Emotet恶意软件变种分析

目录

[Emotet恶意软件变种分析 1](#_Toc29222736)

[1. 概述 2](#_Toc29222737)

[2. 恶意文档分析 2](#_Toc29222738)

[3. Payload分析 4](#_Toc29222739)

[4. Shellcode分析 6](#_Toc29222740)

[5. PE文件分析 8](#_Toc29222741)

[6. 执行流程 16](#_Toc29222742)

[7. 行为特征 16](#_Toc29222743)

[8. 威胁分析 17](#_Toc29222744)

[9. 防范措施 18](#_Toc29222745)

[10. IOC 18](#_Toc29222746)

# 概述

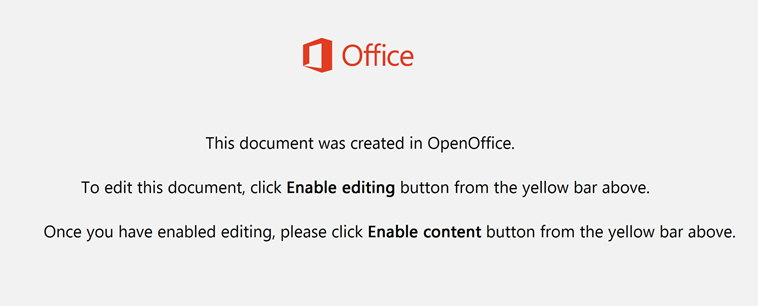
Emotet是一种通过垃圾邮件传播的恶意软件木马，自2014年被发现以来，历经过多次版本的迭代。其早期版本是作为恶意JavaScript文件提供的，后来的版本逐渐演变为使用启用了宏的Office文档从C2服务器检索恶意有效负载。

由于具有模块化架构及自我传播功能，该木马可以根据不同情形传播恶意软件。因此，该木马从早期的针对欧洲的银行客户的银行木马，逐渐发展成为了为全球其他恶意者提供恶意软件包装和交付服务。近来，对开源威胁情报源进行分析，发现Emotet僵尸网络恶意活动剧增，出现了多种不同的恶意Word文档样本，国内多家企业受到了Emotet木马邮件的攻击。

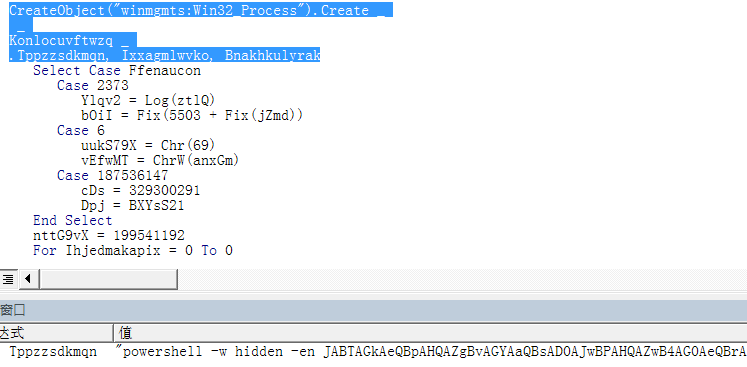
本文中，将对12月初发现的样本进行详细分析，包括邮件诱导用户启用宏进而执行宏代码，PowerShell命令下载并运行Emotet恶意软件，Emotet木马与C2服务器进行通信等。

# 恶意文档分析

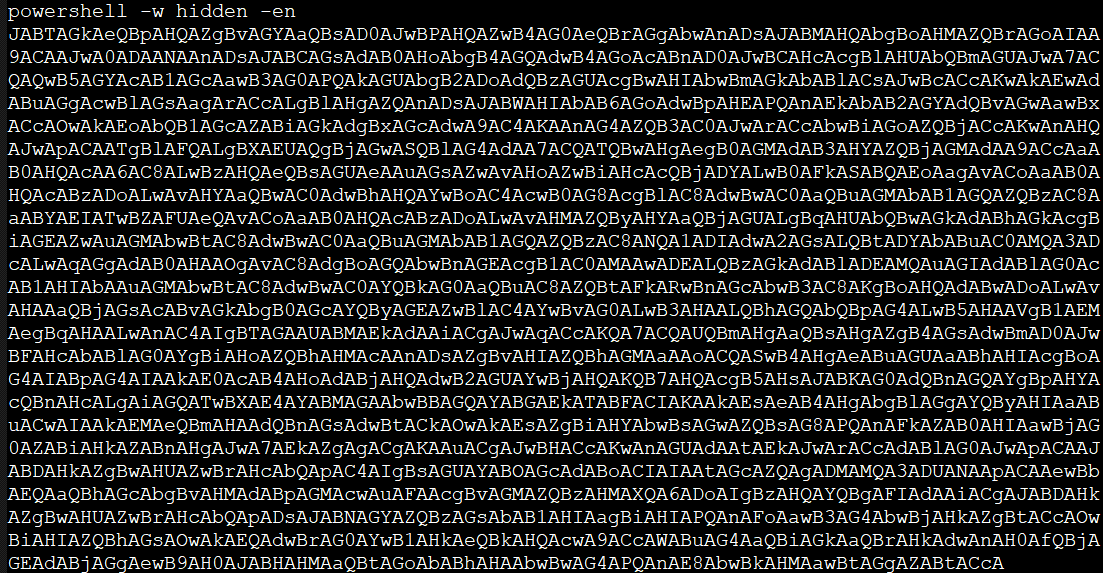
恶意文件为伪造的word文档，显示内容为诱导用户启用宏：



若用户启用宏功能，则会触发AutoOpen自动宏，从而执行宏代码。这个恶意文档中的宏代码的功能是拼接一段由base64编码的PowerShell代码，然后调用Win32\_Process类的Create方法创建一个新进程执行PowerShell代码：



下面是提取出来的PowerShell代码：



将这段PowerShell脚本用base64解码，并对其中的混淆进行处理，得到了最终的PowerShell脚本内容：



显然，这个脚本的功能是从5个远程服务器上下载payload，若下载成功，则执行这个payload（本文中的payload为404.exe）。

# Payload分析

这个Payload相关的文件信息如下：

|  |  |
| --- | --- |
| 文件名 | 404.exe |
| 文件大小 | 462854 bytes |
| 编译时间 | 2019年12月6日 8:49:05 |
| MD5 | 0b158b803453519011f207708d3baff9 |
| SHA 256 | fd6cd0466f97acdd70376364729e85b  29eaefea3f2d93f53afe9bfa7c45e02d2 |

