新形势下的未知威胁应对之道

涂小毅
安恒高级经理

当前安全形势

互联网攻击事件频发

国家正规军

高度针对拉美国家特定语系、特定种族人群且跨平台传播的定制化、规模化攻击战术“弯刀”

黑客雇佣兵

境外敌对组织（匿名者等）

政治诉求与经济诉求相结合的境外黑客组织，接受雇佣请求，计划、组织与发起具有高度目的性的攻击行动，如OP HK和OP CHINA

军火供应

Hacking Team事件

英国Gamma公司事件

国际数字军火商偏爱系统底层0 day，尤以GrSecurity/PaX类Linux内核漏洞为最，一旦规模化利用则会对国家级重要信息系统造成毁灭性后果

乌克兰电力系统APT事件

近期，在乌克兰，至少有三个区域的电力系统被具有高度破坏性的恶意软件攻击并导致大规模的停电，造成成千上万的家庭在黑暗中度过。

这次大规模的电力中断使得近一半的乌克兰伊万诺 - 弗兰科夫斯克地区的家庭陷入在黑暗当中，乌克兰新闻通讯社 TSN 报道了本次大规模停电事件。报道中指出，黑客在乌克兰国家电网中植入了恶意软件，从而导致发电站意外关闭。

乌克兰电力APT攻击过程

1、本次攻击过程开始于一个带有恶意宏的XLS文件，黑客通过钓鱼链接或钓鱼邮件诱使用户下载恶意文件。

2、当用户无意下打开XLS文件，会启动恶意宏代码执行，宏代码会在临时文件目录下释放文件vba_macro.exe，释放完成后立即启动其运行。

3、宏释放的恶意程序vba_macro.exe通过释放BlackEnergy来执行后续操作，例如与控制端通信以及下载KillDisk、SSH后门等一系列组件来执行攻击。

4、系统一旦被感染，BlackEnergy会释放出破坏性的KillDisk组件和SSH后门，修改注册表，创建服务，然后遍历进程和硬盘，删除系统关键数据，并且会执行关机命令。

5、通过攻击过程来看，BlackEnergy（黑色力量）运行于Windows平台，因此，除电力系统外，其它使用Windows平台的行业用户也可能会被波及。

跨国公司遭受黑客攻击

夜龙攻击

2011.2.10

5家西方跨国能源公司遭到的黑客

“有组织、隐蔽、有针对性”的攻击

大量的 敏感文件、 机密信息 泄漏

始于2007年，目前攻击行动仍在持续。

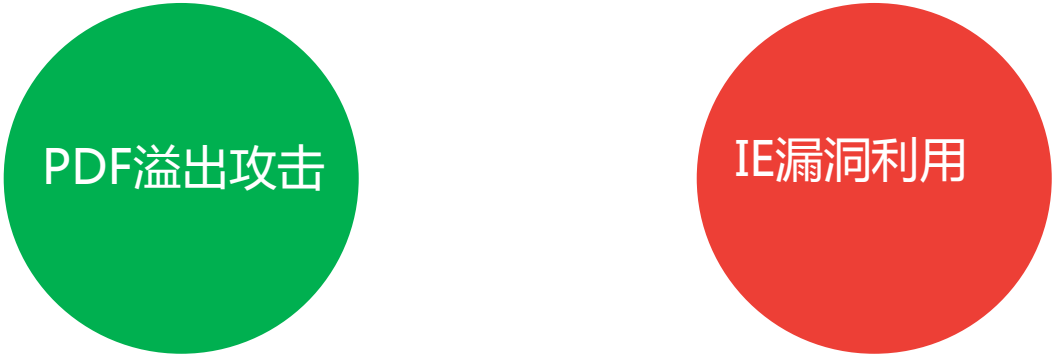
跨国公司遭受黑客攻击过程

攻击过程分析

- 通过SQL注入，入侵外网Web服务器；
- 以Web服务器为跳板，对内网其他服务器及终端电脑进行扫描；
- 通过密码暴力破解等方式入侵内网AD服务器及开发人员电脑；
- 向被入侵电脑植入恶意代码，并安装远端控制工具；
- 建立直接通道，传回大量机敏文件；
- 更多内网遭到入侵，更多高级主管点击了看似正常的邮件附件，却不知其中含有恶意代码。

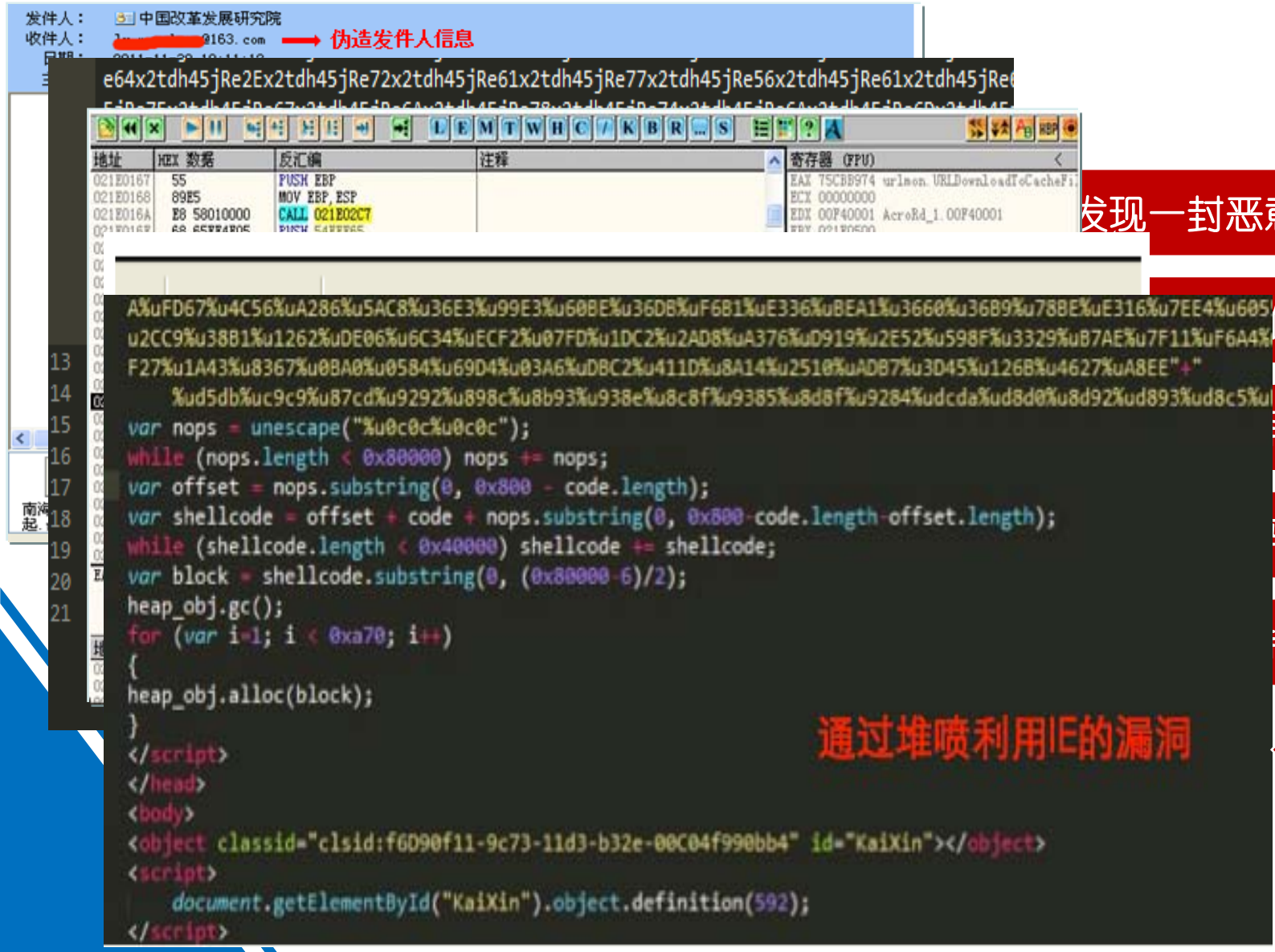
国内政府机构遭受攻击事件

一次利用两种零日漏洞的攻击事件



攻击者利用两种手段综合攻击

国内政府机构遭受攻击过程



利用购物狂欢节发起的攻击事件

根据对来自北美的流量监控的过程中，发现一封来自美国的可疑邮件，该邮件的主题是《您收到的优惠券》，发件人名称显示为天猫。

利用购物狂欢节发起的攻击事件

网络行为

涉及ip信息

ip
86.[redacted].232
189[redacted]79

进程行为

进程名	进程ID	子进程名	子进程ID	创建子进程命令行启动参数
107084.exe	3816	lq3sgdnrfnvpoz3xfrtr.exe	2604	
lq3sgdnrfnvpoz3xfrtr.exe	2604	aazrqppx.exe	3916	
aazrqppx.exe	3916	ydouklz.exe	1652	t38btgayz8cn "c:\mfhboug\aazrqppx.exe"

