Petya 勒索病毒

安全预警通告

360安全监测与响应中心

2017 年 06 月 28 日

第1章 安全通告

尊敬的客户：

北京时间 2017 年 6 月 27 日晚，据外媒消息，乌克兰、俄罗斯、印度、西班牙、法国、英国以及欧洲多国正在遭遇 Petya 勒索病毒袭击，政府、银行、电力系统、通讯系统、企业以及机场都不同程度的受到了影响。

此次黑客使用的是 Petya 勒索病毒的变种 Petwarp，使用的攻击方式和 WannaCry 相同，360 天擎（企业版）和 360 安全卫士（个人版）可以查杀该病毒。

据悉，该病毒和勒索软件很类似，都是远程锁定设备，然后索要赎金。据赛门铁克最新发布的消息显示此次攻击时仍然使用了永恒之蓝勒索蠕虫，还会获取系统用户名与密码进行内网传播。

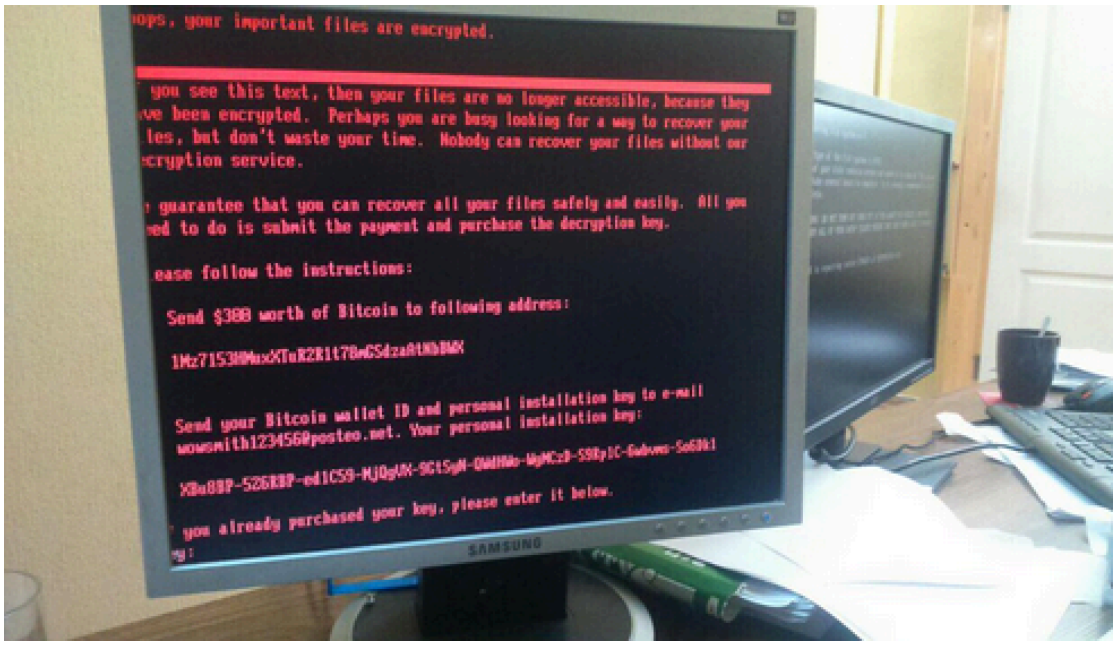
360 安全监测与响应中心也将持续关注该事件进展，并第一时间为您更新该漏洞信息。

第2章 事件信息

2.1 事件描述

Petya 和传统的勒索软件不同，不会对电脑中的每个文件都进行加密，而是通过加密硬盘驱动器主文件表（MFT），使主引导记录（MBR）不可操作，通过占用物理磁盘上的文件名，大小和位置的信息来限制对完整系统的访问，从而让电脑无法启动。如果想要恢复，需要支付价值相当于 300 美元的比特币。

