周一开机保障指南及工具包



2017年05月15日



目录

第1章	事件概述3
第2章	受影响系统4
第3章	本文档及工具包的作用5
第4章	本文档及工具包的内容6
4.1	所包含的文档说明6
4.2	所包含的工具说明
第5章	风险提示9
5.1	域环境下禁用 445 端口风险9
5.2	关键数据被加密的处置建议9
第6章	安全开机操作指南10
6.1	如果你是网络管理员10
6.2	如果你是服务器管理员12
6.3	如果你是桌面终端管理员
6.4	如果你是普通电脑用户26



第1章 事件概述

2017 年 4 月,美国国家安全局(NSA)旗下的"方程式黑客组织"使用的部分网络武器被公开,其中有十款工具最容易影响 Windows 用户,包括永恒之蓝、 永恒王者、永恒 浪漫、永恒协作、翡翠纤维、古怪地鼠、爱斯基摩卷、文雅学者、日食之翼和尊重审查。 不法分子利用"永恒之蓝",通过扫描开放 445 文件共享端口的 Windows,无需任何操作,只要开机上网,不法分子就能在电脑和服务器中植入执行勒索程序、远程控制木马、虚拟 货币挖矿机等恶意程序,就像冲击波、震荡波等著名蠕虫一样可以瞬间影响互联网。

2017 年 5 月 12 日晚间起,我国各大高校的师生陆续发现自己电脑中的文件和程序 被加密而无法打开,弹出对话框要求支付比特币赎金后才能恢复,如若不在规定时间内 提供赎金,被加密的文件将被彻底删除。同时,英国多家医院也受到了类似的勒索攻击, 导致医院系统趋于瘫痪,大量病患的诊断被延误。而此次事件不是个案,后续不断报道出 全球各国遭受勒索软件威胁,近100个国家遭受了攻击。加油站、火车站、政府办事终端 等设备以及邮政、医院、电信运营商,部分工业设施等行业都被"中招",部分设备己完 全罢工,无法使用。 目前,该事件的影响已逐步扩展到国内各类规模的企业内网、教育 网、政府机构 等多类单位。

需要了解该永恒之蓝"(蠕虫 WannaCry)攻击详情的用户请参考附件 1《 360 针对"永恒之蓝"(蠕虫 WannaCry)攻击预警通告》。

本开机保障指南在线阅读地址:

http://b.360.cn/assets/doc/OnionWorm_handbook.pdf



第2章 受影响系统

本次威胁主要影响以下操作系统:

桌面版本操作系统:

Windows 2000

Windows XP

Windows Vista

Windows7

Windows8

Windows8.1

Windows10

服务器版本操作系统:

Windows Server 2000

- Windows Server 2003
- Windows Server 2008

Windows Server 2012

Windows Server 2016



第3章 本文档及工具包的作用

由于本次攻击爆发在 5 月 12 日周五下午,感染高峰出现在众多机构下班之后,周六 和周日两天恰逢公休,360 安全监测与响应中心判断在 5 月 15 日周一上班时,存在大量 电脑或服务器开机的情况,此时应该存在新的一轮感染高峰,为了确保周一开机时用户电 脑和服务器免遭病毒感染或避免更大范围的传播,360 企业安全制定了本文档,用于指导 机构用户不同角色根据指南内容进行安全操作。