首先定位到Payload的WinMain函数，发现这个Payload是使用MFC基础类库编写的：



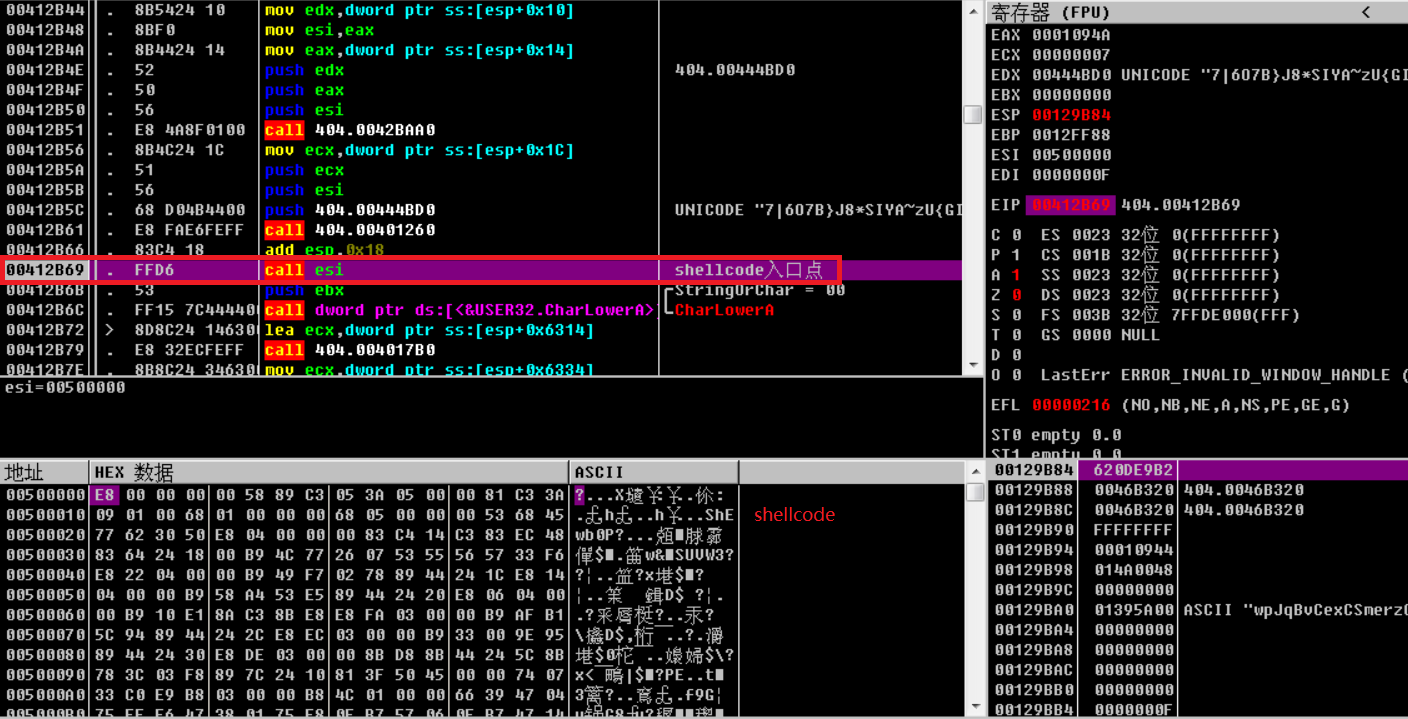
进入payload的核心代码区域，主要功能为解密Shellcode。解密的过程是由上百个类似的代码块组成，每个代码块由一个硬编码的密钥和两个复杂的解密函数构成。这个解密过程会完成整个Shellcode的第一次解密。单个代码块构成如下：



