

# 周一开机保障指南及工具包



360安全监测与响应中心

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 .....	7
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.....	18
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”，部分设备已完全罢工，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](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
1	360CERT 针对本次攻击的操作指南，包含在不使用安全产品的前提下，如何进行影响范围确定、网络及终端层面的临时抑制方案及相关根治方法及恢复建议。 <a href="http://b.360.cn/assets/doc/OnionWorm_Report.pdf">http://b.360.cn/assets/doc/OnionWorm_Report.pdf</a>	附件 1 360 针对“永恒之蓝”（蠕虫 WannaCry）攻击预警通告
2	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护操作流程及方法 <a href="http://zt.360.cn/1101061855.php?dtid=1101062514&amp;did=490458365">http://zt.360.cn/1101061855.php?dtid=1101062514&amp;did=490458365</a>	附件 2 针对“永恒之蓝”攻击紧急处置手册（蠕虫 WannaCry）
3	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，从如果返回的补丁信息中包含对应的 KB 号，漏洞修复成功。 <a href="http://b.360.cn//main_web/assets/doc/MSID_KBID_lib.xlsx">http://b.360.cn//main_web/assets/doc/MSID_KBID_lib.xlsx</a>	附件 3 微软高危漏洞-MSID 与 KBID 对照表
4	360 追日团队（专业高级威胁追踪溯源团队）针对本次攻击的技术分析报告，包含蠕虫攻击流程、蠕虫利用漏洞分析、相关释放文件分析、勒索加密过程及解密	附件 4 WanaCrypt0r 勒索蠕虫完全分析报告

	<p>过程分析等模块。</p> <p><a href="http://m.bobao.360.cn/learning/detail/3853.html?from=timeline&amp;isappinstalled=1">http://m.bobao.360.cn/learning/detail/3853.html?from=timeline&amp;isappinstalled=1</a></p>	
5	<p>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。</p> <p>其中要注意的是：使用 DNS 诱导的方法时一定要建立一个运行在 80 端口的正常的 HTTP 服务，隔离网用户建议在内部 DNS SERVER 上同时增加相关 DNS 诱导配置。</p> <p><a href="http://bobao.360.cn/interref/detail/109.html">http://bobao.360.cn/interref/detail/109.html</a></p>	附件 5 360 防火墙产品针对“永恒之蓝”勒索蠕虫的防护方案 v3.1
6	<p>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、补丁升级等多个方面的防护操作流程及方法。</p> <p><a href="http://b.360.cn//main_web/assets/doc/OnionWorm_protect.docx">http://b.360.cn//main_web/assets/doc/OnionWorm_protect.docx</a></p>	附件 6 360 天擎产品针对“永恒之蓝”勒索蠕虫病毒的防护方案 1.13
7	<p>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、未购买防火墙模块的情况下终端加固操作流程及方法。</p> <p><a href="http://bbs.360.cn/forum.php?mod=viewthread&amp;tid=14974137">http://bbs.360.cn/forum.php?mod=viewthread&amp;tid=14974137</a></p>	附件 7 360 虚拟化安全产品“永恒之蓝”应急处置办法

## 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 服务关闭和各系统下 MS17-010 漏洞检测与修复于一体。	NSAScan.exe

	<p>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： <a href="http://b.360.cn/other/onionwormfix">http://b.360.cn/other/onionwormfix</a></p>	
2	<p>360 勒索蠕虫免疫工具，可用于主机免疫勒索蠕虫的破坏过程。下载地址： <a href="http://b.360.cn/other/onionwormimmune">http://b.360.cn/other/onionwormimmune</a></p>	OnionWormImmune
3	<p>勒索软件漏洞扫描工具，可通过扫描端口远程或本地检测主机是否存在漏洞。该工具具有一定风险性，建议寻求 360 企业安全技术支持获取该工具及服务支持。开源工具下载地址：<a href="https://github.com/RiskSense-Ops/MS17-010">https://github.com/RiskSense-Ops/MS17-010</a></p>	ms17010detectv4
4	<p>360 勒索蠕虫文件恢复工具(非解密)，有可能恢复一部分被加密的文件，用于紧急数据恢复，存在一定概率无法恢复。下载地址： <a href="https://dl.360safe.com/recovery/RansomRecovery.exe">https://dl.360safe.com/recovery/RansomRecovery.exe</a></p>	RansomRecovery.exe
5	<p>360 安全卫士个人版在线安装程序，可用于联网环境下的补丁升级及安全防护。下载地址： <a href="http://down.360safe.com/inst.exe">http://down.360safe.com/inst.exe</a></p>	inst==.exe
6	<p>360 禁用 445 端口的脚本工具，可禁用 Server 服务并添加 ipsec 规则禁止 445 端口访问 <a href="http://dl.b.360.cn/tools/EternalBlueBat.zip">http://dl.b.360.cn/tools/EternalBlueBat.zip</a></p>	永恒之蓝漏洞端口关闭.zip