网络攻击发展趋势

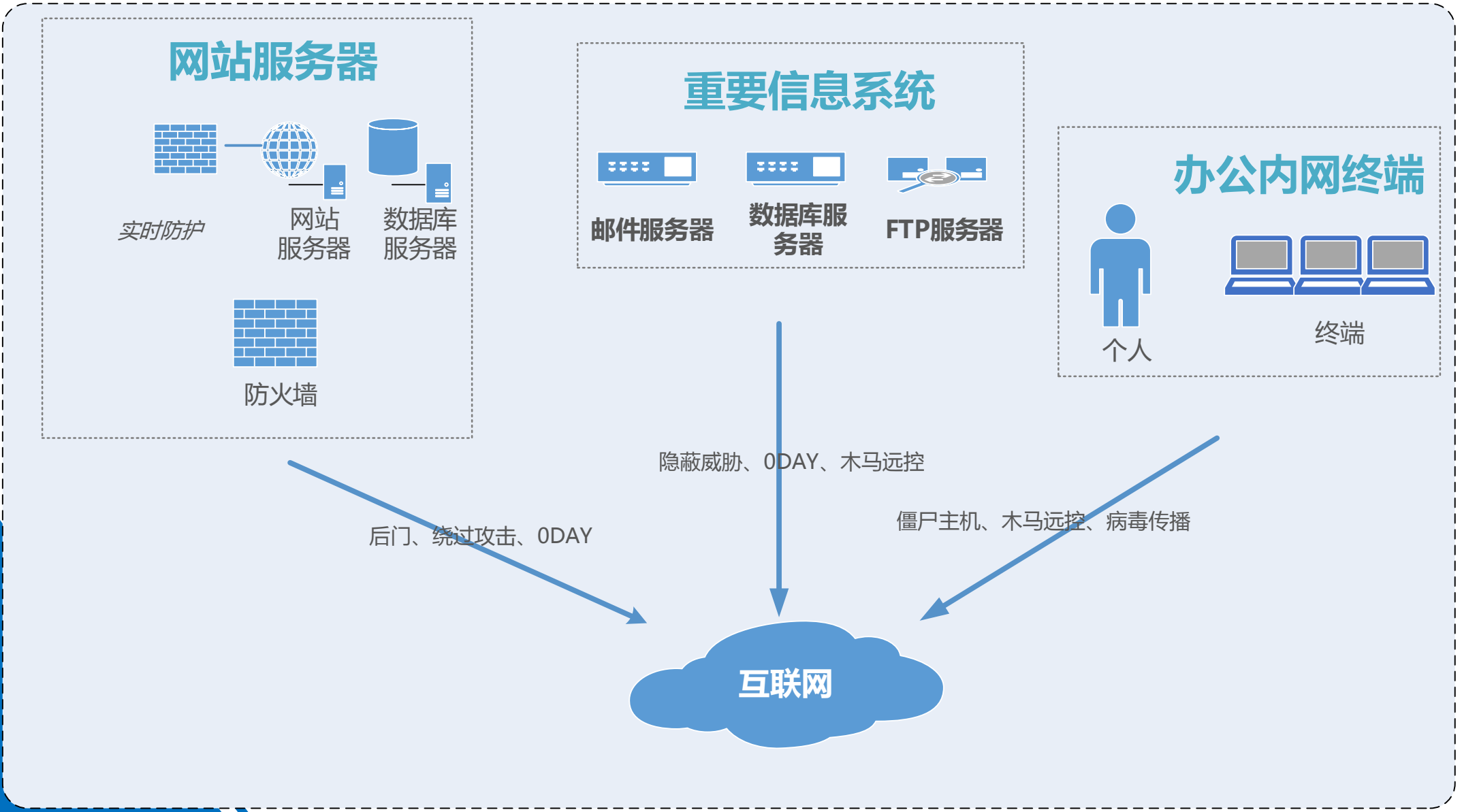
- 以破坏网络为目的
- 大面积扩散僵尸网络
- 攻击频率一次性
- 以常见的攻击工具为主

APT攻击

- 以获取敏感数据为目的
- 明确的攻击目标
- 长期持续潜伏攻击
- RAT、精心构造工具

未知威胁应对方案

如何评估安全威胁？


网站服务器
实时防护
网站
服务器
数据库
服务器
防火墙
重要信息系统
邮件服务器
数据库服
务器
FTP服务器
办公内网终端
个人
终端
隐蔽威胁、0DAY、木马远控
后门、绕过攻击、0DAY
僵尸主机、木马远控、病毒传播
互联网

