

勒索病毒WannaCry深度技术分析：详解传播、感染和危害细节

转载 gukehui2012 2017-12-22 10:45:17  22489  收藏 25

文章标签：

病毒

技术

一、综述

5月12日，全球爆发的勒索病毒WannaCry借助高危漏洞“永恒之蓝”（EternalBlue）在世界范围内爆发，据报道包括美国、英国、中国、俄罗斯、西班牙、意大利、越南等百余个国家均遭受大规模攻击。我国的许多行业机构和大型企业也被攻击，有的单位甚至“全军覆没”，损失之严重为近年来所罕见。

本报告将从传播途径、危害方式和结果、受威胁用户群等角度，逐一厘清这个恶性病毒方方面面的真相，用以帮助大家认识、解决该病毒，防范未来可能出现的变种病毒，同时澄清一些谣传和谎言。

1.1病毒攻击行为和结果

遭受WannaCry病毒侵害的电脑，其文件将被加密锁死，惯常来说，受害用户支付赎金后可以获得解密密钥，恢复这些文件。但是根据火绒工程师的分析，遭受WannaCry攻击的用户可能会永远失去这些文件。

WannaCry病毒存在一个致命缺陷，即病毒作者无法明确认定哪些受害者支付了赎金，因此很难给相应的解密密钥，所以用户即使支付了赎金，也未必能顺利获得密钥该电脑系统及文件依旧无法得到恢复。

至于网上流传的各种“解密方法”，基本上是没用的，请大家切勿听信谎言，以防遭受更多财产损失。一些安全厂商提供的“解密工具”，其实只是“文件恢复工具”，可以恢复一些被删除的文件，但是作用有限。

因为病毒是生成加密过的用户文件后再删除原始文件，所以存在通过文件恢复类工具恢复原始未加密文件的可能。但是因为病毒对文件系统的修改操作过于频繁，导致被删除的原始文件数据块被覆盖，致使实际恢复效果有限。且随着系统持续运行，恢复类工具恢复数据的可能性会显著降低。

1.2传播途径和攻击方式

据火绒实验室技术分析追溯发现，该病毒分蠕虫部分及勒索病毒部分，前者用于传播和释放病毒，后者攻击用户加密文件。

其实，蠕虫病毒是一种常见的计算机病毒。通过网络和电子邮件进行传播，具有自我复制和传播迅速等特点。此次病毒制造者正是利用了前段时间美国国家安全局(NSA) 泄漏的Windows SMB远程漏洞利用工具“永恒之蓝”来进行传播的。

据悉，蠕虫代码运行后先会连接域名：

http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

如果该域名可以成功连接，则直接停止。而如果上述域名无法访问，则会安装病毒服务，在局域网与外网进行传播。

但是无论这个“神奇开关”是否开启，该病毒都会攻击用户，锁死文件。另外，这个开关程序很容易被病毒制造者去除，因此未来可能出现没有开关的变种病毒。

1.3易受攻击用户群

目前看来，该病毒的受害者大都是行业机构和大型企业，互联网个人用户受感染报告很少。下面我们从操作系统和网络结构两个角度，来说明容易受到攻击的用户群。

首先，该病毒只攻击Windows系统的电脑，几乎所有的Windows系统如果没有打补丁，都会被攻击。而Windows Vista、Windows Server 2008、Windows 7、Windows Server 2008 R2、Windows 8.1、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016 版本，用户如果开启了自动更新或安装了对应的更新补丁，可以抵御该病毒。

Windows10是最安全的，由于其系统是默认开启自动更新的，所以不会受该病毒影响。同时，Unix、Linux、Android等操作系统，也不会受到攻击。

同时，目前这个病毒通过共享端口传播同时在公网及内网进行传播，**直接暴露在公网上且没有安装相应操作系统补丁的计算机有极大风险会被感染**，而通过路由拨号的个人和企业用户，则不会受到来自公网的直接攻击。

