清华大学出版社
TSINGHUA UNIVERSITY PRESS

勒索型恶意代码

刘功申
上海交通大学网络空间安全学院
2019.03.20

本章内容

- 概念及背景知识
- 勒索型恶意软件的原理
- 勒索型恶意软件示例
- 勒索型恶意软件防范

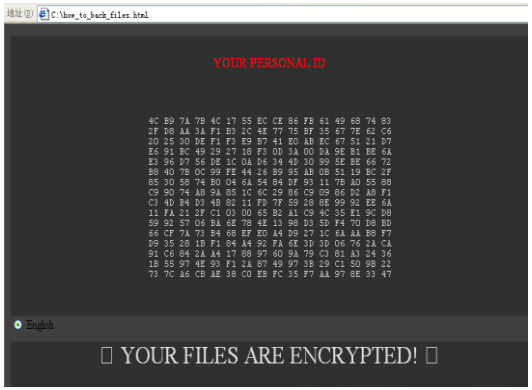
清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

勒索型恶意软件的概念

什么是勒索病毒？

主机感染勒索病毒文件后，会在主机上运行勒索程序，**遍历本地所有磁盘指定类型文件进行加密操作**，加密后文件无法读取。然后生成勒索通知，要求受害者在规定时间内支付一定价值的比特币才能恢复数据，否则会被销毁数据。



WannaCry勒索病毒

2017年5月12日WannaCry在全球爆发，勒索病毒使用MS17-010永恒之蓝漏洞进行传播感染。短时间内感染全球30w+用户，包括学校、医疗、政府等各个领域

GlobeImposter勒索病毒

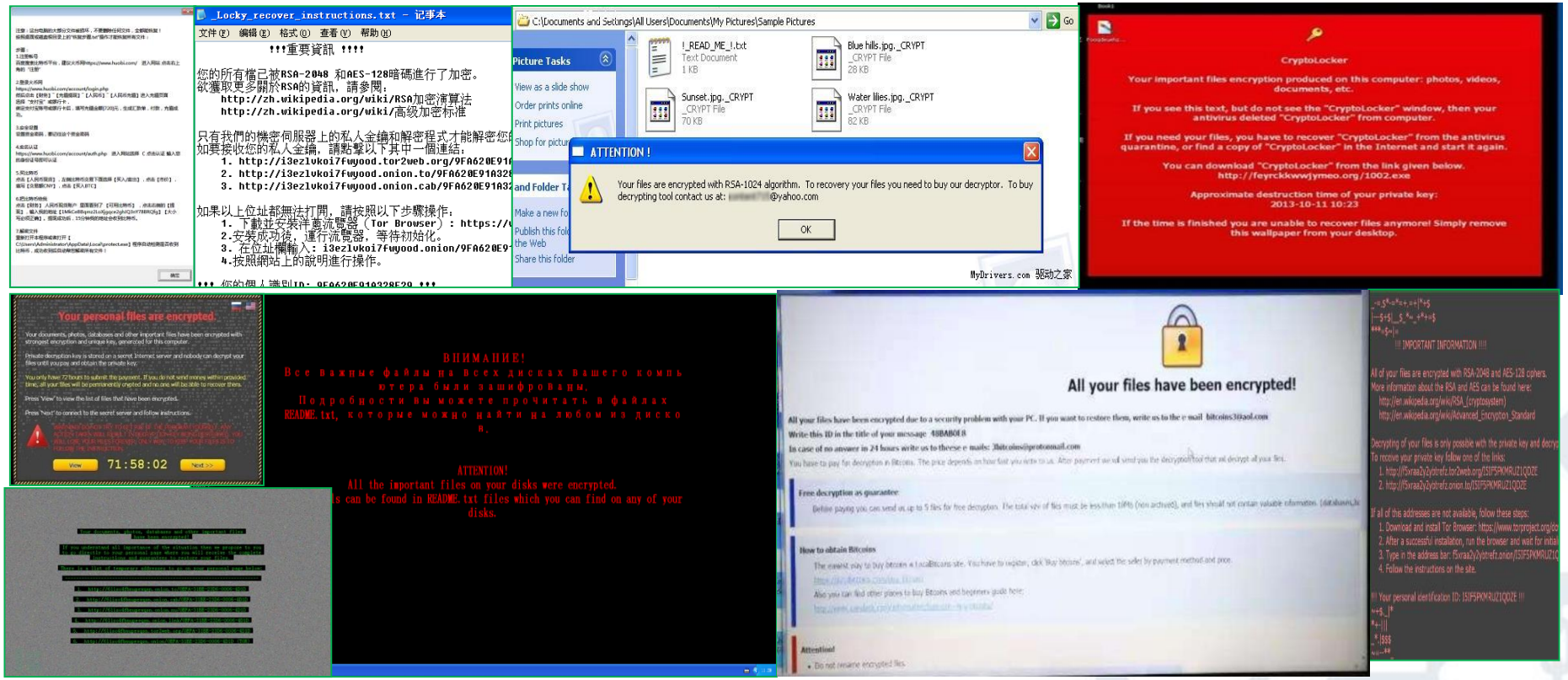
首次出现在2017年5月，主要钓鱼邮件传播，期间出现多种变种会利用RDP进行传播 。2018年2月中旬新年开工之际**GlobeImposter**变种再度来袭。

