# 高级威胁的新动态

## —— 永恒之蓝引起的思考

2017/06

360企业安全 马江波

360企业安全 安全第一® 企业安全领导者

**目录**

# 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、重要业务无法正常开展



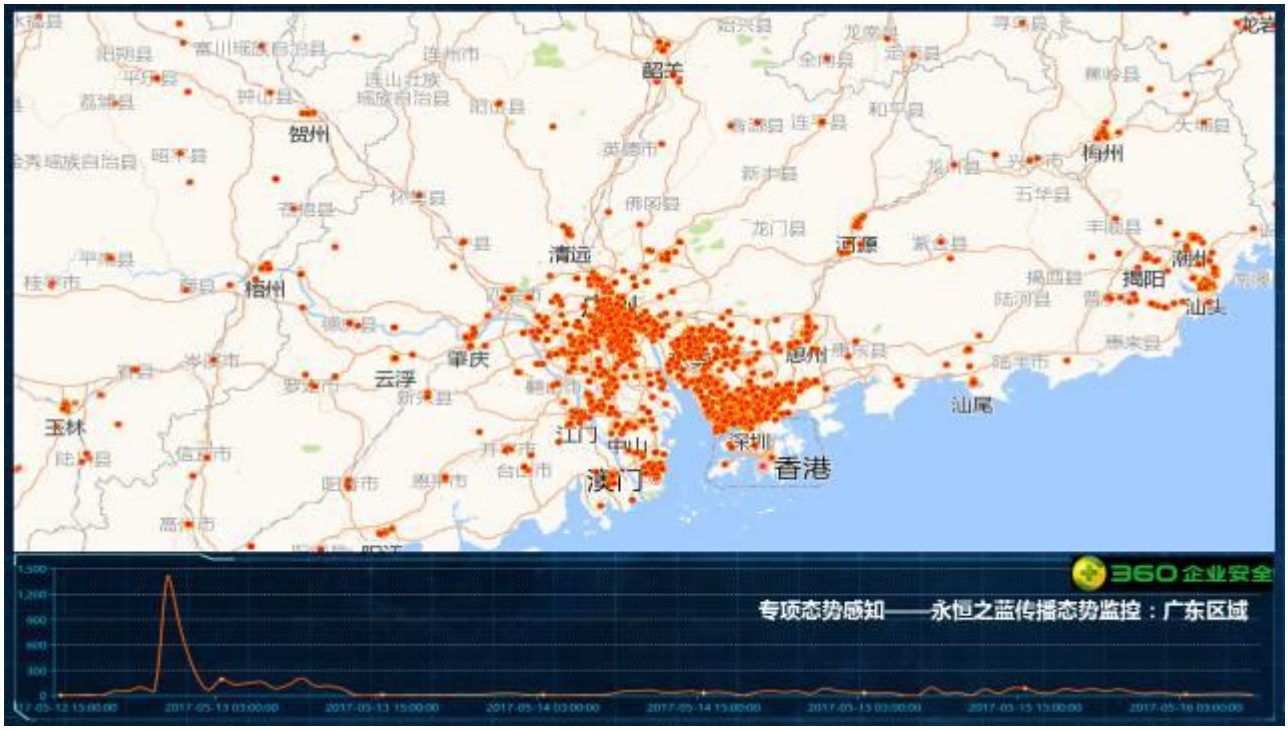

# 全球感染波及范围

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，目前攻击事态仍在蔓延，被感染的电脑数字还在不断增长中


360 企业安全
专项态势感知——永恒之蓝传播态势监控：中国


韶关
贺州
梅州
清远
梧州
肇庆
云浮
玉林
江门
中山
深圳
香港
澳门
汕尾
揭阳
潮州
汕头
360 企业安全
专项态势感知——永恒之蓝传播态势监控：广东区域

