

# APT事件及样本的分析和关联

安天实验室 胡星儒

# 写在汇报前面

- ❖ 主要是通过真实案例展开
- ❖ 相关案例基于第三方公开数据或报告进行相关研究，内部部分真实APT案例由于其特殊性暂不能公开。
- ❖ 通过相关第三方报告和我们的研究案例来了解相关APT事件如何进行分析 and 关联

# 提纲

APT特性

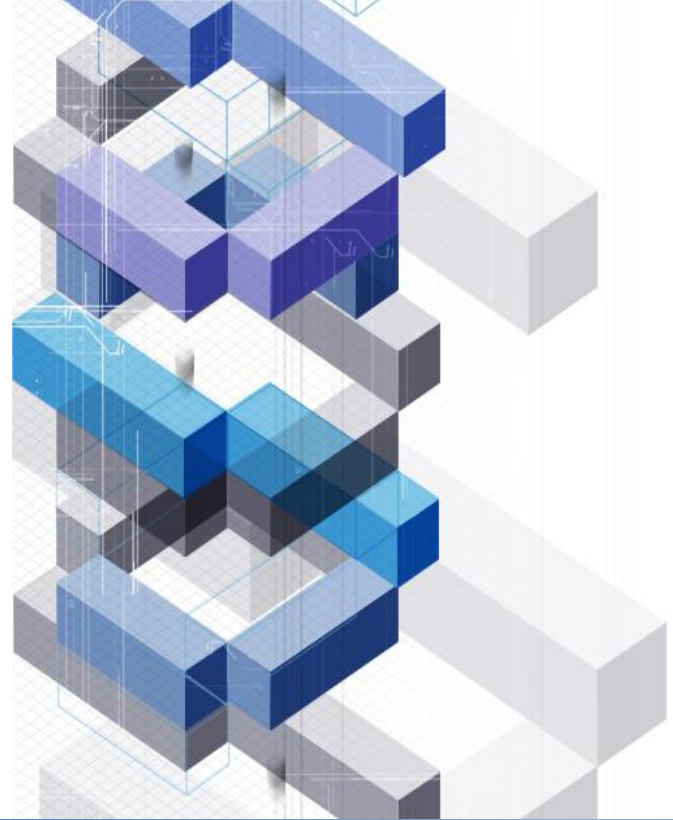
发现APT

关联分析方法

组织判定

他山之石

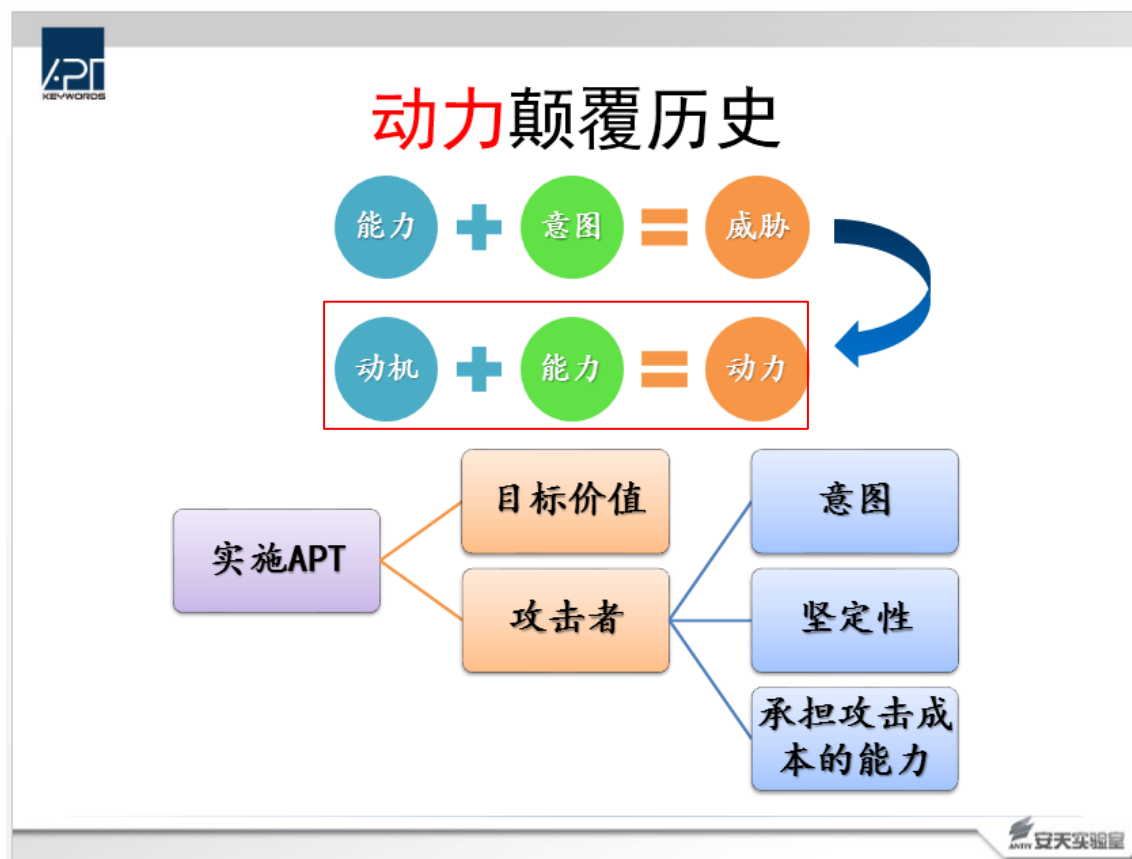
总结



# APT特性

# APT本质辨析

- ❖ Advanced Persistent Threat ?
- ❖ Targeted Attack ?



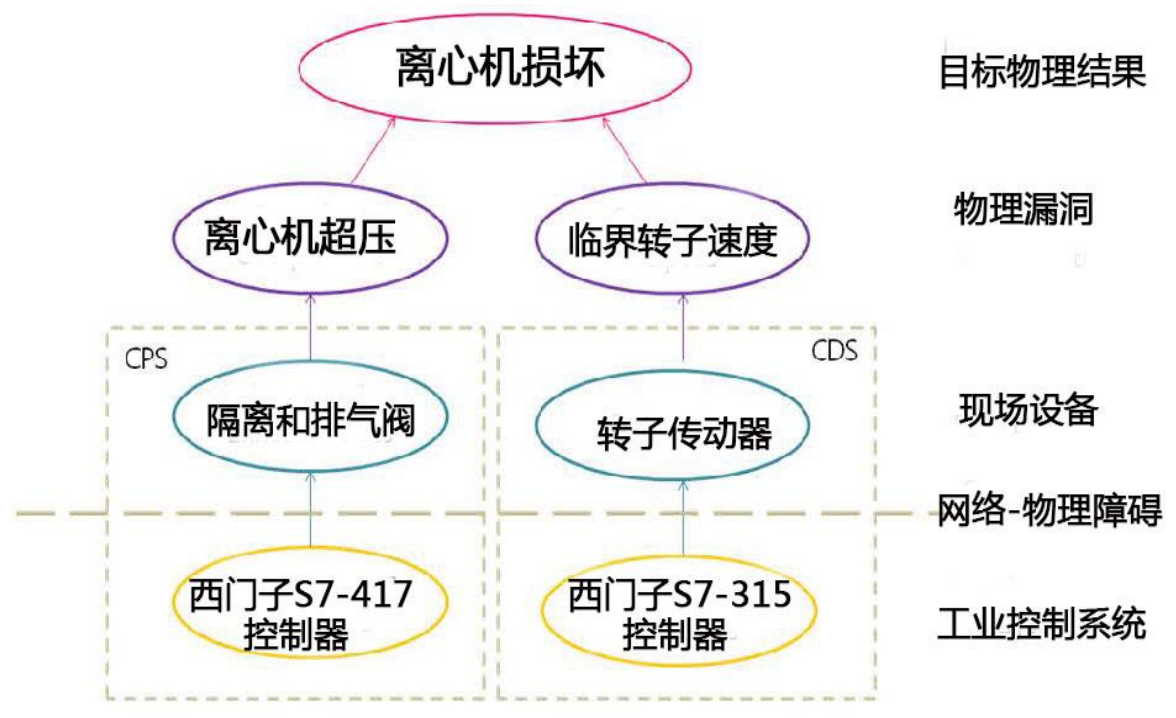
## 3.20 South Korea Cyber Attack

- ❖ 此次攻击影响了韩国YIN、MBC和KBS三大电视台及Shinhan、NongHyup和Jeju三大银行的服务器，使其无法正常工作。



# Stuxnet

## ❖ 破坏离心机



# APT Lifecycle

## ❖ Mandiant

初始攻击、创建据点、提权、内部侦察、横向移动、持续存在、完成任务

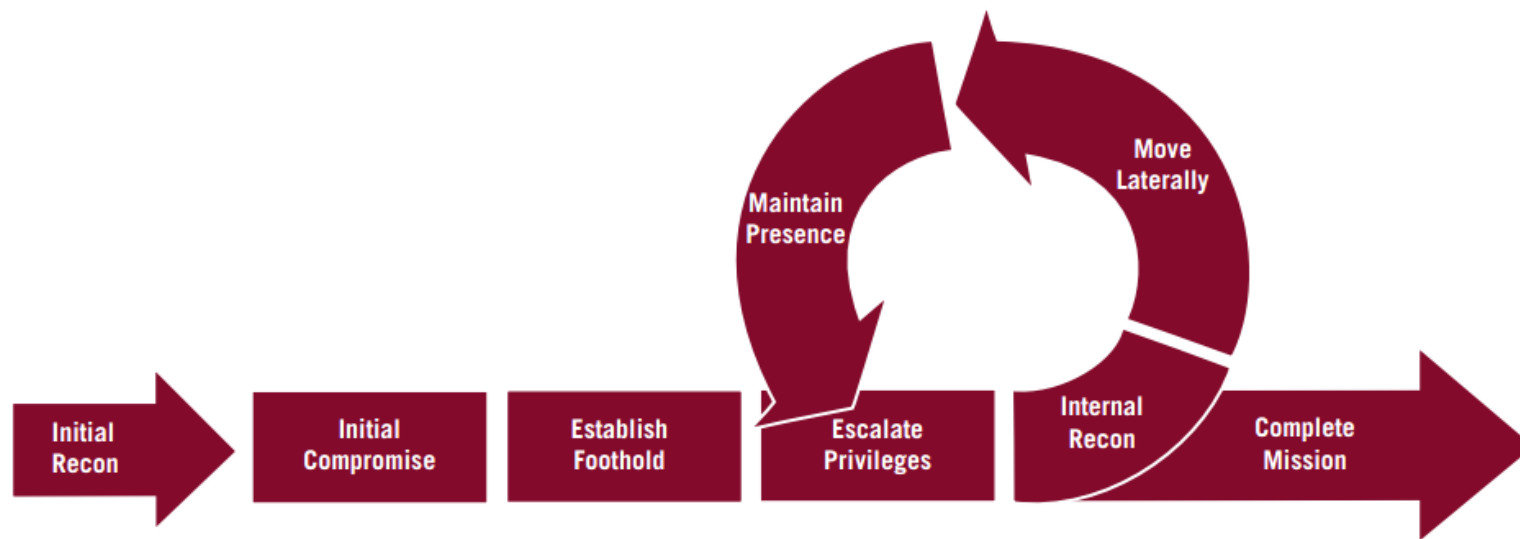


FIGURE 14: Mandiant's Attack Lifecycle Model



# APT Lifecycle

## ❖ Trend Micro

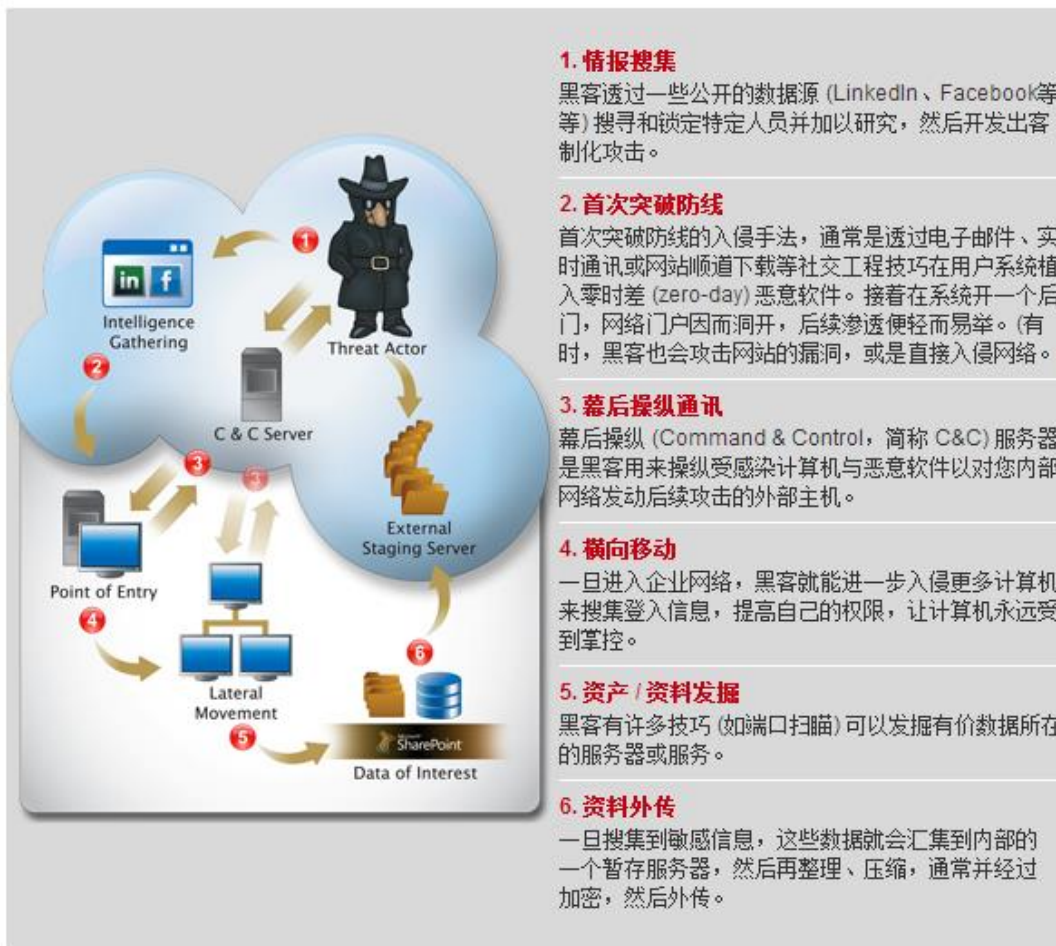
情报搜集

首次突破防线

幕后操纵通讯

横向移动

资产/资料发掘



# APT Lifecycle



入侵

发现

捕获

窃取信息

## Advanced Persistent Threat (APT): The Uninvited Guest

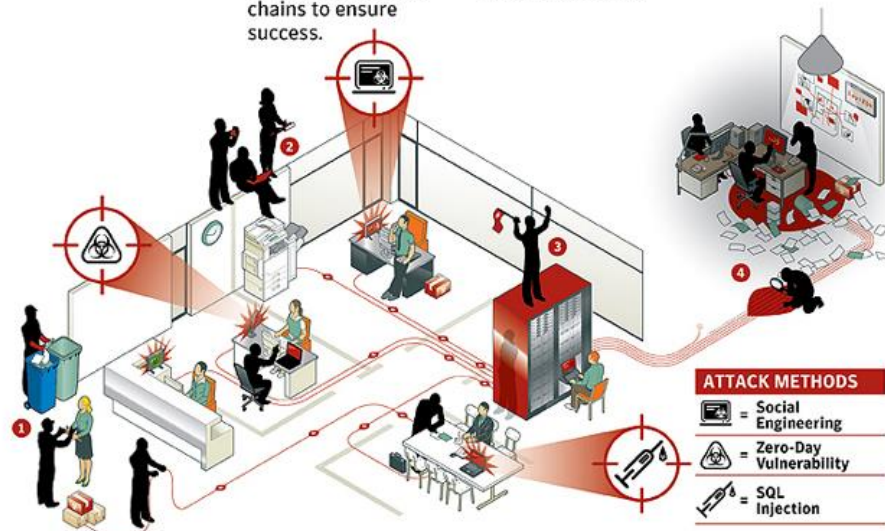
How attackers remain in your network harvesting information and avoiding detection over time

**1. INCURSION**  
Attackers break into network by using social engineering to deliver targeted malware to vulnerable systems and people.

**2. DISCOVERY**  
Once in, the attackers stay "low and slow" to avoid detection. They then map the organization's defenses from the inside and create a battle plan and deploy multiple parallel kill chains to ensure success.

**3. CAPTURE**  
Attackers access unprotected systems and capture information over an extended period. They may also install malware to secretly acquire data or disrupt operations.

**4. EXFILTRATION**  
Captured information is sent back to attack team's home base for analysis and further exploitation fraud—or worse.



