

互联网威胁情报的落地与应用

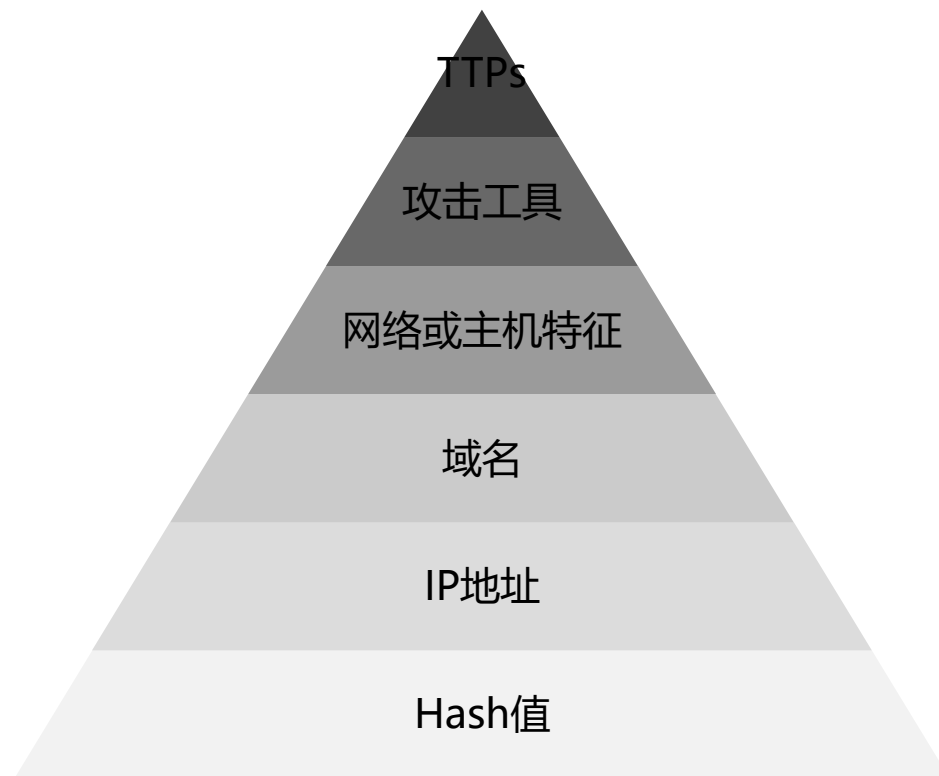
赵林林@微步在线

情报是什么

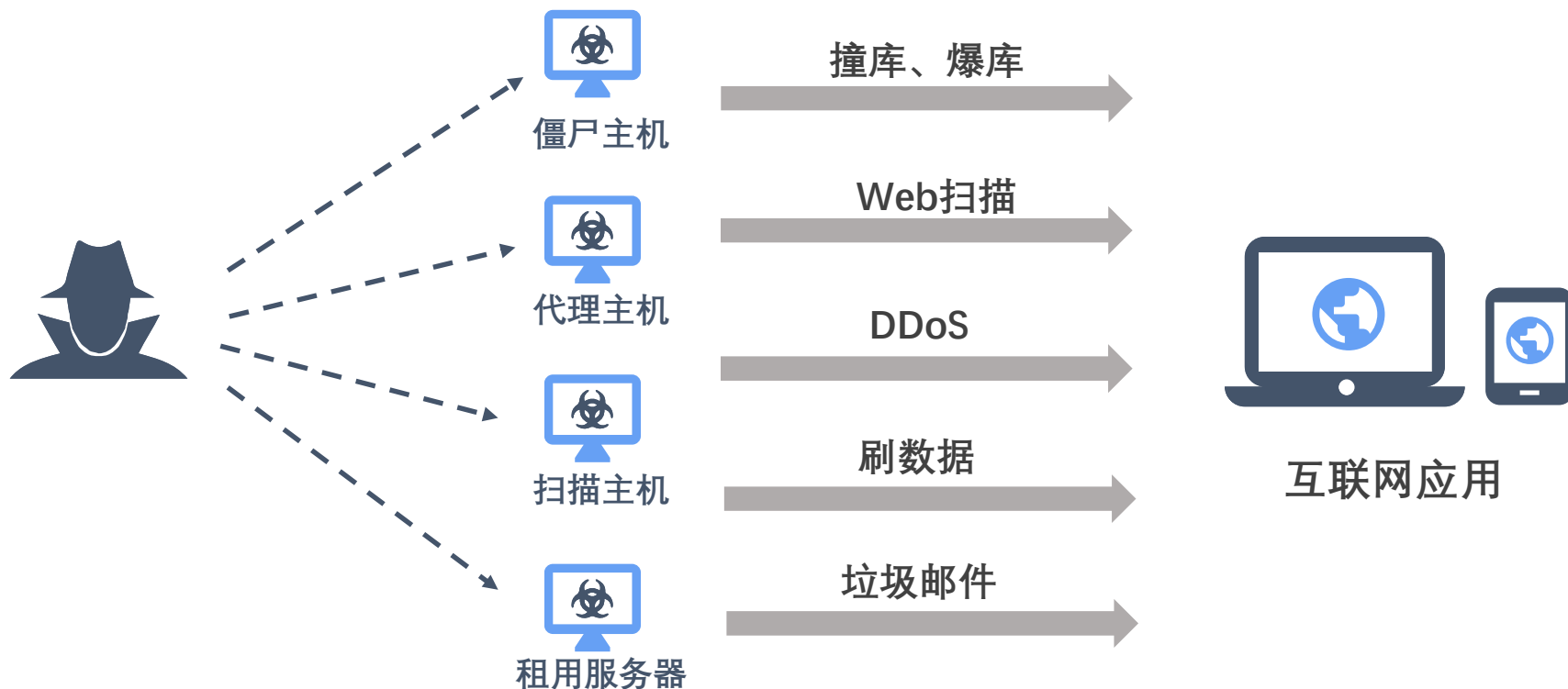


情报包含哪些内容

- 文件HASH值
- IP地址
- 域名
- 网络与主机特征
- 攻击工具
- TTPS



以IP画像为例



- ◆ 仅靠频率统计难以发现撞库、爆库行为
- ◆ 大量的攻击报警，那些是风险最大的？
- ◆ 这个异常到底是攻击，或者是正常访问？
- ◆ 如何快速识别DDoS的IP？
- ◆ 如何快速识别那些非正常客户IP？

基础信息	IDC主机	动态IP	网关IP	未启用IP	教育网、移动基站	风险信息	傀儡机	代理IP	VPN/Tor	扫描IP
	5亿	12亿	200万+	6.5亿	数千万		数千万	数万	100万+	数万

威胁情报 — 格式

```
{
  "protocol": 6,
  "opened_port": [
    443,
    80
  ],
  "ioc_type": "domain",
  "related_sample": [
    "3f65dc1c20b04834a1d3bf4d1c9fdd3f38d40635afc8f3c0ee8862918e751b0e"
  ],
  "confidence": 85,
  "severity": "high",
  "port": 2013,
  "status": 2,
  "tags": [
    "Nitot"
  ],
  "timestamp": 1471619740,
  "ssl": [],
  "resolves": 1,
  "ioc": "ns.msffncsi.com",
  "tlp": 3,
  "level": 4,
  "industry": [
    "Government",
    "Finance"
  ],
  "intel_type": "c2",
  "APT": 1
}
```

关联样本

严重级别

威胁类型

失陷指标

针对行业

是否APT

ThreatBook

微步在线安全事件分析报告

银行 SWIFT 系统再遭 APT 组织 Lazarus 攻击

TAG: 高级持续性攻击、APT、SWIFT、台湾、远东国际商业银行、Lazarus

TLP: 🟡 (仅限接受报告的组织内部使用)

日期: 2017-10-20

概要

2017 年 10 月 3 日, 台湾远东国际商业银行遭遇黑客攻击, 攻击者通过 SWIFT (环球同业银行金融电讯协会) 系统向位于斯里兰卡、柬埔寨和美国的外国银行电汇 6000 万美元, 银行方面发现后通过警方及时冻结了大部分被盗款项, 实际损失金额约 15.65 万美元。