然后，再分配一块内存空间，将加密的Shellcode拷贝到这个内存中，再进行一次简单的解密操作，如下图：

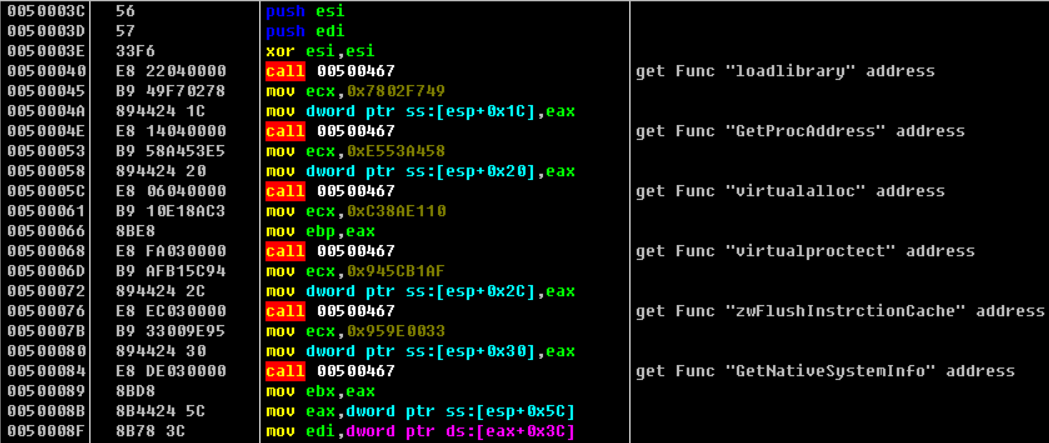


得到最终解密完成的Shellcode, 并执行这个Shellcode：

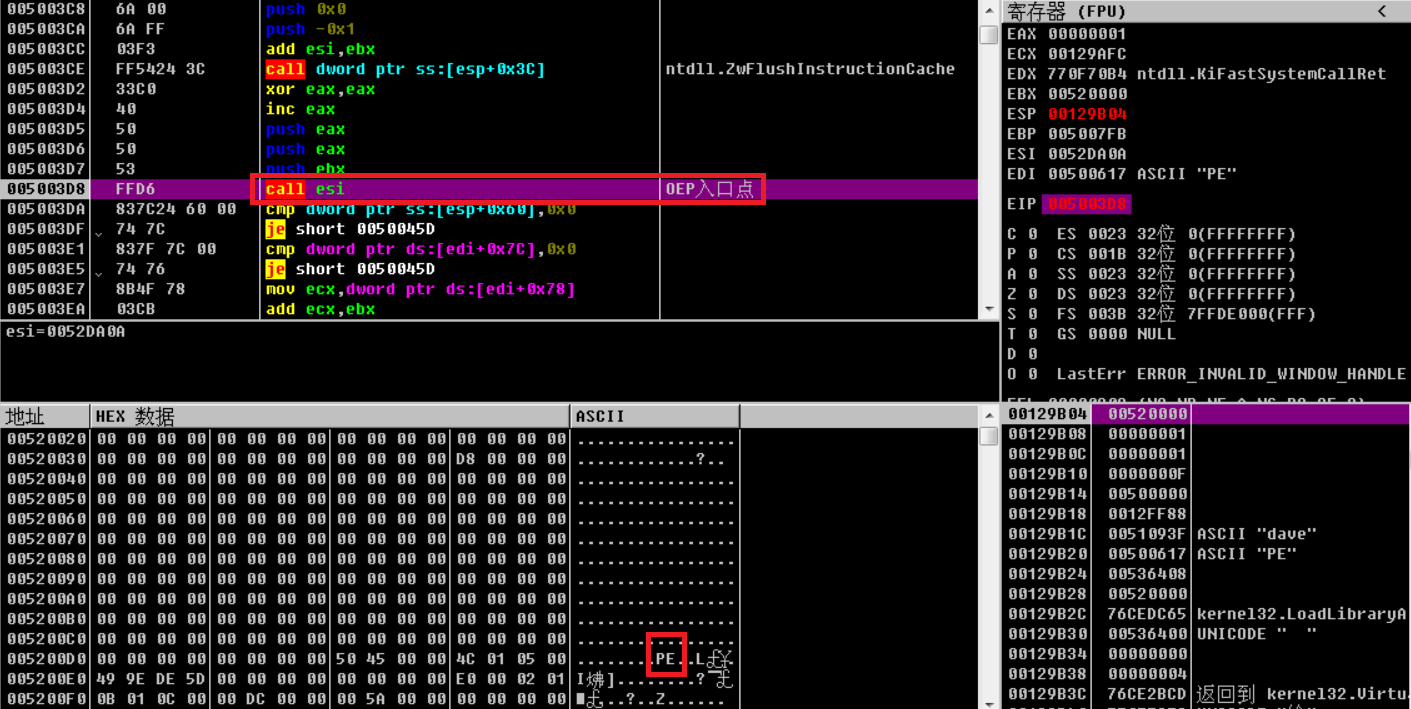


# Shellcode分析

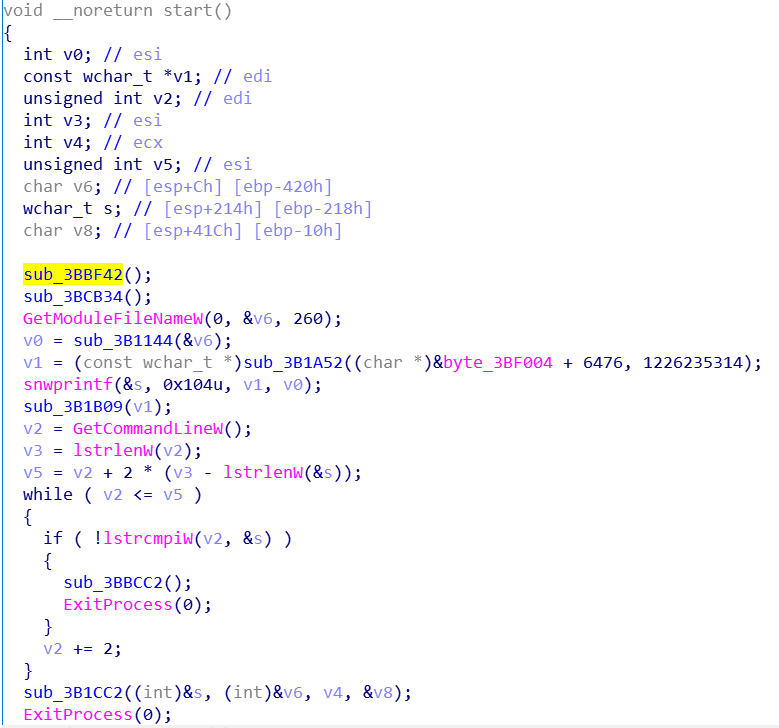
Shellcode加载了所需函数的地址，如下图：



经过调试分析，Shellcode在内存中加载了一个PE文件（删除了DOS头）：

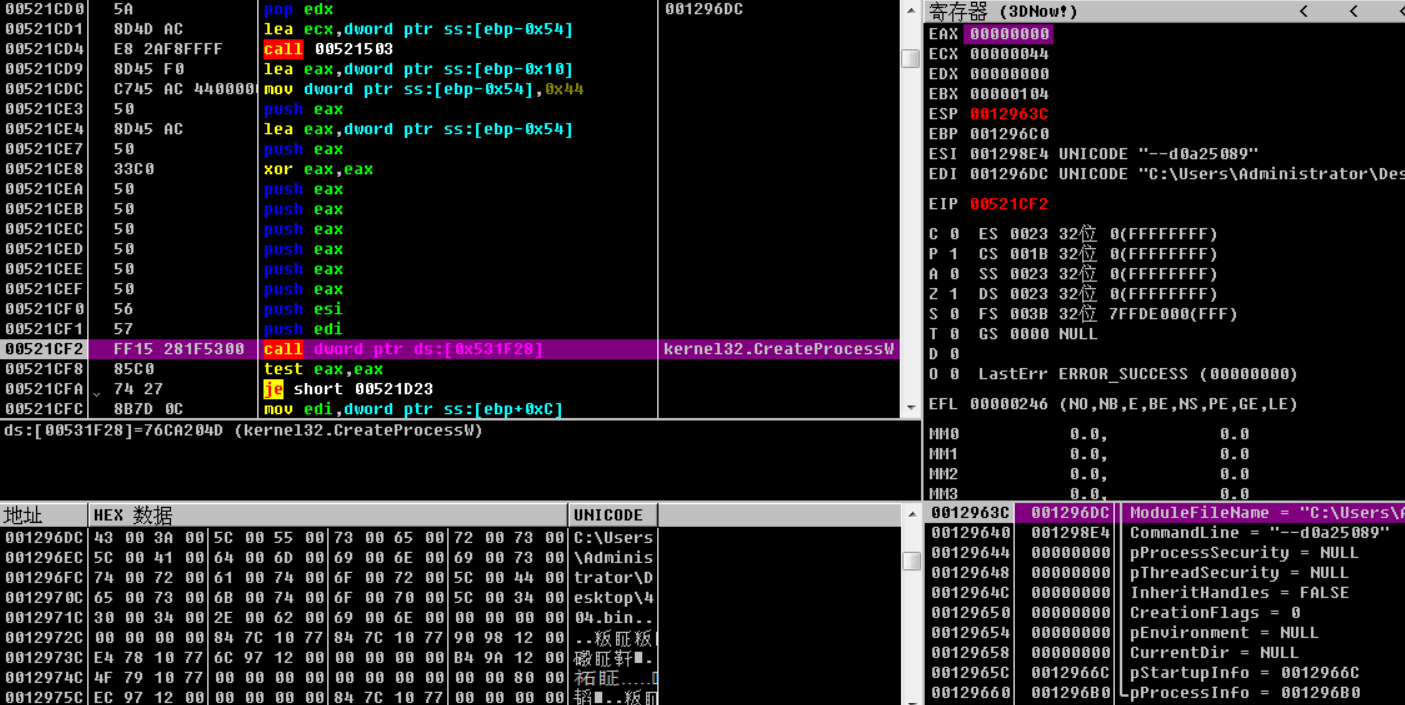


因此，可以先修复PE文件的DOS头，再从内存dump出PE文件进行静态分析。这个PE文件实现了Emotet恶意软件的核心功能。

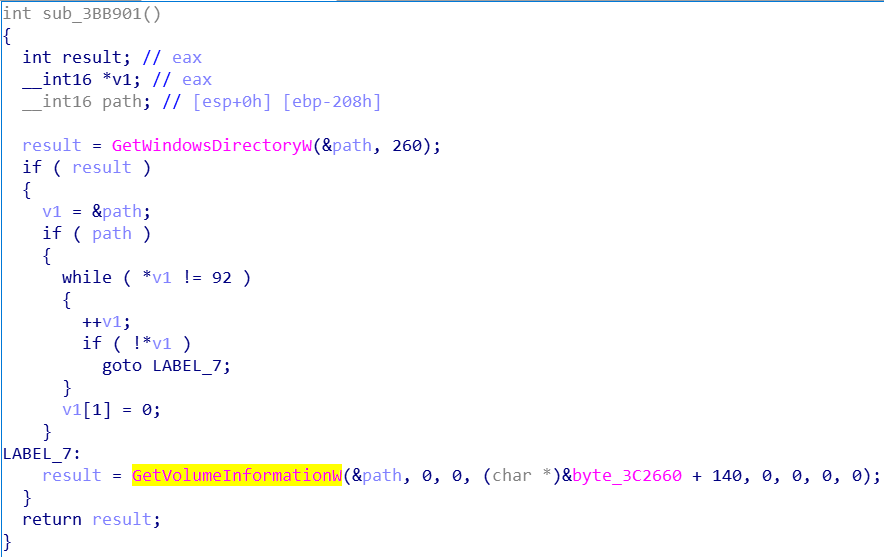


# PE文件分析

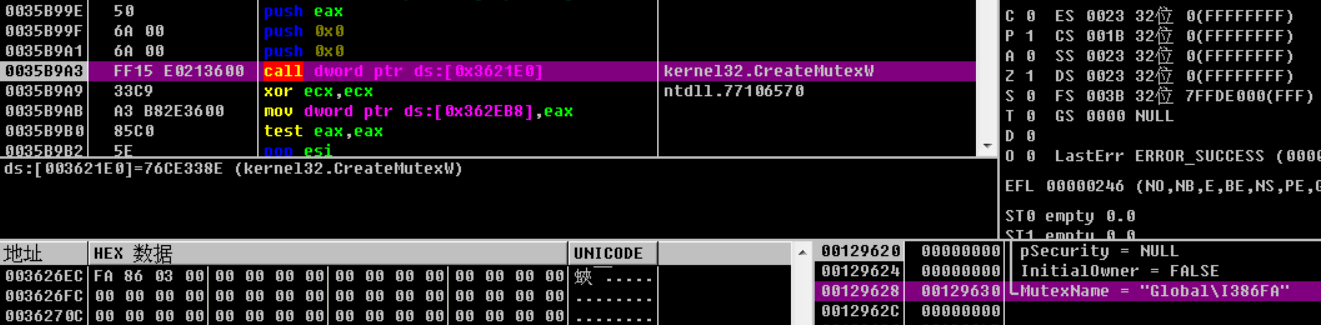
Emotet恶意软件会先获取进程的文件路径，然后根据这个路径计算得到一个命令行参数，这里是“--d0a25089”。然后获取当前进程的命令行参数与“--d0a25089”进行比较：如果参数不同，则以参数“--d0a25089”重新启动自身并退出当前进程：

