360 针对“永恒之蓝”（蠕虫 WannaCry）

攻击预警通告

第五次更新

360安全监测与响应中心

2017 年 05 月 13 日

目录

第1章 事件描述

1.1 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、ATM 机、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。

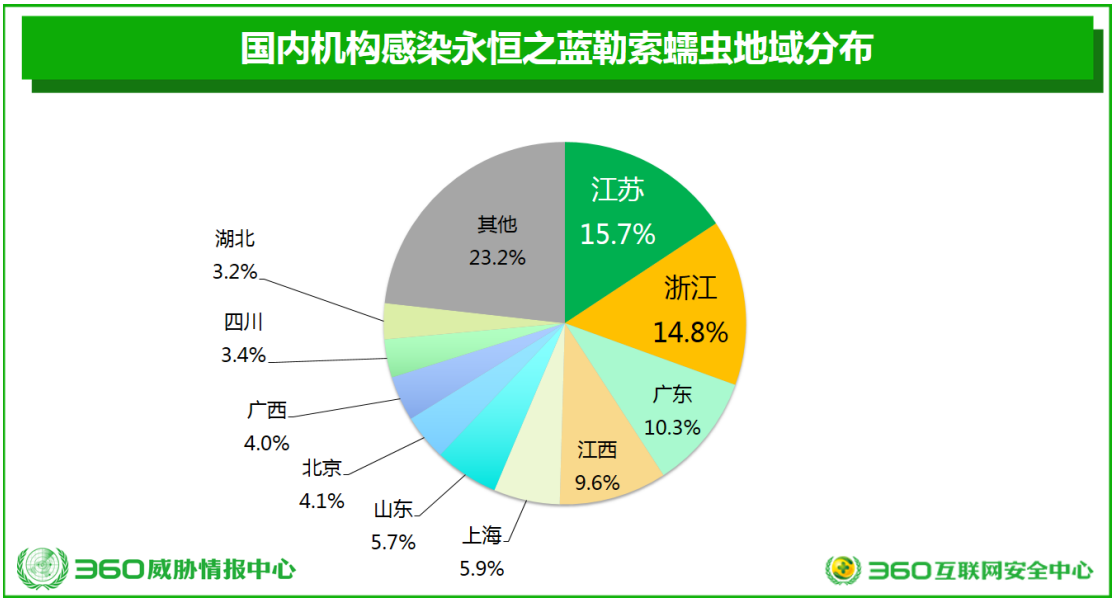
1.2 影响对象

“永恒之蓝”勒索蠕虫针对的是微软 Windows 操作系统，它利用了 Windows 系统的一个漏洞，微软桌面版本操作系统：Windows2000、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 server2016 等无一幸免。

虽然微软早已在 3 月份就发布了针对 Win7 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，也是造成本次蠕虫爆发的重要原因。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，这些系统极易被感染。

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 家俄罗斯组织和 6500 家中国组织和企业都受到了攻击，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，影响范围遍布高校、ATM 机、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，且攻击事态仍在蔓延，被感染的电脑数字还在不断增长中。该事件被认为是迄今为止最大的勒索交费恶意活动事件。