当前用户面临的安全威胁

网站外网

（WEB、DB服务器）

- 网站后门、挂马
- 绕过攻击
- 0day漏洞利用

办公内网

（终端、网络设备）

- 僵尸主机
- 木马远控
- 勒索病毒等变种恶意代码

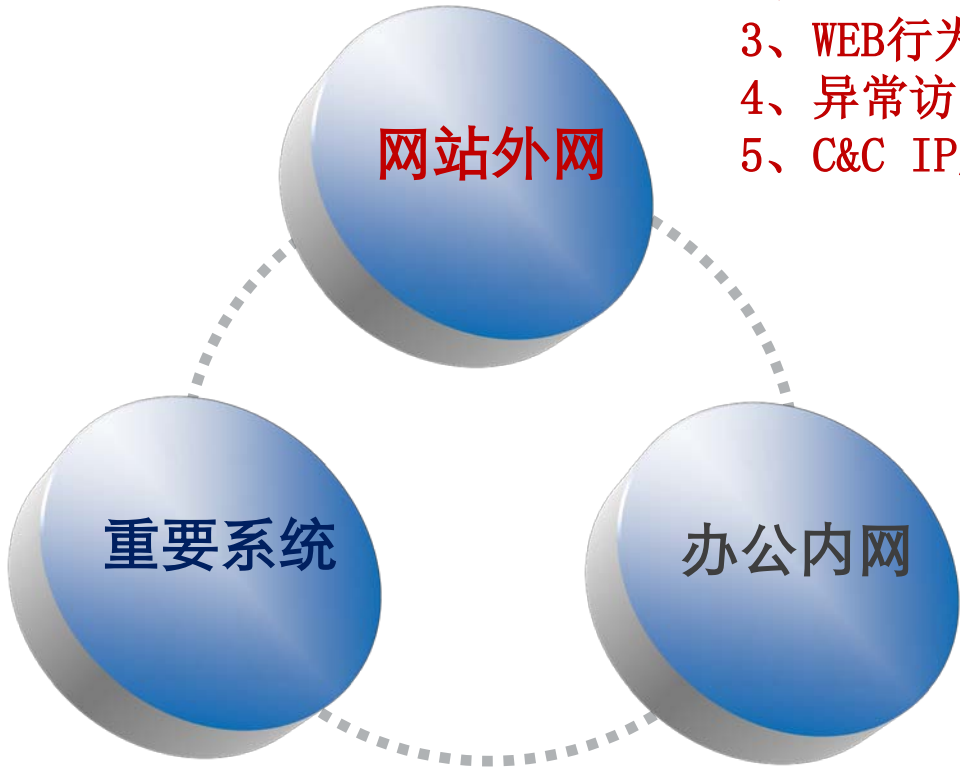
重要系统

（FTP、邮件服务器）

- 邮件钓鱼、欺骗等社工
- 数据窃取
- 0day样本攻击

如何应对这些威胁？

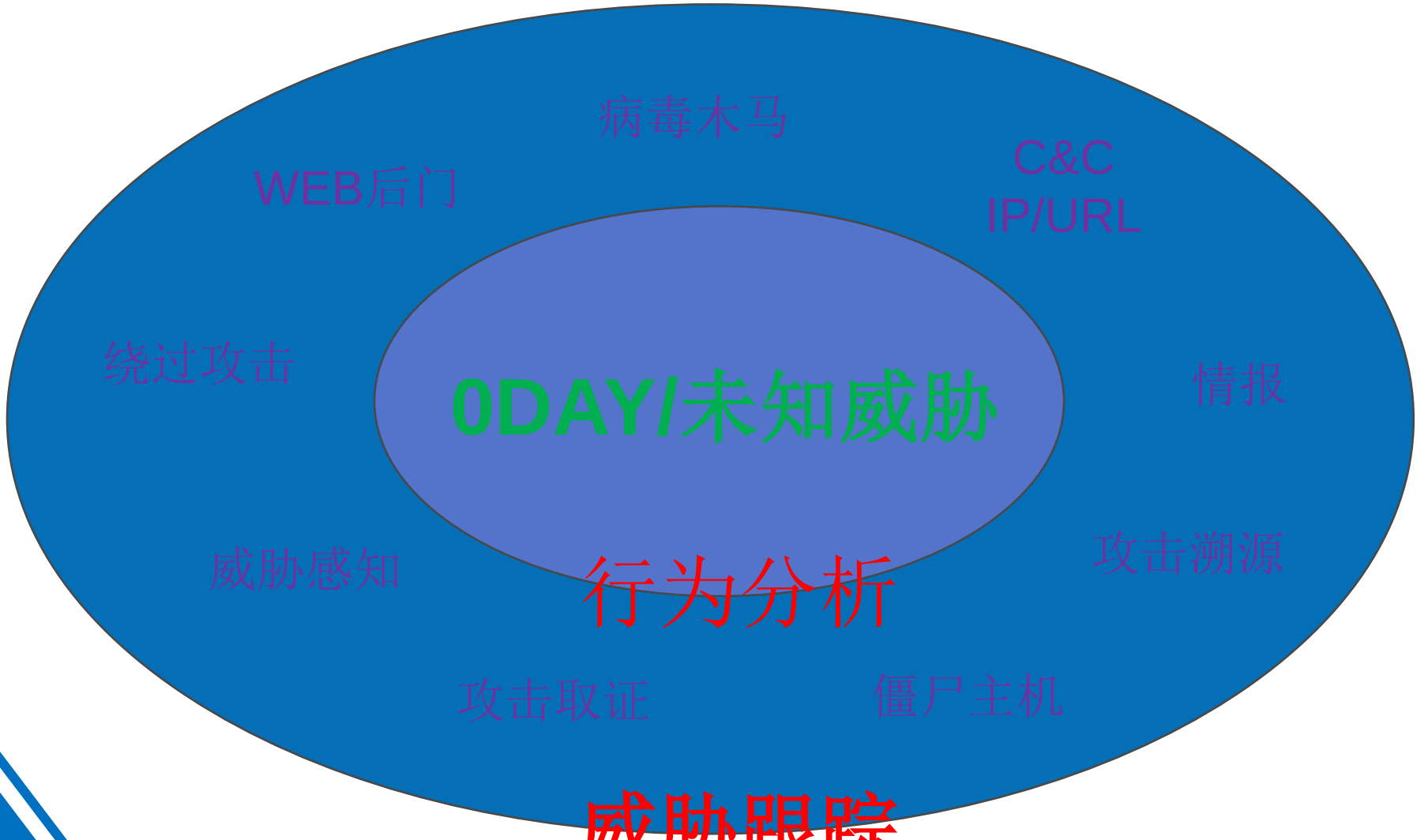
1、WEB特征检测
2、WEBSHELL检测
3、WEB行为分析
4、异常访问
5、C&C IP/URL



1、邮件社工检测
2、WEB Mail攻击
3、邮件附件检测

1、多引擎检测已知特征攻击
2、Shellcode检测
3、动态沙箱分析
4、木马回连分析

未知威胁应对思路


病毒木马
WEB后门
C&C
IP/URL
绕过攻击
0DAY/未知威胁
情报
威胁感知
行为分析
攻击溯源
攻击取证
僵尸主机
威胁跟踪

未知威胁应对技术

WEBSHELL检测

返回

[响应码]

200(OK)

[返回长度]

2836

[返回内容]

```
font-family : Verdana, sans-serif;font-size : 12px;
}
input {
                        font-family: "Verdana";
                        font-size: "11px";
                        BACKGROUND-COLOR: "#FFFFFF";
                        height: "18px";
                        border: "1px solid #666666";
                }
</STYLE>
</head>
<body bgcolor="#EEEEEE" text="#000000" link="#006699" vlink="#5493B4">

<form action="/servu.php" method="get">
<center><b>Serv-U本地提升权限Exp10it By 我非我</b>
<center><b>提升权限部分</b>
<hr>
<table width="760" border="0" cellpadding="0">
<tr><td width="150">主机Ftp端口: </td>   <td width="660"><input name="ftpport" type="text" class="INPUT" value="1"></td></tr>
<tr><td width="150">添加的用户名: </td>   <td width="660"><input name="user" type="text" class="INPUT" value="\' or 1=1--"></td></tr>
<tr><td width="150">添加的用户名密码: </td><td wi
```