第4章 本文档及工具包的内容

本指南包含多个文档及工具,下表针对文档和工具提供详细说明。

4.1 所包含的文档说明

序号	文档说明	文件名
	360CERT 针对本次攻击的操作指南,包含在不使用安	附件 1 360 针对"永恒
1	全产品的前提下,如何进行影响范围确定、网络及终	之蓝"(蠕虫
I	端层面的临时抑制方案及相关根治方法及恢复建议。	WannaCry)攻击预警通
	http://b.360.cn/assets/doc/OnionWorm_Report.pdf	告
	360CERT 本次攻击的紧急处置手册,包含应急响应推	
	荐操作及隔离网、互联网、网络设备等多个方面的防	附件 2 针对"永恒之
2	护操作流程及方法	蓝"攻击紧急处置手册
	http://zt.360.cn/1101061855.php?dtid=1101062514	(蠕虫 WannaCry)
	&did=490458365	
	微软相关高危漏洞 MSID 与 KBID 对照表,用于检验相	
	关的 CVE 漏洞是否被修复。人工操作方法:开始菜单	
	运行 cmd.exe ,输入 systeminfo 命令等待返回,从如	附件 9
3	果返回的补丁信息中包含对应的 KB 号,漏洞修复成	的什 3 版状间池确视-
	功。	MOID J KDID M RRAC
	http://b.360.cn//main_web/assets/doc/MSID_KBID_	
	lib.xlsx	
	360 追日团队(专业高级威胁追踪溯源团队)针对本次	附件 4 WanaCryptOr 勘
4	攻击的技术分析报告,包含蠕虫攻击流程、蠕虫利用	索蠕中完全分析报告
	漏洞分析、相关释放文件分析、勒索加密过程及解密	7: 40 - ムノレエ /J 1/ 1 人



	过程分析等模块。	
	http://m.bobao.360.cn/learning/detail/3853.html	
	?from=timeline&isappinstalled=1	
	360 网关产品线对本次攻击的操作指南,包含网络策	
	略配置、IPS 防护引擎配置、DNS 诱导、失陷主机隔离	
	等多个方面的防护操作流程及方法。	附供 5 260 防止 按 立 日
5	其中要注意的是:使用 DNS 诱导的方法时一定要建立	附件 3 300 四八個) 四
Ð	一个运行在 80 端口的正常的 HTTP 服务,隔离网用户	打八 小但之 则系
	建议在内部 DNS SERVER 上同时增加相关 DNS 诱导配	s 出的防护刀杀 V3.1
	置。	
	http://bobao.360.cn/interref/detai1/109.html	
	360终端安全产品线针对本次攻击的操作指南,包含	
	临时免疫工具使用、病毒特征更新、补丁升级等多个	附件 6 360 天擎产品针
6	方面的防护操作流程及方法。	对"永恒之蓝"勒索蠕
	http://b.360.cn//main_web/assets/doc/OnionWorm_	虫病毒的防护方案 1.13
	protect.docx	
	360 虚拟化产品线针对本次攻击的操作指南,包含轻	
	代理及无代理解决方案下的防火墙模块操作指南、未	附件 7 360 虚拟化安全
7	购买防火墙模块的情况下终端加固操作流程及方法。	产品"永恒之蓝"应急
	http://bbs.360.cn/forum.php?mod=viewthread&tid=	处置办法
	14974137	

4.2 所包含的工具说明

序号	工具	文件名
1	360 勒索蠕虫漏洞修复工具,此修复工具集成免疫、SMB	NSASaan ava
T	服务关闭和各系统下 MS17-010 漏洞检测与修复于一体。	Nonocall. exe



	可在离线网络环境下一键式修复系统存在的 MS17-010 漏	
	洞,根本解决勒索蠕虫利用 MS17-010 漏洞带来的安全隐	
	患。修复工具下载地址:	
	http://b.360.cn/other/onionwormfix	
	360 勒索蠕虫免疫工具,可用于主机免疫勒索蠕虫的破坏	
2	过程。下载地址:	OnionWormImmune
	http://b.360.cn/other/onionwormimmune	
	勒索软件漏洞扫描工具,可通过扫描端口远程或本地检测	
0	主机是否存在漏洞。该工具有一定风险性,建议寻求 360	
3	企业安全技术支持获取该工具及服务支持。开源工具下载	ms17010detectv4
	地址: https://github.com/RiskSense-Ops/MS17-010	
	360 勒索蠕虫文件恢复工具(非解密),有可能恢复一部分	
4	被加密的文件,用于紧急数据恢复,存在一定概率无法恢	D
4	复。下载地址:	kansomkecovery.exe
	https://dl.360safe.com/recovery/RansomRecovery.exe	
	360 安全卫士个人版在线安装程序,可用于联网环境下的	
5	补丁升级及安全防护。下载地址:	inst==.exe
	http://down.360safe.com/inst.exe	
	360 禁用 445 端口的脚本工具,可禁用 Server 服务并添	シセンギを通知時日子
6	加 ipsec 规则禁止 445 端口访问	小但之 鱼 佩 們 垧 口 大
	http://dl.b.360.cn/tools/EternalBlueBat.zip	M1. Z1D