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

受害者勒索界面

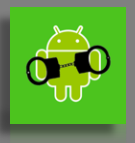


勒索病毒的发展和进化

AIDS木马
世界首例勒索病毒

Archievus木马
首次采用非对称加密

LockerPin
首例安卓勒索软件



WannaCry
军用级漏洞利用

利用机器学习
物联网设备
……

1989
无特定目标
勒索手段粗糙

2006
针对特定目标
难以解密、追踪
15年损失约3.15亿美元

2015

2017
大规模破坏
损失2年增长15倍
勒索即服务（RaaS）
市场规模年增长 25 倍

2019
每14秒一次勒索攻击
病毒数量指数级增加
损失将达到115亿美元

计算机感染案例

无孔不入的感染

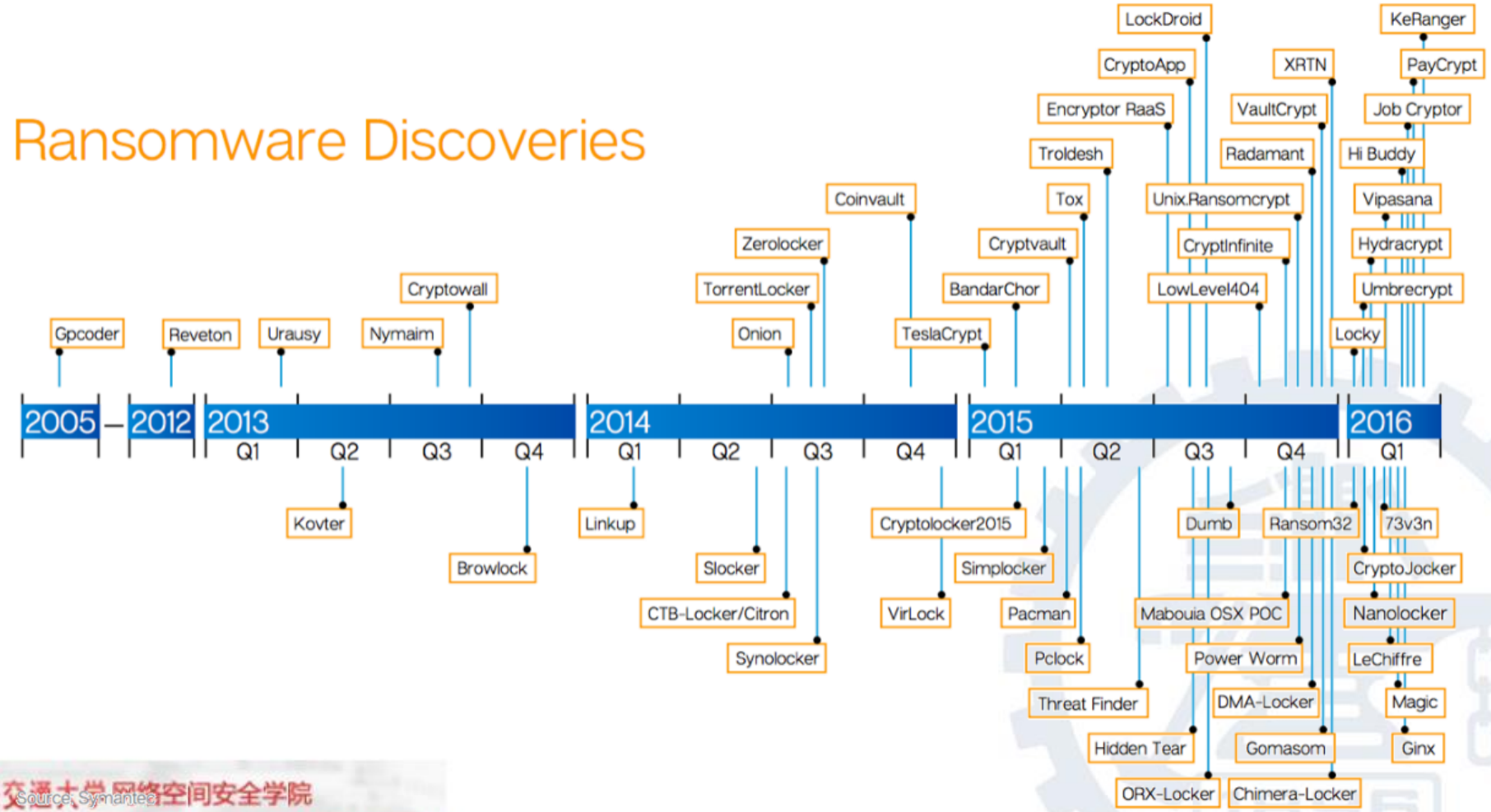
全球主流的敲诈者病毒家族（类型）有75种之多

7ev3n	CryptoJoker	KimcilWare	Radamant
8lock8	CryptoMix	Kriptovo	RemindMe
Alpha	CryptoTorLocker	KryptoLocker	Rokku
AutoLocky	CryptoWall	LeChiffre	Samas
BitCryptor	CryptXXX	Locky	Sanction
BitMessage	CrySiS	Lortok	Shade
Booyah	CTB-Locker	Magic	Shujin
Brazilian Ransomware	DMA Locker	Maktub Locker	SNSLocker
BuyUnlockCode	ECLR Ransomware	MireWare	SuperCrypt
Cerber	EnCiPhErEd	Mischa	Surprise
Chimera	Enigma	Mobef	TeslaCrypt
CoinVault	GhostCrypt	NanoLocker	TrueCrypter
Coverton	GNL Locker	Nemucod	UmbreCrypt
Crypren	Hi Buddy!	Nemucod-7z	VaultCrypt
Crypt0L0cker	HydraCrypt	OMG! Ransomcrypt	Virlocker
CryptoDefense	Jigsaw	PadCrypt	WonderCrypter
CryptoFortress	JobCrypter	PClock	Xort
CryptoHasYou	KeRanger	PowerWare	XTBL
CryptoHitman	KEYHolder	Protected Ransomware	