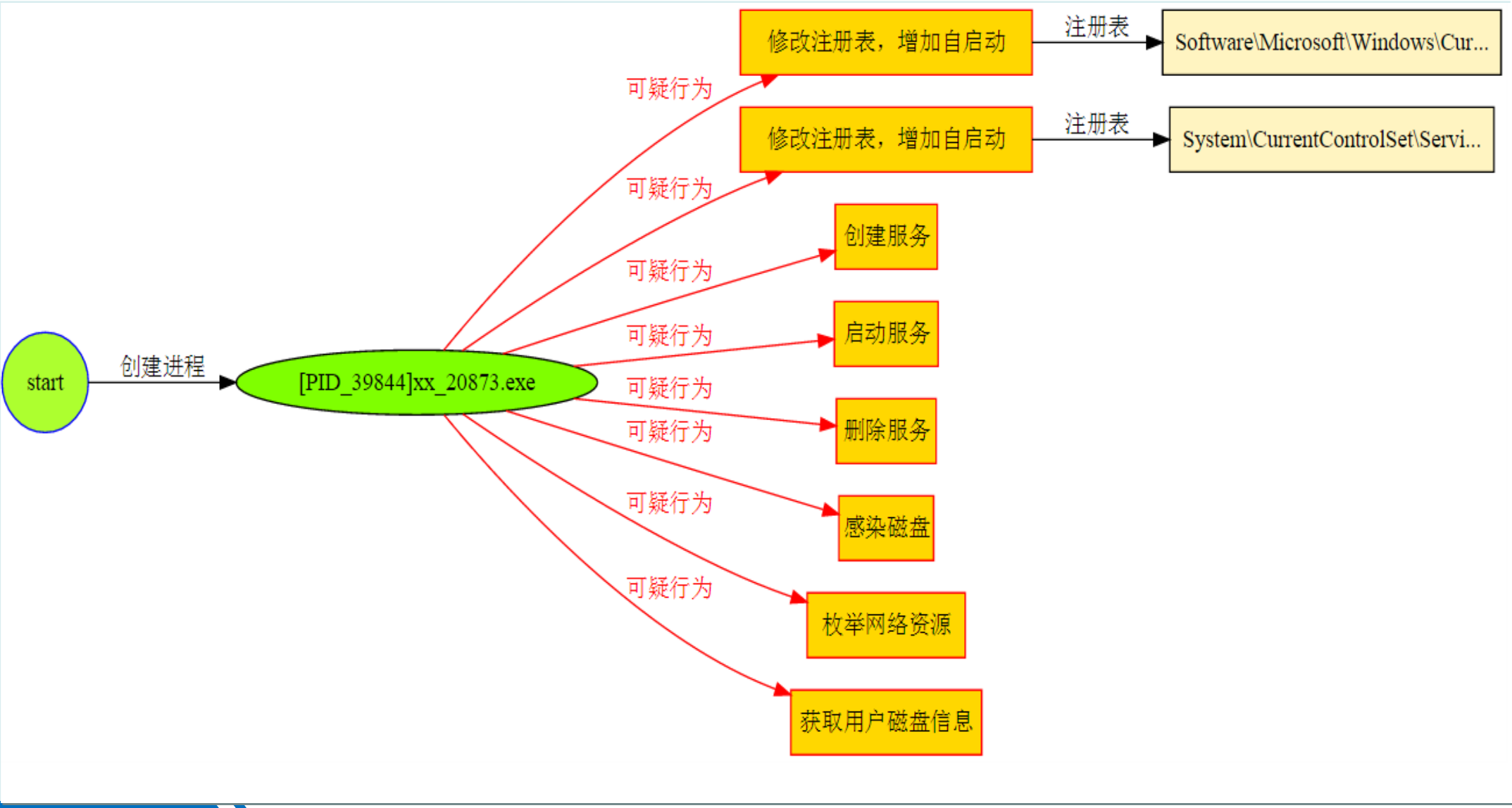
WEB行为分析

高	2015-03-12 10:08:18	WEB行为分析 sql注入select取数据	未处理	[redacted]	[redacted]	sql注入select取数据

基本信息 | 客户端信息 | 服务端信息 | 关联信息 | 处理

客户端IP	服务端IP	URL	响应码	时间	操作
[redacted]	[redacted]	GET http://[redacted]...f...	200	2015-03-12 10:04:15	
[redacted]	[redacted]	GET http[redacted]=1 anD (select 1 f...	200	2015-03-12 10:04:15	
[redacted]	[redacted]	GET http[redacted]cts.php?artist=1 anD (select as...	200	2015-03-12 10:04:20	
[redacted]	[redacted]	GET http[redacted]php?artist=1 anD (select as...	200	2015-03-12 10:04:20	
[redacted]	[redacted]	GET h[redacted]?artist=1 anD (select as...	200	2015-03-12 10:04:20	

文件行为分析


start
创建进程
[PID_39844]xx_20873.exe
可疑行为
修改注册表，增加自启动
注册表
Software\Microsoft\Windows\Cur...
可疑行为
修改注册表，增加自启动
注册表
System\CurrentControlSet\Servi...
可疑行为
创建服务
可疑行为
启动服务
可疑行为
可疑行为
删除服务
可疑行为
感染磁盘
可疑行为
枚举网络资源
可疑行为
获取用户磁盘信息

文件沙箱分析

文件行为

检测有恶意的

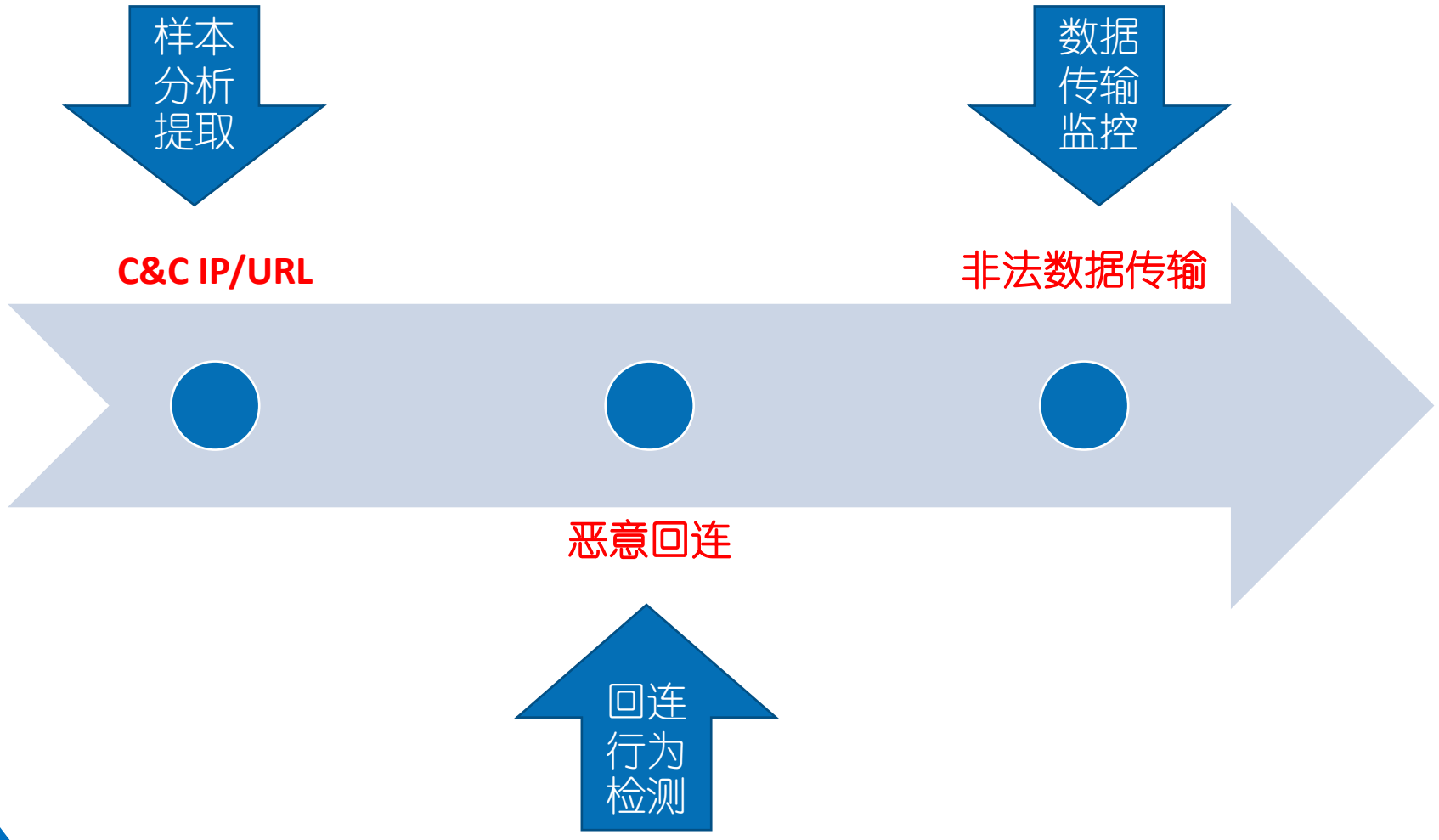
svchost.exe ryhul.exe

检测安全的

MPS1.tmp	~WRS{CE5E140F-84C2-463D-8468-6855C6256B63}.tmp	~WRS{2D32DC49-FE04-4FE6-90EF-38CE0CAB85AF}.tmp	~WRS{9516BD86-1674-4CD8-9F16-5BEA8AD0B729}.tmp	xune.oci
Administrator.wab	Administrator.wab~	tmp1e2551db.bat	~WRC0000.tmp	~WRS{DE904475-F1B8-46B3-B33B-007B41BF57A2}.tmp
aaa.doc.LNK	index.dat	Temp.LNK	desktop.ini	aaa.doc.lnk
Temp.lnk				

进程	名称	详细描述
Explorer.EXE[pid=1336]	遍历文件	NtQueryDirectoryFile
Explorer.EXE[pid=1336]	删除文件	DeleteFileA
Explorer.EXE[pid=1336]	删除目录	RemoveDirectoryA
cmd.exe[pid=1516]	遍历文件	NtQueryDirectoryFile