第5章 风险提示

5.1 域环境下禁用 445 端口风险

域环境下关闭 445 有可能造成以下影响,请知悉。

- 文件共享与打印机共享功能将不可用。
- 依赖于命名管道的 RPC 功能将不可用。
 若域控关闭 445 端口,将会影响以下功能:
- 域控间的数据同步
- 用户与计算机身份验证
- 组策略
- 域之间的信任关系

5.2 关键数据被加密的处置建议

关键数据被加密后处置建议如下:

- 硬盘对拷备份3份以上,原始主机封存
- 采取磁盘恢复的方式尝试恢复备份数据
- 等待机会,部分勒索软件会在一定时期后公开秘钥



第6章 安全开机操作指南

本指南根据用户角色的不同进行针对性的操作指导,本次操作指南区分四种用户角色: 网络管理员、服务器管理员、桌面终端管理员、普通用户。

6.1 如果你是网络管理员

步骤一: 请阅读附件文档的附件 1《360 针对"永恒之蓝"(蠕虫 WANNACRY)攻击预 警通告》文档以了解整个事件的全貌,掌握应急响应所需要必备知识。

步骤二: <流程1 网络管理员用户操作流程>进行处置。





流程图示中的环节1说明:

检查系统中是否有可用的 web 服务器,监听的端口需要是 80,保证该服务器能够正确 响应根目录的 Get 请求,即保证 web 服务器正常工作。

流程图示中的环节2说明:

搭建针对秘密开关域名的服务器,最简单的方式是通过 python 开启一个 web 服务 (python - m SimpleHTTPServer 80),如果内网环境较大,怀疑可能感染的设备较多, web 服务器压力过大,可以搭建性能较好的 nginx 或者 apache 服务器。

Python2 简单开启 web 如下如下图所示:



← → C ☆ ③ 10.17.34.113

Directory listing for /



流程图示中的环节3说明:

修改内网的 DNS 服务器配置,

将 www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

和 www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com 的解析地址指向内网 Web 服务器 ip 地址。

流程图示中的环节4说明:

网络管理员从内网中多处访问如上的两个域名,访问正常,则秘密开关域名服务器搭 建完成,如果有不能正常访问,检测步骤2和步骤3是否配置正确。

6.2 如果你是服务器管理员

步骤一: 请阅读附件文档的附件 1《360 针对"永恒之蓝"(蠕虫 WannaCry) 攻击预 警通告》 文档以了解整个事件的全貌,掌握应急响应所需要必备知识。

步骤二:请准备好工具软件包中的工具 1、工具 2 和工具 3,这些工具软件已经包含 在 360 企业安全为您提供的安全 U 盘,或选择未被感染的电脑从网络上下载,在使用 U 盘



时,请确保打开 U 盘的写保护功能,以避免 U 盘遭受感染。

步骤三:请按照<流程1服务器管理员操作流程>流程进行安全操作:





流程2 服务器管理员操作流程

流程图示中的环节1说明:

该步骤使用工具 3 检测管辖范围内的服务器是否存在本次勒索蠕虫所利用的漏洞,尽快确认存在漏洞的服务器数量和范围。其中工具 3 的使用方法:在命令行环境下执行工具 3,示例如下:

ms17010detectv4.exe 192.168.1.1 扫描单个 IP

ms17010detectv4.exe 192.168.1.0/24 扫描单个网段

ms17010detectv4.exe 192.168.1.1-23 扫描单个网段连续 IP

ms17010detectv4.exe 192.168.1.* 扫描单个网段全部 IP

ms17010detectv4.exe -list iplist.txt 扫描多个 IP, 地址每行一个输入到 txt 文件中

🛤 C:\WINDOWS\system32\cmd.exe	 X	
C:\>ms17010detectv4.exe -list ip.txt	^	
192.168.232.137 is likely VULNERABLE to MS17-010!		
detect over!		
C:\>type ip.txt		
192.168.232.137		
192.168.232.2		
	-	
		4