微步在线通过对其中部分木马样本进行关联分析后, 发现幕后团伙仍是近期非常活跃的疑似具有朝鲜官方背景的黑客组织 Lazarus。目前主要发现如下:

- 攻击者首先利用钓鱼邮件突破了银行工作人员的电脑主机, 并以此作为跳板对内部网络进行侦察。
- 在获取了内网主机的认证凭证后, 攻击者直接将账号密码硬编码在木马中并投放至目标网络环境中直接运行。
- 分析发现, 在此次攻击事件的样本集合中有 2 个后门样本与 Lazarus 今年 2 月攻击波兰银行使用的木马高度相似, 另有一个具备勒索功能的木马 Hennes, 推测用于盗取资金后对关键主机文件实施破坏, 并以普通勒索软件的表现迷惑分析人员, 以增加追查和取证的难度。
- Lazarus 团伙通晓银行内部业务流程和 SWIFT 系统操作方式, 且持续对银行业和 SWIFT 系统实施渗透攻击, 对金融行业的威胁程度极高, 需引起有关部门的高度重视。
- 微步通过对本次事件提取 IOC 7 条, 部署微步在线威胁情报平台(TIP)的用户, 可通过系统告警定位到失陷主机, 并使用微步在线提供的应急响应予以分析和处理。

情报的使用



如何使用情报?

- 外网
- 内网
- 业务
- 溯源

如何使用情报?

- 检测出口流量中，连接黑客资源的主机
 - 准确性、实时性、覆盖范围
 - 使用位置?

案例：WannaCry

微步在线：国内首家发布WannaCry秘密开关的威胁情报报告

```
{“ioc”：“www.aaylmaotjhsstasdfasdfasdfasdfasdf.com”,  
“related_samples”:[“22ccdf145e5792a22ad6349aba37d960db77af7e0b6cae826d228b8246705092”],  
“patches”:[“CVE-2017-0144”]}
```