200个加密型的RansomWare

CryptoHasYou., 777, 7ev3n, 7h9r, 8lock8, **Alfa Ransomware**, **Alma Ransomware**, Alpha Ransomware, AMBA, Apocalypse, ApocalypseVM, AutoLocky, BadBlock, BaksoCrypt, Bandarchor, Bart, BitCryptor, BitStak, BlackShades Crypter, Blocatto, Booyah, Brazilian, BrLock, Browlock, Bucbi, BuyUnlockCode, Cerber, Chimera, CoinVault, Coverton, Cryaki, Crybola, CryFile, CryLocker, **CrypMIC**, Crypren, Crypt38, Cryptear, **CryptFile2**, CryptInfinite, CryptoBit, CryptoDefense, CryptoFinancial, CryptoFortress, CryptoGraphic Locker, CryptoHost, CryptoJoker, **CryptoLocker**, Cryptolocker 2.0, CryptoMix, CryptoRoger, CryptoShocker, CryptoTorLocker2015, CryptoWall 1, CryptoWall 2, CryptoWall 3, CryptoWall 4, CryptXXX, CryptXXX 2.0, CryptXXX 3.0, **CryptXXX 3.1**, CTB-Faker, **CTB-Locker**, CTB-Locker WEB, CuteRansomware, DeCrypt Protect, DEDCryptor, DetoxCrypto, DirtyDecrypt, DMALocker, DMALocker 3.0, Domino, EDA2 / HiddenTear, EduCrypt, El-Polocker, Enigma, FairWare, Fakben, Fantom, Fonco, Fsociety, Fury, GhostCrypt, Globe, GNL Locker, Gomasom, Goopic, Gopher, Harasom, Herbst, Hi Buddy!, Hitler, HolyCrypt, HydraCrypt, iLock, iLockLight, International Police Association, JagerDecryptor, Jeiphoos, Jigsaw, Job Crypter, **KeRanger**, KeyBTC, KEYHolder, KimcilWare, Korean, Kozy.Jozy, KratosCrypt, KryptoLocker, LeChiffre, Linux.Encoder, Locker, **Locky**, Lortok, LowLevel04, Mabouia, Magic, MaktubLocker, MIRCOP, MireWare, Mischa, MM Locker, Mobef, NanoLocker, Nemucod, NoobCrypt, Nullbyte, ODCODC, Offline ransomware, OMG! Ransomware, Operation Global III, PadCrypt, Pclock, **Petya**, PizzaCrypts, PokemonGO, PowerWare, PowerWorm, PRISM, R980, RAA encryptor, Radamant, Rakhni,, Rannoh, Ransom32, RansomLock, Rector, RektLocker, RemindMe, Rokku, Samas-Samsam, Sanction, Satana, Scraper, Serpico, Shark, ShinoLocker, Shujin, Simple_Encoder, SkidLocker / Pompous, Smrss32, SNSLocker, Sport, Stampado, Strictor, Surprise, SynoLocker, SZFLocker, TeslaCrypt 0.x - 2.2.0, TeslaCrypt 3.0+, TeslaCrypt 4.1A, TeslaCrypt 4.2, Threat Finder, **TorrentLocker**, TowerWeb, Toxcrypt, Troldesh, TrueCrypter, Turkish Ransom, UmbreCrypt, Ungluk, Unlock92, VaultCrypt, VenusLocker, Virlock, Virus-Encoder, WildFire Locker, Xorist, XRTN, Zcrypt, **Zepto**, Zimbra, Zlader / Russian, Zyklon