## 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

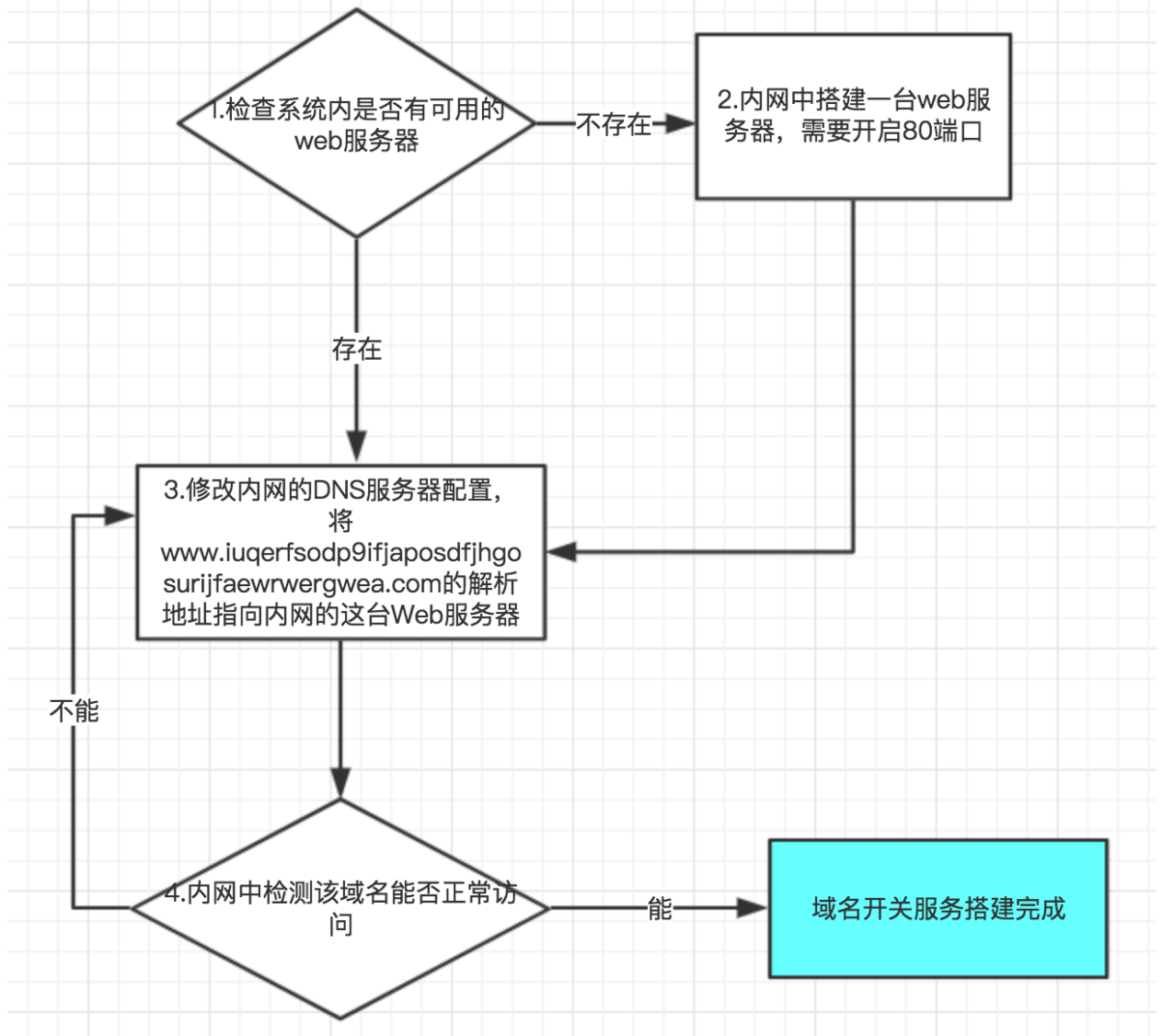
## 第6章 安全开机操作指南

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1 网络管理员操作流程

**流程图示中的环节 1 说明：**

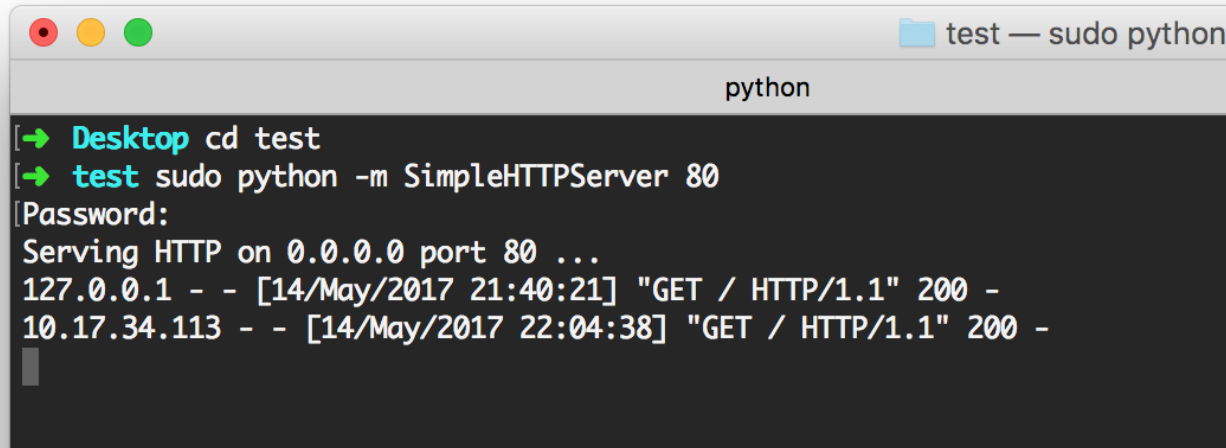
检查系统中是否有可用的 web 服务器，监听的端口需要是 80，保证该服务器能够正确响应根目录的 Get 请求，即保证 web 服务器正常工作。

**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：

## Directory listing for /



```
python
[→ Desktop cd test
[→ test sudo python -m SimpleHTTPServer 80
[Password:
Serving HTTP on 0.0.0.0 port 80 ...
127.0.0.1 - - [14/May/2017 21:40:21] "GET / HTTP/1.1" 200 -
10.17.34.113 - - [14/May/2017 22:04:38] "GET / HTTP/1.1" 200 -
```

