360 针对“永恒之蓝”（蠕虫 WannaCry）

攻击预警通告

第十一次更新

360安全监测与响应中心

2017 年 05 月 18 日

目录

第1章 事件描述

1.1 事件概述

2017 年 5 月 12 日晚上起国内多处高校网络和企业内网出现蠕虫病毒传播的勒索软件感染爆发情况，受感染系统的磁盘文件会被病毒加密，提示用户支付高额赎金才能解密恢复文件。如果在规定时间内不支付，文件数据就会被“撕票”，在企业环境下系统应用文件的破坏很多时候直接导致业务中断。

根据 360 企业安全集团的研判，事件是由不法分子利用上月泄露的 NSA 黑客数字武器库中“永恒之蓝”工具发起蠕虫病毒攻击进行勒索的恶性事件，我们把相应的蠕虫病毒命名为“永恒之蓝”蠕虫（也称为 WannaCry）。不法分子构造的恶意代码会扫描攻击存在漏洞的 Windows 机器，无需用户任何操作，只要开机上网，不法分子就能在电脑和服务器中植入恶意代码加密用户数据实施数字勒索。

由于以前国内多次爆发利用 SMB 服务传播的蠕虫，部分运营商在主干网络上封禁了相关 445 端口，但是教育网及大量企业内网并没有此限制而且并未及时安装补丁，所以仍然存在大量易受攻击的电脑，导致目前蠕虫的泛滥。目前蠕虫存在几个变种，有消息说已有新的感染能力更强的变种出现。

2017 年 5 月 18 日，360 威胁情报中心关注到一个疑似通过利用 NSA 网络攻击武器库工具进行分发的恶意代码的样本，对其进行了分析。分析报告：

http://b.360.cn/assets/doc/uiwix_report.docx

360 威胁情报中心正在持续密切关注，有新变化会随时更新本通告。

1.2 影响对象

“永恒之蓝”勒索蠕虫针对的是微软 Windows 操作系统，它利用了 Windows 系统的一个远程命令执行漏洞，微软桌面版本操作系统：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、

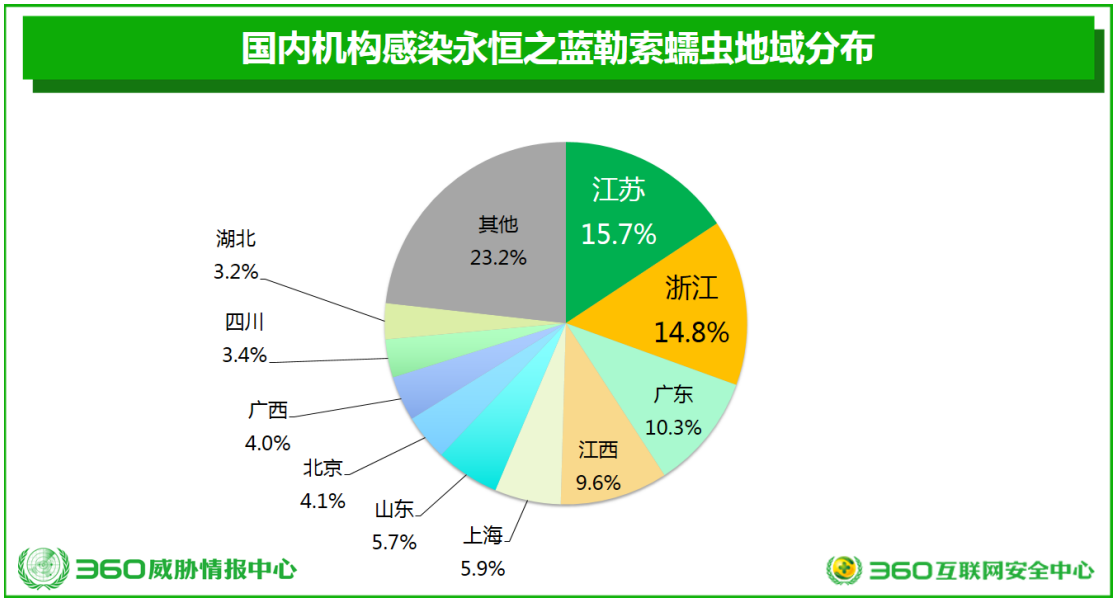
Windows Server 2012、Windows Server 2016 等均受影响。

