翰海源

VULNHUNT

那些企业网络中的未知威胁、未知攻击事件

翰海源 王伟
微博 _alert7_

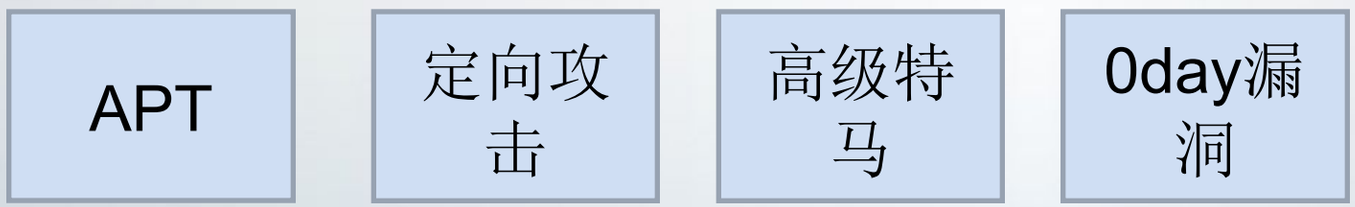
内容概要

- 未知威胁/未知攻击
- 著名/非著名的APT/未知攻击事件
- 新一代网络威胁下传统安全软件的弊端
- 未知威胁检测手段
- 翰海源未知威胁/攻击解决方案
- 翰海源捕获的攻击事件

未知威胁/未知攻击

- 2010前 传统木马/蠕虫攻击时代
  - 传统防御产品
    - 杀软
    - IDS/IPS
    - WAF
    - Firewall
    - 漏洞扫描等
- 2010后 进入APT时代

  随着**APT、定向攻击、高级特马、0day漏洞**攻击等**新一代网络威胁**日益增多，传统防御产品在面对新型网络威胁前失效，这些威胁和攻击来说对传统产品来讲都是未知的。



内容概要

- 未知威胁/未知攻击
- 著名/非著名的APT/未知攻击事件
- 新一代网络威胁下传统安全软件的弊端
- 未知威胁检测手段
- 翰海源未知威胁/攻击解决方案
- 翰海源捕获的攻击事件

APT概述

- 安全威胁近些年来发生巨大的变化，黑客攻击从传统带有恶作剧与技术炫耀性质逐步转变为利益化、商业化、政治化。

- APT是advanced persistent threat的缩写，译为高级持续性威胁。它是指近年来,专业且有组织的黑客（甚至可能有国家背景支持），针对重要目标和系统发起的一种攻击手段

- APT攻击是未知威胁、未知攻击的高级形态。在APT之下，还有更多的未知威胁/未知攻击的事件

APT攻击典型案例

2010：震网攻击伊朗核电站

2009：极光攻击

2011：窃取RSA令牌种子

2011：夜龙

2012：火焰

金融行业-攻击事件1

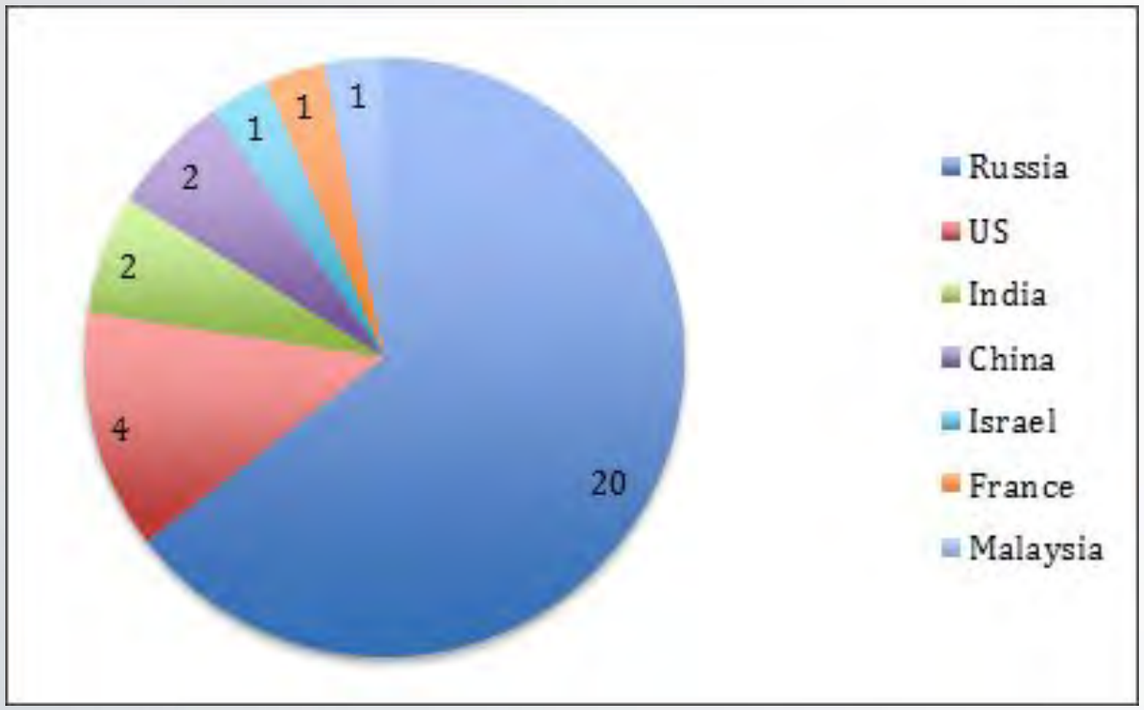
- 韩国银行及广播电视网攻击事件
  - 活动时间：2013年3月20日
  - 受害者：韩国农协银行及广播电视网 （领域：金融、广播）
  - 影响：损毁主开机记录(MBR)，抹除硬盘所有资料，破坏了48700台计算机。银行无法交易；无法进行新闻播报
  - 绕过防护：针对韩国的安博士软件，进行躲避
  - 类型：破坏型攻击，不回连C&C，不窃取信息

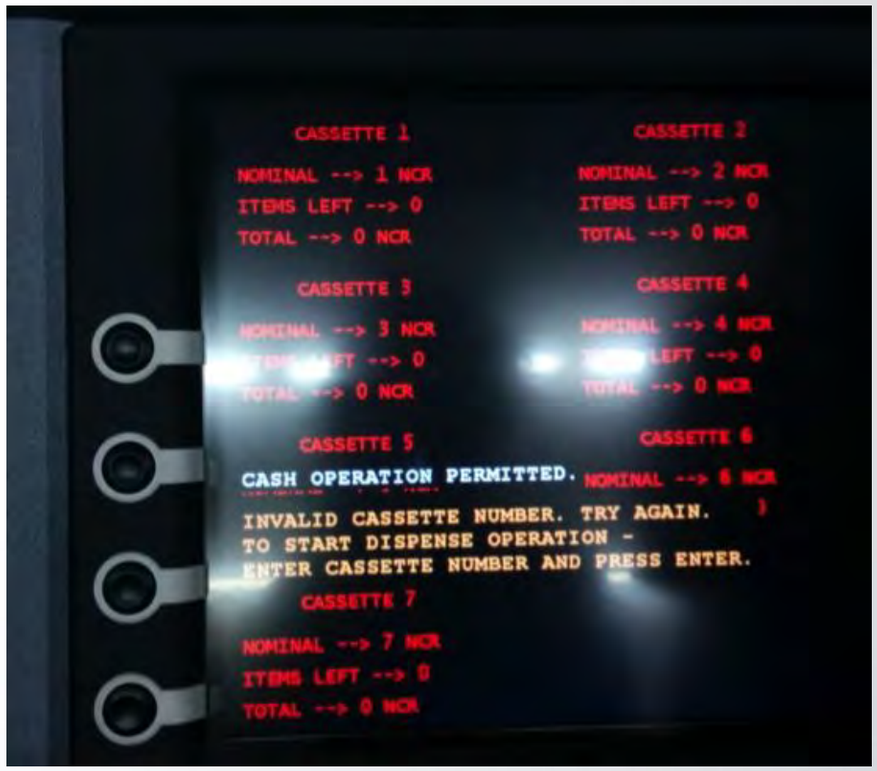
金融行业-攻击事件2

- 对ATM机的攻击（tyupkin）
  - 活动时间：2014年年初
  - 受害者：东欧银行机构所属的超过50台ATM机
  - 影响：攻击者直接操控ATM机，掏空ATM机上的现金
  - 发现者：卡巴斯基

金融行业-攻击事件2

- 该恶意软件活跃在东欧银行机构所属的超过50个ATM机上。根据提交到VirusTotal的数据，我们相信该恶意软件已经传播到其他几个国家，包括美国、印度和中国。





金融行业-攻击事件3

- 对金融POS机系统的攻击（brutpos）
  - 报道时间：2014-7
  - 受害者：POS机 （领域：金融）
  - 影响：控制系统、窃取信用卡信息等
  - 类型：新型攻击

金融行业-攻击事件4

- 史上最大卡信息泄露事件：美国家得宝5600万信用卡信息被盗
  - 时间：2014年4月
  - 受害者：美国家得宝 （领域：金融）
  - 影响：5600万信用卡信息被盗
  - 类型：APT

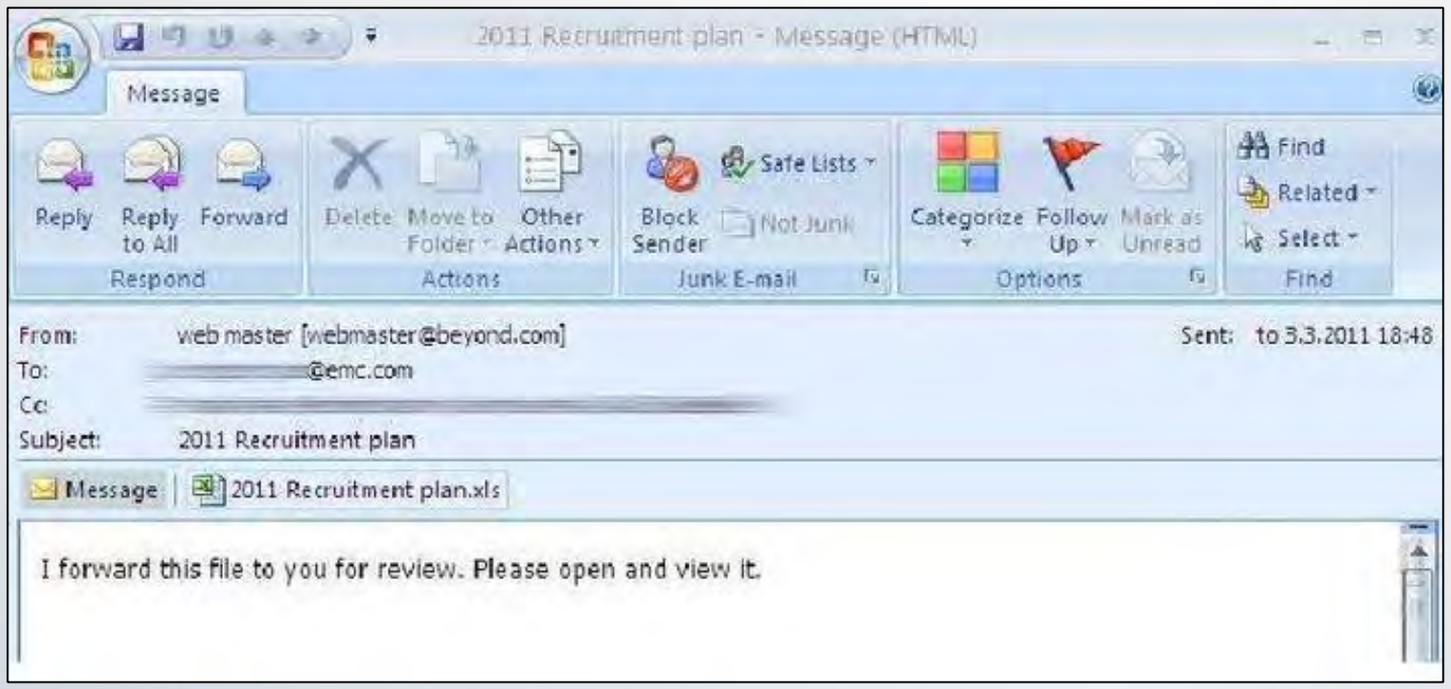
金融行业-攻击事件5

- Inputs.io 比特币交易市场被攻击
  - 时间：2013年7月2日
  - 受害者：Inputs.io
  - 影响：刚建立的一个比特币在线钱包商，虽然才运行几个月，但是在比特币社区中的口碑还是不错的，日前，国外黑客攻击了Inputs.io，并从中盗取了4100个比特币（折合130万美元）
  - 类型：APT