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。

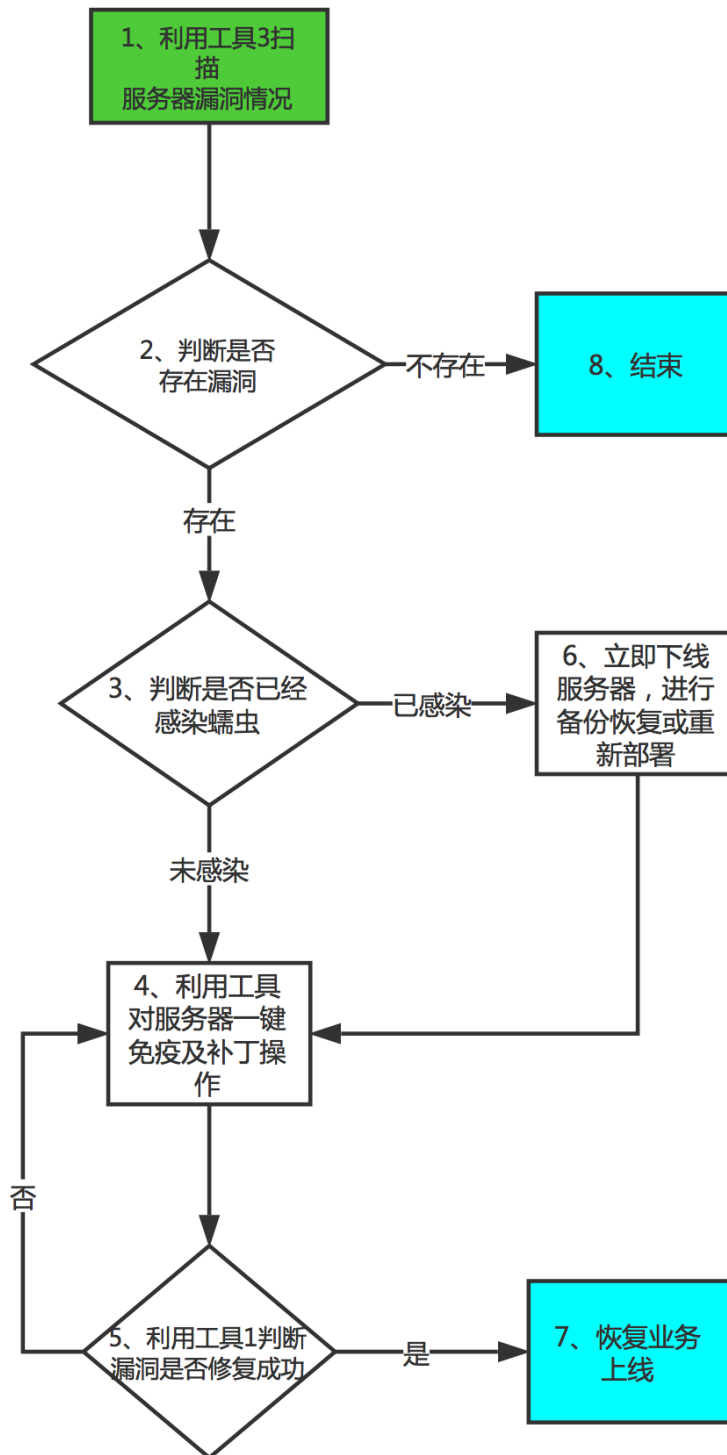
## 6.2 如果你是服务器管理员

**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：

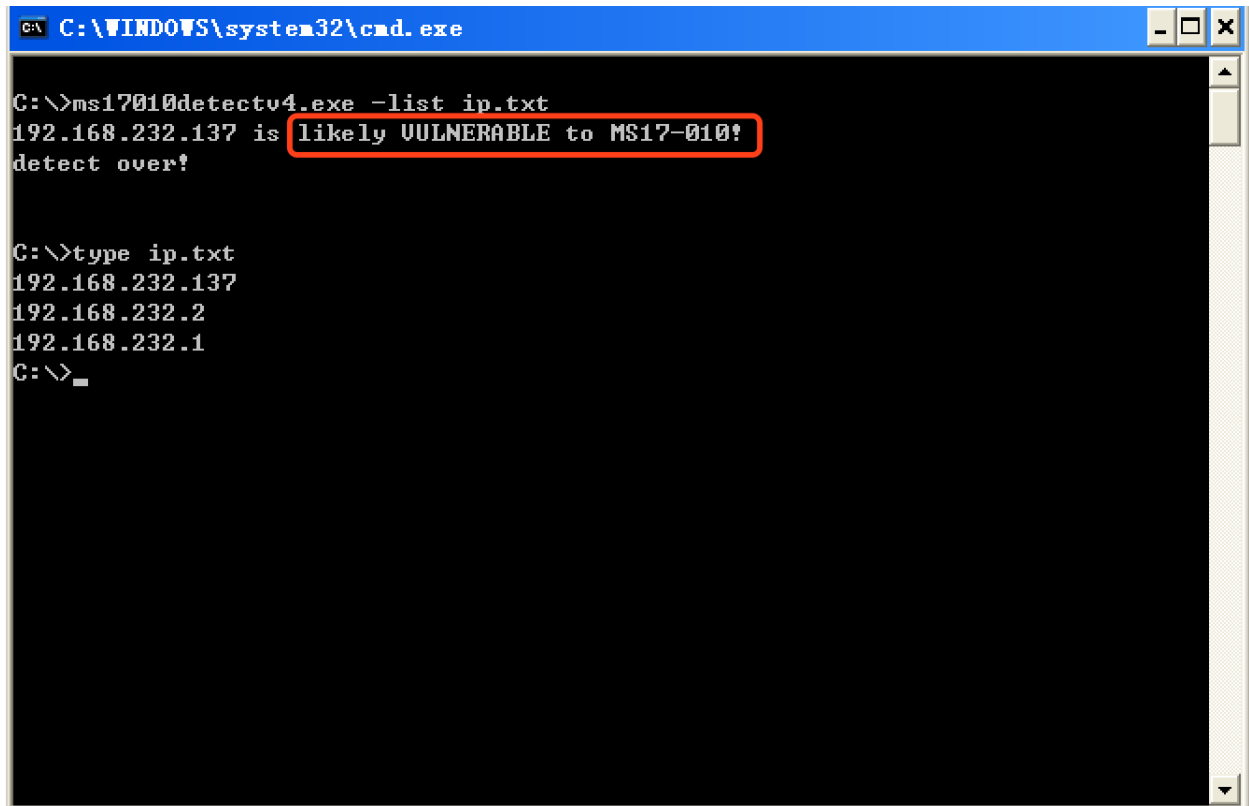
ms17010detectv4.exe 192.168.1.1 扫描单个 IP

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

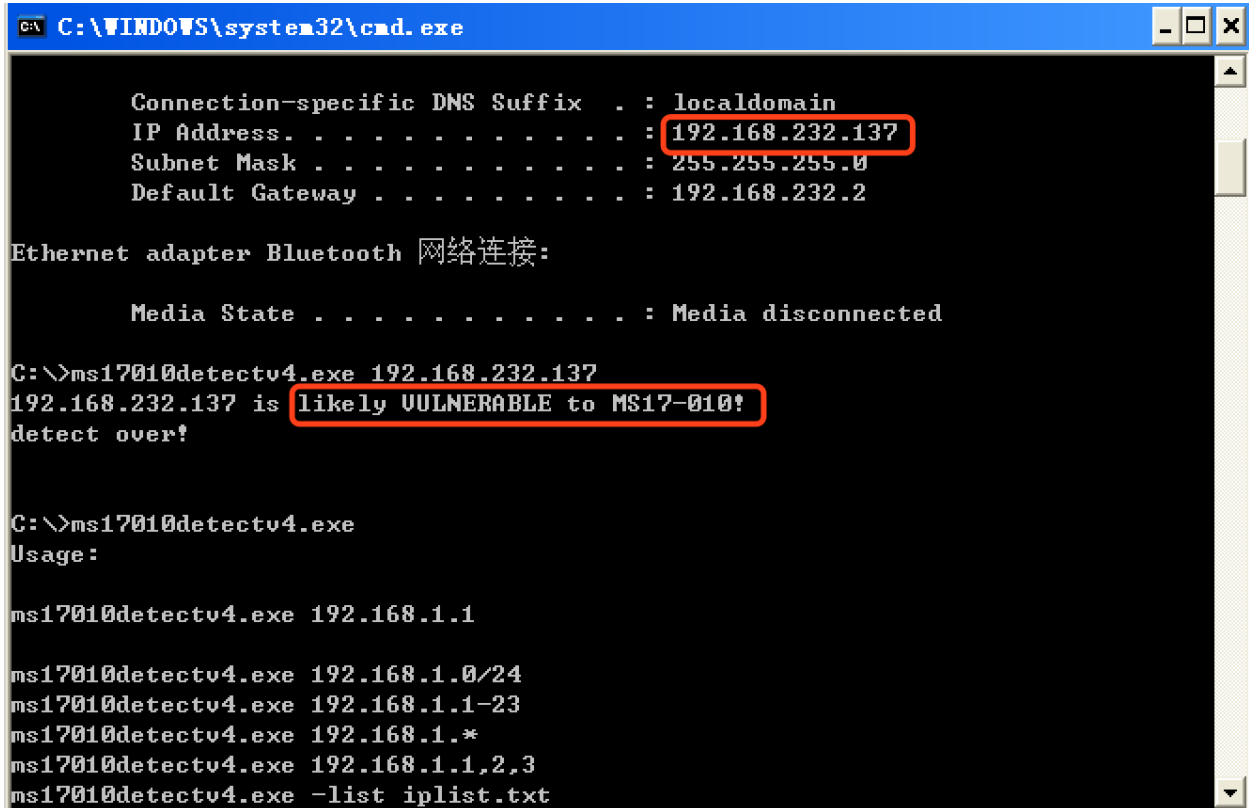


```
C:\WINDOWS\system32\cmd.exe
C:\>ms17010detectv4.exe -list ip.txt