虽然微软早已在 3 月份就发布了针对 Windows 7 及以上版本操作系统的相关安全漏洞补丁 MS17-010，但由于许多系统未及时安装更新，导致本次蠕虫爆发时未受到恰当的保护。此外，对于 Windows XP、2003 等老旧操作系统，微软已不再提供安全更新，而国内大量的教育机构、政务办公系统、业务应用终端仍旧在使用 Windows XP 或 2003 系统，这也是造成本次蠕虫爆发的重要原因。

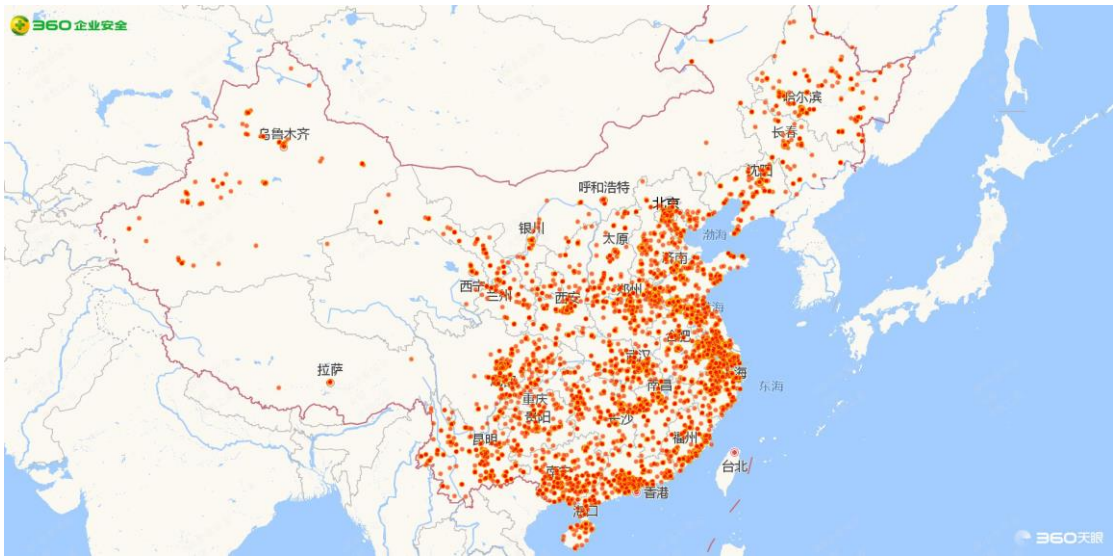
1.3 当前影响

该勒索软件同时具备加密勒索功能和内网蠕虫传播能力，属于新型的勒索软件家族，危害极大。该病毒能够轻而易举的入侵具有相关漏洞的 Windows 计算机中的任何一台，目前监测到的受感染 IP 已超过 75000 个。受感染系统在感染后即被锁定，所有文件被加密，用户被要求支付价值 300 美元的比特币才能解锁，不能按时支付赎金的系统会被销毁数据，造成严重损失。

从 2017 年 5 月 12 日开始，仅仅几个小时，该勒索软件已经攻击了近百个国家，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上千家企业及公共组织，至少 1600 家美国组织，11200 家俄罗斯组织都受到了攻击。据 360 威胁情报中心监测，全球超 10 万台机器中招，国内至少有 28388 个机构被感染，覆盖了国内几乎所有地区，在受影响的地区中，江苏、浙江、广东、江西、上海、山东、北京和广西排名前八位。攻击所影响的影响范围遍布高校、火车站、自助终端、邮政、加油站、医院、政府办事终端等多个领域，不仅破坏大量高价值数据，而且直接导致很多公共服务无法正常工作。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。本次攻击受影响系统在国内的省份分布如下:



此次勒索蠕虫病毒爆发被国内外安全业专家认为是同类中危害程度空前的攻击之一，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、教育网、政府机构已面临此类威胁并有爆发态势。下面是 360 威胁情报中心对全国范围内受影响者的实时监控图：



第2章 处置建议

2.1 确认影响范围

- **潜在受影响系统定位**

使用开源（OpenVAS）或商业漏洞扫描工具检查内网，发现所有开放 445 SMB 服务端口的被认定存在漏洞终端和服务器，对于 Win7 及以上版本的系统确认是否安装了 MS17-010 补丁，如没有安装则受威胁影响；Win7 以下的 Windows XP/2003 如果没有安装 KB4012598 补丁，则也受漏洞的影响。

- **已感染蠕虫系统发现**

被感染的机器屏幕会显示如下的告知付赎金的界面：

360 企业安全天眼的未知威胁感知系统已添加蠕虫相关的威胁情报，自动更新即可检测；天眼流量探针可及时检测针对 MS17-010 漏洞的攻击，请将规则升级到最新版本。

2.2 根治方法

对于Win7及以上版本的操作系统，目前微软已发布补丁MS17-010修复了“永恒之蓝”攻击的系统漏洞，请立即电脑安装此补丁。

对于 Windows XP、2003 等微软按计划已不再提供安全更新的机器，针对本次影响巨大的网络攻击事件，微软特别提供了补丁，请到如下网址下载安装：

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

基于攻击面最小化的安全实践，建议用户关闭并非必需使用的 Server 服务，操作方法见 应急处置 节。

2.3 应急处置

- **网络层面**

目前利用漏洞进行攻击传播的蠕虫开始泛滥，360 企业安全强烈建议网络管理员在网络边界的防火墙上阻断 445 端口的访问，如果边界上有 IPS 和 360 新一代智慧防火墙之类的设备，请升级设备的检测规则到最新版本并设置相应漏洞攻击的阻断，也可以在智慧防火墙上配置临时的 DNS 诱导配置，直到确认网内的电脑已经安装了 MS17-010 补丁或关闭了 Server 服务。

