WannaMine?警惕"永恒之蓝"挖矿长期潜伏

深信服千里目安全实验室 / 2018-03-10 09:30:56 / 浏览数 20991 安全技术 漏洞分析 顶(0) 踩(0)

近一段时间，千里目安全实验室EDR安全团队持续收到大量用户反馈，其内网很多主机存在蓝屏和卡顿现象。经过我们跟踪分析，发现这是利用"永恒之蓝"漏洞的新玩法，其

此病毒变种，传播机制与WannaCry勒索病毒一致（可在局域网内，通过SMB快速横向扩散），故我们将其命名WannaMine。

0x01 攻击场景

此次攻击，是经过精心设计的，涉及的病毒模块多，感染面广，关系复杂。

如上图，压缩包MsraReportDataCache32.tlb含有所需要的所有攻击组件，其目录下有hash、spoolsv、srv等病毒文件，此外，子压缩包crypt有"永恒之蓝"漏洞攻击工具集

其中
hash/hash64：为32位/64位挖矿程序，会被重命名为TrueServiceHost.exe。
spoolsv/spoolsv64：为32位/64位攻击母体，会被重命名为spoolsv.exe。
srv/srv64：为32位/64位为主服务，攻击入口点，会被重命名为tpmagentservice.dll。

本文所述病毒文件，释放在下列文件目录中
C:\Windows\System32\MsraReportDataCache32.tlb
C:\Windows\SecureBootThemes\
C:\Windows\SecureBootThemes\Microsoft\
C:\Windows\SecureBootThemes\Crypt\

攻击顺序：
1.srv是主服务，每次都能开机启动，启动后加载spoolsv。
2.spoolsv对局域网进行445端口扫描，确定可攻击的内网主机。同时启动挖矿程序hash、漏洞攻击程序svchost.exe和spoolsv.exe。
3.svchost.exe执行"永恒之蓝"漏洞溢出攻击（目的IP由第2步确认），成功后spoolsv.exe(NSA黑客工具包DoublePulsar后门）安装后门，加载payload（x86.dll、x64.dll）
4.payload（x86.dll、x64.dll）执行后，负责将MsraReportDataCache32.tlb从本地复制到目的IP主机，再解压该文件，注册srv主服务，启动spoolsv执行攻击（每感染一台

0x02病毒自更新

此次攻击，病毒本身做了很健壮的自更新机制，包括外网更新和局域网更新两个方面。病毒自更新主要是获取新的压缩包MsraReportDataCache32.tlb。

如上图，只要局域网内有一台感染主机可以上网，则该主机可以从公网上下载到最新的MsraReportDataCache32.tlb，并解压自更新（外网更新）。
然后，该主机可以创建微型Web服务端，供内网其它无法上网的主机下载更新（局域网更新）。
这样的一个更新机制，保障了全网都能及时更新到最新的病毒变种，且在主服务没有被删除的情况下，即使其它病毒文件被删除，很快又可以重新下载生成！极大保障了此僵

如上图，我们追踪到的外网下载链接为：
hxxp://acs.njaavfxcgk3.club:4431/f79e53
hxxp://rer.njaavfxcgk3.club:4433/a4c80e
hxxp://rer.njaavfxcgk3.club:4433/5b8c1d
hxxp://rer.njaavfxcgk3.club:4433/d0a01e
主控模块每次执行，会删除主机已存在的病毒模块文件，并结束相应的进程。然后，执行更新模块，使用ServiceCrtMain函数进行下载更新操作。

创建Web服务端，局域网内的其他计算机主控模块可以通过WebServer下载相应的压缩包。

0x03 漏洞利用

主控程序spoolsv/spoolsv会被重命名为spoolsv.exe,其运行后会获得自身主机HOST，然后对局域网内的主机进行扫描。通过获得的IP表，扫描局域网内开放的445端口号，

如果发现局域网内开放的445端口，就会将相应的IP地址和端口号写入到EternalBlue攻击程序svchost.exe的配置文件svchost.xml中，如下图。

然后通过CreateProcessA函数启动svchost.exe（永恒之蓝攻击程序）进行局域网主机的攻击，同时将这个行为特征记录到stage1.txt。
永恒之蓝攻击完成之后，会修改DoublePulsar后门程序spoolsv.exe的配置文件spoolsv.xml，如下图。

然后，通过CreateProcessA函数启动spoolsv.exe(NSA黑客工具包DoublePulsar后门）安装后门程序，同时将这个行为特征记录在stage2.txt。

上述配合完成后，会执行Payload，解压MsraReportDataCache32.tlb，从中提取srv到系统目录下，并命名为tpmagentservice.dll。然后，将tpmagentservice.dll安装为

srv服务安装后，可以启动spoolsv，进行一轮新的漏洞利用与Payload加载。

0x04 集体挖矿

此次攻击的手法，多数是沿用WannaCry的套路，所不同的是，这次攻击的目的不是勒索，是挖矿，而且是瞄准了大规模的集体挖矿。何解？之前的挖矿都是相对独立的事件

我们从压缩包中解压出挖矿程序hash/hash64。逆向分析后，发现其会被复制到system32系统目录下，重命名为TrueServiceHost.exe，并进行挖矿操作，挖矿的矿池钱包地

0x05 解决方案

1、隔离感染主机：已中毒计算机尽快隔离，关闭所有网络连接，禁用网卡。
2、切断传播途径：关闭潜在终端的SMB 445等网络共享端口，关闭异常的外联访问。
3、查找攻击源：手工抓包分析或借助态势感知类产品分析。
4、查杀病毒：推荐使用EDR工具进行查杀。

上一篇：网站漏洞——文件判断函数的安全风险... 下一篇：Encryption 101系列：...

1. 0 条回复
   - 动动手指，沙发就是你的了！