192.168.232.137 is likely VULNERABLE to MS17-010!
detect over!

C:\>type ip.txt
192.168.232.137
192.168.232.2
192.168.232.1
C:\>
```

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

Connection-specific DNS Suffix . : localdomain
IP Address. . . . . : 192.168.232.137
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.232.2

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：



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。



×



## 勒索蠕虫漏洞修复工具

- 该漏洞可用来远程攻破全球约70%的Windows电脑
- 不需要用户任何操作，任何联网机器（包括企业内网）都可能被远程攻破
- 已有勒索蠕虫WannaCry利用“永恒之蓝”漏洞攻击企业内网

ⓘ 经检测，发现电脑存在被“永恒之蓝”勒索蠕虫利用的漏洞。该蠕虫攻击事件已经造成非常严重的现实危害，各类规模的企业内网也已经面临此类威胁，请立即修复。

立即修复

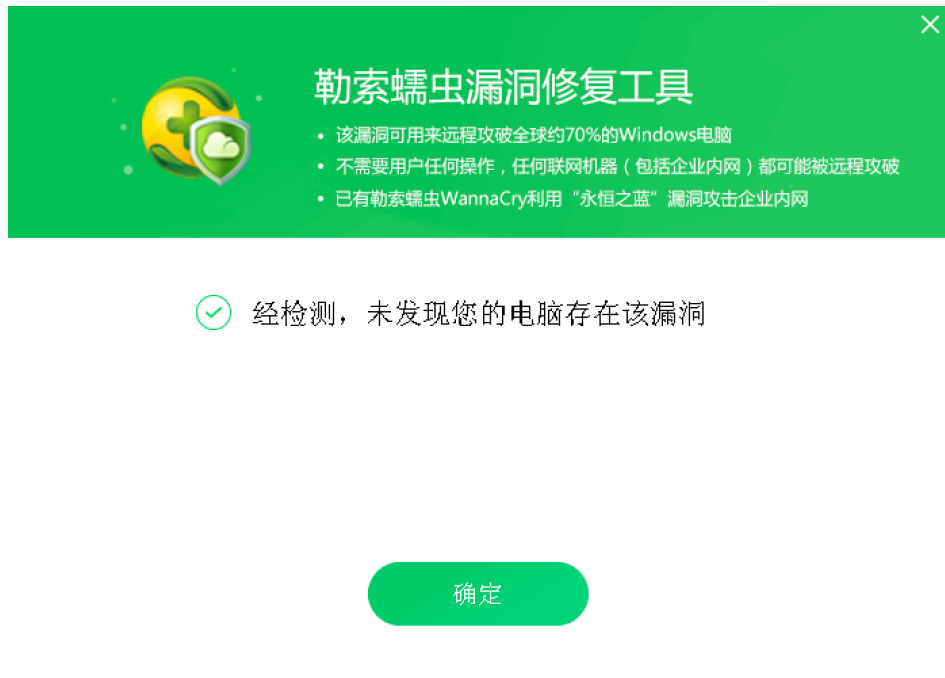
如果免疫工具运行异常，也可使用工具6、永恒之蓝漏洞端口关闭.zip禁用445端口。将工具解压后，双击运行“执行我.bat”检查并关闭电脑相关服务和端口，出现以下窗口为服务已经关闭。

```
Server 服务正在停止。
Server 服务已成功停止。
[SC] ChangeServiceConfig 成功

"Server没有运行"
[SC] ChangeServiceConfig 成功
```

