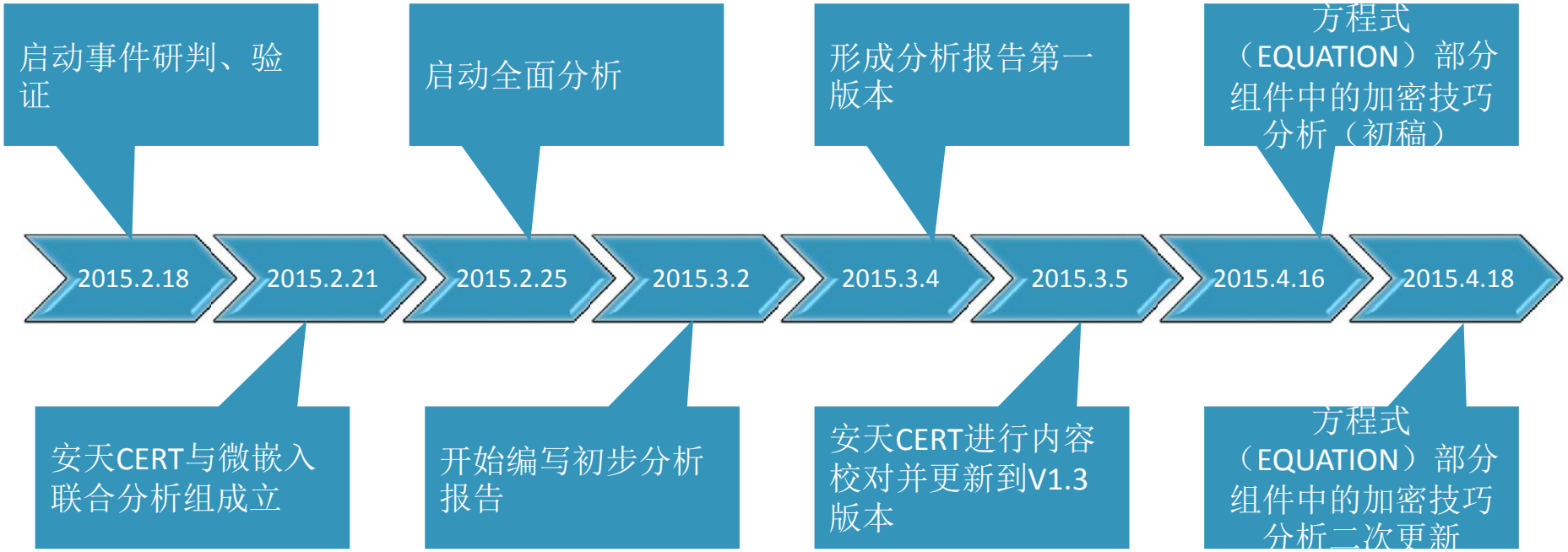
- 方程式特点
- 响应过程
- 组件相关示意图
- 修改硬盘固件的流程
- 需要思考的问题

方程式特点

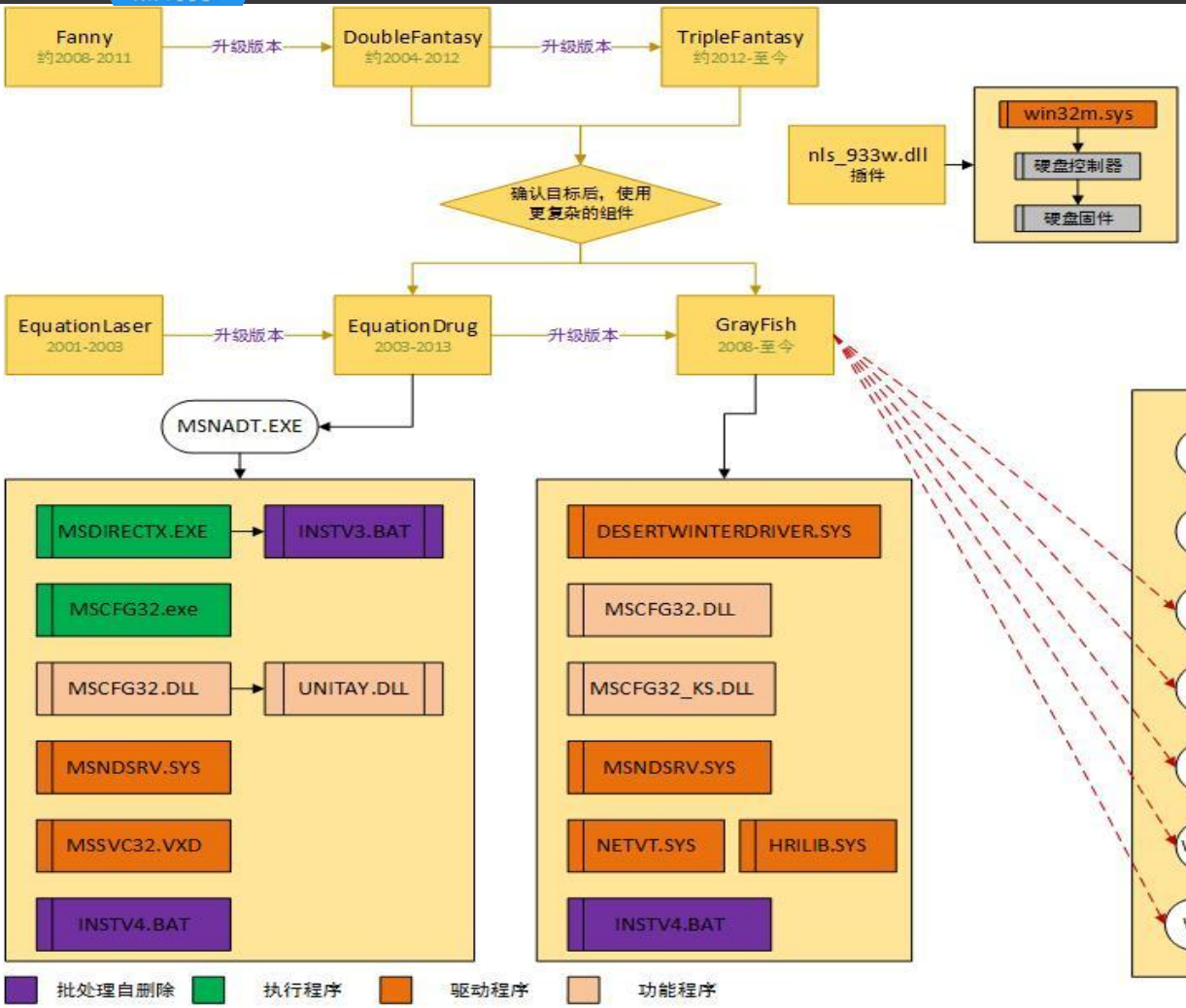


- 具有硬盘固件改写能力
- 至少包含6个组件
- 13个主版本，若干小版本
- 无文件实体（利用注册表）
- 借助bootkit加载
- 潜伏近20年，多平台攻击

响应过程


启动事件研判、验证
启动全面分析
形成分析报告第一版本
方程式（EQUATION）部分组件中的加密技巧分析（初稿）
2015.2.18
2015.2.21
2015.2.25
2015.3.2
2015.3.4
2015.3.5
2015.4.16
2015.4.18
安天CERT与微嵌入联合分析组成立
开始编写初步分析报告
安天CERT进行内容校对并更新到V1.3版本
方程式（EQUATION）部分组件中的加密技巧分析二次更新