WannaCry

Ransomware Attack



全面监控与检测

用户应用开关域名（IOC）进行全面的失陷检测



快速响应

应用配置DNS解析的方式保护主机达数百万台



自动联动修复

应用情报中的CVE标识自动联动终端管理进行补丁修复

情报发现后的困难与问题

- 入侵的路径 – 点、面
- 如何定位
- 横向移动

问题的解决

- 定位与攻击路径
 - 端 + 流量
 - 端 → 信任
- 横向移动（可控，杠杆率）
 - 边界
 - 域控



来自用户的挑战



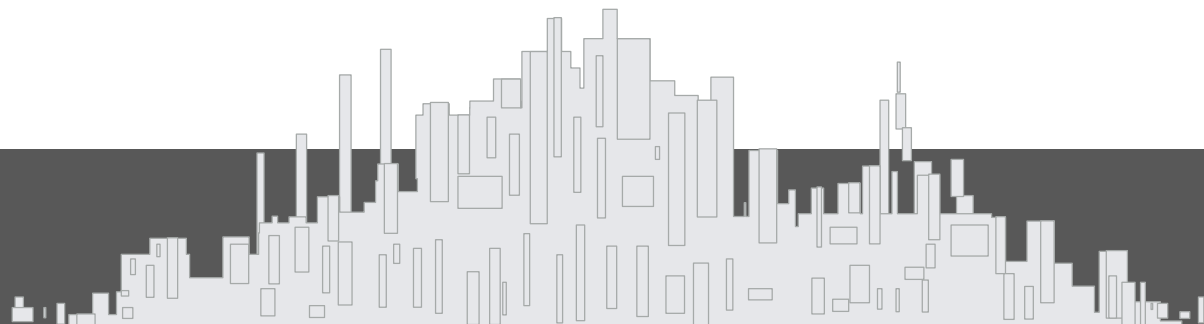
用户的挑战

- 服务器区比办公网更重要
- 每天扫我的这些人都在干什么？
- 攻击我服务器的这些人，你为什么不报警？

外部攻击中，情报的作用

- 利用情报筛选攻击源
 - 访问即监测
- 利用情报来排除掉非针对性攻击
- 大胆封阻

大型互联网公司的挑战



用户的挑战

你们的情报还不错，但是：

- 我流量很大
- 我们自己有开发
- 我们还是希望有自己的情报库
- 有钱，不太可能只用你一家的情报

状态

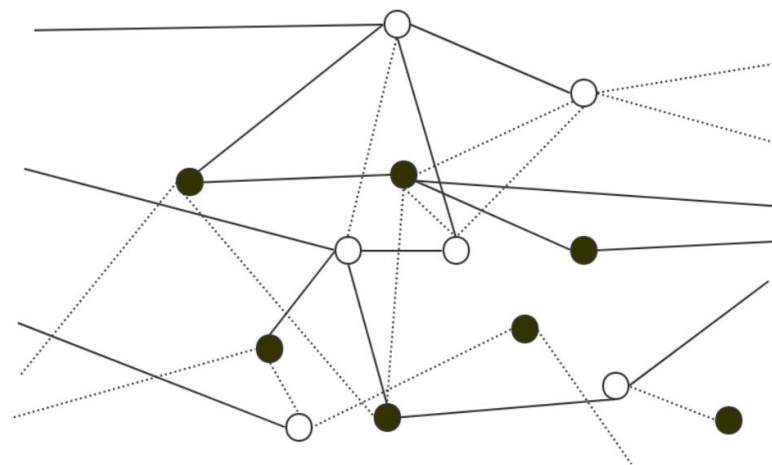
- 数据区域划分是完整的
- 边界的数据、系统的日志、审计的信息
- 有完善的组织系统/平台
- 能够自产情报