**ATTACK METHODS**

- 1 = Social Engineering
- 2 = Zero-Day Vulnerability
- 3 = SQL Injection

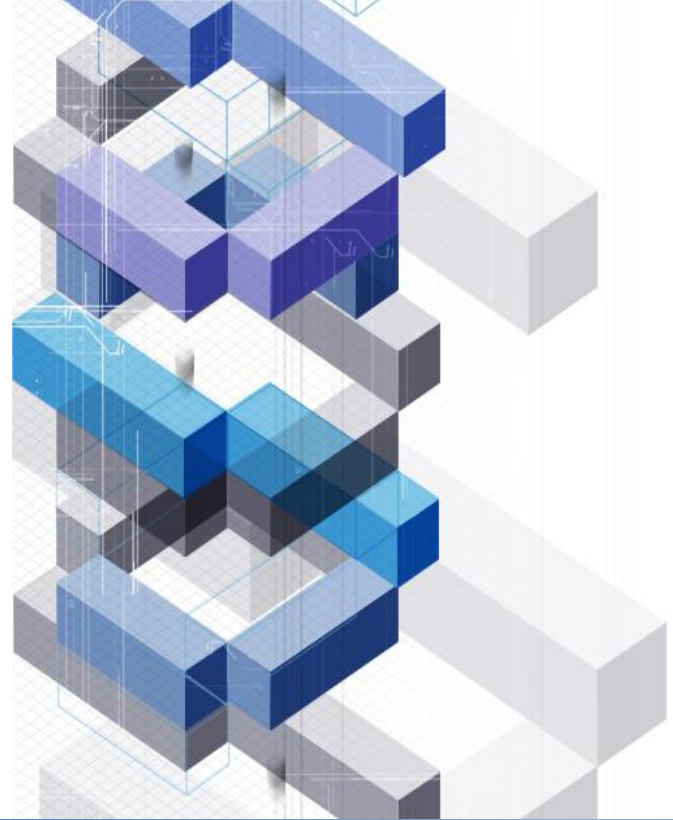


# APT Lifecycle



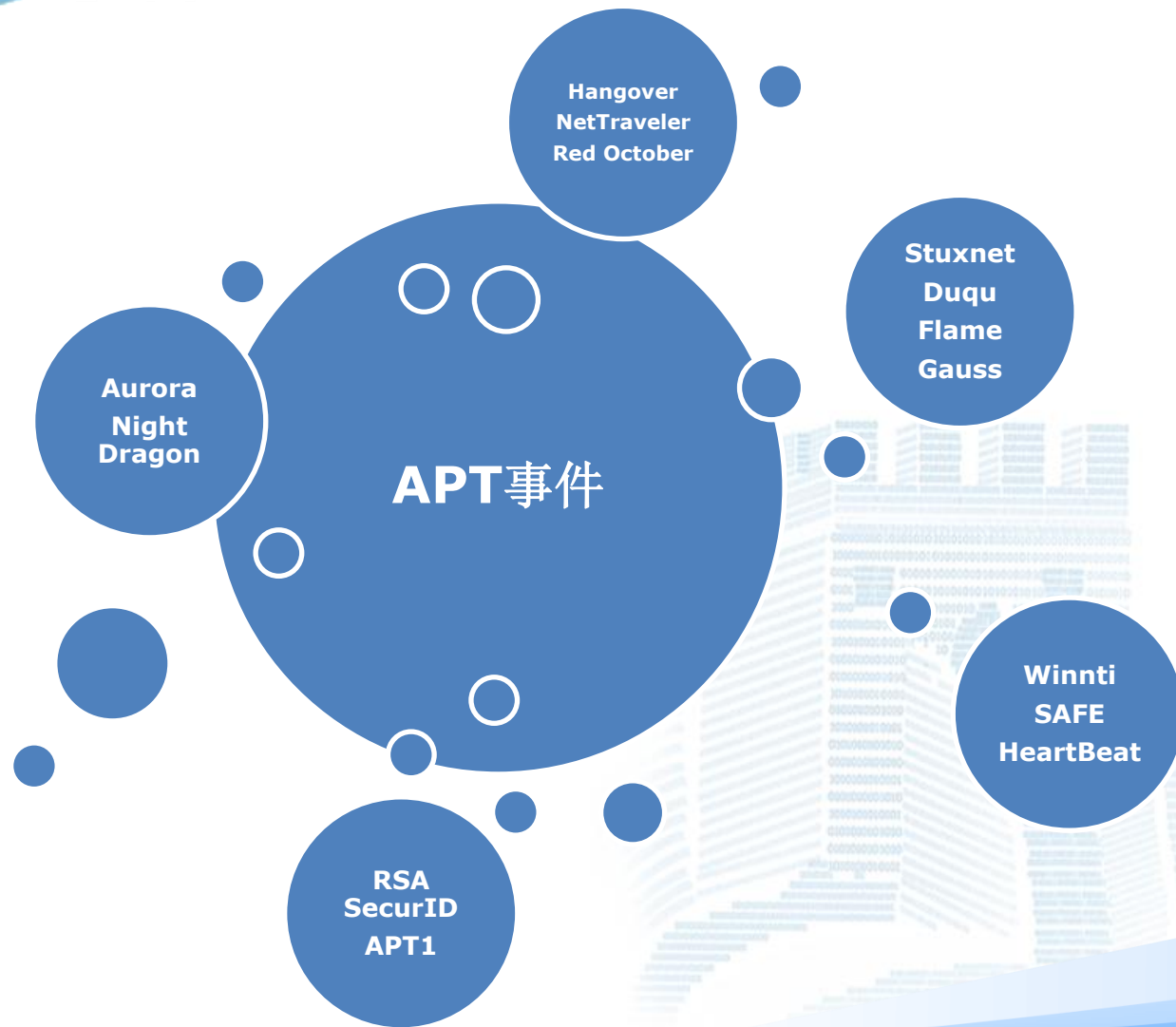
确定目标、找到并组织从犯、创建或获取工具、研究目标基础设施/员工、检出测试、部署、初始入侵、发起连接、展开访问并取得认证、巩固据点、溢出数据和掩盖痕迹保持不被检出



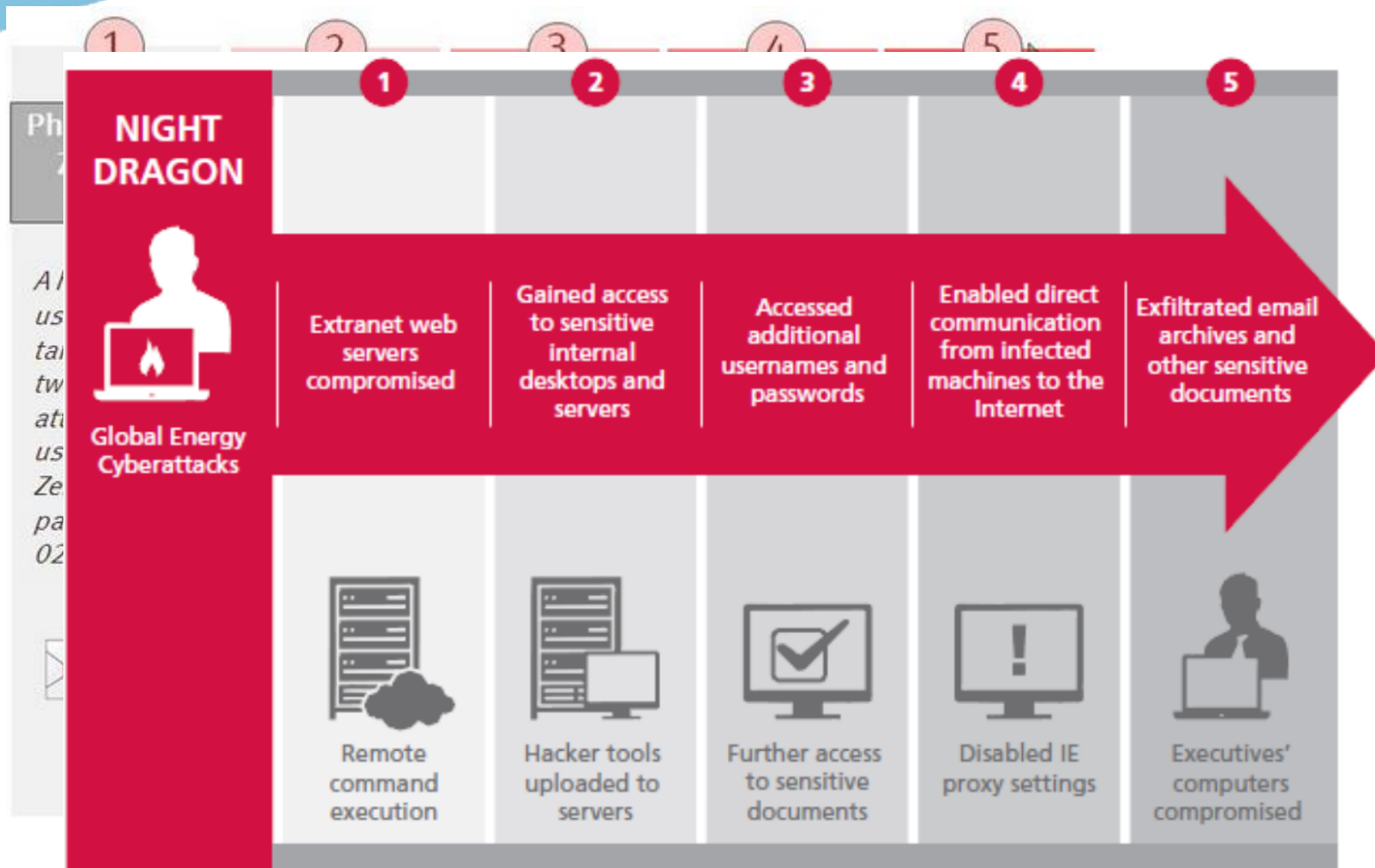


# 发现APT——持续对抗

# 相关APT事件



# RSA和Night Dragon



# 主要方法



# 海量已知样本

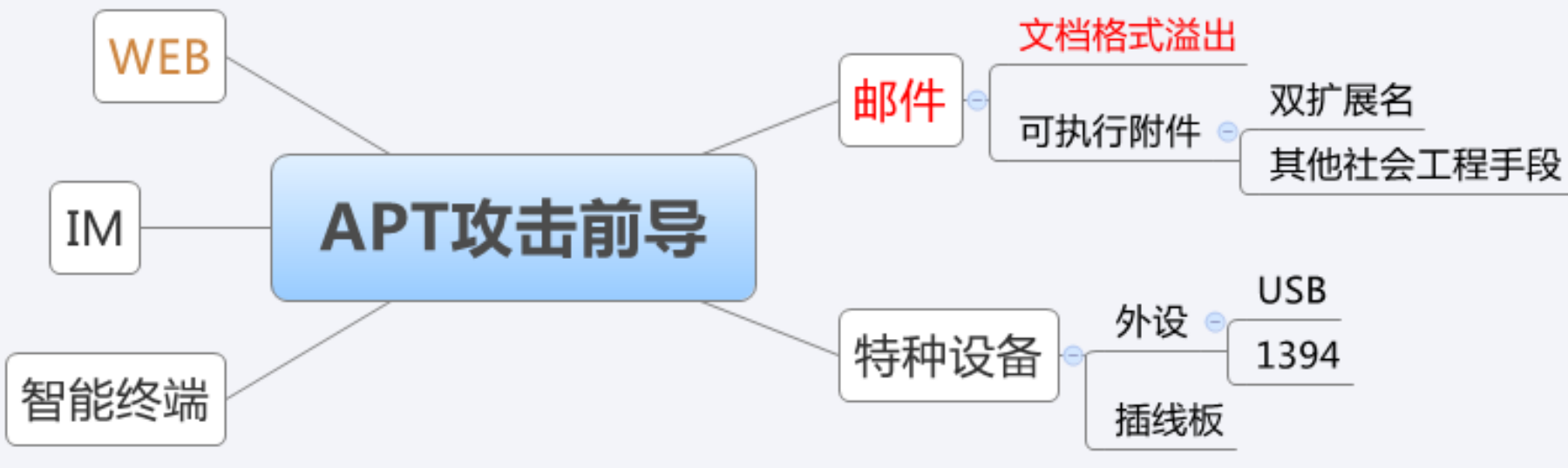
- ❖ 海量已知样本中需找同源样本：震网、FLAME、DUQU
- ❖ 在之后关联分析中会体现
- ❖ 某事件中采用的RAT：Poison Ivy、gh0st、灰鸽子





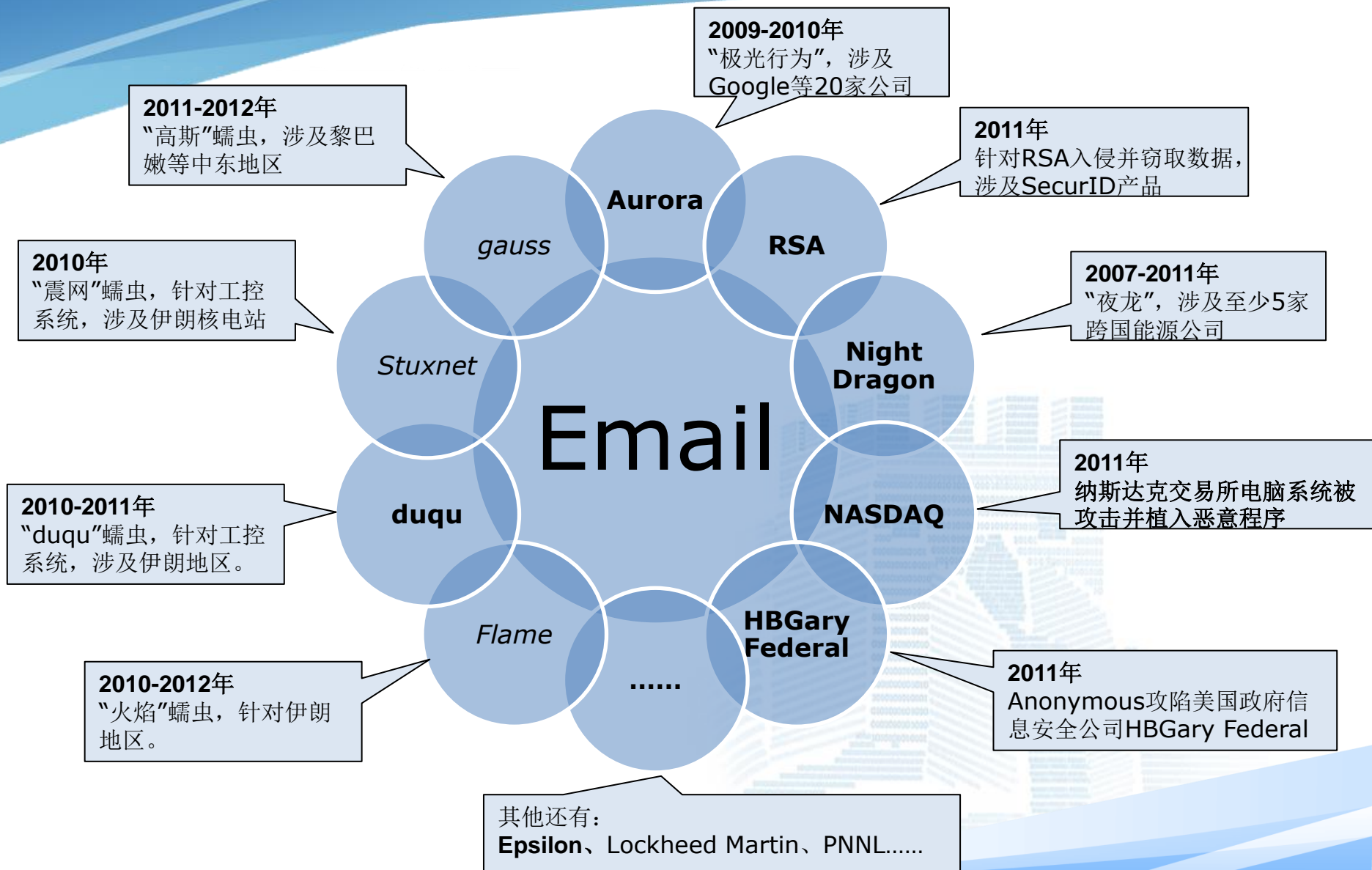
# 攻击前导

Watering Hole  
Drive-by download



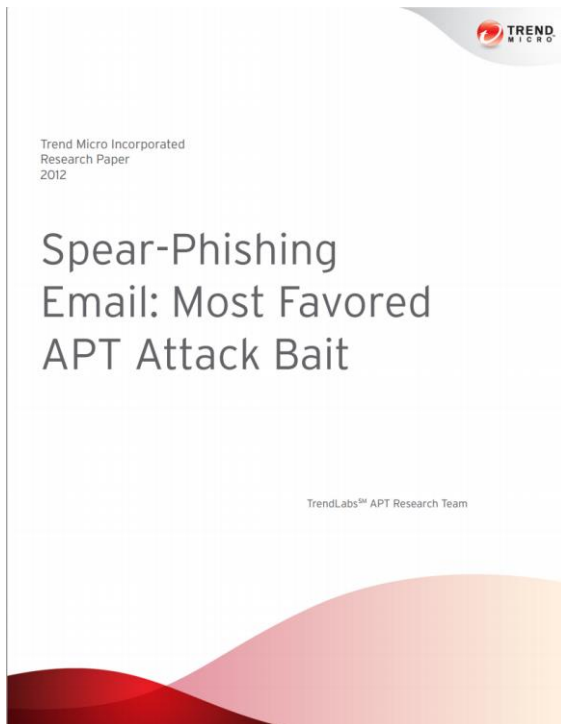
SQL injection、XSS、Social engineering.....

# 邮件载体的重要性



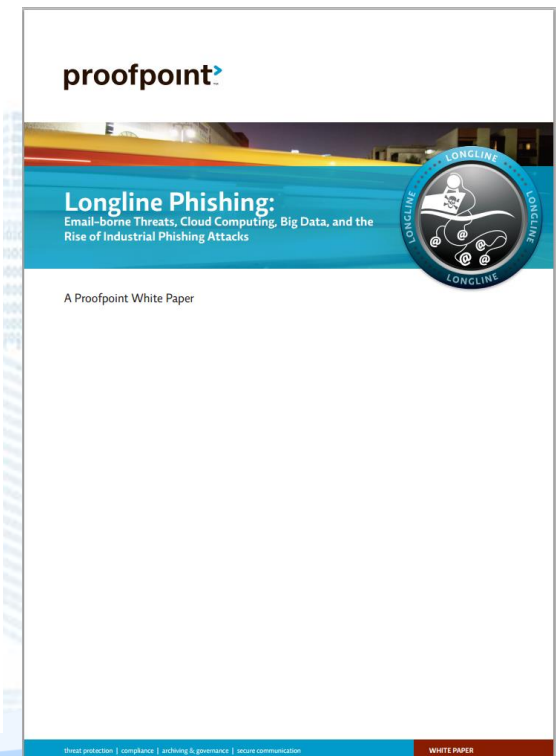
# 邮件威胁

- ❖ Spear-Phishing ( 鱼叉式攻击 )
- ❖ Targeted Malicious Email ( 针对性恶意邮件 ) —— 《DETECTING TARGETED MALICIOUS EMAIL THROUGH SUPERVISED CLASSIFICATION OF PERSISTENT THREAT AND RECIPIENT ORIENTED FEATURES》
- ❖ Proofpoint : Longline Phishing Attacks ( 延绳钓 ? )



		Email Distribution	
		broad	targeted
Motivation	financial	SPAM Phishing	Spear Phishing
	pride	Email Worms	
	sensitive data		Targeted Malicious Email (TME)