组件关系示意图



了解Equation方程式APT组织的信息武器库

Equation方程式组织拥有一套用于植入恶意代码的超级信息武器库，卡巴斯基在在2月16日开始进行了系列报道，其中针对硬盘固件进行重编程的恶意代码，是首次出现，也是恶意代码中首个能进行固件重写的功能被发现。这里结合卡巴斯基与安天的结分结果，进行方程式组织信息武器库的展示与纰漏。

修改硬盘固件的流程

nls_933w.dll的导出函数

- nls_933w_1 (0x100013F4)：获取实现硬盘操作功能的函数指针
- nls_933w_2 (0x100013DD)：传入参数、解密一个注册表键
- nls_933w_3 (0x100013F0)：用于测试接口函数是否可正常调用，只是返回1
- nls_933w_4 (0x10001408)：获取文件的版本号（0x30，0x00，0x01，0x10000）
- nls_933w_5 (0x10001425)：获取插件的版本号（0x80AB）

Name	Address	Ordinal
nls_933w_1	100013F4	1
nls_933w_2	100013DD	2
nls_933w_3	100013F0	3
nls_933w_4	10001408	4
nls_933w_5	10001425	5
DllEntryPcint	10001DCE	

nls_933w.dll调用的接口编号及功能

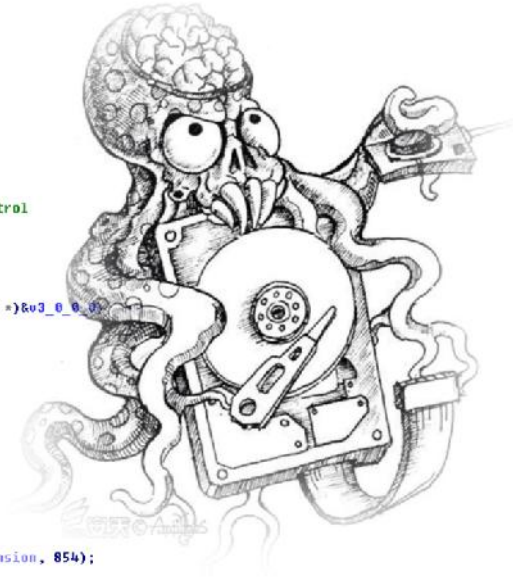
- 0x51：安装驱动程序并启动服务
- 0x52：卸载驱动程序删除服务
- 0x53：获取版本号
- 0x54：获取硬盘信息(序列号、固件版本等)
- 0x55：对指定序列号的硬盘进行写加密文件操作
- 0x56：对指定序列号的硬盘进行读解密文件操作
- 0x5F：驱动程序、初始化ATA指令操作
- 0x63：对指定序列号的硬盘执行ATA操作
- 0x60：清空并释放在内存中的一些全局指针结果

```
case 0x51:
  result = sub_10003470(a1, Memory);
  break;
case 0x52:
  result = sub_10003340(a1, Memory);
  break;
case 0x53:
  result = sub_10002CF0(a1, Memory);
  break;
case 0x64:
  result = sub_10002E30(a1, Memory);
  break;
case 0x54:
  result = sub_10003690(a1, Memory);
  break;
case 0x55:
  result = sub_10002FD0(a1, Memory);
  break;
case 0x62:
  result = sub_10003190(a1, Memory);
  break;
case 0x56:
  result = sub_10002890(a1, Memory);
  break;
case 0x61:
  result = sub_10002B40(a1, Memory);
  break;
case 0x57:
  result = sub_10002790(a1, Memory);
  break;
case 0x58:
case 0x59:
case 0x5A:
case 0x5B:
case 0x5C:
case 0x5D:
case 0x5E:
case 0x63:
  result = sub_10002350(a1, Memory);
  break;
case 0x5F:
  result = sub_10002000(a1, Memory);
  break;
case 0x60:
  result = sub_100022A0(a1, Memory);
  break;
default:
  result = 0x302;
  break;
```

操作磁盘控制器

- 0x87002100：读版本号
- 0x87002104：初始化硬盘控制器
- 0x87002108：检查C4初始化后驱动的状态
- 0x870021D0：操作硬盘控制器

```
goto LABEL_6;
}
CTL_CODE = *(_DWORD *)pCurrentStackLocation + 3);// Enter deviceIoControl
if ( CTL_CODE == 0x87002100                    // 读版本号
{
  if ( pBuffer && OutBufferSize >= 8 )
  {
    Irp->IoStatus.Information = 8;
    qmemcpy(pBuffer, decode((unsigned __int8 *)&temp, (unsigned __int8 *)&v3_0_0_0,
    goto LABEL_16;
  }
  ret = 0xC0000023;
}
else
{
  if ( CTL_CODE == 0x87002104 )                // 初始化硬盘控制器
  {
    if ( InBufferSize == 854 )
    {
      if ( *((_DWORD *)pDeviceExtension + 22) )
        goto LABEL_10;
      if ( Wait_TakeMutex(&Mutex) )
      {
        v12 = InitFunctionList_HookIRQL((int)pBuffer, (int)pDeviceExtension, 854);
        ReleaseMutex(&Mutex);
        v2 = Irp;
        if ( v12 )
          goto LABEL_10;
      }
      sub_1032((int)pDeviceExtension);
      goto LABEL_18;
    }
    goto LABEL_22;
  }
  if ( CTL_CODE == 0x87002108 )
  {
    sub_1082((int)pDeviceObject->DeviceExtension);
    goto LABEL_18;
  }
  if ( CTL_CODE == 0x870021CC )                // 检查C4初始化后驱动的状态
  {
    if ( !*((_DWORD *)pDeviceExtension + 24) )
      goto LABEL_20;
```



需要思考的问题

- 为什么该组织活跃了近20年之久才被发现？
- 该组织如何拿到硬件厂商ATA指令？
- 硬盘固件中篡改的内容是什么？

木马程序

导出PDF

"1b0eb1a1591140175d1ac111a98c89472b196599baf13ef67ee7f63d0052b00e.exe"分析报告

文件被 页面手工提交 发现，经由BD静态分析鉴定器、YARA自定义规则鉴定器、美国软件交叉索引(NSRL)鉴定器、数字证书鉴定器、可交换信息(EXIF)鉴定器、静态分析鉴定器、动态行为(默认环境)鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。
最终依据BD静态分析鉴定器、静态分析鉴定器、动态行为鉴定器、智能学习鉴定器、安全云鉴定器将文件判定为 木马程序 。
该文件具有以下行为：加载内核文件;其他进程写入可疑数据;从资源中释放PE文件到系统目录;创建特定窗体;请求调试权限;创建互斥体(mutex);篡改系统文件创建时间;请求加载驱动的权限;获取驱动器类型;独占打开文件;获取计算机名称;获取主机用户名称。

文件名：	1b0eb1a1591140175d1ac111a98c89472b196599baf13ef67ee7f63d0052b00e.exe
文件类型：	BinExecute/Microsoft.EXE[:X86]
大小：	372 KB
MD5：	4556CE5EB007AF1DE5BD3B457F0B216D
首次发现时间：	2016-01-08 19:50
末次发现时间：	2016-01-08 19:50
结果：	木马程序
恶意判定/病毒名称：	Trojan/Win32.EquationDrug
判定依据：	安全云

运行环境

操作系统	内置软件
Windows XP 5.1.2600 Service Pack 3 Build 2600	默认,IE6,Office 2003,Flash,WPS,FoxitReader,Adobe Reader

