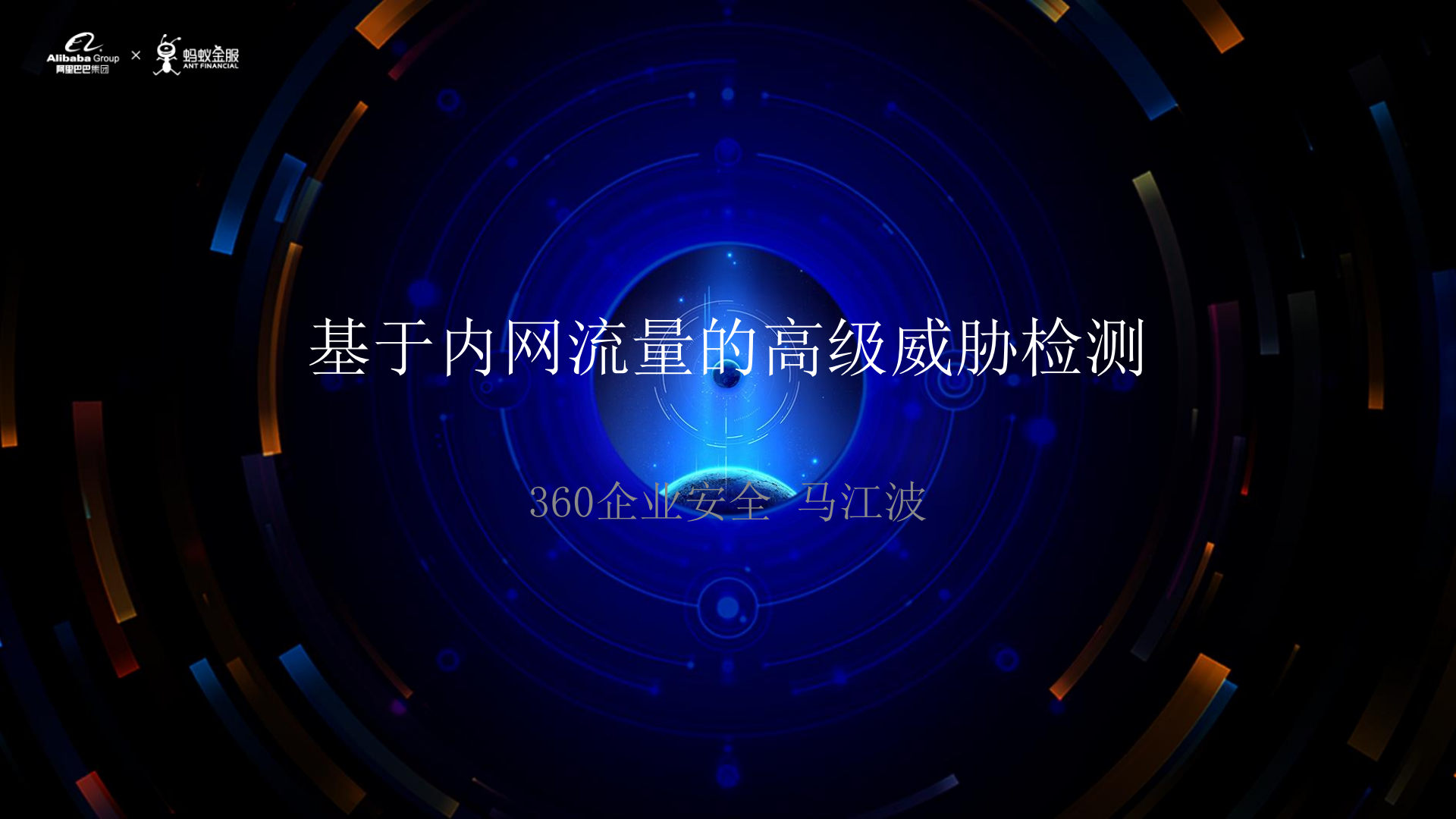


基于内网流量的高级威胁检测

360企业安全 马江波

『永恒之蓝』的回顾和思考

5月12日发生什么

受害主机中招后，病毒就会在受害主机中植入勒索程序，硬盘中存储的文件将会被加密无法读取，勒索蠕虫病毒将要求受害者支付价值300/600美元的比特币才能解锁，而且越往后可能要求的赎金越多，不能按时支付赎金的系统会被销毁数据