被感染的机器屏幕会显示如下的告知付赎金的界面：



2.2 风险等级

360 安全监测与响应中心风险评级为：危急

第3章 处置建议

3.1 安全操作提示

从目前掌握的情况来看：

1. 不要轻易点击不明附件，尤其是 rtf、doc 等格式，可以安装 360 天擎（企业版）和 360 安全卫士（个人版）等相关安全产品进行查杀。

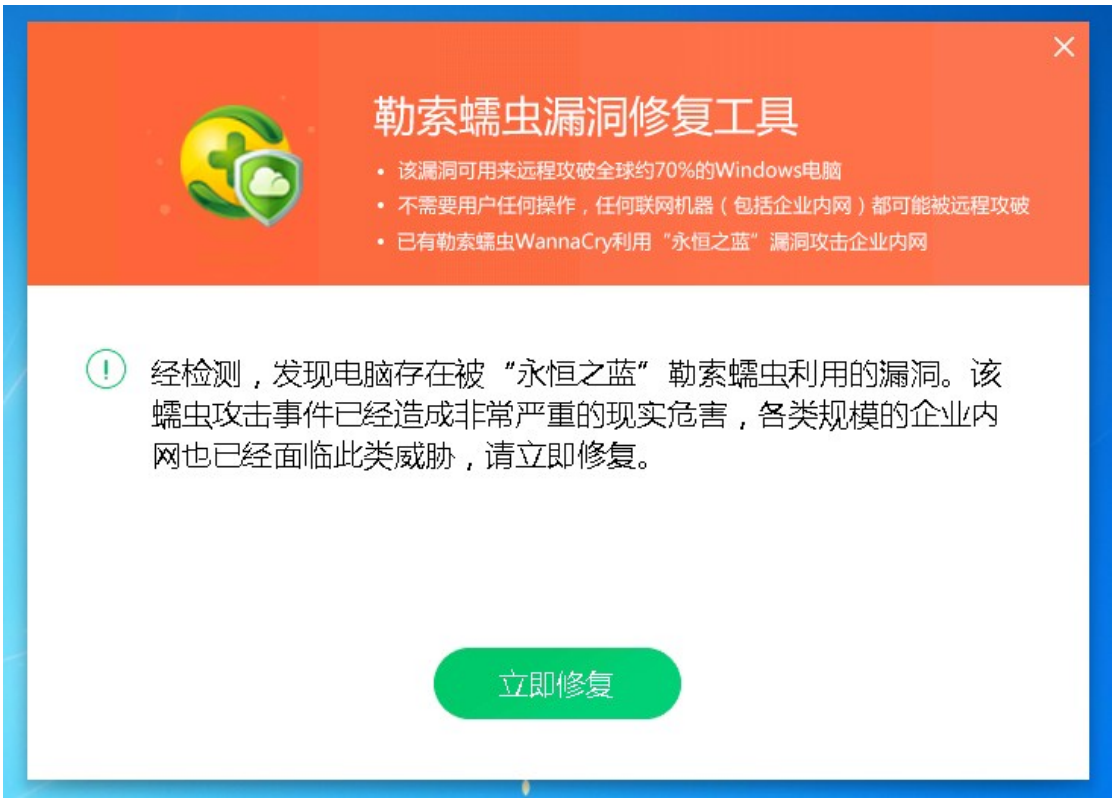
2. 及时更新 windows 系统补丁，具体修复方案请参考“永恒之蓝”漏洞修复工具。

3. 内网中存在使用相同账号、密码情况的机器请尽快修改密码，未开机的电脑请确认口令修改完毕、补丁安装完成后再进行联网操作。

3.2 修复工具

360 企业安全天擎团队开发的勒索蠕虫漏洞修复工具，可根本解决勒索蠕虫利用 MS17-010 漏洞带来的安全隐患。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。可在离线网络环境下一键式修复系统存在的 MS17-010 漏洞，工具下载地址：