危险行为

行为描述：	加载内核文件	
附加信息：	LibFileName	ntkrnlpa.exe
危险等级：	★★★	

行为描述：	其他进程写入可疑数据	
附加信息：		
危险等级：	★★★	

行为描述：	从资源中释放PE文件到系统目录	
附加信息：	FilePath	C:\WINDOWS\system32\msnadt.exe
	FilePath	C:\WINDOWS\system32\MSDIRECTX.EXE
	FilePath	C:\WINDOWS\system32\MSCFG32.DLL
	FilePath	C:\WINDOWS\system32\MSCFG32.EXE
	FilePath	C:\WINDOWS\system32\drivers\MSNDSRV.SYS
危险等级：	★★★	

其他行为

行为描述：	创建特定窗体	
附加信息：	ClassName	STATIC
	WindowName	h
危险等级：	★	

行为描述：	请求调试权限	
附加信息：	Name	SeDebugPrivilege
危险等级：	★	

行为描述：	创建互斥体(mutex)	
附加信息：	Name	prkMtx
危险等级：	★	

行为描述：	篡改系统文件创建时间	
附加信息：	CreationTime	2008-4-14 12:0:0:0
	FilePath	C:\WINDOWS\system32\msnadt.exe
	CreationTime	2008-4-14 12:0:0:0
	FilePath	C:\WINDOWS\system32\MSDIRECTX.EXE
	CreationTime	2008-4-14 12:0:0:0
	FilePath	C:\WINDOWS\system32\MSCFG32.DLL
	CreationTime	2008-4-14 12:0:0:0
	FilePath	C:\WINDOWS\system32\MSCFG32.EXE
	CreationTime	2008-4-14 12:0:0:0
	FilePath	C:\WINDOWS\system32\drivers\MSNDSRV.SYS
危险等级：	★★	

行为描述：	请求加载驱动的权限	
附加信息：	Name	SeLoadDriverPrivilege
危险等级：	★	

行为描述：	获取驱动器类型	
附加信息：	RootPathName	C:\
危险等级：	★	

行为描述：	独占打开文件	
附加信息：	FileName	C:\WINDOWS\system32\msnadt.exe
	FileName	C:\WINDOWS\system32\MSCFG32.EXE
	FileName	C:\WINDOWS\system32\drivers\MSNDSRV.SYS
	FileName	C:\WINDOWS\system32\iosubsys\MSSVC32.VXD
	FileName	C:\WINDOWS\system32\MSLOG32.DAT
	FileName	C:\WINDOWS\system32\MSCFG32.DLL
危险等级：	★	

行为描述：	获取计算机名称	
附加信息：	Buffer	AZ
危险等级：	★	

行为描述：	获取主机用户名称	
附加信息：	NameBuffer	Administrator
危险等级：	★	

文件操作

操作	文件路径
新建	c:\windows\system32\msnadt.exe
重启删除	c:\target.exe
新建	c:\windows\system32\msdirectx.exe
新建	c:\windows\system32\mscfg32.dll
新建	c:\windows\system32\mscfg32.exe
新建	c:\windows\system32\drivers\msndsrv.sys
新建	c:\docume~1\admini~1\locals~1\temp\instv4.bat
新建	c:\docume~1\admini~1\locals~1\temp\instv3.bat

进程监控

PID : 1416	创建：C:\WINDOWS\system32\msnadt.exe
	命令行：(null)
PID : 1692	创建：MSDIRECTX.EXE
	命令行：C:\WINDOWS\system32\MSDIRECTX.EXE
PID : 528	创建：cmd.exe
	命令行：C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\INSTV4.BAT
PID : 1964	创建：C:\WINDOWS\system32\attrib.exe
	命令行：attrib -r "C:\WINDOWS\system32\msnadt.exe"
PID : 1372	创建：cmd.exe
	命令行：C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\INSTV3.BAT

进程衍生关系

- target.exe
  - (null)
    - C:\WINDOWS\system32\MSDIRECTX.EXE
      - C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\INSTV3.BAT
    - C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\INSTV4.BAT
      - attrib -r "C:\WINDOWS\system32\msnadt.exe"

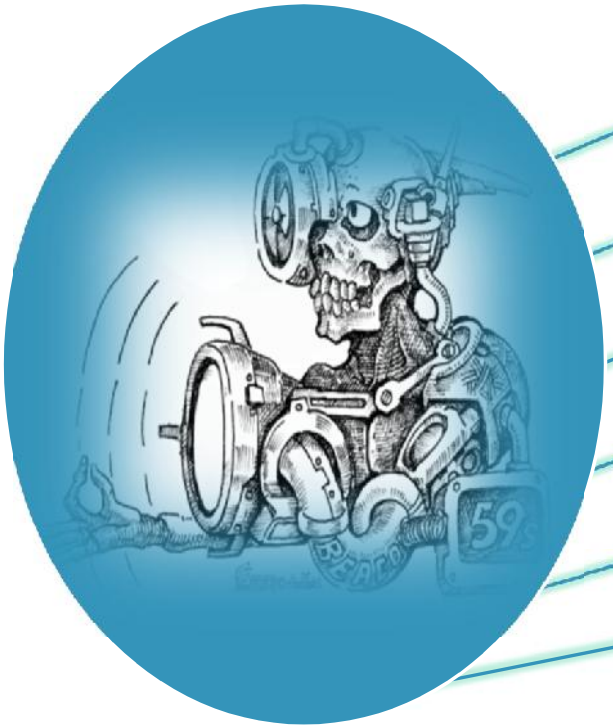
Part 02

一例准APT事件回顾

APT-TOCS

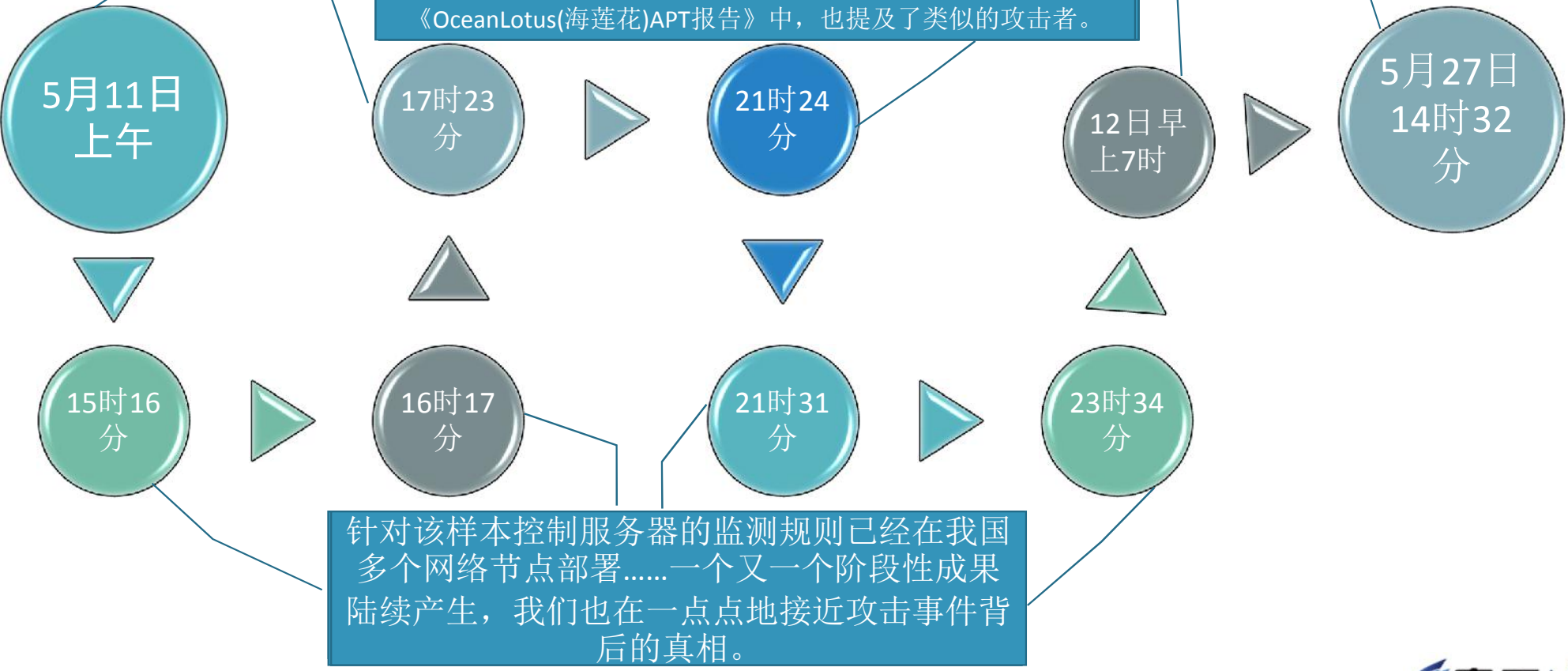
APT-TOCS是安天在今年**5**月发现一例针对中方机构的准**APT**攻击事件，安天**CERT**分析小组之所以将**APT-TOCS**事件定位为准**APT**事件，是因为该攻击事件一方面符合**APT**攻击针对高度定向目标作业的特点，同时隐蔽性较强、具有多种反侦测手段。

