关于大型机构防范

“永恒之蓝”勒索蠕虫攻击的建议

360安全监测与响应中心

2017 年 05 月 13 日

1 遭受攻击信息

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机构、企业内网、高校等单位大量传播，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对此事件的风险评级为：危急。

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。

2 确认影响范围

建议首先确认影响范围，主要工作包括：

1) **网络边界：**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 目前没有补丁，只要开启 SMB 服务就受影响。

2) **网关设备：** 查看网关设备的 IOC _IP 连接情况，确认感染范围。

3) **DNS 流量：** 查看 DNS_IOC 请求情况，确认内网感染范围。

4) **安全设备：** 监测所有对 445 端口的扫描事件。

3 紧急抑制方法

大型机构针对永恒之蓝勒索蠕虫的应急防范措施，应从 DMZ 非军事化隔离区、生产区域、办公区域、互联网边界的网络和终端层面全面做好紧急抑制工作。

大型机构具有网络庞大、接入方式复杂、设备数量众多、敏感数据多、业务连续性要求高等特点，尤其是生产系统的可用性和可靠性要求极高，出现安全事件的负面影响很大。为切实避免“永恒之蓝”勒索蠕虫对业务系统和办公终端带来影响，建议通过集中管控的方式对防护策略进行统一下发和管理。

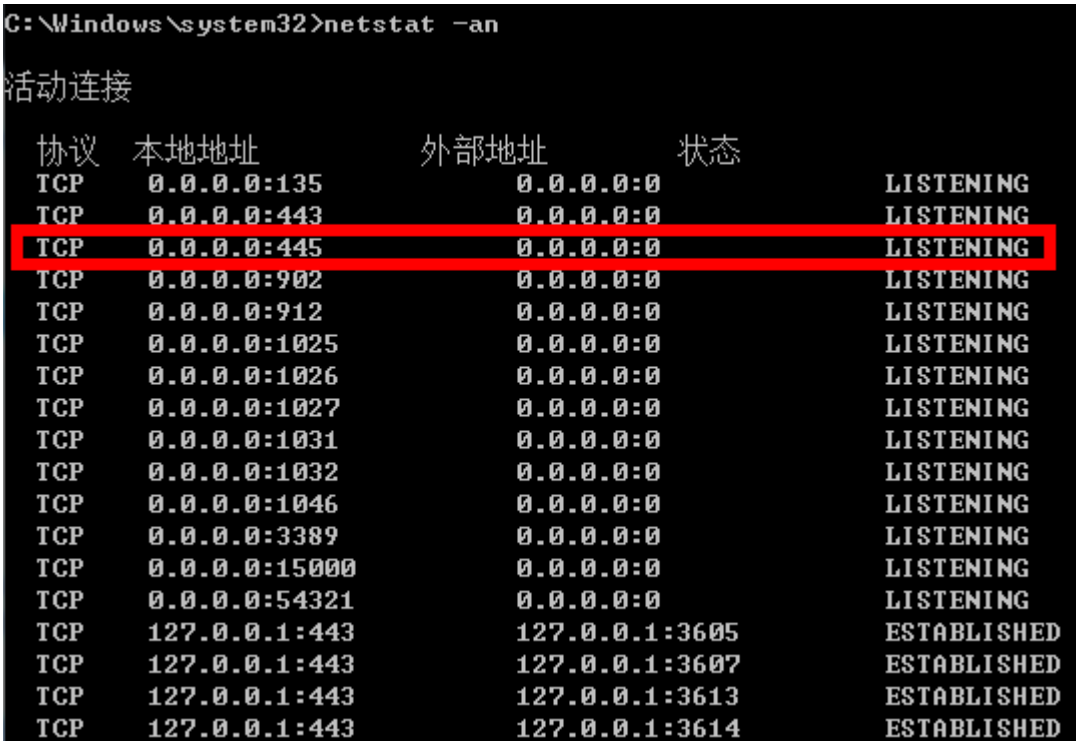
3.1 DMZ 非军事化隔离区

- **网络层面**

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 MS17-010 补丁或关闭了 Server 服务。

- **主机层面**

1) **暂时关闭 Server 服务：**在命令行下输入 netstat –an 命令，查看结果中是否还有 445 端口（如下图所示）。



如果发现 445 端口开放，需要关闭 Server 服务（Win7 系统：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，出现“server 服务已成功停止”提示即可）。