Figure 1.2: Email taxonomy



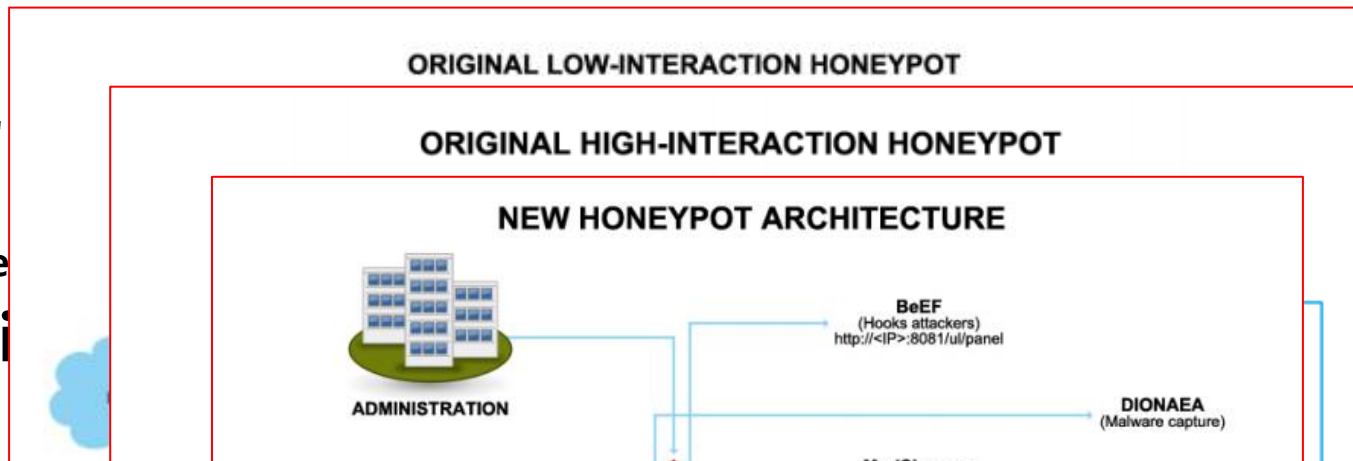
# Honeypot

## ❖ 传统行为分析



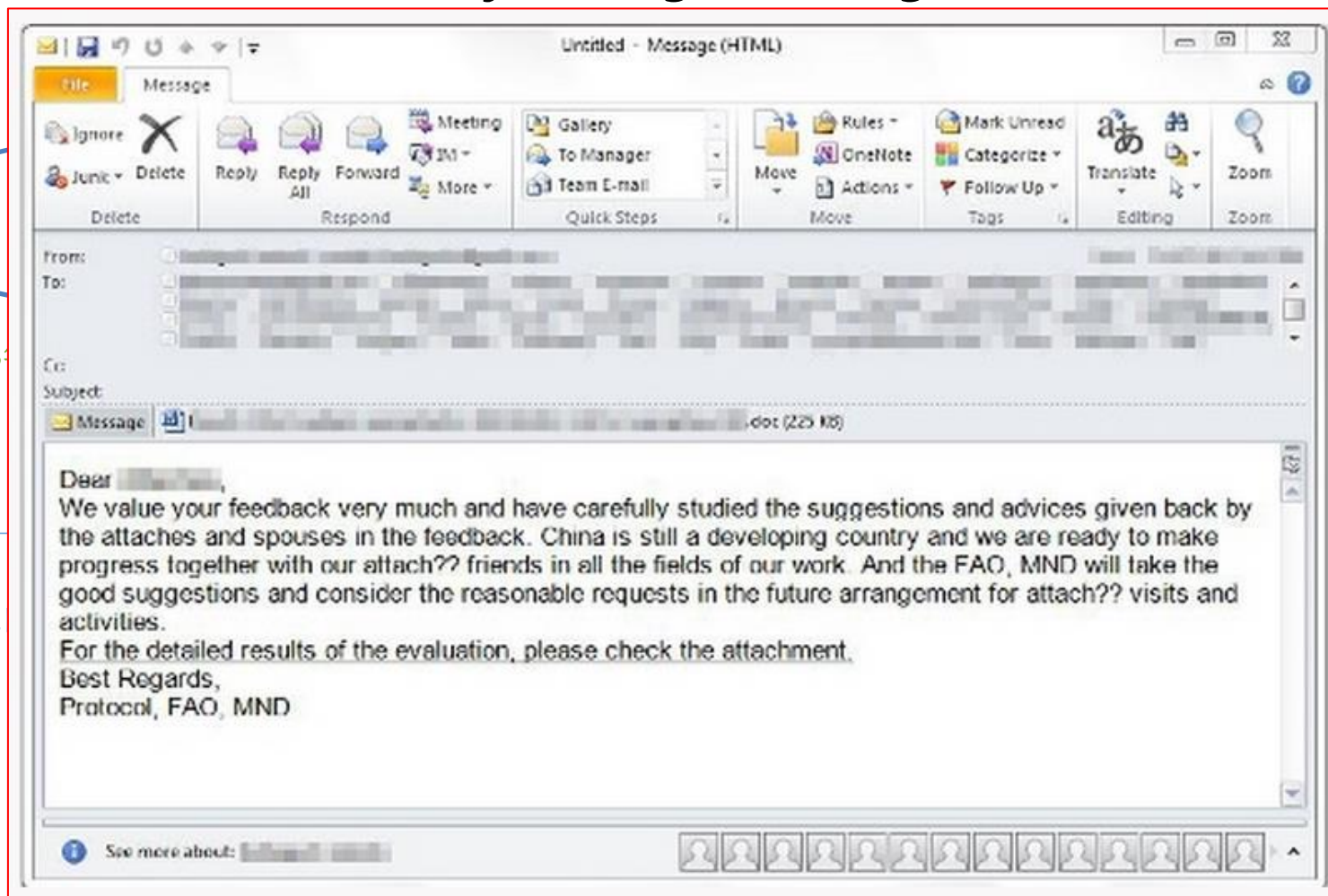
# Honeypot

❖ 蜜罐诱饵  
趋势水电站  
Your ICS Equipme  
卡斯基Wi



The screenshot shows the SECURELIST website interface. At the top, there is a green navigation bar with 'Threats', 'Analysis', 'Blog' (highlighted), and 'Statistics'. Below the navigation bar, a breadcrumb trail reads: Home → Blog → Research → April 11 2013 → The Winnti honeypot - luring intruders. The main content area features a red-bordered box containing the title 'The Winnti honeypot - luring intruders'. Below the title is a profile picture of Dmitry Tarakanov, followed by his name 'Dmitry Tarakanov', his title 'Kaspersky Lab Expert', the post date 'Posted April 11, 13:23 GMT', and a list of tags: 'Tags: Rootkits, Online Games, Certificate authorities, Cyber espionage, Spearphishing, Winnti'.

## ❖ TrendLabs Security Intelligence Blog



2013

11月27日

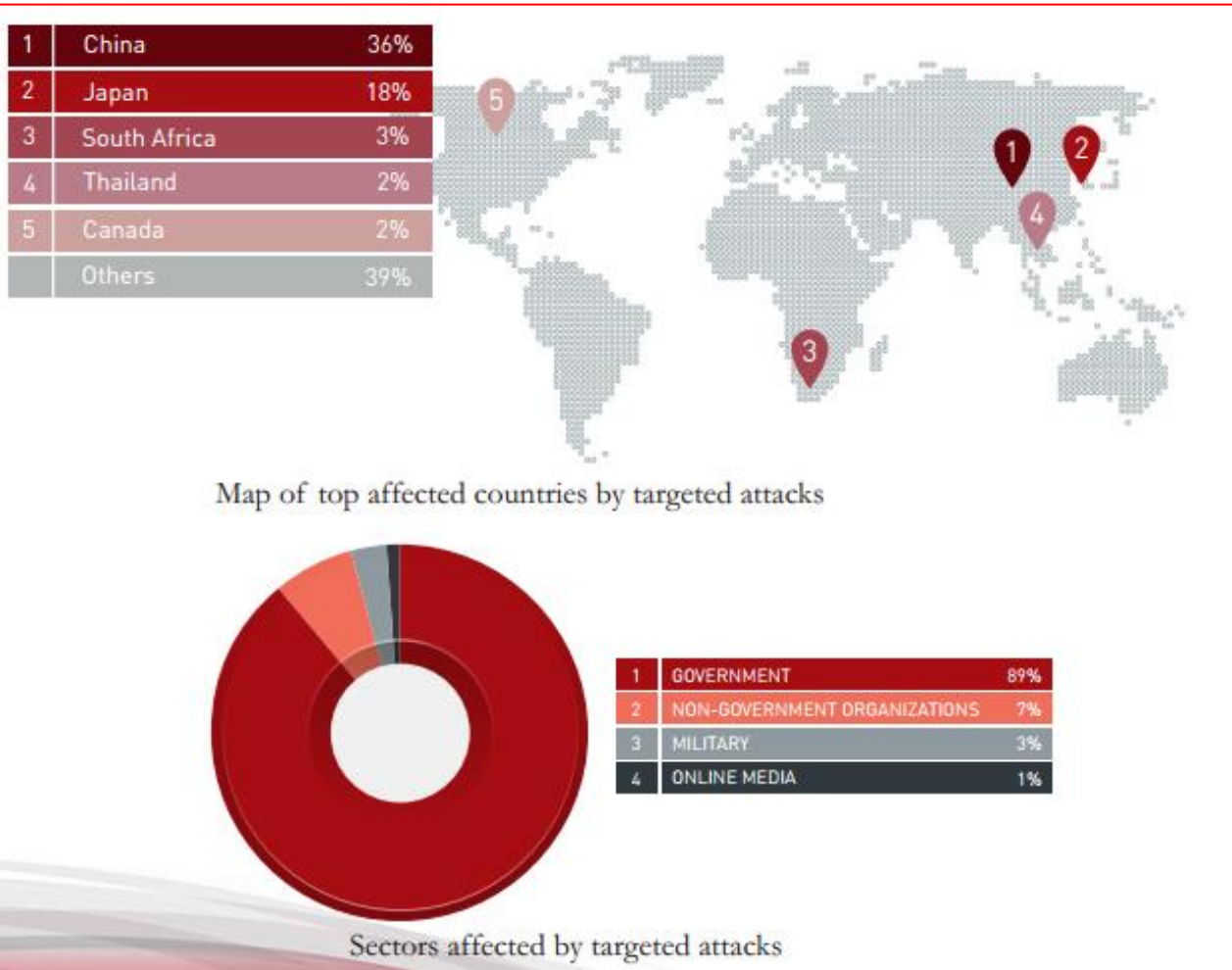
2013年7月1

2013年11月30日

## ❖ TrendLabs Security Intelligence Blog

Targeted  
Asia  
Governme

2013年7月15日



年11月27日

2013年11月30日

2013年7月1日

## ❖ TrendLabs Security Intelligence Blog

Targeted Attacks Hit  
Asian, European  
Government Agencies

EvilGrab Malware Family  
Used In Targeted Attacks  
In Asia

2013年7月1日

*Update as of September 26, 2013*

2013年11月27日

The MD5 hashes of the files involved in this attack are:

- 2E991260E42266DB9BCCFA40DC90AE16
- 7ED71CF0B98E60CC5D4296220F47C5A2

2013年11月30日

更新两个样本HASH

2013年7月1日



## ❖ TrendLabs Security Intelligence Blog

Targeted At  
Asian, E  
Government

2013年7月15日

SHA256: 872ced09e28da56322af6cff6e7f9d4d41cdf2d34a99  
File name: 最新版本的请愿书-让我们一同为书记呐喊 (请修改  
Detection ratio: 32 / 47  
Analysis date: 2013-11-21 07:49:23 UTC ( 1 month, 3 weeks ago



2013年9月26日

更新两个样本HASH

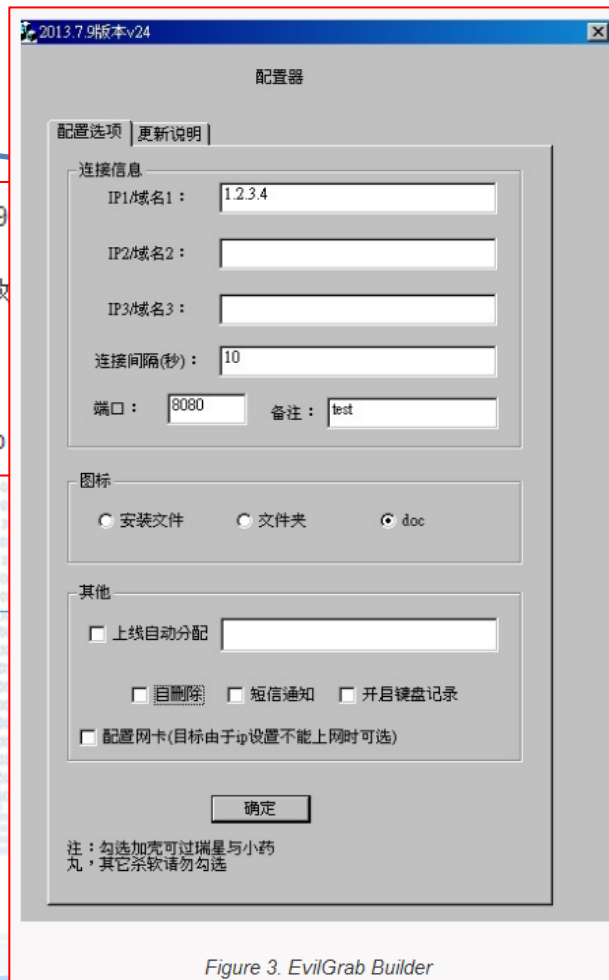
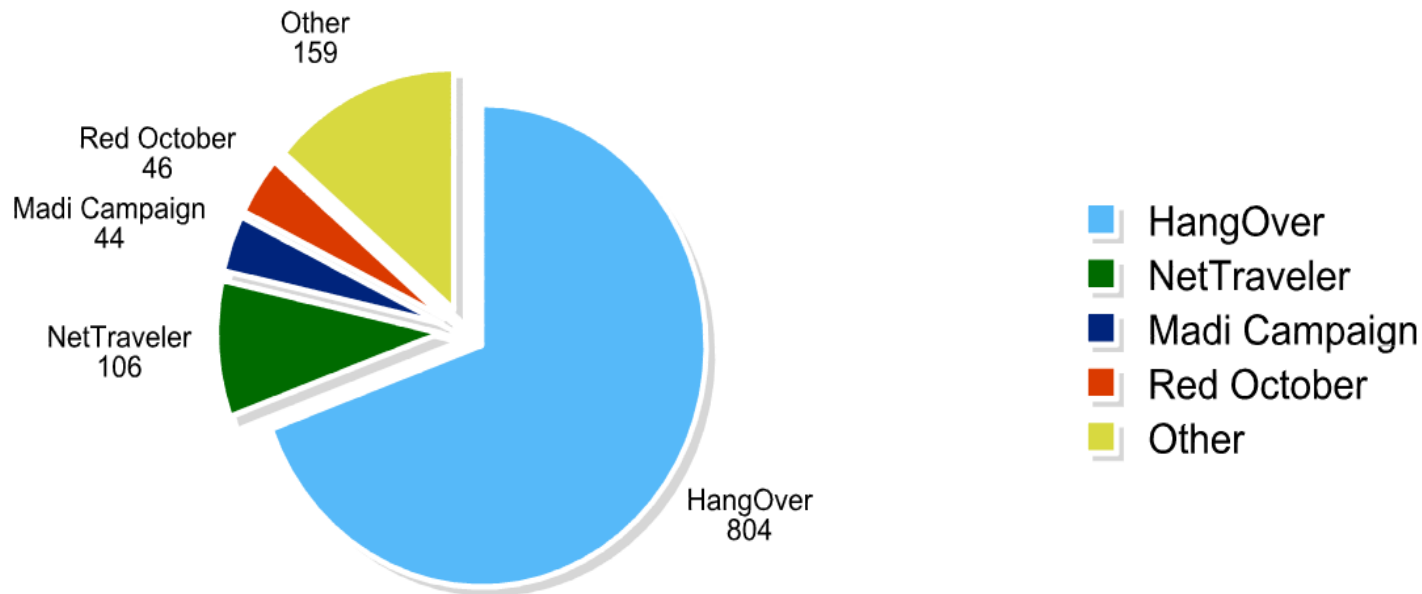


Figure 3. EvilGrab Builder

# 选定目标集合



2012年至2013年相对影响力较大的，变种数量较多的一些APT事件、网络间谍事件，将事件相关分析报告中公布的恶意样本HASH值汇总，并在相关系统数据中进行检索。事件包括2012的“红色十月”、“Madi运动”和2013年的“NetTraveler”和印度的网络间谍活动（HangOver）。另外还搜集了一些相对变种数量较少的窃密样本hash值（Other）

# HASH集合与样本查询命中中的统计

数据查询量与命中量对比



事件名称	hash数量	命中数量	命中率
HangOver	804	158	20%
NetTraveler	106	12	11%
Madi Campaign	44	11	25%
Red October	46	4	9%
other	159	9	6%
总数	1159	194	17%

# HASH集合与前台查询命中的统计

探针捕获时间	样本hash列表	代号
<b>2012-08-10</b>	0D46*****	Sample 1
<b>2012-10-21</b>	734E*****	Sample 2
<b>2012-07-24</b>	9A20*****	Sample 3
<b>2012-07-06</b>	CE00*****	Sample 4
<b>2012-09-24</b>	DE81*****	Sample 5
<b>2012-08-01</b>	F37D*****	Sample 6

我们将相关HASH列表与前台探针的检测、捕获日志进行了比对，发现前台探针共捕获了6个样本的事件。这6个样本均来自“HangOver”印度网络攻击中的APT样本。

# 样本的第三方检测情况

Sample	卡巴	BitDefender	微软	江民	小红伞	McAfee	金山	瑞星	Norton	命中率
Sample 1										0/9
Sample 2	✓	✓		✓	✓					4/9
Sample 3		✓						✓	✓	3/9
Sample 4										0/9
Sample 5	✓									1/9
Sample 6										0/9
以上是样本捕获时入库对照扫描结果										
Sample 1	✓	✓	✓		✓					4/9
Sample 2	✓	✓	✓	✓	✓				✓	6/9
Sample 3	✓	✓	✓	✓	✓				✓	6/9
Sample 4	✓	✓		✓	✓				✓	5/9
Sample 5	✓	✓			✓					3/9
Sample 6	✓	✓	✓	✓	✓			✓	✓	7/9
以上是 2013 年 08 月 20 日对应样本对照扫描结果										

# 样本情况

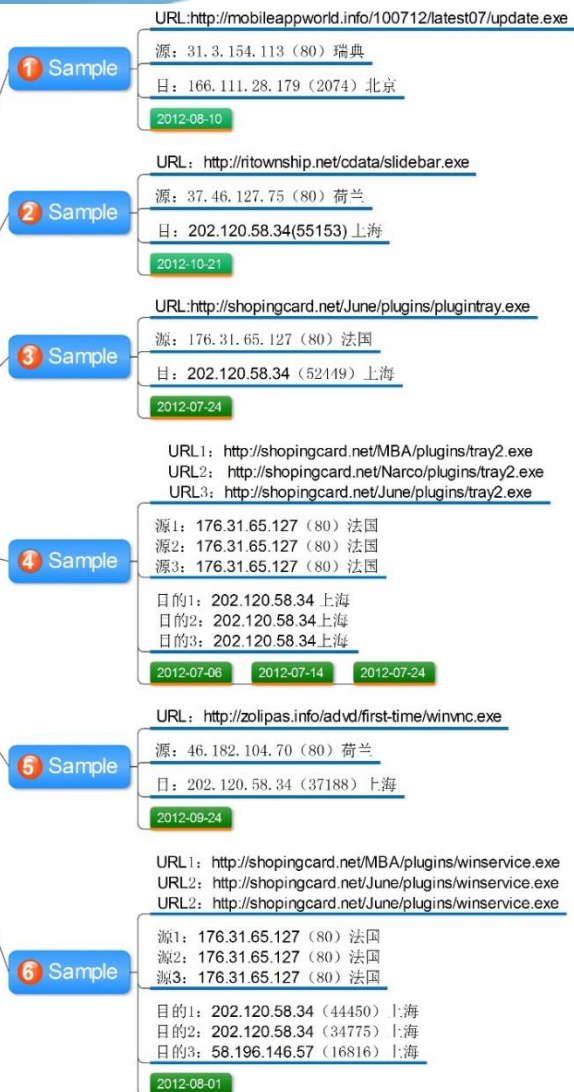
	壳	编译器	主要行为
<b>Sample 1</b>	无	Microsoft Visual Basic 5.0 / 6.0	释放的VBScript脚本,脚本执行后连接远程服务器zolipas.info。(域名失效)。
<b>Sample 2</b>	无	Microsoft Visual Studio .NET 2005 -- 2008	运行后将 以下文件设置为Run自启 C:\WINDOWS\system32\CatRoot2\ {F750E6C3-38EE-11D1-85E5- 00C04FC295EE}\slidebar.exe, 后续无其他行为
<b>Sample 3</b>	UPX 0.89.6 - 1.02 / 1.05 - 1.24	Dev-C++ 4.9.9.2	运行后在C:\ApplicationData\Prefetch\ 目录下生存log.txt文件,不断的记录键盘、窗口标题、浏览器搜索内容、计算机用户名等信息。
<b>Sample 4</b>	UPX 0.89.6 - 1.02 / 1.05 - 1.24	Microsoft Visual C++ 7.0	运行后链接域名secureplanning.net欲下载其他恶意代码(URL失效)。
<b>Sample 5</b>	无	Microsoft Visual Studio .NET 2005 -- 2008	运行后在 c:\Documents and Settings\Administrator\Local Settings\Application Data\NTUSR\目录下创建文件ntusr1.ini进行键盘记录
<b>Sample 6</b>	无	Dev-C++ 4.9.9.2	样本运行后在 C:\ApplicationData\ 目录下释放logFile.txt文件,收集各种相关扩展名文档名称。