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：

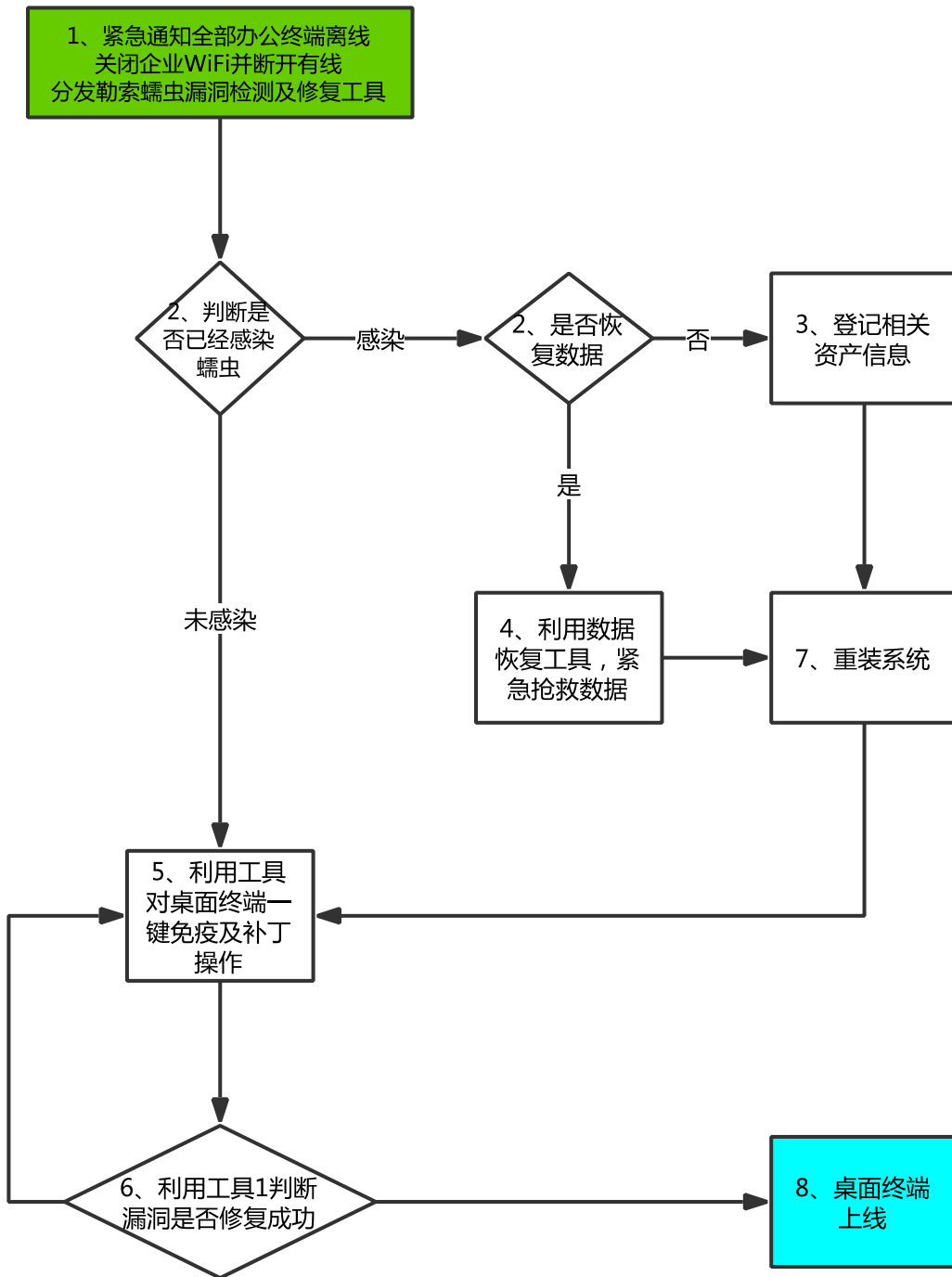
经业务部门确认稳定后重新上线。

## 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：



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



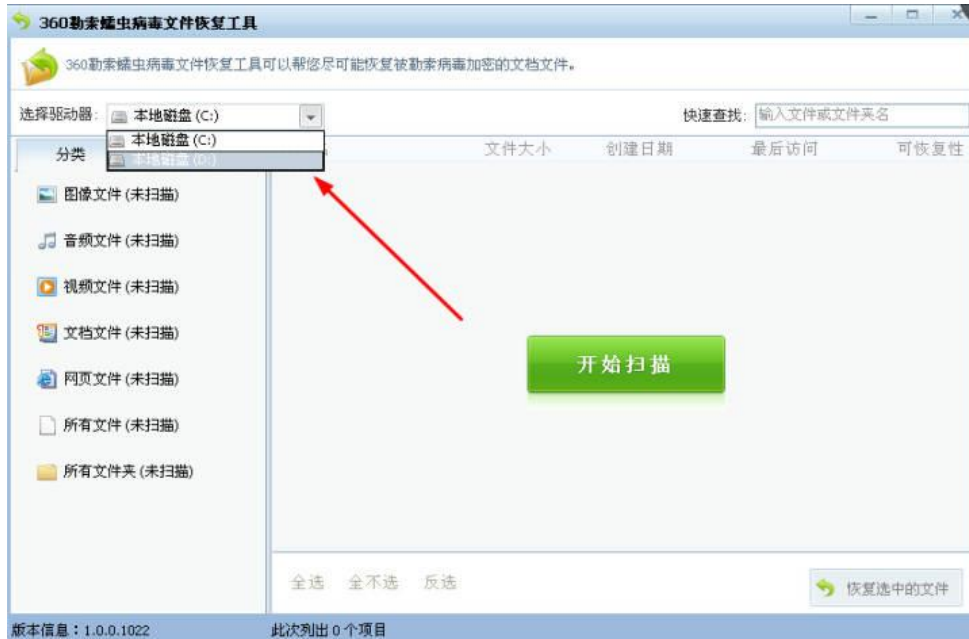
2) 使用 360 木马查杀功能, 清除全部木马, 防止反复感染。



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





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。



×