-
- 怎么点亮这些大数据
 - 怎么持续追踪和积累情报

splunk>

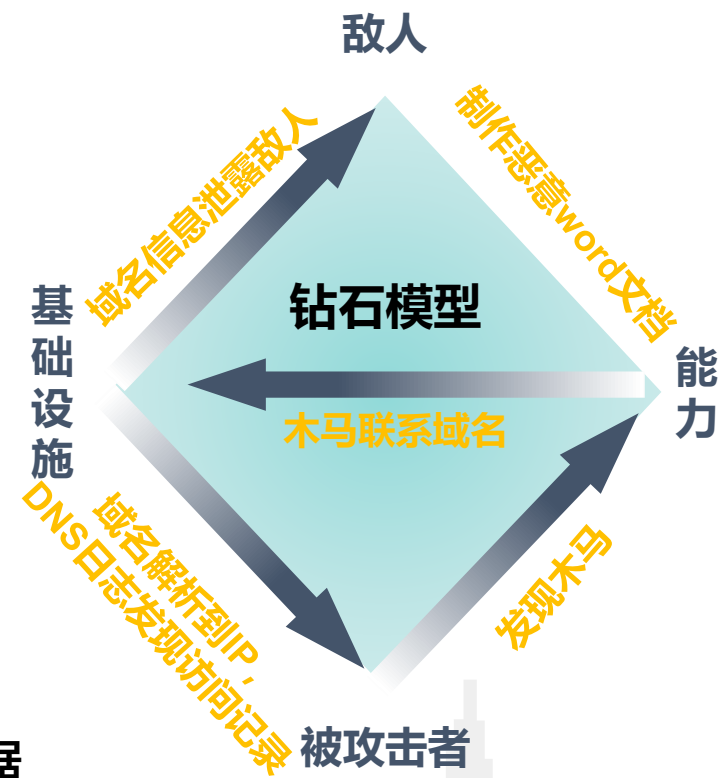
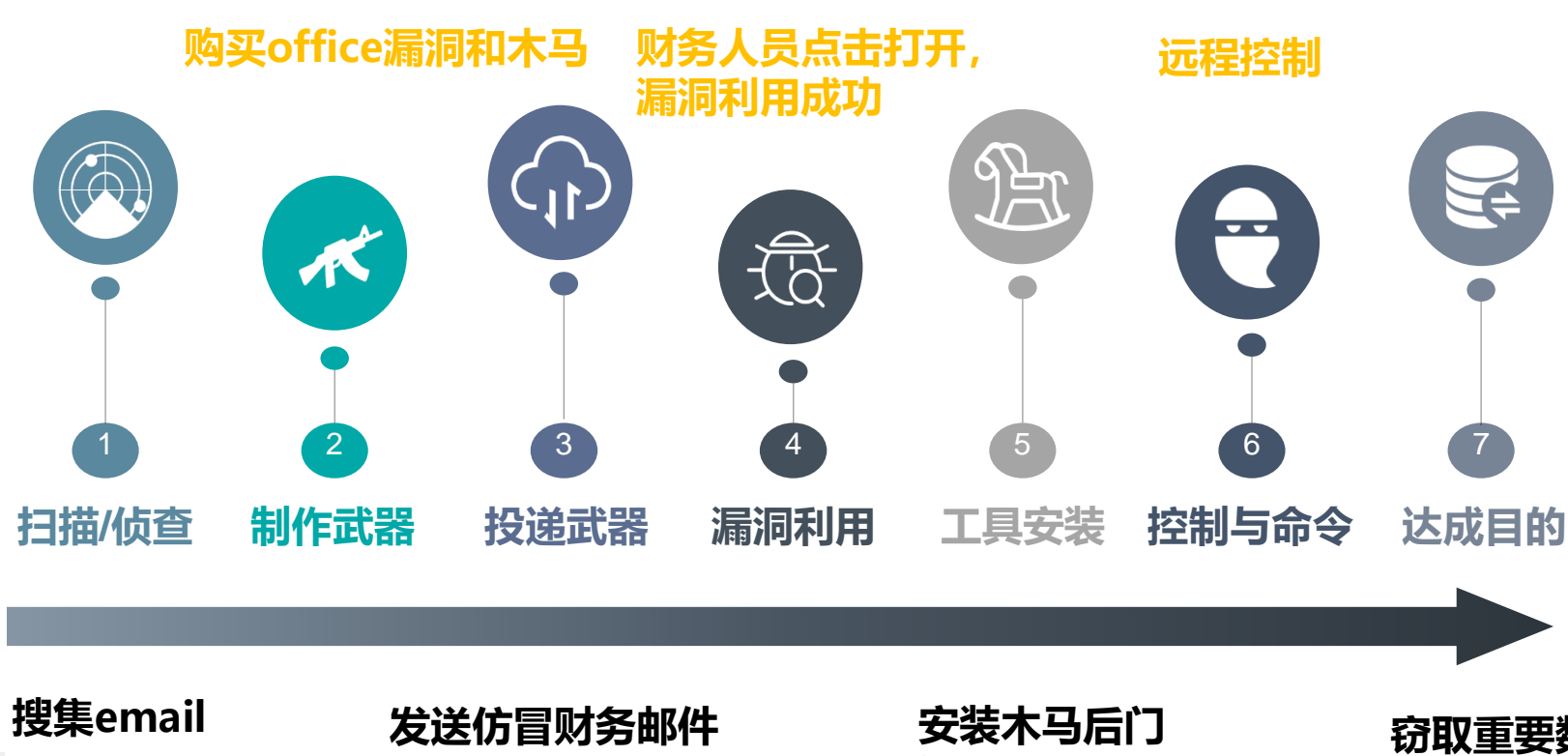
SIEM

大数据平台



情报积累样例

挑战：如何管理，如何长期、自动跟踪？



关于利用情报溯源



XSHELL追踪

- 团伙特点:
 - 有组织、有计划
 - 目的清楚
 - 会隐藏、保护自己
 - 有技术能力



ThreatBook 中文 97363d50a279492fda14cbab53429e75 分析

检出率 12 / 24

SHA256 462a02a8094e833fd456baf0a6d4e18bb7dab1a9f74d5f163a8334921a4ffde8

分析时间 2017-08-21 10:50:02 (94天前)