# 勒索攻击还将常伴我们左右

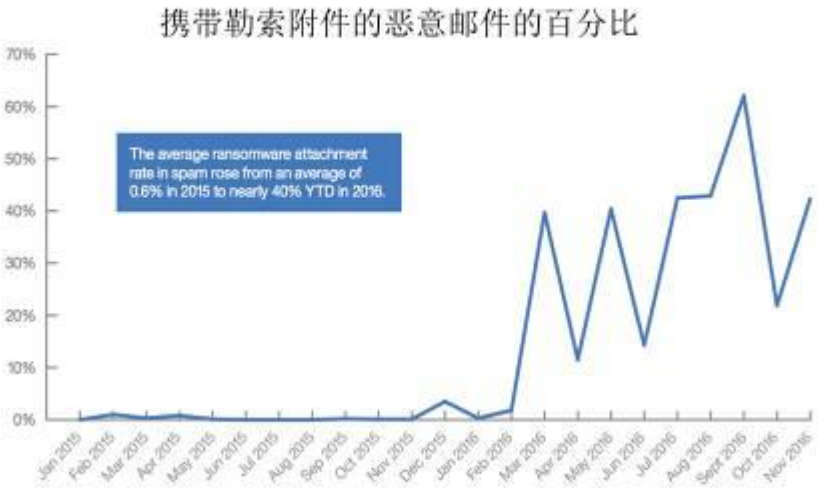


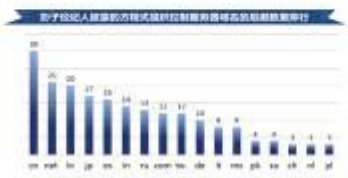

**Figure 1.** Source: IBM X-Force, 2016

# 永恒之蓝悄悄走了，让我们却陷入沉思...

# WannaCry事件发生的时间轴


# 『NSA武器』+『高级勒索』


Theshadowbrokers——影子经纪人
2016年8月13日，首度公开方程式组织部分工具



影响微软产品的漏洞攻击工具一共12个：

1. EternalBlue（永恒之蓝）：SMBv1漏洞攻击工具
2. EmeraldThread（翡翠纤维）：SMBv1漏洞攻击工具
3. EternalChampion（永恒王者）：SMBv1漏洞攻击工具
4. ErraticGopher（古怪地鼠）：SMB漏洞攻击工具
5. EskimoRoll（爱斯基摩卷）：Kerberos漏洞攻击工具
6. EternalRomance（永恒浪漫）：SMBv1漏洞攻击工具
7. EducatedScholar（文雅学者）：SMB漏洞攻击工具
8. EternalSynergy（永恒增效）：SMBv3漏洞攻击工具
9. EclipsedWing（日食之翼）：Server netAPI漏洞攻击工具
10. EnglishManDentist（英国牙医）：针对Exchange Server的远程攻击工具
11. EsteemAudit（尊重审计）：针对XP/2003的RDP远程攻击工具
12. ExplodingCan（爆炸罐头）：针对2003 IIS6.0的远程攻击工具

其他受影响产品和对应工具5个：

EasyBee（轻松蜂）：MDaemon邮件服务器系统
EasyPi（轻松派）：Lotus Notes
EwokFrenzy（狂暴伊沃克）：Lotus Domino 6.5.4~7.0.2
EmphasisMine（说重点）：IBM Lotus Domino的IMAP漏洞
ETRE：IMail 8.10~8.22远程利用工具