1.4火绒将持续追杀WannaCry

目前，对抗“蠕虫”勒索软件攻击的行动仍未结束，在此，火绒安全专家提醒广大用户无需过度担心，“火绒安全软件”已迅速采取措施，完成紧急升级，通过火绒官网下载软件，升级到最新版本即可防御、查杀该病毒。

自5月12日，WannaCry病毒一出，各机构和用户人心惶惶，草木皆兵，日前更是出现了2.0新变种等耸人听闻的言论。截止到今日，火绒已经收集到的所谓的“WannaCry”最新版本的“变种”，但通过对比分析发现，该“变种”有明显的人为修改痕迹，是好事者在造谣蹭热度。火绒实验室可以负责任地告诉大家，目前还没有出现新版本变种。

而日后病毒是否会变异出现新“变种”？火绒实验室将持续跟踪新的病毒变种，一旦遇到新变种会随时升级产品。火绒产品默认自动升级，请广大用户放心使用，无需做任何设置。内网用户通过外网下载火绒产品升级到最新版本，然后覆盖安装内网电脑即可。

此次勒索病毒WannaCry传播速度快，影响范围广，是互联网历史上所罕见的一次“网络安全事故”。对安全厂商而言，是一次极大的考验，“安全”重回主流势在必行，同时也促进了全社会对网络安全意识的提升。

二、样本分析

该病毒分为两个部分：

- 1.蠕虫部分，用于病毒传播，并释放出勒索病毒。
- 2.勒索病毒部分，加密用户文件索要赎金。

2.1 蠕虫部分详细分析：

2.1.1.蠕虫代码运行后先会连接域名：

http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

如果该域名可以成功连接，则直接退出。

关于这个“Kill Switch”的存在网络上众说纷纭，我们认为相对可靠的解释是：开关的存在是为了检测安全软件沙箱。这种手法多见于恶意代码混淆器，但是除了看到几个人为修改“Kill Switch”的样本外，该病毒并没有批量生成、混淆的迹象。另外，如果真是为了对抗安全软件沙箱，和以往对抗沙箱的样本比起来，这段代码过于简单，而且出现的位置也过于明显。所以，放置这样一个“低级”的“Kill Switch”具体出于何种原因，恐怕只有恶意代码作者能够解释了。

2.1.2.如果上述域名无法访问，则会安装病毒服务，服务的二进制文件路径为当前进程文件路径，参数为：-m security，并启动服务。

2.1.3.释放资源到C:WINDOWS目录下的tasksche.exe（该程序是勒索病毒），并将其启动。

2.1.4.蠕虫病毒服务启动后，会利用MS17-010漏洞传播。传播分为两种渠道，一种是局域网传播，另一种是公网传播。如下图所示：

局域网传播主要代码如下图：

病毒会根据用户计算机内网IP，生成覆盖整个局域网网段表，然后循环依次尝试攻击。相关代码如下：

公网传播主要代码如下图，病毒会随机生成IP地址，尝试发送攻击代码。

SMB漏洞攻击数据包数据，如下图所示：

Worm病毒的PE文件中包含有两个动态库文件，是攻击模块的Payload，分别是：x86版本的payload，大小0x4060和x64版本的payload，大小0xc8a4。

两个Payload都是只有资源目录结构没有具体资源的无效PE动态库文件。病毒在攻击前，会构造两块内存，在内存中分别组合Payload和打开Worm病毒自身，凑成有效攻击Payload，代码如下图所示：

有效攻击Payload模型如下：

完整的攻击Payload的资源如下图，资源中的第一个DWORD是病毒大小，之后就是病毒本身。



gukehui2012

关注

👍 8

💬 1

🌟 25



然后使用MS17-010漏洞，通过APC方式注入动态库到被攻击计算机的Lsass.exe，并执行Payload动态库的导出函数PlayGame，该函数非常简单，功能就是释放资源“W”到被攻击计算机“C:Windowsmssecsvc.exe”，并执行，如下图所示：

火绒剑监控被攻击计算机的如下：

被攻击的计算机包含病毒的完整功能，除了会被勒索，还会继续使用MS17-010漏洞进行传播，这种传播呈几何级向外扩张，这也是该病毒短时间内大规模爆发的主要原因。如下图：

