威胁情报与APT

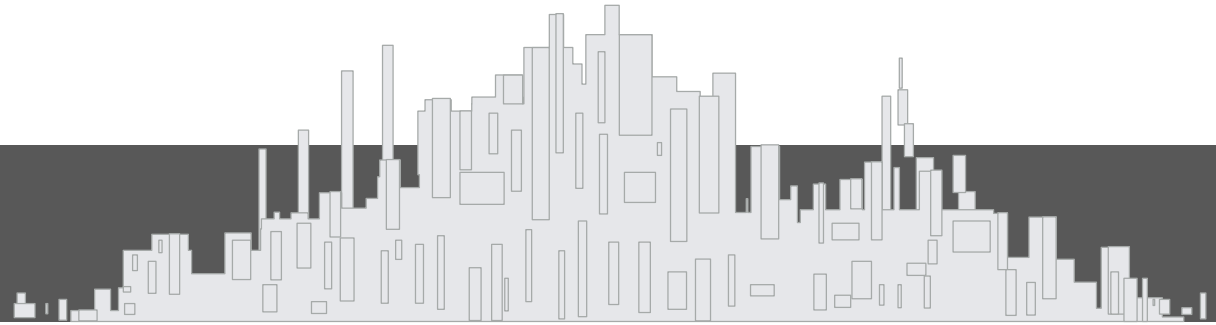
微步在线CEO - 薛锋

微步在线

第1位	100人	1.65亿
唯一入选Gartner威胁情报市场指南	**专注于威胁情报分析与产品**	**2017年完成B轮融资**
服务国内超过1000家企业，金融、能源、互联网、政府	亚马逊、微软、百度、美团、阿里巴巴等	北极光、 如山创投、高瓴资本等