RansomWare上升趋势



Source: Symantec

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

勒索型恶意软件原理

上海交通大学 网络空间安全学院
School Of Cyber Security,ShanghaiJiao Tong University

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

勒索病毒常见传播方式

勒索病毒传播需要植入到受害者主机的常见四种方式

钓鱼邮件

恶意代码伪装在邮件附件中，诱使打开附件

典型案例：Locky、Petya变种

主要对象：个人PC

蠕虫式传播

通过漏洞和口令进行网络空间中的蠕虫式传播

典型案例：WannaCry、Petya变种

主要对象无定向，自动传播都有可能

Exploit Kit分发

通过黑色产业链中的Exploit Kit来分发勒索软件

典型案例：Cerber

主要对象：有漏洞的业务Server

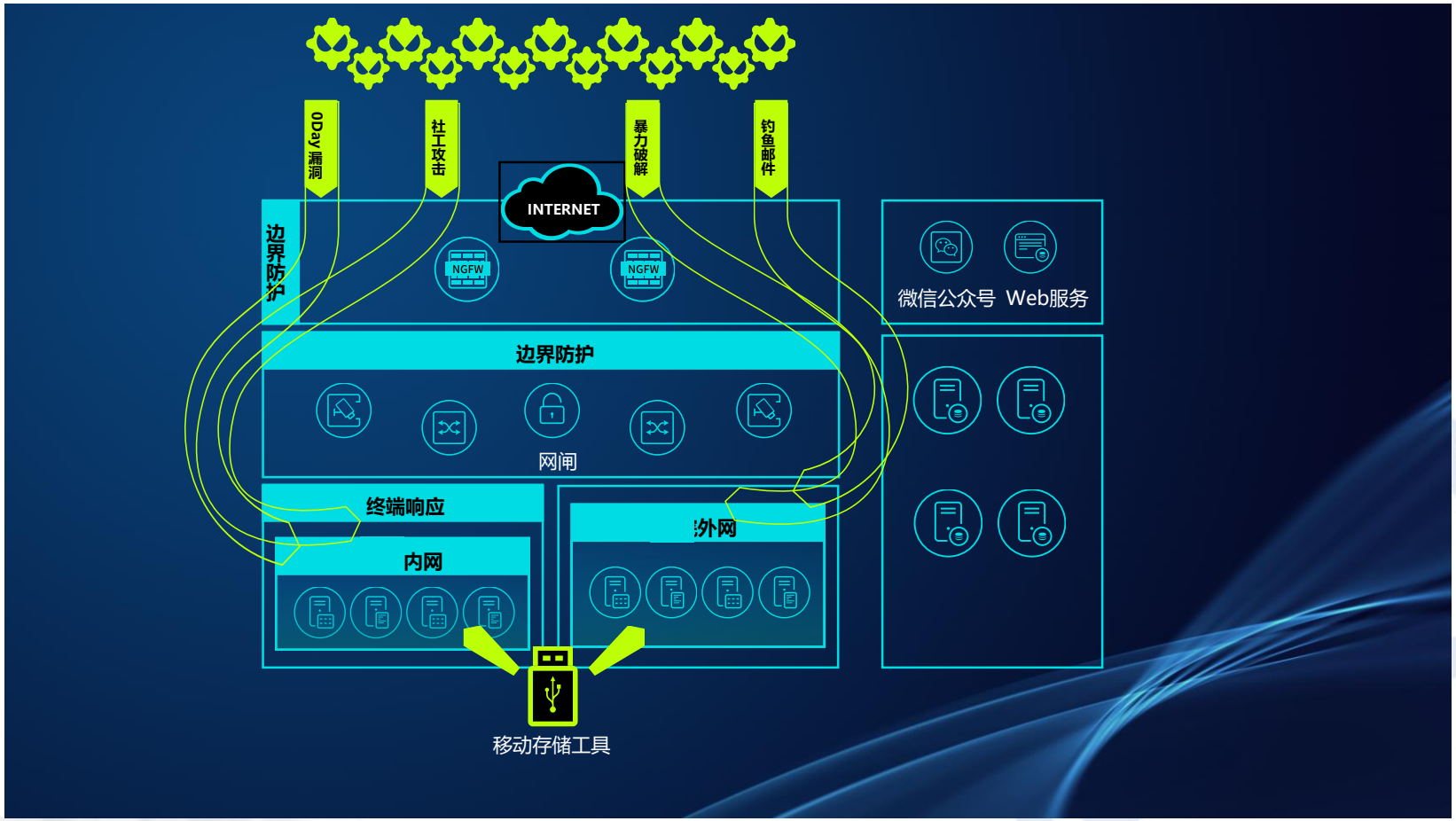
暴力破解

通过暴力破解RDP端口、SSH端口，数据库端口

典型案例：.java 、**GlobeImposter变种**

主要对象：开放远程管理的Server

勒索病毒常见传播方式


0Day漏洞
社工攻击
暴力破解
钓鱼邮件
INTERNET
边界防护
NGFW
NGFW
微信公众号
Web服务
边界防护
网闸
终端响应
内网
外网
移动存储工具

勒索病毒内网传播方式

内网传播感染

网络探测

对内部网络主机
进行弱点探测

内网传播

对存在弱点的内网主机进行
弱点利用并传播勒索病毒

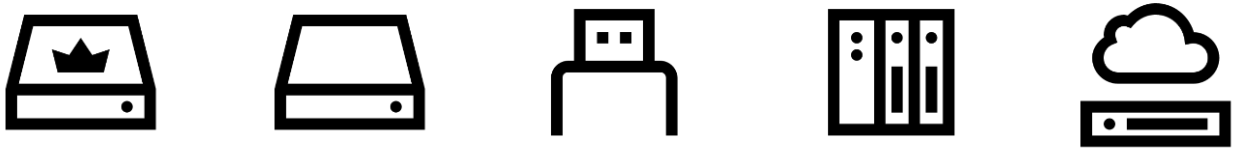
文件加密

勒索病毒运行后对预定的
文件类型进行加密

弹框勒索

完成文件加密后，弹出勒索
对话框引起受害者注意

破坏对象



OS Disk

Local Disk(s)

Connected Device(s)
(USB)
(e.g. Backup Disk)

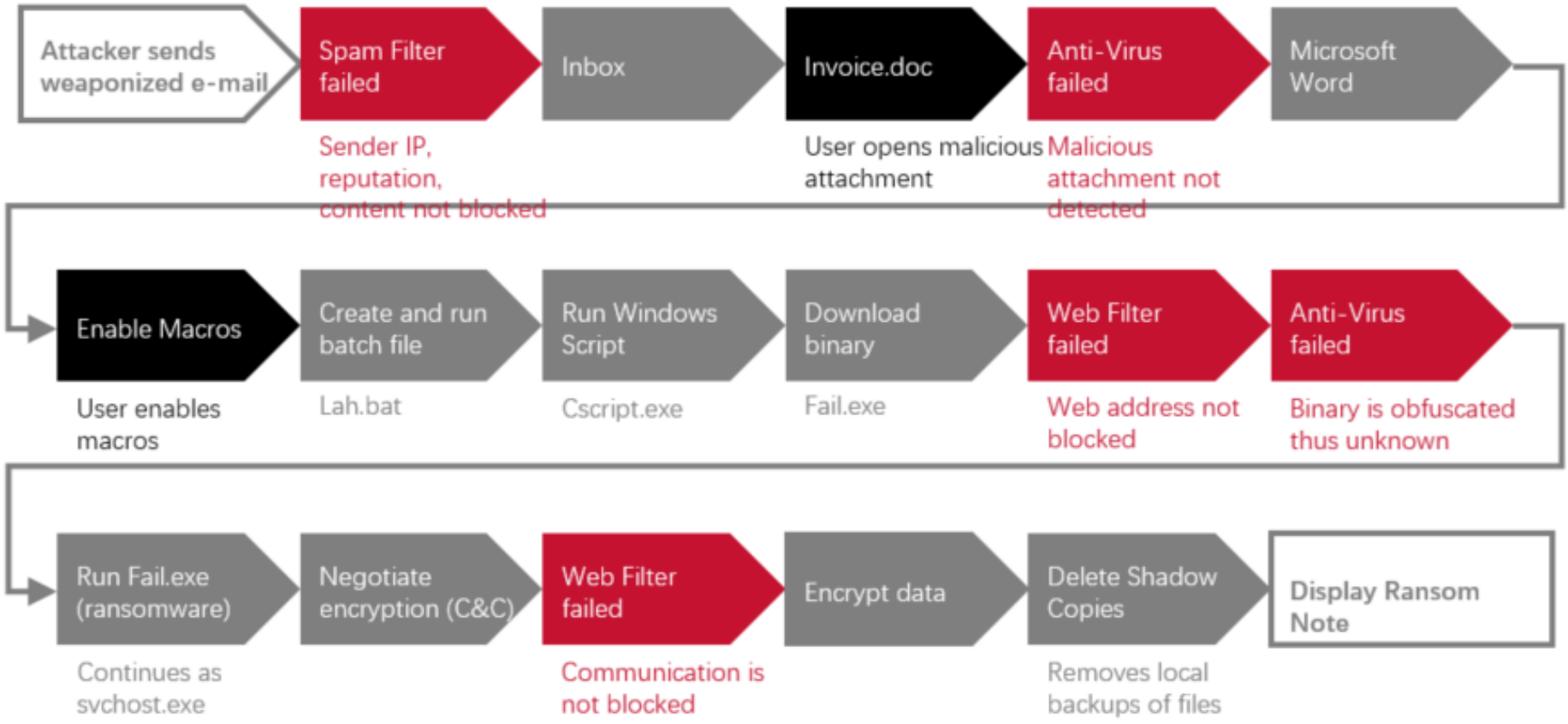
Mapped Network Drive(s)
(e.g. NAS / File Servers)