目前，攻击内网IP需要用户计算机直接暴露在公网且没有安装相应操作系统补丁的计算机才会受到影响，因此那些通过路由拨号的个人用户，并不会直接通过公网被攻击。如果企业网络也是通过总路由出口访问公网的，那么企业网络中的电脑也不会受到来自公网的直接攻击。但是，现实中一些机构的网络存在直接连接公网的电脑，且内部网络又类似一个大局域网，因此一旦暴露在公网上的电脑被攻破，就会导致整个局域网存在被感染的风险。

2.2 勒索病毒部分详细分析：

2.2.1 该程序资源中包含带有密码的压缩文件，使用密码“WNCry@2oI7”解压之后释放出一组文件：

- 1) taskdl.exe，删除临时目录下的所有“*.WNCRYT”扩展名的临时文件。
- 2) taskse.exe，以任意session运行指定程序。
- 3) u.wnry，解密程序，释放后名为@WanaDecryptor@.exe。
- 4) b.wnry勒索图片资源。
- 5) s.wnry，包含洋葱路由器组件的压缩包。病毒作者将勒索服务器搭建在“暗网”，需要通过tor.exe和服务器进行通信。
- 6) c.wnry，洋葱路由器地址信息。
- 7) t.wnry，解密后得到加密文件主要逻辑代码。
- 8) r.wnry，勒索Q&A。

2.2.2 通过命令行修改所有文件的权限为完全访问权限。命令行如下：

icaccls . /grant Everyone:F /T /C /Q

2.2.3 解密t.wnry文件数据得到含有主要加密逻辑代码的动态库，通过其模拟的LoadLibrary和GetProcAddress函数调用该动态库中的导出函数执行其加密逻辑。

调用勒索动态库代码，如下图所示：

勒索主逻辑执行，先会导入一个存放在镜像中的RSA公钥，之后调用CryptGenKey生成一组RSA算法的Session key。之后将这组Key的公钥通过CryptExportKey导出，再写入到00000000.pky文件中。将Session key中的私钥用刚导入RSA公钥进行加密，存放在00000000.eky如下图所示：

如果遍历到的文件扩展名在欲加密的文件扩展名列表中，如下图所示：

则会将当前文件路径加入到文件操作列表中，在遍历文件结束后一并进行文件操作。代码如下图：

对于每个需要加密的文件，都会调用CryptGenRadom随机生成AES密钥，之后使用Session Key中的RSA公钥对AES密钥进行加密，存放在加密后的数据文件头中，之后将原始文件数据用该AES密钥进行加密。如下图所示：

整体加密流程，如下图所示：

因为病毒是生成加密过的用户文件后再删除原始文件，所以存在通过文件恢复类工具恢复原始未加密文件的可能。但是因为病毒对文件系统的修改操作过于频繁，导致被删除的原始文件数据块被覆盖，致使实际恢复效果有限。且随着系统持续运行，恢复类工具恢复数据的可能性会显著降低。

三、关于“WannaCry”新变种的说明

早期版本的“WannaCry”病毒存在“Kill Switch”开关，也就是病毒中检测：

“http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com”

这个网址是否可以访问的代码片段，如果可以访问则不会利用“永恒之蓝”漏洞继续传播。

现在这个域名已经被注册，这个版本“WannaCry”传播功能等于已经关闭，因为这段代码本身没有加密，所以很可能会被得到改病毒样本的“骇客”修改，放开开关，使病毒继续传播。

截止到今日，火绒已经收集到的所谓“WannaCry”最新版本的“变种”，正如我们推测的一样，网上两个“热炒”变种，SHA256分别为：

32f24601153be0885f11d62e0a8a2f0280a2034fc981d8184180c5d3b1b9e8cf
c8d816410ebfb134ee14d287a34cea9d34d627a2c5e16234ab726cf9fde47ec6