# 最新的对照命名情况

	Sample1	Sample2	Sample3	Sample4	Sample5	Sample6
卡巴	Trojan-Downloader. Win32. VB.bkrb	Trojan-Spy.  Win32.  KeyLogger.actw	Trojan-Spy.  Win32.  KeyLogger.absi	Trojan.Win32.  Agent.sryd	Trojan-Spy.Win32.  KeyLogger.acqh	Trojan.Win32.  Agent2.fhog
McAfee	未识别	未识别	未识别	未识别	未识别	未识别
Norton	未识别	Infostealer	Trojan.ADH	Trojan.Gen.2	未识别	Trojan.Gen
金山	未识别	未识别	未识别	未识别	未识别	未识别
瑞星	未识别	未识别	未识别	未识别	未识别	Trojan.Win32.Generic.12D C27CD
江民	未识别	Backdoor/Agent.doyw	TrojanSpy.KeyLogger. cwwy	Trojan/Agent.gnxxm	未识别	Trojan/Agent.gkpg
小红伞	TR/Zoli.A	TR/Agent.74328.1	TR/Agent.21265	TR/Spy.21504.351	WORM/Agent.22813	TR/Offend.KD.532260
微软	TrojanDownloader:Win32/Ado db.A	TrojanSpy:Win32/Key logger.CB	Trojan:Win32/Sulunc h	未识别	未识别	Trojan:Win32/Sulunch
BitDefender	Trojan.Generic.KDV.735533	Trojan.Spy.Keylogger .WY	Trojan.Generic.76421 55	Gen:Trojan.Heur.RP.b mGfa05AQRai	IRC- Worm.Generic.22813	Trojan.Generic.KD.532260

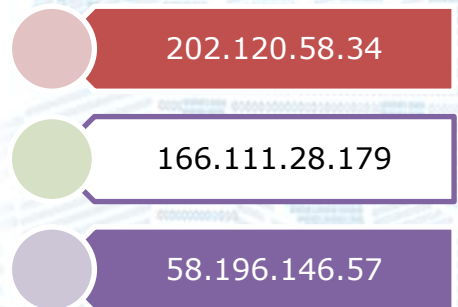
# 捕获样本事件串联

## 样本来源与目的IP



瑞典  
荷兰  
荷兰  
法国

涉及到4个域名

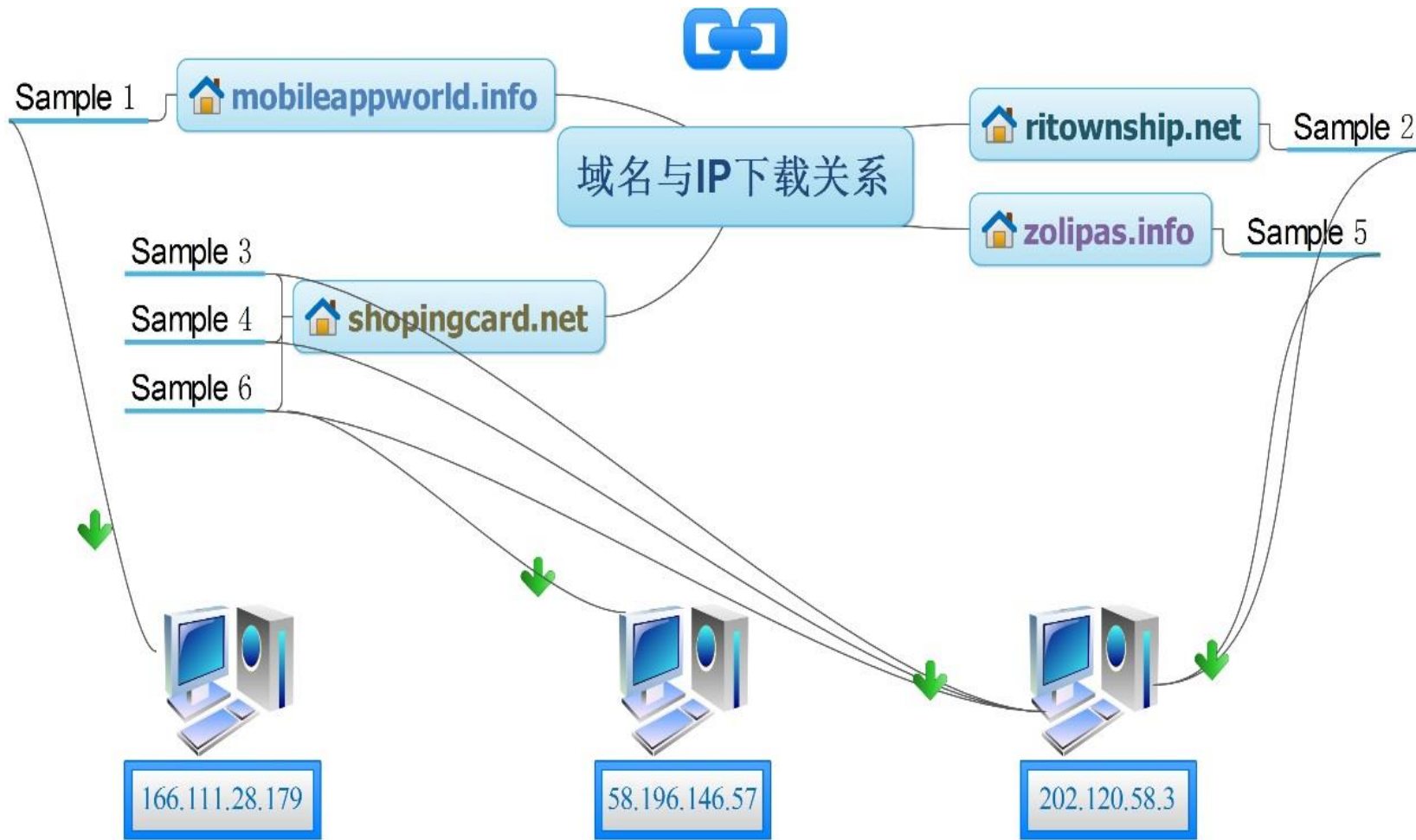


上海  
北京  
上海

捕获到3个目的IP

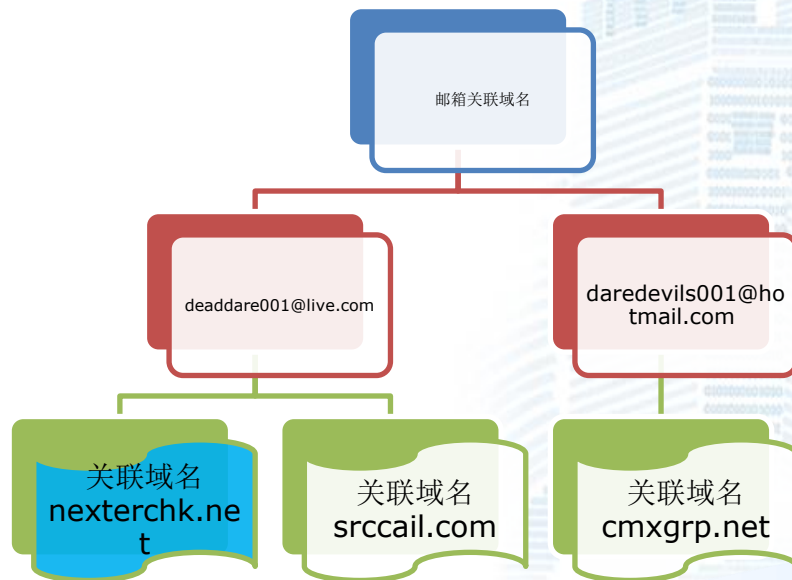


# 样本与资源间的关联



# 事件域名与IP的溯源

	mobileappworld.info	ritownship.net	shopingcard.net	zolipas.info
注册人姓名	过期很久	aman kumar	过期很久	amit Trivedi
注册时间	3年之前	2012.07.05		2012.06.23
更新时间		2013.08.04		2013.08.02
过期时间		2013.07.05	2013-02-22.	2014.06.23
联系方式		deaddare001@live.com		aredevils001@hotmail.com



# 目标IP的位置与原因

您查询的IP:202.120.58.34

- 本站主数据: 上海市 上海交通大学闵行校区
- 参考数据一: 上海市 上海交通大学闵行校区

您查询的IP:166.111.28.179

- 本站主数据: 北京市 清华大学
- 参考数据一: 北京市 清华大学

您查询的IP:58.196.146.57

- 本站主数据: 上海市 上海交通大学
- 参考数据一: 上海市 上海交通大学

IP地址段详细地址: 上海交通大学闵行校区 CZ88.NET

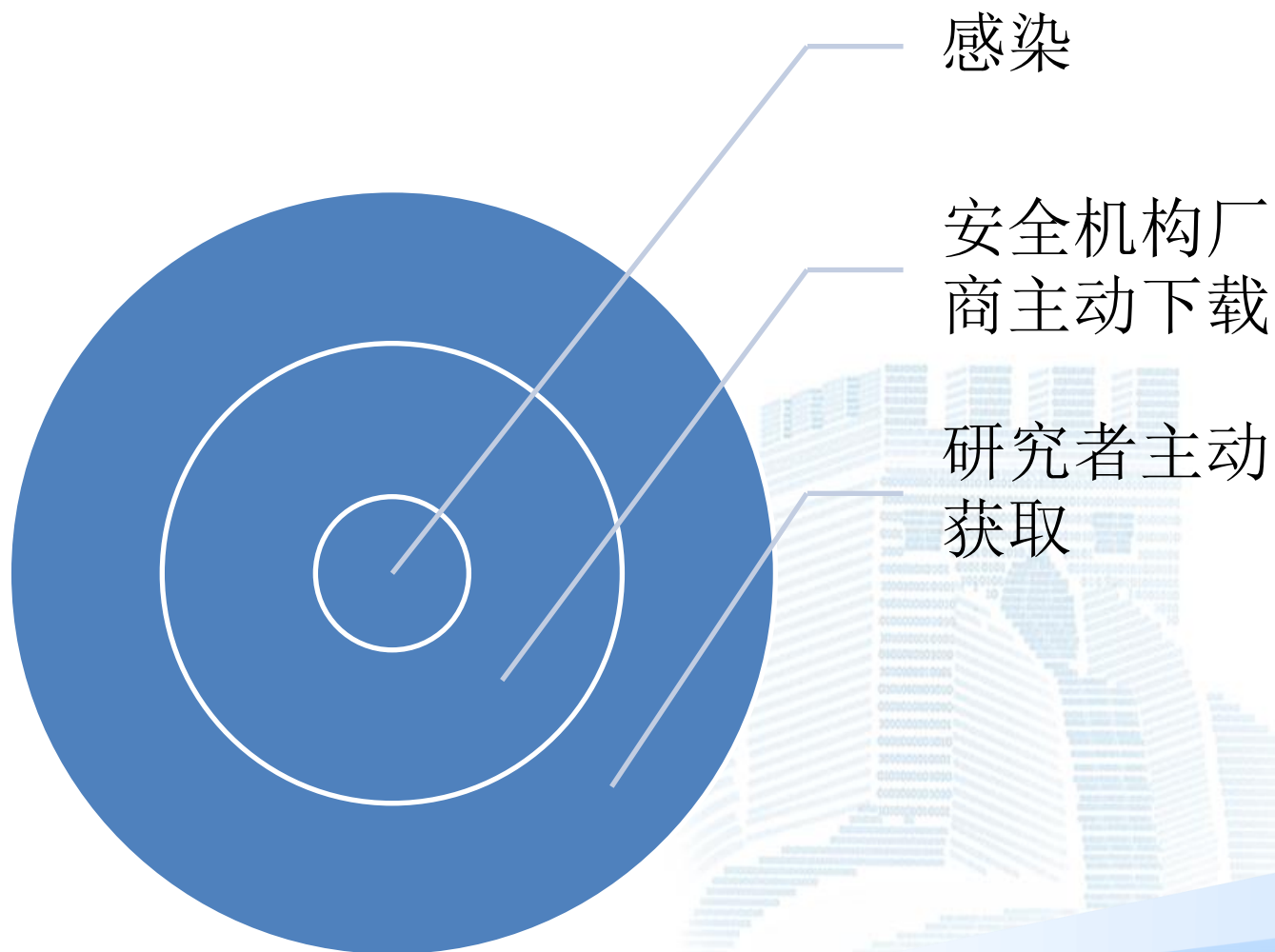
地址段IP详细列表

202.120.58.0 202.120.58.1 202.120.58.2 202.120.58.3 202.120.58.4 202.120.58.5 202.120.58.6  
202.120.58.7 202.120.58.8 202.120.58.9 202.120.58.10 202.120.58.11 202.120.58.12  
202.120.58.13 202.120.58.14 202.120.58.15 202.120.58.16 202.120.58.17 202.120.58.18  
202.120.58.19 202.120.58.20 202.120.58.21 202.120.58.22 202.120.58.23 202.120.58.24  
202.120.58.25 202.120.58.26 202.120.58.27 202.120.58.28 202.120.58.29 202.120.58.30  
202.120.58.31 202.120.58.32 202.120.58.33 202.120.58.34 202.120.58.35 202.120.58.36  
202.120.58.37 202.120.58.38 202.120.58.39 202.120.58.40 202.120.58.41 202.120.58.42  
202.120.58.43 202.120.58.44 202.120.58.45 202.120.58.46 202.120.58.47 202.120.58.48  
202.120.58.49 202.120.58.50 202.120.58.51 202.120.58.52 202.120.58.53 202.120.58.54  
202.120.58.55 202.120.58.56 202.120.58.57 202.120.58.58 202.120.58.59 202.120.58.60  
202.120.58.61 202.120.58.62 202.120.58.63 202.120.58.64 202.120.58.65 202.120.58.66  
202.120.58.67 202.120.58.68 202.120.58.69 202.120.58.70 202.120.58.71 202.120.58.72

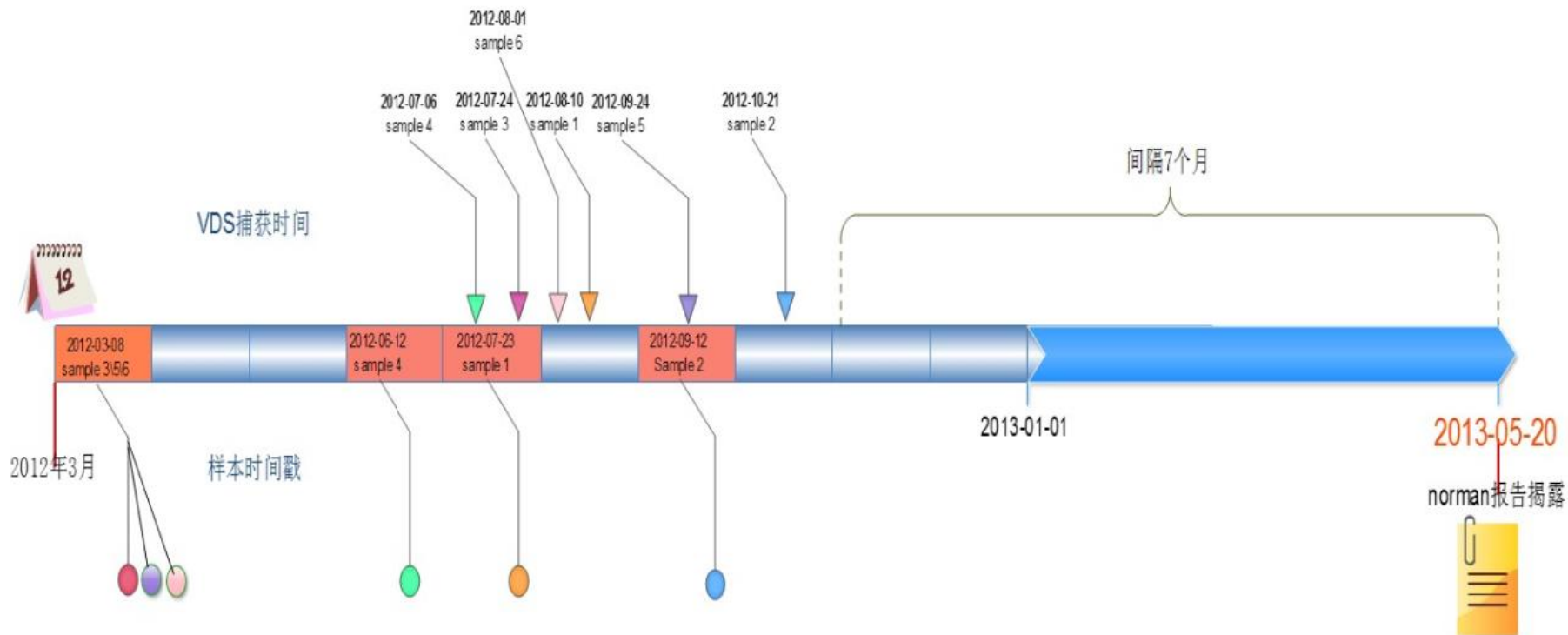


| 166.111.022.000 | 166.111.023.255 | 清华大学四教/旧水利馆  
| 166.111.025.000 | 166.111.025.255 | 清华大学应用数学系(理学院馆群)  
| 166.111.026.000 | 166.111.027.255 | 清华大学现代应用物理系(理学院馆群)  
| 166.111.028.000 | 166.111.028.255 | 清华大学化学系  
| 166.111.030.000 | 166.111.030.255 | 清华大学生物系(生命科学馆)  
| 166.111.032.000 | 166.111.032.255 | 清华大学工程物理系(工物馆)  
| 166.111.033.000 | 166.111.033.127 | 清华大学工物馆/化工馆

# 事件成因分析



# 时间链



# 捕获时间与URL互联网公开时间

捕获日期	公开日期	目的 IP	URL
2012/10/21	2012/09/20	202.120.58.34	http://ritownship.net/cdata/sidebar.exe
2012/7/24	未公开	202.120.58.34	http://shopingcard.net/June/plugins/plugintray.exe
2012/7/24	2012/07/24	202.120.58.34	http://shopingcard.net/June/plugins/tray2.exe
2012/7/14	未公开	202.120.58.34	http://shopingcard.net/Narco/plugins/tray2.exe
2012/7/6	未公开	202.120.58.34	http://shopingcard.net/MBA/plugins/tray2.exe
2012/7/25	2012/07/24	202.120.58.34	http://shopingcard.net/June/plugins/winservice.exe
2012/7/23	未公开	202.120.58.34	http://shopingcard.net/MBA/plugins/winservice.exe
2012/9/24	未公开	202.120.58.34	http://zolipas.info/advd/first-time/winvnc.exe
2012/8/10	未公开	166.111.28.179	http://mobileappworld.info/100712/latest07/update.exe
2012/8/1	2012/07/24	58.196.146.57	http://shopingcard.net/June/plugins/winservice.exe