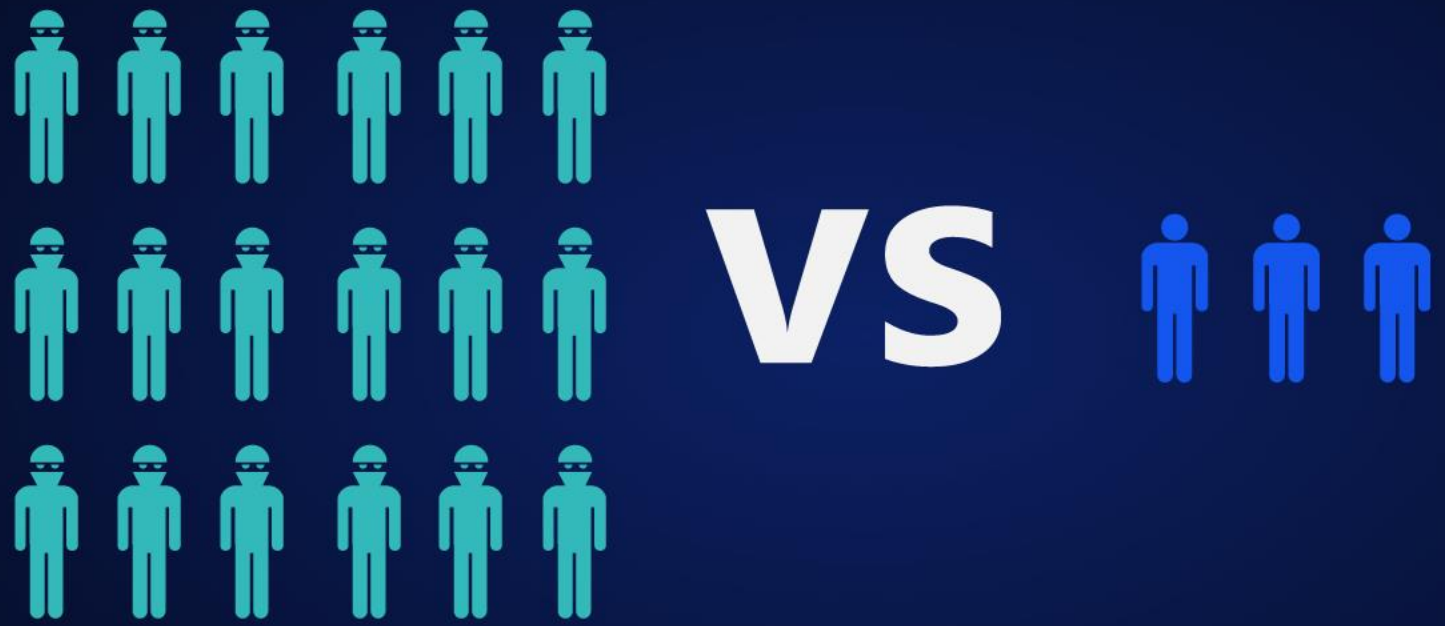
入选全球网络安全500强的9家中国公司之一

安全的挑战
Challenges to Cybersecurity



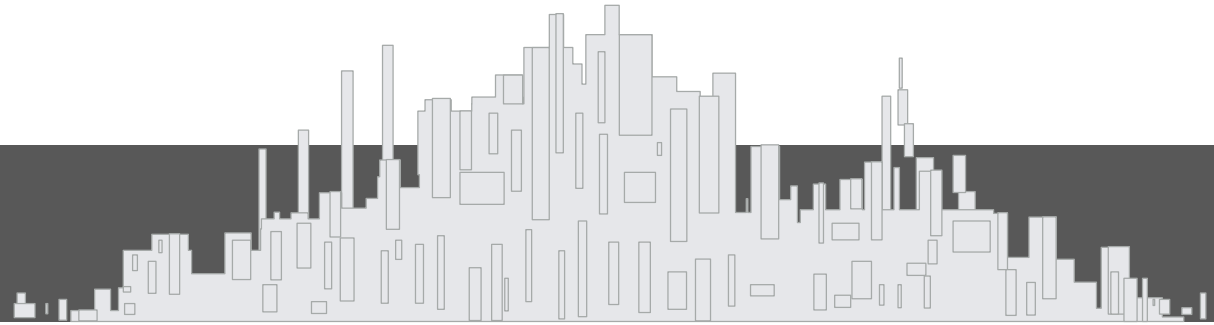
VS

VS

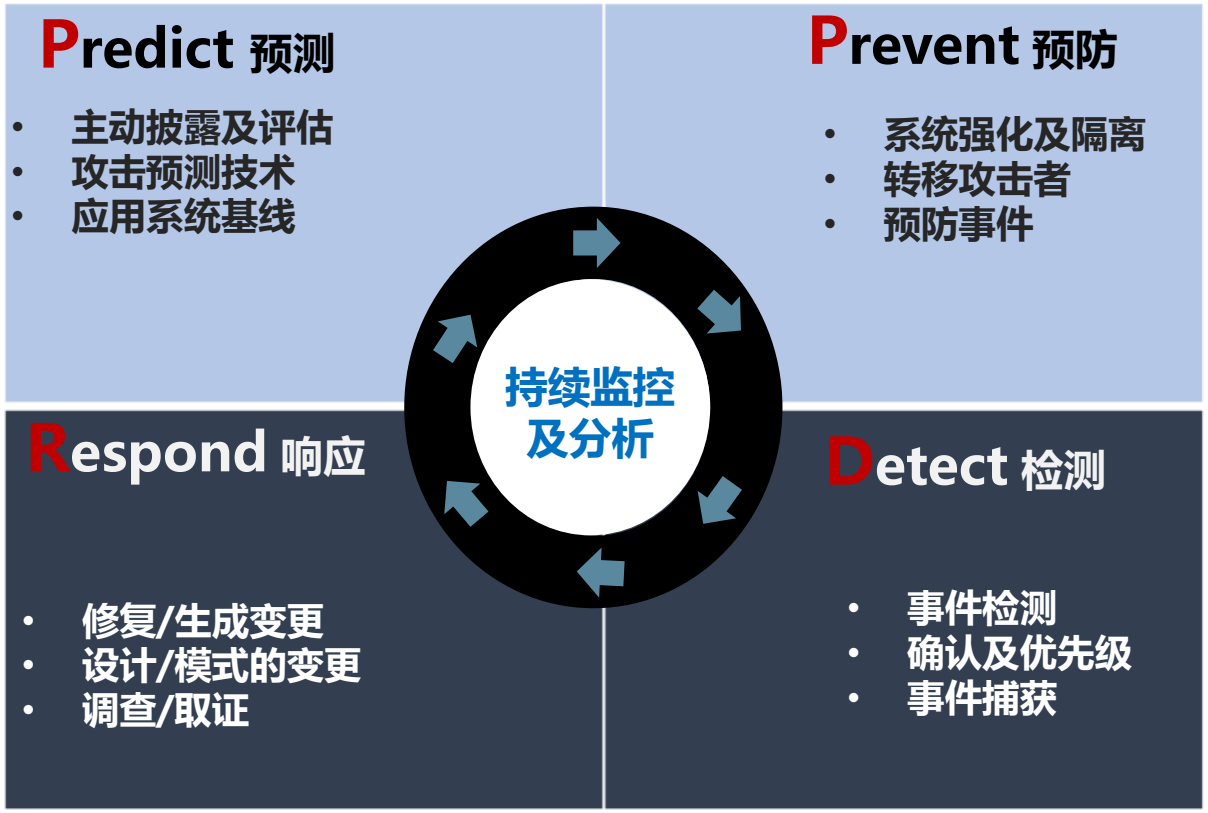

VS

人力有限、经验有限	人	专业团队、团伙作战
有限的时间做迅速的响应	时间	充裕的攻击准备和移动时间
依赖有限的组织内外支持	资源	成熟的工具、服务支持
手工操作与分析	自动化	自动化的工具和流程
资产不可见、攻击不可见	可见性	更了解组织的网络结构