2) **升级网内的电脑，安装 MS17-010 补丁。**补丁下载地址：https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx

3) **安装敲诈者病毒免疫工具。**目前 360 企业安全天擎团队已经开发一个系统免疫工具，程序在电脑上运行以后，现有蠕虫将不会感染系统。请到如下地址下载：https://eyun.360.cn/surl_yZ3RsYgQuvu （提取码：e2ab）

3.2 生产区域

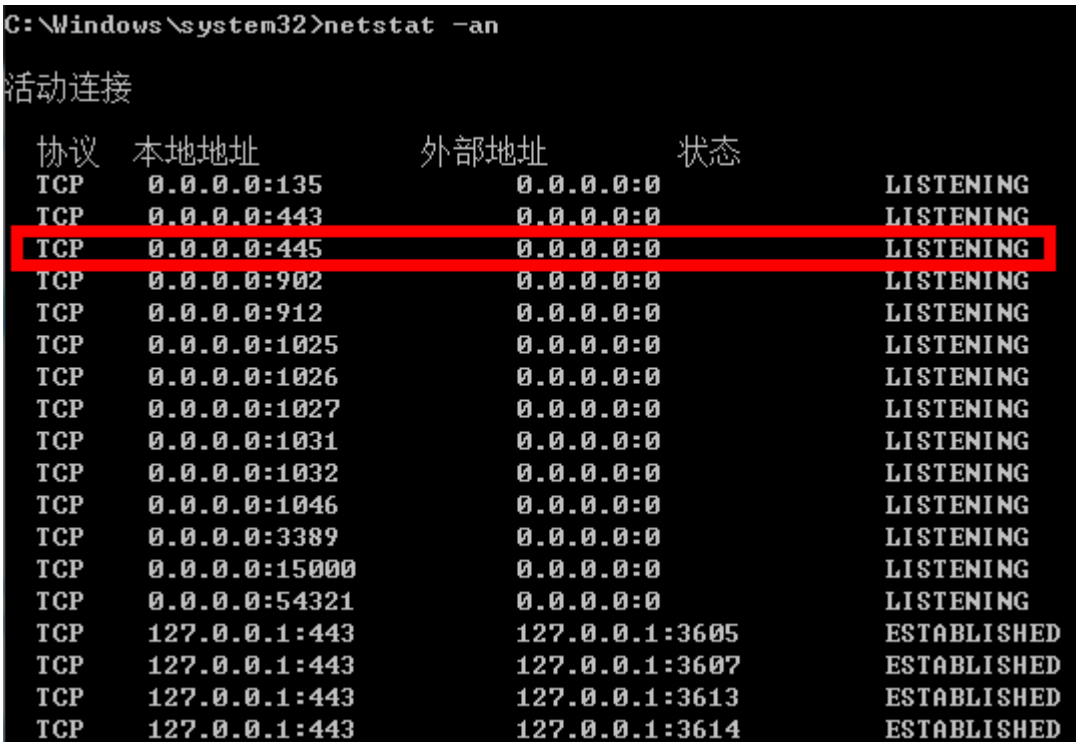
- **网络层面**

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 MS17-010 补丁或关闭了 Server 服务。

对于已经感染勒索蠕虫的机器，建议紧急隔离处置。

- **主机层面**

1) **暂时关闭 Server 服务：**在命令行下输入 netstat –an 命令，查看结果中是否还有 445 端口（如下图所示）。



如果发现 445 端口开放，需要关闭 Server 服务（Win7 系统：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，出现“server 服务已成功停止”提示即可）。

2) **升级网内的电脑，安装 MS17-010 补丁。**补丁下载地址：https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx

3) **安装敲诈者病毒免疫工具。**目前 360 企业安全天擎团队已经开发一个系统免疫工具，程序在电脑上运行以后，现有蠕虫将不会感染系统。请到如下地址下载：https://eyun.360.cn/surl_yZ3RsYgQuvu （提取码：e2ab）

