关于“永恒之蓝勒索病毒”爆发安全事件应急处置方案

杭州安恒信息技术有限公司

2017 年 05 月 13 日

版权申明

目　　录

1. 相关说明

北京时间 2017 年 05 月 12 日，安恒信息监测到黑客利用 NSA 黑客武器库泄漏的“永恒之蓝”工具发起的网络攻击事件：大量服务器和个人 PC 感染病毒后被远程控制，成为不法分子的比特币挖矿机（挖矿会耗费大量计算资源，导致机器性能降低），甚至被安装勒索软件，磁盘文件会被病毒加密为.onion 或者.WNCRY 后缀，用户只有支付高额赎金后才能解密恢复文件，对个人及企业重要文件数据造成严重损失。受感染图片如下所示：

“EternalBlue”工具利用的是微软Windows操作系统的SMBv1协议中的安全漏洞。未经身份验证的攻击者可以向目标机器发送特制报文触发缓冲区溢出，导致在目标机器上远程执行任意代码。“永恒之蓝”工具会扫描开放445文件共享端口的Windows机器，只要用户开机上网，黑客就可能在电脑和服务器中植入勒索软件。

之前国内曾多次爆发利用445端口传播的蠕虫，运营商对个人用户封掉此端口；但国内特定行业的网络无此限制，存在大量暴露445端口的机器，因此也成为了此次感染事件的重灾区，已经有大量该行业网络的用户报告个人PC被安装了勒索软件。此外，根据国外媒体的报道，目前英国、美国、俄罗斯、西班牙、意大利、越南、中国台湾等国家和地区也出现了被感染的情况。

2.影响范围

MS17-010 漏洞主要影响以下操作系统：

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

3.检测方法

由于“EternalBlue”的利用代码主要针对Windows XP、Windows7、Windows Server 2008等，这些版本的操作系统占桌面、服务器操作系统的大部分，因此此次事件对于Windows的影响非常严重。

