Wannacry 勒索软件分析

diffway / 2017-05-14 00:48:00 / 浏览数 6413 技术文章 技术文章 顶(0) 踩(0)

作者：兰云科技@diffway

1概述

Wannacry勒索软件在全球大规模爆发，主要利用了NAS前一个月泄露的黑客工具中Elternal Blue (MS_17_010)
漏洞,变成了可怕的勒索软件蠕虫，在全球多处发现被攻击，并在在以惊人的速度进行传播，下面是最勒索软件加密的详细分析，供大家参考。

2静态分析

MD5	84c82835a5d21bbcf75a61706d8ab549
编译时间	2010\11\21
编译器信息	Microsoft Visual C++ ver 5.0/6.0
壳信息	无壳

3详细分析

在我们分析的样本中，启动后判断有没有参数/I
如果有则将样本拷贝重命名并以服务的方式启动（并没有像其他分析报告中提到的会连接一个特定的网址，连接成功后就不再发作，因此我们一定要注意遇到的是哪个样本，

我们先看看当加上 /i的参数后会执行什么：

首先设置C:\Intel\aypxkvhkzwrro805为当前目录，并将样本重命名为tasksche.exe 然后复制过去。

接着创建服务并以服务的方式启动起来 。

下面我们看看当没有参数的时候是如何 进行加密的

首先样本会创建一个注册表项，我们可以看到注册表项包含了勒索软件的名称WanaCrypt

接着新建了一个键值，将当前目录写入。

之后开始查找资源，资源名称为80A，会释放很多文件。

msg文件夹里面包含多种语言的付款方法。

其中c.wnry里面存了黑客的比特币地址，是硬编码在里面的

之后执行了两个命令分别是设置当前目录隐藏属性 赋予Everyone用户完整控制权限

导入加密函数，对抗一些静态查杀

先是初始化容器，可以看到加密类型为 0x18，也就是PROV_RSA_AES加密类型。

之后导入RSA公钥（这个公钥经过分析主要是用于解密内置密文，而非用于加密数据）

之后打开了之前释放的t.wnry,并读取其中的内容，对其中内容进行了解密，里面是关键加密代码

把文件dump 出来进行分析，可以看到这个文件是一个DLL文件，导出函数有一个为

TaskStart,而样本最终会跳转过去的执行的就是这个TaskStart

TaskStart函数包含了关键的加密功能，下面我们详细分析这个DLL文件：

首先说一下整体的加密过程，样本首先生成一对2048位的RSA公私钥，这对密钥的公钥用于加密一会生成的AES密钥，私钥主要用于以后的解密。黑客自己有一对RSA的公私

下面是加密过程详细分析：

首先创建了一个加密容器 加密类型仍然为 PROV_RSA_AES

仍然导入了一个RSA公钥，这个公钥是黑客的公钥，用于加密下面生成的私钥

然后程序继续生成了一对2048位RSA公私密钥

之后黑客导出了刚才生成的RSA 2048位公钥

并将公钥放入创建的00000000.pky文件中

导出私钥，并且用黑客自己的公钥将这个私钥进行加密

之后黑客又加密这段数据放到上面加密的私钥的末尾，并最后存在0000000.eky

之后启动一些线程，做后续的准备工作

先生成一个文件00000000.res,,将之前生成的一些随机数存入文件

启动之前生成的taskdl.exe 这个程序主要是删除临时文件夹下的文件

设置自启动

之后运行了一个bat文件主要是设置一个链接

将u.wnry重命名为@WanaDecryptor@.exe ，这是解密程序

然后开始进行寻找目标文件进行加密

这个时候导入了两个公钥，一个导入从0000000.pky中公钥，这个公钥主要用于加密生成的128位AES密钥，另外一个用于加密一些可免费解密的文件

之后开始遍历文件进行加密，会被加密的文件类型为：

```
".doc" ".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"

".potm"".edb"".hwp"".602"".sxi"".sti"".sldx"".sldm"".vdi"".vmdk"".vmx"".gpg"".aes"".ARC" ".PAQ"".bz2" ".tbk"".bak"".tar"".tgz"

".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"

".stw"".sxw"".ott"".odt"".pem"".p12"".csr" ".crt" ".key"".pfx"".der"
```