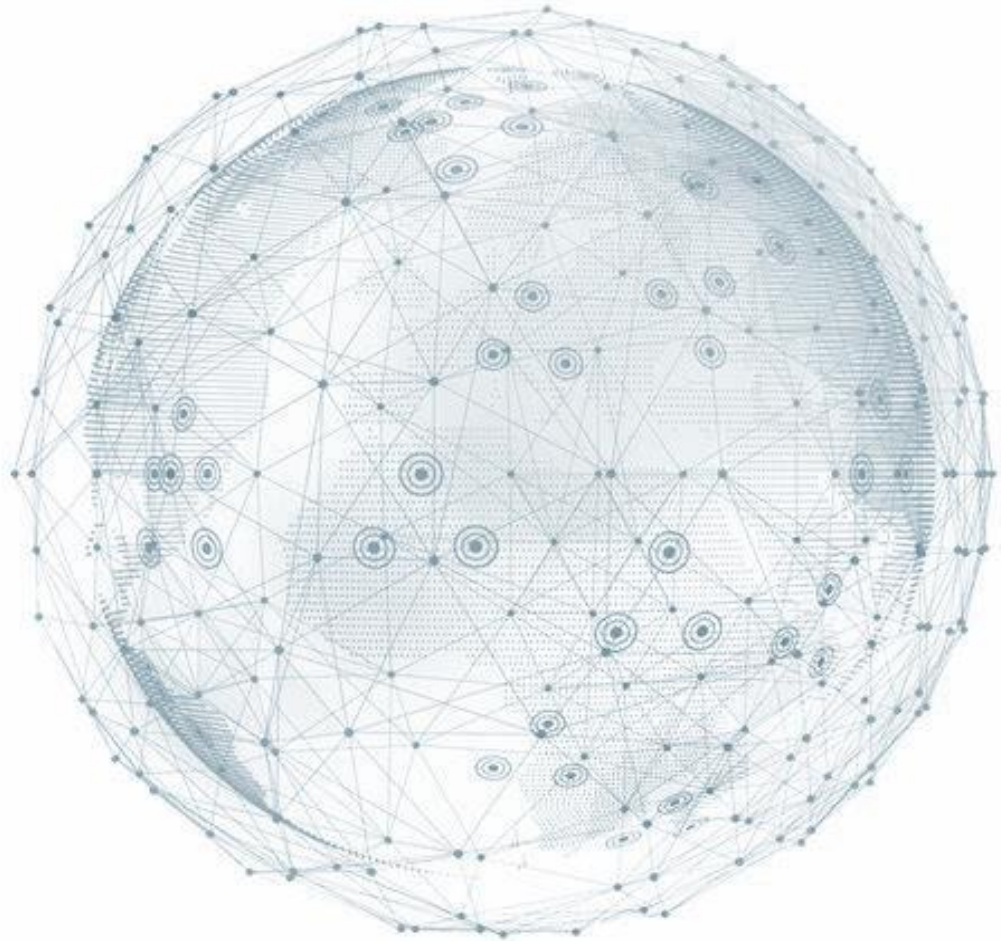
威胁情报的应用
Threat Intelligence: Zero to One



“企业将处于持续被攻陷的状态…” - 检测和响应成为重心

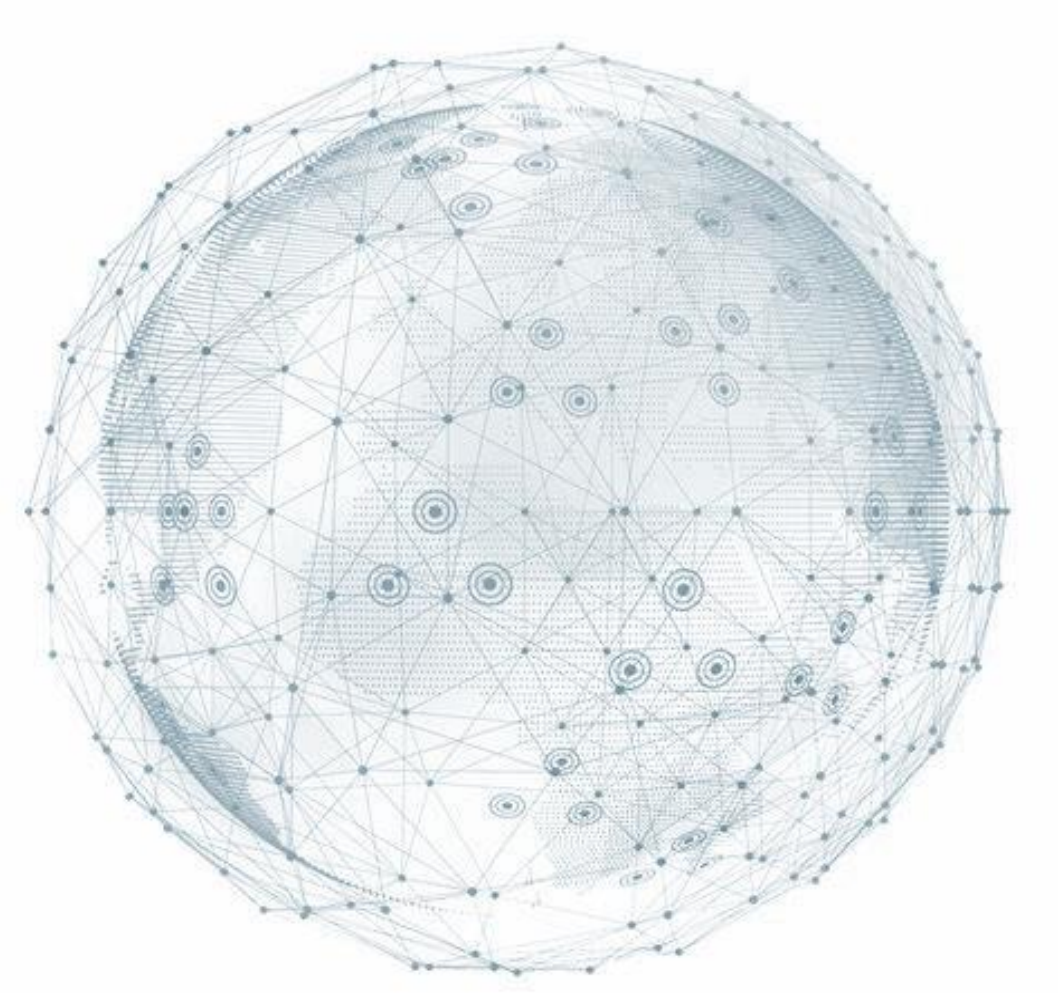


威胁情报 vs. APT



Threat Graph

出站情报
IOC: C&C，malware，
域名/IP/URL



入站情报
IP信誉和情报

搜索引擎

威胁情报是高级应用？

企业威胁情报落地

iSOC
(Intelligence-Driven Security Operation Center)