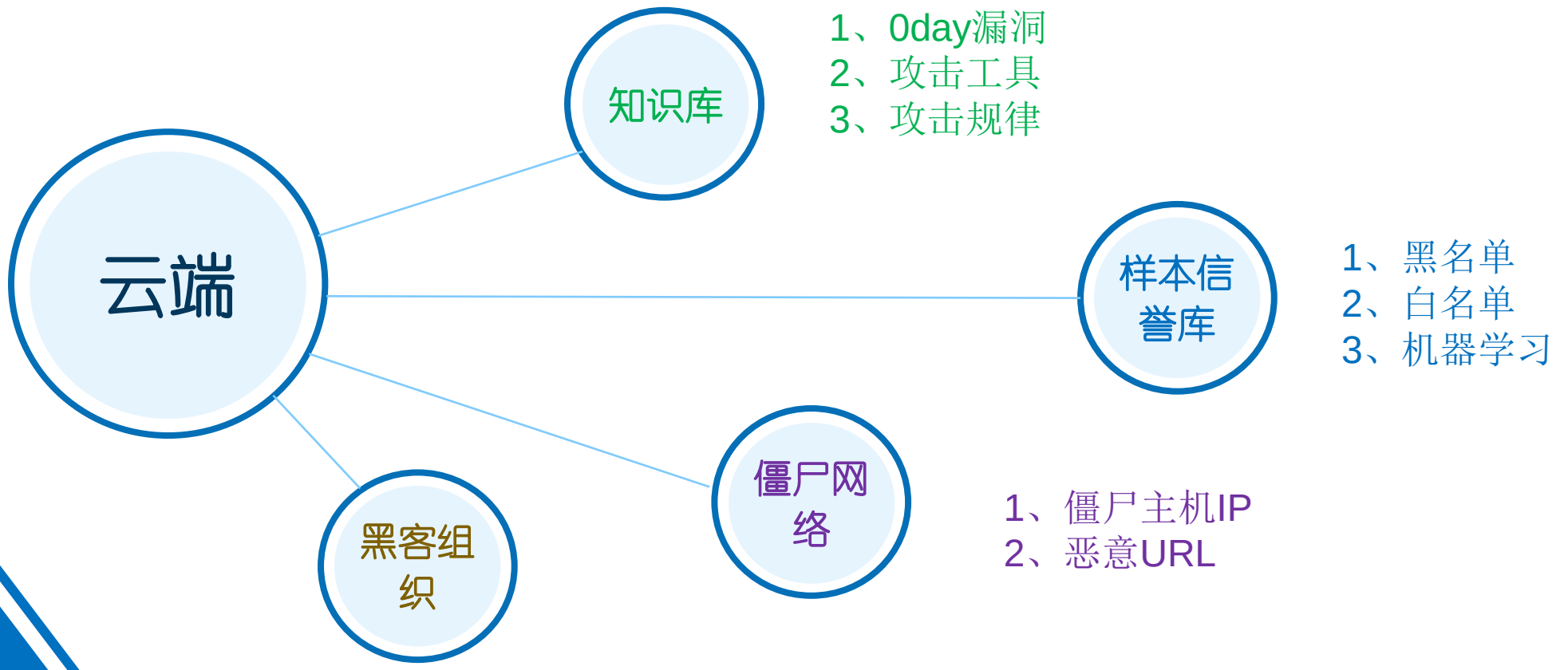
木马回连分析



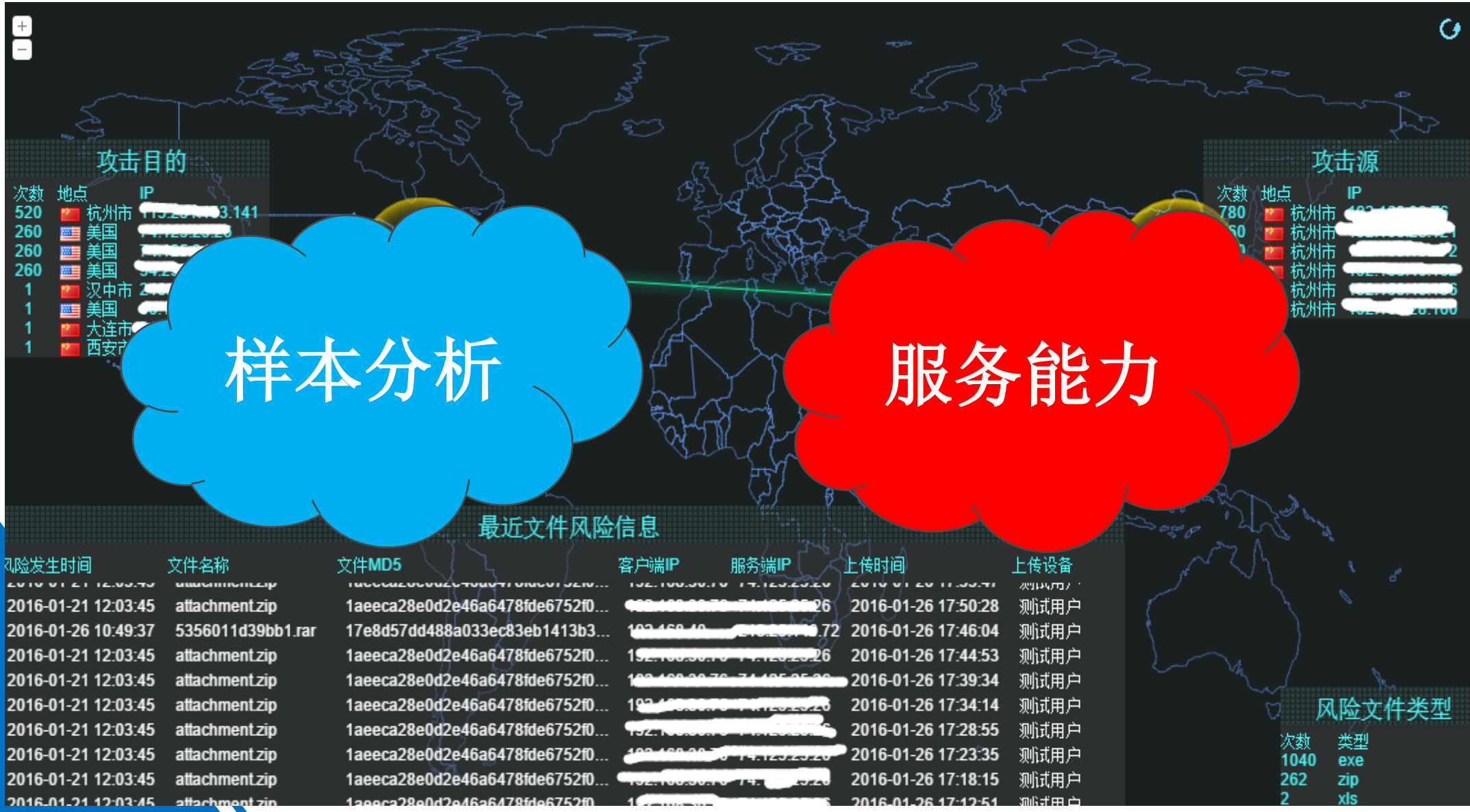
基于攻击链的应对技术


1
2
3
4
5
6
侦查目标
发现弱点
1、扫描攻击
2、WEB探测
执行攻击
1、WEB攻击
2、恶意代码攻击
3、邮件社工
4、0day攻击
获取权限
1、后门植入
2、文件上传
3、溢出攻击
4、暴力破解
命令与控制
1、C&C IP/URL
2、WEB CC
3、异常流量
数据回传
1、木马回连
2、数据盗取