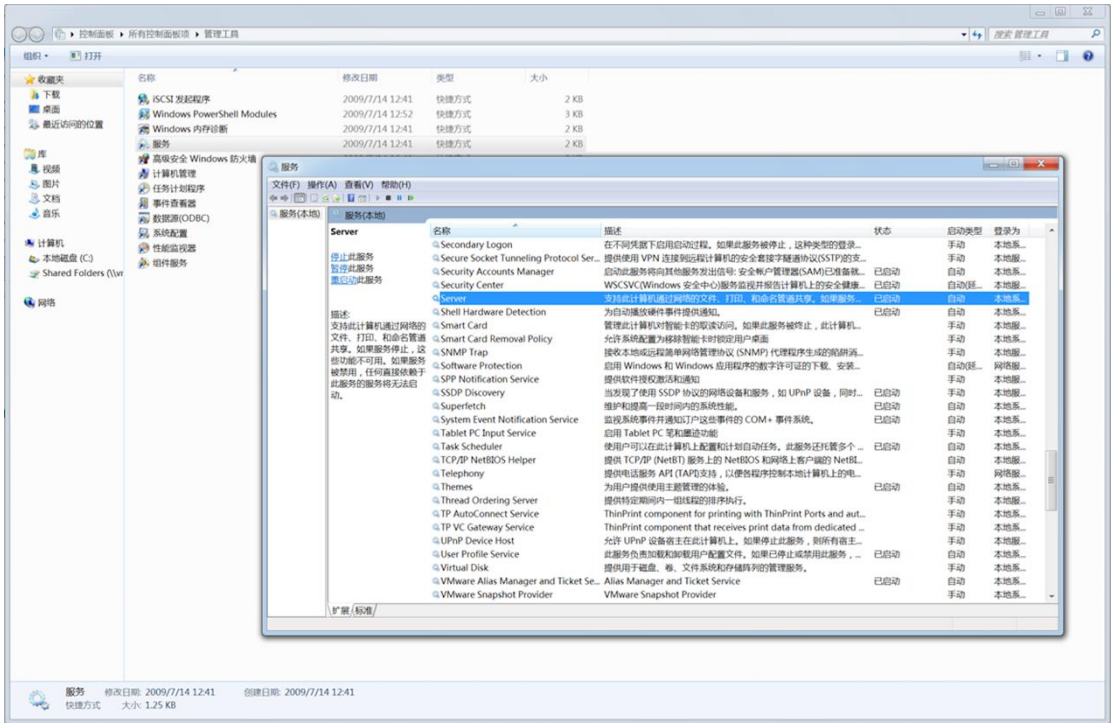
- **终端层面**

暂时关闭 Server 服务。

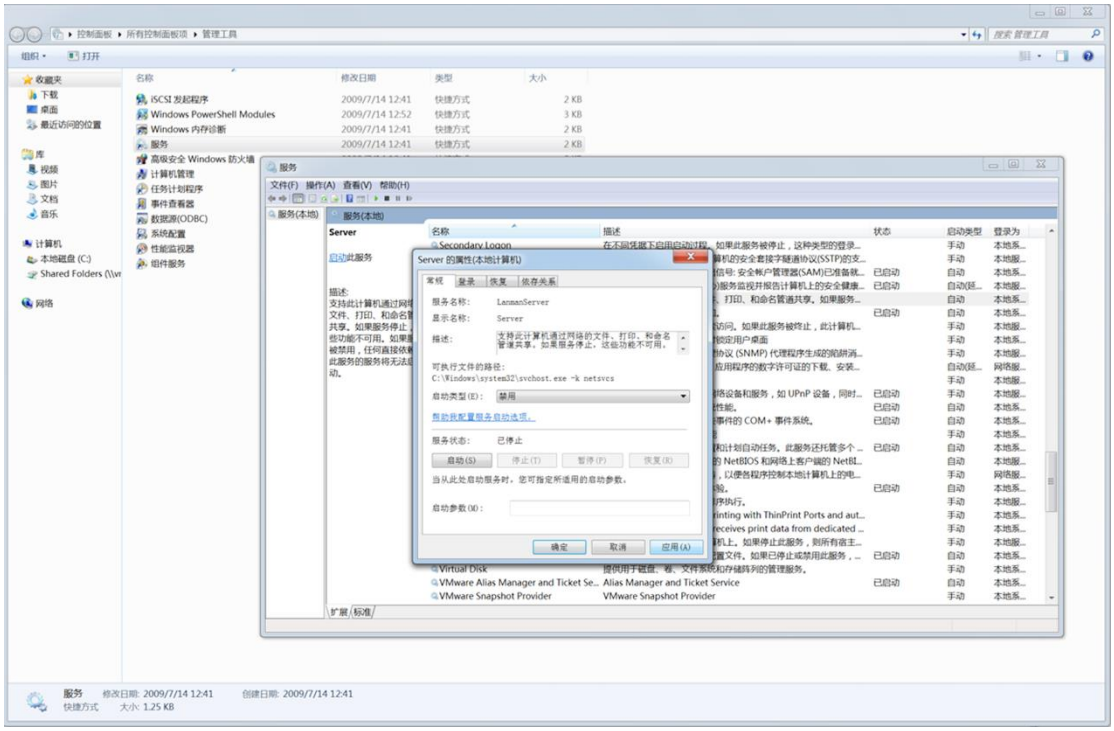
检查系统是否开启 Server 服务，以 Win7 系统为例，其他系统类似：

打开 开始 按钮，选择 控制面板，选择 管理工具， 双击 服务

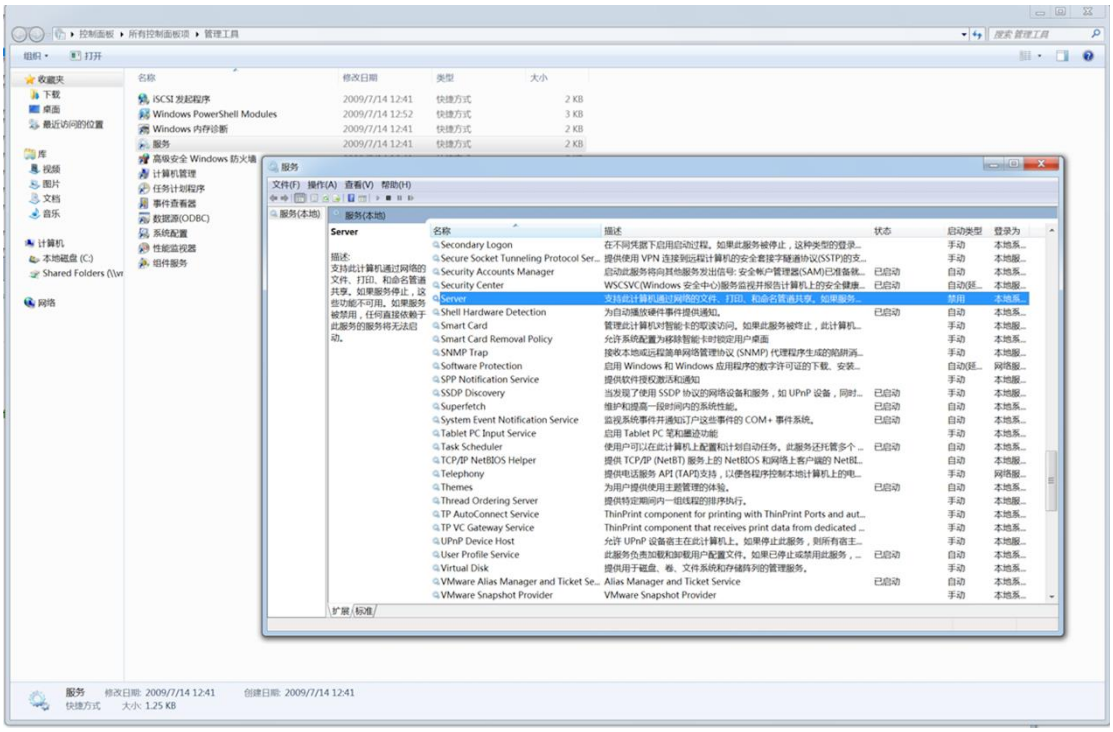
在出来选择框中选择 Server ，如果如下图，状态 为 已启动 ，则当前 Server 服务为启动状态，需要加以关闭。



如果如上述 Server 服务为当前开启状态，右键点击 Server 条目，选择 属性，在出来的对话框中点击 停止（T） 按钮，以关闭服务，在 启动类型 下拉框中选择 禁用 ，点击右下角的 应用（A） ，完成配置的修改。界面情况如下图：