各类安全设备
(WAF\IPS\NGFW)

TDP-威胁检测与响应平台

NTA
(Network Traffic Analysis)

EDR
(Endpoint Detection and Response)

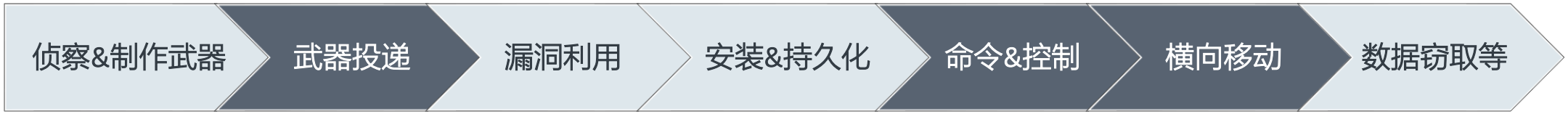
应急响应服务

情报应用实例：WannaCry

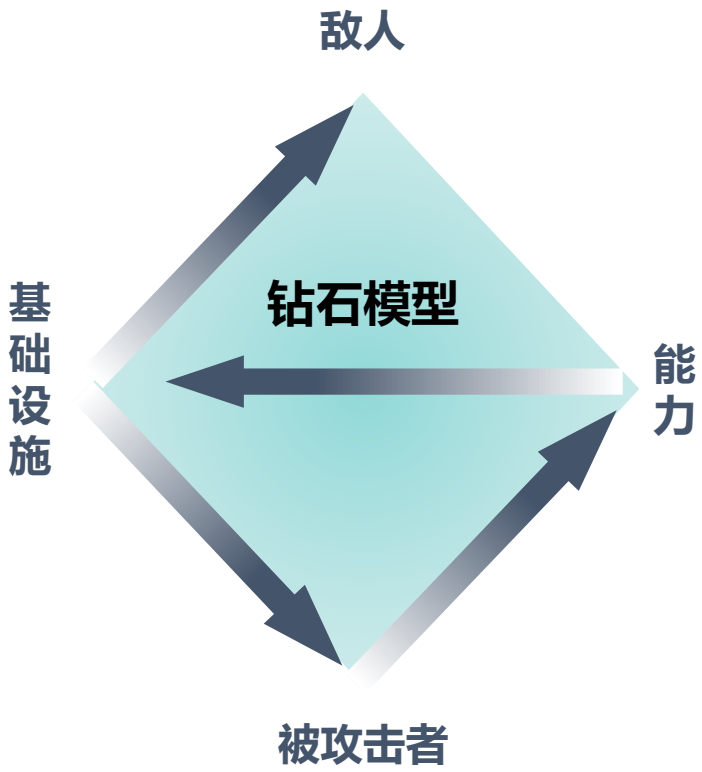
发布WannaCry秘密开关的威胁情报报告

{“ioc”:”www. iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com”,
“related_samples”:[“22ccdf145e5792a22ad6349aba37d960db77af7e0b6cae826d228b8246705092”],
“patches”:[“CVE-2017-0144”]}

情报积累 - Kill Chain



情报积累 – 钻石模型



AD域被黑事件

各位朋友，前天提及的某客户AD和Exchange服务器被入侵的事件，目前已经大部分恢复（在活动目录和Exchange服务器层面已经恢复完整控制权）。该客户全网的域控制器数量接近30台，是截止到目前为止，我们在国内所遭遇到的规模最大的一次真实的（不含红蓝对抗场景）活动目录入侵事件[尴尬]，在此我做一个小结。

1、攻击事件尚在溯源中，打开突破口的方式 90% 可能是通过 **Web 注入或钓鱼邮件**实现，目前还没有找到最初的跳板机和 Downloader；

2、该木马的载体是 **PowerShell**（Windows 下最强大也是最危险的工具，我的最爱 [调皮]），通过脚本实现，全程无 EXE 可执行文件，杀毒软件基本无用；