安全公司事件1 – RSA SecurID窃取

- RSA SecurID窃取事件(2011):

  - 2011年3月，EMC公司下属的RSA公司遭到入侵，部分SecurID技术及客户资料被窃取。
  - 导致很多使用SecurID作为认证建立VPN网络的公司受到攻击，重要资料被窃取。



安全公司事件1 – RSA SecurID窃取

- RSA SecurID窃取事件回放：
  - 时间：2011年3月
  - 攻击者给RSA的母公司EMC的4名员工发送两组恶意邮件。
  - 其中一位员工将其从垃圾邮件中取出来阅读，被当时的Adobe Flash Player的0day漏洞(CVE-2011-0609)命中。
  - 该员工电脑被植入木马，从C&C服务器接收指定执行恶意行为。之后相关联的员工包括IT与非IT等服务器管理员相继被黑。
  - RSA发现开发服务器遭入侵，攻击者立即撤离，加密并压缩所有资料传送至远程主机，随后清除入侵痕迹。
  - 在拿到SecurID信息后，攻击者开始对使用SecurID的公司展开进一步攻击。
- 攻击RSA的意图
  - 导致很多使用SecurID作为认证凭据建立VPN网络的公司-包括洛克希德马丁公司、诺斯罗普公司等美国国防外包商等受到攻击，重要资料被窃取。

洛克希德·马丁公司

洛克希德·马丁公司，全称洛克希德·马丁空间系统公司（英语：Lockheed Martin Space Systems Company）前身是洛克西德公司（Lockheed Corporation），创建于1912年，是一家美国航空航天制造商。公司在1995年与马丁·玛丽埃塔合并，并更名为洛克希德·马丁公司。目前洛克希德·马丁的总部位于马里兰州蒙哥马利县的贝塞斯达。

公司名称	洛克希德·马丁	成立时间	1995
外文名称	Lockheed Martin	经营范围	航空航天制造 国防工业承包
总部地点	美国 马里兰州 蒙哥马利县 贝塞斯达	年营业额	420亿美元（2010年公开）
		著名战斗机	F-35、F-22、F-117、F-16、SR-71

诺斯罗普公司

旗下拥有12万名员工的诺思罗普·格鲁曼公司是美国军火界的巨头之一，它的老板就是号称"引领军火工业攀登未来科技高峰的旗手"—59岁的罗纳德·休格。诺思罗普·格鲁曼公司目前正在弗吉尼亚的船厂建造"乔治·H·W·布什"号航母（CVN 77）。"布什"号是"尼米兹"级航母的最后一艘，该舰于2009年1月10日服役

公司名称	诺思罗普·格鲁曼公司	经营范围	军火
外文名称	Northrop Grumman Gorp	公司性质	美国军火商
总部地点	美国	公司口号	引领军火工业攀登未来科技高峰的旗手
成立时间	1994年	年营业额	1997年销售额为92亿美元
		员工数	1997年5.2万人

安全公司事件2 – DigiNotar公司被攻击而破产

- DigiNotar公司被攻击：
  - 时间：2011年9月
  - DigiNotar是一家提供根证书的公司
  - 攻击者共发行了531个伪造证书，包括了Google、微软、雅虎、Twitter、Facebook、中情局、军情六处和摩萨德等。
  - 攻击导致微软等大厂商撤销了DigiNotar根证书
  - 没有了信任，DigiNotar公司破产

工控行业事件1 – 震网（Stuxnet）

- 针对伊朗核电站的震网（Stuxnet）攻击事件(2010)：
  - 在2010年7月开始爆发，利用了微软操作系统中至少4个漏洞，其中3个为全新的0day漏洞，同时恶意驱动程序使用了有效的数字签名。
  - 一套完整的入侵和传播流程，突破工业专用局域网的物理限制，利用WinCC系统的2个漏洞，对其展开攻击。
  - 第一个直接破坏现实世界中工业基础设施的恶意代码，伊朗政府已确认该国的布什尔核电站遭到震网的攻击。

工控行业事件1 – 震网（Stuxnet）

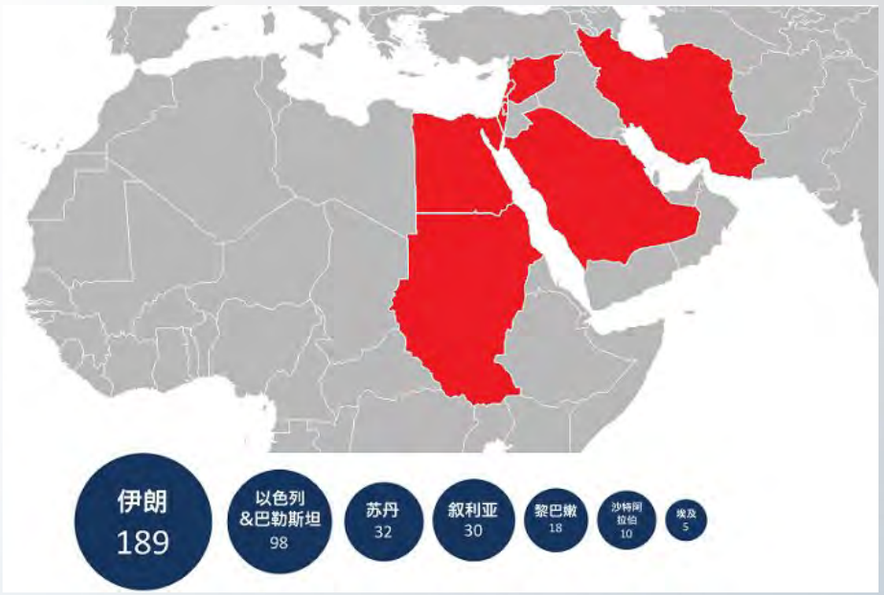
- 震网(Stuxnet)事件回放：
  - 通过感染科移动存储设备对物理隔离网络实现“摆渡”攻击，利用快捷方式文件解析漏洞（MS10-060），传播到内部网络。
  - 在内网中，通过快捷方式文件解析漏洞、RPC远程执行漏洞(MS08-067)、打印机后台程序服务漏洞（MS10-061）实现联网主机之间的传播。
  - 抵达了安装WinCC软件的主机，展开进一步攻击。

Duqu病毒攻击事件

- Duqu攻击事件（2011年）：
  - Duqu病毒被认为是由震网蠕虫的开发者编写，其用途是从诸如工业控制系统制造商这样的公司收集情报数据，目的是在未来更容易完成针对第三方的攻击。
  - 当时，国内一家拥有蓝牙软硬件技术的高科技企业也遭到“Duqu病毒”攻击。
  - 利用Windows内核0day漏洞（CVE-2011-3402）寄生在Word文档中传播

网络武器：超级火焰（Flame）

- 超级火焰Flame攻击事件(2012):
  - 2012年5月由卡巴斯基发现，针对中东地区国家，迄今为止结构最复杂的网络武器，模块体积比Stuxnet大20倍。
  - 既是一种后门、木马程序，又具有蠕虫的特点。
  - 接收操控者指令，可以在本地网络、可移动设备中自我复制。
  - 具有勘察网络流量、抓取截屏、记录音频对话、截获键盘输入、文件数据搜集等功能。
  - 利用windows签名0day漏洞进行攻击
  - 7个主要受到感染的国家：



工控行业事件2：Havex攻击ICS或SCADA系统

- Havex恶意程序(2014)：
  - 活动时间：2013-214
  - 受害者：2个法国众所周知的教育机构、2个德国工业应用程序和机器制造商、1个法国工业机器生产商、1个专门从事结构工程的俄罗斯建筑公司等 （领域：工业，能源）
  - 影响：窃取敏感数据
    - 感染ICS/SCADA制造商用来提供给用户的软件
    - 感染用户的主机并寻找局域网内的OPCServer。
    - 搜集OPCServer信息并上传
  - 类型：APT

