**关于防范基于SMB文件共享传播的蠕虫病毒攻击**

**紧急安全预警通告**



**2017年05月12日**

目录

[第1章 安全通告 3](#_Toc482413507)

[第2章 漏洞信息 4](#_Toc482413508)

[2.1 漏洞描述 4](#_Toc482413509)

[2.2 风险等级 4](#_Toc482413510)

[第3章 处置建议 5](#_Toc482413511)

[3.1 确认影响范围 5](#_Toc482413512)

[3.2 应急处置方法 5](#_Toc482413513)

[ 网络层面 5](#_Toc482413514)

[ 终端层面 5](#_Toc482413515)

[ 感染处理 7](#_Toc482413516)

[3.3 根治方法 7](#_Toc482413517)

[3.4 恢复阶段 7](#_Toc482413518)

[第4章 技术分析 8](#_Toc482413519)

[4.1 整体影响评估 8](#_Toc482413520)

[4.2 可受影响区域 8](#_Toc482413521)

# 安全通告

尊敬的客户：

2017年5月12日起，在国内外网络中发现爆发基于Windows网络共享协议进行攻击传播的蠕虫恶意代码，这是不法分子通过改造之前泄露的NSA黑客武器库中“永恒之蓝”攻击程序发起的网络攻击事件。

目前发现的蠕虫会扫描开放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执行勒索程序、远程控制木马、虚拟货币挖矿机等恶意程序。

此蠕虫目前在没有对445端口进行严格访问控制的教育网及企业内网大量传播，呈现爆发的态势，受感染系统会被勒索高额金钱，不能按时支付赎金的系统会被销毁数据造成严重损失。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。

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

前情提要：北京时间2017年4月14日晚，一大批新的NSA相关网络攻击工具及文档被Shadow Brokers组织公布，其中包含了涉及多个Windows系统服务（SMB、RDP、IIS）的远程命令执行工具。

# 漏洞信息

## 漏洞描述

近期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。

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。

## 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

# 处置建议

## 确认影响范围

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MS07-010补丁，如没有安装则受威胁影响。Win7以下的Windows XP/2003目前没有补丁，只要开启SMB服务就受影响。

## 应急处置方法

### 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天堤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，直到确认网内的电脑已经安装了MS07-010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：

1、打开开始按钮，点击运行，输入cmd，点击确定

2、输入命令：netstat -an 回车

3、查看结果中是否还有445端口



如果发现445端口开放，需要关闭Server服务，以Win7系统为例，操作步骤如下：

点击开始按钮，在搜索框中输入cmd，右键点击菜单上面出现的cmd图标，选择以管理员身份运行，在出来的 cmd 窗口中执行“net stop server”命令，会话如下图：



### 感染处理

对于已经感染勒索蠕虫的机器建议隔离处置。

## 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。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。

对于Windows XP、2003等微软已不再提供安全更新的机器，推荐使用360“NSA武器库免疫工具”检测系统是否存在漏洞，并关闭受到漏洞影响的端口，以避免遭到勒索蠕虫病毒的侵害。免疫工具下载地址：<http://dl.360safe.com/nsa/nsatool.exe>。这些老操作系统的机器建议加入淘汰替换队列，尽快进行升级。

## 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。

# 技术分析

## 整体影响评估

此安全事件影响范围包括全部开放445端口的系统，影响范围巨大。

## 可受影响区域

企业内网将是受本次攻击事件影响的重灾区。