WanaCrypt0r勒索蠕虫完全分析报告

05月13, 2017

0x1 前言

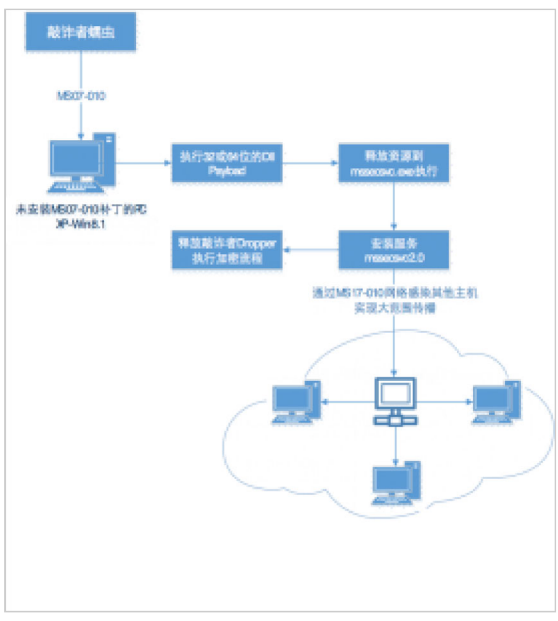
360互联网安全中心近日发现全球多个国家和地区的机构及个人电脑遭受到了一款新型勒索软件攻击，比于5月12日国内率先发布紧急预警，外媒和多家安全公司将该病毒命名为“WanaCrypt0r”（直译：“想哭勒索蠕虫”），常规的勒索病毒是一种趋利明显的恶意程序，它会使用非对称加密算法加密受害者电脑内的重要文件进行勒索，除非受害者交出勒索赎金，否则加密文件无法被恢复，而新的“想哭勒索蠕虫”尤其致命，它利用了窃取自美国国家安全局的黑客工具EternalBlue（直译：“永恒之蓝”）实现了全球范围内的快速传播，在短时间内造成了巨大损失。360追日团队对“想哭勒索蠕虫”国内首家对该蠕虫进行了完全的技术分析，帮助大家深入了解此次攻击！

0x2 抽样分析样本信息

MD5: DB349B97C37D22F5EA1D1841E3C89EB4
文件大小: 3,723,264
影响面：除Windows 10外，所有未打MS-17-010补丁的Windows系统都可能被攻击
功能: 释放加密程序，使用RSA+AES加密算法对电脑文件进行加密勒索，通过MS17-010漏洞实现自身的快速感染和扩散。

0x03 蠕虫的攻击流程

该蠕虫病毒使用了ms07-010漏洞进行了传播，一旦某台电脑中招，相邻的存在漏洞的网络主机都会被其主动攻击，整个网络都可能被感染该蠕虫病毒，受害感染主机数量最终将呈几何级的增长。其完整攻击流程如下



0x04 蠕虫启动安装逻辑分析

1. 蠕虫启动时将连接固定url: http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
   a) 如果连接成功,则退出程序
   b) 连接失败则继续攻击
   这个一个比较奇怪的启动逻辑，起初我们猜测这个启动逻辑是蠕虫作者是为了控制蠕虫活跃度的云开关，蠕虫作者可能怕被追踪而放弃注册这个域名。 另外一种可能是蠕虫作者有丰富的病毒检测对抗经验，目前的沙箱分为在线检测和离线检测两种， 要做”离线病毒分析”会对沙箱环境做很多处理，在离线的情况下为了保证病毒的网络连通，可能会加入Fake DNS Responses（欺骗DNS响应）的技术，作者使用这个开关来识别沙箱环境是否有网络欺骗行为，保护蠕虫不被沙箱进一步的分析检测发现。

2. 接下来蠕虫开始判断参数个数,小于2时,进入安装流程;大于等于2时,进入服务流程.

a) 安装流程

i. 创建服务,服务名称: mssecsvc2.0

● 参数为当前程序路径 –m security

ii. 释放并启动exe程序

● 移动当前 C:\WINDOWS\tasksche.exe到 C:\WINDOWS\qeriuwjhrf

● 释放自身的1831资源(MD5: 84C82835A5D21BBCF75A61706D8AB549),到 C:\WINDOWS\tasksche.exe,并以 /i参数启动

b) 服务流程

i. 服务函数中执行感染功能,执行完毕后等待24小时退出.

ii. 感染功能

● 初始化网络和加密库,初始化payload dll内存.

a) Payload包含2个版本,x86和x64

b) 功能为释放资源到c:\windows\mssecsvc.exe并执行

● 启动线程,在循环中向局域网的随机ip发送SMB漏洞利用代码

0x05 蠕虫利用漏洞确认

通过对其中的发送的SMB包进行分析，我们发现其使用漏洞攻击代码和 https://github.com/rapid7/metasploit-framework近乎一致，为Eternalblue工具使用的攻击包。

蠕虫 SMB数据包:

Eternalblue工具使用的MS17-010 SMB数据包:

https://github.com/RiskSense-Ops/MS17-010/tree/master/exploits/eternalblue/orig_shellcode

文件内容在DB349B97C37D22F5EA1D1841E3C89EB4中出现
orig_shellcode文件内容:

DB349B97C37D22F5EA1D1841E3C89EB4 文件:

0x06 蠕虫释放文件分析

蠕虫成功启动后将开始释放文件，流程如下：

释放文件与功能列表，如下：

0x07 关键勒索加密过程分析

蠕虫会释放一个加密模块到内存，直接在内存加载该DLL。DLL导出一个函数TaskStart用于启动整个加密的流程。程序动态获取了文件系统和加密相关的API函数，以此来躲避静态查杀。