Tags Backdoor Shadowpad 恶意软件 XshellGhost

用户标记 木马(1) 后门(1) 官网被搞(1) 添加用户标签

检测结果

静态信息

行为分析

网络活动

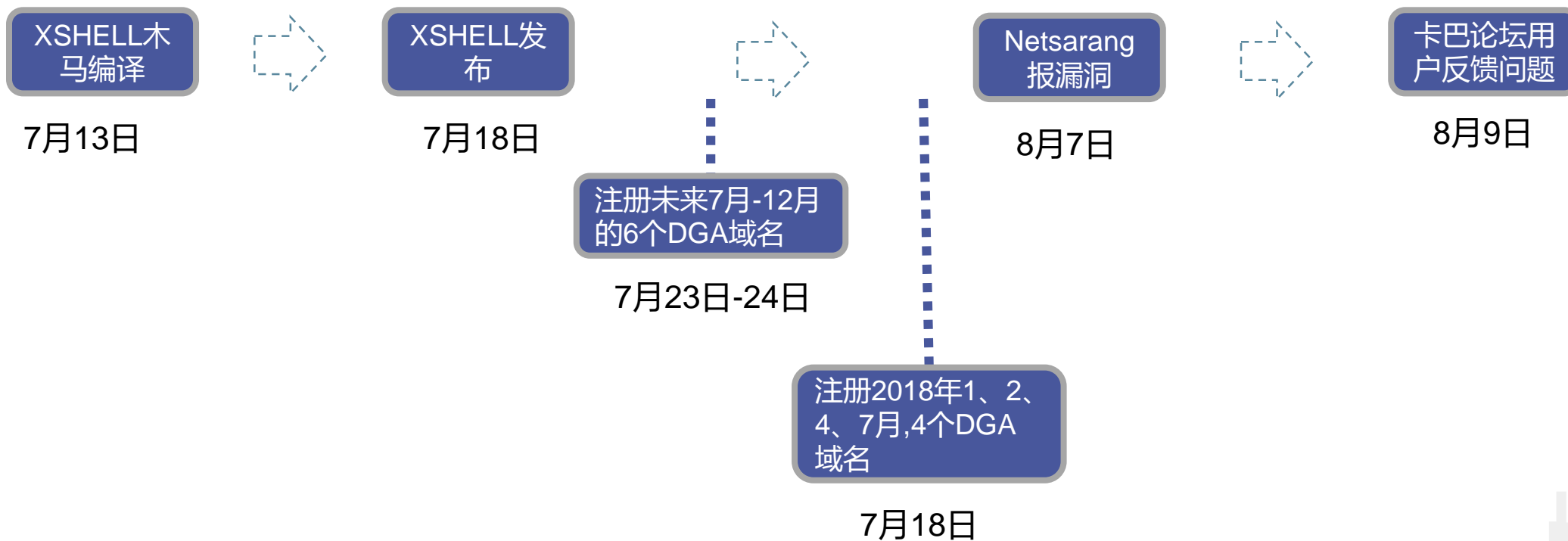
威胁情报

可视分析

用户标签

反病毒软件	结果	病毒库日期
IKARUS	Backdoor.Win32.Shadowpad	2017-08-21
火绒 (Huorong)	Backdoor/Shadowpad.a	2017-08-21
腾讯 (Tencent)	Win32.Backdoor.Shadowpad.Cbwa	2017-08-21
小红伞 (Avira)	TR/Wdfload.tnvhv	2017-08-21
Sophos	Troj/Agent-AWXP	2017-08-21

活动



APT事件 – XSHELL追踪

ribotqtonut.com 分析报告

域名服务商 NameSilo, LLC
域名服务器 ns1.qhoster.net; ns2.qhoster.net; ns3.qhoster.net; ns4.qhoster.net
Alexa排名 N/A
Tags 远控 XshellGhost
用户标记 木马(1) 后门(1) 官网被搞(1) [添加用户标签](#)