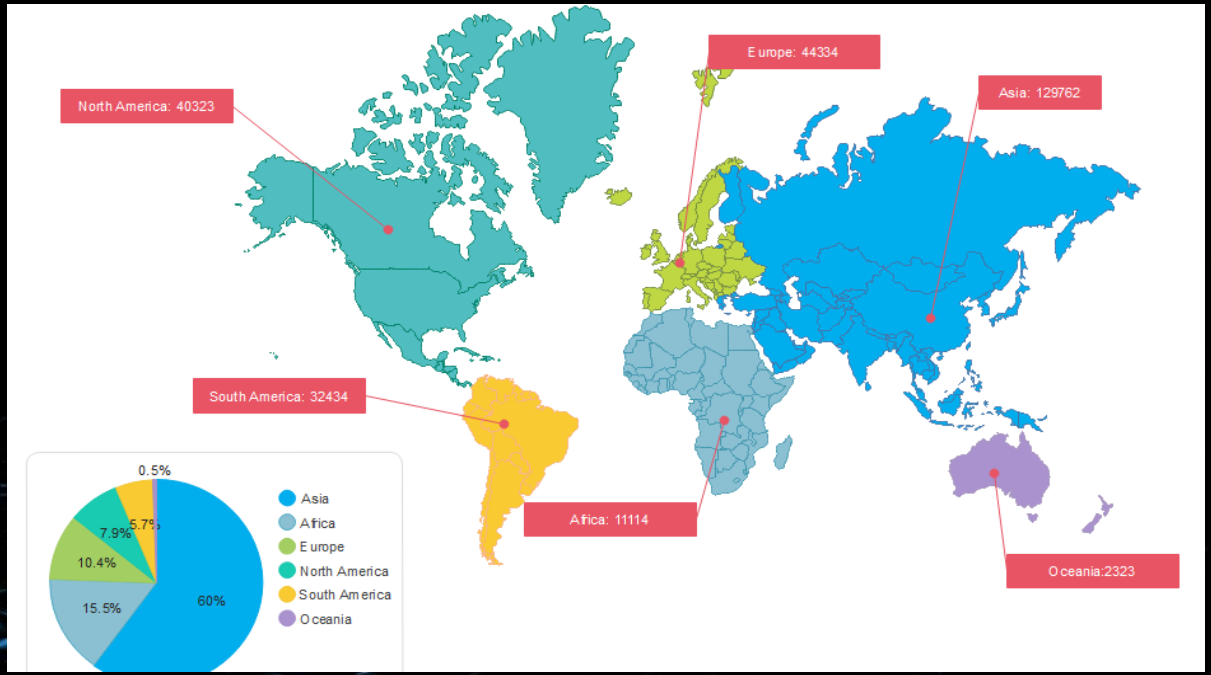
蠕虫不但破坏大量高价值数据，而且导致很多公共服务（教育、公安、加油站）

全球感染波及范围

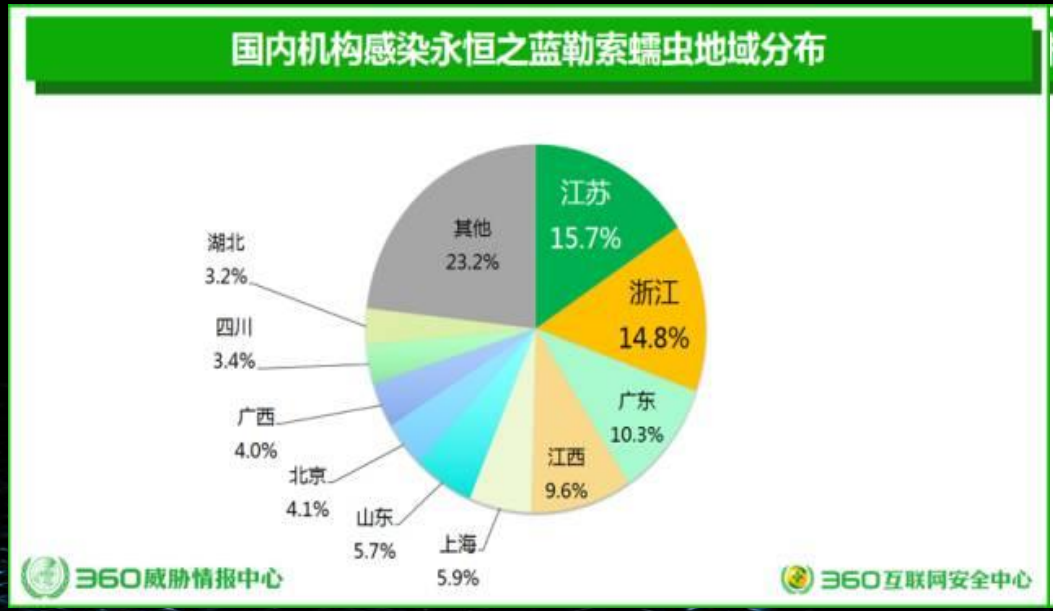
勒索软件已经攻击了99个国家，中国、英国、美国、德国、日本、土耳其、西班牙、意大利、葡萄牙、俄罗斯和乌克兰等国家的数千家企业及公共组织