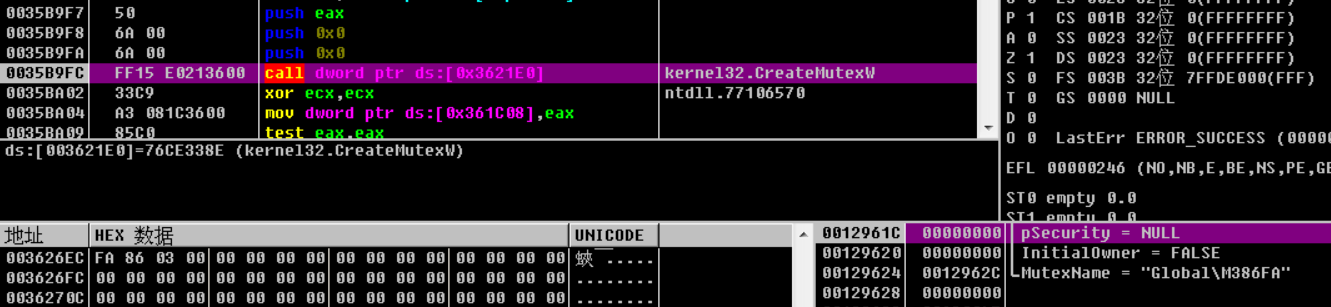


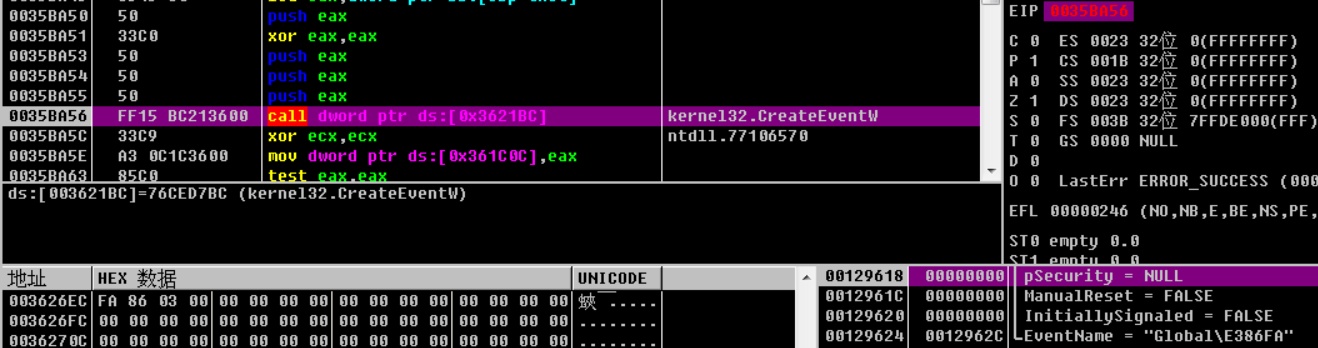
带参数启动后，检索Windows目录的路径，获取Windows目录所在磁盘（C:\）的磁盘序列号：



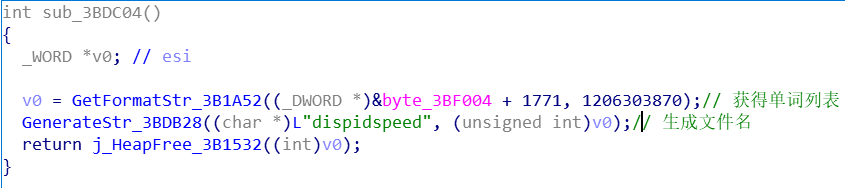
根据获得的磁盘序列号，创建互斥体“Global\I386FA”、“Global\M386FA”和“Global\E386FA”：







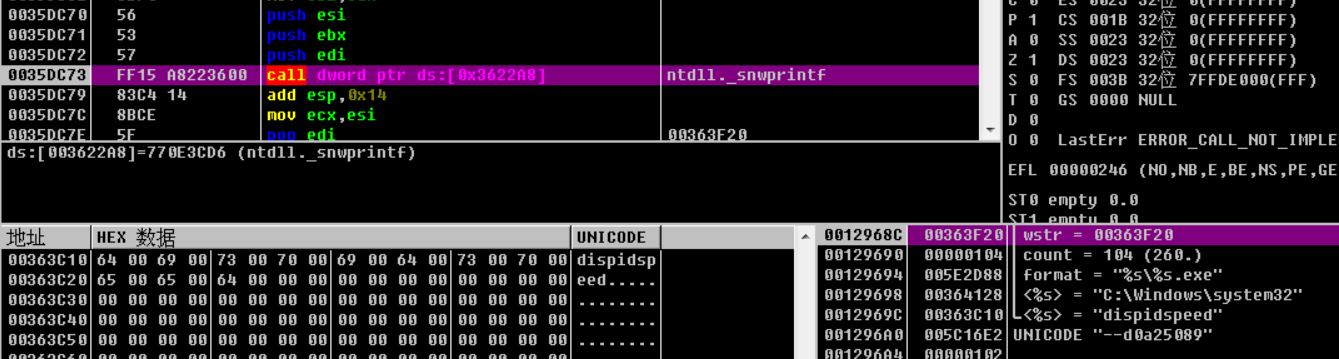
接着，根据算法从单词列表中挑选两个单词生成一个文件名（用于实现隐藏功能）：



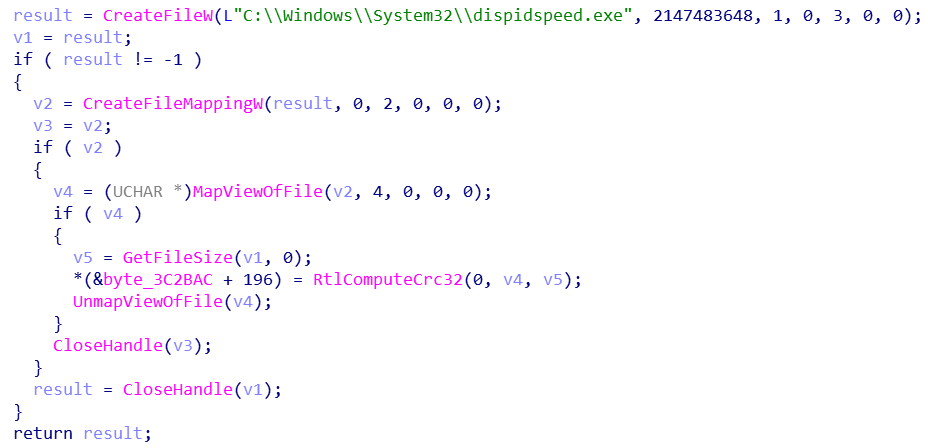
单词列表中包含下列64个单词，共4096种组合方式：

|  |
| --- |
| texas,func,deploy,run,leel,stuck,def,print,hal,monthly,pdf,char,netsh,memo,trns,rds,maker,  more,textto,chunker,mailbox,compon,shades,scan,non,wsat,speed,publish,manual,hant,inbox,  malert,zap,fill,angle,wrap,boost,cors,iplk,sitka,wow,prints,acquire,wiz,smo,footer,attrib,  group,appid,xcl,sensor,methods,ipmi,raw,title,nic,ias,lua,dispid,special,serial,wsa,tcg,msp |