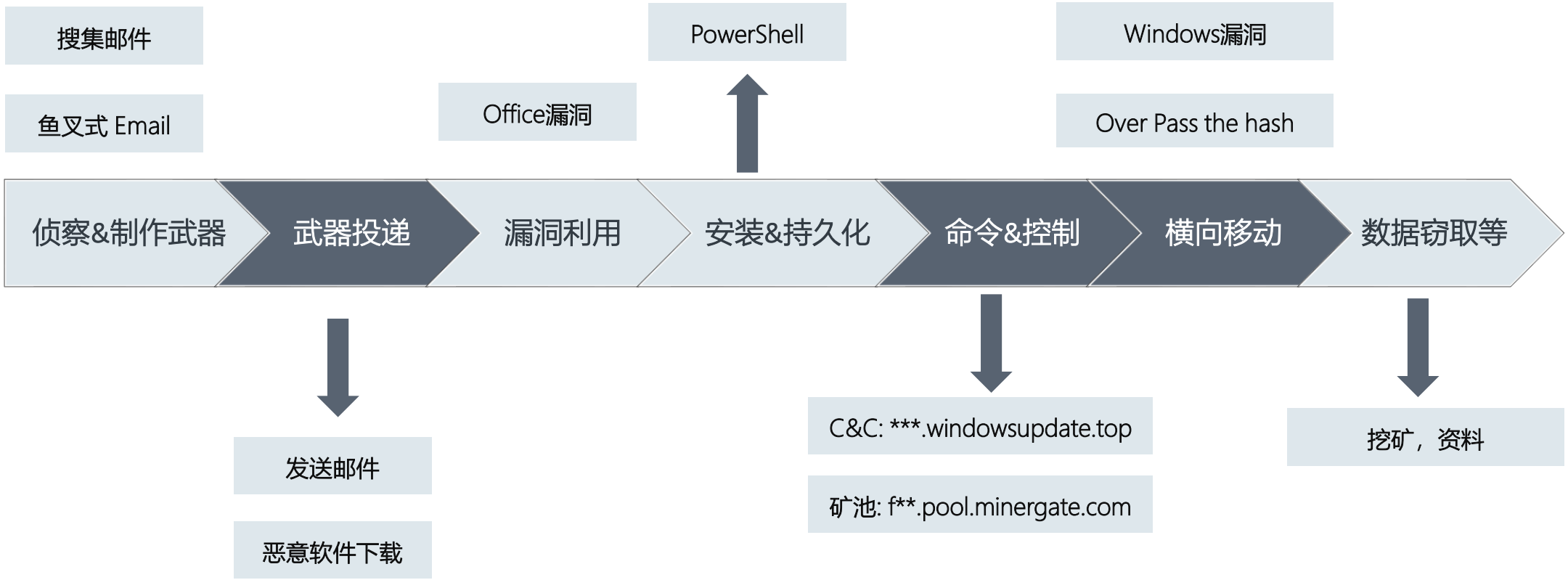
3、木马传播方式以多个系统漏洞（包含去年 WannaCry 勒索病毒所使用的 MS17-010等）和 Pass the hash 方式为主，可能还包含其他方式；

4、该木马持续保有系统控制权的方式，主要通过去年美国中情局泄露的 Vault 7 入侵工具中的方式来实现；

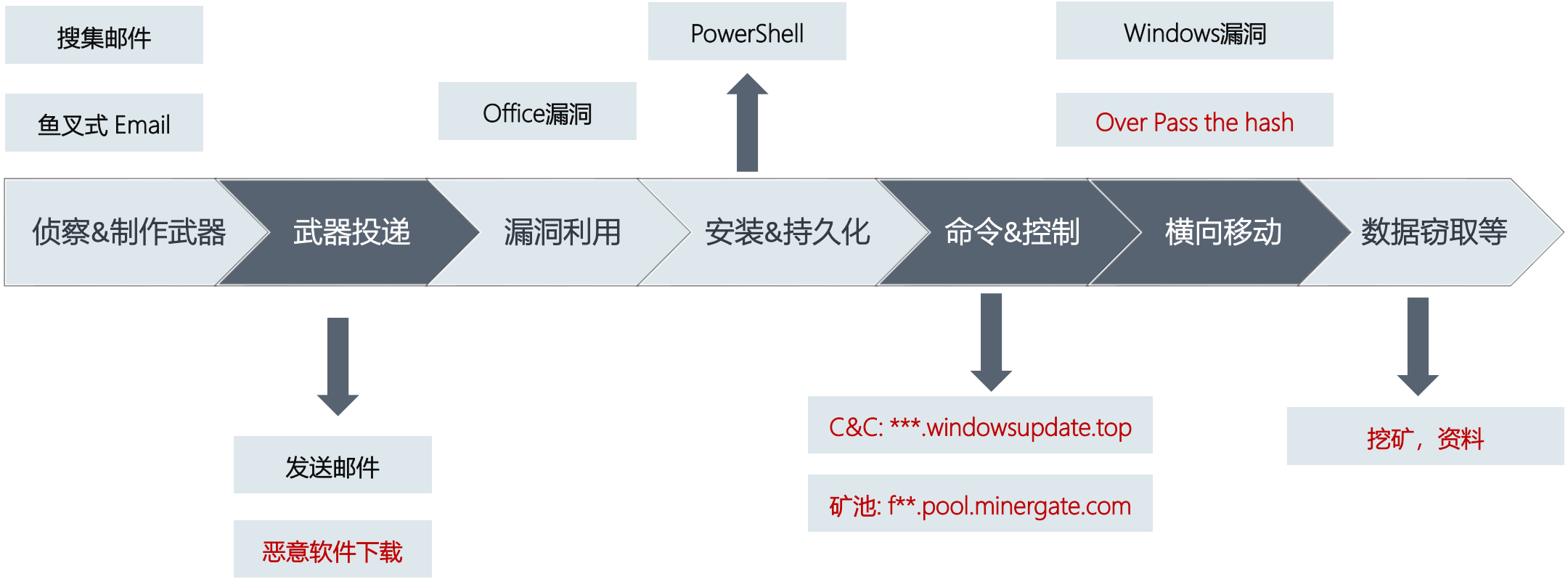
5、攻破域控制器之后，木马通过活动目录进行疯狂的传播，全网中的绝大部分 Windows 服务器和客户端均中招，但是部分未加入域的计算机一样被感染，具体原因还在分析之中；

6、该木马自带挖矿功能，并反向连接国外的 C&C 服务器。该 C&C 服务器位于法国，并使用多个 Windows Update 相似域名来规避监测。不幸中的万幸，不是去年 WannaCry 那种加密勒索型木马，否则损失就巨大了[大哭]。

Kill Chain


搜集邮件
鱼叉式 Email
Office漏洞
PowerShell
Windows漏洞
Over Pass the hash
侦察&制作武器
武器投递
漏洞利用
安装&持久化
命令&控制
横向移动
数据窃取等
发送邮件
恶意软件下载
C&C: ***.windowsupdate.top
矿池: f**.pool.minergate.com
挖矿，资料