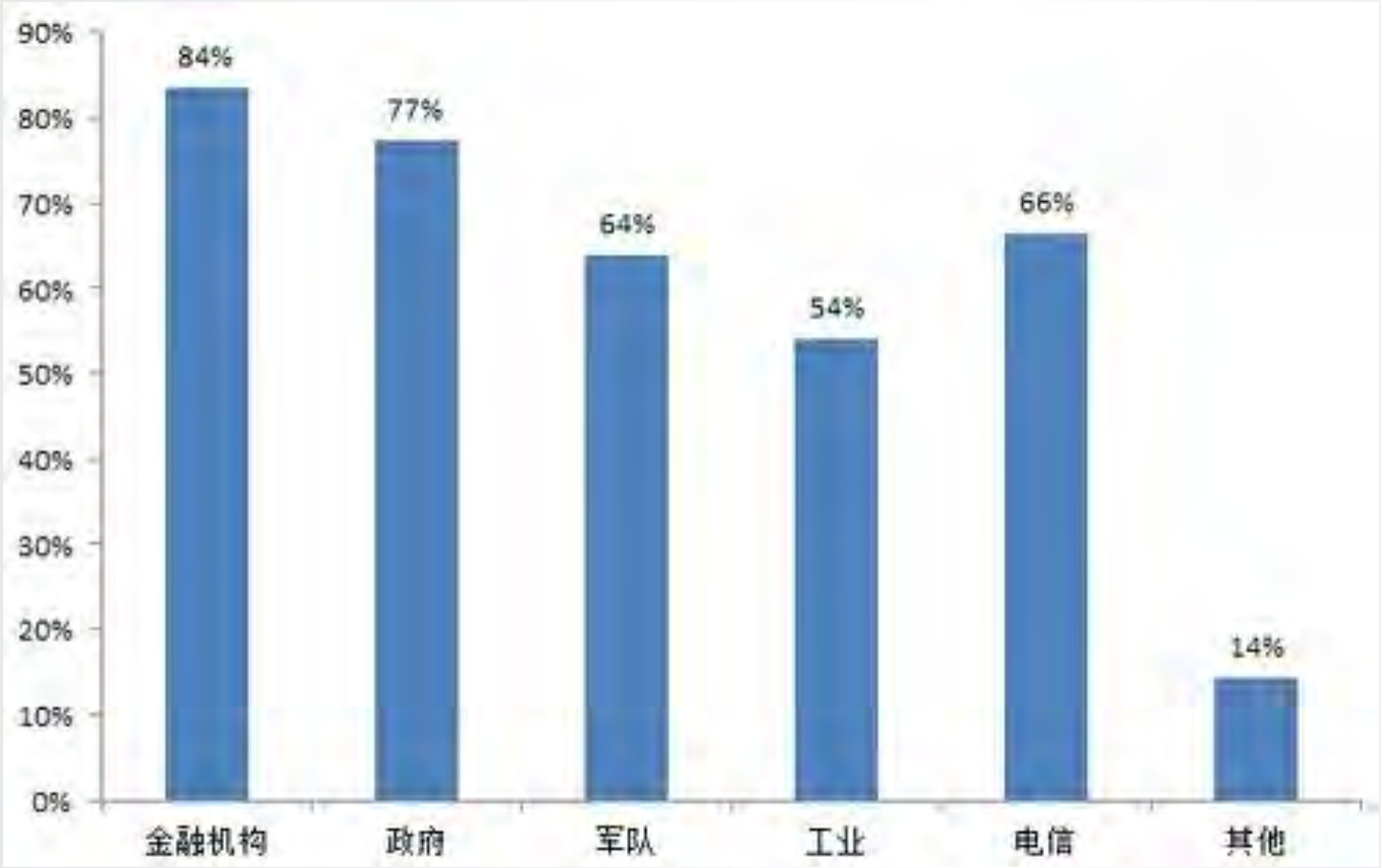
游戏公司事件1：Winnti组织

- 多家游戏公司被攻击
  - 报道时间：2013-4
  - 针对游戏公司托管的服务器，窃取源代码创建私服，同时盗窃钱财或虚拟货币。它攻击了超过30家网络游戏公司，受害者包括了2家北美公司，14家韩国公司，2家德国公司，2家俄罗斯公司
  - Winnti的网络间谍活动至少持续了四年

从事件中我们看到了什么？

- APT攻击一般都会附带一个或多个0day漏洞，而且比较高级有效数字签名、动态解密等）
- 往往企业都部署了传统的安全软件和设备
- 都有未知的威胁：未知的0day漏洞攻击，杀毒软件、IPS设备等检测不了的东西
- 行业覆盖将越来越广，只要有重要信息资产
- 报道中的事件往往是危害比较大的事件，更多的未知威胁和攻击其实是没有报道出来的

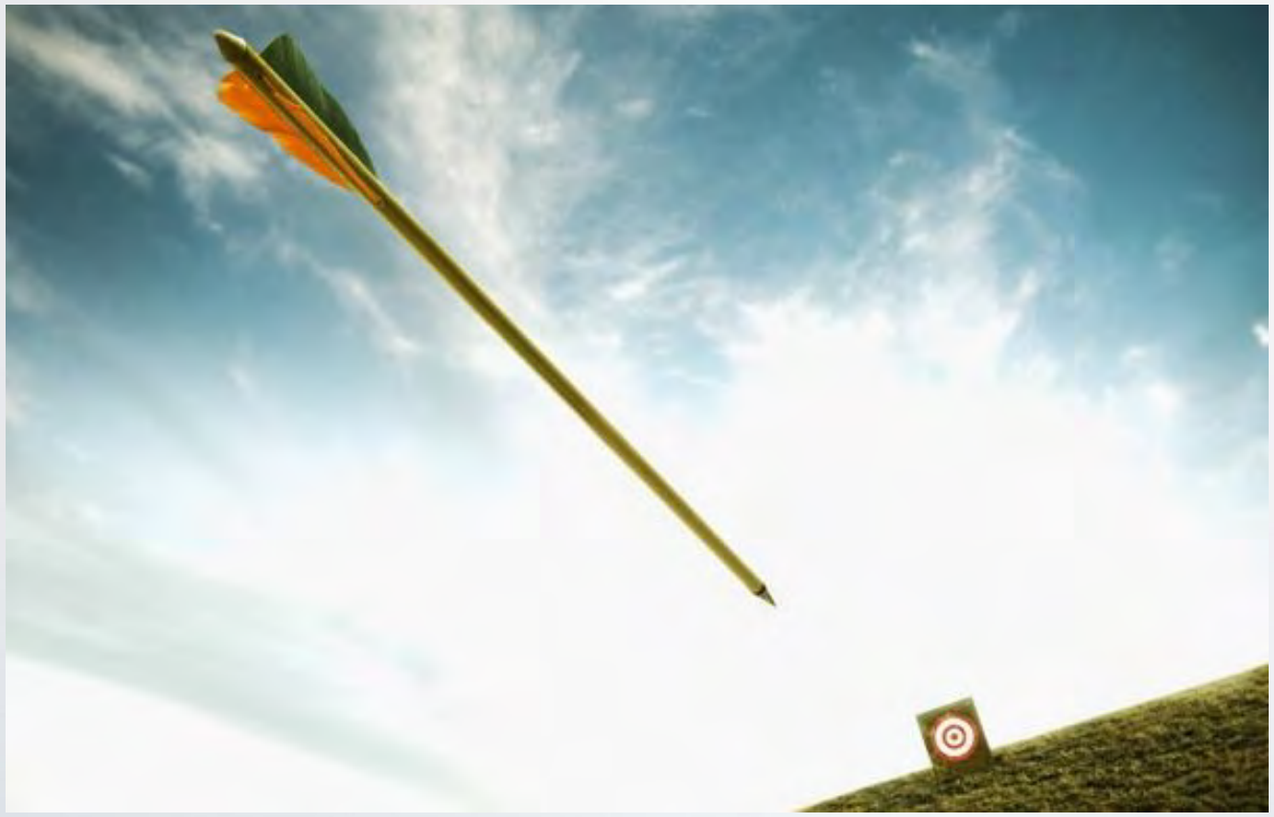
APT攻击的主要目标行业有哪些?



来自 2014 IT168调研平台

你会是APT的目标吗？

- 你的企业是否存在竞争对手想得到的商业机密？（公司受关注度无关）
- 你的企业的是否存在于价值链的某一环节？（公司规模大小无关）
- 你的企业的某些电子形式的东西是否可以被卖掉获利？（公司资产形式内容无关）



为什么APT/未知攻击从2010年开始井喷

我们的对手 biger than biger

内容概要

- 未知威胁/未知攻击
- 著名/非著名的APT/未知攻击事件
- 新一代网络威胁下传统安全软件的弊端
- 未知威胁检测手段
- 翰海源未知威胁/攻击解决方案
- 翰海源捕获的攻击事件

时间上：感知能力

2000年

病毒名称	释放时间	发现时间
CodeRedII	2001年8月3日	2001年8月3日
冲击波(Blaster)	2003年8月11日	2003年8月12日
震荡波(Sasser)	2004年4月30日	2004年5月1日
Zotob	2005年8月13日	2005年8月16日

2010年后

病毒名称	释放时间	发现时间
Stuxnet	2009年6月	2010年7月
Duqu	2007年或2008年？	2011年8月
Flame	2007年12月之前？	2012年5月

结论：APT时代，感知能力很差，以年为单位

事后的签名机制

- 签名机制的产品
  - 入侵检测/防御系统IPS/IDS
  - AV杀病毒

…

- 由于感知能力差，感知时间长，面对APT攻击时，事后签名机制几乎无效

传统技术很难检测到APT

翰海源 VULNHUNT SECURITY

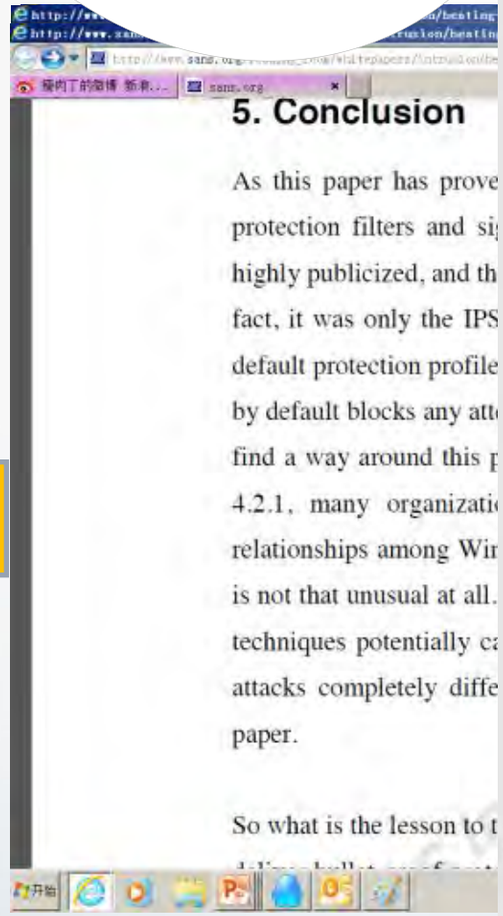
辅助安全措施：审计加固风评

主机边界防护

网络边界防护

基于已知知识：
已知安全漏洞与缺陷
已知木马行为与特征
已知攻击行为
明文内容
限定的权限

难以应对
未知或变形安全漏洞与缺陷
未知或变形木马行为与特征
未知攻击行为
加密内容
社会工程


5. Conclusion

As this paper has prove
protection filters and si
highly publicized, and th
fact, it was only the IPS
default protection profile
by default blocks any att
find a way around this p
4.2.1, many organizati
relationships among Wir
is not that unusual at all.
techniques potentially ca
attacks completely diffe
paper.