Other Accessible Folders / Shared Local Network
(e.g. NAS / File Servers)

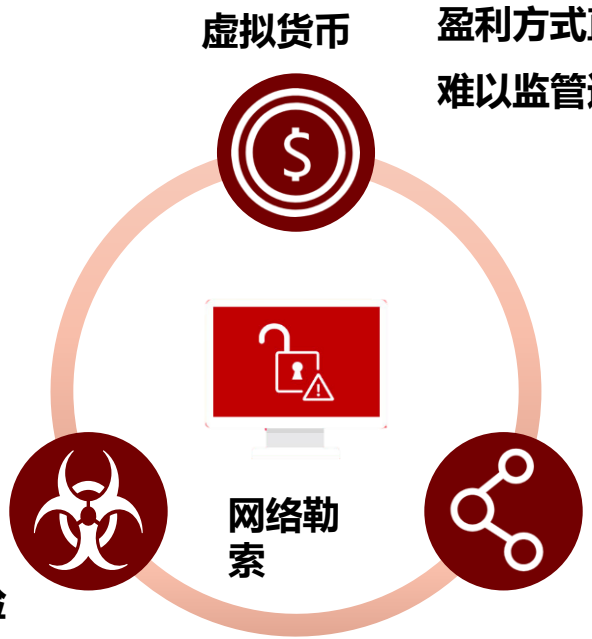
Dropbox

OneDrive

Social Engineering Flow



勒索病毒的特点和挑战


虚拟货币
盈利方式直接
难以监管追踪
病毒变异
传统杀软难以检验
难以人力收集样本
网络勒索
传播手段
多种传播手段
单一防御检测方法难以应对

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

勒索型恶意软件案例
——WannaCry

上海交通大学 网络空间安全学院
School Of Cyber Security,ShanghaiJiao Tong University

WannaCry怎么来的？

2016.08

- Shadow Brokers入侵了Equaiton Group,并窃取了大量机密文件。

公开&出售

- 公开了部分文件
- 100万比特币出售其他的。

怒而公开

- 由于没人接手，怒而公开机密工具。其中包括EnternalBlue

WannaCry产生

- 黑客们利用EnternalBlue的原理制作勒索型恶意代码

WannaCry是什么？

WannaCry，一种电脑软件勒索病毒。该恶意软件会扫描电脑上的TCP 445端口以类似于蠕虫病毒的方式传播，攻击主机并加密主机上存储的文件，然后要求以比特币的形式支付赎金。

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

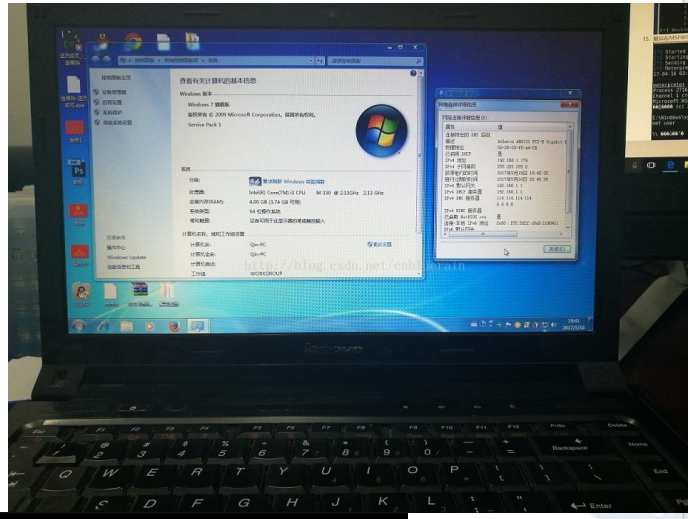
永恒之蓝是什么？

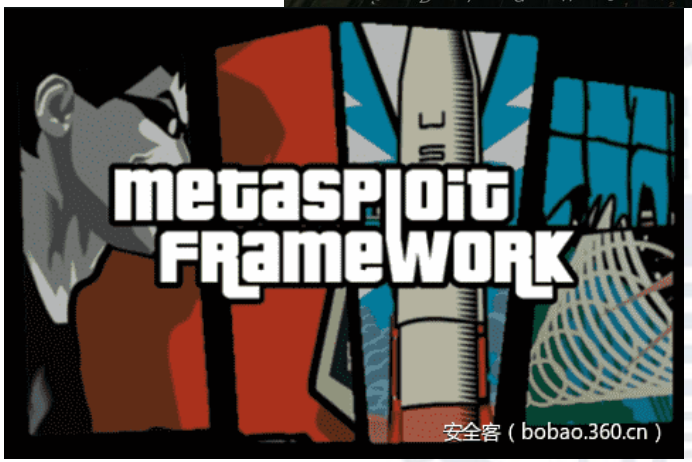
EternalBlue这个工具就是利用windows系统的Windows SMB远程执行代码漏洞向Microsoft服务器消息块 (SMBv1) 服务器发送经特殊设计的消息，就能允许远程代码执行。