## 勒索蠕虫漏洞修复工具

- 该漏洞可用来远程攻破全球约70%的Windows电脑
- 不需要用户任何操作，任何联网机器（包括企业内网）都可能被远程攻破
- 已有勒索蠕虫WannaCry利用“永恒之蓝”漏洞攻击企业内网

ⓘ 经检测，发现电脑存在被“永恒之蓝”勒索蠕虫利用的漏洞。该蠕虫攻击事件已经造成非常严重的现实危害，各类规模的企业内网也已经面临此类威胁，请立即修复。

立即修复

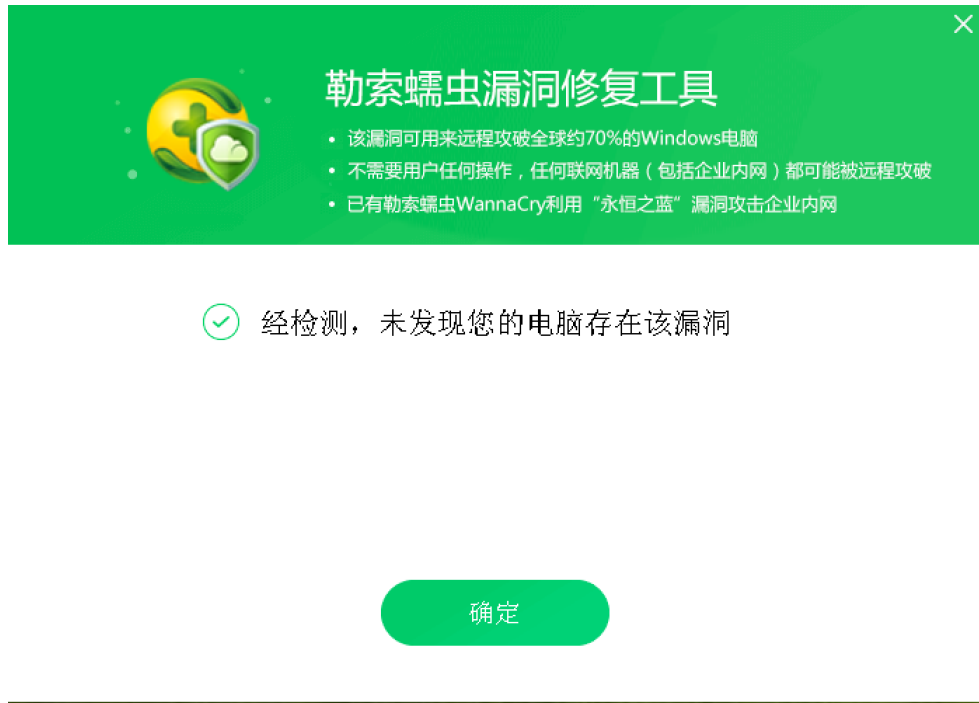
如果免疫工具运行异常，也可使用工具6、永恒之蓝漏洞端口关闭.zip禁用445端口。将工具解压后，双击运行“执行我.bat”检查并关闭电脑相关服务和端口，出现以下窗口为服务已经关闭。

```
Server 服务正在停止。
Server 服务已成功停止。
[SC] ChangeServiceConfig 成功

"Server没有运行"
[SC] ChangeServiceConfig 成功
```

