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

360安全监测与响应中心

2017 年 05 月 12 日

目录

第1章 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。

第2章 漏洞信息

2.1 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。

2.2 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

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。

3.2 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

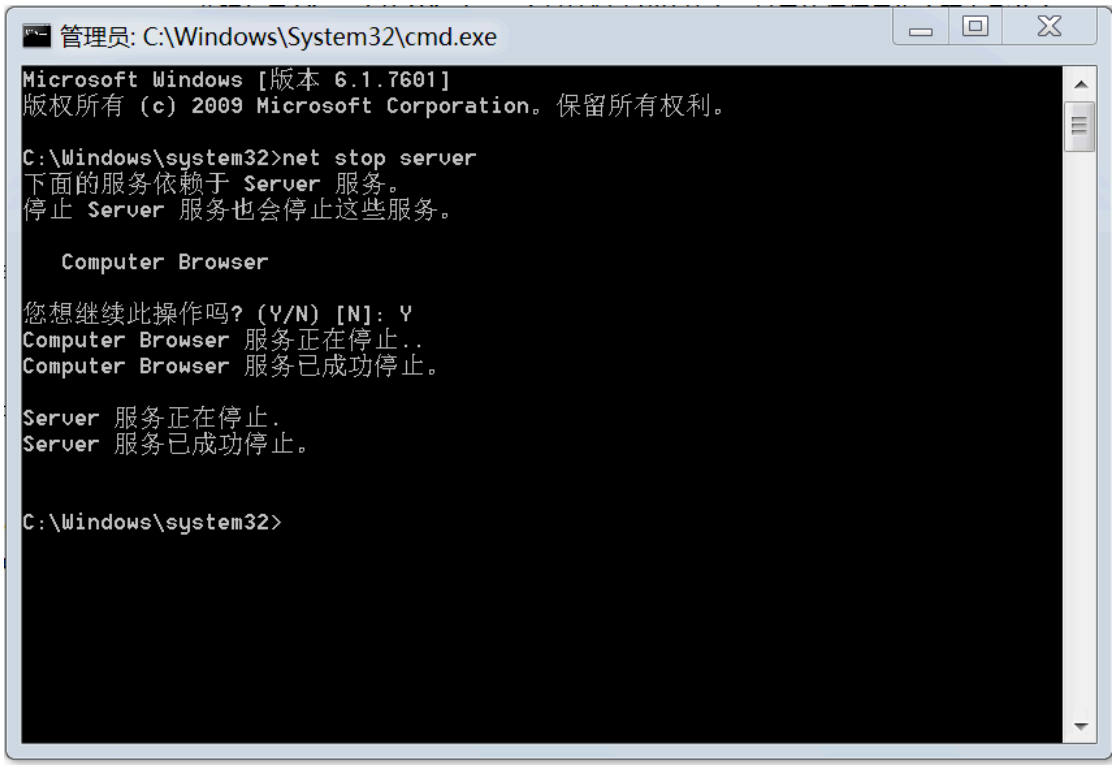
```
C:\Windows\system32>netstat -an

活动连接

  协议  本地地址          外部地址        状态
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1031           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1032           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1046           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:15000          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:54321          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:443          127.0.0.1:3605         ESTABLISHED
  TCP    127.0.0.1:443          127.0.0.1:3607         ESTABLISHED
  TCP    127.0.0.1:443          127.0.0.1:3613         ESTABLISHED
  TCP    127.0.0.1:443          127.0.0.1:3614         ESTABLISHED
```

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。

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。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。

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。

第4章 技术分析

4.1 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。

4.2 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。