威胁情报

IP分析

子域名

Whois

数字证书

可视分析

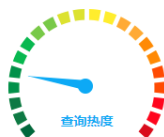
vmvahedczyrml.com 分析报告

域名服务商 NameSilo, LLC
域名服务器 ns1.qhoster.net; ns2.qhoster.net; ns3.qhoster.net; ns4.qhoster.net
Alexa排名 N/A
Tags 远控 XcodeGhost
用户标记 木马(1) 后门(1) 官网被搞(1) [添加用户标签](#)

当前注册信息

当前注册信息

注册者 Lucy Anteo (相关域名 3 个)
注册机构
邮箱 lucyaggregate@gmail.com (相关域名 3 个)
地址
电话 +43.37066841323
注册时间 2017-08-01 00:00:00
过期时间 2018-08-01 00:00:00
更新时间: 2017-08-08 00:00:00
域名服务商 NameSilo, LLC
域名服务器 ns1.qhoster.net; ns2.qhoster.net; ns3.qhoster.net; ns4.qhoster.net



Domain Administrator ([通用注册名称不再显示相关域名](#))

See PrivacyGuardian.org

pw-27a93b32c963de1655e3ef9d0fad7575@privacyguardian.org ([相关域名 0 个](#))

+1.3478717726

2017-07-23 00:00:00

2018-07-23 00:00:00

2017-07-24 00:00:00

NameSilo, LLC

ns1.qhoster.net; ns2.qhoster.net; ns3.qhoster.net; ns4.qhoster.net

APT事件 – XSHELL追踪

ribotqtonut.com 分析报告

域名服务商 NameSilo, LLC
域名服务器 ns1.qhoster.net; ns2.qhoster.net; ns3.qhoster.net; ns4.qhoster.net
Alexa排名 N/A
Tags 远控 XshellGhost
用户标记 木马(1) 后门(1) 官网被搞(1) [添加用户标签](#)



威胁情报 IP分析 **子域名** Whois 数字证书 可视分析 用户标签

子域名

共8个，免费用户最多可查看10个子域名

[ns1.ribotqtonut.com](#)
[ns3.ribotqtonut.com](#)
[dns.ribotqtonut.com](#)
[oajjlyoogrmkakhpnjnnmndopwlvajmkdubjgwbvajokhplviodym.nvayawbjckjmonnsjmaterhsgtoknxiolxkvbkfngulnhpjslubuhv.dpbudp.ribotqtonut.com](#)
[www.ribotqtonut.com](#)
[ns4.ribotqtonut.com](#)
[ns2.ribotqtonut.com](#)
[ns5.ribotqtonut.com](#)

共有 8 条信息 [收起](#)

ns1.ribotqtonut.com 分析报告

域名服务商 NameSilo, LLC
域名服务器 ns1.qhoster.net; ns2.qhoster.net; ns3.qhoster.net; ns4.qhoster.net
Alexa排名 N/A
Tags 远控 XshellGhost
用户标记 远控服务器(0) 恶意网站(0) 正常网站(0) [添加用户标签](#)

威胁情报 **IP分析** 子域名 Whois 数字证书 可

IP地址

IP地址 **209.105.242.187** 共有 1 个域名指向此地址
地理位置 美国,德克萨斯州,达拉斯 (corexchange.com)
ASN 13354 (ASN-EBLGLOBAL - EBL Global Networks, Inc., US)

历史解析记录

时间	IP	国家	省 / 州
2017-07-25	209.105.242.187	美国	德克萨斯州

APT事件 – XSHELL追踪

另一个邮箱浮出水面: hostay88@gmail.com



微步在线产品概览



威胁分析云

威胁检测产品

威胁检测平台-TDP

攻击感知平台-TDPS

威胁情报产品

威胁情报管理平台TIP

情报检测与分析API

SaaS服务

云沙箱分析API

追踪溯源平台-Z

安全DNS

企业安全服务-MDR

应急响应服务

威胁监控服务

高级情报订阅

安全从业者社区与分析平台

威胁情报社区-X

云沙箱分析平台-S

招人

- 安全分析师、大师
- 销售、售前
- 客户成功经理
- 开发工程师

推荐成功，送iPhone XR



林海 

中国



扫一扫上面的二维码图案，加我微信