# 捕获与公开时间对比

## 根据IP位置统计URL公开数量

清华大学

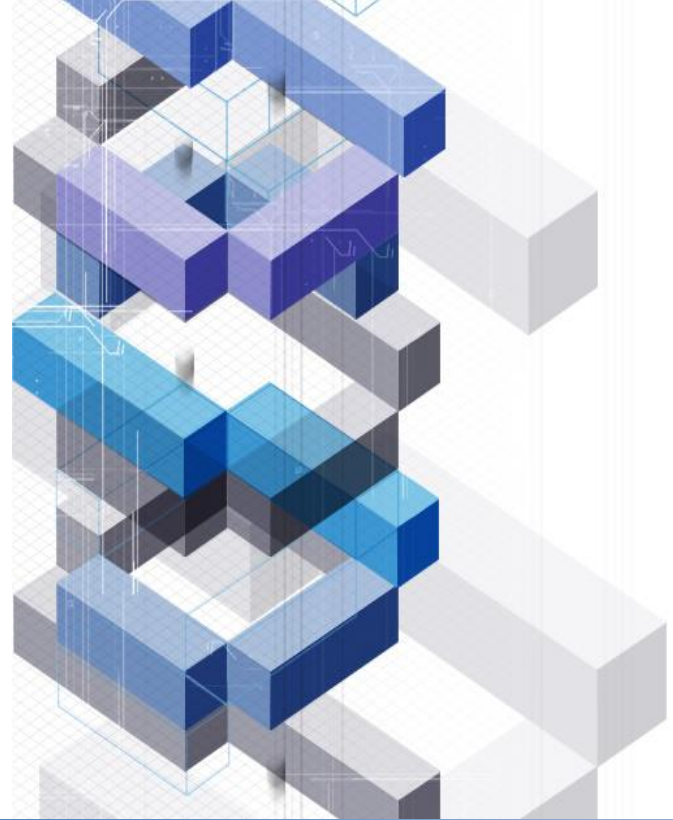
- <http://mobileappworld.info/100712/latest07/update.exe> 未被公开

上海交大闵行校区

- <http://ritownship.net/cdata/sliderbar.exe> 公开早于捕获时间31天
- <http://shopingcard.net/June/plugins/plugintray.exe> 未被公开
- <http://shopingcard.net/June/plugins/tray2.exe> 公开早于捕获6个小时
- <http://shopingcard.net/Narco/plugins/tray2.exe> 未被公开
- <http://shopingcard.net/June/plugins/winservice.exe> 公开早于捕获1天
- <http://shopingcard.net/MBA/plugins/tray2.exe> 未被公开
- <http://shopingcard.net/MBA/plugins/winservice.exe> 未被公开
- <http://zolipas.info/advd/first-time/winvc.exe> 未被公开

上海交大

- <http://shopingcard.net/June/plugins/winservice.exe> 公开早于捕获1天

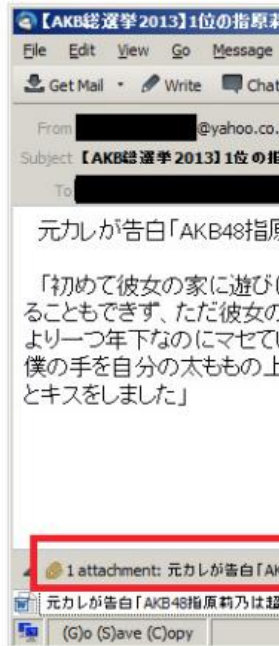


# 关联分析方法

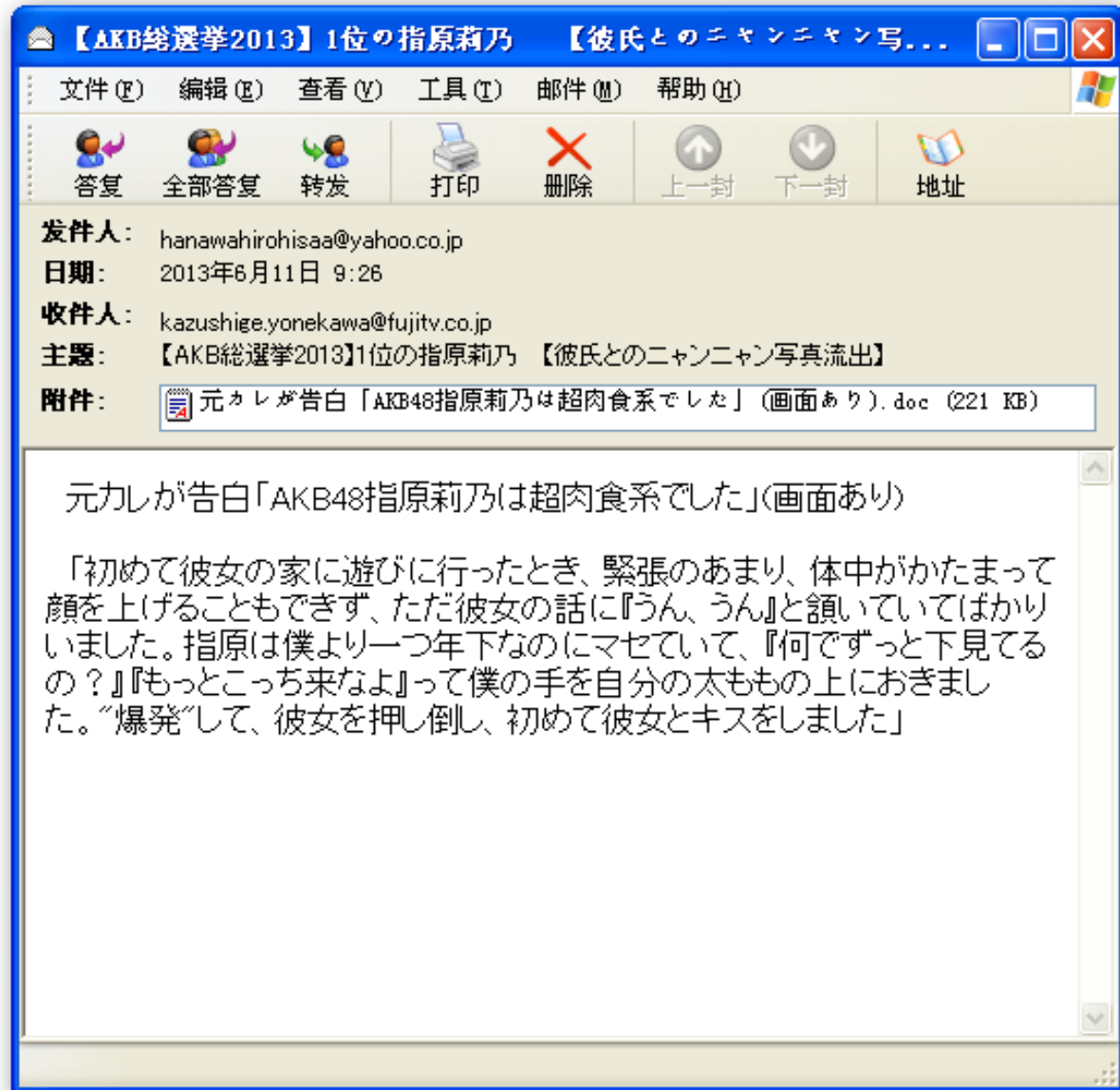


# 单事件纵向关联——ICEFOG

The attachment is a standard "Tran



Sai



# ICEFOG——EXAMPLE 'A'

 virustotal

2013年6月12日

 ANTIY 安天

2013年7月29日

 KASPERSKY

2013年9月25日

 KASPERSKY

2014年1月14日



 ANTIY 安天

关联出其他4个

# 从ICEFOG看卡巴斯基的分析方法

## 攻击目标

- 国家
- 行业领域
- .....

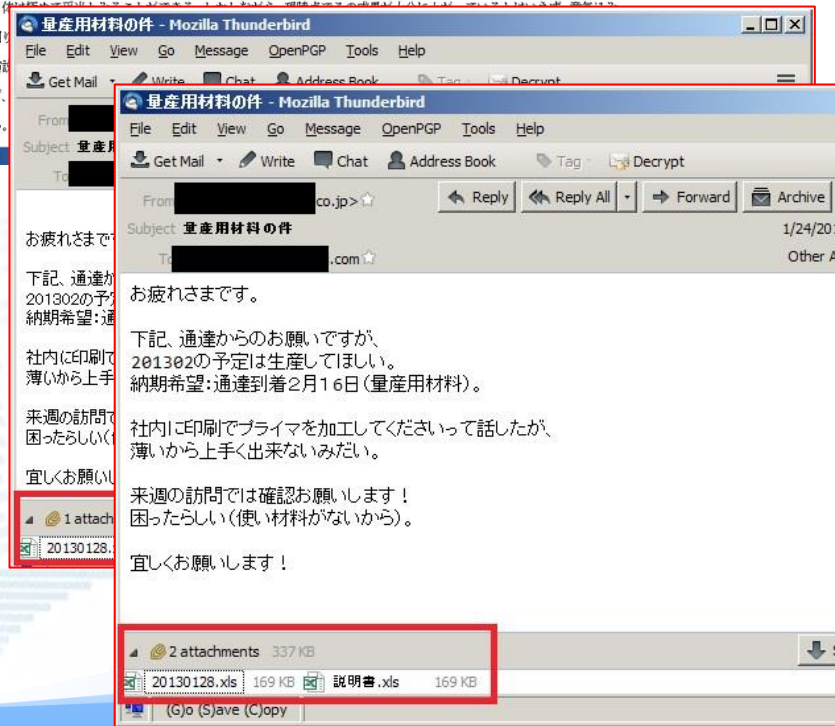
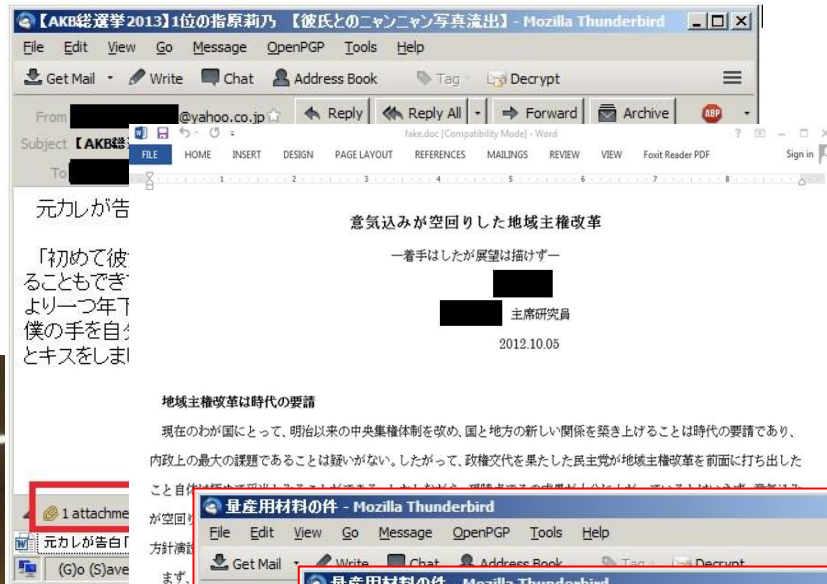
## 攻击前导

- 邮件
- IM
- 智能终端
- .....

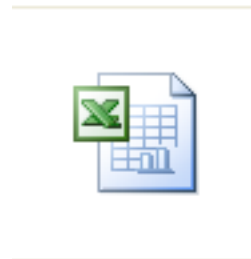
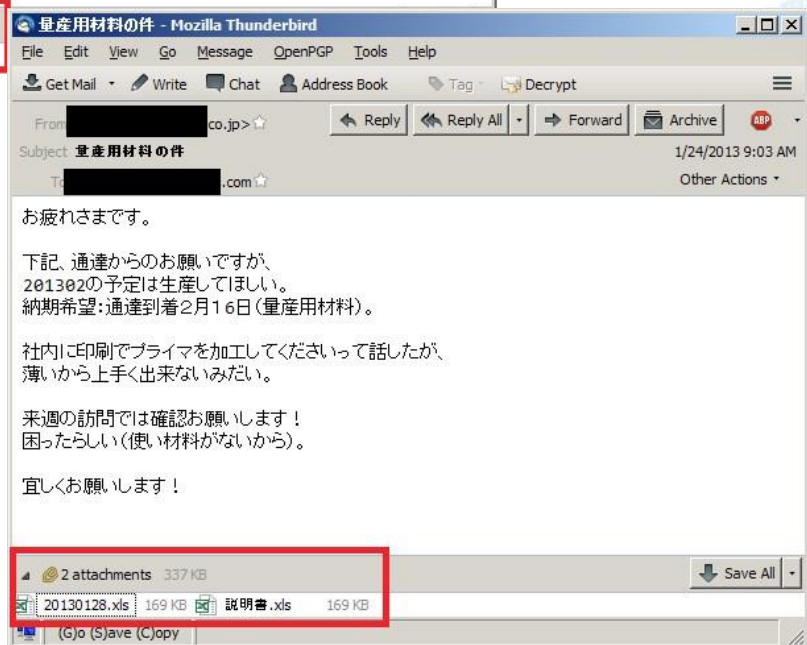
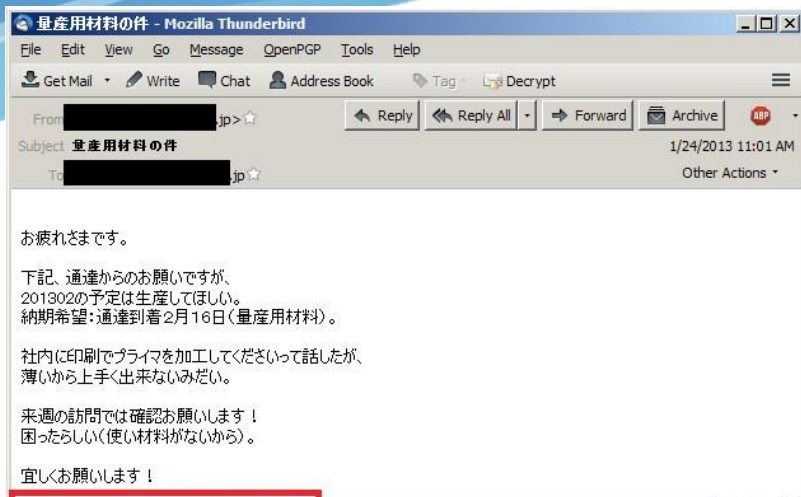
## 行为特征

- 互斥量
- C&C
- 衍生文件路径
- .....

# ICEFOG分析——攻击目标



# ICEFOG分析——攻击前导



20130128.xls



# ICEFOG分析——攻击前导



元カレが告白「AKB48  
指原莉乃は超肉食系で  
した」(画面あ

文档格式漏洞文件HASH

APT事件

561244132751410771410... ICEFOG

## ▶ ATTACK ANALYSIS



The Icefog targeted attacks rely on spear-phishing e-mails that attempt to trick the victim into opening a malicious attachment or a website.

During our investigation, we identified several types of exploits being used through spear-phishing e-mails against the targets:

- > CVE-2012-1856 (the "Tran Duy Linh" (also see: <http://blog.malwaretracker.com/2013/06/tomato-garden-campaign-possible.html>) exploit fixed in Microsoft's MS12-060 security bulletin)



# ICEFOG分析——行为相似性

## 互斥量

my\_horse\_mutex\_jd2\_new

my\_horse\_mutex\_jd2\_923

myhorse\_macfee

horse\_for360

.....

## 衍生文件路径

%TEMP%\msuc.dat

%TEMP%\order.dat

%TEMP%\cmd1.dat

%TEMP%\tmpxor.dat

.....

## HTTP AGENT域

"MyAgent"

"mydownload"

.....

## C2 PATH域

/jd/upload.aspx

/news/upload.aspx

/jd2web/upload.aspx

/jian3/upload.aspx

.....


## 硬编码异或值

\*&~^%@0hh8979

&\*^\*~^%9?i0h

# 开曼群岛律师事务所事件——元数据

发信时间	主题	发件人	收件人	收件人 (CC)	附件名
2013 年 5月21日	SHAREHOLDER agreement STAKIS	antony.duckworth @card.com.ky	david.collier@card. com.ky	rebecca.hum e@card.com .ky	Shareholder Agreement May 2103.doc
2013 年 5月17日	Director change	stcsama@emirate s.net.ae	antony.duckworth @card.com.ky	graham.ritch ie@card.com .ky	Client Director Change.doc





# 多事件横向关联

- ❖ Stuxnet和duqu
- ❖ hangover2和hangover1
- ❖ Statement案例
- ❖ “京东” 案例



# Stuxnet和duqu

## ❖ 事件间关联性

比较项目	Duqu木马	Stuxnet蠕虫
功能模块化		是
Ring0注入方式		PsSetLoadImageNotifyRoutine
Ring3注入方式		Hook ntdll.dll
注入系统进程		是
资源嵌入DLL模块	一个	多个
利用微软漏洞		是
使用数字签名		是
包括RPC通讯模块		是
配置文件解密密钥	0xae240682	0x01ae0000
注册表解密密钥		0xae240682
Magic number		0x90,0x05,0x79,0xae
运行模式判断代码存在Bug		是
注册表操作代码存在Bug		是
攻击工业控制系统	否	是
驱动程序编译环境	Microsoft Visual C++ 6.0	Microsoft Visual C++ 7.0

# hangover2和hangover1

## ❖ 事件间关联性 ( AlienVault )

Zeroday downloader

Hangover Deksila Downloader

This payload communicates with the C&C server using the HTTP protocol:

```
GET /logitech/rt.php?cn=XXXXX@Administrator&str=&file=no HTTP/1.1
User-Agent: WinInetGet/0.1
```

When we showed this traffic we realized it was familiar. In fact the same protocol was used by one of the [Operation Hangover](#) payloads. We can confirm that the downloader is based on the Deksila

```
InternetReadFile failed, error = %d (0x%x)
deliaf
Excep
&res=
failed
sucessfully
GET
&file=
&str=
?cn=
no
WinInetGet/0.1
CmshellcssOdn
tu-riq
Global{YS9JC88T7GB9-38NA7-94FDKHKY457}
```

```
InternetReadFile failed, error = %d (0x%x)
htt
p://
/downtab/
\temp\
sucessfully
&res=
Global{DF97D191AD-92E9-FC504RC25E9A8A3F}
/c xcopy "
" /Y
dekstop2007.ico
mozilla20
windows directory
```

# Statement案例：传统恶意？APT攻击？

**Merchant Statement - 西欧 (ISO)**

文件(F) 编辑(E) 查看(V) 工具(T) 邮件(M) 帮助(H)

答复 全部答复 转发 打印 删除 上一封

发件人: Citibank  
日期: 2013年5月29日 3:35  
收件人: panhm@ndrc.gov.cn  
主题: Merchant Statement  
附件: statement id 452-189.zip (222 KB)

Attached (xls|Excel file|document|file) is your Citibank Paymentech electronic Merchant Billing Statement. If you need help, please (contact|message|call) your Account Executive or call Merchant Services at the telephone number listed on your statement. PLEASE DO NOT RESPOND BY USING REPLY. This (email|mail) is sent from an unmonitored email address, and your response will not be received by Citibank Paymentech. Citibank Paymentech will not be responsible for any liabilities that may result from or relate to any failure or delay caused by Citibank Paymentech's or the Merchant's email service or otherwise. Citibank Paymentech recommends that Merchants continue to monitor their

**BOA Merchant Statement - 中欧 (Windows)**

文件(F) 编辑(E) 查看(V) 工具(T) 邮件(M) 帮助(H)

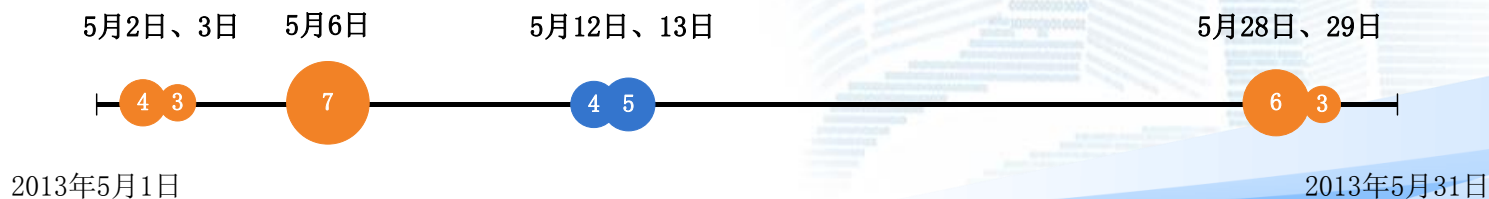
答复 全部答复 转发 打印 删除 上一封

发件人: Bank of AmericaK  
日期: 2013年5月13日 15:04  
收件人: info@payeshsanat.com  
主题: BOA Merchant Statement  
附件: BOA statement id 454-33-2463.doc (322 KB)