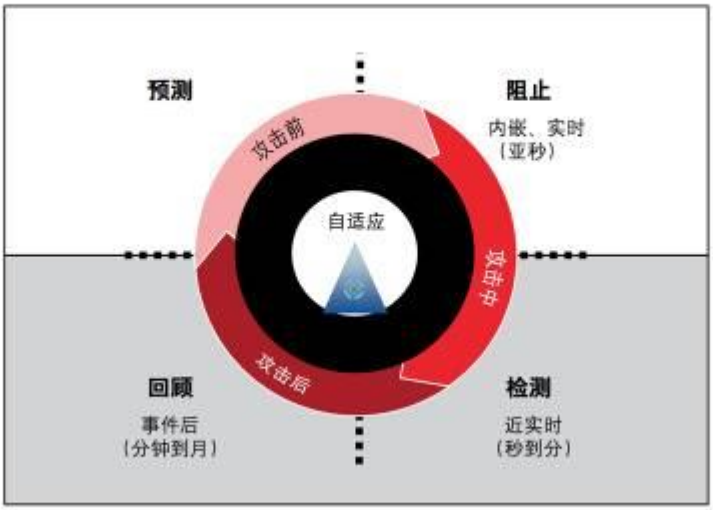
## 英雄也无法挽救隔离网

www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

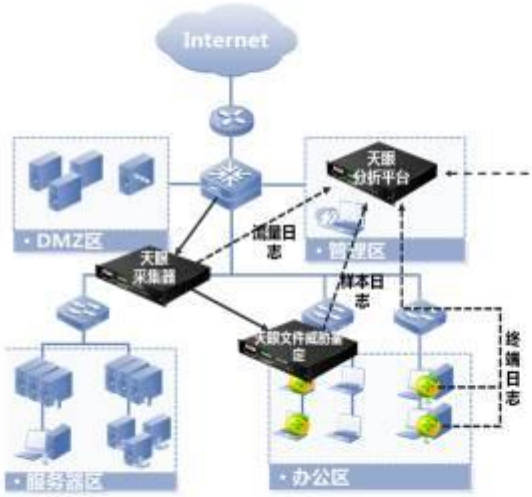

## 目录

# Gartner设计自适应安全构架



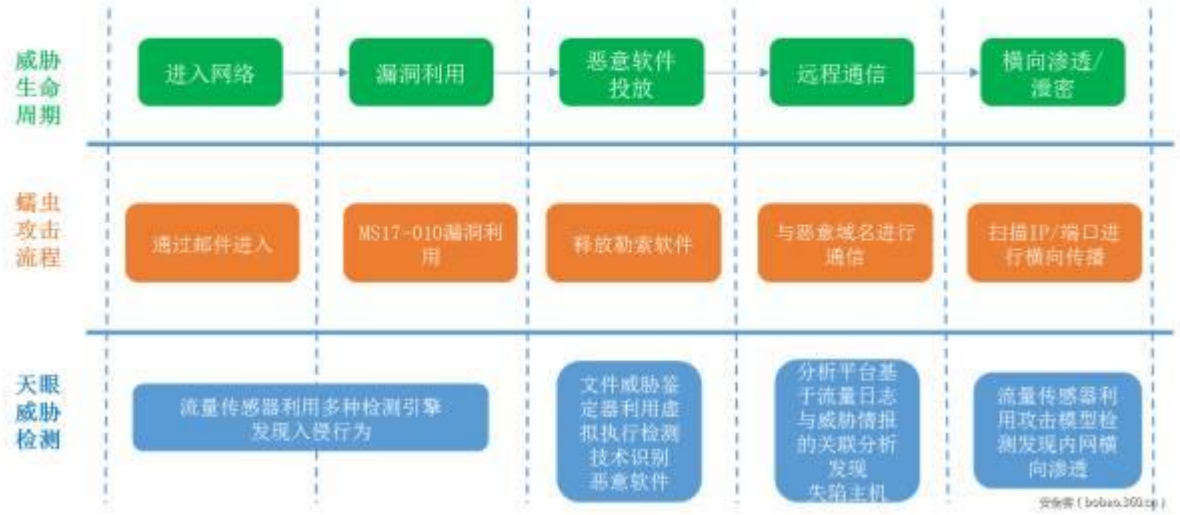

来源：Gartner（2014 年 2 月）

# 360天眼新一代威胁感知系统




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”