So what is the lesson to t


more clear i made this table where i report the "score" obtained by the AntiVirus against CVE-1493

this scale of values:

- 0 = Exploit and "malicious" exe executed successfully
- 1 = Exploit executed successfully but "malicious" exe not executed or sandboxed
- 2 = Exploit blocked/not executed

AntiVirus Name	Score
Ad-Aware Free Antivirus+	0
AVG Antivirus Free 2013	0
Avira Free Antivirus 2013	0
Bitdefender Antivirus Free Edition	0
Quick Heal Antivirus Pro 2013	0
Immunet 3.0	0
Dr.Web Anti-virus Pro	0
ESET NOD32 Antivirus 6	0
FortiClient Endpoint Security Management	0
F-PROT Antivirus	0
F-Secure Anti-Virus	0
G Data AntiVirus 2013	0
IKARUS anti.virus	0
Kingsoft Internet Security 9	0
Malwarebytes Anti-Malware Free	0
McAfee AntiVirus Plus 2013	0
Microsoft Security Essentials	0
NANO Antivirus	0
Norman Antivirus 10	0
Outpost Antivirus Pro	0
Panda Cloud Antivirus	0
Rising Free Antivirus	0
VIPRE Antivirus 2013	0
VirusBuster Personal Antivirus	0
ArcaVir 2013 Antivirus	1
Avast! Free Antivirus	1
Comodo Antivirus Free	1
Emsisoft Anti-Malware 7.0	1
Trend Micro Titanium Antivirus Plus	1
Kaspersky Anti-Virus 2013	2
Norton AntiVirus	2
Sophos Anti-Virus	2

Summarizing the results

- 24 (75 %) don't detect the exploit neither the executable
- 5 (16 %) don't detect the exploit but they warn you about the executable
- 3 (9 %) detect the exploit

Looking only the exploit, 91 % don't detect it and 9 % are able to block it

基础安全设施：加密等基础安全设施与信任

内容概要

- 未知威胁/未知攻击
- 著名/非著名的APT/未知攻击事件
- 新一代网络威胁下传统安全软件的弊端
- 未知威胁检测手段
- 翰海源未知威胁/攻击解决方案
- 翰海源捕获的攻击事件

未知威胁检测手段

- 传统的签名技术已知检测
  - –杀病毒
  - –IPS/IDS规则库等
- 未知威胁检测
  - –基于攻击特性的检测
  - –基于行为分析的检测
  - –基于异常流量的检测
  - –基于黑白名单的检测

内容概要

- 未知威胁/未知攻击
- 著名/非著名的APT/未知攻击事件
- 新一代网络威胁下传统安全软件的弊端
- 未知威胁检测手段
- 翰海源未知威胁/攻击解决方案
- 翰海源捕获的攻击事件

星云是什么

随着APT、定向攻击、高级特马、0day漏洞攻击等**新一代网络威胁**日益增多，而基于签名机制的传统防御产品在面对新型网络威胁前失效。星云多维度威胁预警系统是为企业检测/防御**新一代网络威胁**提供的一套先进的解决方案，让特马、0day攻击等无所遁形。

APT	定向攻击	高级特马	0day漏洞

星云的全称：**星云多维度威胁预警系统**

星云
解决了哪些问题？

1 企业部署了传统杀毒/IDS/IPS等安全设备，新型攻击/病毒事件还是爆发，如何发现？

星云
解决了哪些问题？

2　真的攻击，有哪些危害行为，做了哪些坏事情？

星云
解决了哪些问题？

3　哪些机器受攻击，更想知道哪些机器中招

星云
解决了哪些问题？

4 设备报了警后，如何判断是真假？成千上百的警告，如何运维？

星云
多维度，聚焦在未知威胁

- 攻击者思路 *VS* 防御者对策
  - –攻击者思路
    - 想方设法进去，而且不被发现
    - 想方设法找到要的东西，不被发现
    - 找到要的东西后想方设法把东西，不被发现
  - –防御者对策
    - 想方设法多点覆盖，减少检测盲点
    - 多种技术手段
    - 多维度检测，攻击负载-主机层-网络层

星云
多维度

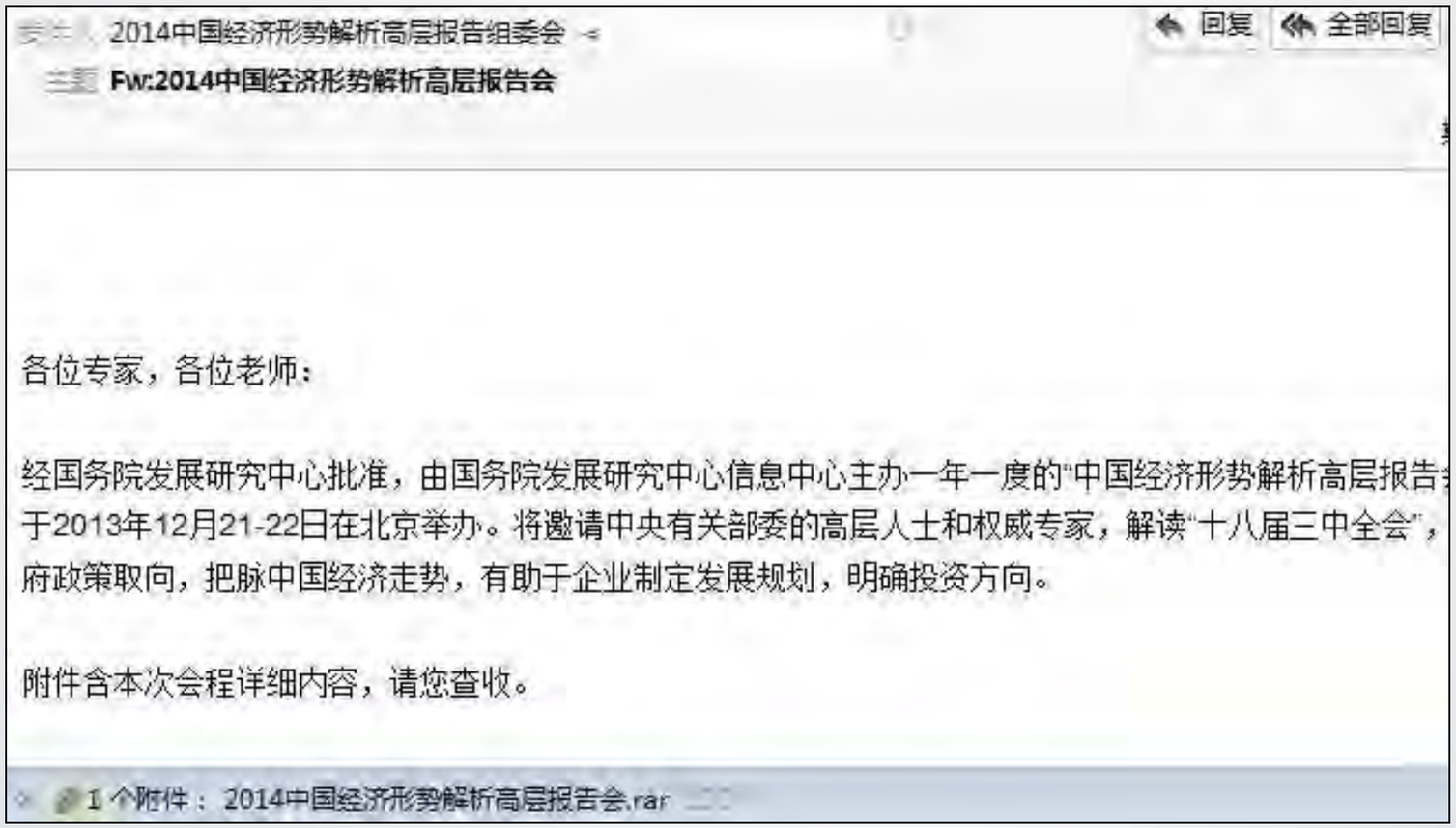
- 贯穿攻击过程的检测点
  - 恶意文档→shellcode执行→小马执行→大马执行→C&C控制
- 网络层检测和主机层检测动态关联
  - 网络层检测：木马协议，C&C,恶意url等
  - 主机层检测：恶意行为(可动态产生恶意木马，C&C等）
- 检测技术多维度
- 已知签名
- 未知深度内容
- 动态行为
- 事件关联

内容概要

- 未知威胁/未知攻击
- 著名/非著名的APT/未知攻击事件
- 新一代网络威胁下传统安全软件的弊端
- 未知威胁检测手段
- 翰海源未知威胁/攻击解决方案
- 翰海源捕获的攻击事件

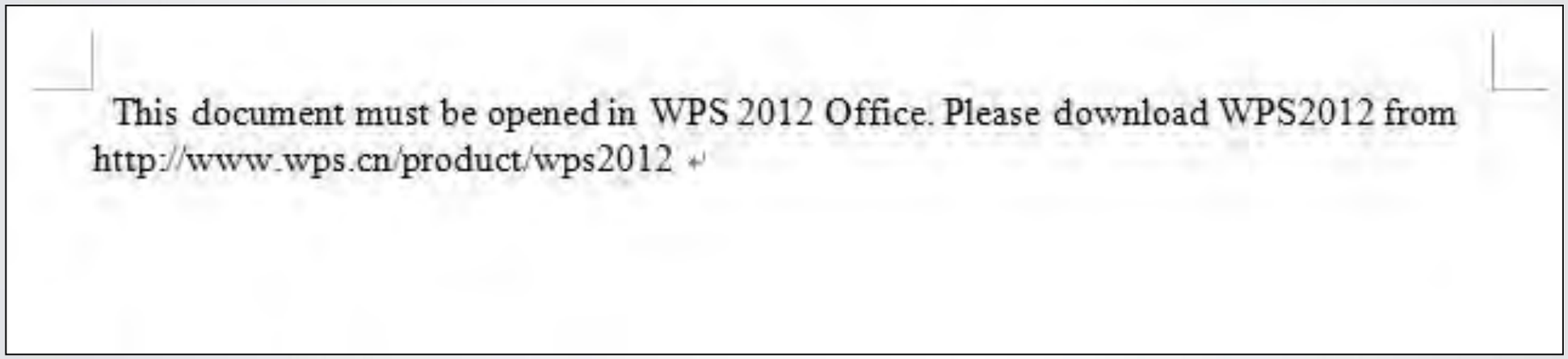
事件1：WPS 0day攻击事件

- 2013年12月，我们捕获到利用WPS 0day漏洞攻击政府部门的攻击事件，攻击者通过伪造的邮件进行定向攻击。



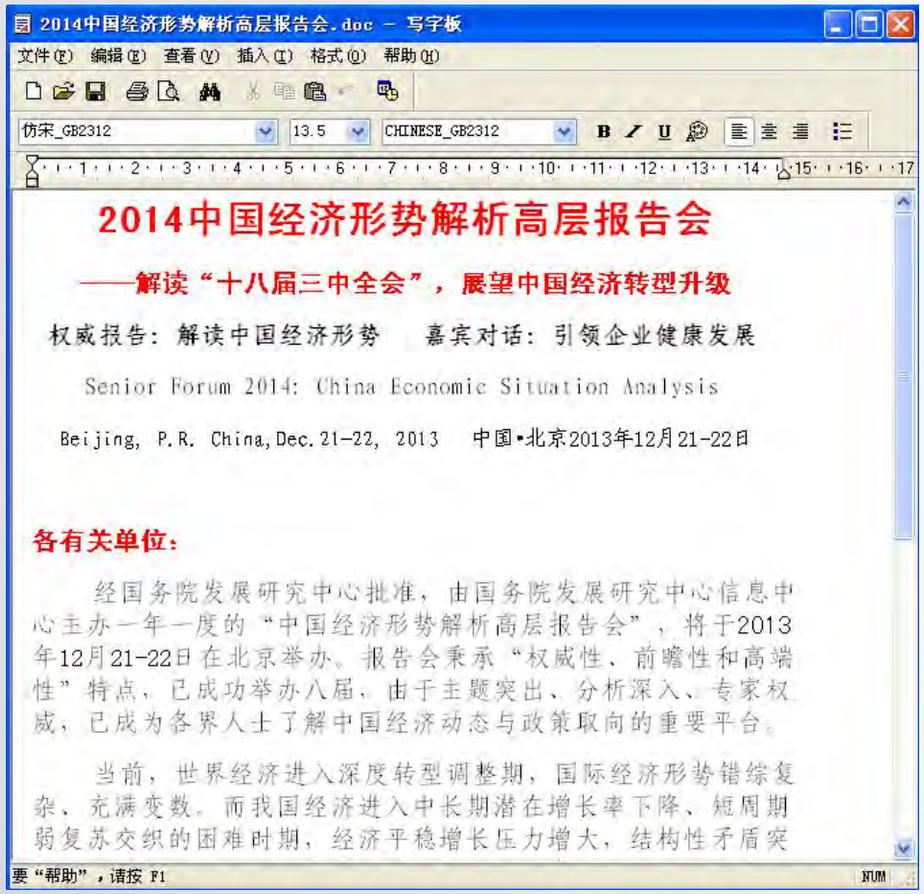
事件1：WPS 0day攻击事件

- 攻击者针对安装WPS的用户，如果用OFFICE WORD将会正常打开，内容诱骗你安装使用WPS并打开恶意附件。


This document must be opened in WPS 2012 Office. Please download WPS2012 from http://www.wps.cn/product/wps2012