“MS017-010”漏洞，SMB漏洞。

开放445文件共享端口的Windows机器。

利用Metasploit中针对ms17-101漏洞的攻击载荷进行攻击获取主机控制权限。





WannaCry的危害范围

2017年5月12日，WannaCry勒索病毒事件造成99个国家遭受了攻击，其中包括英国、美国、中国、俄罗斯、西班牙和意大利。

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

WannaCry的危害范围





2017年5月14日，WannaCry 勒索病毒出现了变种：WannaCry 2.0，取消Kill Switch将会使传播速度或更快。截止2017年5月15日，WannaCry造成至少有150个国家受到网络攻击，已经影响到金融，能源，医疗等行业，造成严重的危机管理问题。中国部分Window操作系统用户遭受感染，校园网用户首当其冲，受害严重，大量实验室数据和毕业设计被锁定加密。

我们该如何防范WannaCry入侵你的电脑呢？

微软声称如果用户采用全新版本的Windows 10系统，并开启Windows Defender的话，他们将会免疫这些勒索病毒。也就是说Windows 10用户大可放心，将不会受到这个勒索病毒的传播。另一方面，失去安全更新支持的Windows XP和Windows Vista操作系统非常容易遭受此类病毒的感染，微软建议用户尽早更新至全新操作系统应对。

确保运行Windows操作系统的设备均安装了全部补丁，并在部署时遵循了最佳实践。此外，组织还应确保关闭所有外部可访问的主机上的SMB端口(445,135,137,138,139端口，关闭网络共享)。

清华大学出版社
TSINGHUA UNIVERSITY PRESS

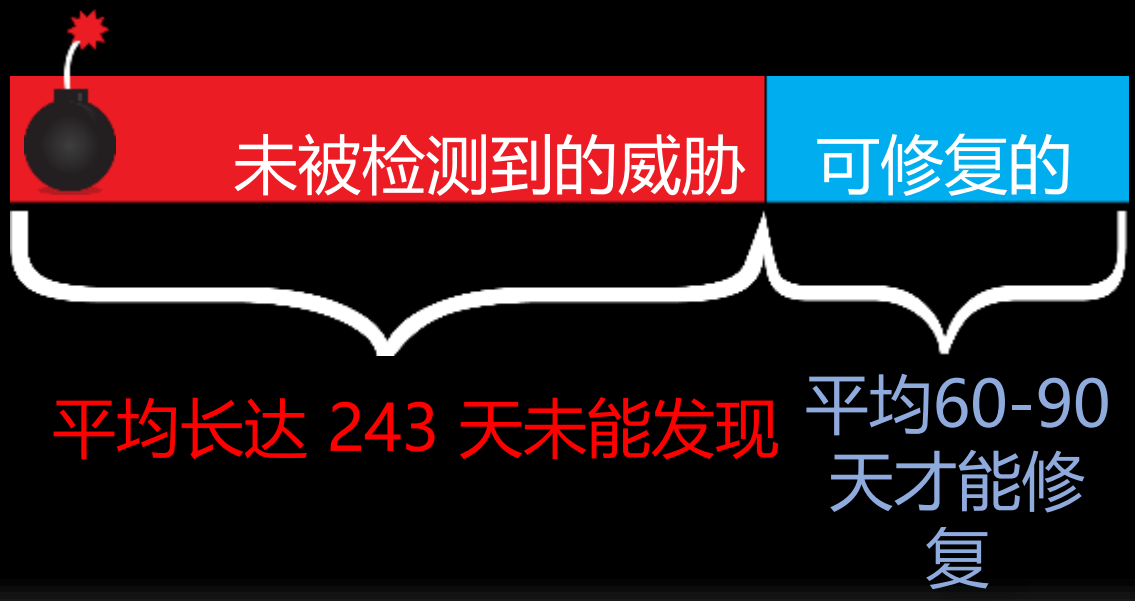
重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