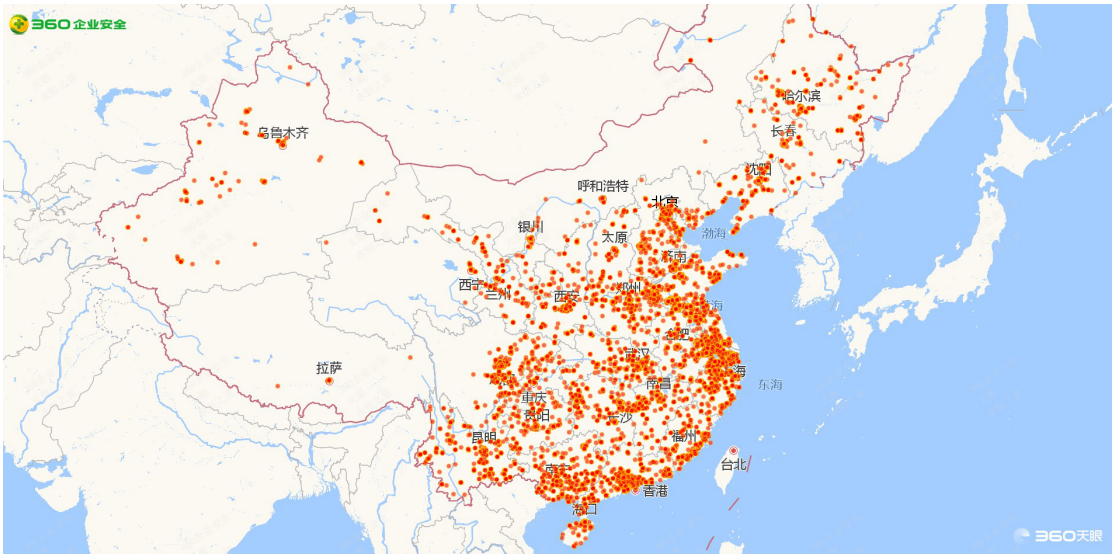


1.3 严重程度

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。

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。下面是全国范围内受影响者的实时监控图：



第2章 事件分析

2.1 事件描述

2017 年 5 月 12 日国内多处高校网络和企业内网出现 WannaCry 勒索软件感染情况，磁盘文件会被病毒加密，只有支付高额赎金才能解密恢复文件，对重要数据造成严重损失，甚至直接导致业务中断。

根据网络安全机构通报，这是不法分子利用 NSA 黑客武器库泄漏的“永恒之蓝”发起的蠕虫病毒攻击传播勒索恶意事件。恶意代码会扫描开放 445 文件共享端口的 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勒索软件、远程控制木马、虚拟货币挖矿机等恶意程序。

由于以前国内多次爆发利用 445 端口传播的蠕虫，部分运营商在主干网络上封禁了 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，仍然存在大量暴露 445 端口且存在漏洞的电脑，导致目前蠕虫的泛滥。

2.2 分析报告

360 企业安全追日安全团队发布权威报告《WanaCrypt0r 勒索蠕虫完全分析报告》，报告地址：

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

2.3 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

第3章 处置建议

3.1 确认影响范围

- **潜在受影响系统确认**

扫描内网，发现所有开放 445 SMB 服务端口的终端和服务器，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。