流程图示中的环节2说明:

如果存在 VULNERABLE 提示,则说明该主机极有可能存在该漏洞,需要立即进行检测 及修复。如下图:

C:\WINDOWS\system32\cmd.exe	_ [ı ×	¢
Connection-specific DNS Suffix . : localdomain IP Address]
Ethernet adapter Bluetooth 网络连接:			
Media State : Media disconnected			
C:\>ms17010detectv4.exe 192.168.232.137 192.168.232.137 is likely VULNERABLE to MS17-010! detect over!			
C:\>ms17010detectv4.exe Usage:			
ms17010detectv4.exe 192.168.1.1			
ms17010detectv4.exe 192.168.1.0/24 ms17010detectv4.exe 192.168.1.1-23 ms17010detectv4.exe 192.168.1.* ms17010detectv4.exe 192.168.1.1,2,3			
ms17010detectv4.exe -list iplist.txt		-	•

流程图示中的环节3说明:

被感染的机器屏幕会显示如下的告知付赎金的界面:



Tana DecryptOr 2.0		×
	Ooops, your files have beer	n encrypted! Chinese (simpli
	我的电脑出了什么问题? 您的一些重要文件被我加密保存了。	<u>^</u>
	照片、图片、文档、压缩包、音频、视频3 文件都被加密了,因此不能正常打开。 这和一般文件提场有本质上的区别。你大同	文件、exe文件等,几乎所有类型的
Payment will be raised on	保证,没有我们的解密服务,就算老天爷系	来了也不能恢复这些文档。
5/16/2017 02:26:59	有没有恢复这些文档的方法?	
Time Left 22:22:35:15	当然有可恢复的方法。只能通过我们的解释 够提供安全有效的恢复服务。 但这是收费的,也不能无限期的推迟。 请点击 <decrypt> 按钮,就可以免费恢复</decrypt>	密服务才能恢复。我以人格担保,能 一些文档。请您放心,我是绝不会
Your files will be lost on	骗你的。 但想要恢复全部文档,需要付款点费用。	
5/20/2017 02:26:59	是否随时都可以固定金额付款,就会恢复的 对你不利。	竹吗,当然不是,推迟付款时间越长
Time Left 26:22:35:15	最好3天之内付款费用,过了三天费用就会 还有,一个礼拜之内未付款,将会永远恢复 对了,忘了告诉你,对半年以上没钱付款的	翻倍。 夏不了。 勺穷人,会有活动免费恢复,能否轮 <mark>、</mark>
<u>About bitcoin</u> <u>How to buy bitcoins?</u>	B bitcoin ACCEPTED HERE Send \$300 worth of bi	tcoin to this address: QepoHkHSQuy6NgaEb94
Contact Us	Check Payment	Decrypt

请注意:如果你的数据非常关键且无法支付赎金,请不要轻易格式化关键数据所在的 服务器,相应处置请参见第5章5.2

流程图示中的环节4说明:

运行工具 1,对服务器进行一键免疫及补丁操作并重新启动系统。也可以根据操作系统版本,手动选择对应补丁升级。

请注意:服务器补丁升级一定要缓步进行,可以采用测试环境升级补丁、测试业务正常之后,邀请业务开发、运营团队一起逐步对线上服务器进行升级,做好必要的回退及热备机制。如果该业务系统极其重要,且没有补丁对该业务系统影响的信息,请采取其他抑制措施,诸如配置网络ACL手段。





如果免疫工具运行异常,也可使用工具6、永恒之蓝漏洞端口关闭.zip禁用445端口。 将工具解压后,双击运行"执行我.bat"检查并关闭电脑相关服务和端口,出现以下窗口 为服务已经关闭。



流程图示中的环节5说明:

运行工具1,对服务器进行安全检查,也可以按照环节1的方法进行二次验证。





流程图示中的环节7说明:

经业务部门确认稳定后重新上线。

6.3 如果你是桌面终端管理员

步骤一:请阅读附件文档的"附件 1《360 针对"永恒之蓝"(蠕虫 WANNACRY)攻击预警通告》文档以了解整个事件的全貌,掌握应急响应所需要必备知识。

步骤二:请准备好工具软件包中的工具 1、工具 2、工具 4 和工具 5,这些工具软件 已经包含在 360 企业安全为您提供的安全 U 盘或选择未被感染的电脑从网络上下载,请确 保打开 U 盘的写保护功能,以避免 U 盘遭受感染。

步骤三:参照<流程 2 桌面终端管理员操作流程>进行桌面终端安全检查及处置流程。





流程3 桌面终端管理员操作流程

流程图示中的环节1说明:

紧急通知全体员工断开网络连接,在内网建立工具分发网站或创立多个工具分发介质。



流程图示中的环节2说明:

被感染的机器屏幕会显示如下的告知付赎金的界面:

💕 Tana DecryptOr 2.0		×
	Ooops, your files have bee	en encrypted! Chinese (simpli
1	我的电脑出了什么问题? 您的一些重要文件被我加密保存了。 照片、图片、文档、压缩包、音频、视频 文件都被加密了,因此不能正常打开。 这和一般文件损坏有本质上的区别。您大	▲ 文件、exe文件等,几乎所有类型的 可在网上找找恢复文件的方法,我敢
Payment will be raised on	保证,没有我们的解密服务,就算老天爷	来了也不能恢复这些文档。
5/16/2017 02:26:59	有没有恢复这些文档的方法?	
Time Left (22:22:35:15	当然有可恢复的方法。只能通过我们的解 够提供安全有效的恢复服务。 但这是收费的,也不能无限期的推迟。 请点击 <decrypt> 按钮,就可以免费恢复</decrypt>	密服务才能恢复。我以人格担保,能
Your files will be lost on 5/20/2017 02:26:59	骗你的。 但想要恢复全部文档,需要付款点费用。 是否随时都可以固定金额付款,就会恢复 对你不利。	的吗,当然不是,推迟付款时间越长
Time Left 26: 22: 35: 15	最好3天之内付款费用,过了三天费用就会 还有,一个礼拜之内未付款,将会永远恢 对了,忘了告诉你,对半年以上没钱付款	▲翻倍。 复不了。 的穷人,会有活动免费恢复,能否轮
<u>About bitcoin</u> <u>How to buy bitcoins?</u>	B bitcoin Accepted Here Send \$300 worth of b 13AM4VW2dhxYgXe	pitcoin to this address: QepoHkHSQuy6NgaEb94
<u>Contact Us</u>	Check Payment	Decrypt

请注意:如果你的数据非常关键且无法支付赎金,请不要轻易格式化关键数据所在的 服务器,相应处置请参见第5章5.2

流程图示中的环节3说明:

如果需要尝试数据恢复操作,请执行操作5

流程图示中的环节4说明:

登记被攻陷主机相关的信息,汇总至管理员,示例如下:

序号	主机名	IP	MAC 地址	所有 人	联系方式	部门
1	PC-0001	192. 168. 0. 123	00-0C-29-8D-E6-5	张三	13888888888	业务 部

流程图示中的操作5说明:

1) 首先安装 360 安全卫士,选择漏洞修复,打好安全补丁,预防再次被攻击



补漏	洞、装驱动	,修复异常系	统
修复电影		1驱动,确保电脑安全	
	全面修复	 ※ 	
「「」」 「「」」 「 「」 「	/	 2 2 30 191 2 30 30 191 2 30 30 191 2 30 30 191 3 30 30	夏
60安全卫士11 + 	A Chaile Triffic to a	(亡) 安全就组 软件面	
扫描已完成,发现潜在危 共发现7个维导修复项目。修复可使系统稳定正	加险项,请立即 ^{演运行,请立即修复!}	修复	一键修复
編編修复 - 7項 这些高两可能会被木马、病毒利用、破坏器	的电脑,请立即惨复。		一壁回路へ
✓ KB3212642 - Windows 月度安全更新(2017.01) 目	2017-01-08	6.2MB	部略
✓ KB4012212 · Windows 月度安全更新(2017.03)	2017-03-12	33.2MB	忽略
✓ KB4014565Net Framework 3.5 SP1安全更新 目	2017-04-10	7.3MB	(2)路
✓ KB4014504Net Framework 3.5 SP1安全更新 Ⅲ	2017-05-05	17.1MB	忽略
V K84014579Net Framework 3.5 SP1安全更新 回	2017-05-05	15.7MB	3386