勒索病毒应急处置与加固

上海交通大学 网络空间安全学院
School Of Cyber Security,ShanghaiJiao Tong University

如今那些有威胁的攻击

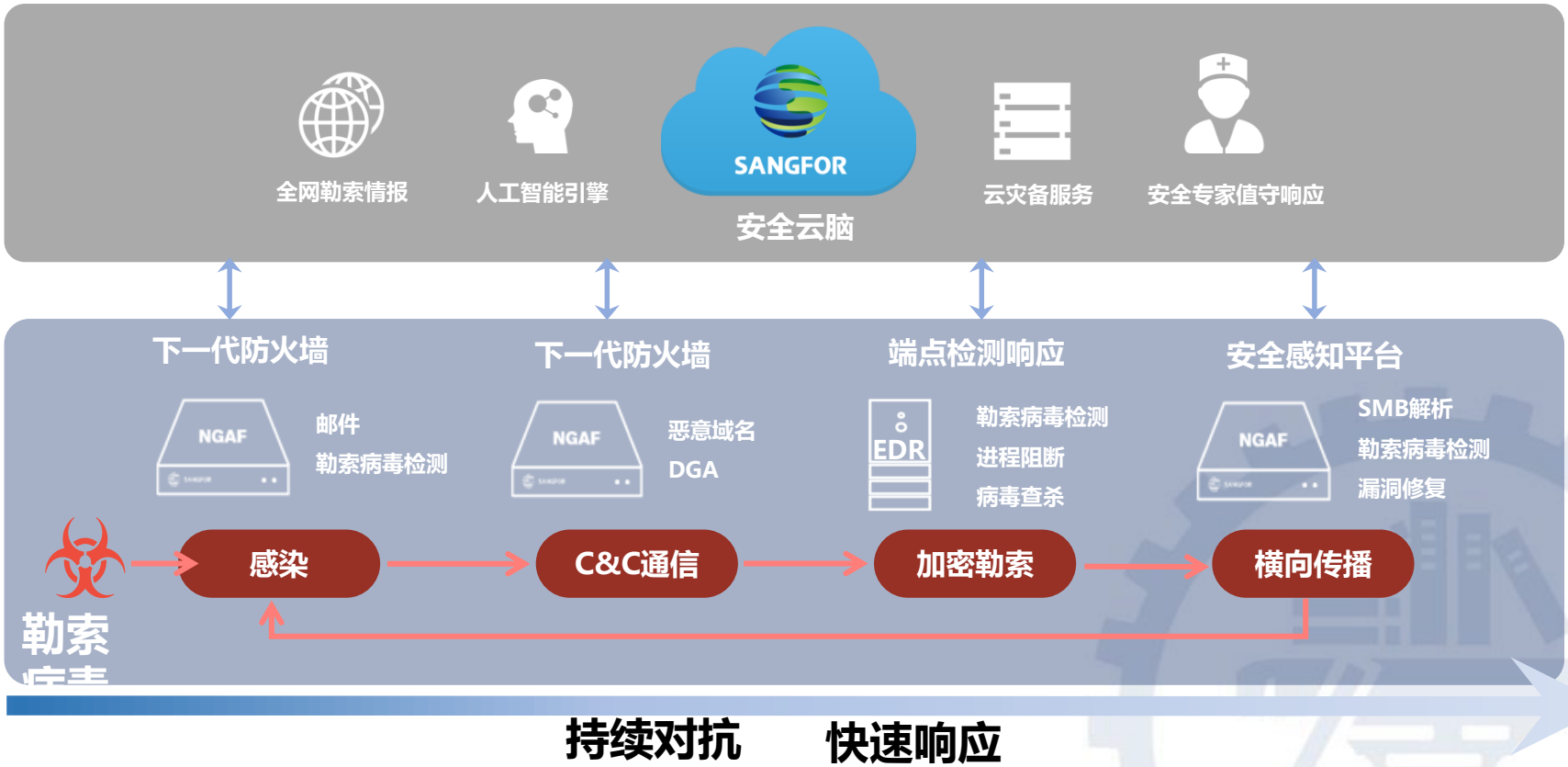


勒索病毒防御体系

勒索病毒是一个动态的攻击过程，没有一劳永逸的解决方案

检测防御能力生成

全生命周期的勒索防护



勒索病毒预防措施----安全管理制度

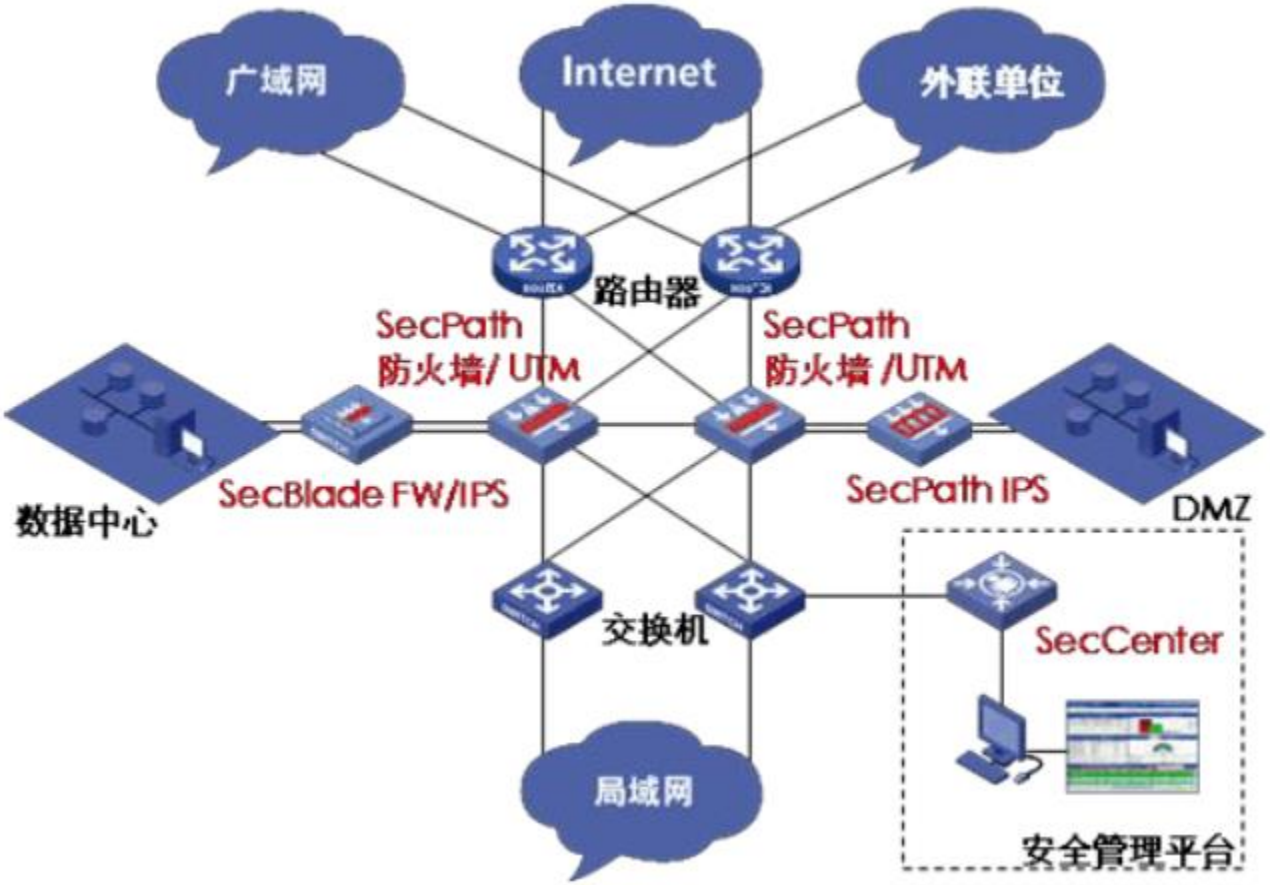
建立完善的安全管理制度并严格执行

- 严格管理互联网访问权限，避免引入外部风险；
- 严格控制内网终端接入移动存储设备，避免引入安全风险；
- 网络管理员应该周期性的使用网络检查设备检查网络或关注和整理网络安全设备生成的日志报表，了解网络是否存在安全风险，及时整改；
- 禁止人为关闭计算机终端防病毒软件等安全软件；
- 私人计算机终端禁止接入医院网络；
- 强制所有安全设备/软件每天更新规则库并每隔一段时间检查更新情况；
- ……