Kill Chain


搜集邮件
鱼叉式 Email
Office漏洞
PowerShell
Windows漏洞
Over Pass the hash
侦察&制作武器
武器投递
漏洞利用
安装&持久化
命令&控制
横向移动
数据窃取等
发送邮件
恶意软件下载
C&C: ***.windowsupdate.top
矿池: f**.pool.minergate.com
挖矿，资料

恶意软件下载


威胁发现
24小时
7天
内网主机
检出威胁行为
检出
可疑
10.9.154.22
尝试下载可疑文件: altocloudmedia.com
12
时间
类别
主题
长度
2018-05-30 17:36:32 流量 文件(HTTP) 307 KB
2018-05-30 03:16:08 流量 文件(HTTP) 307 KB
2018-05-30 01:11:12 流量 文件(HTTP) 307 KB
2018-05-29 17:36:03 流量 文件(HTTP) 307 KB
2018-05-29 03:43:07 流量 文件(HTTP) 336 KB
2018-05-29 01:11:12 流量 文件(HTTP) 336 KB
2018-05-28 17:35:37 流量 文件(HTTP) 687 KB
2018-05-28 03:37:09 流量 文件(HTTP) 4 MB
显示更多
可疑
10.9.154.22
尝试下载可疑文件: 106.75.75.68
6
[2018-05-30 17:36:32] 尝试下载可疑文件: altocloudmedia.com
HTTP 80
10.9.154.22
178.63.50.9
下载 altocloudmedia....
altocloudmedia....
行为
文件(HTTP)
文件下载URL: altocloudmedia.com/tunnel/netstream.exe
Sha256: c04d45640b7422105d6ee3a982dafb3b58c54f6a6eff08ef2d7555274c4e03e5
查看完整云沙箱结果
源IP地址: 10.9.154.22
源端口: 58061
目的IP地址: 178.63.50.9
目的端口: 80
方法: GET

C&C检测


威胁发现
24小时
7天
30天
内网主机
检出威胁行为
检出
严重
10.10.72.18
连接海莲花_安全事件远控地址: chinanetworkvub.info
8
时间
类别
主题
长度
2018-05-30 07:11:02 网络行为 DNS -
2018-05-30 07:11:02 网络行为 HTTP 1 KB
2018-05-29 07:11:02 网络行为 DNS -
2018-05-29 07:11:02 网络行为 HTTP 1 KB
2018-05-28 07:11:02 网络行为 DNS -
2018-05-28 07:11:02 网络行为 HTTP 1 KB
2018-05-27 07:11:02 网络行为 HTTP 1 KB
2018-05-27 07:11:01 网络行为 DNS -
[2018-05-30 07:11:02] 连接海莲花_安全事件远控地址: chinanetworkvub.info
HTTP 80
连接
10.10.72.18
chinanetworkvub...
行为
pcap下载
HTTP
源IP地址: 10.10.72.18
源端口: 38892
目的IP地址: 144.202.47.216
目的端口: 80
方法: GET
URL: /
请求长度: 1 KB
Request→
GET / HTTP/1.1
Host: chinanetworkvub.info
Connection:

挖矿检测


威胁发现
24小时
7天
30天
内网主机
检出威胁行为
检出
可疑
10.10.100.17
连接矿池地址MiningPool: fcn-xmr.pool.minergate.com
12
时间
类别
主题
长度
2018-05-30 05:11:11
网络行为
DNS
-
2018-05-30 05:11:10
网络行为
DNS
-
2018-05-29 05:11:11
网络行为
DNS
-
2018-05-29 05:11:11
网络行为
DNS
-
2018-05-28 05:11:10
网络行为
DNS
-
2018-05-28 05:11:10
网络行为
DNS
-
2018-05-27 05:11:11
网络行为
DNS
-
2018-05-27 05:11:10
网络行为
DNS
-
[2018-05-30 05:11:11] 连接矿池地址MiningPool: fcn-xmr.pool.minergate.com
DNS 53
查询
10.10.100.17
fcn-xmr.pool.mi...
行为
pcap下载
DNS
DNS服务器地址:
8.8.4.4
源端口:
53
内网主机:
10.10.100.17
目的端口:
54913
查询类型:
A
查询域名:
fcn-xmr.pool.minergate.com
查询结果:
94.130.48.154

内网横向移动检测

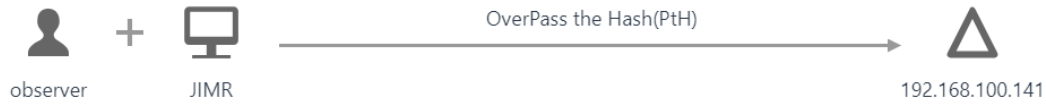
威胁发现

24小时 | 7天 | 30天

内网主机	检出威胁行为	检出
严重 JIMR	发现域192.168.100.141内横向移动行为:OverPass the Hash(P... 降低Kerberos协议的加密等级	7

时间	类别	主题	长度
2018-05-25 19:45:59	域行为	Kerberos	-
2018-05-25 19:45:18	域行为	Kerberos	-
2018-05-25 19:33:22	域行为	Kerberos	-
2018-05-24 20:48:19	域行为	Kerberos	-
2018-05-24 20:43:38	域行为	Kerberos	-
2018-05-24 20:37:33	域行为	Kerberos	-
2018-05-24 20:15:19	域行为	Kerberos	-