身出震海信息 這理补丁安装包

2) 使用 360 木马查杀功能,清除全部木马,防止反复感染。



◆ 380安全卫士11 + ◆	电脑清理 系统	第2 代化加速	日 功能大全 3	60 钱包 软件管	
		您已长时	 间没有查	涂,请立日	即扫描
		最近童茶时间是快速重	2016-7-12; 30(勝載 登 茶 全	每周进行一次木马查 一 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、	·····································
					开启强力模式(仅限本次扫描)
 福祉区 修道区 上部区 第60安全卫士11 + 电脑体检 木马查杀 	自己 电脑清理 系统	修复 优化加速	() 功能大全 3	东筑2 60铁包 软件管	日本市 手引 品 政治 WinPE 叙 ● 6235 ↓ 1.5% 3550 ↓ 2.8% 第. 単表350株号 ◆
	日描:文件和 WS\system32\shimgvw.	口系统内存		己用时; 00:0	21:47 暂停扫描
正在进行术与扫描 - 共 顽固术马 安全	BERE SC	▲ 新田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田	问题的危险项; \Documents and S\mss \Documents and Setting \Document\Www.maDecry	zeczvc.eze \u.wary ⊭ /ptor@.exe	() 系統資源和服务 (安全)
文详和系统内存 正在扫描	(1) 常用软件 等待扫描	系统综合 等待扫描	采 妖修复项 茶妖修复项 等待扫描		
● 沙尘暴又双叒叕来了?浴葱怎么办!					晶完成后自动关机(自动清除术马)

3)下载使用"360勒索蠕虫病毒文件恢复工具"恢复被加密的文件

下载地址: http://dl.360safe.com/recovery/RansomRecovery.exe 选择加密文件所在驱动器





扫描后,选择要恢复的文件

择驱动器: 🚞 :	本地磁盘 (D:)	- 重新扫描		快速查找	输入文件或文件夹名	5	
分类	日录	文件名	文件大小	创建日期	最后访问	可恢复	王怡
	M AV	🖌 🙀 defs. h	289 Byte	2015-9-30 15:40:12	2017-5-14 1:22:56	高	
📓 图像文件 (未找到)		🔽 🔓 Horphine. zip	108.86 KB	2015-9-30 15:40:12	2017-5-14 1:22:56	高	
		🔽 🚂 null. c	668 Byte	2015-9-30 15:40:12	2017-5-14 1:22:56	高	
□ 音频文件 (5	未找到)	🔽 🚂 readme. txt	106 Byte	2015-9-30 15:40:12	2017-5-14 1:22:56		
		🗹 🗽 masm_plugin. asm	2.27 KB	2015-9-30 15:40:12	2017-5-14 1:22:56	高	
◎ 视频文件/=	# # 至 1)	🗹 🚂 defs. h	263 Byte	2015-9-30 15:40:12	2017-5-14 1:22:56	』 高	
Manager (Maxadi)		🔽 🚂 null. c	668 Byte	2015-9-30 15:40:12	2017-5-14 1:22:56	』 高	
🧾 文档文件 (2个文件)		🗹 🚂 Eula tzt	6.84 KB	2015-9-30 15:40:14	2017-5-14 1:22:54	山 高	
		🔽 🚂 psversion. txt	39 Byte	2015-9-30 15:40:14	2017-5-14 1:22:56	山高	
The second second second	*****	🔽 🚂 readme.txt	7.72 KB	2015-9-30 15:40:14	2017-5-14 1:22:54	山商	
€ 网贝又件(2	村(231)	🗹 🗽 File Type Signatu	18.04 KB	2015-9-30 15:40:14	2017-5-14 1:22:54	前商	
-	- 100 IV	🔽 🚡 indexcha txt	26 Byte	2015-9-30 15:40:14	2017-5-14 1:22:56	山高	
所有文件(6	2个文件) 🕈	🛛 💽 系统给错的穿越者. doc	4.46 MB	2017-5-14 1:19:36	2017-5-14 1:20:03	前商	
🗾 所有文件夹 (37个文件夹)		🔽 🗽 直播在游戏异界. doc	2.98 MB	2017-5-14 1:19:36	2017-5-14 1:20:15	山高	
		🗹 🚡 幻善少年. txt	6.55 MB	2017-5-14 1:22:32	2017-5-14 1:22:32	画面	
		🔽 🗽 庆余年. tst	6.80 MB	2017-5-14 1:22:32	2017-5-14 1:22:32	高加	
		🔽 🗽 麻衣神算子. txt	10.33 MB	2017-5-14 1:22:32	2017-5-14 1:22:33	高加	
		<					5