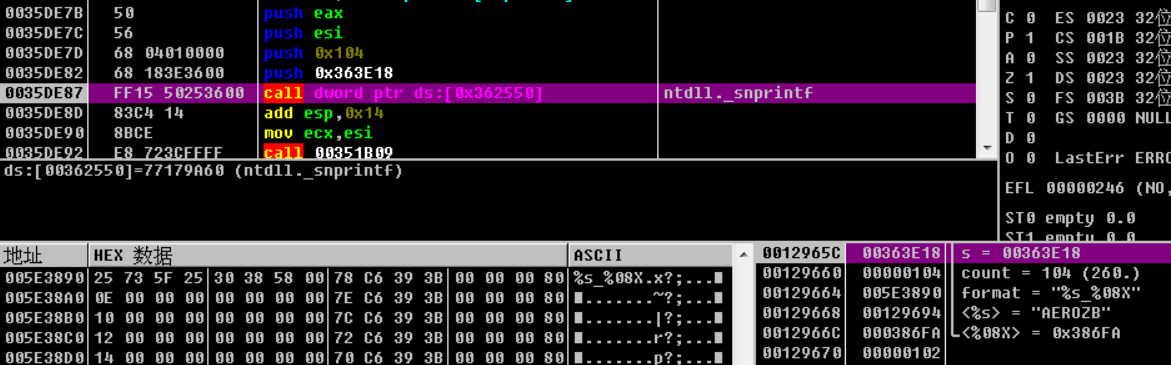
用文件名（这里是dispidspeed）和系统目录拼接出新的文件路径：



打开当前进程的文件，将自身文件映射到内存并计算crc32的值：



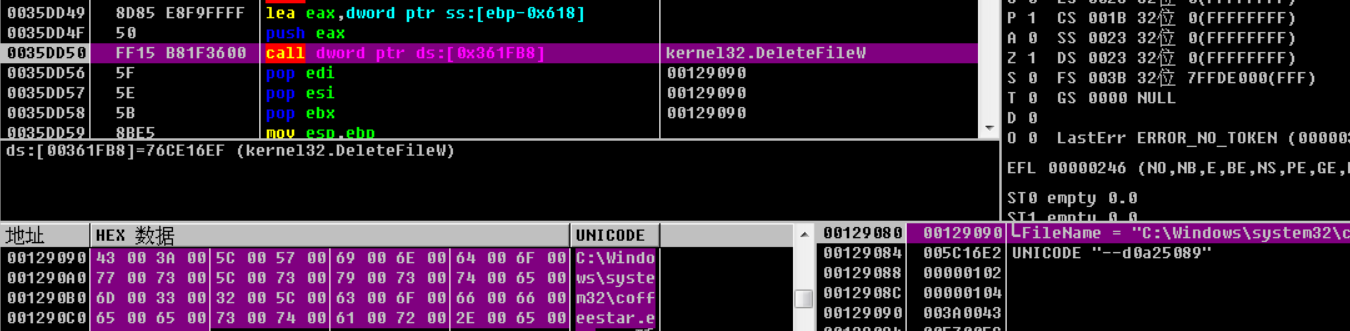
获得计算机名，和前面获得的磁盘序列号拼接成一个字符串：



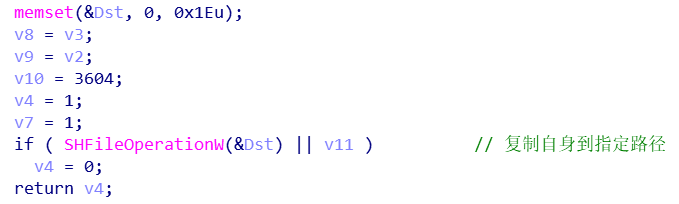
接着，又获取了一个单词列表（与前面的不同），使用相同的算法计算得到一个文件名（这里是coffeestar）,单词列表如下：

|  |
| --- |
| delete,band,ipsm,sspi,div,rdp,whole,dir,privacy,make,watched,pano,which,goto,wnd,rep,ceip,  date,render,bag,vsc,vsa,mouse,counter,tech,wheel,ranker,iterate,store,sum,package,timeout,  idebug,junos,site,trc,url,coffee,poller,remote,gapa,changes,duck,ppl,tlogcm,tlb,cube,hexa,  vol,paint,star,nav,grp,avatar,center,cipher,brm,resize,markup,pausea,loan,emboss,vsperf,teal |

同样的，拼接成系统文件路径“C:\Windows\system32\coffeestar.exe”，将该路径的文件删除。但是分析环境中并不存在这个文件。经过查阅资料可知，这个单词列表是旧版本的Emotet木马的文件名生成列表，因此，这个操作是删除旧版本的Emotet木马。



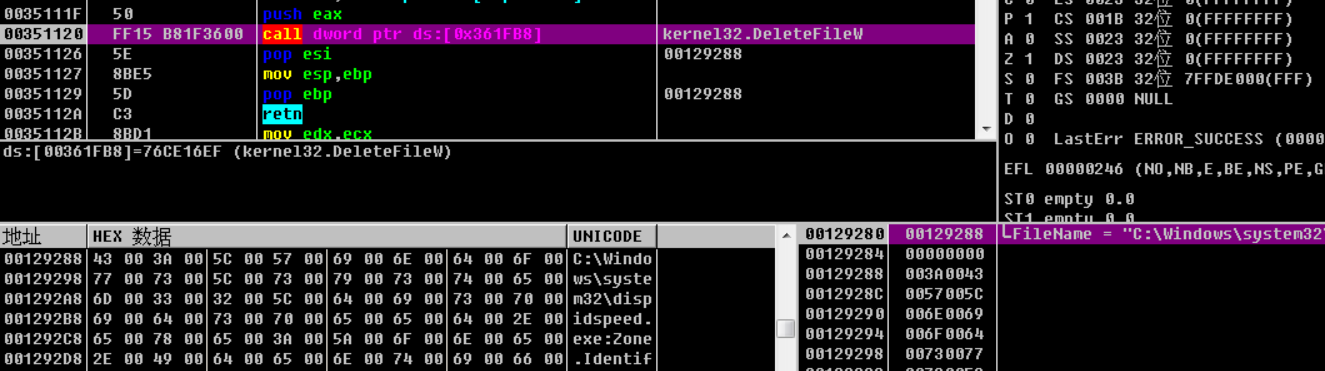
经过前面的铺垫后，判断系统目录下dispidspeed.exe文件是否存在：如果不存在，则将自身文件拷贝到系统目录下：



如果拷贝到系统目录失败，则拷贝到临时目录：



拷贝完成后，删除文件的Zone.Identifier属性（是否是从Internet上下载）：



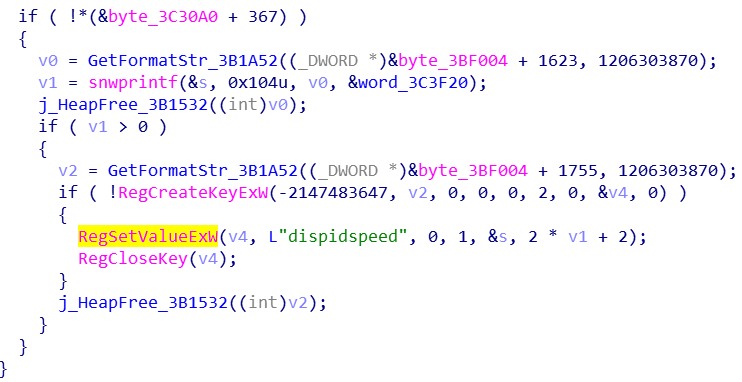
创建名为“dispidspeed”的系统服务，然后启动服务dispidspeed.exe，退出当前进程：



