Spore勒索软件分析

diffway / 2017-02-08 13:34:00 / 浏览数 3842 技术文章 技术文章 顶(0) 踩(0)

---

1. 概述

Spore勒索软件，通过邮件进行传播，其中整个勒索软件有以下特点
1完美的密钥管理，无需C&C服务器上传密钥
2 一个简洁的提供勒索解密的网站（可聊天、提供免疫方案）
3 文件夹快捷方式传播

1. 详细分析

首先看一下勒索软件运行之后会在本地留下一个网页，并显示网页，如下图所示

看不懂俄文，翻译成中文

在输入IP之后，发现页面做的非常简洁，可以看到下面提供的服务，这些服务相比其他的勒索软件价格还是比较低的在，这个样本最大的特点是提供了一个免疫的选项，你可

下面是样本的详细分析

文件类型
Hta
文件MD5
37477dec05d8ae50aa5204559c81bde3

此文件的主要功能在临时文件存放一个close.js文件，然后运行这个文件

下面开始分析这个js文件

文件类型
Js
文件MD5
fc1b2bec47aaa059319f4a47cb37c5e2

可以看下这个js文件

转换成比较好看的格式，可以看个前面是个解密的过程的，加个断点，重点关注下b这个变量

放到VS中进行调试

经过解密后，调用解密出的函数

弄出可读形式更高的

又解密出一个函数，进行调用

又继续解密

在临时文件夹中添加一个docx文件，但是只写入一个字节

并运行这个doc文件

运行之后是崩溃，应该黑客是为了，让用户忙于关闭这个崩溃的doc文件，为运行自己的勒索软件赢取时间，最后运行释放在临时文件中的exe

下面分析exe样本
文件类型
Exe
文件大小
19,456 字节
文件MD5
312445d2cca1cf82406af567596b9d8c
壳信息
UPX 2.90
文件编译时间
2017-01-09 23:44:29

首先进行脱壳，这个压缩壳EXP定律法就可以搞定了

样本首先会取得C:\WINDOWS\system32\ntdll.dll 文件的主版本号，用于判断样本实在XP中或者是在xp以上的系统中

获取硬盘序列号

获取硬盘序列号之后，前面加上m，创建互斥量，并且已经创建则退出

样本会判断是否有参数 /u

当没有参数U的时候，首先会解密出公钥和要最后展示的HTML文件

下面开始对文件进行加密，要加密的文件有
Xls doc xlsx docx rtf odt pdf psd dwg cdrcd mdb 1cd dbf sqlite accdb jpg jpeg tiff zip rar 7z backup

并对下面的四个文件夹是不进行加密的

对共享文件要进行加密的文件进行收集

将收集到的需要的加密的文件路径进行加密然后保存在文件中，用于解密时候调用

下面说说加密，会产生一个1024比特的RSA公私密钥

然后导出公私钥，并加入一些计算机信息 比如时间、计算机名称等等，并将这段MD5哈希

继续创建 AES 256位密钥

用生成的AES密钥加密生成的RSA私钥，然后用硬编码的RSA公钥加密AES密钥

创建密钥文件，并将上面加密的数据存入

然后分别将key文件拷贝到以下目录
C:\CH775-9FETR-TZTZT-ROTRF.KEY
C:\Documents andSettings\Administrator\Templates\CH775-9FETR-TZTZT-ROTRF.KEY

C:\Documents and Settings\Administrator\桌面\CH775-9FETR-TZTZT-ROTRF.KEY

然后对文件开始加密，首先会计算文件CRC32，只计算80字节

然后继续创建一个AES密钥，然后将文件内容和CRC32算出的值进行加密

最后将计算AES密钥的CRC，并将计算的CRC和AES密钥写入文件

最后将HTML文件显示出来

然后执行，下图的的命令，首先删除所有的卷影副本，防止数据恢复
并却通过下面的两个命令防止修复
bcdedit /set {default} recoveryenabledno 禁用自动修复
bcdedit /set {default} bootstatuspolicyignoreallfailures 启动策略，禁用Windows 7 的自动修复（忽略错误）

这个并没有pypassUAC,所以每次在win7及以上运行的时候都会弹框提示需要权限

最后，样本还有感染快捷方式的动作，也就是说，即使解密了，不进行免疫的话，样本也会再次运行，我们可以看到下面的文件夹快捷方式都被感染，会运行样本

C:\Windows\system32\cmd.exe /c explorer.exe"Windows" & type"0ae282d1-ebb3-fa26-c2c4-243ecd668970.exe"
>"%tmp%\0ae282d1-ebb3-fa26-c2c4-243ecd668970.exe" & start"Windows" "%tmp%\0ae282d1-ebb3-fa26-c2c4-243ecd668970.exe"

删除快捷方式的小箭头后无法将图标锁定到任务栏

3 免疫方案（预防措施）

由于样本会获取硬盘序列号，前面加上m,创建互斥量，如果有则推出，我们可以事先创建一个这样的互斥量，可以达到免疫的效果

上一篇：Chrome中"自动填充"安全性研究 下一篇：我回阿里的29个月
1. 2 条回复


笑然 2017-02-08 13:45:46

勒索软件精品文章，双倍奖励。

0 回复Ta

熊猫正正 2017-02-10 03:40:14

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板