云端情报应对技术

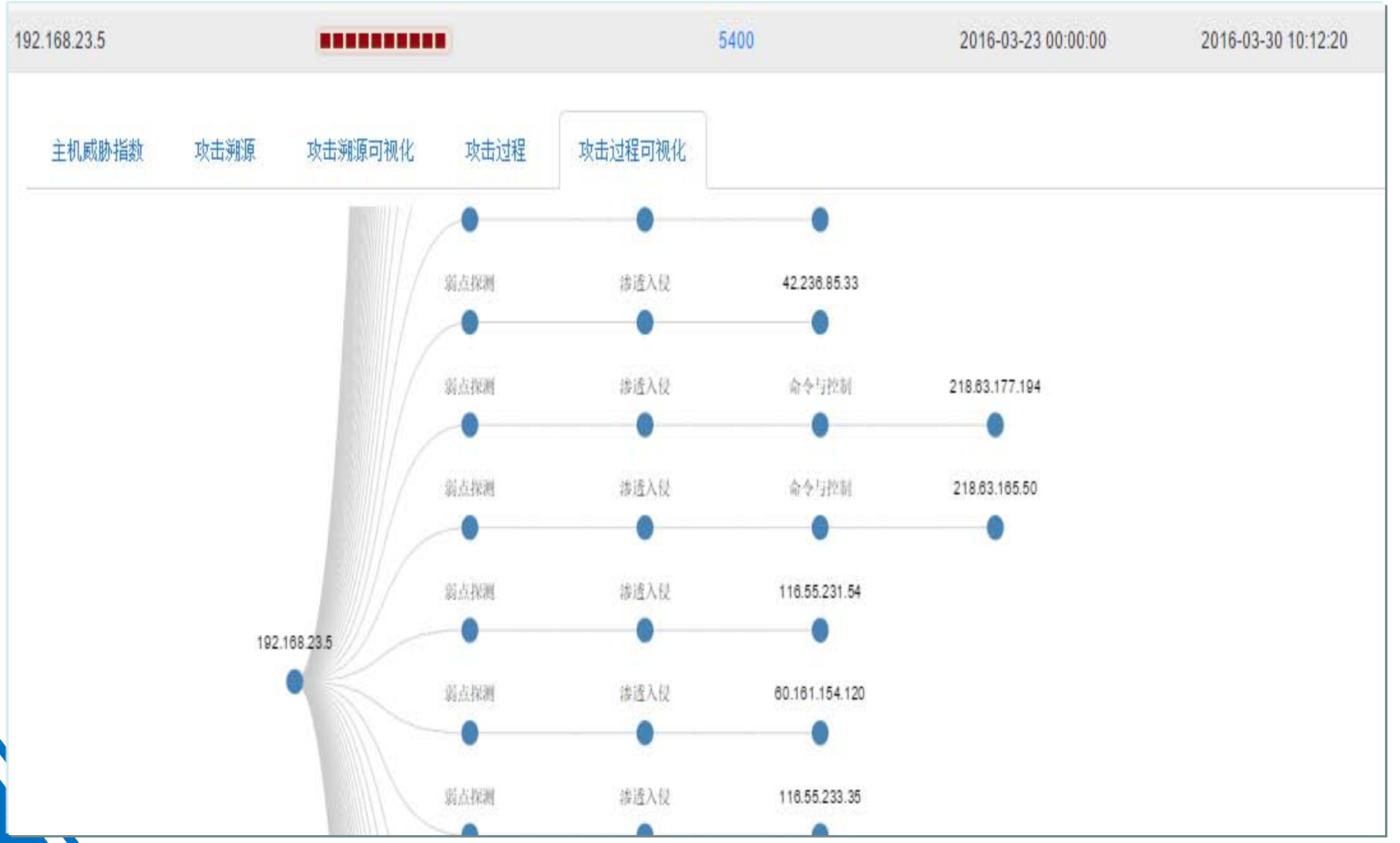

云端
知识库
1、0day漏洞
2、攻击工具
3、攻击规律
样本信誉库
1、黑名单
2、白名单
3、机器学习
僵尸网络
1、僵尸主机IP
2、恶意URL
黑客组织
1、攻击特点
2、惯用手段
3、利用工具特点

云端即服务


攻击目的
次数 地点 IP
520 杭州市
260 美国
260 美国
260 美国
1 汉中市
1 美国
1 大连市
1 西安市
攻击源
次数 地点 IP
780 杭州市
杭州市
杭州市
杭州市
杭州市
杭州市
样本分析
服务能力
最近文件风险信息
风险发生时间 文件名称 文件MD5 客户端IP 服务端IP 上传时间 上传设备
2016-01-21 12:03:45 attachment.zip 1aeeca28e0d2e46a6478fde6752f0... 2016-01-26 17:50:28 测试用户
2016-01-26 10:49:37 5356011d39bb1.rar 17e8d57dd488a033ec83eb1413b3... 2016-01-26 17:46:04 测试用户
2016-01-21 12:03:45 attachment.zip 1aeeca28e0d2e46a6478fde6752f0... 2016-01-26 17:44:53 测试用户
2016-01-21 12:03:45 attachment.zip 1aeeca28e0d2e46a6478fde6752f0... 2016-01-26 17:39:34 测试用户
2016-01-21 12:03:45 attachment.zip 1aeeca28e0d2e46a6478fde6752f0... 2016-01-26 17:34:14 测试用户
2016-01-21 12:03:45 attachment.zip 1aeeca28e0d2e46a6478fde6752f0... 2016-01-26 17:28:55 测试用户
2016-01-21 12:03:45 attachment.zip 1aeeca28e0d2e46a6478fde6752f0... 2016-01-26 17:23:35 测试用户
2016-01-21 12:03:45 attachment.zip 1aeeca28e0d2e46a6478fde6752f0... 2016-01-26 17:18:15 测试用户
风险文件类型
次数 类型
1040 exe
262 zip
2 xls

攻击溯源思路分析

攻击取证溯源思路


192.168.23.5
5400
2016-03-23 00:00:00
2016-03-30 10:12:20
主机威胁指数
攻击溯源
攻击溯源可视化
攻击过程
攻击过程可视化
192.168.23.5
弱点探测
渗透入侵
42.236.85.33
弱点探测
渗透入侵
命令与控制
218.63.177.194
弱点探测
渗透入侵
命令与控制
218.63.165.50
弱点探测
渗透入侵
116.55.231.54
弱点探测
渗透入侵
60.161.154.120
弱点探测
渗透入侵
116.55.233.35

内网僵尸主机事件

网站后门利用事件


192.168.1.5
71
2016-05-05 15:04:12
2016-05-09 15:04:12
2016-05-05 15:04:12
2016-05-05 16:14:12
2016-05-05 16:34:12
2016-05-05 16:54:12
2016-05-05 16:54:13
2016-05-05 17:14:12
2016-05-05 18:44:13
2016-05-05 22:14:12
2016-05-06 05:44:12