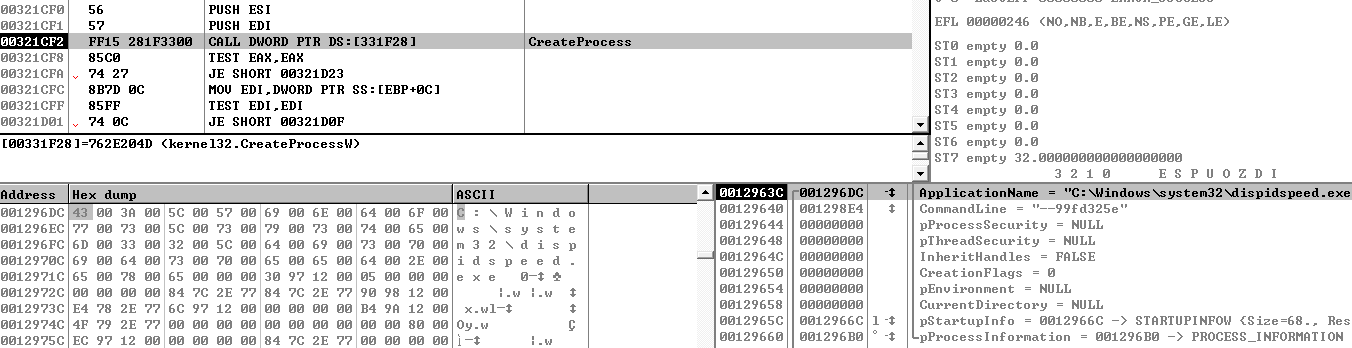
并且，服务的描述信息也被修改了，非常具有迷惑性：



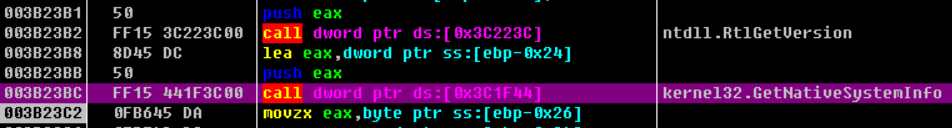
如果打开服务控制管理器失败，不能以服务的方式实现自启动，则通过写入Run注册表的方式确保自身可以自启动：



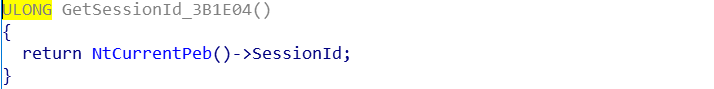
以系统服务的方式启动后，会再次验证启动的参数（这里是“—99fd325e”）：如果不是，则退出当前进程，带参数“—99fd325e”重新启动：



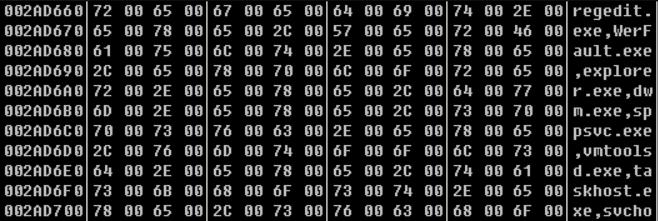
获取当前的系统信息：



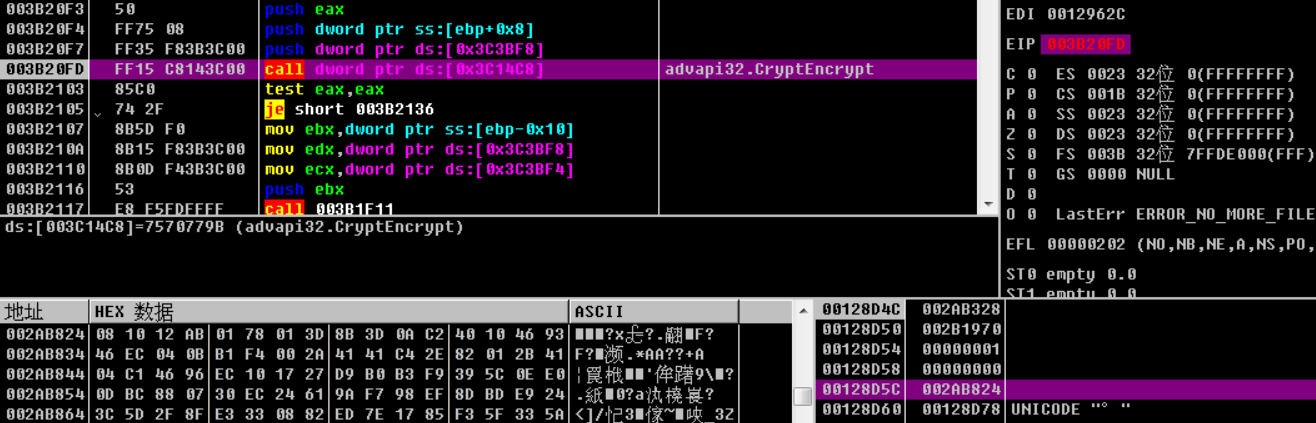
获取当前进程的SessionID：



枚举当前的进程，把进程名存储在内存中：



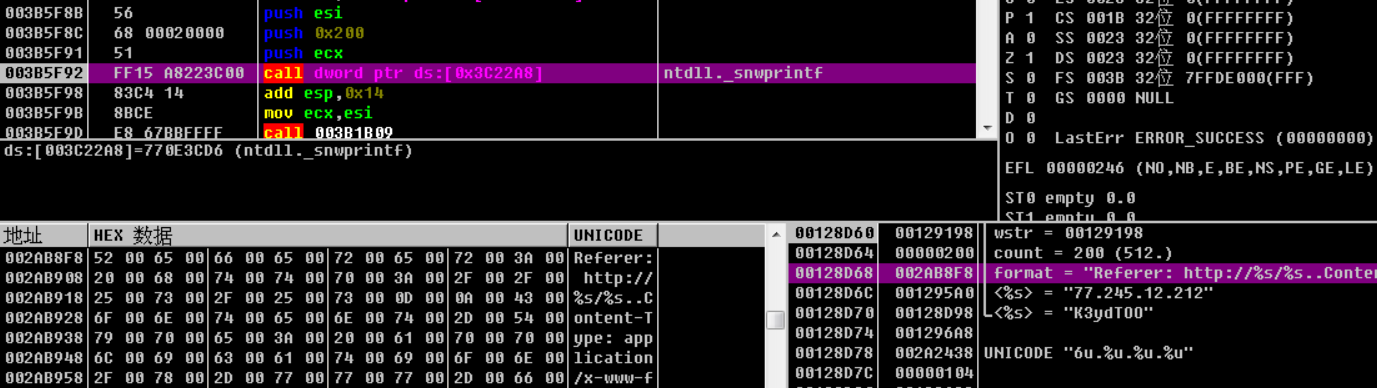
将计算机名、磁盘序列号、系统版本和进程列表信息拼接成字符串，使用算法将其压缩后加密：