[2018-05-25 19:45:59] 发现域192.168.100.141内横向移动行为:OverPass the Hash(PtH)



攻击过程

攻击者在 JIMR 机器上利用 observer 的Hash，加密降级尝试登录域控服务器 192.168.100.141

相关实体

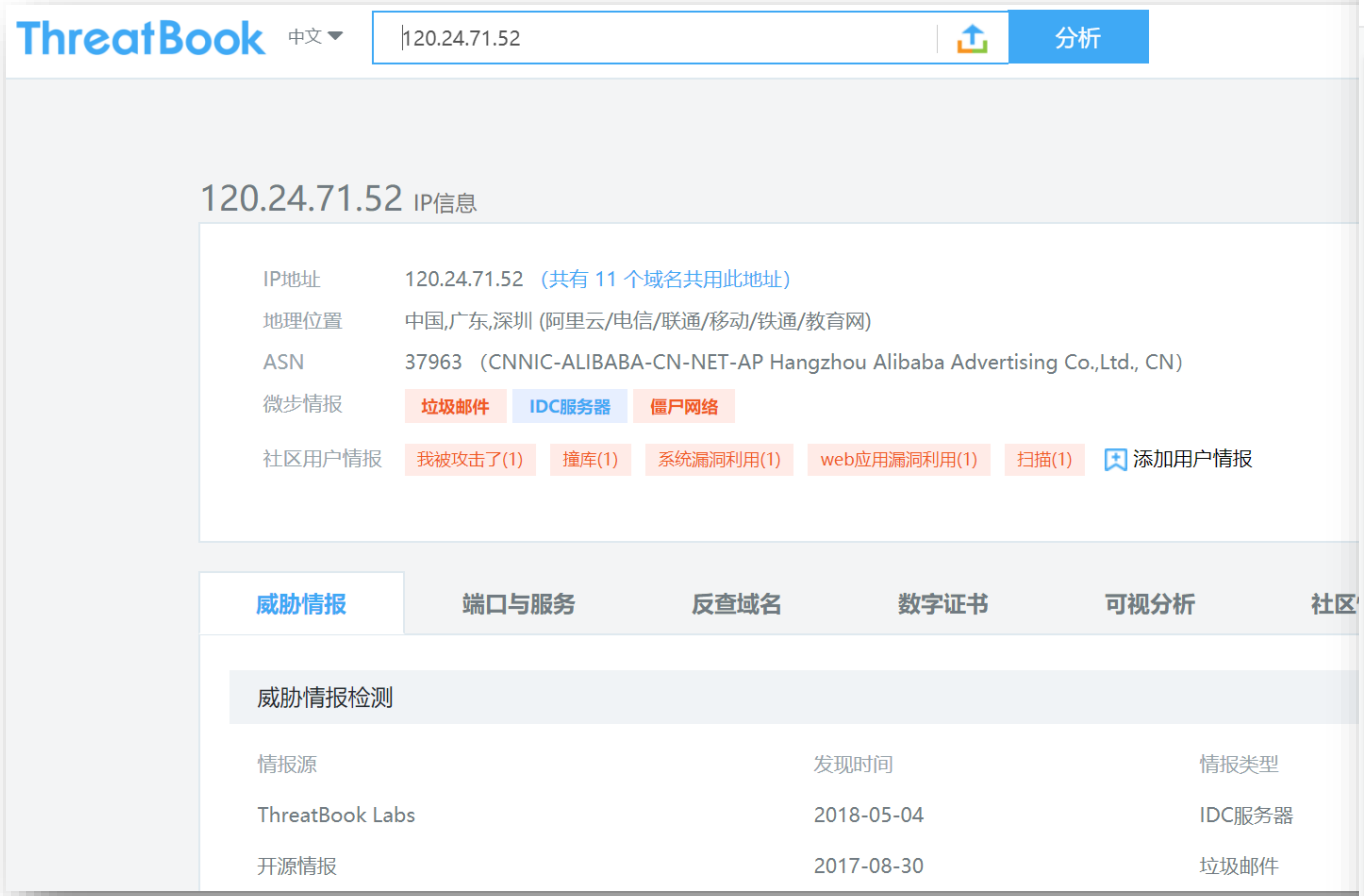
JIMR（攻击者） observer（攻击者） 192.168.100.141（域控）