4) **安装 XP 漏洞免疫工具。**

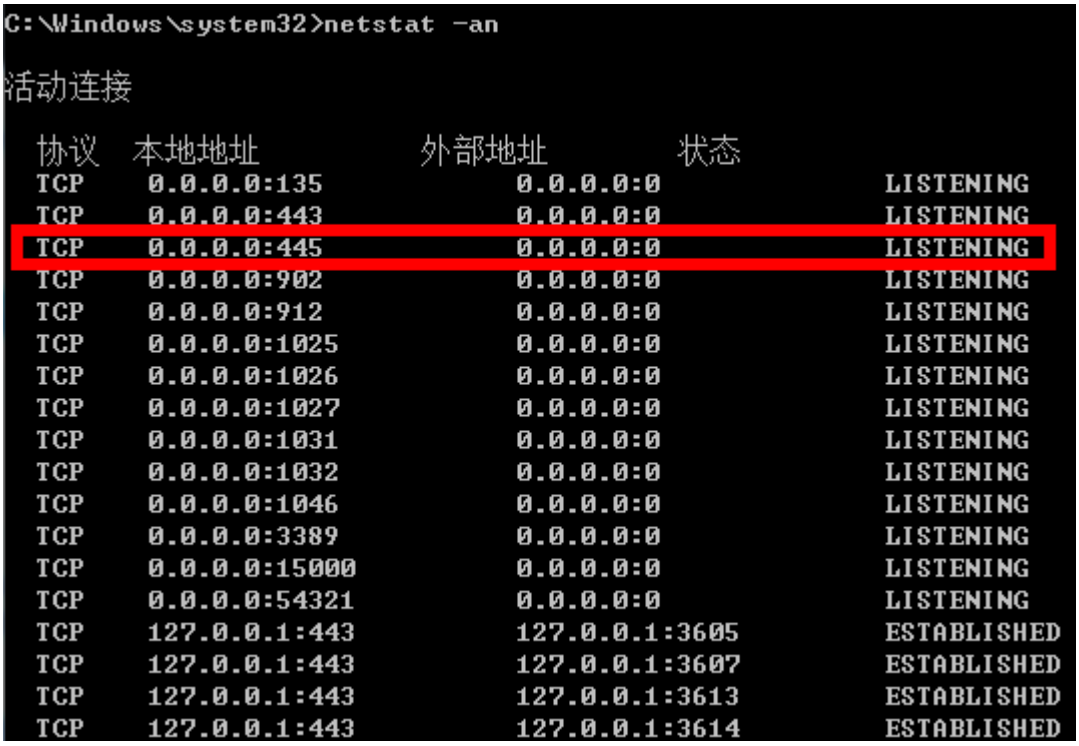
3.3 办公网络

- **网络层面**

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 MS17-010 补丁或关闭了 Server 服务。

- **主机层面**

1) **暂时关闭 Server 服务：**在命令行下输入 netstat –an 命令，查看结果中是否还有 445 端口（如下图所示）。



如果发现 445 端口开放，需要关闭 Server 服务（Win7 系统：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，出现“server 服务已成功停止”提示即可）。

2) **升级网内的电脑，安装 MS17-010 补丁。**补丁下载地址：https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx

3) **安装敲诈者病毒免疫工具。**目前 360 企业安全天擎团队已经开发一个系统免疫工具，程序在电脑上运行以后，现有蠕虫将不会感染系统。请到如下地址下载：https://eyun.360.cn/surl_yZ3RsYgQuvu （提取码：e2ab）

4) **安装 xp 漏洞免疫工具。**

3.4 互联网边界

互联网各接入边界的网络层面应采取如下措施：

1) 紧急下线尚未关闭 445 端口的服务器。

2) 封锁 445 端口的双向流量。

3) 封锁已知扫描源 IP。

4 隐患根除方法

隐患根除方法主要内容如下：

1) 对于 Win7 及以上版本操作系统，立即升级 MS17-01 补丁。
2) 关闭非必要的 Server 服务，特别是 445 文件共享端口服务，操作方法见“紧急抑制方法”节。
3) 进行安全域之间的访问控制隔离，在网络访问层面封锁 445 文件共享端口服务。
4) 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 。这些老旧操作系统的机器建议加入淘汰替换队列，尽快进行升级。

5 业务恢复建议

1) 针对重点服务器、重要业务系统，立即进行数据备份。
2) 建立快速系统重装机制。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。