

360 天擎终端安全管理系统针对“永恒之蓝”勒索蠕虫病毒的防护方案

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。

针对于已感染勒索蠕虫的终端的处置建议：

- 1、针对于被感染的机器屏幕会显示如下的告知付赎金的界面，则要立即对该主机进行断网隔离（拔网线）。



- 2、如客户存在主机备份，则启动程序恢复功能。

针对于未安装 360 天擎产品的用户建议如下：

- 1、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。
- 2、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>
- 3、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。

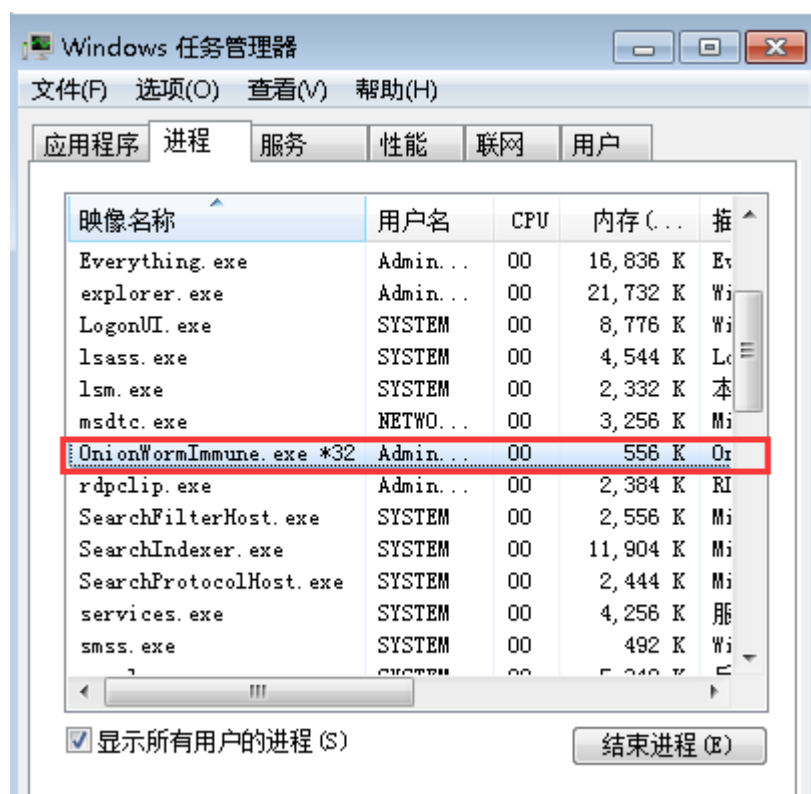
针对于 360 天擎用户防范措施如下：

1. 安装免疫工具：

目前 360 天擎团队已经开发了一套免疫工具，在终端运行后，现已发现的勒索蠕虫将不会感染系统。

下载地址如下：<http://dl.b.360.cn/tools/OnionWormImmune.exe>

保存该工具到任意位置后双击执行即可。切勿删除该工具，该工具重启系统后会自启动。在进程列表中可以查看到该进程存在，则对该勒索蠕虫病毒进行免疫。

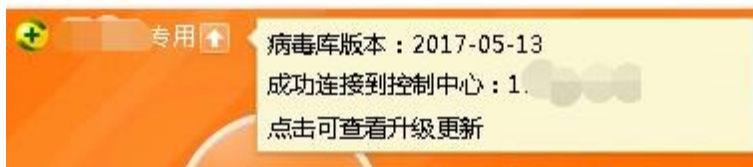


2. 更新病毒特征库：

在天擎控制台升级 Windows 病毒库到最新版本，2017-05-13 版本。可有效查杀此次勒索蠕虫病毒。

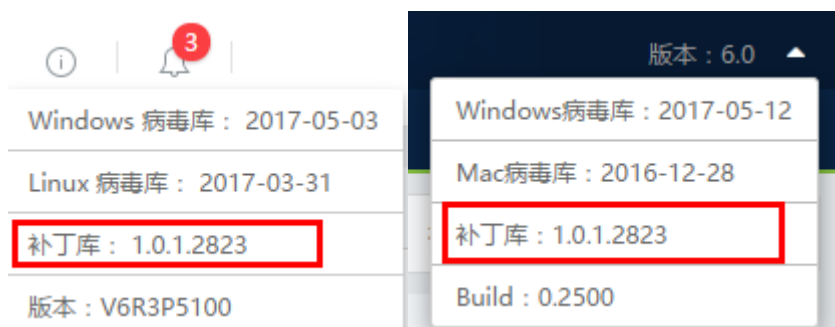


打开终端右上角可以查看到病毒库版本与控制台对应。



3. 安装漏洞补丁

此次对于病毒传播方式的根治方法对于 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。
先检查天擎补丁库版本，天擎补丁库版本在右上角检查，确保补丁库升级到 1.0.1.2823 版本，该补丁库包含 3 月、4 月、5 月的高危漏洞。控制他补丁库更新成功后终端会立即进行终端补丁库的更新。