检测方法只需检测受影响的Windows操作系统版本只要打开了445端口、且没有安装MS17-010的机器则确认会受到影响。

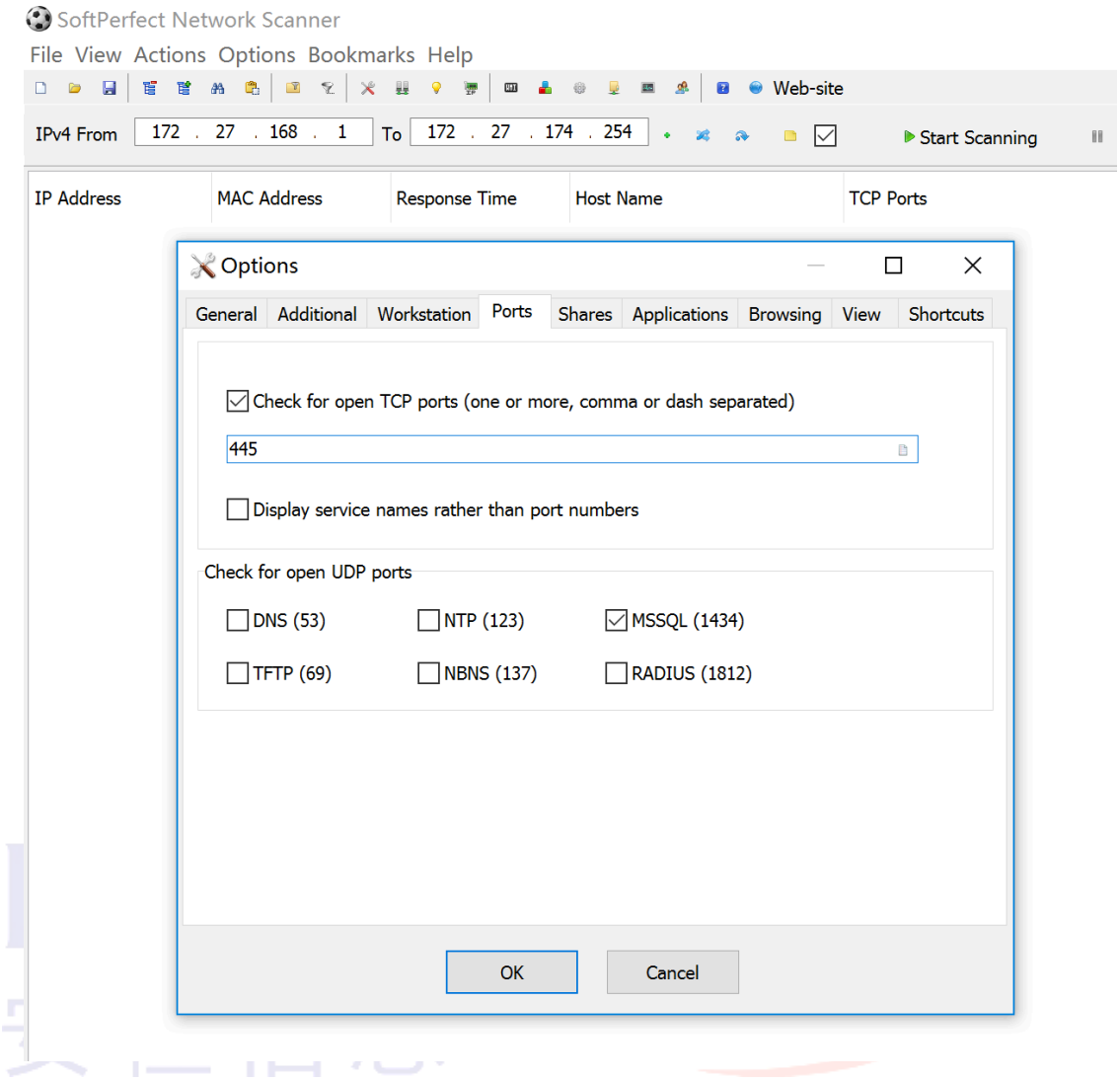
端口扫描方法：

```
# nmap -sS -p 445 -vv 192.168.1.1/24
```

或者使用其他端口扫描工具

例如：Softperfect Network Scanner（https://www.softperfect.com/）

配置扫描端口为445



漏洞检测POC脚本：

https://github.com/countercept/doublepulsar-detection-script

“DOUBLEPULSAR SMB IMPLANT DETECTED!!!”说明系统存在漏洞

```
root@kali:~# python detect_doublepulsar_smb.py --ip 192.168.175.128
[-] [192.168.175.128] No presence of DOUBLEPULSAR SMB implant

root@kali:~# python detect_doublepulsar_smb.py --ip 192.168.175.128
[+] [192.168.175.128] DOUBLEPULSAR SMB IMPLANT DETECTED!!!

root@kali:~# python detect_doublepulsar_rdp.py --file ips.list --verbose --threads 1
[*] [192.168.175.141] Sending negotiation request
[*] [192.168.175.141] Server explicitly refused SSL, reconnecting
[*] [192.168.175.141] Sending non-ssl negotiation request
[*] [192.168.175.141] Sending ping packet
[-] [192.168.175.141] No presence of DOUBLEPULSAR RDP implant
[*] [192.168.175.143] Sending negotiation request
[*] [192.168.175.143] Server chose to use SSL - negotiating SSL connection
[*] [192.168.175.143] Sending SSL client data
[*] [192.168.175.143] Sending ping packet
[-] [192.168.175.143] No presence of DOUBLEPULSAR RDP implant
[*] [192.168.175.142] Sending negotiation request
[*] [192.168.175.142] Sending client data
[*] [192.168.175.142] Sending ping packet
[+] [192.168.175.142] DOUBLEPULSAR RDP IMPLANT DETECTED!!!

root@kali:~# python detect_doublepulsar_smb.py --ip 192.168.175.136 --uninstall
[+] [192.168.175.136] DOUBLEPULSAR SMB IMPLANT DETECTED!!! XOR Key: 0x7c3bf3c1
[+] [192.168.175.136] DOUBLEPULSAR uninstall successful
```