Enclosed (DOC|WORD file|document|file) is your Bank of America Paymentech electronic Merchant Billing Statement. If you need assistance, please (contact|message|call) your Account Executive or call Merchant Services at the telephone number listed on your statement. PLEASE DO NOT RESPOND BY USING REPLY. This (email|mail) is sent from an unmonitored email address, and your response will not be received by Bank of America Paymentech. Bank of America Paymentech will not be responsible for any liabilities that may result from or relate to any failure or delay caused by Bank of America Paymentech's or the Merchant's email service or otherwise. Bank of America Paymentech recommends that Merchants continue to monitor their

# Statement案例：邮件相关信息对比

	statement传统恶意攻击（共23封）	statement针对性攻击（共9封）
发信时间	2013年5月2日、3日、6日、28日和29日	2013年5月12日、13日
发信人	noreply@citibank.com noreply@secure.fundsexpress.com	noreply@bankofamerica.com
邮件主题	Merchant Statement	BOA Merchant Statement
收信人 (域统计)	@nekonet.co.jp @ms1.gsn.gov.tw @ndrc.gov.cn	@ms1.gsn.gov.tw @nekonet.co.jp
正文	花旗银行相关信息	美国银行相关信息
正文相似度	0.934386042472	0.994779832038
正文相似度	0.930820476968	
附件名	Statement ID 4657-345-347-0332.zip statement id 452-189.zip	BOA statement id 454-33-2463.doc
附件文件格式	ZIP压缩包	RTF
附件病毒名	Trojan[Spy]/Win32.Zbot.lvwb	Exploit/MSWord.CVE-2012-0158
PE病毒名 (最终释放)	Trojan[Spy]/Win32.Zbot.lvwb	Trojan[Spy]/Win32.Zbot.lnas



# Statement案例：“传统恶意”和“APT”相似性对比

相同处	
ID	特征或行为
1	Borland Delphi v3.0
2	释放的文件路径： c:\Documents and Settings\Administrator\Application Data\4-6位随机\4-6位随机.exe
3	释放的文件路径： c:\Documents and Settings\Administrator\Application Data\Microsoft\Address Book\Administrator.wab
4	释放的文件路径： c:\WINDOWS\SoftwareDistribution\DataStore\DataStore.edb
5	释放的文件路径： c:\WINDOWS\SoftwareDistribution\DataStore\Logs\edb.log
6	释放的文件路径： c:\WINDOWS\SoftwareDistribution\DataStore\Logs\edb.chk
7	衍生文件Administrator.wab MD5:
8	衍生文件edb.chk MD5: 99108371dd23582abcce511d841a1b38
9	注入到C:\WINDOWS\Explorer.EXE
10	随机开启本地UDP高端口
11	P2P网络行为
12	TCP访问随机域名
13	家族都是ZBOT

# “京东” 案例

京东网  
文件  
答复

发件人:  
日期:  
收件人:  
主题:  
附件:

亲爱的常字峰:

感谢您在京东商城 (<http://www.360buy.com>) 购物, 您订购的商品已经出库, 正在发往各地配送点, 到达配送点后, 我们将尽快为您送货。具体订单状态及到货时间请关注[订单详情](#)

**订单信息:**

订单编号: 15106176

订单总金额: **68069.00**

下单时间: 2012-6-15

支付方式: **网银付款**

**收货人: 常字峰**

产品信息

字数: 469 插入 100%

# “京东” 案例

订单详情.doc 属性

常规 自定义 摘要

属性	值
字符数	48
行数	1
段落数	1
比例	否
链接脏了吗?	0
备注	

来源

作者	Administrator
最后一次保存者	Administrator
修订版号码	3
应用程序名	Microsoft Office Word
公司	
创建日期	2012-5-31 16:51
最后一次保存的日期	2012-5-31 16:51
编辑时间	

<< 简化(M)

确定 取消 应用(A)

FireEye 2012年12月10日  
To Russia With Targeted  
Attack



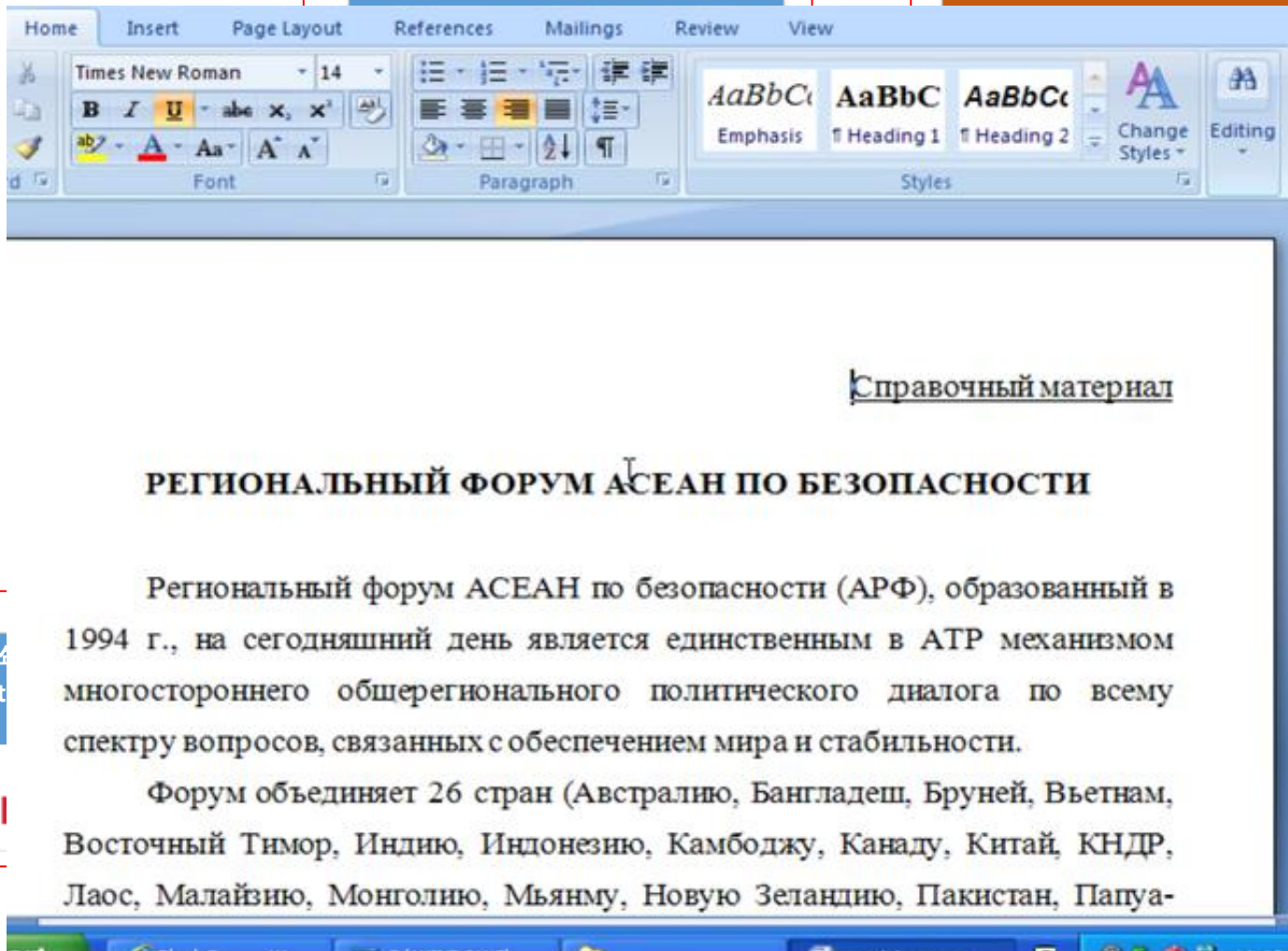
dw20.Exe  
37059c2f27e9fab9eae7bc85432

c:\Documents and  
Settings\Administrator\  
Application Data\Intel\  
Nensidit32.dll

371240c66655d6ad8cfb4869b5



# “京东” 案例



FireEye 2012  
To Russia With  
Attack

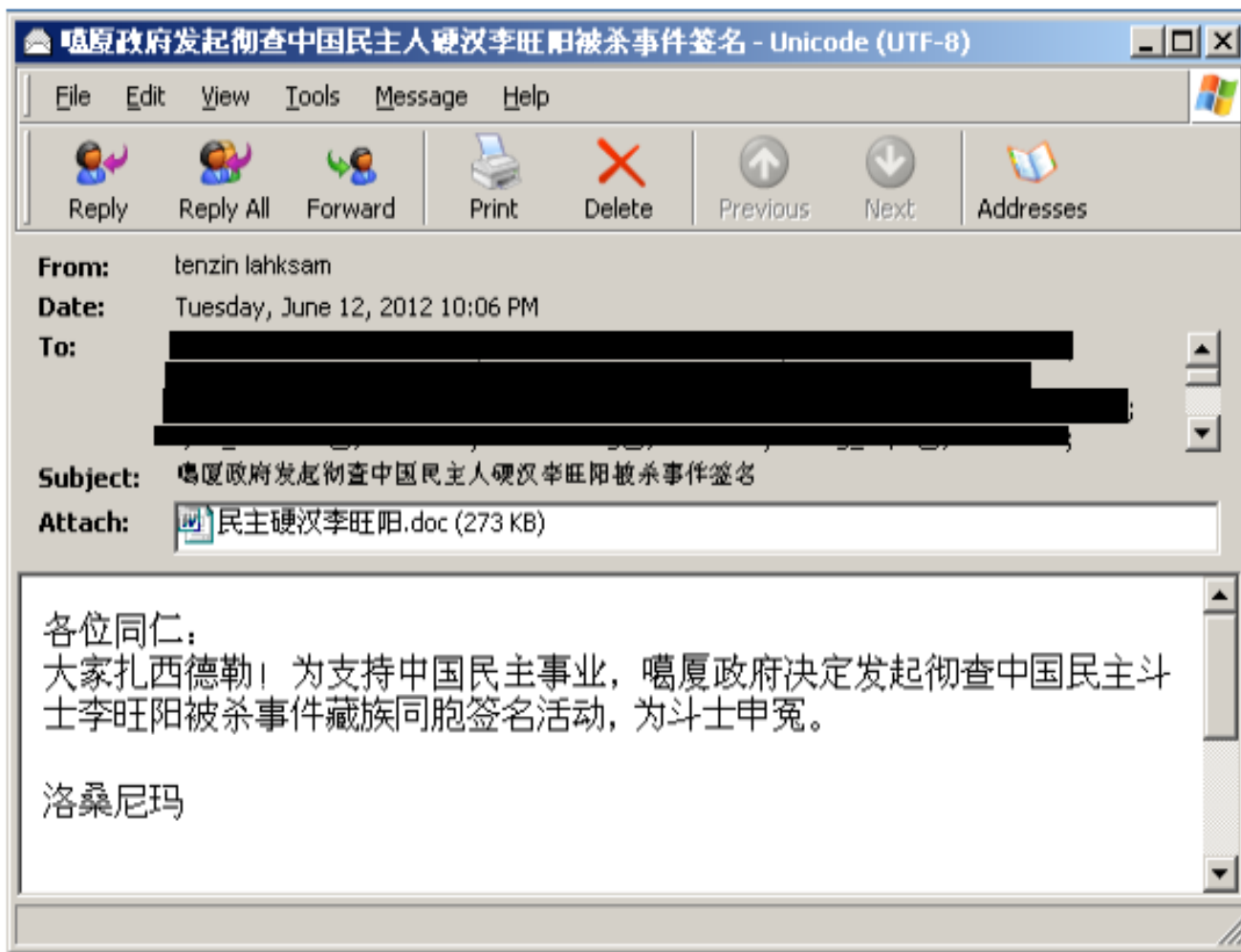


7bc85432

or/  
e/\

fb4869b5

# “京东” 案例



e7bc85432

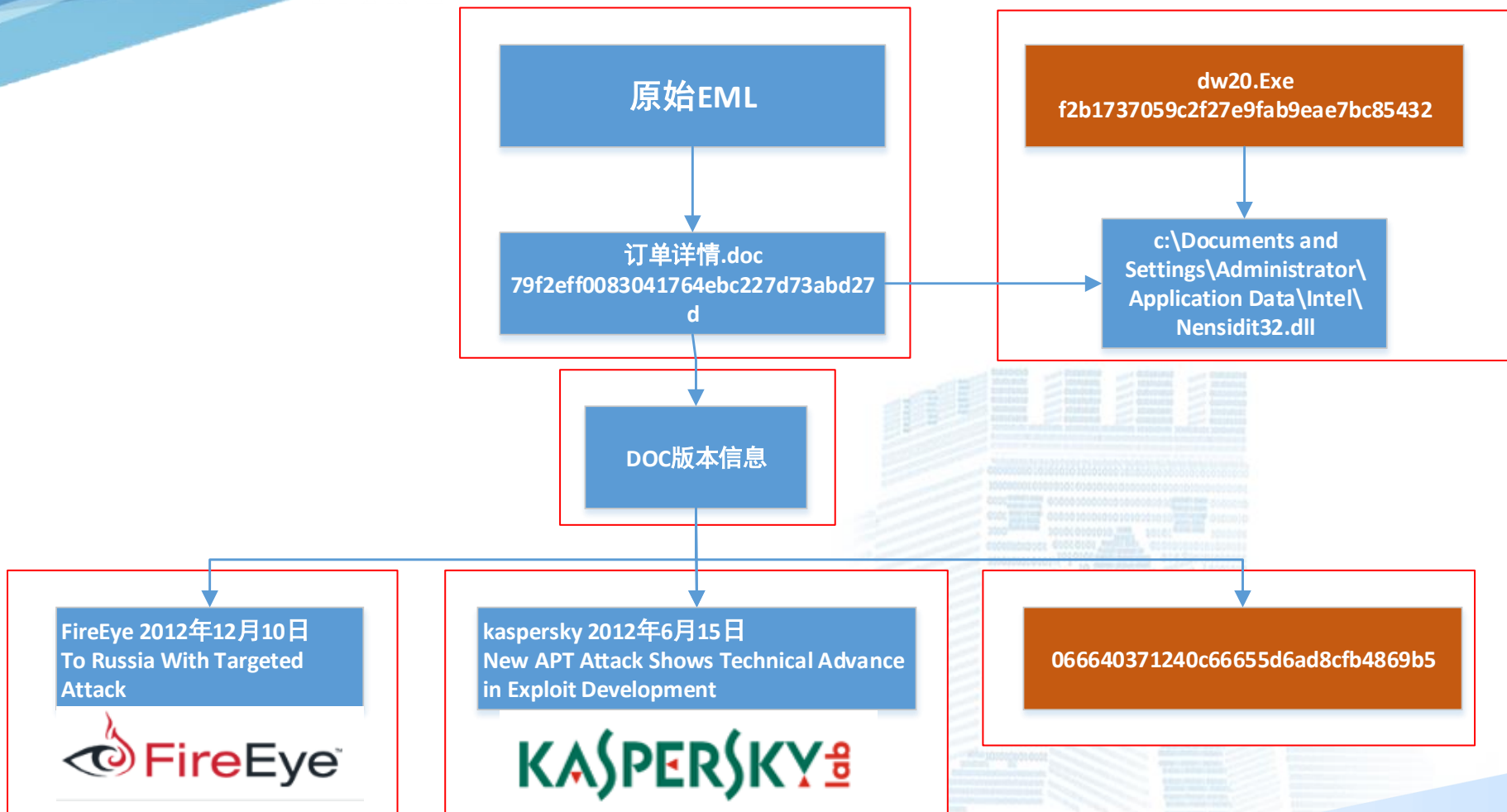
nd  
ator\  
ntel\

FireEye 2012年1月  
To Russia With T  
Attack



8cfb4869b5

# “京东” 案例



# 相关关联分析方法

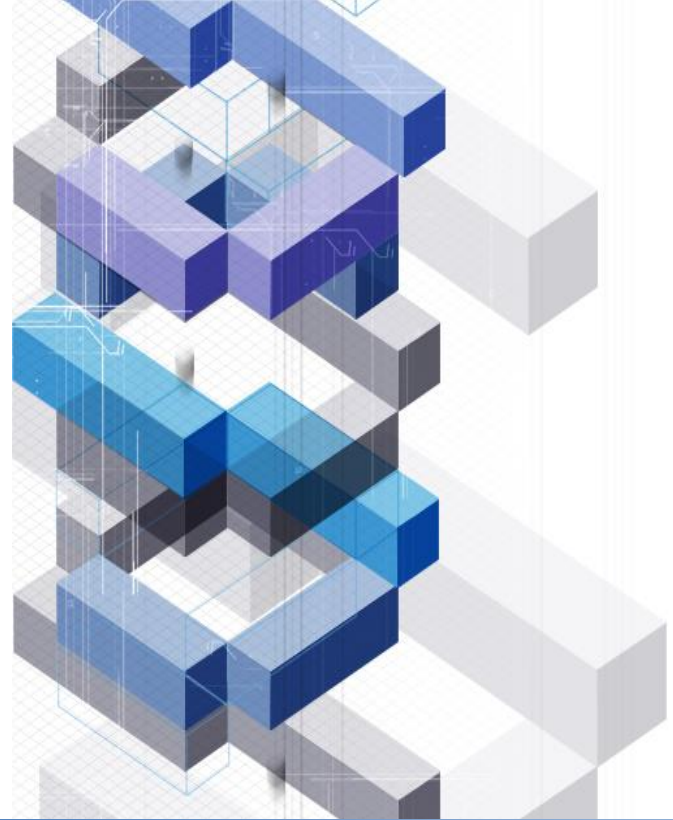
## 关联分析方法

### 前端（网络）

- Domain
  - 动态域名
    - 动态域名服务器提供商
  - 非动态域名
    - WHOIS
- IP
  - ASN
- URL Path
- port
- 网络数据包

### 后端（海量样本相关结果信息）

- 哈希
  - MD5
  - 模糊HASH
- 文件名
  - 语种
- 文件大小
- 版本信息
  - PE
  - 文档
- 时间戳
  - PE
  - 文档
- 互斥量
- 病毒名
- 衍生文件
  - 恶意
  - 正常
- 样本内部字符串信息
- .....



# 组织判定

# “虚拟”组织

THE 'I OF CL DAGG

MAND

The NetTravel

Operation "P

- Activists
- Government
- Military
- Financial
- Research
- Industrial
- Unknown
- Press
- Aerospace
- Private
- Health
- Diplomatic
- IT

- Government
- Diplomatic / embassies
- Research institutions
- Trade and commerce
- Nuclear / energy research
- Oil and gas companies
- Military
- Aerospace
- Unknown victims

KAS

## Contents

- Executive Summary
- Winnti 1.0 Technical
- Real Case Investigation
- Source of Attack
- The Search for
- Conclusions...
- Appendix.....