和早期的“WannaCry”相比

SHA256：

24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

有明显人为修改痕迹，如下图所示：

这个样本仅仅是16进制修改了两个字节，让“Kill Switch”失效，这个修改不会影响火绒的检测。

另外一个样本除了修改了“Kill Switch”域名，还修改了病毒携带勒索模块。经过测试勒索代码已经被修改坏了，无法运行。如下图：

除了以上两个样本，火绒还截获另一个人修改的“WannaCry”样本，同样被修改的不能运行，火绒依然可以检测。SHA256如下：

99c0d50b088df94cb0b150a203de6433cb97d4f8fd3b106ce442757c5faa35c4

截止到本篇分析完成火绒还没截获所谓关闭“Kill Switch”开关的病毒样本。

四、附录

样本SHA256

Worm

24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

32f24601153be0885f11d62e0a8a2f0280a2034fc981d8184180c5d3b1b9e8cf

C8d816410ebfb134ee14d287a34cea9d34d627a2c5e16234ab726cf9fde47ec6

Ransom

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79

2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d

e2d1e34c79295e1163481b3683633d031cab9e086b9ae2ac5e30b08def1b0b47

ec9d3423338d3a0bfccacaf685366cfb8a9ece8dedbd08e8a3d6446a85019d3a

f5cbff5c100866dd744dcbb68ee65e711f86c257dfcc41790a8f63759220881e

f7c7b5e4b051ea5bd0017803f40af13bed224c4b0fd60b890b6784df5bd63494

88be9ee3ce0f85086aec1f2f8409247e8ab4a2a7c8a07af851f8df9814adeee5

5d26835be2cf4f08f2beeff301c06d05035d0a9ec3afacc71dff22813595c0b9

e989935bb173c239a2b3c855161f56de7c24c4e7a79351d3a457dbf082b84d7b

4d67e6c708062e970d020413e460143ed92bebd622e4b8efd6d6a9fdcd07bda8

eeb9cd6a1c4b3949b2ff3134a77



gukehui2012

关注

8

1

25



24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
32f24601153be0885f11d62e0a8a2f0280a2034fc981d8184180c5d3b1b9e8cf
C8d816410ebfb134ee14d287a34cea9d34d627a2c5e16234ab726cf9fde47ec6
fc626fe1e0f4d77b34851a8c60cdd11172472da3b9325bfe288ac8342f6c710a
be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844
1be0b96d502c268cb40da97a16952d89674a9329cb60bac81a96e01cf7356830
c354a9a0bbb975c15e884916dce251807aae788e68725b512a95f7b580828c64
6bf1839a7e72a92a2bb18fbedf1873e4892b00ea4b122e48ae80fac5048db1a7
e0ec1ad116d44030ad9ef5b51f18ff6160a227a46ffcf64693335c7fb946fad6
63c8a30963265353532d80a41cae5d54b31e5c2d6b2a92551d6f6dcadd0dedeb
b4d607fae7d9745f9ced081a92a2dcf96f2d0c72389a66e20059e021f0b58618
67eedfe3f13e2638de7d028aaf1e116410562cc5d15a9e62a904f758770dc6bf
5f2b33deee53390913fd5fb3979685a3db2a7a1ee872d47efc4f8f7d9438341f
01b628fa60560c0cb4a332818cb380a65d0616d19976c084e0c3eaa433288b88
16493ecc4c4bc5746acbe96bd8af001f733114070d694db76ea7b5a0de7ad0ab
d8a9879a99ac7b12e63e6bcae7f965fbf1b63d892a8649ab1d6b08ce711f7127
7e369022da51937781b3efe6c57f824f05cf43cbd66b4a24367a19488d2939e4
9b60c622546dc45cca64df935b71c26dcf4886d6fa811944dbc4e23db9335640
a1d23db1f1e3cc2c4aa02f33fec96346d9d5d5039ffc2ed4a3c65c34b79c5d93
ceb51f66c371b5233e474a605a945c05765906494cd272b0b20b5eca11626c61
3dcbb0c3ede91f8f2e9efb0680fe0d479ff9b9cd94906a86dec415f760c163e1
043e0d0d8b8cda56851f5b853f244f677bd1fd50f869075ef7ba1110771f70c2
b66db13d17ae8bcaf586180e3dcd1e2e0a084b6bc987ac829bbff18c3be7f8b4
940dec2039c7fca4a08d08601971836916c6ad5193be07a88506ba58e06d4b4d
b3c39aeb14425f137b5bd0fd7654f1d6a45c0e8518ef7e209ad63d8dc6d0bac7
aee20f9188a5c3954623583c6b0e6623ec90d5cd3fdec4e1001646e27664002c
a141e45c3b121aa084f23ebbff980c4b96ae8db2a8d6fde459781aa6d8a5e99a
09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
7966d843e5760ece99bd32a15d5cd58dc71b1324fdc87e33be46f377486a1b4b
11d0f63c06263f50b972287b4bbd1abe0089bc993f73d75768b6b41e3d6f6d49
5d8123db7094540954061ab1fbc56eedcd9e01110b62d0f54206e3e75a39776a
11011a590796f6c52b046262f2f60694310fa71441363d9116ada7248e58509a
9cc32c94ce7dc6e48f86704625b6cdc0fda0d2cd7ad769e4d0bb1776903e5a13
4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
5ad4efd90dcde01d26cc6f32f7ce3ce0b4d4951d4b94a19aa097341aff2acaec
b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
63bd325cc229226377342237f59a0af21ae18889ae7c7a130fbe9fd5652707af
a50d6db532a658ebbebe4c13624bc7bdada0dbf4b0f279e0c151992f7271c726
2584e1521065e45ec3c17767c065429038fc6291c091097ea8b22c8a502c41dd
b47e281bfbeeb0758f8c625bed5c5a0d27ee8e0065ceeadd76b0010d226206f0
c1f929afa37253d28074e8fdaf62f0e3447ca3ed9b51203f676c1244b5b86955
4c69f22dfd92b54fbc27f27948af15958adfbfc607d68d6ed0faca394c424ccee
201f42080e1c989774d05d5b127a8cd4b4781f1956b78df7c01112436c89b2c9
22ccdf145e5792a22ad6349aba:



gukehui2012

关注

8

1

25





5dee2ac983640d656f9c0ef2878ee34cda5e82a52d3703f84278ac372877346d1e6753f948fa648ef9e0d85795b7f090968ee1f240efc0628283776ea55ccb0f7bb9ea2c0f53fa96883c54fa4b107764a6319f6026e4574c9feec2cb7d9e7d219174c0772a5f871e58c385c01eea1ed4b706675bf9bd6aa1667b9d3c40acb6fc3e6de9e2baacf930949647c399818e7a2caea2626df6a468407854aaa515eed9a3900daf137c81ca37a4bf10e9857526d3978be085be265393f98cb075795740ca29de1dc8817868c93e54b09f557fe14e40083c0955294df5bd91f52ba469c857c12d8573d2f3883a8a0ba14e3eec02ac1c61dee6b675b6c0d16e221c3777f4fc626fe1e0f4d77b34851a8c60cdd11172472da3b9325bfe288ac8342f6c710a190d9c3e071a38cb26211bfffefeb6c4bb88bd74c6bf99db9bb1f084c6a7e1df4e31c2024d0df684a968115e4c3fc5703ef0ea2de1b69ece581589e86ba084568a0bb221bf62d875cca625778324fe5bd6907640f6998d21f3106a0447aabc1e3ce14f1a655d54254d06d51cd23a2fa57b6ffdf371cf6b828ee483b1b1d6d21079e8450dd6f908b23c9cbd6011fe3d940b24c0420a208d6924e2d920f92c894a96aea79945c0f2f60de43193e1973fd30485b81d06f3397d397cb02986b31e30d99fb39f162c1e1eb55fbf38e670d5e329d84542d3dfcdc341a99f5d07c4b5097778e3f87f31688355c0f398317b2d87d803bd87ee3656c5a7c80f0561ec8606df7c465ea7bcccf4f94147add808f24629644be11c0ba4823f16e8c19e0090f0ff24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c2ddc29a646c1579e79c0b4cc86a5d0c9ed57af6ff240e959b17cdcf77d8630264b76e54de0243274f97430b26624c44694fbde3289ed81a160e0754ab9f56f32498b8b889bb1f02a377a6a8f0e39f9db4e70cccad820c6e5bc5652e989ae6204f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235ccbe782d85dff26a9a44baa3ce109b8df41ae0a301d9e4a28ad7bd7721bbb7ccd137bfd696593bbcc8f34047da9960b8456094c0eaf69caaf16f1626b813484207df8bd8af149601e15002f78866ab73033eb8577f11bd489a4cea87b10c52a70fdf78d9ffac7f0fb9a7bb68640612567153a157e91d457095eadfd2a76d27a7f65c53ba82