APT-TOCS特点



- PowerShell 脚本加载
- 加密算法简单： Base64编码、XOR
- 载荷为Shellcode形式
- 无文件实体（利用注册表）
- **借助bootkit加载**
- 通过Cookie发送心跳

响应过程


公开发布了分析报告（该报告可以在安天网站 www.antiy.com 下载），借此揭示境外攻击者的攻击手段，提醒我国重要机构提高警惕。该报告是我国较早出现的一篇公开揭示境外攻击者针对我国网络攻击手段的分析报告，在安全厂商360随后发布的《OceanLotus(海莲花)APT报告》中，也提及了类似的攻击者。
5月11日上午
17时23分
21时24分
12日早上7时
5月27日14时32分
15时16分
16时17分
21时31分
23时34分
针对该样本控制服务器的监测规则已经在我国多个网络节点部署.....一个又一个阶段性成果陆续产生，我们也在一点点地接近攻击事件背后的真相。

APT-TOCS原始样本

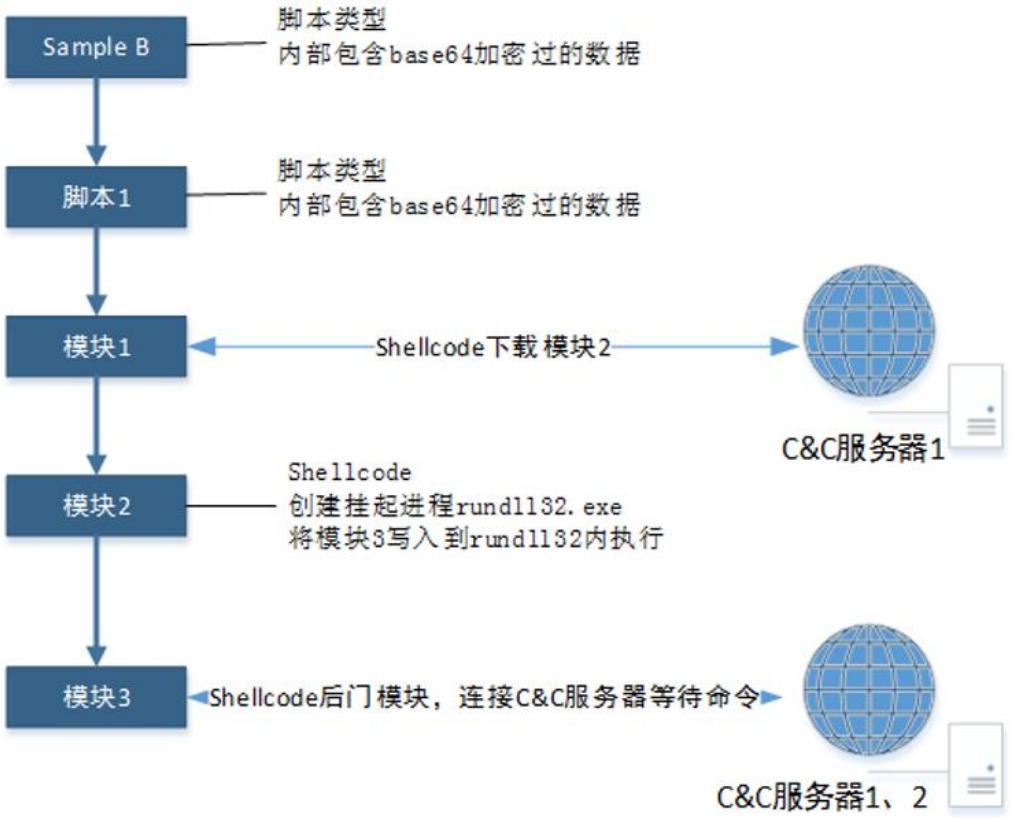
- 无实体文件
- 通过注册表启动后，调用powershell执行脚本

44BCF2DD262F12222ADEAB6F59B2975B

```
          0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00005300h: 70 6F 77 65 72 73 68 65 6C 6C 2E 65 78 65 20 2D ; powershell.exe -
00005310h: 65 78 65 63 20 62 79 70 61 73 73 20 2D 6E 6F 70 ; exec bypass -nop
00005320h: 20 2D 57 20 68 69 64 64 65 6E 20 2D 6E 6F 6E 69 ;  -W hidden -noni
00005330h: 6E 74 65 72 61 63 74 69 76 65 20 49 45 58 20 24 ; nteractive IEX $
00005340h: 28 24 73 3D 4E 65 77 2D 4F 62 6A 65 63 74 20 49 ; ($s=New-Object I
00005350h: 4F 2E 4D 65 6D 6F 72 79 53 74 72 65 61 6D 28 2C ; O.MemoryStream(,
00005360h: 5B 43 6F 6E 76 65 72 74 5D 3A 3A 46 72 6F 6D 42 ; [Convert]::FromB
00005370h: 61 73 65 36 34 53 74 72 69 6E 67 28 27 48 34 73 ; ase64String('H4s
00005380h: 49 41 4A 30 7A 52 56 55 43 41 35 31 56 58 55 2F ; IAJ0zRVUCA51VXU/
00005390h: 62 4D 42 52 39 37 36 2B 34 36 6A 4B 61 69 4D 5A ; bMBR976+46jKaiMZ
000053a0h: 4B 30 53 6F 42 55 74 45 67 77 49 62 45 6F 46 6F ; K0SoBUtEgwIbEoFo
000053b0h: 37 38 56 42 56 77 6B 30 75 4E 43 4F 31 4D 38 66 ; 78VBVwk0uNCO1M8f
000053c0h: 70 68 34 44 2F 50 6A 74 78 50 71 43 67 54 65 51 ; ph4D/PjtxPqCgTeQ
```