勒索病毒预防措施----网络层面

- 根据企业内网络实际情况，重新规划安全隔离区域，通过防火墙设备修改配置策略实现区域与区域之间的安全隔离，避免勒索病毒在内网扩散；
- 严格配置外联网络的边界访问控制策略，例如互联网接入区、外联网络接入区等（默认外联机构的网络都是不安全的）；关闭不必要的端口访问，仅开放必须的业务端口；
- 加强边界安全防护设备的策略配置，重新检查配置情况，避免因策略配置缺失带来的安全风险；
- 及时更新内外网所有安全设备/安全软件的规则库，目前绝大部分安全产品都是基于特征库匹配的防护模式，更新到最新的规则库有助于防御最新的安全风险；

勒索病毒预防措施----边界隔离



H3C边界防护解决方案可彻底解决以上问题，是针对边界安全防护的最佳方案。方案由安全网关、入侵防御系统和安全管理平台组成。安全网关SecPath防火墙/UTM融合2-4层的包过滤、状态检测等技术，配合SecPath IPS 4-7层的入侵防御系统，实现全面的2-7层安全防护，有效地抵御了非法访问、病毒、蠕虫、页面篡改等攻击；并通过安全管理平台对安全网关、入侵防御系统以及网络设备进行统一安全管理。

产品型号	描述
SecPath/SecBlade 防火墙	解决边界隔离安全需求
SecPath/SecBlade IPS	解决 4-7 层入侵防御需求
SecPath UTM	解决中小用户安全需求
SecCenter	收集和分析全网安全事件，并审计输出安全报告

勒索病毒预防措施----系统及应用层面

- 避免使用弱口令，口令强度要符合规范，并且定期更换，禁止多个终端/服务器使用同一口令；
- 关闭Windows共享服务、远程桌面控制等不必要的服务，仅开放服务器所必需的服务；
- 定期对主机/服务器执行打补丁的操作，确保操作系统时刻处于最新的状态；
- 对重要系统及数据进行定期非本地备份或组建异地灾备平台；
- 不要点击来历不明的邮件正文链接及查看或下载附件信息；

勒索病毒应急处置

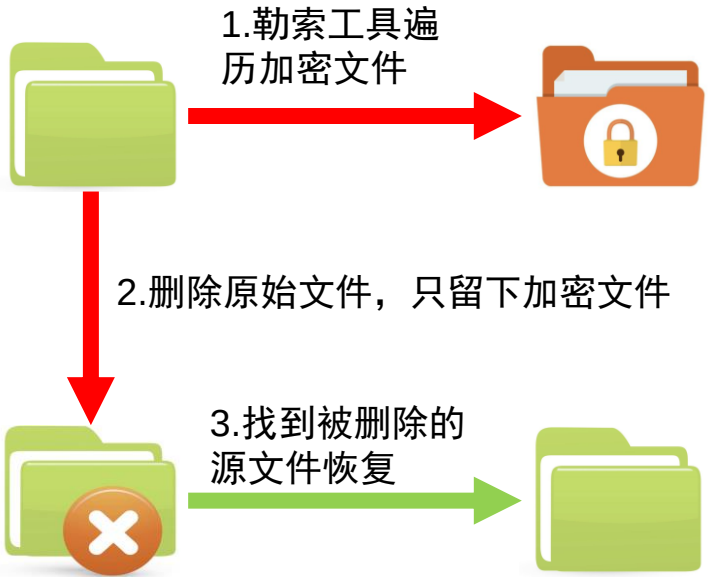
“中招”怎么办?

1.隔离感染主机	2.切断传播途径	3. 查找攻击源	4.查杀病毒修复漏洞
已中毒计算机尽快隔离，关闭所有网络连接，禁用网卡；	关闭潜在终端的SMB，RDP端口。关闭异常的外联访问。	抓包分析攻击源，网内查找其他受感染的终端及服务器	查杀病毒，如有漏洞及时打补丁修复漏洞，修改管理员权限帐号口令；

勒索病毒数据恢复

加密原理

1.不同勒索病毒可能采用不同加密算法
2.针对大文件勒索病毒为了提升加密效率只加密文件头
3.具体加密步骤如下



数据恢复方法

勒索病毒的数据恢复难度较大，防范应以预防为主，如下提供几个思路尝试

方案一：尝试用数据恢复软件找到被删除的源文件；

方案二：通过解密工具破解，解密文件；

方案三：通过winhex对比历史文件分析文件头内容恢复

方案四：支付赎金恢复数据，部分勒索病毒即便支付攻击者赎金也未必可以解密被勒索文件

勒索病毒给我们的启示

持续对抗

- 勒索时代
- 前赴后继的黑客
- 新的家族、变种
- 新的攻击方式

快速响应

- 事件第一时间响应
- 风险隔离
- 紧急处置
- 持续待命

安全体系

- 构建安全体系
- 严格执行
- 实时监控
- 防护策略落地

人工智能

- 识别未知风险
- 自动化检测防御
- 提高准确率
- 持续进化

清华大学出版社
TSINGHUA UNIVERSITY PRESS

重点大学信息安全专业规划系列教材

恶意代码与计算机病毒
——原理、技术和实践

Any Questions