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:

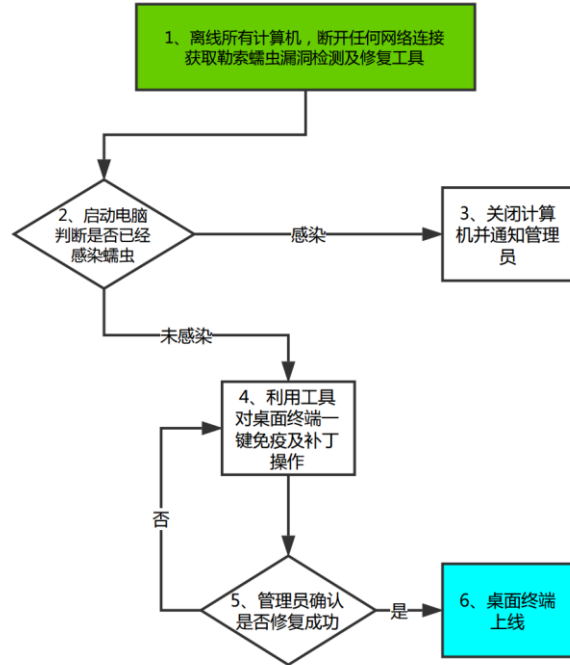
管理员确认补丁修复完成, 未感染蠕虫后恢复上线。

## 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



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	13888888888	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。



## 勒索蠕虫漏洞修复工具

- 该漏洞可用来远程攻破全球约70%的Windows电脑
- 不需要用户任何操作，任何联网机器（包括企业内网）都可能被远程攻破
- 已有勒索蠕虫WannaCry利用“永恒之蓝”漏洞攻击企业内网

! 经检测，发现电脑存在被“永恒之蓝”勒索蠕虫利用的漏洞。该蠕虫攻击事件已经造成非常严重的现实危害，各类规模的企业内网也已经面临此类威胁，请立即修复。

立即修复

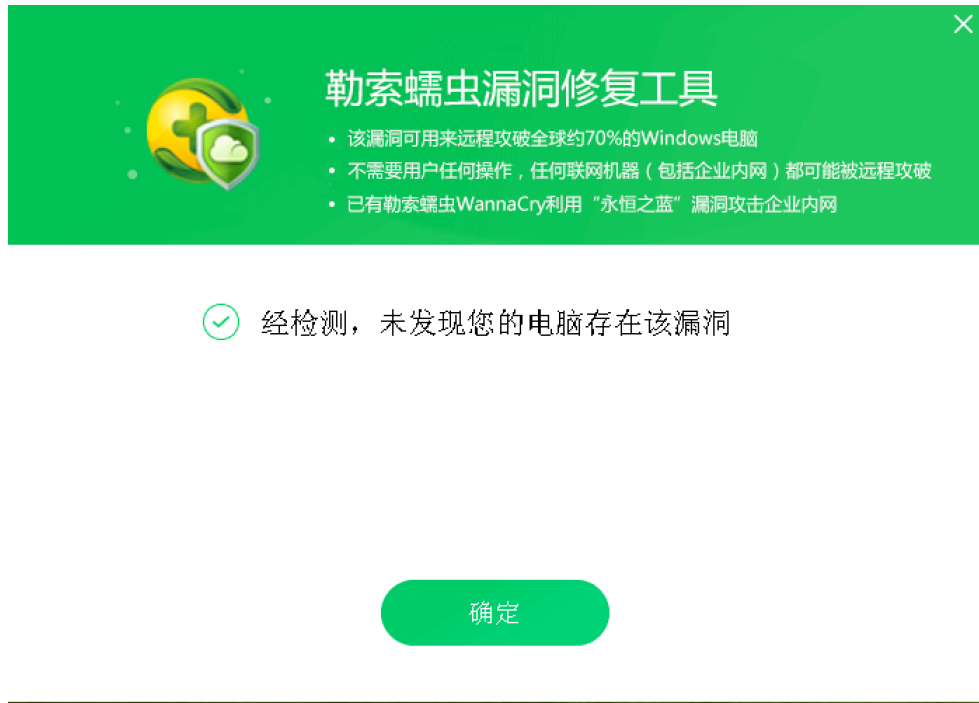
如果免疫工具运行异常，也可使用工具6、永恒之蓝漏洞端口关闭.zip禁用445端口。将工具解压后，双击运行“执行我.bat”检查并关闭电脑相关服务和端口，出现以下窗口为服务已经关闭。

```
Server 服务正在停止。
Server 服务已成功停止。
[SC] ChangeServiceConfig 成功

"Server没有运行"
[SC] ChangeServiceConfig 成功
```

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。