APT-TOCS执行流程

- 脚本解密shellcode并执行



碰到的问题

难以取证

1、无恶意代码进程（该恶意脚本是借用powershell来运行的，因此进程为powershell，并非恶意）

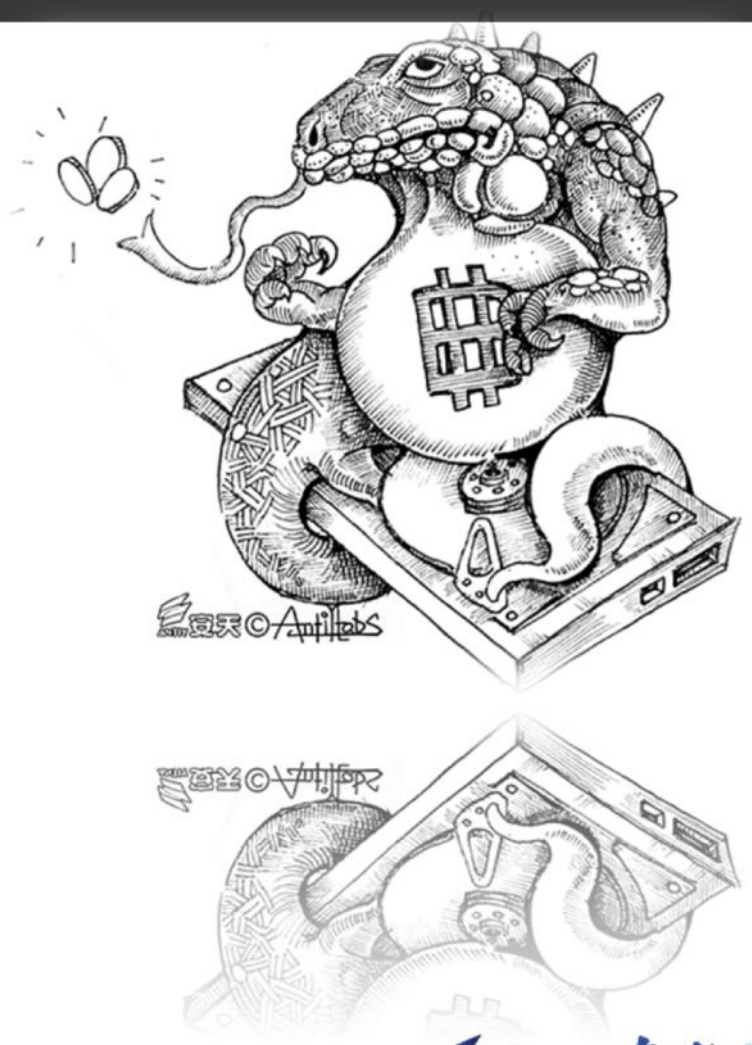
2、无文件实体（脚本可以保存在注册表中，可以躲避杀软的查杀）

3、技术难度低（借助Cobalt Strike来生成shellcode，在脚本中可以很方便的进行shellcode的替换）

Part 02

“谁”绑架了文件回顾

揭开勒索软件的真面目



何谓勒索软件

勒索软件（ransomware）是一种流行的木马，通过骚扰、恐吓甚至采用绑架用户文件等方式，使用户数据资产或计算资源无法正常使用，并以此为条件向用户勒索钱财。这类用户数据资产包括文档、邮件、数据库、源代码、图片、压缩文件等多种文件。赎金形式包括真实货币、比特币或其它虚拟货币。一般来说，勒索软件作者还会设定一个支付时限，有时赎金数目也会随着时间的推移而上涨。有时，即使用户支付了赎金，最终也还是无法正常使用系统，无法还原被加密的文件。

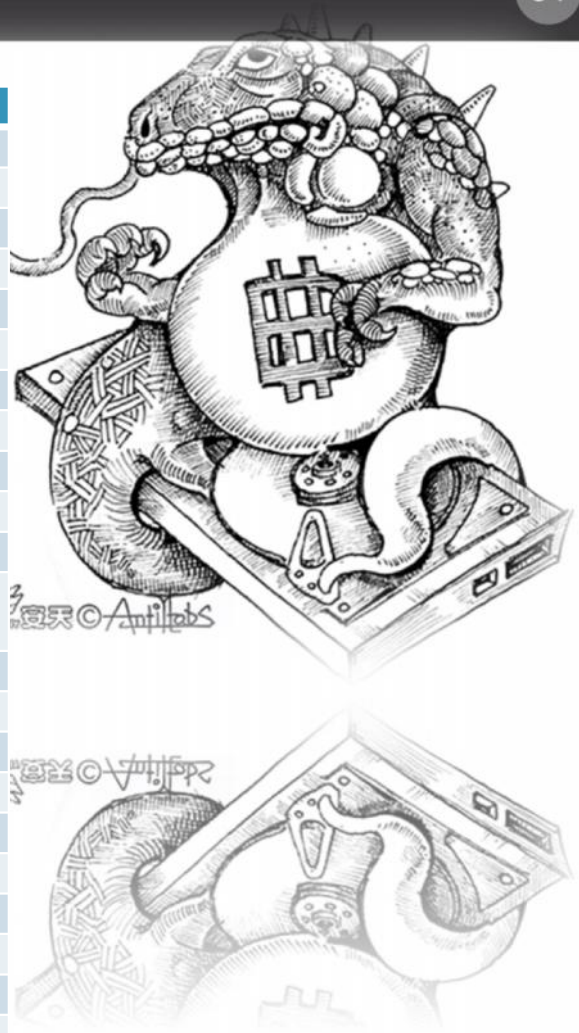
主要传播手段

勒索软件的传播手段与常见的木马非常相似，主要有以下几种：

- 借助网页木马传播，当用户不小心访问恶意网站时，勒索软件会被浏览器自动下载并在后台运行
- 与其他恶意软件捆绑发布
- 作为电子邮件附件传播
- 借助可移动存储介质传播

勒索软件的分类

方式	具体行为	平台	其它名称
影响使用	锁定系统屏幕	Windows	QiaoZhaz
		Android	DevLockeer
			Koler
			Locker
	修改文件关联	Windows	QiaoZhaz
	拦截手机来电	Android	Cokri
	色情无限弹窗	Android	Koler
	伪装色情应用	Android	simplelock
恐吓用户	伪装杀毒软件	Windows	FakeAV
		Android	Svpeng
			simplelock
	伪装当地执法机构	Windows	Reveton
绑架数据	隐藏用户文件	DOS	PC Cyborg
		Windows	Redplus
	删除用户文件	Windows	QiaoZhaz
		Android	Koler
	加密用户文档数据	Windows	CTB-Locker
			CrytoLocker
			Locker
		Android	simplelock
		Android	Koler
	加密通讯录	Android	Cokri



20多年的演进史

1987年 反病毒软件登上历史舞台

1987

1989
1989.6 PC Cyborg

2001
2001.2 FakeAV

仿装反病毒软件

2005
2005.5 Gpcode

2006
2006.5CRYZIP
2006.6Redplus

2007
2007.3 QiaoZhaz

2008年 第一款运行Android系统的商用智能手机发布

2008

2009年 比特币被发明

2009

勒索

运行于

2012
2012.8 REVETON

2013
2013.9 CryptoLocker
2013.9 Dirty Decrypt
2013.12 Cryptorbit
2013.12 Cryptographic locker

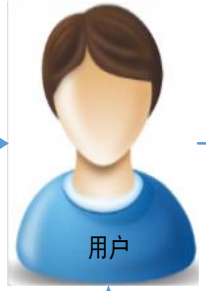
2014
2014.2 CryptoDefense
2014.4 CryptoWall Ransomware
2014.4 Koler （安卓平台）
2014.5 KOVTER
2014.5 simplelock （安卓平台）
2014.6 Cokri （安卓平台）
2014.7 CTB-Locker
2014.8 TorrentLocker
2014.10 VIRLOCK
2014.11 Locker
2014.11 CoinVault
2014.11 Svpeng （安卓平台）