威胁实时感知分析

攻击指纹分析

攻击工具

- 扫描器类型
- 渗透方式
- 登陆工具
- 控制通道

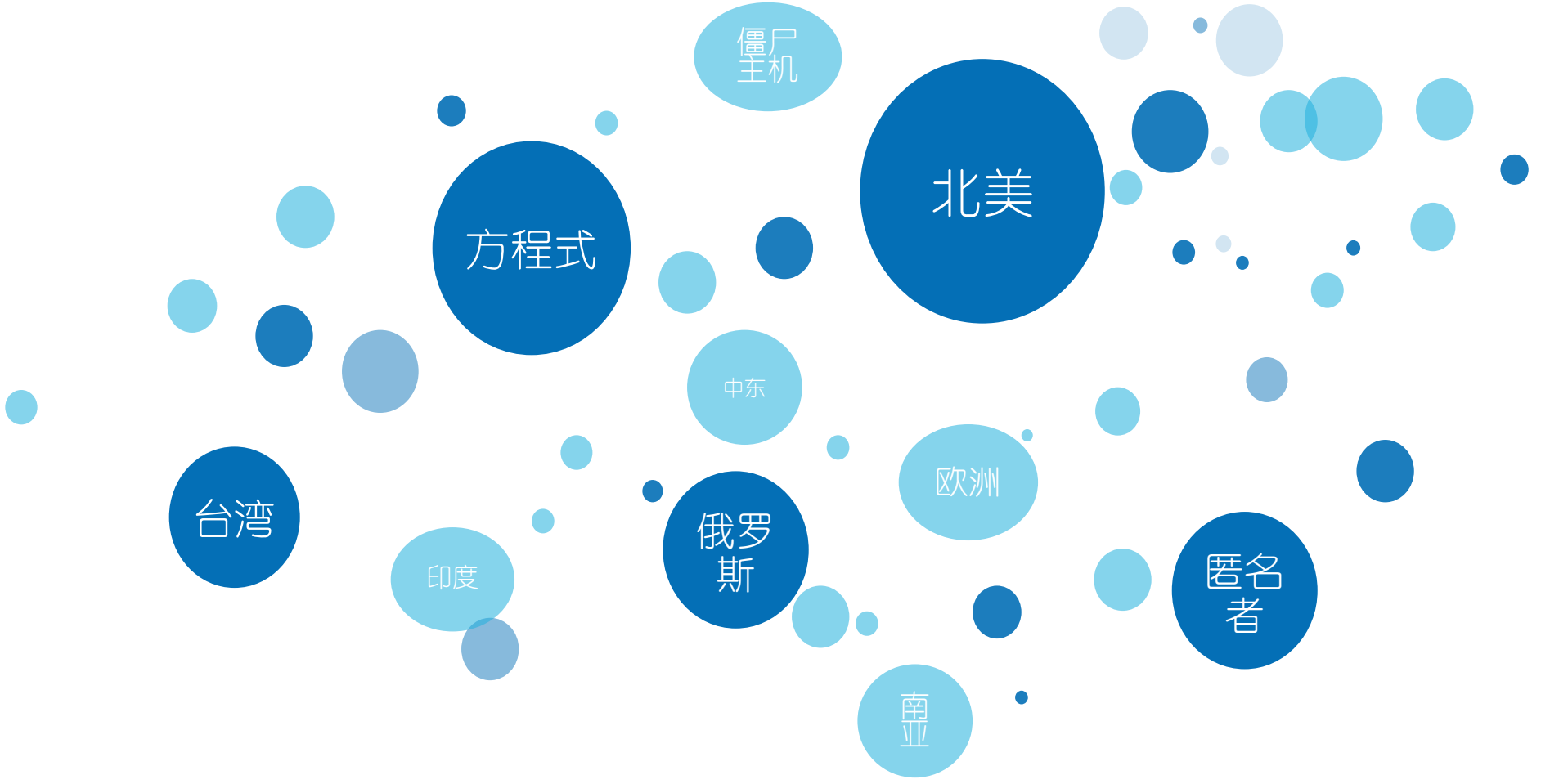
样本同源

- 加壳信息、逃逸方式
- 代码片段
- 进程、注册表行为
- C&C IP/URL

攻击指纹

- 来源区域
- C&C区域
- 区域代码、邮编、语言等
- 样本编码方式、所属时区

支持来源及组织信息



未知威胁应对案例

攻击事件状态分析

紧急事件列表

处理

发生时间	感染主机	事件	操作
2016-11-14 09:21:14		检测到WEB后门访问行为，后门URL为[/elmaliseker.asp]	详细 处理
2016-11-14 09:21:14		检测到WEB后门访问行为，后门URL为[/mssql.jsp]	详细 处理
2016-11-14 09:21:14		检测到WEB后门访问行为，后门URL为[/myxx.jsp]	详细 处理
2016-11-14 09:21:14	192.168.30.78	检测到WEB后门访问行为，后门URL为[/myxx1.jsp]	详细 处理
2016-11-14 09:21:14	192.168.30.78	检测到WEB后门访问行为，后门URL为[/no.jsp]	详细 处理
2016-11-14 09:21:14	192.168.30.78	检测到WEB后门访问行为，后门URL为[/nossssx.jsp]	详细 处理
2016-11-14 09:21:14	192.168.30.78	检测到WEB后门访问行为，后门URL为[/queryDong.jsp]	详细 处理
2016-11-14 09:19:34	192.168.30.78	检测到WEB后门访问行为，后门URL为[/dbapp.aspx]	详细 处理
2016-11-14 09:19:34	陈华才 <huacai.cheng@dbappsecurity.com.cn>	基于邮件的APT攻击入侵，恶意文件为[fc8ee45507fe3f808cdf720bf0fc4c1c.doc]	详细 处理
2016-11-04 20:30:06	陈华才 <huacai.cheng@dbappsecurity.com.cn>	基于邮件的APT攻击入侵，恶意文件为[fc8ee45507fe3f808cdf720bf0fc4c1c.doc]	详细 处理
2016-11-04 20:30:03	陈华才 <huacai.cheng@dbappsecurity.com.cn>	基于邮件的APT攻击入侵，恶意文件为[fc8ee4550	理
2016-11-04 20:30:03	陈华才 <huacai.cheng@dbappsecurity.com.cn>	基于邮件的APT攻击入侵，恶意文件为[fc8ee4550	理
2016-11-04 20:30:03	陈华才 <huacai.cheng@dbappsecurity.com.cn>	基于邮件的APT攻击入侵，恶意文件为[fc8ee45507	处理
2016-11-04 20:30:03	陈华才 <huacai.cheng@dbappsecurity.com.cn>	基于邮件的APT攻击入侵，恶意文件为[fc8ee45507fe3f808cdf720bf0fc4c1c.doc]	详细 处理