4. 应急处置

4.1 对于已经感染的系统

- 断开已经感染的主机系统的网络连接，防止进一步扩散；
- 优先检查未感染主机的漏洞状况，做好漏洞加固工作后方可恢复网络连接。
- 已经感染终端，根据终端数据重要性决定处置方式，如果重新安装系统则建议完全格式化硬盘、使用全新操作系统、完善操作系统补丁、安装防病毒软件并通过检查确认无相关漏洞后再恢复网络连接。

4.2 对于未感染的系统

注意：以下操作有先后顺序，请逐步开展

- **[*非常重要*] 拔掉网线之后再开机启动**
- 做好重要文件的备份工作（最好备份到存储介质中）

- 开启系统防火墙，并设置阻止向 445 端口进行连接，可以使用以下命令开展：

方法一：

```
echo "请务必以管理员身份运行"
netsh firewall set opmode enable
netsh advfirewall firewall add rule name="deny445" dir=in protocol=tcp localport=445 action=block
```

方法二：

Windows 32 位关闭 445 端口批处理（bat）：

```
REG ADD HKLM\SYSTEM\CurrentControlSet\services\NetBT\Parameters /v SMBDeviceEnabled /T REG_DWORD /D 0 /F&&sc  config LanmanServer start= disabled&&net stop lanmanserver /y
```

Windows x64 位关闭 445 端口批处理（bat）：

```
REG ADD HKLM\SYSTEM\CurrentControlSet\services\NetBT\Parameters /v SMBDeviceEnabled /T REG_QWORD /D 0 /F&&sc  config LanmanServer start= disabled&&net stop lanmanserver /y
```

新建文本文档，然后复制以上脚本内容，另存为【.bat】格式的文件，并右键【管理员运行】，待 CMD 对话框消失后，重启电脑即可。

- 如无必需，建议关闭 SMB 共享服务
- 打开系统自动更新，并检测系统补丁进行安装，如果是内网环境可以采用离线补丁方式更新
- 安装杀毒软件并升级病毒库；
- 增强个人主机病毒防范意识，不随意打开位置来源的文件，关闭移动存储自动播放功能等

4.3 网络层防护

- 边界交换机、路由器、防火墙等设备禁止双向 135/137/139/445 端口的 TCP 连接
- 内网核心主干交换路由设备禁止双向 135/137/139/445 端口的 TCP 连接
- 更新入侵防御、入侵检测、APT 等安全设备漏洞库，开启防御策略

5. 离线补丁下载地址

Security Update for Windows XP SP3 (KB4012598)

http://download.windowsupdate.com/d/csa/csa/secu/2017/02/windowsxp-kb4012598-x86-custom-chs_dca9b5adddad778cfd4b7349ff54b51677f36775.exe

Security Update for Windows Server 2003 (KB4012598)

http://download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x86-custom-chs_b45d2d8c83583053d37b20edf5f041ecede54b80.exe

Security Update for Windows Server 2003 for x64 Systems (KB4012598)

http://download.windowsupdate.com/c/csa/csa/secu/2017/02/windowsserver2003-kb4012598-x64-custom-chs_68a2895db36e911af59c2ee133baee8de11316b9.exe

Security Update for Windows 7 (KB4012212)

http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x86_6bb04d3971bb58ae4bac44219e7169812914df3f.msu

Security Update for Windows 7 x64 (KB4012212)

http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x64_2decefaa02e2058dcd965702509a992d8c4e92b3.msu

Security Update for Windows Server 2008 R2 x64 (KB4012212)

http://download.windowsupdate.com/d/msdownload/update/software/secu/2017/02/windows6.1-kb4012212-x64_2decefaa02e2058dcd965702509a992d8c4e92b3.msu

Security Update for Windows10 ()

http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4012606-x86_8c19e23de2ff92919d3fac069619e4a8e8d3492e.msu

Security Update for Windows10 x64 ()

http://download.windowsupdate.com/c/msdownload/update/software/secu/2017/03/windows10.0-kb4012606-x64_e805b81ee08c3bb0a8ab2c5ce6be5b35127f8773.msu