整个加密过程采用RSA+AES的方式完成，其中RSA加密过程使用了微软的CryptAPI，AES代码静态编译到dll。加密流程如下图所示。

使用的密钥概述：

目前加密的文件后缀名列表：

“.docx”, ”.xls”, ”.xlsx”, ”.ppt”, ”.pptx”, ”.pst”, ”.ost”, ”.msg”, ”.eml”, ”.vsd”, ”.vsdx”, ”.txt”, ”.csv”, ”.rtf”, ”.123", ”.wks”, ”.wk1", ”.pdf”, ”.dwg”, ”.onetoc2", ”.snt””.jpeg”,”.jpg””.docb”,”.docm”,”.dot”,”.dotm”,”.dotx”,”.xlsm”,”.xlsb”,”.xlw”,”.xlt”,”.xlm”,”.xlc”,”.xltx”,”.xltm”,”.pptm”,”.pot”,”.pps”,”.ppsm”,”.ppsx”,”.ppam”,”.potx”,”.potm”,”.edb”,”.hwp”,”.602",”.sxi”,”.sti”,”.sldx”,”.sldm”,”.sldm”,”.vdi”,”.vmdk”,”.vmx”,”.gpg”,”.aes”,”.ARC”,”.PAQ”,”.bz2",”.tbk”,”.bak”,”.tar”,”.tgz”,”.gz”,”.7z”,”.rar”,”.zip”,”.backup”,”.iso”,”.vcd”,”.bmp”,”.png”,”.gif”,”.raw”,”.cgm”,”.tif”,”.tiff”,”.nef”,”.psd”,”.ai”,”.svg”,”.djvu”,”.m4u”,”.m3u”,”.mid”,”.wma”,”.flv”,”.3g2",”.mkv”,”.3gp”,”.mp4",”.mov”,”.avi”,”.asf”,”.mpeg”,”.vob”,”.mpg”,”.wmv”,”.fla”,”.swf”,”.wav”,”.mp3",”.sh”,”.class”,”.jar”,”.java”,”.rb”,”.asp”,”.php”,”.jsp”,”.brd”,”.sch”,”.dch”,”.dip”,”.pl”,”.vb”,”.vbs”,”.ps1",”.bat”,”.cmd”,”.js”,”.asm”,”.h”,”.pas”,”.cpp”,”.c”,”.cs”,”.suo”,”.sln”,”.ldf”,”.mdf”,”.ibd”,”.myi”,”.myd”,”.frm”,”.odb”,”.dbf”,”.db”,”.mdb”,”.accdb”,”.sql”,”.sqlitedb”,”.sqlite3",”.asc”,”.lay6",”.lay”,”.mml”,”.sxm”,”.otg”,”.odg”,”.uop”,”.std”,”.sxd”,”.otp”,”.odp”,”.wb2",”.slk”,”.dif”,”.stc”,”.sxc”,”.ots”,”.ods”,”.3dm”,”.max”,”.3ds”,”.uot”,”.stw”,”.sxw”,”.ott”,”.odt”,”.pem”,”.p12",”.csr”,”.crt”,”.key”,”.pfx”,”.der”

值得注意的是，在加密过程中，程序会随机选取一部分文件使用内置的RSA公钥来进行加密，这里的目的是解密程序提供的免费解密部分文件功能。

能免费解密的文件路径在文件f.wnry中

0x08 蠕虫赎金解密过程分析

首先，解密程序通过释放的taskhsvc.exe向服务器查询付款信息，若用户已经支付过，则将eky文件发送给作者，作者解密后获得dky文件，这就是解密之后的Key。
解密流程与加密流程相反，解密程序将从服务器获取的dky文件中导入Key。

可以看到，当不存在dky文件名的时候，使用的是内置的Key，此时是用来解密免费解密的文件使用的。

之后解密程序从文件头读取加密的数据，使用导入的Key调用函数CryptDecrypt解密，解密出的数据作为AES的Key再次解密得到原文件。

总结

该蠕虫在全球首例使用了远程高危漏洞进行自我传播复制，危害不小于冲击波和震荡波蠕虫，并且该敲诈者在文件加密方面的编程较为规范，流程符合密码学标准，因此在作者不公开私钥的情况下，很难通过其他手段对勒索文件进行解密（但是，因为其删除文件不彻底，可以通过文件删除恢复工具来恢复部分文件），同时微软已对停止安全更新的xp和2003操作系统紧急发布了漏洞补丁，请大家通过更新MS17-010漏洞补丁来及时防御蠕虫攻击。

360追日团队（Helios Team）

360 追日团队（Helios Team）是360公司高级威胁研究团队，从事APT攻击发现与追踪、互联网安全事件应急响应、黑客产业链挖掘和研究等工作。团队成立于2014年12月，通过整合360公司海量安全大数据，实现了威胁情报快速关联溯源，独家首次发现并追踪了三十余个APT组织及黑客团伙，大大拓宽了国内关于黑客产业的研究视野，填补了国内APT研究的空白，并为大量企业和政府机构提供安全威胁评估及解决方案输出。

本文链接：https://blogs.360.cn/post/wanacrypt0r_ch.html

-- EOF --

作者 heliosteam 发表于 *2017-05-13 12:00:49*，添加在分类 勒索软件 下，最后修改于 *2018-08-14 15:07:00*

分享到：新浪微博微信Twitter印象笔记QQ好友有道云笔记

« EternalRomance (永恒浪漫) 漏洞分析

从永恒之蓝到勒索病毒大爆发 »

Comments

© 2021 - 360 核心安全技术博客 - blogs.360.cn

Powered by ThinkJS & FireKylin 1.3.1