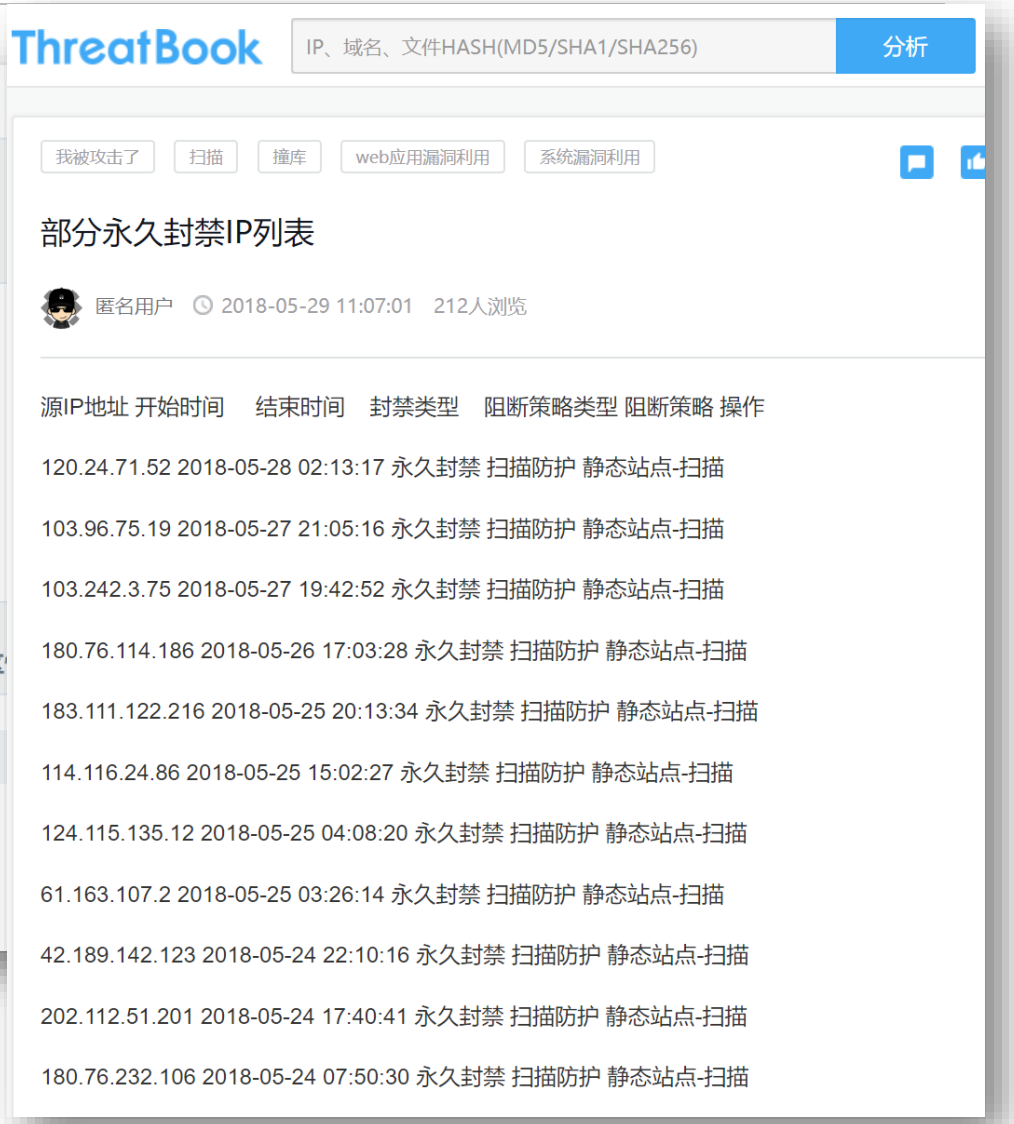
行为

Kerberos

内网主机: JIMR
用户名: observer
域控服务器: 192.168.100.141

情报共享


ThreatBook
中文
120.24.71.52
分析
120.24.71.52 IP信息
IP地址 120.24.71.52 （共有 11 个域名共用此地址）
地理位置 中国,广东,深圳 (阿里云/电信/联通/移动/铁通/教育网)
ASN 37963 （CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd., CN）
微步情报 垃圾邮件 IDC服务器 僵尸网络
社区用户情报 我被攻击了(1) 撞库(1) 系统漏洞利用(1) web应用漏洞利用(1) 扫描(1) 添加用户情报
威胁情报 端口与服务 反查域名 数字证书 可视分析 社区
威胁情报检测
情报源 发现时间 情报类型
ThreatBook Labs 2018-05-04 IDC服务器
开源情报 2017-08-30 垃圾邮件


ThreatBook
IP、域名、文件HASH(MD5/SHA1/SHA256)
分析
我被攻击了 扫描 撞库 web应用漏洞利用 系统漏洞利用
部分永久封禁IP列表
匿名用户 2018-05-29 11:07:01 212人浏览
源IP地址 开始时间 结束时间 封禁类型 阻断策略类型 阻断策略 操作
120.24.71.52 2018-05-28 02:13:17 永久封禁 扫描防护 静态站点-扫描
103.96.75.19 2018-05-27 21:05:16 永久封禁 扫描防护 静态站点-扫描
103.242.3.75 2018-05-27 19:42:52 永久封禁 扫描防护 静态站点-扫描
180.76.114.186 2018-05-26 17:03:28 永久封禁 扫描防护 静态站点-扫描
183.111.122.216 2018-05-25 20:13:34 永久封禁 扫描防护 静态站点-扫描
114.116.24.86 2018-05-25 15:02:27 永久封禁 扫描防护 静态站点-扫描
124.115.135.12 2018-05-25 04:08:20 永久封禁 扫描防护 静态站点-扫描
61.163.107.2 2018-05-25 03:26:14 永久封禁 扫描防护 静态站点-扫描
42.189.142.123 2018-05-24 22:10:16 永久封禁 扫描防护 静态站点-扫描
202.112.51.201 2018-05-24 17:40:41 永久封禁 扫描防护 静态站点-扫描
180.76.232.106 2018-05-24 07:50:30 永久封禁 扫描防护 静态站点-扫描

情报在防范、检测、响应与预测中的重要价值

预测 Predict

- 提供最新的攻击事件、攻击趋势与防护措施，帮助企业及时进行预先防御
- 自动化跟踪和掌握黑客动向

响应 Response

- 提供安全事件更多的外部攻击者信息，上下文，包括威胁类型、攻击者手法、意图等
- 自动化联动响应

防范 Prevent

- 攻击的拦截，如防火墙，OneDNS

检测 Detection

- 应用情报结合网络流量定位内部失陷主机，下载恶意软件、非法横向移动、数据泄露等

微步在线欢迎优秀的人才加盟