择驱动器: 📠	本地磁盘 (D:)	■ 重新扫描		t	央速查找 :	输入文件或文件美名	5		
分类	目录	文件名	文件大小	创建日期		最后访问	可作	友复	性
	H St	🗹 🔓 defs h	289 Byte	2015-9-30 1	5:40:12	2017-5-14 1:22:56	all	高	-
■ 图像文件	(未找到)	🗹 🚂 Morphine. zip	108.86 KB	2015-9-30 1	5:40:12	2017-5-14 1:22:56	all	商	1
		🔽 🚂 null. c	668 Byte	2015-9-30 1	5:40:12	2017-5-14 1:22:56	all	商	
□ 音频文件)	(未找到)	🗹 🚂 readme. txt	106 Byte	2015-9-30 1	5:40:12	2017-5-14 1:22:56	all	高	
an Haven (Haven		🔽 😼 masm_plugin asm	2.27 KB	2015-9-30 1	5:40:12	2017-5-14 1:22:56	al	高	
🚺 視频文件 (未找到)		E			40:12	2017-5-14 1:22:56	all	高	
		E 正在恢复:未统给错的)穿越者.doc		40:12	2017-5-14 1:22:56	all	商	
1 文档文件 (2个文件)		E			40:14	2017-5-14 1:22:54	all	商	
		6			40:14	2017-5-14 1:22:56	all	商	
		6		取消	40:14	2017-5-14 1:22:54	all	高	
E MULCH	(#3230)	🗹 🙀 File Type Signatu	18.04 KB	2015-9-30 1	5:40:14	2017-5-14 1:22:54	at	高	
College and		🛛 🗹 🗽 indexcha. txt	26 Byte	2015-9-30 1	5:40:14	2017-5-14 1:22:56	.al	商	
所有文件(62个文件) 🔶 🌳		🔽 🚂 系统给错的穿越者. doc	4.46 MB	2017-5-14 1	:19:36	2017-5-14 1:20:03	all	商	
🛁 所有文件夹 (37个文件夹)		🔽 🚂 直播在游戏异界. doc	2.98 MB	2017-5-14 1	:19:36	2017-5-14 1:20:15	all	商	
		📝 🚂 幻兽少年. txt	6.55 MB	2017-5-14 1	:22:32	2017-5-14 1:22:32	.al	商	
		🗹 🚂 庆余年. txt	6.80 MB	2017-5-14 1	:22:32	2017-5-14 1:22:32	.all	高	
		🔽 🚂 麻衣神算子. txt	10.33 MB	2017-5-14 1	:22:32	2017-5-14 1:22:33	in.	高	~
		<						>	

强烈建议您选择把恢复的文件保存在干净的移动硬盘或U盘上



本工具的文件恢复成功率会受到文件数量、时间、磁盘操作情况等因素影响。一般来 说,中毒后越早恢复,成功的几率越高,无法确保能够成功恢复多大比例的文件。

流程图示中的环节6说明:

运行工具 1,对服务器进行一键免疫及补丁操作并重新启动系统。也可以根据操作系统版本,手动选择对应补丁升级。





如果免疫工具运行异常,也可使用工具6、永恒之蓝漏洞端口关闭.zip禁用445端口。 将工具解压后,双击运行"执行我.bat"检查并关闭电脑相关服务和端口,出现以下窗口 为服务已经关闭。