# 天眼的检测结果

## 360天眼推NSA武器库专查工具

天眼临检版提出**NSA**武器库专查功能，主要包括：

- 『永恒之蓝』专查
- **NSA**武器库特征的情报流量行为检测
- 主动扫描和被动探测发现已经失陷和潜在的失陷主机；

快速发现

运用威胁情报技术，快速发现高级针对性网络攻击

机器学习

有机结合机器学习技术和异常行为检测技术，发现未知攻击和0day攻击

回溯取证

完整保存网络流量数据，帮助客户进行原始数据取证和回溯

便携式设计

便携式设计，且具备高速海量存储能力

## 目录

# 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；

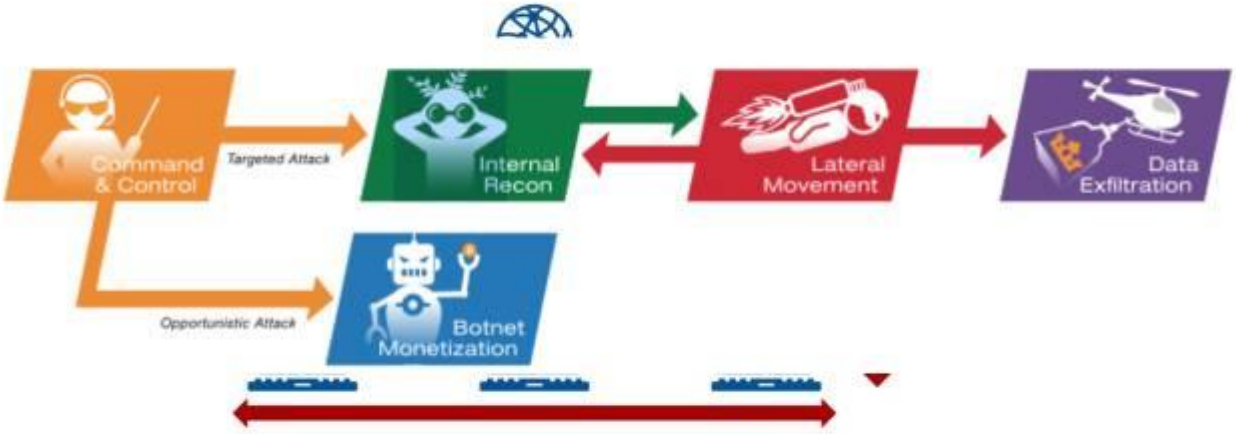
### 威胁情报

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

# 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


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

## 目录

## 『永恒之蓝』对企业安全的新挑战

### 隔离网络安全

- 无法提供情报服务和防护的自动化升级
- 无法提供自动化的在线应急响应服务

### 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

### 政策和法规有待健全

- 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
- 企业在信息安全方面的投入严重不足

## 新政策积极应对高级攻击


◆ 要健全和完善国家信息安全等级保护制度

◆ 强化关键信息基础设施保护

◆ 将监测预警与应急处置措施制度化、法制化

# 『等保2.0』积极应对高级攻击

《网络安全等级保护基本要求 第1部分：安全通用要求》

第七章“第三级安全要求”中明确提出：”实现对网络攻击特别是未知的新型网络攻击的检测和分析

7.1.2.5 入侵防范

本项要求包括：

a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；

b) 应在关键网络节点处检测和限制从内部发起的网络攻击行为；

c) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是未知的新型网络攻击的检测和分析；

d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

# 『等保2.0』积极应对高级攻击

《网络安全等级保护测评要求 第1部分：安全通用要求》

在第7章中的等保三级的测评对象涵盖抗APT攻击的系统或设备

7.1.2.5 入侵防范

7.1.2.5.1 测评单元（L3-NCS1-17）

a) 测评指标

应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；（本条款引用自 GB/T 22239.1-20XX 7.1.2.5 a））

b) 测评对象

入侵保护系统、入侵检测系统、抗 APT 攻击、抗 DDoS 攻击和网络回溯等系统或设备。

# 360抗击勒索蠕虫 72小时


**从5月12日下午三点开始**，360企业安全针对该勒索病毒的事件响应超过了**72小时**，取得了阶段性的胜利！

72小时内，我们为政企客户及时推送了**8个版本的预警通告**，提供了**7份修复指南文档**，制作了**6个软件工具**，帮助各类机构和个人快速响应和修复提供了指引。

72小时内，我们**出动了近千人**，提供了**上万次上门支持服务**，接听了**两万多次的电话咨询**，还制作了**近千个U盘和光盘**发放到客户手上，甚至**手把手教会客户应急**，取得了多个行业客户的高度认同。

72小时内，我们通过媒体发布了**45篇新闻稿件**，接受了**33次媒体采访**，获得了整个社会和行业客户的关注和认同。

# 360 天擎敲诈先赔 2016年底开始提供

**360 天擎敲诈先赔是 360 天擎针对敲诈者病毒，向企业用户免费提供的专属服务。**
**并郑重承诺：在企业用户开启 360 天擎敲诈先赔功能后，如果 360 天擎仍无法防护，感染了敲诈者 病毒，360 天擎负责赔付赎金，并帮助用户恢复数据**



- ✓ ***每终端企业用户上限￥1万元人民币或者3个比特币。***
- ✓ ***每企业用户上限金额￥100万元人民币或者 200个比特币***

*服务协议：http://b.360.cn/special/agreement/agreement.html*
*配置指南：http://b.360.cn/special/agreement/guide.html*


谢 谢
360 企业安全 安全第一 企 业 安 全 领 导 者