漏洞管理界面，选择全网终端进行扫描。在线终端会上报终端的高危漏洞展示。



控制台上可以看到终端扫描的漏洞信息：【终端管理-漏洞管理-按漏洞显示】可以看到发布日期中有 3 月 4 月和 5 月的更新补丁信息。可以对高危漏洞进行选中修复。
该页面中显示未修复的终端数和已修复的终端数，勾选后点击修复则对未修复终端数进行修复。



点击以忽略的终端数，弹窗显示以忽略的终端，全选后取消忽略。对于用户手动忽略该漏洞的终端将重新在漏洞界面显示可修复。

漏洞			
高危漏洞			
漏洞名：Windows 月度安全更新(2017.03)(KB...补丁级别：高危漏洞			
已忽略终端数：23			
补丁描述：此更新程序包含了当月 Microsoft Windows 安全更新			
取消忽略			
计算机名	分组	IP地址	系统盘剩余空间
A003030-NC01(高线)	默认分组	10.74.20.14	68559MB
A002307-NC01(高线)	临时增加数据采集	10.74.20.47	175962MB
15210-PC01(高线)	行政部（来）	172.24.16.200	46548MB
A003112-NC01(高线)	默认分组	172.24.87.183	119975MB
A003003	默认分组	172.24.187.120	144084MB

终端上验证：终端可以扫描到 3 月 4 月 5 月的漏洞信息，选择修复即可。
或者通过补丁管理界面可以搜索补丁号，确保需要修复的补丁都在已安装的补丁中。

漏洞修复

发现 12 个高危漏洞，需要立即修复。
共选择了 12 个补丁，共需下载 301.34 MB。

高危漏洞

这些漏洞可能会被木马、病毒利用，破坏您的电脑，请立即修复。

KB2760272 - Office 2013 安全功能绕过漏洞

KB3188730 - .Net Framework 3.5 SP1 安全更新

KB3192391 - Windows 月度安全更新(2016.10)

KB3197867 - Windows 月度安全更新(2016.11)

KB3205394 - Windows 月度安全更新(2016.12)

KB3210131 - .Net Framework 3.5 SP1 安全更新

KB3212642 - Windows 月度安全更新(2017.01)

KB4012212 - Windows 月度安全更新(2017.03)

KB4015546 - Windows 安全月度更新(2017.04)

KB4014565 - .Net Framework 3.5 SP1 安全更新

KB3172519 - Microsoft Outlook 2013 安全更新

软件安全更新

这些更新用于修复一些流行软件的严重安全漏洞，建议立即修复。

推荐选... 补丁管理 导出漏洞信息

360漏洞修复

已安装补丁 已忽略补丁 已过期补丁 已屏蔽补丁

您的系统中已经安装了 192 个补丁。

安装时间

补丁名称

描述

操作

2016-10-09

KB3159398

组策略的安全更新

卸载

2016-10-09

KB3161561

Windows SMB 服务安全更新

卸载

2016-10-09

KB3161949

WPAD 安全更新

卸载

2016-10-09

KB3161958

Windows 搜索组件的安全更新

卸载

2016-10-09

KB3164033

Windows 图形组件的安全更新

卸载

2016-10-09

KB3164035

Windows 图形组件的安全更新

卸载

2016-10-09

KB3163245

.Net Framework 3.5 SP1 安全更新

卸载

2016-10-09

KB3170455

Windows 打印组件安全更新

卸载

2016-10-09

KB3167679

Windows 身份验证方法安全更新

卸载

2016-10-09

KB3177725

Windows 内核驱动安全更新

卸载

2016-10-09

KB3178034

Microsoft 图形组件安全更新

卸载

2016-06-22

KB318612

Windows Update 程序更新

卸载

2016-06-22

KB3142024

.Net Framework 3.5 SP1 安全更新

卸载

修复漏洞后可以有效根治“永恒之蓝”漏洞被勒索蠕虫病毒利用。

附录：参考需要修复的补丁

Windows 7	Windows Server 2008 R2	Windows 8.1	Windows Server 2012 and Windows Server 2012 R2
-----------	------------------------	-------------	--

(4012215) (4012212)	(4012215) (4012212)	(4012216) (4012213)	(4012213) (4012214) (4012216) (4012217)
Windows Vista	Windows Server 2008	Windows 10	Windows Server 2016
(4012598)	(4012598)	(4013198) (4013429) (4012606)	(4013429)