事件1：WPS 0day攻击事件

- WPS 2012/2013 RTF fchars 堆溢出0day漏洞
- 漏洞触发成功后，会释放恶意程序植入主机，同时会打开一个正常的文档，受害者在中招后就浑然不知。



这里注意到文件作者信息：

事件1：WPS 0day攻击事件

逾70家中央部委和60家国企均已使用国产办公软件

2014年06月04日 08:46

来源：中国政库 作者：付珊　　109人参与　28评论

70多家中央部委、60家以上国企均已使用金山WPS办公软件。

6月3日，微博上传出宝钢集团有限公司旗下新疆八一钢铁[-2.09% 资金 研报]有限公司的内部通知。

这个于5月30日发布的《关于统一使用WPS Office软件的通知》，要求南疆各厂（部）统一安装使用金山WPS Office某版本，且各单位员工自行卸载微软Office软件，并将从6月起，每月检查各厂的执行情况。

早在2010年，宝钢集团已经采购了金山WPS Office软件，并明确要求集团包括所有分、子公司的电脑，要百分之百安装金山WPS。

宝钢集团和八一钢铁都出现在了金山WPS官网的“应用案例”中。

根据金山WPS官网，中央政法委、外交部、国家保密局、工业和信息化部、国家国防科技工业局、国土资源部、住房和城乡建设部、民政部等70多家中央部委都已安装该软件。

众多国家部委机构选择使用国产软件，源于2003年国务院的强制规定。

事件1：攻击文件释放的木马

- 然后启动inst.exe执行，连接至远程服务器，建立C&C通道。服务器域名为tencent168.biz，IP地址为162.144.55.235

事件1：释放文件说明

- a) 2014中国经济形势解析高层报告会.doc，释放至当前目录，WPS闪退后打开这个文件，迷惑用户，隐藏自己。
- b) inst.exe，木马引导部分，加载pile.dll。
- c) pile.dll，木马主体功能实现，为PIVY的变种。
- d) win32_453B.dll，用于劫持应用程序，在木马被删除后，恢复自身。

事件1：WPS 0day攻击事件

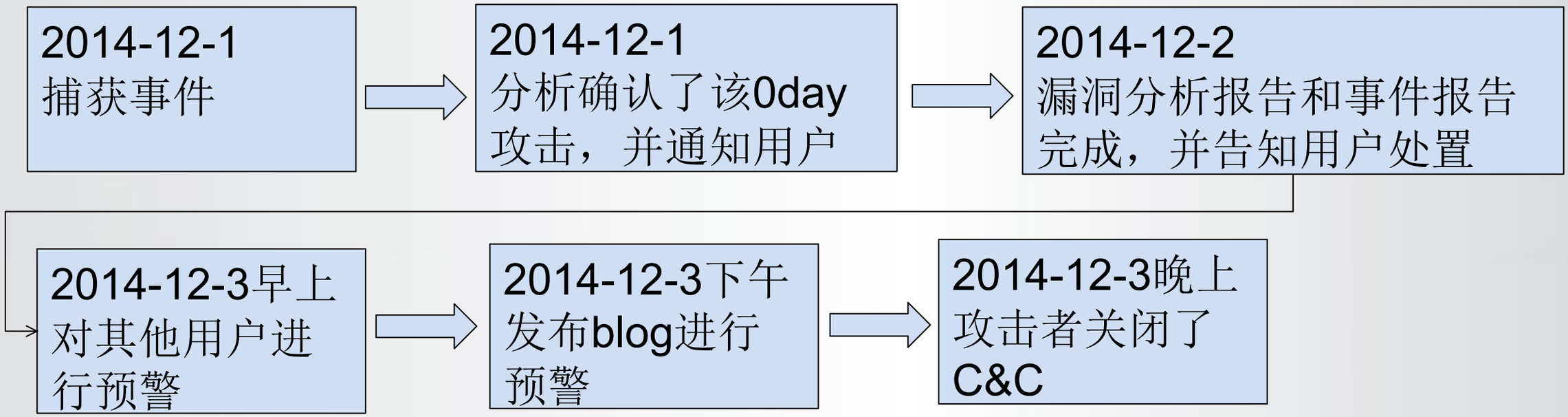
- 攻击者C&C为：tencent168.biz

```
EAX 00000000
ECX 00000000
EDX 71A34098 ws2_32.71A34098
EBX 0012F52E ASCII "C:\Documents and Settings\Administrator\Application Data
ESP 0012E920
EBP 0012EEFC
ESI 0012EF7C
EDI 0012F10C ASCII 0E,"tencent168.biz"
EIP 003F0242
```

- 所在地区为美国

IP Address: 162.144.55.235 Whois IP IP Blacklist IP Weather
Decimal: 2727360491
Continent: North America
Continent Code: NA
Country: United States
Country Code: US

事件1：协助客户处理



- 帮助客户及时发现了该攻击，并分析了攻击事件
- 及时阻止了一起高级定向攻击
  - 帮助用户排查有问题的主机
  - 拦截C&C通道
- 攻击者见事情败露，自己关闭了C&C主机

事件2：某技术博客挂马事件

- 2014年3月，我们捕获到了针对国内某技术博客挂马的攻击事件，攻击者利用Flash漏洞（CVE-2014-0502）进行挂马。挂马页面如下：

```
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">
    <body>
        <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" width="100%" height="100%" id="FlashExp">
            <param name="movie" value="cc.swf" />
            <param name="quality" value="high" />
            <param name="bgcolor" value="#ffffff" />
            <param name="allowScriptAccess" value="sameDomain" />
            <param name="allowFullScreen" value="true" />
            <!--[if !IE]>-->
            <object type="application/x-shockwave-flash" data="cc.swf" width="100%" height="100%">
                <param name="quality" value="high" />
                <param name="bgcolor" value="#ffffff" />
                <param name="allowScriptAccess" value="sameDomain" />
                <param name="allowFullScreen" value="true" />
            <!--<![endif]-->
            <!--[if !IE]>-->
            </object>
            <!--<![endif]-->
        </object>

    </body>
</html>
```

事件2：威胁情报分析

- 攻击者使用C&C：hk.msfcli.epac.to
- 恶意程序创建互斥体：)!eThddt4
- 恶意程序释放文件路径：
  - C:\Documents and Settings\User\Application Data\mydesktop.ini
- DNS解析记录：
  - 115.23.172.151（韩国）

文件名	MD5	VT
d.exe	E3AF2857178B7AB5A86269{ BLOCKED }	2/51
cc.swf	1283F2A755386709DE78D{ BLOCKED }	2/51

事件2：威胁情报分析

- qohub.info的域名注册信息：

注册人：Aya Stark

公司：Aya Stark

Registrant Street: Bofulin road east

城市：Hongkong

Registrant State/Province:Hongkong

邮编：999077

国家：HK

电话：+852.69835762

Registrant Phone Ext:

Registrant Fax:

Registrant Fax Ext:

邮箱：ayastark@hotmail.com

Admin ID:CR172096911

Admin Name:Aya Stark

Admin Organization:Aya Stark

Admin Street: Bofulin road east

Admin City:Hongkong

Admin State/Province:Hongkong

Admin Postal Code:999077

ayastark@hotmail.com

事件2：威胁情报分析

- 总结：

  –该组织从2012年左右开始活动

  –该组织擅长使用网页挂马(水坑攻击)的手法，使用包括Java、Flash等软件漏洞利用程序。

事件3：国外军事资讯网站挂马事件

- 国外军事资讯网站挂马事件（2014年7月）

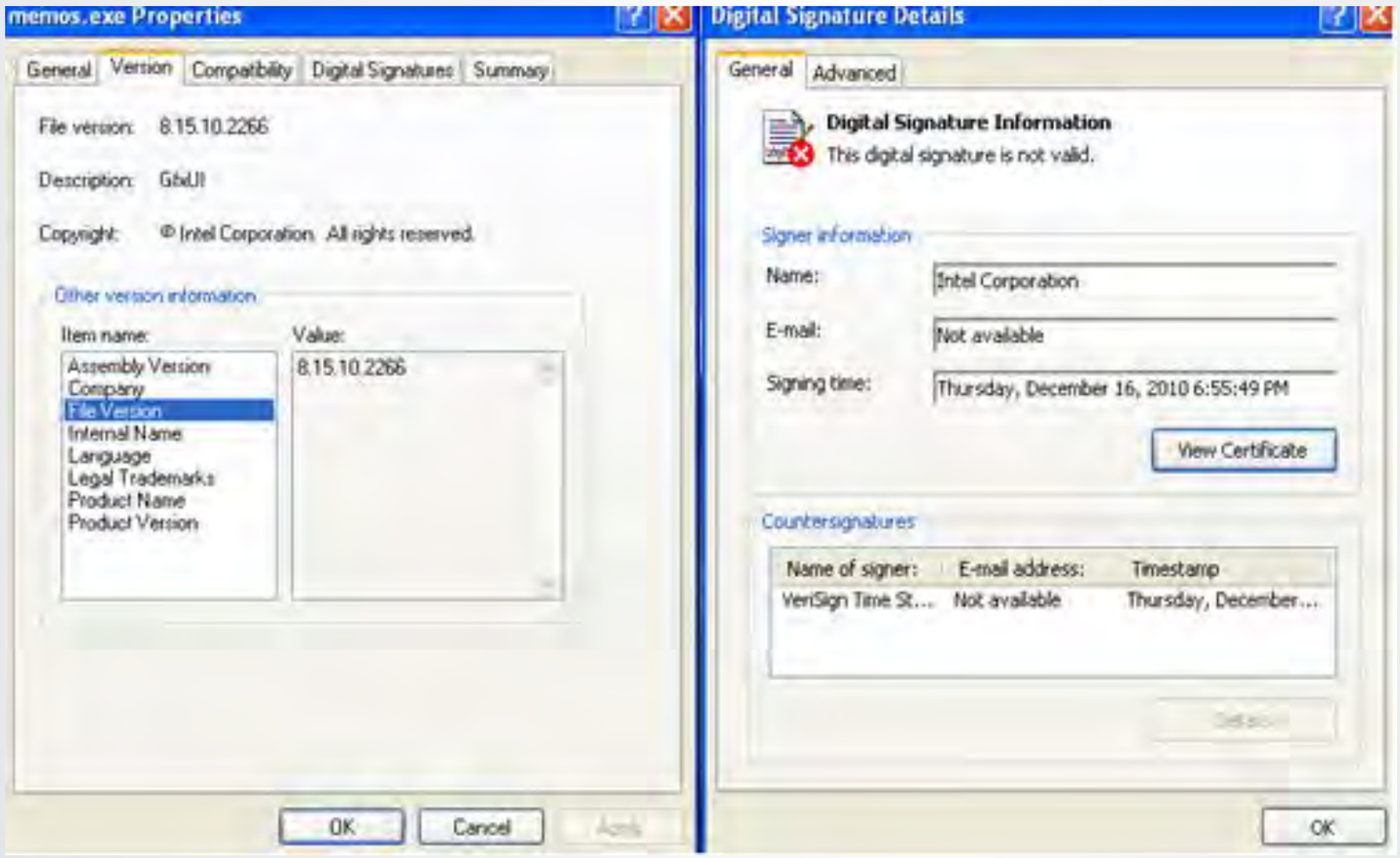
  –攻入国外著名军事资讯网站（defencetalk.com）挂马，主要目标可能是针对军事感兴趣的人群。