http://b.360.cn/other/onionwormfix



3.3 缓解措施

关闭 TCP 135 端口

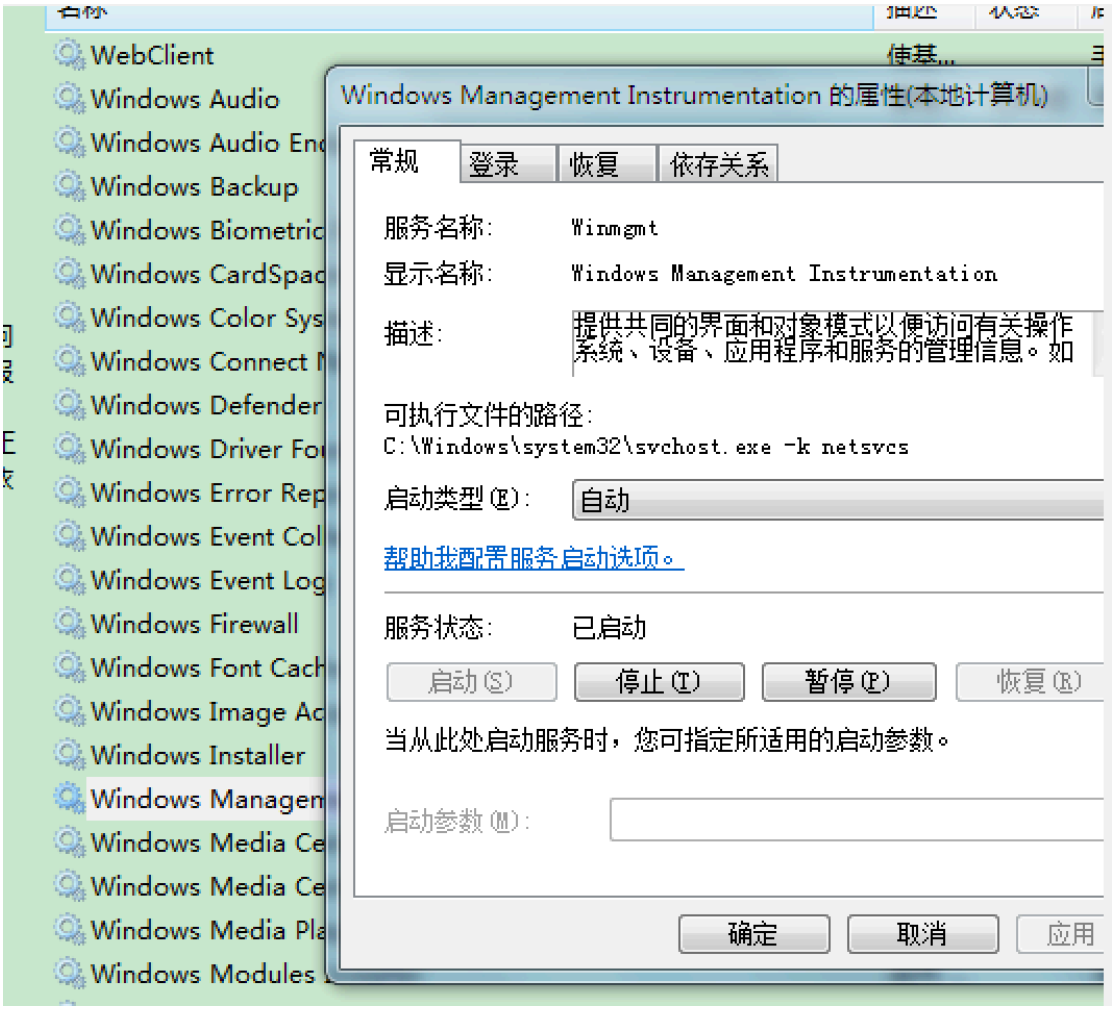
建议在防火墙上临时关闭 TCP 135 端口以抑制病毒传播行为。

停止服务器的 WMI 服务

WMI（Windows Management Instrumentation Windows 管理规范）是一项核心的 Windows 管理技术 你可以通过如下方法停止 ：

在服务页面开启 WMI 服务。在开始-运行，输入 services.msc，进入服务。或者，在控制面板，查看方式选择大图标，选择管理工具，在管理工具中双击服务。

在服务页面，按 W，找到 WMI 服务，找到后，双击 ，直接点击停止服务即可，如下图所示：


WebClient
Windows Audio
Windows Backup
Windows Biometric
Windows Color Sys
Windows Connect
Windows Defender
Windows Driver Fo
Windows Error Rep
Windows Event Col
Windows Event Log
Windows Firewall
Windows Font Cach
Windows Image Ac
Windows Installer
Windows Media Ce
Windows Media Ce
Windows Media Pla
Windows Modules
Windows Management Instrumentation 的属性(本地计算机)
常规
登录
恢复
依存关系
服务名称: Winmgmt
显示名称: Windows Management Instrumentation
描述: 提供共同的界面和对象模式以便访问有关操作系统、设备、应用程序和服务的管理信息。如
可执行文件的路径:
C:\Windows\system32\svchost.exe -k netsvcs
启动类型(E): 自动
帮助我配置服务启动选项。
服务状态: 已启动
启动(S)
停止(T)
暂停(P)
恢复(R)
当从此处启动服务时，您可指定所适用的启动参数。
启动参数(M):
确定
取消
应用