完成配置以后不受漏洞影响的状态如下，状态 列为空，启动类型 列为 禁用：



最好能重启系统以确保配置生效。

● 感染处理

对于已经感染勒索蠕虫的机器建议立即隔离处置，避免其进一步攻击其他网内系统。

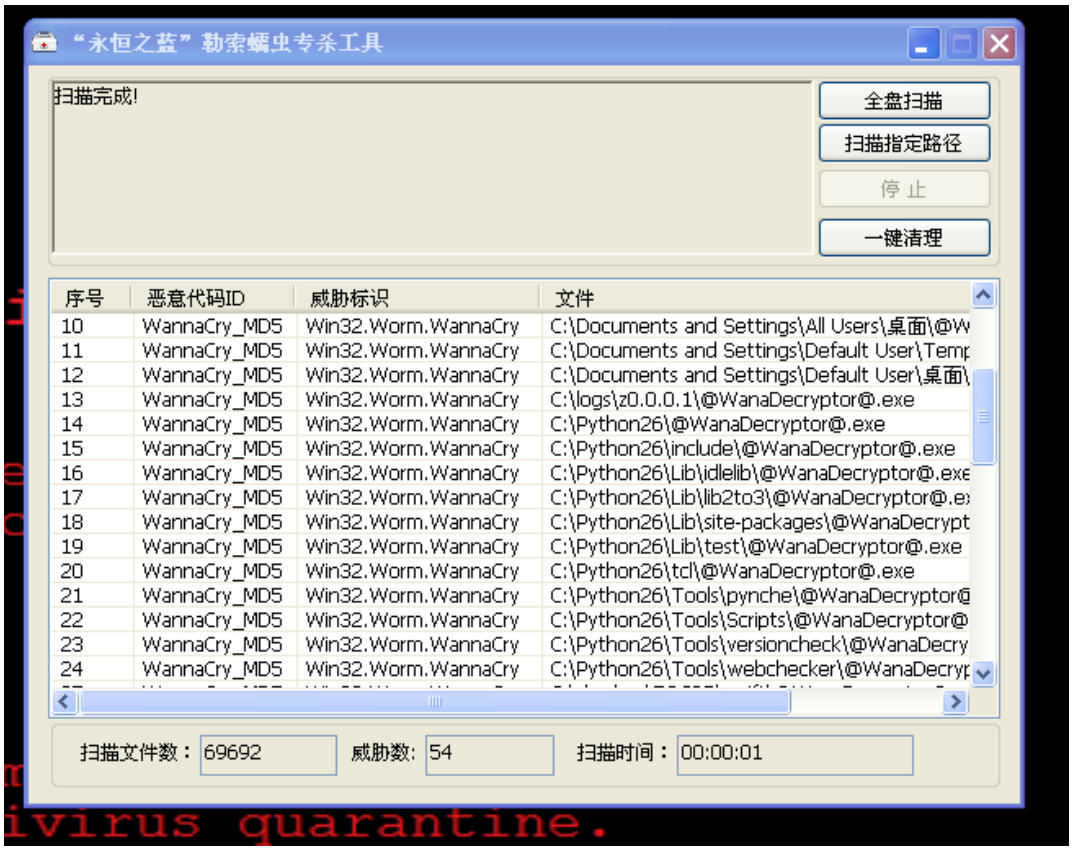
360 公司自 14 日凌晨首家发布恢复工具后，进一步挖掘病毒加密逻辑漏洞，多重算法深度关联出可恢复文件，发布了 360“勒索病毒文件恢复工具 2.0”，经验证，360“勒索病毒文件恢复工具 2.0”成功率遥遥领先于其他数据恢复类产品，工具下载地址：