  –利用Flash漏洞（CVE-2014-0515）进行挂马攻击。

  –漏洞触发成功后会在受害者电脑主机植入木马后门，从而窃取敏感隐私数据、文件等。

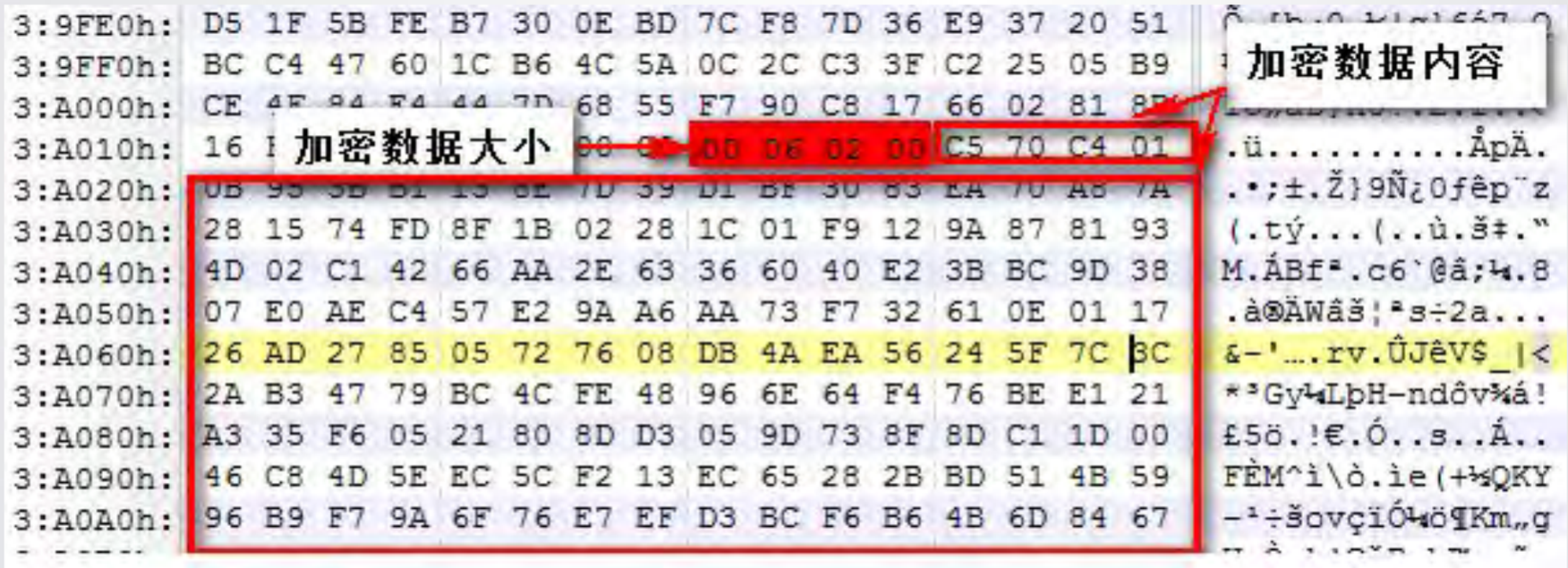
事件3：国外军事资讯网站挂马事件

- 恶意程序伪装成*Intel*显卡程序，并带有无效的数字签名



事件3：国外军事资讯网站挂马事件

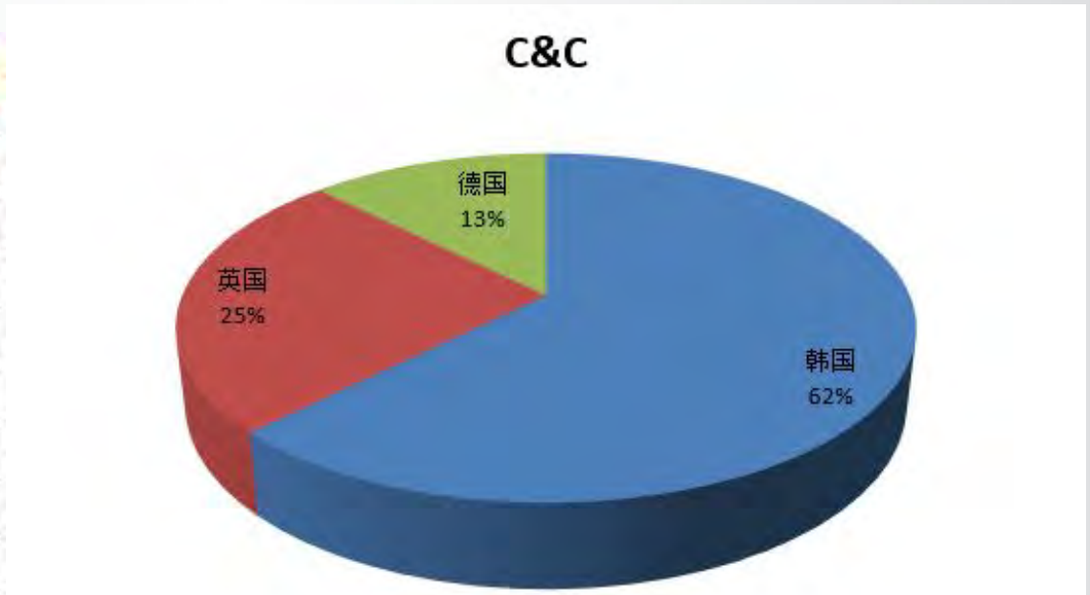
- 恶意程序运行后，会动态加密PAYLOAD，并将控制权交给该段PAYLOAD,传统基于静态特征查杀的安全软件很难检测到。



事件3：国外军事资讯网站挂马事件

- 攻击者使用的C&C主要分布在韩国：

域名	DNS	地区
silverlight.eu5.org	5.9.106.214	德国
study.lifeonet.com	185.27.134.159	英国
sisen.kr	110.45.146.61	韩国
www.duckjin.net	222.122.49.28	韩国
www.seiwooeng.com	211.234.110.166	韩国
www.webtle.net	211.234.110.164	韩国
kaltravel.com	114.108.141.99	韩国
inewstime24.com	110.45.146.230	韩国
pomdoll.com	61.100.7.111	韩国

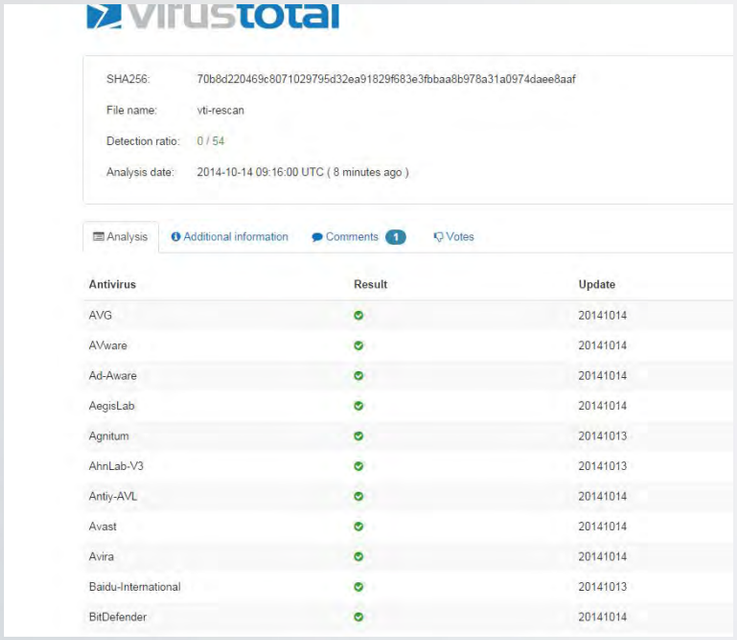


事件4：沙虫APT事件

- 2014/10/14早上 isightpartners报告了沙虫APT事件
  - –俄罗斯攻击北约，欧盟，电信和能源部门的事件
  - –使用一个超厉害windows 0day漏洞- WINDOWS OLE包管理漏洞
- 同时微软例行更新中揭露此漏洞

事件4：沙虫APT事件 SandWorm

- 翰海源应急团队及时应急响应
  - -2014/10/14早上 isightpartners报告沙虫APT事件&微软公告
  - -v1.0 2014/10/14 22:01 发布第一版 高危事件预警



事件4：沙虫APT事件 SandWorm

- 翰海源应急团队及时应急响应
  - v1.1 2014/10/14 (当天）22:48 增加漏洞细节（国内首发漏洞成因报告）
    - 攻击样本包含94.185.85.122的远程文件
    - 利用windows ole 逻辑漏洞CVE-2014-4114
  - 自动下载远程文件slide1.gif和slides.inf
  - 实现了类似右键点击slides.inf进行默认安装过程
    - » 可以过UAC

右键安装最终执行的程序是C:\Windows\System32\InfDefaultInstall.exe 参数为要安装的inf文件。此次攻击样本中的inf通过构造