至少1600家美国组织，11200家俄罗斯组织受到了攻击

中国感染范围覆盖了几乎所有地区，遍布高校、加油站、火车站、自助终端、邮政、医院、政府办事终端等各大领域，



中国境内感染情况统计



据360威胁情报中心监测，国内超30万台机器中招，至少有28388个机构被感染


乌鲁木齐
呼和浩特
银川
西宁
兰州
拉萨
昆明
沙
台北
香港
渤海
黄海
东海
6,000
5,000
4,000
3,000
2,000
1,000
0
17-05-12 15:00:00
2017-05-13 03:00:00
2017-05-13 15:00:00
2017-05-14 03:00:00
2017-05-14 15:00:00
2017-05-15 03:00:00
2017-05-15 15:00:00
2017-05-16 03:00:00

『永恒之蓝』对企业安全的新挑战

隔离网络安全

- 隔离网防护能力薄弱
- 没有建立网络监控和高级威胁检测能力

威胁情报体系建设不足

- 缺乏应对重大网络安全事件的情报应急响应系统
- 大部分企业还没有起威胁情报中心

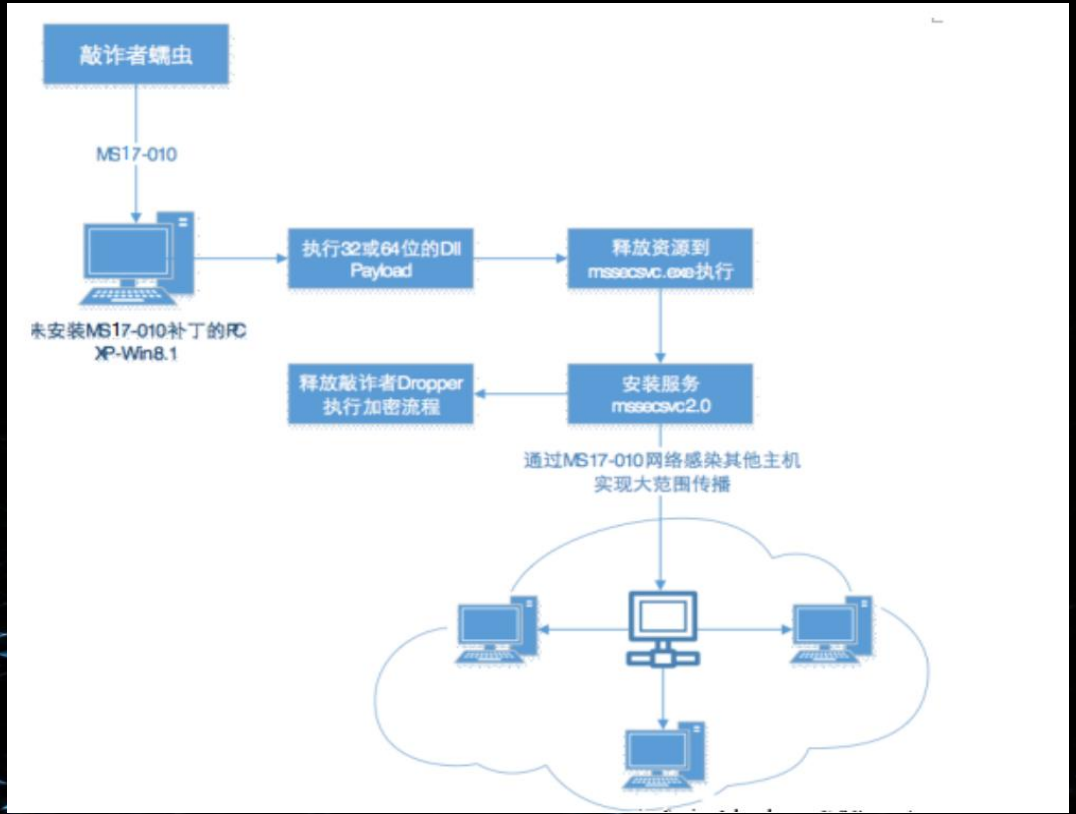
政策法规有待健全

- 缺乏对重点信息基础设施安全和用户隐私保护法规
- 政策和法规的实施有待加强

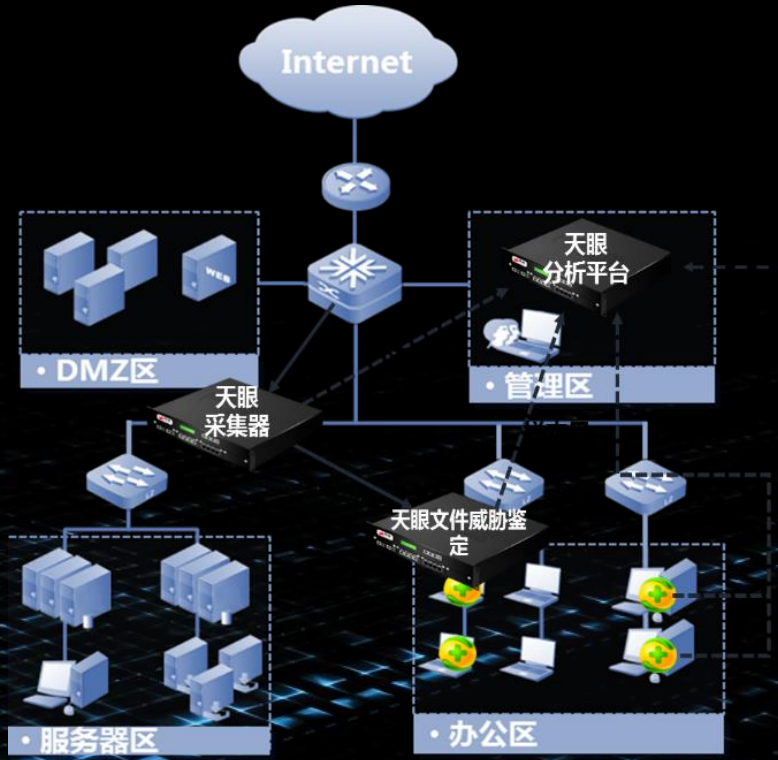
『永恒之蓝』的攻击检测

『永恒之蓝』的攻击分析

样本运行之后，首先访问 http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com 这个地址，如果访问成功则放弃之后的运行，否则进入蠕虫的主流程：
样本运行之后会对内网，外网 445 端口进行扫描之后，通过 MS17-010 漏洞上传并执行 payload 进行传播，之后释放 ransom 样本，ransom 执行初始化之后，再次释放对应的加密模块 ransommodule 对文件进行加密。