2015
2015.1Cryptowall
2015.2 TeslaCrypt
2015.4 Alpha Crypt
2015.4 DevLockeer （安卓平台）
2015.4 Locker （安卓平台）

CTB-Locker攻击流程与执行过程

发送邮件

用户收到邮件



查收邮件

CTB-Locker运行

加密用户数据

弹出敲诈信息

敲诈用户

用户付费

攻击者获取收益


安天安全文档工具
文档安全
全面保护文档安全
实时保护已开启
已阻止0次非授权文档访问
进程名
文件名
访问时间
访问次数
操作
没有内容
文档保护
已开启
全盘锁定
已开启
重要文档1
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
转到
我的电脑
开始
重要文档1
重要文档2
安天安全文档工具
12:26

防御：我该做什么

安全建议

- 及时备份重要文件
- 及时安装更新补丁，避免一些勒索软件利用漏洞感染计算机
- 给信任网站添加书签并通过书签访问
- 对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接
- 定期用反病毒软件扫描系统

通过不段分析研究安天开发出防敲诈者的软件

请看视频（视频1）

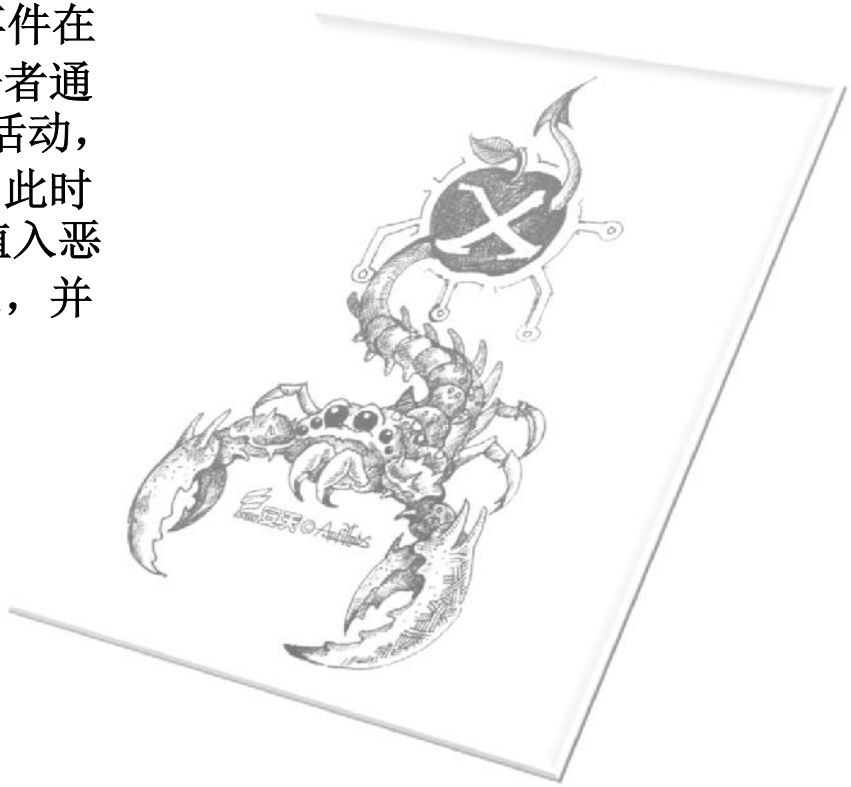
Part 02

供应链污染事件回顾

- 背景介绍
- 响应过程
- Xcode供应链污染事件示意图
- Xcode供应链污染事件危害
- Xcode事件时间链

Xcode非官方供应链污染事件背景

自2015年9月14日起，一例Xcode非官方供应链污染事件在国家互联网应急中心发布预警后，被广泛关注。攻击者通过对Xcode进行篡改，加入恶意模块，进行各种传播活动，使大量开发者获取到相关上述版本，建立开发环境，此时经过被污染过的Xcode版本编译出的App程序，将被植入恶意逻辑，其中包括向攻击者注册的域名回传若干信息，并可能导致弹窗攻击和被远程控制的风险。



响应过程

2015年09月18号

18号12时

19号16时

20号22时

22号-28号

18号9时

19号10时

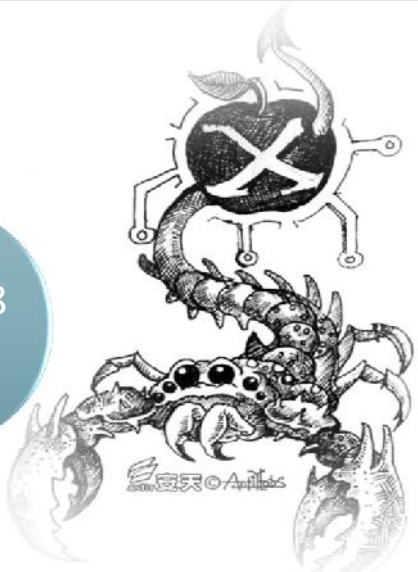
20号18时

21号

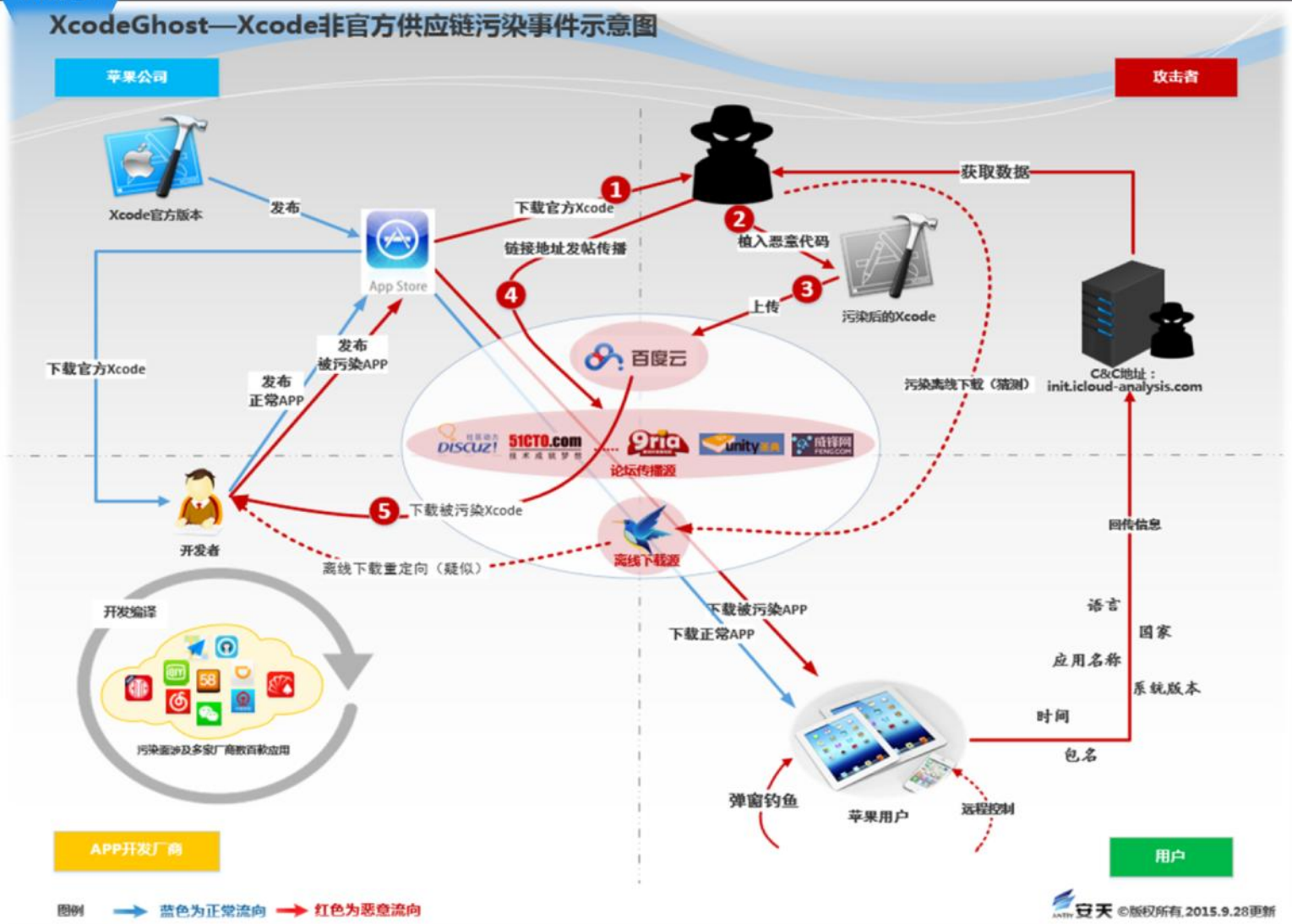
完成Xcode非官方版本恶意代码污染事件（XcodeGhost）的分析与综述并报送了各管理部门。