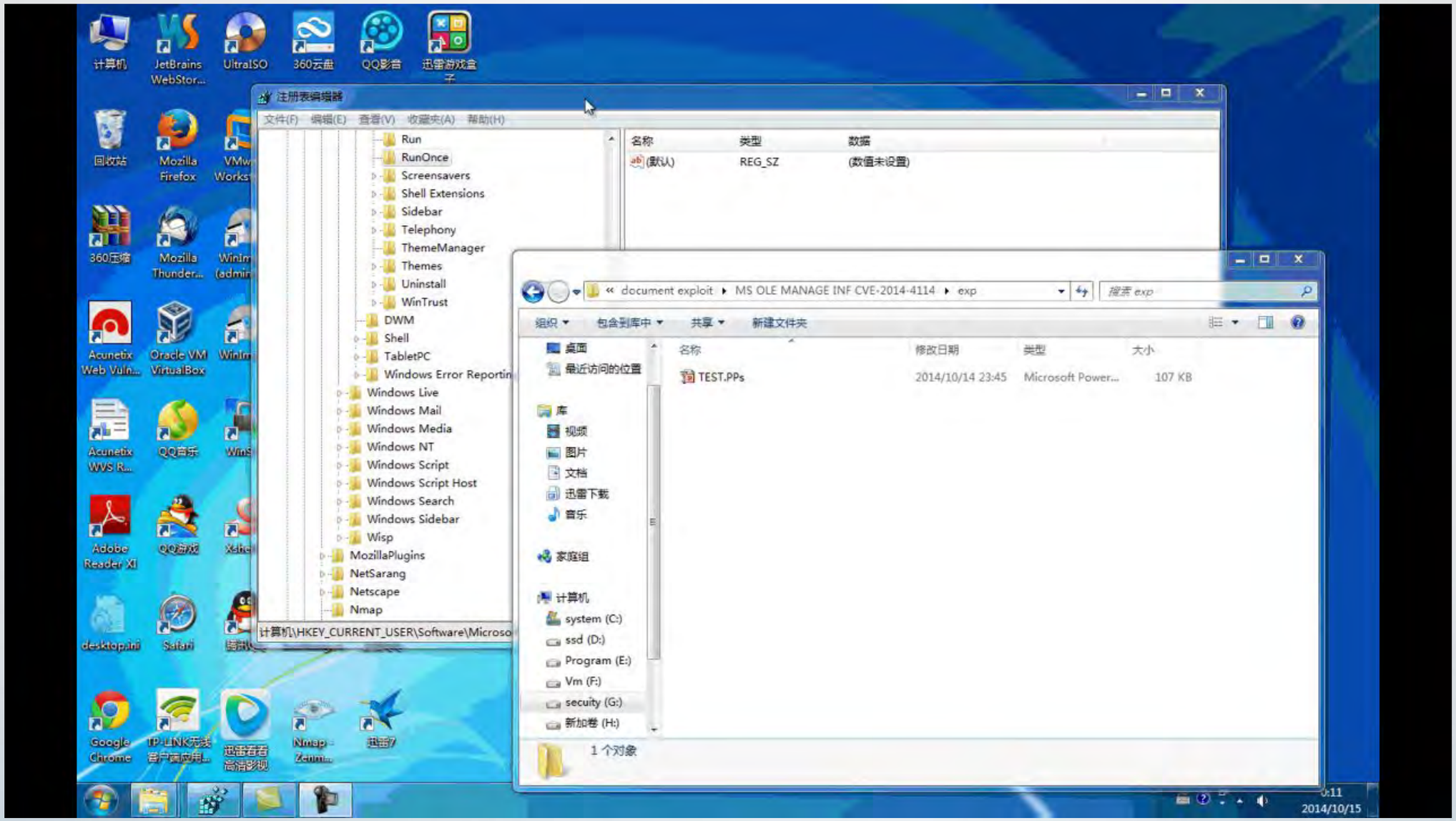
```
[DefaultInstall]
RenFiles = RxRename
AddReg = RxStart

[RxRename]
slide1.gif.exe, slide1.gif#将slide1.gif改名成slide1.gif.exe
[RxStart]
HKLM,Software\Microsoft\Windows\CurrentVersion\RunOnce,Install,,%1%\slide1.gif.exe
```

事件4：沙虫APT事件

SandWorm

- 翰海源应急团队及时应急响应
  - v1.2 2014/10/15 （第二天）08:50 增加了攻击演示视频



事件4：沙虫APT事件

SandWorm

- 翰海源应急团队及时应急响应
  - v1.4 2014/10/16 07:25 (第三天)增加事件中的木马分析报告
    - 识别出木马为BlackEnergy，最新的BlackEnergy3变种
    - “BlackEnergy流通在俄罗斯的地下网络，最早能够追溯到2007年”，F-Secure最近报告指出名为“Quedagh”的组织正在使用BlackEnergy发起一系列针对乌克兰政府的攻击，而此次0day所使用的恶意样本同样的可能来自该组织。
    - slide1.gif被修改掉了部分PE头部信息来对抗静态逆向分析
    - C&C http://95.143.193.131/aG91c2VhdHJlaWRlczk0/dirconf/check.php

子线程在内存中解密C&C并通过HTTP POST请求来通信，POST数据格式如下：

```
id=[BotID]&bid=ER&getpd=***
```

支持以下类型指令：

```
delete:卸载
ldplg: 加载插件
unplg: 卸载插件
update: 更新主程序
dexec: 下载并执行
exec: 下载并执行
updcfg:更新插件
```

Dune

事件4：沙虫APT事件

- 翰海源应急团队及时应急响应 timeline
  - 2014/10/14早上 isightpartners报告沙虫APT事件&微软公告
  - v1.0 2014/10/14 22:01 发布第一版 高危事件预警
  - v1.1 2014/10/14 22:48 增加漏洞细节（国内首发漏洞成本报告）
  - v1.2 2014/10/15 08:50 增加了攻击演示视频
  - v1.3 2014/10/15 14:05 增加细节
  - v1.4 2014/10/16 07:25 增加事件中的木马分析报告
  - 2014年10月18，捕获到不需要远程下载的全新变种APT

事件4：沙虫APT事件

- 反思
  - –内容分析引擎目前没有办法检测这种未知逻辑漏洞攻击
  - –我们的沙盒引擎也没有检测到该未知恶意文档，由于需要自动播放
  - –我们的沙盒引擎检测到了未知恶意文档利用成功后的负载(未知木马)
  - –国外研究团队后来又分析出沙虫APT事件还跟SCADA系统相关
  - –文档是否全部要沙盒引擎跑
    - 线上APT检测系统文档全部要沙盒去跑，性能是否能够扛的住？代价多大？

事件5：协助用户分析处置 Wormsharp蠕虫

- 为传播性很强的蠕虫，通过扫描135、1433、8080端口的弱口令进行传播。同时该蠕虫是使用.NET编写，具有较强的躲避杀软查杀能力。
- ftp下载母体蠕虫的时候被我们设备检测到

Rising	✓	20140418
SUPERAntiSpyware	✓	20140418
TheHacker	✓	20140417
TotalDefense	✓	20140417
TrendMicro	✓	20140418
ViRobot	✓	20140418

- 行为
  - 释放lib32wati.exe，创建WatiSvc服务→释放C:\tcpz-x86.sys驱动，修改指定内存
  - 传播扫描弱口令

事件5：协助用户分析处置 Wormsharp蠕虫

翰海源 VULNHUNT SECURITY

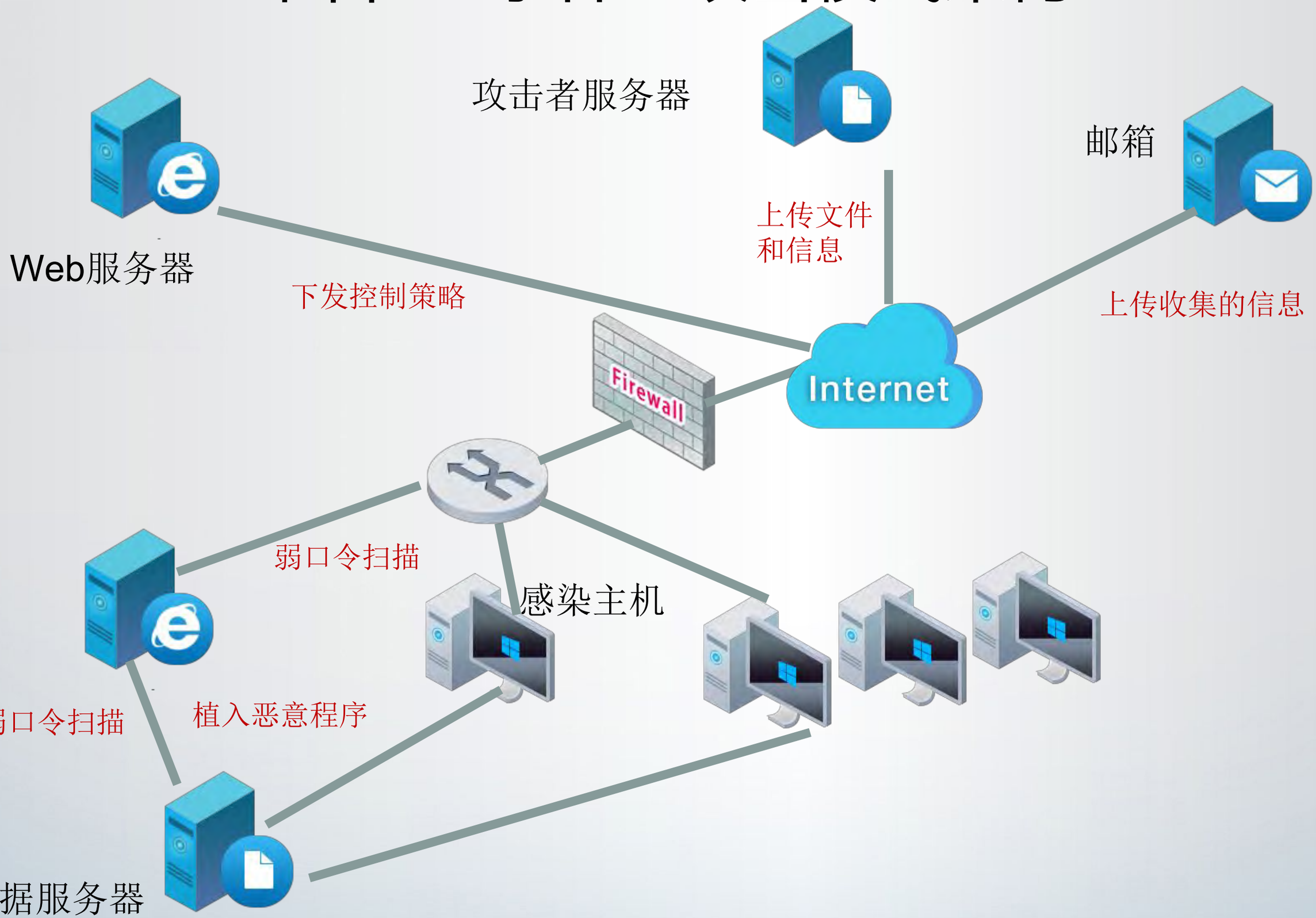
四. 处置建议

1. 参考上述的排查建议后，定位问题主机。
2. 停止名字为 WatiSvc 的服务。
3. 设置文件夹查看状态为“显示隐藏文件”及“显示系统文件”，然后定位到 C:\windows\system32 文件夹下，删除对应的 lib32wati.exe 文件。
4. 为了防止再次被感染，防火墙过滤 135 端口，同时服务器的 Sql Server 口令改为强口令。同时实时密切关注网络中异常的流量行为。
5. 过滤 IP 为 204.45.127.134 的请求，切断蠕虫与母体的联系。