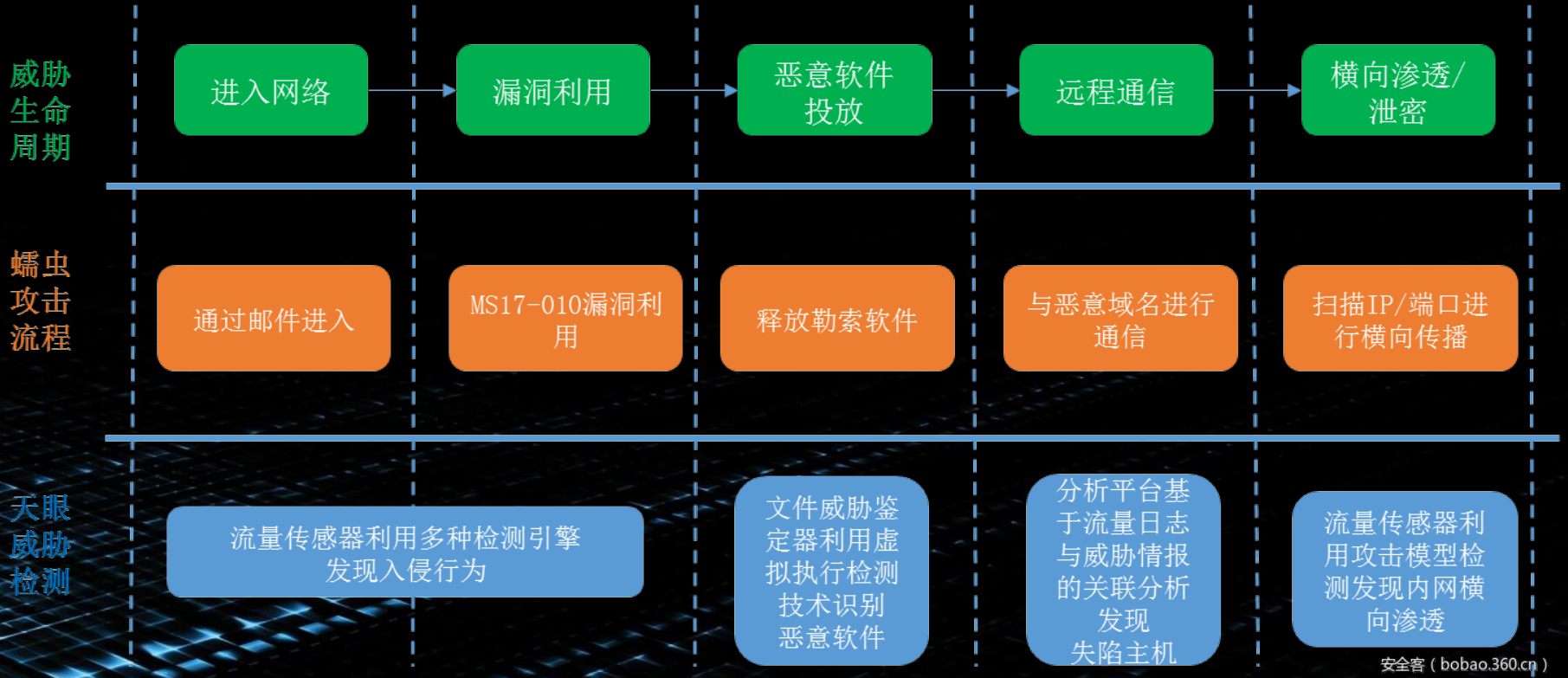
天眼如何对抗『永恒之蓝』



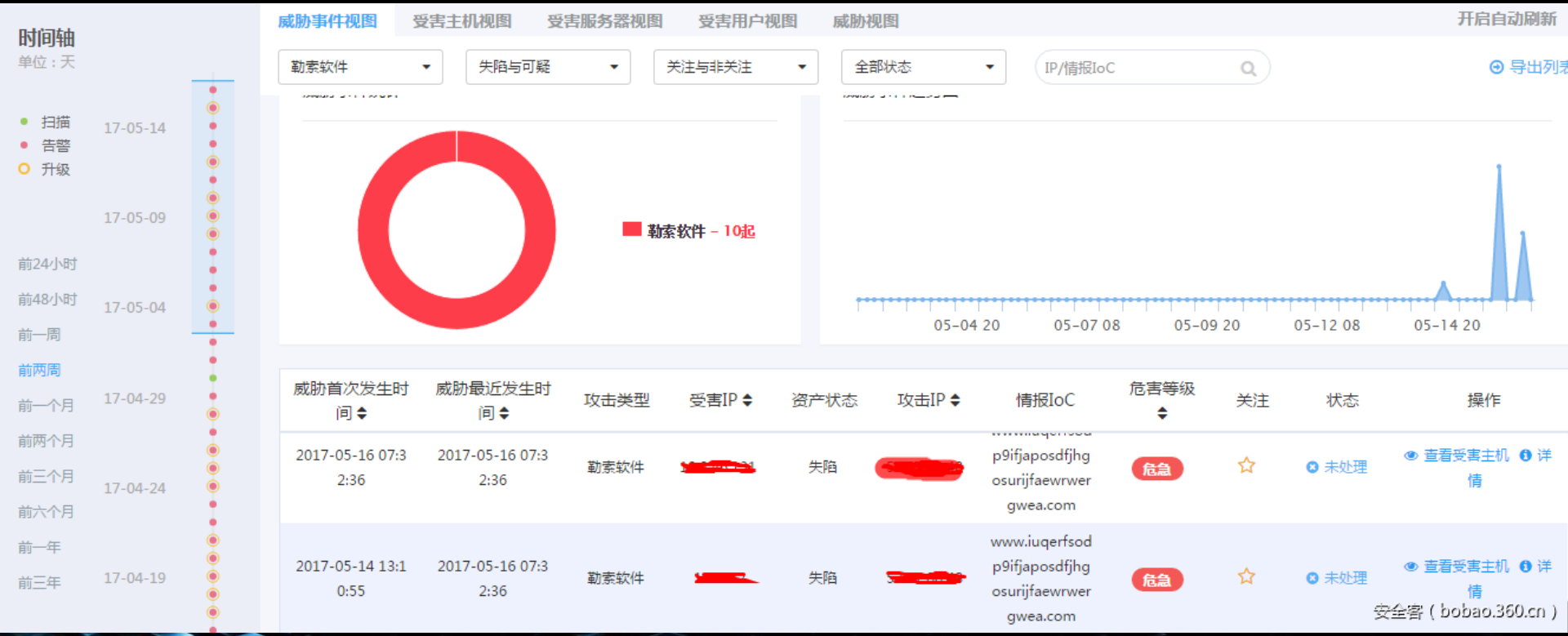
天眼

- 云端威胁情报
- 实时流量采集还原
- 文件威胁鉴定器
- 高级威胁分析平台

天眼如何对抗『永恒之蓝』

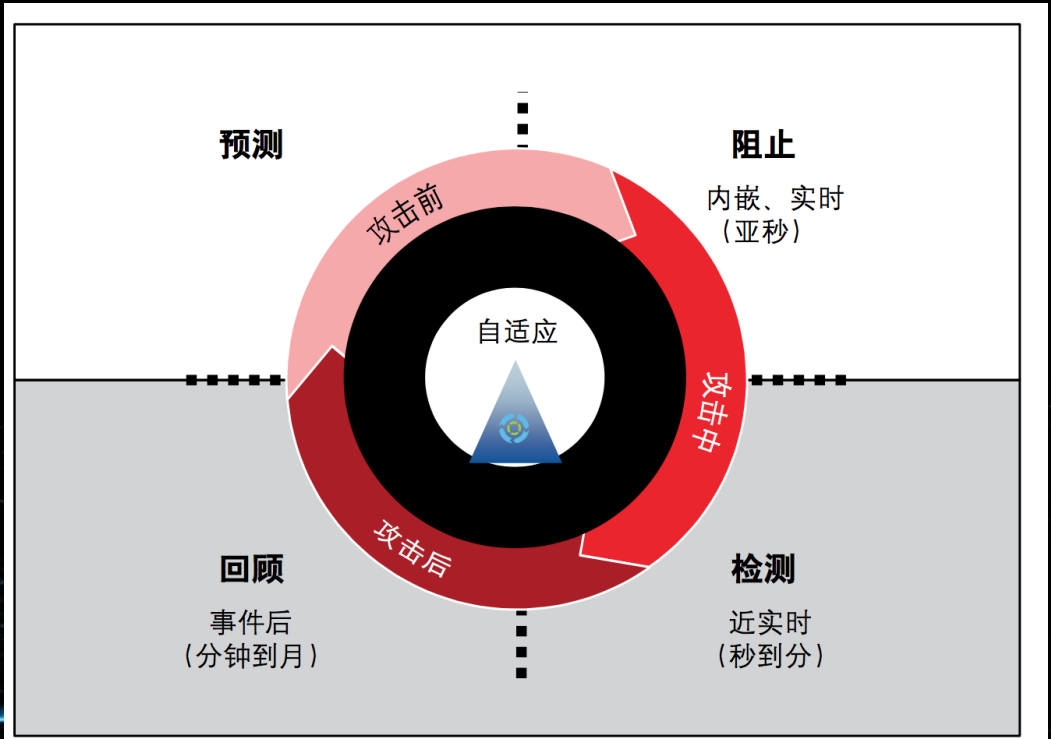


天眼如何对抗『永恒之蓝』


时间轴
单位：天
扫描
告警
升级
17-05-14
17-05-09
17-05-04
17-04-29
17-04-24
17-04-19
前24小时
前48小时
前一周
前两周
前一个月
前两个月
前三个月
前六个月
前一年
前三年
威胁事件视图
受害主机视图
受害服务器视图
受害用户视图
威胁视图
开启自动刷新
勒索软件
失陷与可疑
关注与非关注
全部状态
IP/情报IoC
导出列表
勒索软件 - 10起
05-04 20
05-07 08
05-09 20
05-12 08
05-14 20
威胁首次发生时间
威胁最近发生时间
攻击类型
受害IP
资产状态
攻击IP
情报IoC
危害等级
关注
状态
操作
2017-05-16 07:32:36
2017-05-16 07:32:36
勒索软件
失陷
p9ifjaposdfjhgosurijfaewrwergwea.com
危急
未处理
查看受害主机
详情
2017-05-14 13:10:55
2017-05-16 07:32:36
勒索软件
失陷
www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
危急
未处理
查看受害主机
详情
安全客（bobao.360.cn）