Symantec

## SECURITY RESPONSE

### Hidden Lynx – Professional Hackers for Hire

Stephen Doherty,  
Jozsef Gegeny,  
Branko Spasojevic,  
Jonell Baltazar

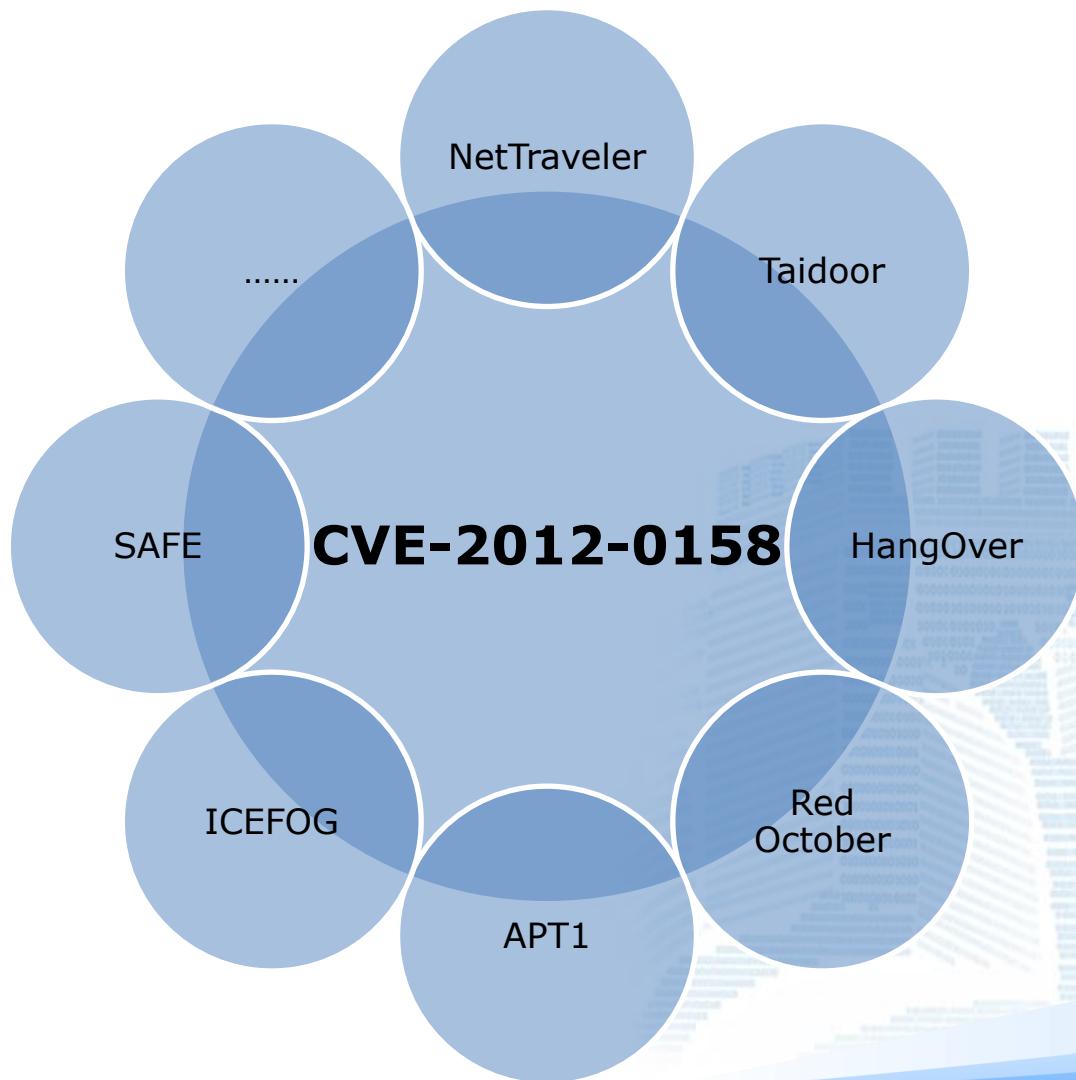
Version 1.0 – September 17, 2013

“ The Hidden Lynx group is a professional team of attackers with advanced capabilities. ”

Follow us on Twitter  
@threatintel

Visit our Blog  
<http://www.symantec.com/connect/symantec-blog/sr>

# 如何定位组织？



# 供应链分析（FireEye）和APT1（Mandiant）



## Executive Summary

In a similar way, cyber intruders leave behind various digital “fingerprints.” They may send spear-phishing emails from a specific IP address or email address. Their emails may contain certain patterns of subject lines. Their files have specific names, MD5 hashes, timestamps, custom functions, and encryption algorithms. Their backdoors may have command and control IP addresses or domain names embedded. These are just a few examples of the myriad of linkages that computer forensic analysts consider when trying to distinguish one cyber threat group from another.

Digital “fingerprints” do not all carry equal weight in attribution analysis. Their validity or value as indicators of a specific threat group depends on the context. For example, the IP address of a HTRAN is not unique and may be shared by many different groups. A specific, custom backdoor, however, is more sufficient, on its own, for attribution.

网络入侵者也会留下各种各样的数字“指纹”。他们的钓鱼邮件是从一个具体的IP地址或邮箱地址发送的，这些邮件里会包含特定的模式和主题，文件中有具体的名字、MD5哈希、时间戳、自定义函数和加密算法。

At the most basic level, we say that the intrusion events are attributed to the same group when we have collected enough indicators to show beyond a reasonable doubt that the same person or group of people were involved.

- A shared malware-builder tool

- Whether the thief carefully researched their target, disabled alarms, and attempted to remove evidence such as fingerprints; or whether he was not very careful, but simply relied on being “stealthy enough” to not get caught.



# 组织判定

- ❖ 需要基于大量资源（以同源样本为主，包含其他资源）进一步分析，获得相关线索、指纹等
- ❖ Hacking Back：也就是从攻击者直接获得相关资源
- ❖ 取证分析：主要指从受害机上获得相关资源

# Hacking Back

The image shows a composite of three screenshots related to a digital investigation. On the left, a browser window displays a menu with links like 'BasicInfo', 'CMD', 'Download', and 'Upload', with a search box containing '实刀三号'. The middle screenshot shows a Gmail inbox for 'dota.d001@gmail.com' with a list of emails and a chat window. The right screenshot shows a social network profile for 'mer4en7y' on 'yoyo2008.com', including a profile picture, personal information, and a list of friends. One friend, 'mayuan', is highlighted.

mer4en7y的个人空间  
http://www.yoyo2008.com/741498 [收藏] [置顶] [分享] [RSS]

空间首页 动态 记录 日志 相册 分享 好友 留言板 个人资料

头像  
个人资料  
性别 保密  
生日  
查看全部个人资料

动态  
现在还没有动态

好友  
ENZO mayuan

最近访客  
现在还没有访客

Mer4en7y profile at yoyo2008.com

One of two friends of **Mer4en7y** in yoyo2008 social network is a user named "**mayuan**" which seems to be from Xinjiang and a graduate of Judicial Police School according to shared private information out there:

Avatar  
Personal Information  
real name Mabuchi  
Gender Male  
Birthday December 25, 1985  
birthplace of Spark streets Dabancheng District, Urumqi, Xinjiang Uygur Autonomous Region  
residence Xinjiang Uygur Autonomous Region the Urumqi Shayibake Bayi Street  
Graduate school in Xinjiang Judicial Police School  
Academic specialist  
View Full Profile

mayuan  
Add as Friend  
Leave me a message  
Say hello  
Send Message

Statistics

Mer4en7y's contact profile at yoyo2008.com

<http://u.pintour.com/uid-b1bf56e230cc42d9bfa003a7718888d2/>

FIGURE 30: dota.d001@gmail.com (inbox view)<sup>41</sup>

# 猜想——嫁祸

## ❖ 动机：

**政治目的：主要在国家利益层次。**

**经济利益：一般为谋取利益或打击竞争对手。**

## ❖ 目的：混淆视听，隐藏真实攻击目标或目的。

### 针对性攻击相关典型行为或特性（技术手段）

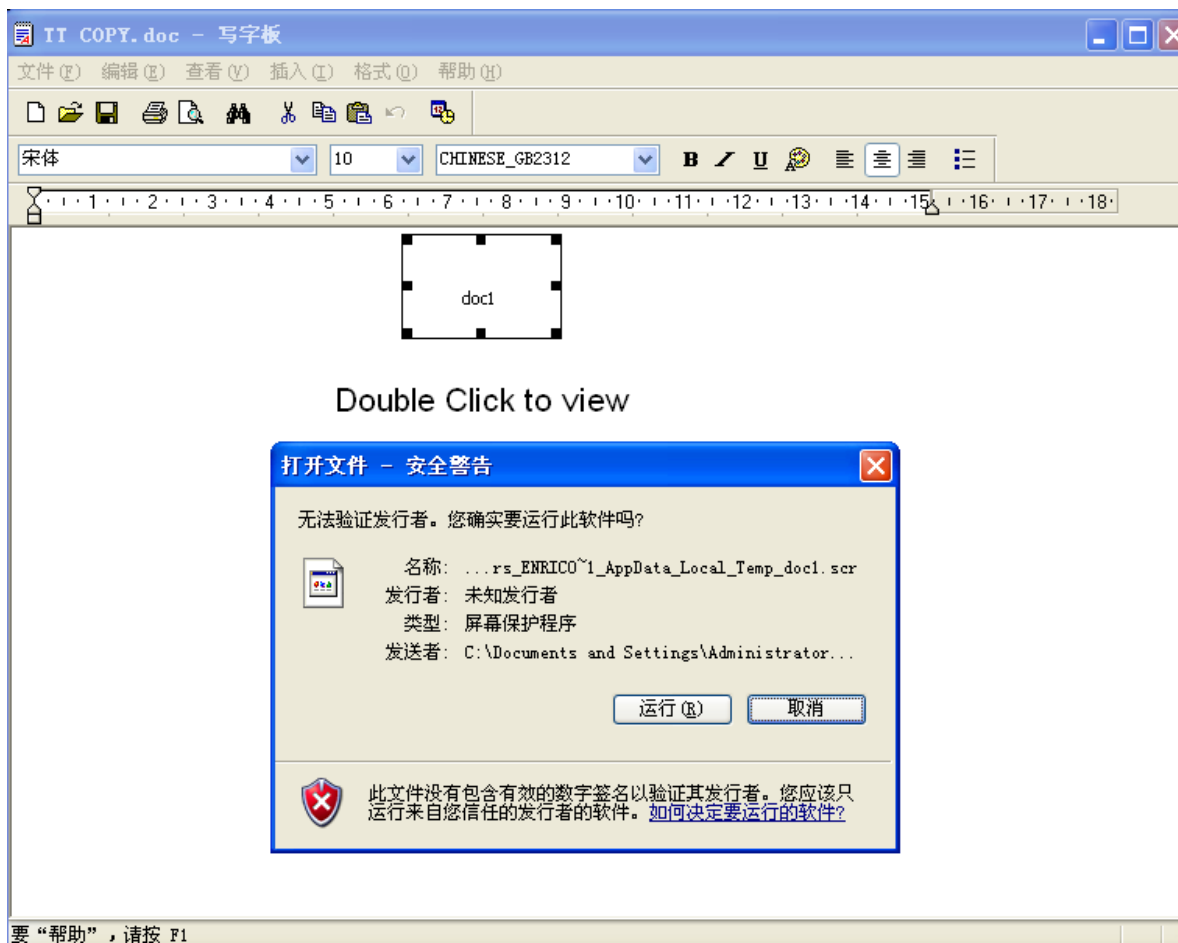
- 1、通过邮件传播携带文件格式漏洞的文件。
- 2、邮件攻击收信人为具体一个机构或组织。
- 3、相关样本或邮件有关联性，且有持续性。
- 4、样本具备窃取信息或其他功能。
- 5、.....

一个秘密的资源丰富的组织，拥有中国大陆的研究人员，能够直接访问位于上海的电信基础设施。该组织与**61398**部队位于同一个地区，多年从事企业规模的间谍活动，执行的任务也与**61398**部队的任务类似。

A secret, resourced organization full of mainland Chinese speakers with direct access to Shanghai-based telecommunications infrastructure is engaged in a multi-year, enterprise scale computer espionage campaign right outside of Unit 61398's gates, performing tasks similar to Unit 61398's known mission.

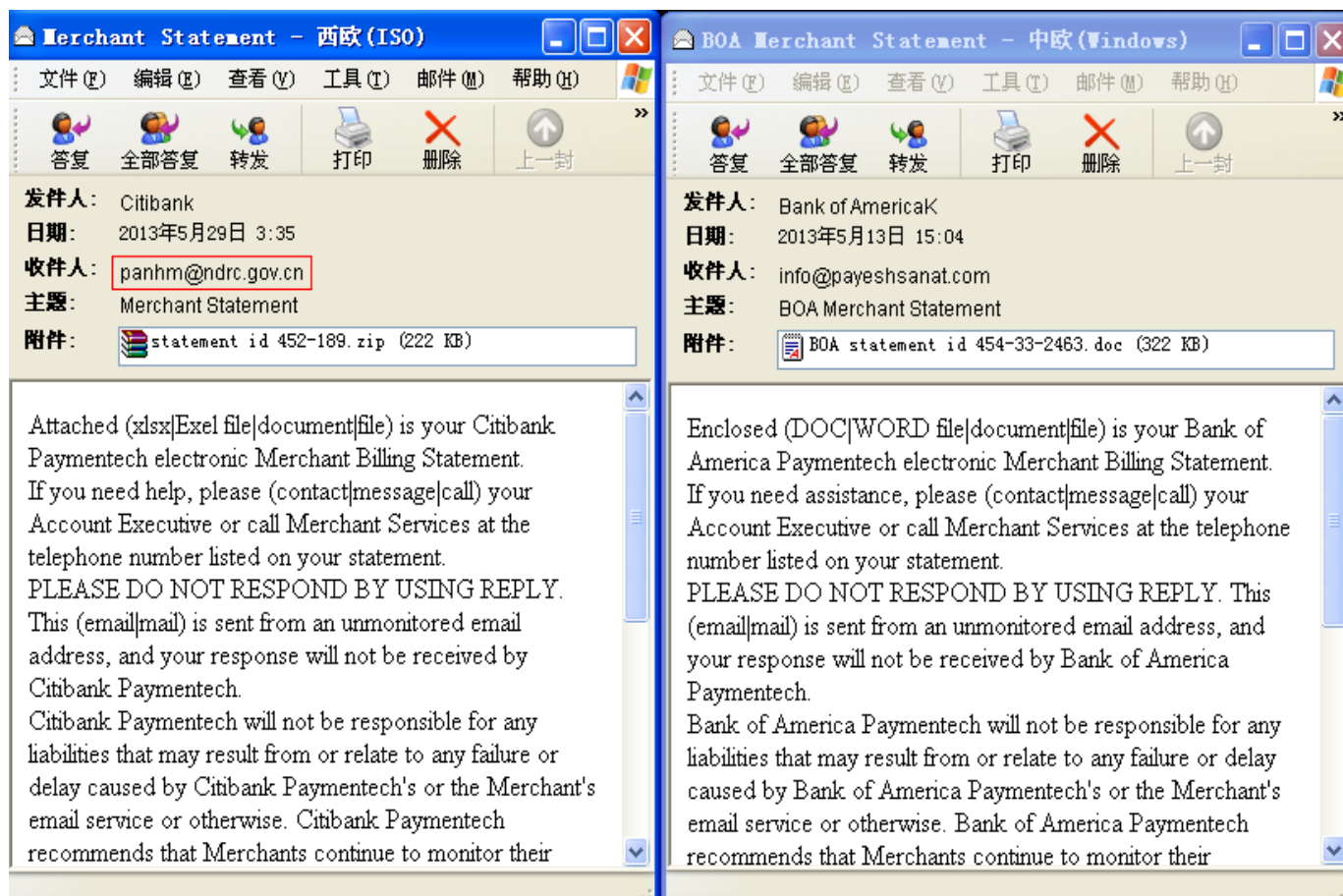
# 猜想——基于传统恶意代码（zbot?）的 针对性攻击

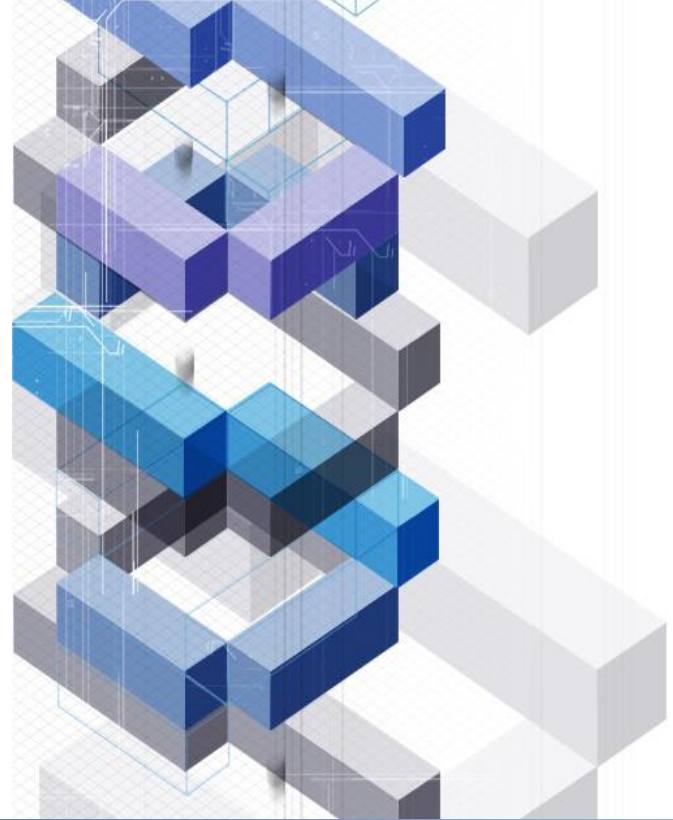
## ❖ 文档内嵌可执行文件，PE样本为ZBOT



# 猜想——基于传统恶意代码 ( zbot? ) 的 针对性攻击

## ❖ 文档为文件格式漏洞文件，PE样本为ZBOT





# 他山之石

# 一些LOGO

VirusView



proofpoint


malwr 

 FireEye


 MANDIANT

 virustotal

 TREND  
MICRO

malware tracker 

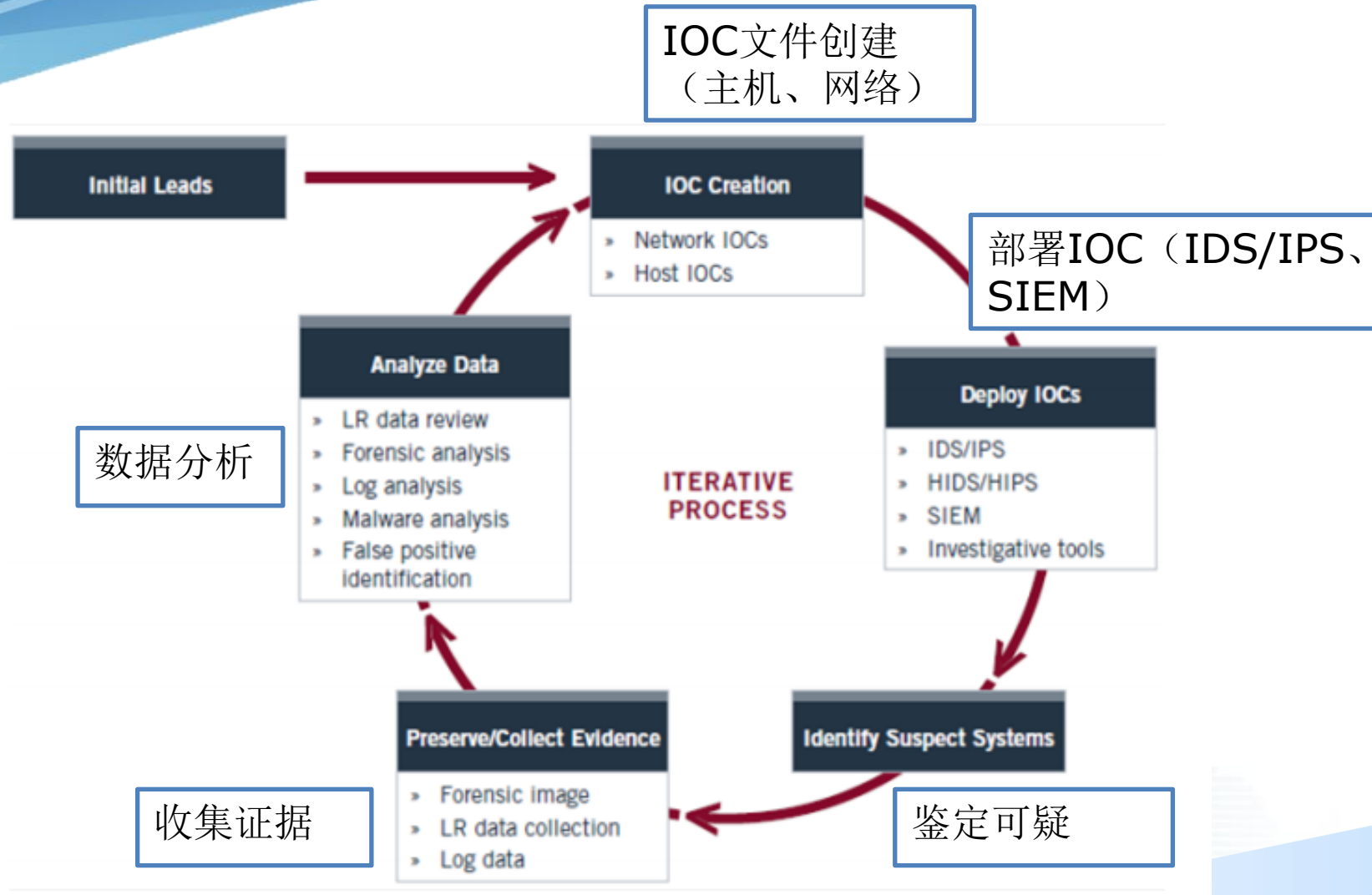
SECURELIST  Symantec.