持续的跟踪分析能力-未名APT事件

- 发生在国内的金融部门
- 持续的
  - 早在2012年前就已经发生，并且持续在发生
  - 已经帮忙客户处理了一些事件，但往往过段时间还会复发

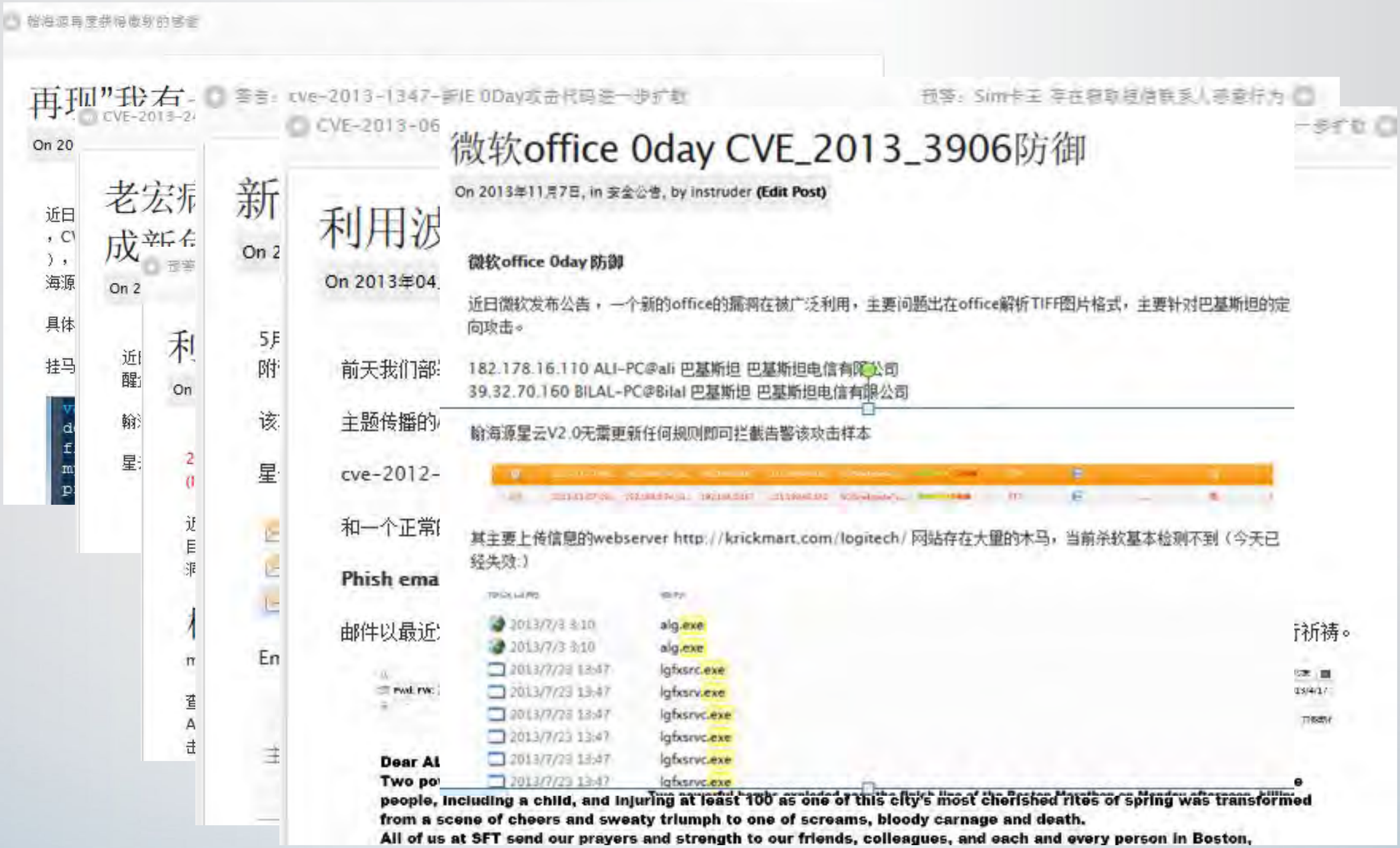
未名APT事件：攻击模式架构



持续的跟踪分析能力：未名APT事件

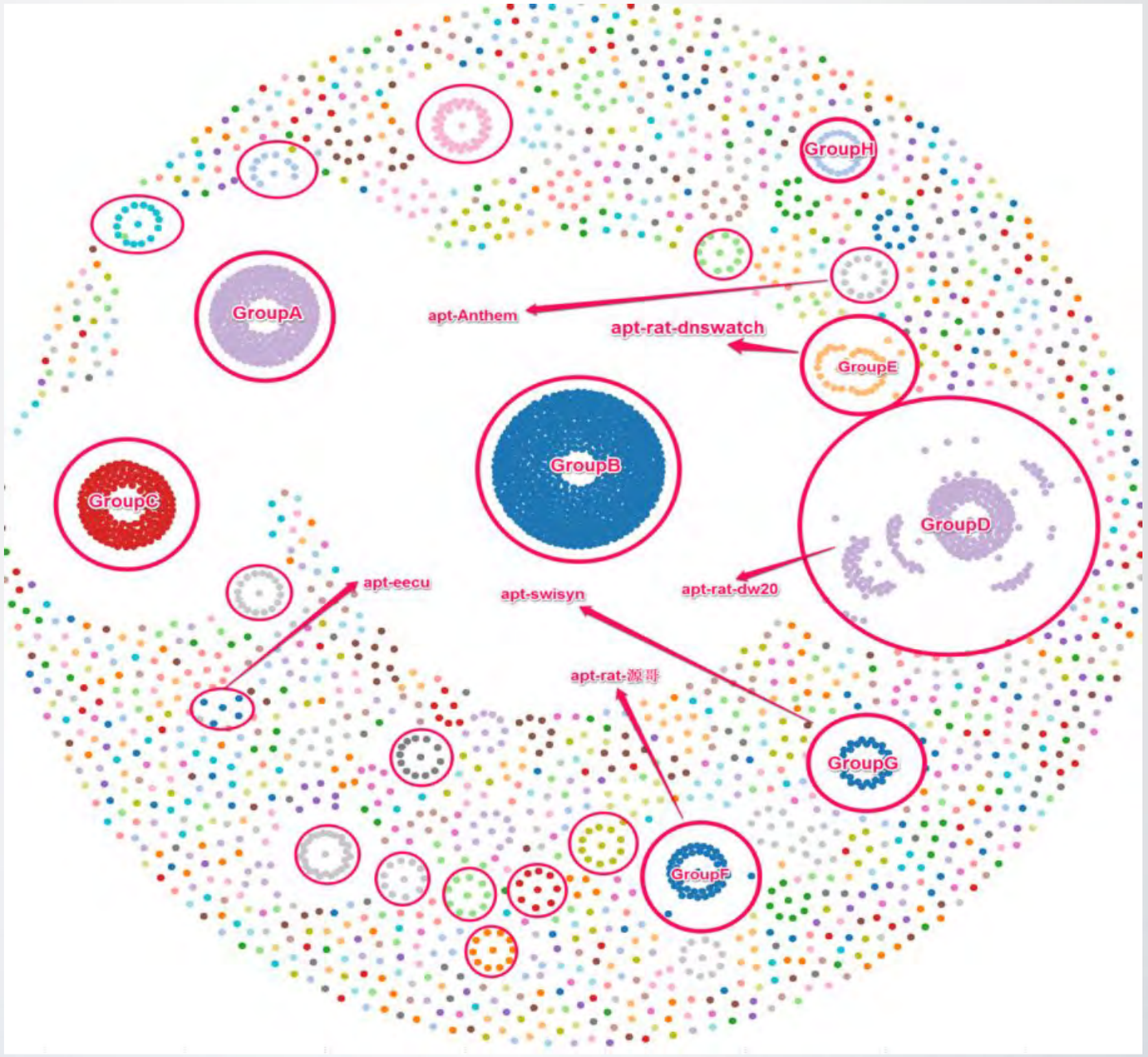
- 高级的
  - 对抗杀软
    - 360、Mcafee、赛门铁克、趋势等
  - 对抗虚拟机
    - 包括VPC、VMWare
  - 图片夹带加密数据实现动态功能
    - 模块的更新、任务的下发等功能
  - 进行内网渗透
    - 暴力破解
  - 进行数据收集
    - 感染主机会先收集主机信息、邮件标题、浏览器标题、聊天记录等大量敏感信息，之后会定向的上传某些特定主机的WORD、EXCEL、PPT、PDF文档
  - 定向攻击：攻击者会通过策略文件，有选择的上传某些主机的指定文件

星云捕获未知威胁实例


微软office 0day CVE_2013_3906防御
On 2013年11月7日, in 安全公告, by instruder (Edit Post)
微软office 0day 防御
近日微软发布公告，一个新的office的漏洞在被广泛利用，主要问题出在office解析TIFF图片格式，主要针对巴基斯坦的定向攻击。
182.178.16.110 ALI-PC@ali 巴基斯坦 巴基斯坦电信有限公司
39.32.70.160 BILAL-PC@Bilal 巴基斯坦 巴基斯坦电信有限公司
翰海源星云V2.0无需更新任何规则即可拦截告警该攻击样本
其主要上传信息的webserver http://krickmart.com/logitech/ 网站存在大量的木马，当前杀软基本检测不到（今天已经失效:）
2013/7/3 3:10 alg.exe
2013/7/3 3:10 alg.exe
2013/7/23 13:47 lgfxsrc.exe
2013/7/23 13:47 lgfxsrv.exe
2013/7/23 13:47 lgfxsrvc.exe
2013/7/23 13:47 lgfxsrvc.exe
2013/7/23 13:47 lgfxsrvc.exe
2013/7/23 13:47 lgfxsrvc.exe
Dear Al
Two po
people, including a child, and injuring at least 100 as one of this city's most cherished rites of spring was transformed from a scene of cheers and sweaty triumph to one of screams, bloody carnage and death.
All of us at SFT send our prayers and strength to our friends, colleagues, and each and every person in Boston,

在APT检测的路上

- APT group分组



在APT检测的路上

- 文件B超 https://b-chao.com

在APT检测的路上

- C&C库和木马协议库输出
  - 轻量级对接专业运维团队
  - 快速感知未知威胁
  - 识别企业中已经中招的机器

未知攻击/APT检测的挑战

- 攻防的不对称性

- 符合木桶原理

未知攻击/APT检测的挑战

- 技术
  - –事件
    - 攻击不是一次性的，是持续性的
    - 事件不是孤立的，能够从看似孤立的事件中还原攻击者意图
  - –攻击点
    - 无文件、无马
    - 绕过部署点
    - 漏洞触发和payload分离
    - 恶意程序只是一个框架性木马，恶意指令靠攻击者下发
  - –流量点
    - 流量的异常，是否可以总结出可以通用的异常流量模型
  - –检测算法
    - 误报率问题

APT时代–未知威胁、未知攻击

翰海源 VULNHUNT SECURITY

Q&A

THANK YOU

翰海源 王伟
微博 _alert7_