在匹配到文件类型以后，会通过CryptGenRandom生成的随机AES128位密钥

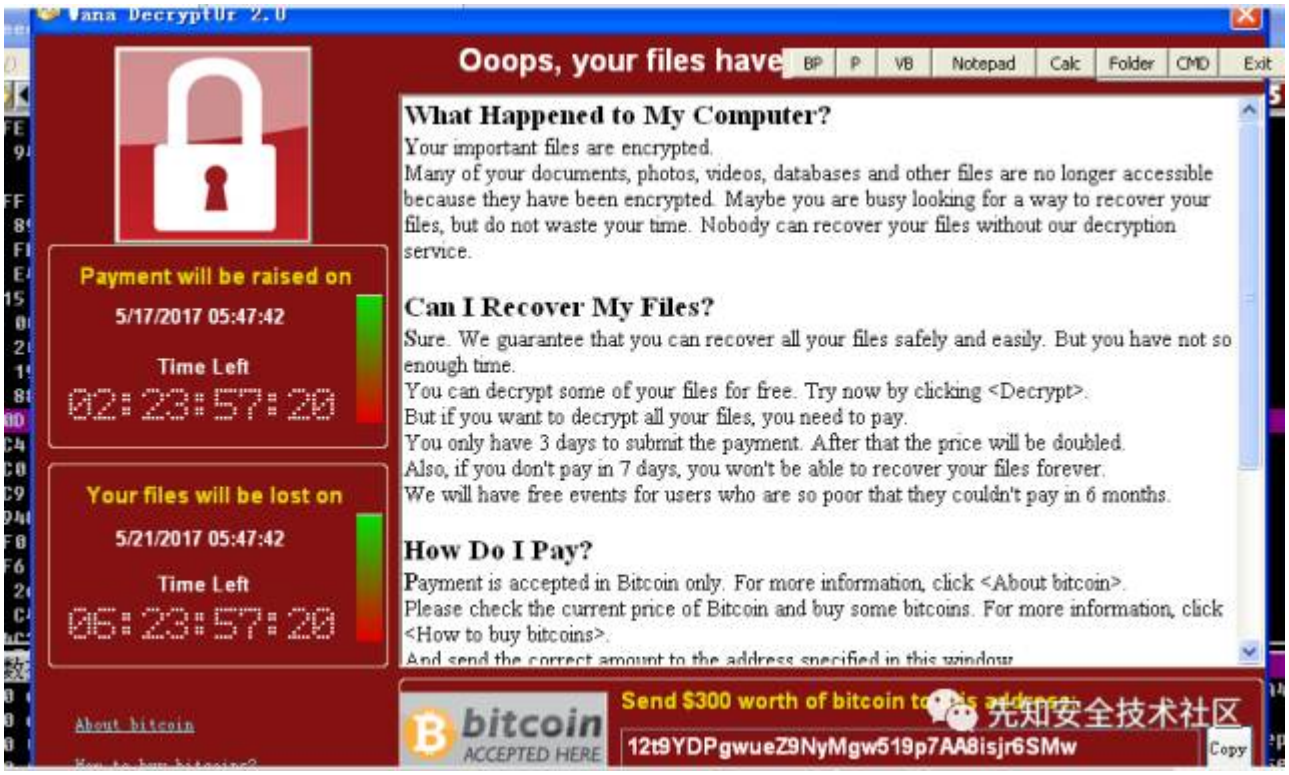
使用通过RSA对AES密钥进行加密

通过AES加密算法对文件进行加密，AES加密算法并没有使用动态调用系统API的方式，而是通过静态编译的方式调用。

在加密免费文件的时候会把文件路径放入到f.wnry中（我们只需查看这个文件就可以找出哪些文件可以被免费恢复）

之后黑客会进行网络连接和传播，主要在taskhsvc这个文件里面

最后是成功运行时的提示用户去支付的界面



本次分析就先到此，我们会进一步分析传播部分。

4总结

□ 此次勒索软件结合高危漏洞变成蠕虫对我们敲响了警钟，对这次事件大家应该积极应对起来，对个人主机通过打补丁结合主机防火墙进行多方位的防护。