 yara-project  
The pattern matching swiss knife for malware

 DOMAINTOOLS

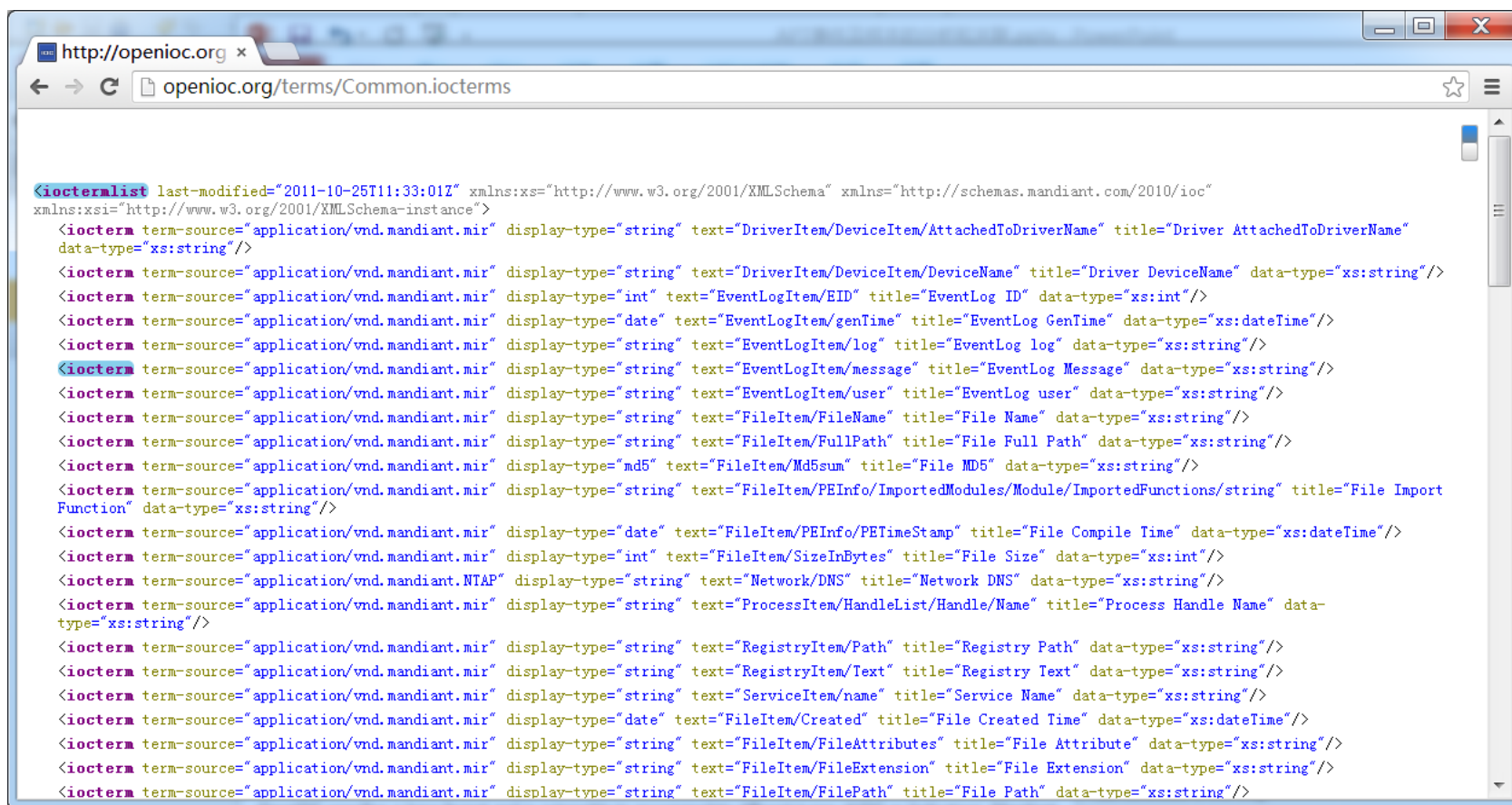
Google

# IOC (Indicators of Compromise)





## ❖ <http://openioc.org/terms/Current.iocterm>s

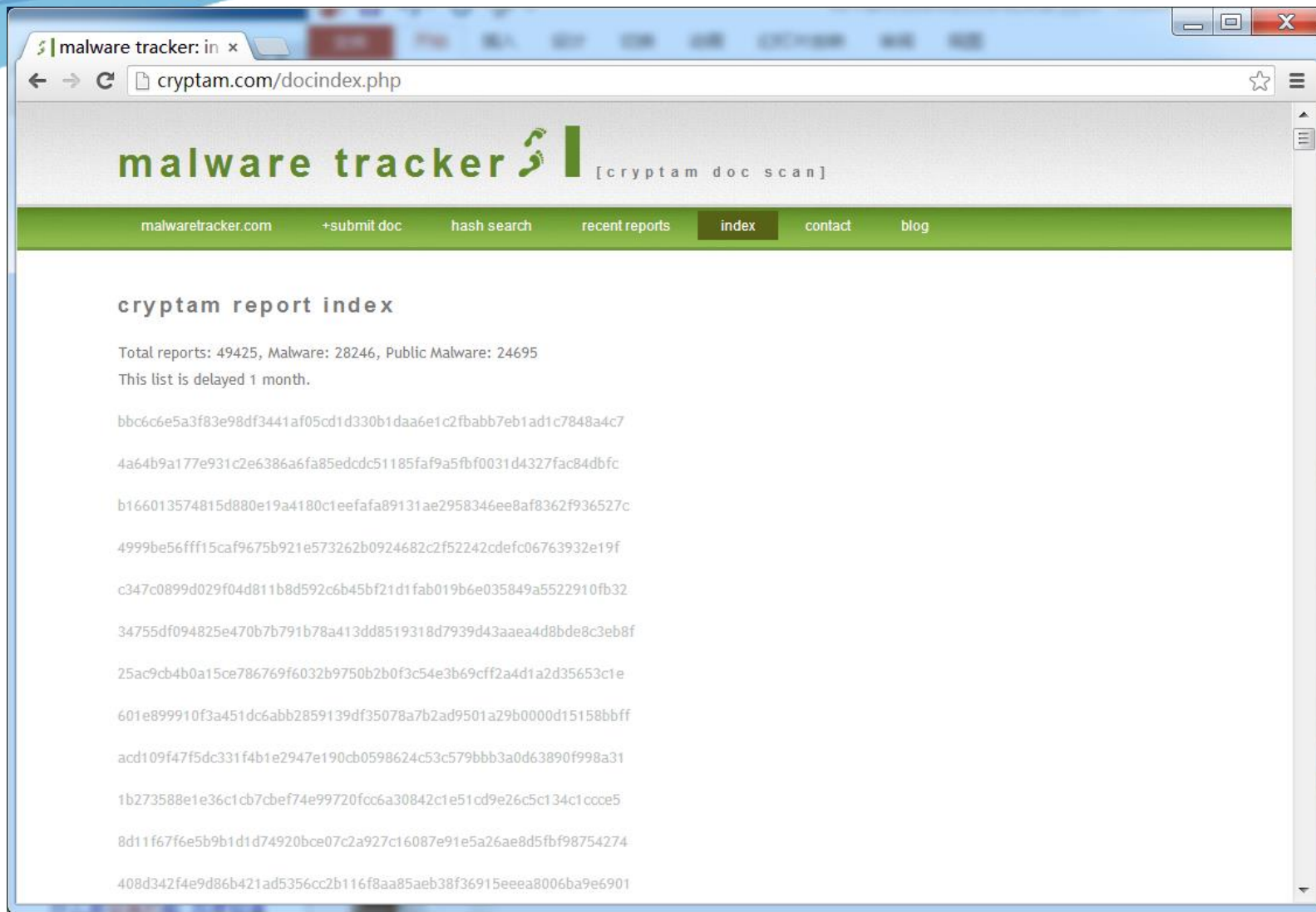


The screenshot shows a web browser window with the address bar displaying `http://openioc.org/terms/Current.iocterm`. The page content is an XML document defining IOCTerm objects. The root element is `<iocetermlist>` with attributes `last-modified="2011-10-25T11:33:01Z"`, `xmlns:xs="http://www.w3.org/2001/XMLSchema"`, and `xmlns="http://schemas.mandiant.com/2010/ioc"`. The XML contains a list of `<ioceterm>` elements, each with attributes for `term-source`, `display-type`, `text`, `title`, and `data-type`. The terms listed include:

- `DriverItem/DeviceItem/AttachedToDriverName` (title: "Driver AttachedToDriverName", data-type: "xs:string")
- `DriverItem/DeviceItem/DeviceName` (title: "Driver DeviceName", data-type: "xs:string")
- `EventLogItem/EID` (title: "EventLog ID", data-type: "xs:int")
- `EventLogItem/genTime` (title: "EventLog GenTime", data-type: "xs:dateTime")
- `EventLogItem/log` (title: "EventLog log", data-type: "xs:string")
- `EventLogItem/message` (title: "EventLog Message", data-type: "xs:string")
- `EventLogItem/user` (title: "EventLog user", data-type: "xs:string")
- `FileItem/FileName` (title: "File Name", data-type: "xs:string")
- `FileItem/FullPath` (title: "File Full Path", data-type: "xs:string")
- `FileItem/Md5sum` (title: "File MD5", data-type: "xs:string")
- `FileItem/PEInfo/ImportedModules/Module/ImportedFunctions/string` (title: "File Import Function", data-type: "xs:string")
- `FileItem/PEInfo/PETimeStamp` (title: "File Compile Time", data-type: "xs:dateTime")
- `FileItem/SizeInBytes` (title: "File Size", data-type: "xs:int")
- `Network/DNS` (title: "Network DNS", data-type: "xs:string")
- `ProcessItem/HandleList/Handle/Name` (title: "Process Handle Name", data-type: "xs:string")
- `RegistryItem/Path` (title: "Registry Path", data-type: "xs:string")
- `RegistryItem/Text` (title: "Registry Text", data-type: "xs:string")
- `ServiceItem/name` (title: "Service Name", data-type: "xs:string")
- `FileItem/Created` (title: "File Created Time", data-type: "xs:dateTime")
- `FileItem/FileAttributes` (title: "File Attribute", data-type: "xs:string")
- `FileItem/FileExtension` (title: "File Extension", data-type: "xs:string")
- `FileItem/FilePath` (title: "File Path", data-type: "xs:string")



# 公开研究资源——malware tracker



# 公开研究资源—— CISCO Threat Outbreak Alerts

The screenshot shows a web browser window displaying a Cisco Security Intelligence Center alert. The browser's address bar shows the URL: `tools.cisco.com/security/center/viewThreatOutbreakAlert.x?alertId=32474`. The page title is "Threat Outbreak Alert: Fake Invoice Processing Failure Notification Email Messages on January 16, 2014".

**Threat Outbreak Alert**

**Threat Outbreak Alert: Fake Invoice Processing Failure Notification Email Messages on January 16, 2014**

Threat Type: IntelliShield: Threat Outbreak Alert

IntelliShield ID:	32474	Urgency:	Possible use	
Version:	1	Credibility:	Confirmed	
First Published:	2014 January 16 20:35 GMT	Severity:	Mild Damage	
Last Published:	2014 January 16 20:35 GMT			
Port:	Not available			

Version Summary: Cisco Security Intelligence Operations has detected significant activity on January 16, 2014.

**Description**

Cisco Security Intelligence Operations has detected significant activity related to spam email messages that claim to contain an invoice document for the recipient. The text in the email message attempts to convince the recipient to open the attachment for a record of the invoice. However, the .zip attachment contains a malicious .exe file that, when executed, attempts to infect the system with malicious code.

Email messages that are related to this threat (RuleID8503) may contain the following files:

- SF2NRWJJA3NC4STR.zip
- SF.exe

The SF.exe file in the SF2NRWJJA3NC4STR.zip attachment has a file size of 18,432 bytes. The MD5 checksum, which is a unique identifier of the executable, is the following string: 0x197FA6DBBB5BC3EEA8735A3A62E64444

The following text is a sample of the email message that is associated with this threat outbreak:

Message Body:

**This message is for the designated recipient only and may contain privileged, proprietary, or otherwise private information. If you have received it in error, please notify the sender immediately and delete the original. Any other use of the email by you is prohibited.**

Record ID: 2NRWJJA3NC4STR  
Supplier: hxxp://spamcop.net  
Invoice No.: 4504196364  
Document No.: 0969152120  
Invoice amount: USD 1808.34  
Rejection reason(s): Approval Required  
Please find enclosed a record of invoice that could not be processed. We would like to ask you to assist us in resolving the noted rejection reasons.

Cisco Security Intelligence Operations analysts examine real-world email traffic data that is collected from over 100,000 contributing organizations worldwide. This data helps provide a range of information about and analysis of global email security threats and trends. Cisco will continue to monitor this threat and automatically adapt systems to protect customers. This report will be updated if there are significant changes or if the risk to end users increases.

Cisco security appliances protect customers during the critical period between the first exploit of a virus outbreak and the release of vendor antivirus signatures. Email that is managed by Cisco and end users who are protected by Cisco Web Security Appliances will not be impacted by these attacks. Cisco security appliances are automatically updated to prevent both spam email and hostile web URLs from being passed to the end user.

Powered by IntelliShield

**Related Links**

**Solutions**

- Security Solutions
- E-mail Security
- Threat Control for Endpoints
- Threat Control for Infrastructure

**Products & Services**

- Cisco Security IntelliShield Alert Manager Service
- Security Products
- Security Services

Feedback

# 公开研究资源——domaintools

**Enter a Domain Name**

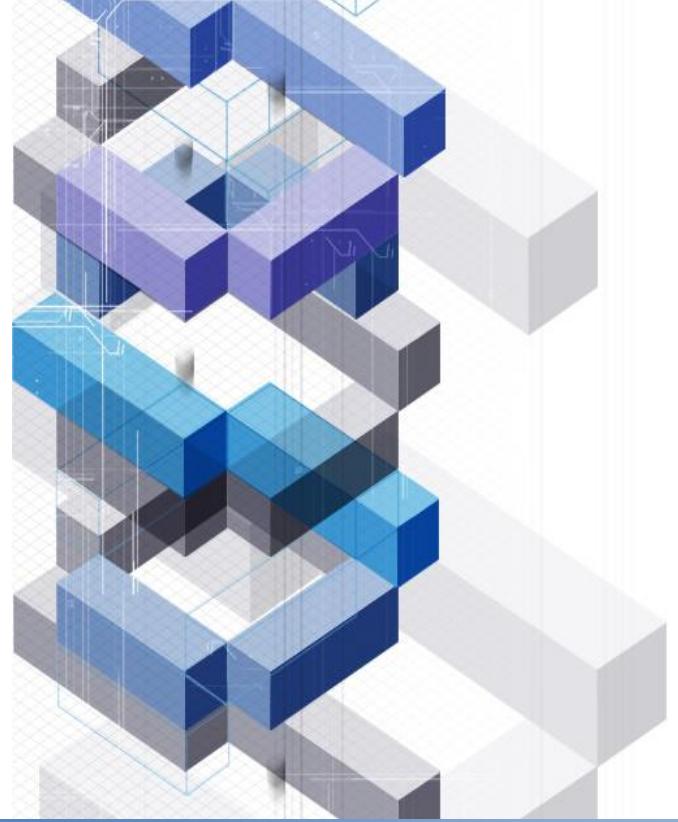
Domain Name:

Enter a domain name into the search box  
to retrieve the hosting history.

**IP Address History**

Event Date	Action	Pre-Action IP	Post-Action IP
2011-07-12	New	-none-	<a href="#">8.22.200.46</a>
2011-08-23	Change	<a href="#">8.22.200.46</a>	<a href="#">173.236.24.254</a>
2011-11-18	Change	<a href="#">173.236.24.254</a>	<a href="#">173.236.24.250</a>
2011-12-22	Change	<a href="#">173.236.24.250</a>	<a href="#">173.236.117.205</a>
2012-03-26	Change	<a href="#">173.236.117.205</a>	<a href="#">95.143.42.218</a>
2012-04-07	Change	<a href="#">95.143.42.218</a>	<a href="#">95.143.42.195</a>
2012-05-27	Change	<a href="#">95.143.42.195</a>	<a href="#">31.3.154.113</a>
2013-02-28	Change	<a href="#">31.3.154.113</a>	<a href="#">109.235.51.254</a>
2013-03-22	Not Resolvable	<a href="#">109.235.51.254</a>	-none-

*Researcherzone.net* 的 IP 历史 ; 来源 : DomainTools



# 总结

# 回顾

- ❖ **APT : APT Lifecycle**
- ❖ **发现APT——持续对抗**
  - **攻击前导：邮件**
  - **蜜罐诱饵**
  - **海量已知样本**
- ❖ **关联分析**
  - **单事件纵向关联**
  - **多事件横向关联**
  - **关联分析方法**
- ❖ **组织判定**
  - **“虚拟”组织**
  - **资源分析**
  - **Hacking Back**
  - **取证分析**
  - **两个猜想：嫁祸、传统的针对性攻击**
- ❖ **他山之石**



**谢谢**  
**欢迎各位专家指导**