http://dl.360safe.com/recovery/RansomRecovery.exe

360“勒索病毒文件恢复工具 2.0”详细教程：

步骤一：请在断网情况下使用专杀工具对电脑进行杀毒。

专杀工具下载地址：http://b.360.cn/other/onionwormkiller

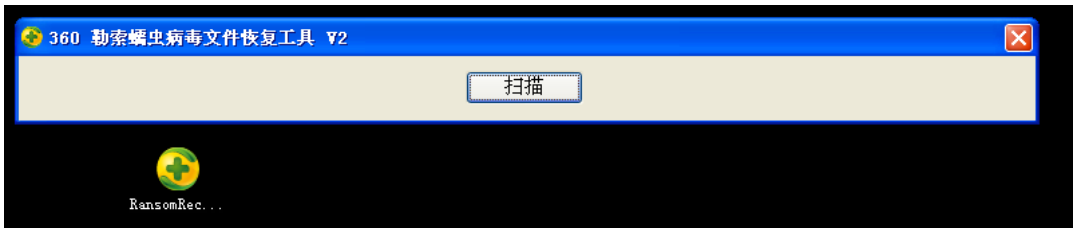


步骤二：请使用勒索蠕虫漏洞修复工具对相关漏洞进行修复。

勒索蠕虫漏洞修复工具下载地址：http://b.360.cn/other/onionwormfix

步骤三：漏洞修复完成后请使用勒索病毒文件恢复工具 2.0 进行文件恢复。

工具下载地址：http://dl.360safe.com/recovery/RansomRecovery.exe



步骤四：选择恢复文件所到的目录即可，建议将文件恢复到 U 盘或移动硬盘中。

● 防护工具

针对目前的复杂事件处理细节，360 企业安全专门发布了《针对“永恒之蓝”攻击紧急处置手册（蠕虫 WannaCry）》，其中包含了更详细的操作处理步骤和 360 提供的特别工具。请到如下网址下载：

http://zt.360.cn/1101061855.php?dtid=1101062514&did=490458365

对此，360 企业安全天擎团队提供了系统免疫工具，在电脑上运行以后，现有蠕虫将不会感染系统。“永恒之蓝”勒索蠕虫免疫工具已更新至 1.0.0.1020 版：

1. 增加删除 WannaCry 服务的功能；
2. 增加对 UIWIX 病毒的免疫；
3. 增加劫持的域名

免疫工具下载地址：http://b.360.cn/other/onionwormimmune

另外，360 企业安全天擎团队还开发了一款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。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。

该工具已完成了一次版本更新，此次更新包括：

1. 解决未关闭 lanmanserver 导致部分环境 445 端口未关闭的问题；
2. 解决 server 2008 r2 系统判断问题；
3. 解决补丁修复配置带上了月度汇总更新造成重复提示的问题；
4. 解决一些小 bug

已经过 server2003 sp2、server 2008 x86 sp2、server 2008 R2 X64 sp1、server2012、server2012 r2 几个系统的完整测试。更新后的主要的表现是解决“用工具处理过一次之后，重启扫描仍然会出现”这个问题。下载地址：

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

360 企业安全新一代智慧防火墙（NSG3000/5000/7000/9000 系列）和下一代极速防火墙（NSG3500/5500/7500/9500 系列）产品系列，通过更新 IPS 特征库和应用识别特征库已经完成了蠕虫变种的防护和识别，强烈建议用户尽快将 IPS 特征库及应用识别特征库均升级至“20170513”版本。并且，针对目前流传的蠕虫，可以在防火墙中临时配置 DNS 诱导，使病毒生效前自动退出。

360 网康上网行为管理 ICG 产品系列通过更新应用协议特征库，已经完成了蠕虫变种的识别，建议用户尽快将应用协议特征库升级至 232 期，从而检测和阻断蠕虫的传播或攻击。

2.4 长效措施

建议针对重要业务系统立即进行数据备份，针对重要业务终端进行系统镜像，制作足够的系统恢复盘或者设备进行替换。

第3章 相关分析

3.1 事件前情

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。本次攻击不法分子利用和改造了“永恒之蓝”攻击工具作为传播勒索程序的载体，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。由于采用了蠕虫的传播方式，就像冲击波、震荡波等著名蠕虫一样可以瞬间影响互联网。

3.2 知识手册

针对用户最关心的“永恒之蓝”勒索蠕虫的相关问题，360 企业安全专家进行专业解答，集成《“永恒之蓝”勒索蠕虫最全知识手册》，在线阅读地址：

http://www.yidianzixun.com/home?page=article&id=0GLQjxAA

3.3 技术分析

360 公司追日安全团队发布了揭露恶意代码工作细节的权威报告《WanaCrypt0r 勒索蠕虫完全分析报告》，对技术有兴趣的人员可以参考，报告地址：

http://m.bobao.360.cn/learning/detail/3853.html?from=timeline&isappinstalled=1

发现了蠕虫新的变种，目前国内尚未发现感染，这次变种的主要内容是更换了 killswitch 域名，新的域名为：

http://www.ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

3.4 风险等级

360 安全监测与响应中心对此事件的风险评级为：危急