3.2 应急处置方法

- **360 针对“永恒之蓝”攻击紧急处置手册（蠕虫 WannaCry）**

下载地址：

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

- **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。

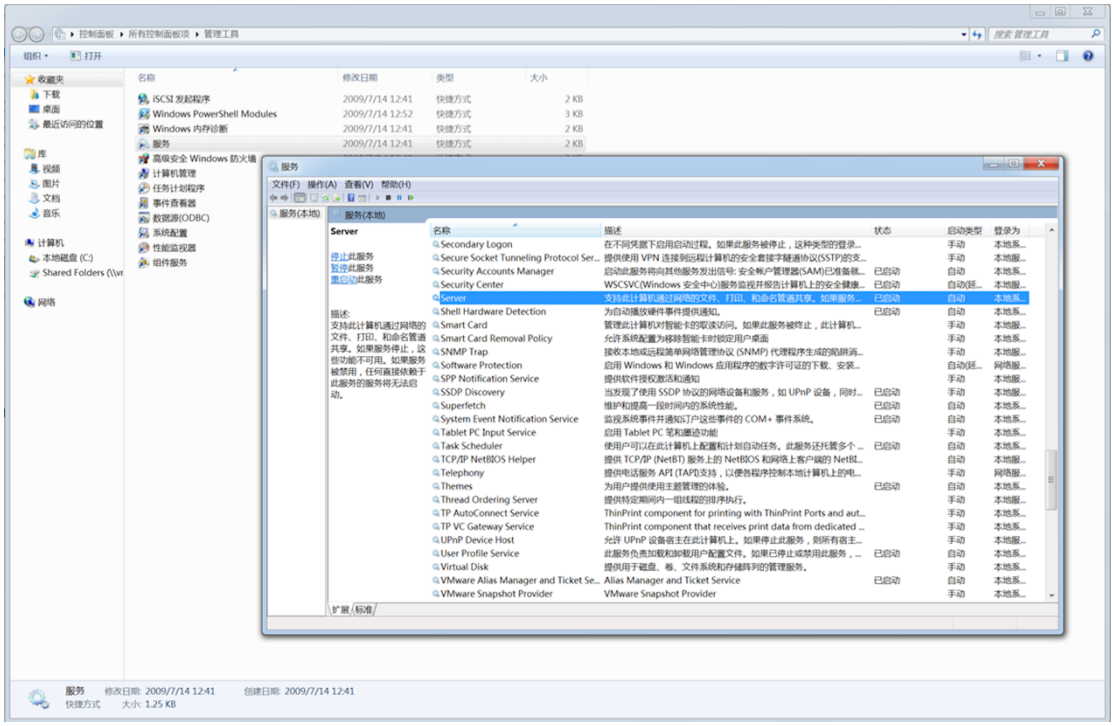
- **终端层面**

暂时关闭 Server 服务。

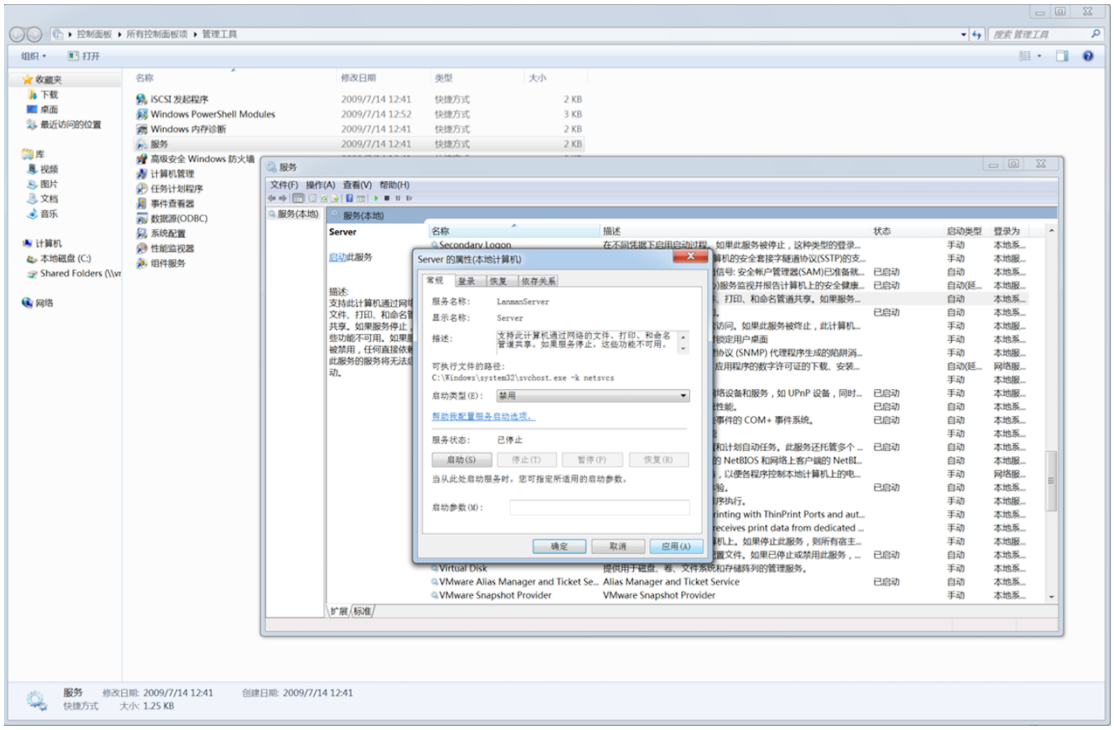
检查系统是否开启 Server 服务，以 Win7 系统为例，其他系统类似：

打开 开始 按钮，选择 控制面板，选择 管理工具， 双击 服务

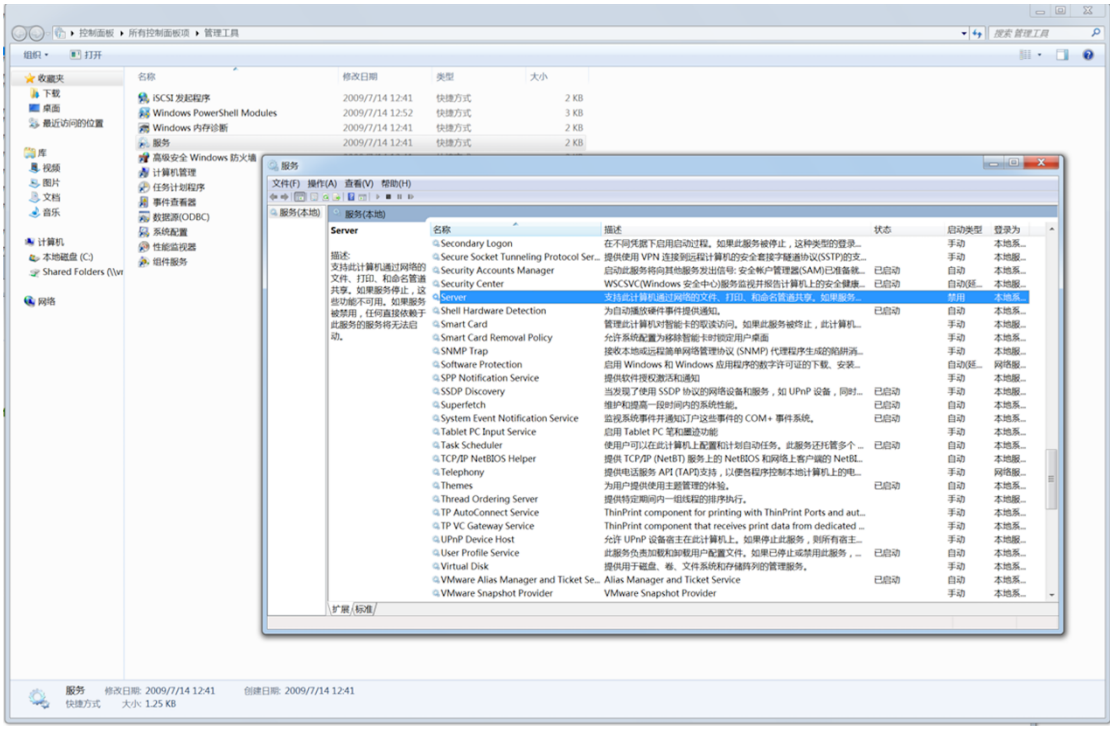
在出来选择框中选择 Server ，如果如下图，状态 为 已启动 ，则当前 Server 服务为启动状态，需要加以关闭。



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：



- **防护工具**

360 企业安全天擎团队已经针对 WannaCry 勒索蠕虫开发了一个免疫工具，此程序在电脑上运行以后，现有蠕虫将不会感染系统。免疫工具下载地址：http://b.360.cn/other/onionwormimmune

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。

- **感染处理**

对于已经感染勒索蠕虫的机器建议隔离处置。

3.3 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

出于基于权限最小化的安全实践，建议用户关闭并非必需使用的 Server 服务，操作方法见 应急处置方法 节。

3.4 恢复阶段

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。