高级威胁检测的参考模型

Gartner设计自适应安全构架



来源：Gartner（2014 年 2 月）

高级威胁检测技术发展历程

文件沙箱

2012年 Fireeye提出全球第一款沙箱；

从本地沙箱发展为云沙箱；

威胁情报

2014年威胁情报已经成为应对高级威胁有效；

2015年360提出国内第一威胁情报中心；

2018年全球60%的大型企业将使用威胁情报；

行为分析和人工智能

网络流量行为分析 – NTA

终端行为分析 – EDR

用户行为分析 – UEBA

新型分析技术

现有检测技术

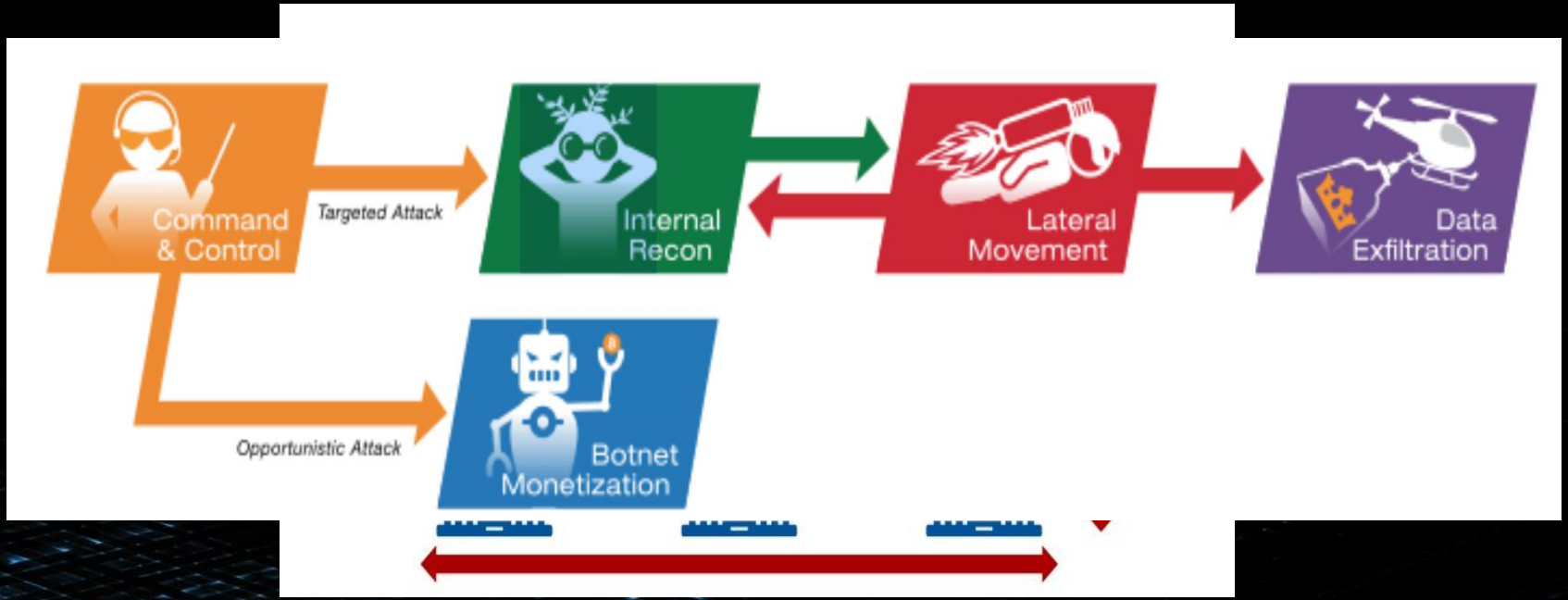
- SIEM Monitoring
- Intrusion Detection/Protection
- Data Loss Prevention
- Identity Access Management
- Anti-Malware Protection

新型分析技术

- UEBA Analytics
- Network Traffic Analytics
- Endpoint Detection and Response

内网威胁检测的新趋势

网络行为分析



基于南北向和东西向流量，依据KILL CHAIN建立网络异常行为的检测模型

用户行为分析

特征计算

机器学习

账号失陷

主机失陷

数据泄露

内部用户滥用

事件调查上下文

攻击链检测模型

CKC阶段	攻击行为及特征
侦察	主机扫描、端口扫描、漏洞扫描
投递	邮件投递、网站钓鱼、及时通信、社工
横向移动	应用部署软件、漏洞利用、登录脚本、域渗透、暴力破解、
C&C通信	DNS隧道、ICMP隧道、HTTP隧道、未知通道、地理位置、通信模型
数据外泄	加密信道、FTP/SMTP/HTTP(S)/DNS、地理位置、未知协议、上下行数据比