作者：曹越超 来源：火绒安全


勒索病毒WannaCry深度技术分析 08-01
勒索病毒，WannaCry，想哭，深度技术分析。勒索病毒自从2017年开始全球泛滥，并且愈演愈烈，引起了广泛关注

WannaCry勒索病毒一键加固v1.1 05-14
WannaCry勒索病毒一键加固v1.1，wana Decrypt0r 2.0 勒索软件。支持系统win7、10、2003、2012、2016。该工具...

 优质评论可以帮助作者获得更高权重

 评论

 weixin_43821688: 火绒? 2 年前 回复 ...

 3

< 1 >

WannaCry 勒索病毒复现及分析,蠕虫传播机制全网源码详... 10-15
WannaCry是一种"蠕虫式"勒索病毒软件,由不法分子利用NSA泄露方程式工具包的危险漏洞"EternalBlue"(永恒之蓝)进...

WannaCry勒索病毒全解读,权威修复指南大集合_dfdhxb995... 10-13
5月15日下午2点,360公司针对此次事件进行了还原及技术解读,安全产品的总负责人孙晓骏、核心安全技术组负责人郑...

关于防范ONION勒索软件病毒攻击的解决办法 Sual的博客 2935
一夜之间，身边的好多同学的电脑都中毒了，特别是许多正在写毕业论文的同学可真是坑大了，磁盘文件会被病毒加...

勒索病毒WannaCry深度技术分析——详解传播、感染和危害细节 liweiminlining的专栏 1115
一、综述 5月12日，全球爆发的勒索病毒WannaCry借助高危漏洞“永恒之蓝”（EternalBlue）在世界范围内爆发，据报...

WannaCry病毒分析 weixin_44953050的博客 446
样本一 查壳 VC6.0编写，未加壳 使用LoadPE查看导入表，根据导入函数猜测功能 猜测可能和文件操作有关，因为导...

[系统安全] 二十七.WannaCry勒索病毒分析 (3)蠕虫传播机制解析及IDA和OD逆向 杨秀璋的专栏 2823
前文分享了MSF利用MS17-010漏洞进行反弹Shell，



gukehui2012

关注

8

1

25



最新评论

解决IE浏览器下document click事件失效...
看把你给能的。: [code=javascript] [/cod
Web页面分页打印小结-简单实现
qq_40995828: 一个通用的Web打印分页插
件，其中：block-box的插入方式适用不 ...
网页实现扫码录入，小问题记录
村里人呐: 可以分享源码吗
实现WebService只返还json结构数据
gukehui2012 回复 HHeroDeng: 创建一个静
态类，然后增加静态方法GetJsonData(...
实现WebService只返还json结构数据
gukehui2012 回复 珠穆郎码疯@: 参数jsonD
ata 是你自己的json 字符串。利用方法： ...

您愿意向朋友推荐“博客详情页”吗？


强烈不推荐


不推荐


一般般


推荐


强烈推荐

最新文章

windows server 2008/2012 忘记登陆密码
超时时间已到。超时时间已到，但是尚未从
池中获取连接。出现这种情况可能是因为所有
池连接均在使用，并且达到了最大池大
小。
win2012下IIS8.5网站权限设置【未证实】
2018年 3篇 2017年 17篇
2016年 1篇