流程图示中的环节7说明:

运行工具1,对服务器进行安全检查,也可以按照操作1的方法进行二次验证。





流程图示中的环节8说明:

管理员确认补丁修复完成,未感染蠕虫后恢复上线。

6.4 如果你是普通电脑用户

步骤一:请阅读附件文档的附件 1《360 针对"永恒之蓝"(蠕虫 WANNACRY)攻击预 警通告》文档以了解整个事件的全貌,掌握应急响应所需要必备知识

步骤二:请准备好工具软件包中的工具 1,这些工具软件已经包含在 360 企业安全为 您提供的安全 U 盘或选择未被感染的电脑从网络上下载,请确保打开 U 盘的写保护功能, 以避免 U 盘遭受感染。

步骤三: 〈流程3 普通电脑用户操作流程〉进行自身设备安全检查及处置流程。





流程4 普通电脑用户操作流程

流程图示中的环节1说明:

断开所属计算机网络连接,并向管理员获取相关工具1

流程图示中的环节2说明:

启动电脑,观察电脑是否感染,如果存在弹出以下页面,则判断已经被感染



💕 Tana DecryptOr 2.0		×
	Ooops, your files have been e	encrypted! Chinese (simpli
	我的电脑出了什么问题?	-
1	忘的一些重要文件被我加密保存了。 照片、图片、文档、压缩包、音频、视频文件 文件都被加密了,因此不能正常打开。	· exe文件等,几乎所有类型的
Payment will be raised on	这和一般文件损坏有本质上的区别。您大可在 保证,没有我们的解密服务,就算老天爷来了	四上找找恢复文件的方法,我敢 也不能恢复这些文档。
5/16/2017 02:26:59	有没有恢复这些文档的方法?	
Time Left 22:22:35:15	当然有可恢复的方法。只能通过我们的解密服 够提供安全有效的恢复服务。 但这是收费的,也不能无限期的推迟。	
Your files will be last on	頃点击 <decrypt> 按钮, 就可以免费恢复一 骗你的。</decrypt>	些又怕。请您 <i>放</i> 心,我是 把 不会
5/20/2017 02:26:59	但想要恢复全部文档,需要付款点费用。 是否随时都可以固定金额付款,就会恢复的吗 对你不利。	3,当然不是,推迟付款时间越长
Time Left (26:22:35:15	股份不利。 最好3天之内付款费用,过了三天费用就会翻 还有,一个礼拜之内未付款,将会永远恢复不 对了,忘了告诉你,对半年以上没钱付款的实	音。 ∵了。 3人,会有活动免费恢复,能否轮 <u>,</u>
<u>About bitcoin</u> <u>How to buy bitcoins?</u>	B bitcoin ACCEPTED HERE Send \$300 worth of bitco 13AM4VW2dhxYgXeQep	in to this address: oHkHSQuy6NgaEb94
Contact Us	Check Payment	Decrypt

请注意:如果你的数据非常关键且无法支付赎金,请不要轻易格式化关键数据所在的 服务器,相应处置请参见第5章5.2

流程图示中的环节3说明:

登记关键信息如下,并关闭计算机

序 号	主机名	IP	MAC 地址	所有 人	联系方式	部门
1	PC-0001	192. 168. 0. 123	00-0C-29-8D-E6-5	张三	138888888888	业务 部

流程图示中的环节4说明:

运行工具 1,对终端进行一键免疫及补丁操作并重新启动系统。也可以根据操作系统版本,手动选择对应补丁升级。





如果免疫工具运行异常,也可使用工具6、永恒之蓝漏洞端口关闭.zip禁用445端口。 将工具解压后,双击运行"执行我.bat"检查并关闭电脑相关服务和端口,出现以下窗口 为服务已经关闭。



流程图示中的环节5说明:

运行工具1,对终端进行安全检查,也可以按照操作1的方法进行二次验证。





流程图示中的环节6说明:

管理员确认补丁修复完成、未感染蠕虫后恢复上线。