后续的几天里我们又增加了Android风险预警、还有“我们的检讨”，和附录等信息

完善了作用机理中样本相关分析，增加了开发环节的安全问题部分等。



Xcode非官方供应链污染事件示意图



安天 | 智者安天下

Xcode非官方供应链污染事件危害

上传隐私

```
objc_retain(v42);
v43 = v41;
v44 = objc_msgSend(
        &OBJC_CLASS___NSDictiona
        "dictionaryWithObjectsA
        v55,
        CFSTR("timestamp"),
        v56,
        CFSTR("app"),
        v57,
        CFSTR("bundle"),
        v58,
        CFSTR("name"),
        v54,
        CFSTR("os"),
        v53,
        CFSTR("type"),
        v51,
        CFSTR("status"),
        v52,
        CFSTR("language"),
        v49,
        CFSTR("country"),
        v33,
        CFSTR("idfv"),
        v42,
        CFSTR("network"),
        v41,
        CFSTR("version"),
```

```
v4 = objc_msgSend(&OBJC_CLASS___NSBundle, "mainBundle");
v6 = (void *)objc_retainAutoreleasedReturnValue(v4);
v5 = objc_msgSend(v5, "bundleIdentifier");
v7 = (void *)objc_retainAutoreleasedReturnValue(v6);
objc_release(v5);
v8 = objc_msgSend(v7, "stringByAppendingString:", CFSTR("~"));
v9 = (void *)objc_retainAutoreleasedReturnValue(v8);
objc_release(v7);
v10 = objc_msgSend(v9, "stringByAppendingString:", CFSTR("i"));
v11 = (void *)objc_retainAutoreleasedReturnValue(v10);
objc_release(v9);
v12 = objc_msgSend(v11, "stringByAppendingString:", CFSTR("O"));
v13 = (void *)objc_retainAutoreleasedReturnValue(v12);
objc_release(v11);
v14 = objc_msgSend(v13, "stringByAppendingString:", CFSTR("S"));
v15 = (void *)objc_retainAutoreleasedReturnValue(v14);
objc_release(v13);
v16 = objc_msgSend(v15, "stringByAppendingString:", CFSTR("~"));
v17 = (void *)objc_retainAutoreleasedReturnValue(v16);
objc_release(v15);
v18 = objc_msgSend(v17, "stringByAppendingString:", CFSTR("UIPasteboard"));
v19 = objc_retainAutoreleasedReturnValue(v18);
objc_release(v17);
v20 = objc_msgSend(&OBJC_CLASS___UIPasteboard, "pasteboardWithName:create:", v19, 1);
v21 = (void *)objc_retainAutoreleasedReturnValue(v20);
objc_msgSend(v21, "setPersistent:", 1);
objc_msgSend(v21, "setString:", v3);
objc_release(v3);
```

任意弹窗

```
goto LABEL_37;
v73 = objc_msgSend(v15, v134, CFSTR("alertHeader"));
v74 = objc_retainAutoreleasedReturnValue(v73);
v75 = objc_msgSend(v15, v134, CFSTR("alertBody"));
v76 = objc_retainAutoreleasedReturnValue(v75);
v77 = objc_msgSend(v15, v134, CFSTR("appID"));
v124 = objc_retainAutoreleasedReturnValue(v77);
v78 = objc_msgSend(v15, v134, CFSTR("cancelTitle"));
v79 = objc_retainAutoreleasedReturnValue(v78);
v126 = v15;
v80 = objc_msgSend(v15, v134, CFSTR("confirmTitle"));
v81 = objc_retainAutoreleasedReturnValue(v80);
v82 = objc_msgSend(&OBJC_CLASS___UIApplication, "sharedApplication");
v83 = (void *)objc_retainAutoreleasedReturnValue(v82);
v84 = objc_msgSend(v83, "applicationState");
```

远控模块

```
v66 = objc_msgSend(&OBJC_CLASS___UIApplication, "sharedApplication");
v67 = (void *)objc_retainAutoreleasedReturnValue(v66);
v134 = v17;
v68 = objc_msgSend(v62, v17, CFSTR("scheme"));
v15 = v62;
v69 = objc_retainAutoreleasedReturnValue(v68);
v70 = objc_msgSend(&OBJC_CLASS___NSURL, "URLWithString:", v69);
v71 = objc_retainAutoreleasedReturnValue(v70);
v72 = (unsigned int)objc_msgSend(v67, "canOpenURL:", v71);
objc_release(v71);
```

Xcode事件响应时间链

发帖时间	厂商与机构	行动
2012-12-29 13:17:07（最后编辑2015-6-15）	威锋网	Xcode最全版本下载，Xcode7以及Xcode6全系列
2015-03-16 11:49	unity圣典	最全Xcode各版本网盘超快下载！！【求加精】
2015-3-24 16:55:59	9ria论坛	Xcode最全版本下载
2015-4-9 18:56	51CTO论坛（百度快照地址）	Xcode 6、Xcode 7全系列，百度网盘下载地址
2015-6-15 09:43:06	威锋网	Xcode最全版本下载，Xcode 7 以及Xcode 6 系列等
2015-09-14	CNCERT/CC	关于使用非苹果官方XCODE存在植入恶意代码情况的预警通报
2015-09-17 16:00	PaloAlto Networks	Novel Malware XcodeGhost Modifies Xcode, Infects Apple iOS Apps and Hits App Store
2015-09-17 17:43	乌云	Xcode编译器里有鬼 – XcodeGhost样本分析
2015-09-18 11::05	PaloAlto Networks	Malware XcodeGhost Infects 39 iOS Apps, Including WeChat, Affecting Hundreds of Millions of Users
2015-09-18 13:45	PaloAlto Networks	Update: XcodeGhost Attacker Can Phish Passwords and Open URLs through Infected Apps
2015-09-18 17:01:01	360	已知有后门的iOS App
2015-09-18 21:32:35	360	Xcode木马样本分析及被挂马的红包插件
2015-09-19 凌晨3点左右	XcodeGhost-Author	"XcodeGhost" Source 关于所谓”XcodeGhost”的澄清
2015-09-19 04:40	XcodeGhost-Author 作者微博	作者声明
2015-09-19 05:43	看雪gjden	发一个批量检测Xcode ghost病毒的检测工具
2015-09-19	T00ls	T00ls首发被植入XcodeGhost病毒的国内IOS应用列表清单，各