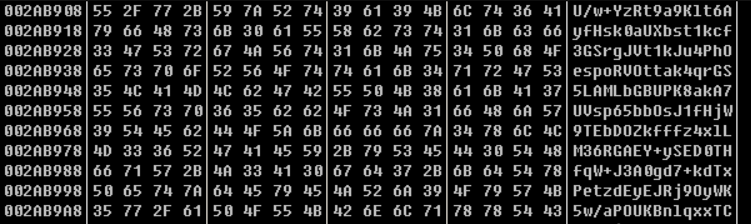
从配置文件中解密得到硬编码的服务器IP地址（共计90个IP地址）：



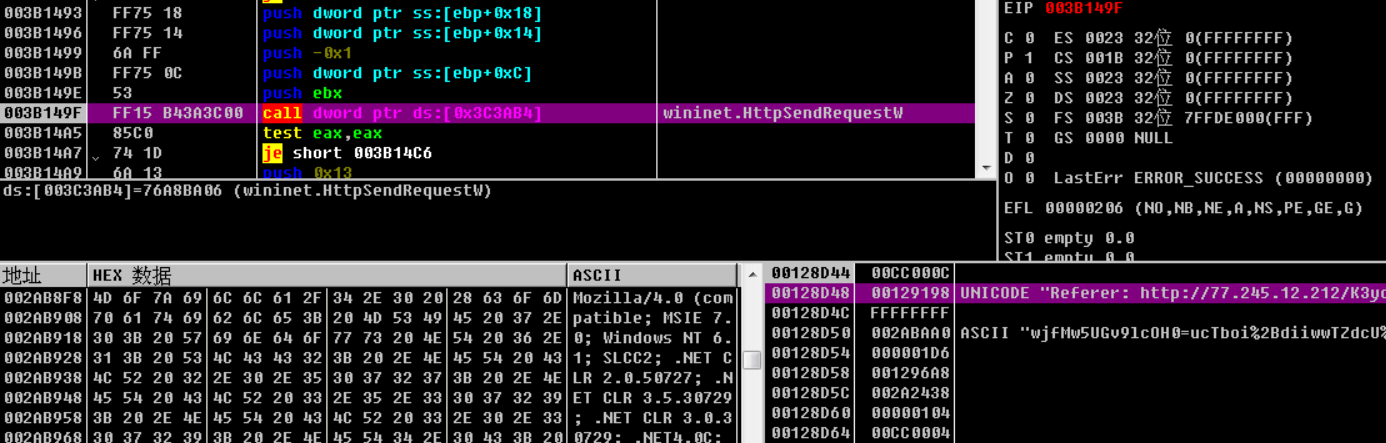
格式化得到连接的URL：



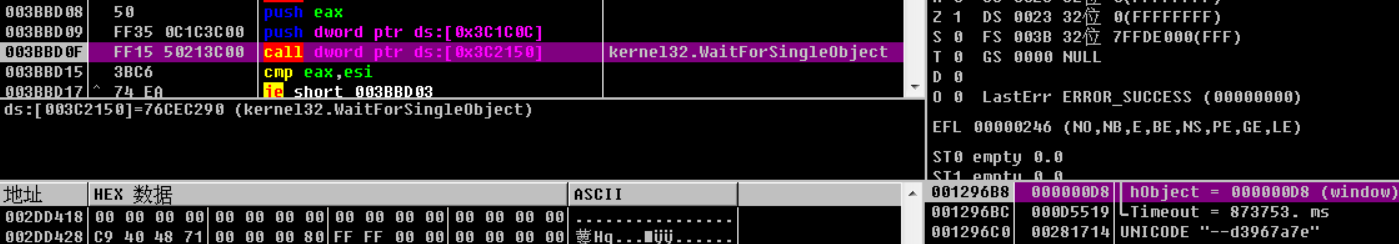
将数据内容（加密过的计算机名、磁盘序列号、系统版本和进程列表信息）再进行一次Base64加密，作为网络传输中的数据：



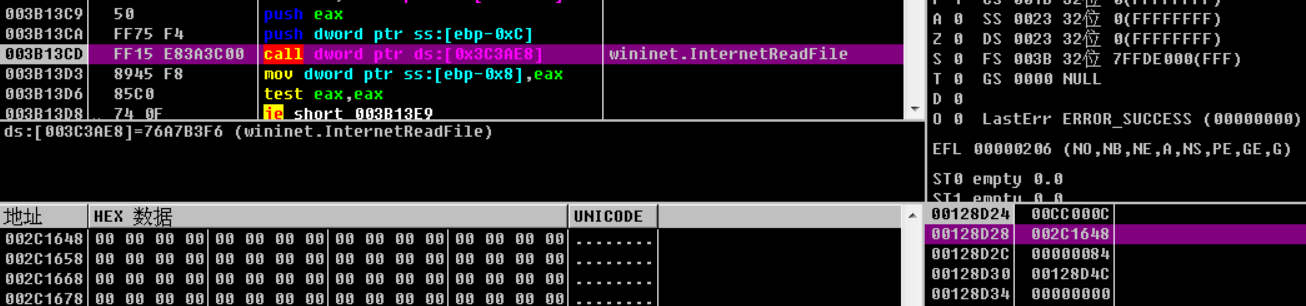
随后，与服务器建立HTTP连接，并发送包含宿主机数据的HTTP请求消息：



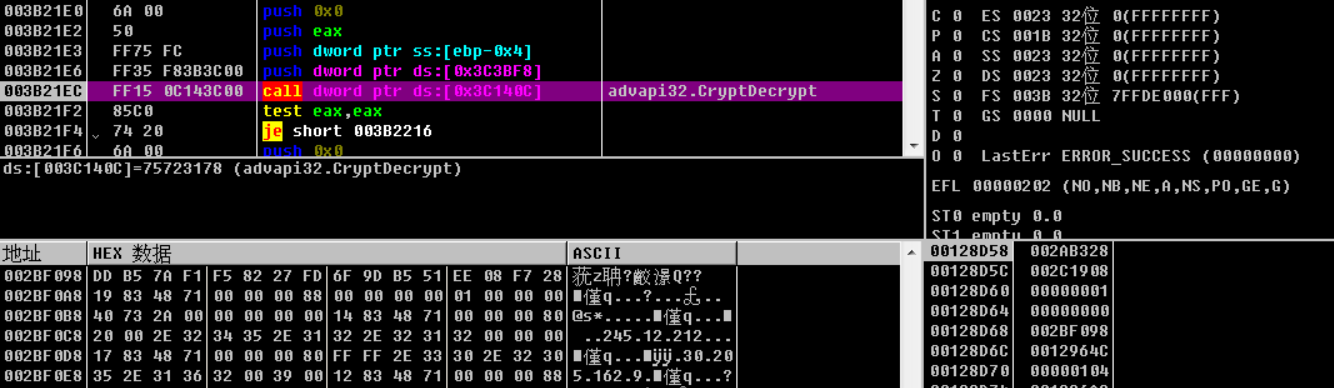
若与服务器通信失败，则调用WaitForSingleObject函数，等待一段时间后再次进行通信（若通信失败则选择下一个IP地址），一直循环这个操作：