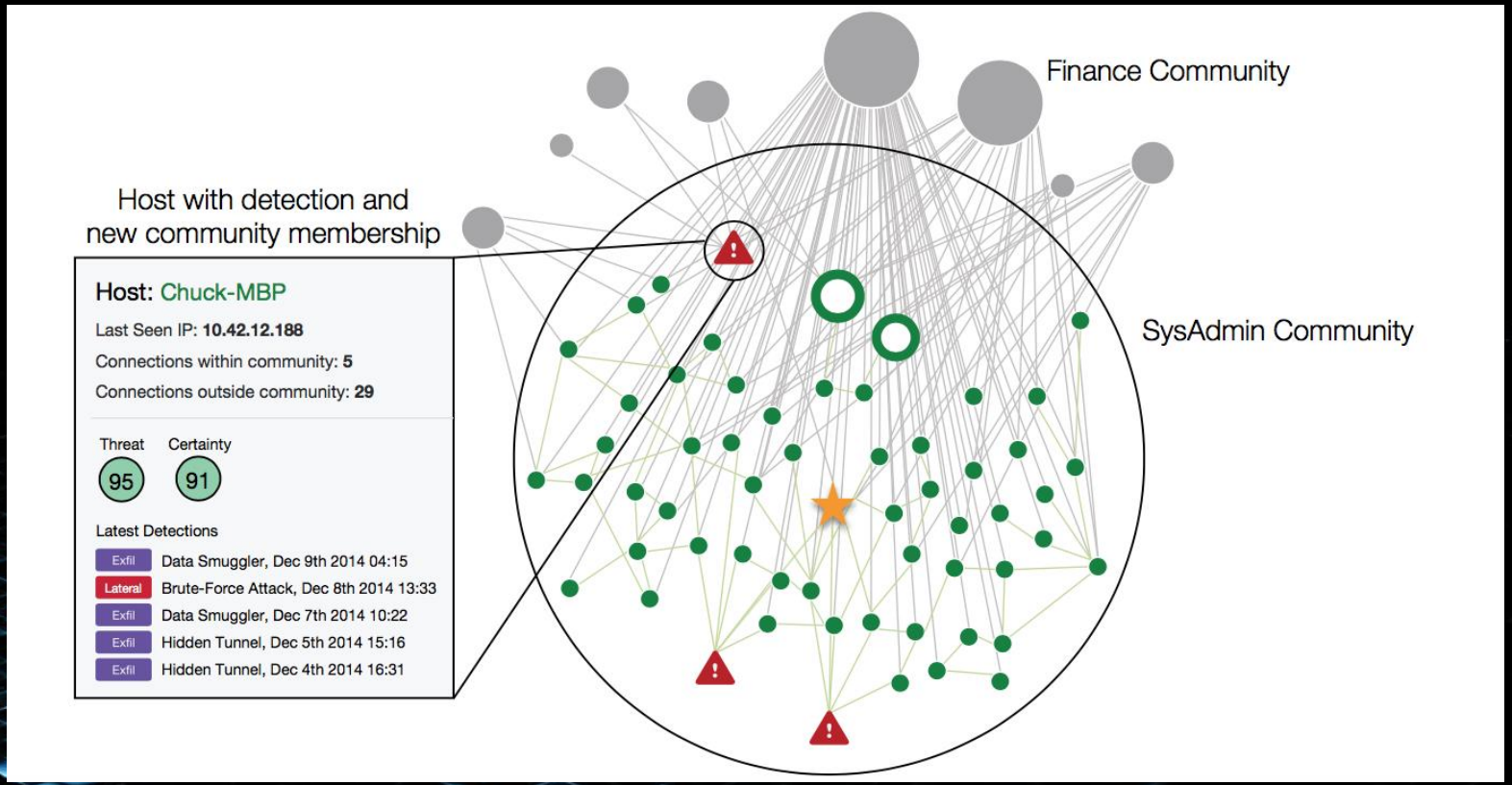
APT28分析案例

CKC阶段	攻击行为及特征	检测
投递	邮件投递	文件沙箱
横向移动	漏洞利用	终端检测响应
C&C通信	DNS域名解析、HTTP通信	伪造域名分析
数据外泄	SMTP、HTTP通信	高级流量分析

APT28分析案例

novinitie.com, n0vinite.com => novinite.com
q0v.pl, mail.q0v.pl => mail.gov.pl
natoexhibitionff14.com => nationexhibition.org

关键资产的流量模型


Finance Community
SysAdmin Community
Host with detection and
new community membership
Host: Chuck-MBP
Last Seen IP: 10.42.12.188
Connections within community: 5
Connections outside community: 29
Threat
Certainty
95
91
Latest Detections
Exfil
Data Smuggler, Dec 9th 2014 04:15
Lateral
Brute-Force Attack, Dec 8th 2014 13:33
Exfil
Data Smuggler, Dec 7th 2014 10:22
Exfil
Hidden Tunnel, Dec 5th 2014 15:16
Exfil
Hidden Tunnel, Dec 4th 2014 16:31

几家国外创新公司

作为企业免疫系统，Darktrace以人工智能运算程序自动部署于各个网络，包括实体网络、云端网络、虚拟网络、物联网及工业控制系统，探测威胁并作出响应。

自动化的异常行为分析的领先公司，使用先进的机器学习的快速、高效、准确地识别基于识别行为异常的内部网络攻击。

自动化的威胁发现企业网络中攻击行为”和“手动消除威胁狩猎将相关信息直接到用户

Thank you