Part 03

2016网络安全展望

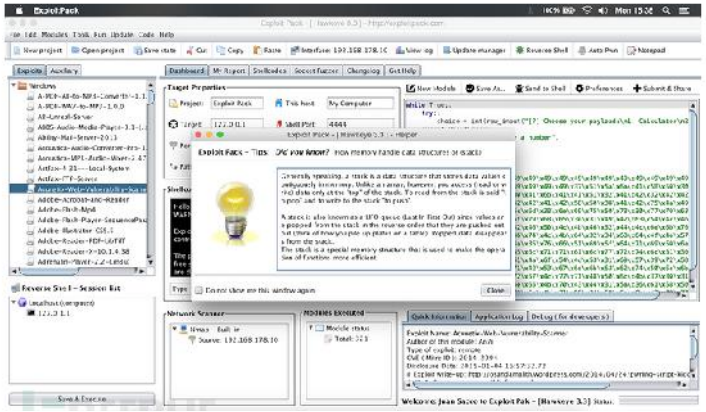
- 对网络安全预测

网络攻击武器-集成化攻击平台（军火库）

集成化的攻击平台

- 入门简单
- 可自定义插件
- 可自定义exploits、shellcode
- 反弹shell和权限提升

开源漏洞利用测试（Exploit）平台 – Exploit Pack



黑产“金钱”目的更加直接

POS机上的恶意代码

ATM机上的恶意代码

勒索软件

短信欺诈

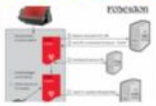
有哪里可以逃过POS机恶意软件的威胁？- 推酷

2014年12月29日 - 我们都应该记得,大约在去年的这个时候,美国零售商Target发生了有史以来最大的资料外泄事件,一起使用BlackPOS机恶意软件的针对性攻击。从那时开始,销售终...
www.tuicool.com/articl... - 百度快照 - 评价

Target数据泄漏调查,揭秘POS恶意软件 - IT经理网

在Target数据泄漏事件中,攻击者利用恶意软件感染门店的POS系统从而捕获用户的借记卡和信用卡的消费信息。那么,攻击者采用的是什么恶意软件?如何实施攻击?...
www.ctocio.com/ccnews/... - 百度快照 - 评价

小心中招 POS机严重新型恶意软件肆虐-ZOL科技频道



2015年3月25日 - PoSeidon 可以说是银行木马程序"Zeus"和 POS 恶意软件"BlackPOS"的结合体,这两种恶意软件的杀伤力究竟有多大,看看美国 Target、Home Depot 近两年...
news.zol.com.cn/articl... - 百度快照

揭秘:针对PoS机的恶意软件工具箱 - FreeBuf.COM | 关注黑客与极客

最近两年,PoS恶意软件由于塔吉特、家得宝、Kmart遭遇的POS机攻击而被广泛关注。随着"黑色星期五"购物季的到来,PoS机恶意软件必定会受到关注。PoS...
www.freebuf.com/news/s... - 百度快照 - 97%好评

POS机发现新恶意程序 能逃过55个杀毒软件_科技_腾讯网

2014年11月29日 - POS机发现新恶意程序 能逃过55个杀毒软件 POS系统中未加密信用卡数据面临被盗威胁。
tech.qq.com/a/20141129... - 百度快照 - 85%好评

定期自我更新!POS机恶意软件Punkey曝光_网络安全软...太平洋电脑网

2015年4月16日 - 外媒消息,安全服务公司Trustwave近期发现了一款名为"Punkey"的POS机恶意软件,并已感染了超过75个活跃的IP地址。Trustwave表示,他们还无法计算出被感染...
network.pconline.com.c... - 百度快照 - 评价

新型恶意软件攻击POS机_安全_cnBeta.COM

2015年4月16日 - 安全服务公司Trustwave已经发现了攻击POS机的新款恶意软件。Trustwave发现这款名为"Punkey"的恶意软件已经感染了超过75个活跃的受害者IP地址。Trust...
www.cnbeta.com/article... - 百度快照 - 82%好评

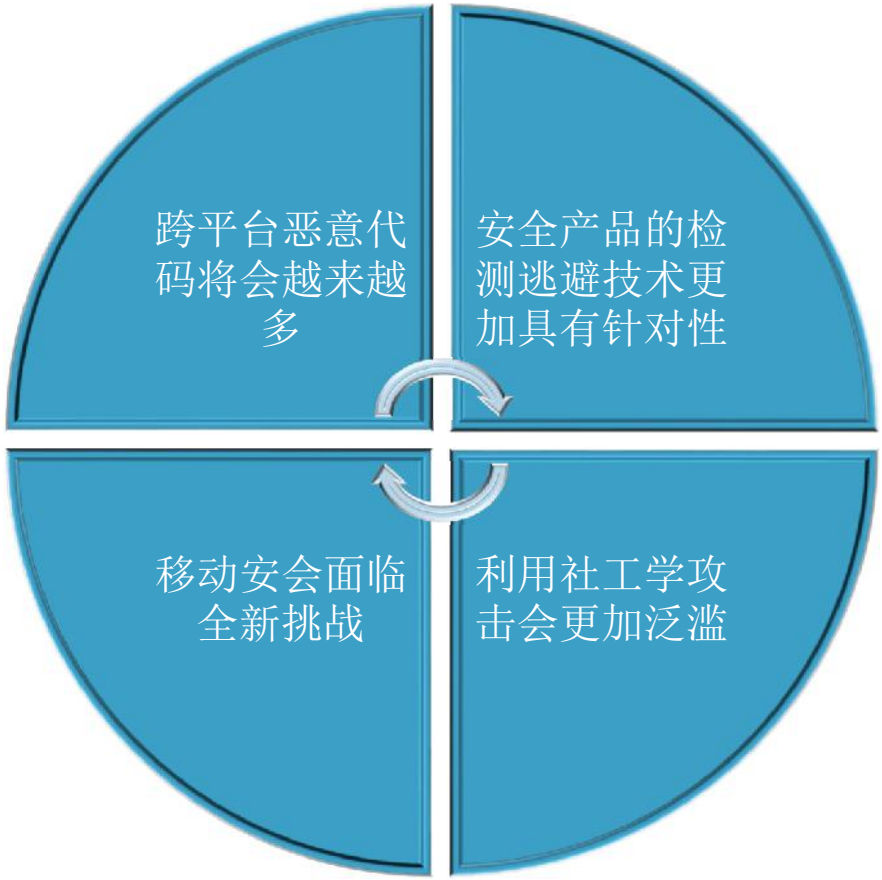
小心中招!POS机严重新型恶意软件肆虐_POS机_病毒_恶意软件_科技...

2015年3月25日 - POS 机是黑客长期以来虎视眈眈的目标之一,最近一种名为"PoSeidon"的新型恶意软件出现了,在复杂性和难缠性上达到了一个新高度。PoSeidon 通过...
tech.weiphone.com/2015... - 百度快照 - 77%好评

第三方供应商将成为攻击目标

- 供应商将遭受更多的攻击
- 设备出厂预安装恶意代码
- 第三方硬件中的后门程序
- 第三方APP存在漏洞

其它安全趋势


跨平台恶意代码将会越来越多
安全产品的检测逃避技术更加具有针对性
移动安会面临全新挑战
利用社工学攻击会更加泛滥

谢谢大家

THANK YOU FOR YOUR ATTENTION


刘佳男


13946012163


ljn@antiy.cn


pluckljn