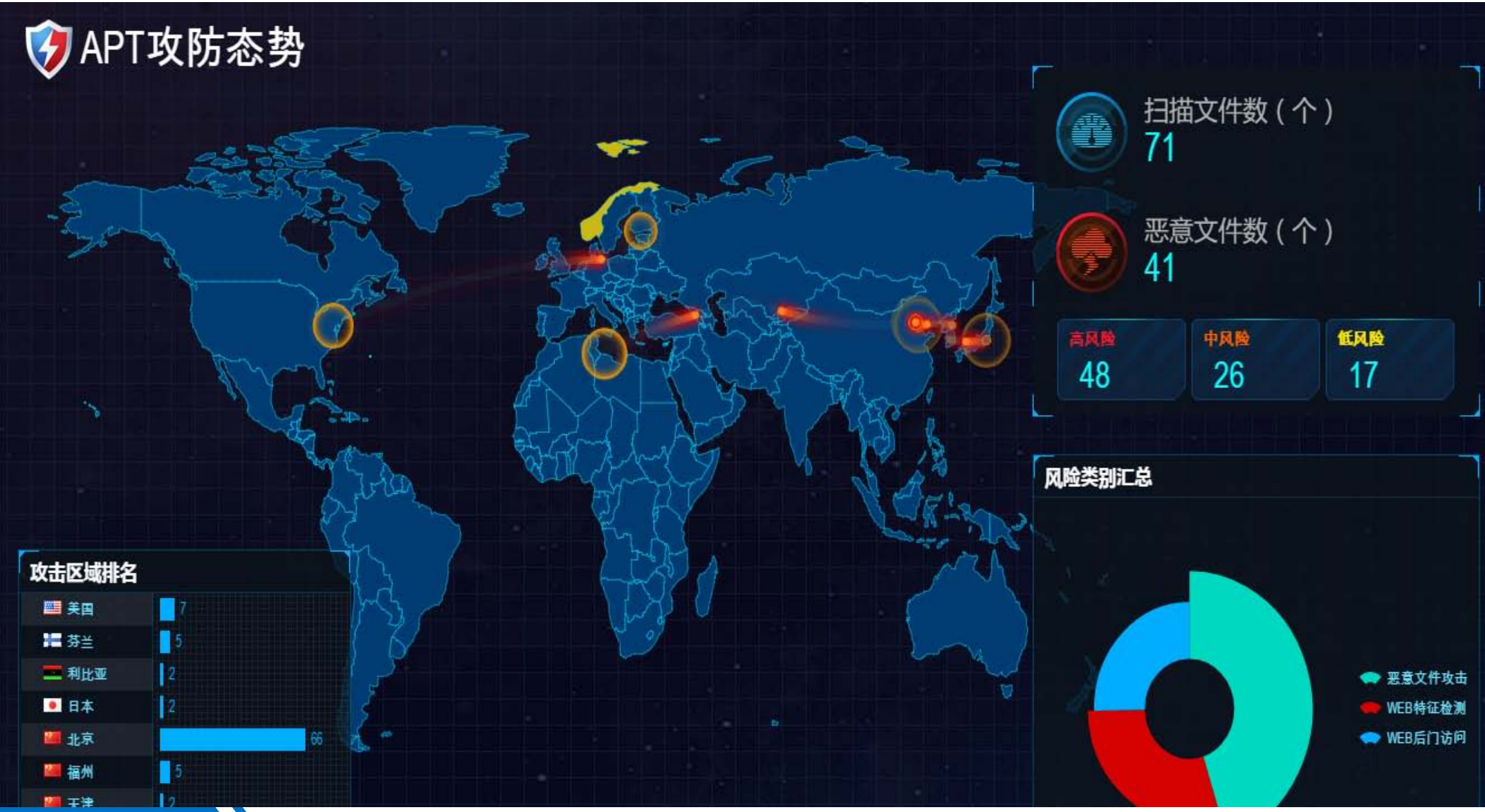
场景化事件分析

攻击事件类型

攻击事件状态分析


192.168.44.51
98
2016-11-11 17:28:06
主机威胁指数
攻击溯源
攻击溯源可视化
攻击过程
攻击过程可视化
2016-11-11 17:28:06
该攻击源对服务器 61.178.65.73 进行了 弱点探测 攻击，攻击次数 6 次，该攻击状态 尝试
2016-11-11 18:35:27
了 弱点探测 攻击，攻击次数 1 次，该攻击状态 尝试
2016-11-11 19:19:23
了 弱点探测 攻击，攻击次数 5 次，该攻击状态
2016-11-12 10:40:49
该攻击源对服务器 119.254.95.228 进行了 弱点探测 攻击，攻击次数 3 次，该攻击状态
2016-11-12 10:50:39
该攻击源对服务器 119.254.95.228 进行了 渗透入侵 攻击，攻击次数 6 次，该攻击状态 尝试
2016-11-12 10:53:43
该攻击源对服务器 119.254.95.228 进行了 获取权限 攻击，攻击次数 47 次，该攻击状态 成功
2016-11-12 10:53:58
该攻击源对服务器 119.254.95.228 进行了 获取权限 攻击，攻击次数 29 次，该攻击状态 尝试
攻击阶段分析
事件状态分析

攻击取证溯源分析


APT攻防态势
扫描文件数（个）
71
恶意文件数（个）
41
高风险
48
中风险
26
低风险
17
风险类别汇总
恶意文件攻击
WEB特征检测
WEB后门访问
攻击区域排名
美国 7
芬兰 5
利比亚 2
日本 2
北京 66
福州 5

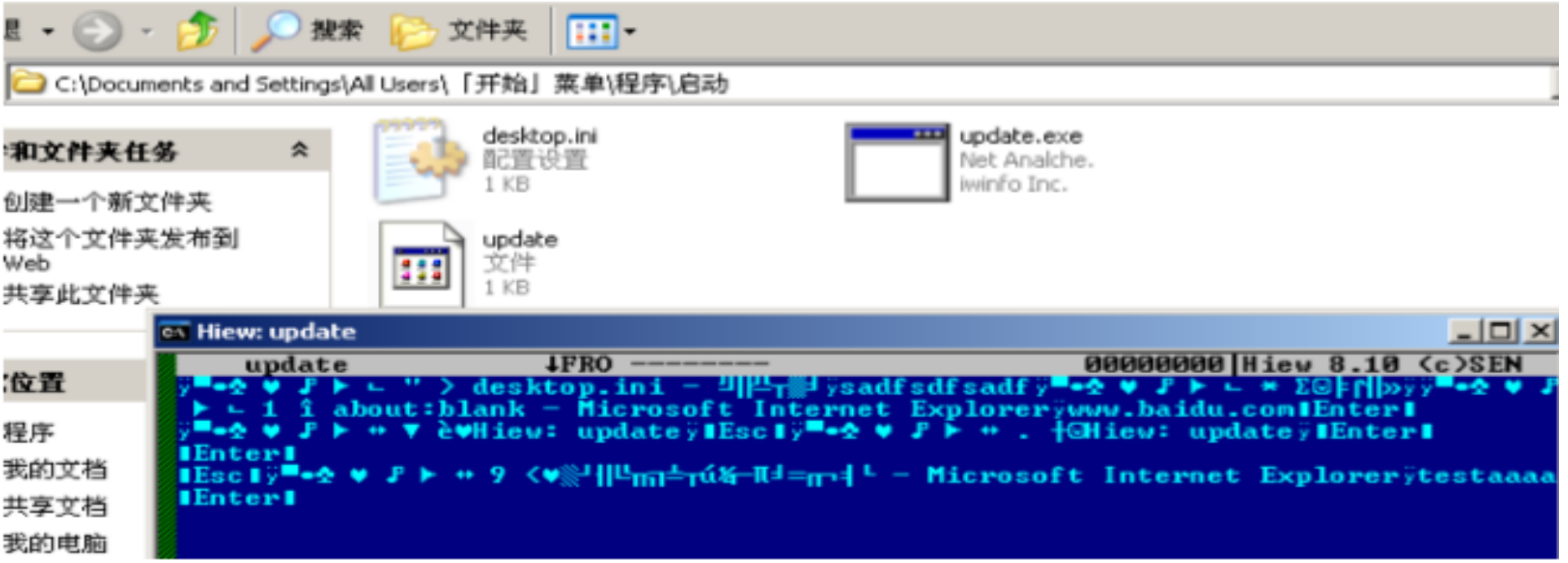
威胁情报分析

文件MD5	威胁指数	传播次数	病毒检测	静态检测	动态检测
2a9fb3dcf97e4d9d8519b7d520ac7f92	■■■■■■■	1	HEUR:Trojan-Downloader.Script.Generic	-	遍历文件 打开服务控制管理器 收集计算机名（通过注册表） 获取当前用户名 通过脚本文件进行Http请求 调用加密算法库

受感染主机 | 威胁情报 | 可视分析 | 回连主机 | 沙箱报告

文件MD5	2a9fb3dcf97e4d9d8519b7d520ac7f92
文件名称	[insurance_c8e0ec886.zip]
云端确认	已确认
威胁指数	■■■■■■■
传播协议	[IMAP]
传播次数	1
病毒检测	HEUR:Trojan-Downloader.Script.Generic
静态检测	-
动态检测	遍历文件 打开服务控制管理器 收集计算机名（通过注册表） 获取当前用户名 通过脚本文件进行Http请求 调用加密算法库

结合邮件社工发起的APT攻击应对案例

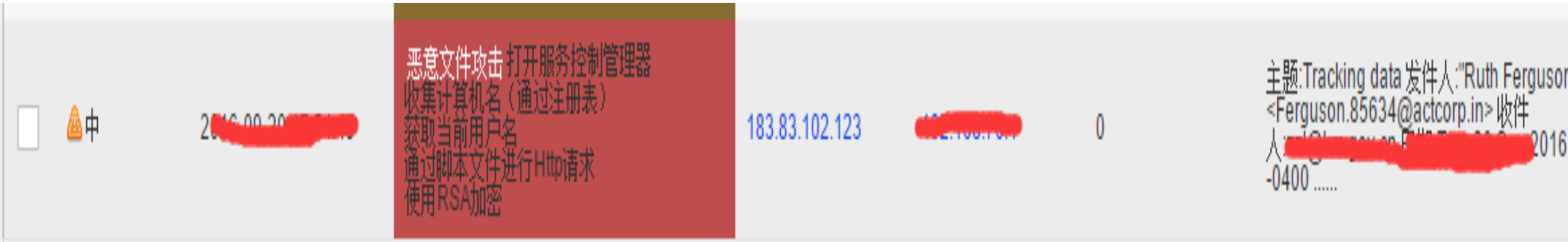


2. 连接远程服务器： sysupdate.ServeUsers.com，发送收集信息.

```
C:\Users\Sean>ping sysupdate.ServeUsers.com
Ping 请求找不到主机 sysupdate.ServeUsers.com。请检查该名称，然后重试。

C:\Users\Sean>
```

变种勒索病毒攻击应对案例



基本信息 | 客户端信息 | 服务端信息 | 分析与建议 | 沙箱运行报告 | 处理

IP	183.83.102.123:58572
MAC	[redacted]BC
发生地点	印度 经度：77.057724 纬度：28.912373

谢　　谢