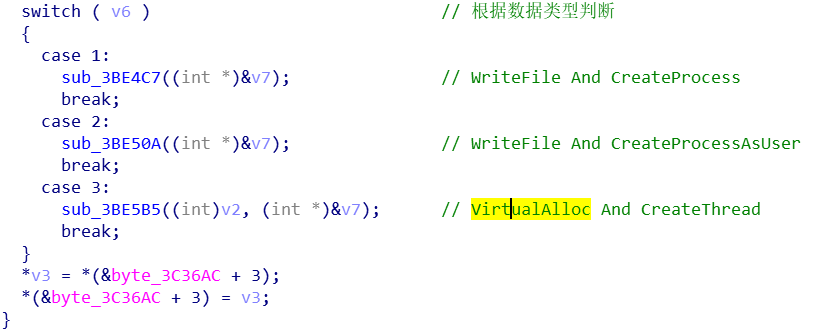
如果与服务器通信成功，则调用InternetReadFile函数读取数据：



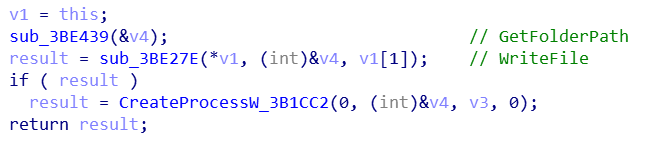
随后，调用CryptDecrypt函数解密数据：



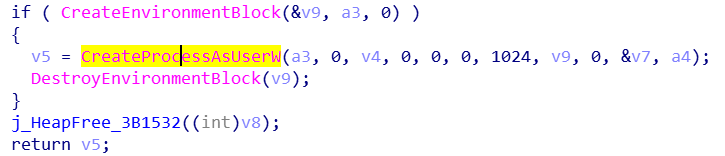
完成数据的解密后，有三种处理方式：



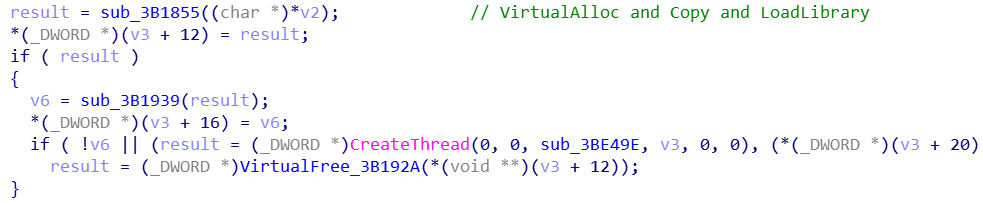
第一种方式是，创建一个文件，将数据写入，创建进程执行这个文件：



第二种方式是，创建一个文件，将数据写入，在指定用户令牌的安全上下文中创建进程运行文件：

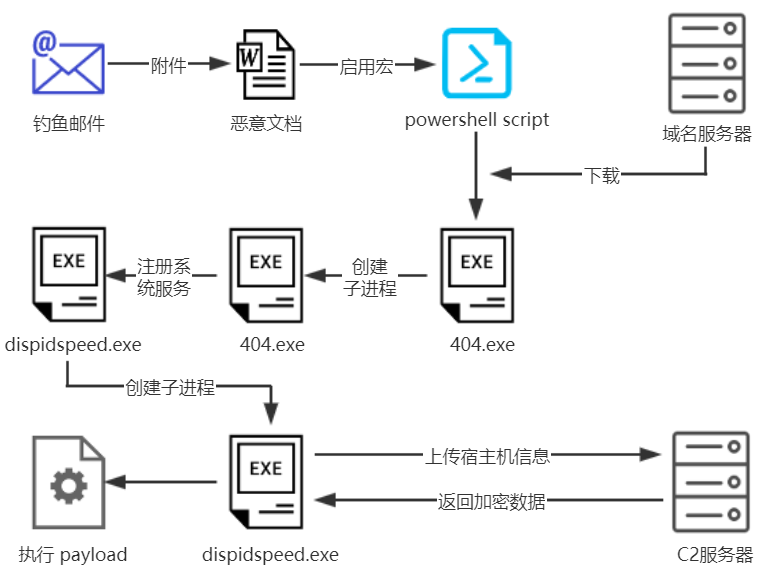


第三种方式是，分配一块内存空间，写入数据并导入DLL模块，以创建线程的方式来执行shellcode：



最后，木马继续以隐蔽的方式和服务器进行通信。

# 执行流程



# 行为特征

通过上述的分析，可以总结出该Emotet木马变种的相关特征：

**传播方式：**

1. 采用钓鱼邮件中包含恶意链接或恶意文档的方式进行传播，邮件内容多为伪装成各种类型的商务往来邮件
2. 使用Emotet僵尸网络进行传播，传播到同一局域网中的其他主机中。

**防御机制：**

1. 混淆：对VBA脚本和PowerShell脚本进行混淆处理。
2. 反调试技术：自定义的加壳方式，代码混淆，动态加载链接库，加密导入函数名等。
3. 隐藏自身：复制到系统目录，拼接文件名，设置为系统服务。
4. 隐藏通信：随机生成URL目录路径，使用了自定义的HTTP请求头。
5. 数据加密：采用Base64编码，RSA和AES算法加密通信数据。

**核心功能：**

1. 获取宿主机系统信息，发送到C2服务器。
2. 从C2服务器下载并执行具体的攻击模块。

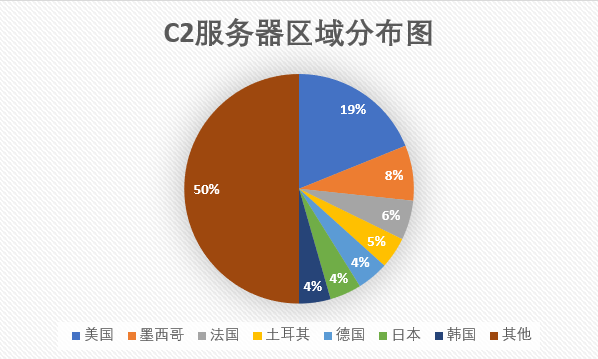
# 威胁分析

Emotet已演变成了当前一个不断扩大的威胁，除了技术上的变化，其核心模式也发生了转变——从一手资料盗窃转向了将其僵尸网络作为“恶意软件即服务”（MAAS）提供给其他网络犯罪团伙，让后者自己选择恶意软件进行分发,从而确立了自身作为恶意软件传播的关键地位。另一方面，Emotet的破坏力巨大，动辄对企业内部造成成千上万美元的损失，危害严重。

目前，Emotet恶意软件被认为是由Mealybug网络犯罪组织运营，其至今仍保持活跃。除了Emotet恶意软件，该组织还与Bugat、Feodo、Geodo、Heodo、Cridex、Dridex等银行木马恶意软件有着千丝万缕的关系。由于这些恶意软件广泛且具有破坏性，过去几年具有很高的知名度。而且，该组织的每次攻击行动包含众多的攻击目标，且规模巨大，可以推测该网络犯罪组织具有相当的规模。

过去几年，Emotet曾分发过AZORult、IcedID、Zeus Panda、TrickBot等恶意软件，受到了反病毒领域、执法机关、安全研究人员的高度关注。为了确保恶意软件的长期有效，恶意软件作者还持续定期更新代码库和攻击方式，以避免被检测和清除。

这次的恶意行动，Emotet足迹遍布全球，且不会根据地区进行区分。根据此次样本中获得的数据，C2服务器所在地区除数量最多的美国外，还包含墨西哥、法国、德国、日本等诸多地区。C2服务器的区域分布图如下所示（详细的IOC见文末）：



另一个关键点，当前大多数被感染的域都是运行WordPress的站点。由于WordPress软件存在大量已披露的漏洞，所以攻击者很容易利用WordPress漏洞攻陷服务器。而网络犯罪组织常使用被攻陷的合法域名服务器来散布恶意软件，因为来自合法域的网络不太可能被屏蔽，恶意软件的到达率更高。

Emotet恶意软件所使用的域名和IP地址主要有三个用途：

1. 托管Emotet恶意文档：用于托管恶意文档，当用户点击钓鱼邮件中的链接时，会从被攻陷的合法域名服务器上下载恶意文档。
2. 托管Emotet可执行载荷：用于存放恶意软件，由恶意文档中的宏代码执行PowerShell脚本下载Payload。
3. 提供C2服务器功能：用于收集失陷主机的系统信息，分发具体的攻击模块或其他家族的恶意软件。

# 防范措施

1. 不打开来历不明的电子邮件，不下载可疑邮件中的附件。
2. 对于不可靠的文档，采用禁用宏的方式打开。
3. 安装杀毒软件，及时更新病毒库。
4. 安装防火墙，配置黑名单拦截。
5. 养成良好的上网习惯，提高个人的网络安全意识。

# IOC

**恶意文件MD5值：**

|  |
| --- |
| 8a44f5aed7a4ec1803aeb09e08ea5b32 |
| 0b158b803453519011f207708d3baff9 |

**放马地址(失陷合法域名服务器)：**

|  |
| --- |
| http://stylex.kg/zgbwqc6/tYHPJj/ |
| https://vip-watch.store/wp-includes/hXBOYUy/ |
| https://service.jumpitairbag.com/wp-includes/552w6k-m6ln-177/ |
| http://vhdogaru-001-site11.btempurl.com/wp-admin/emYGggow/ |
| http://pickpointgarage.com/wp-admin/ypVuCzjp/ |

**C2服务器IP地址：**

|  |  |  |  |
| --- | --- | --- | --- |
| IP地址 | 归属地 | 运营商 | 威胁情报 |
| 77.245.12.212 | 约旦 | zain.com | 僵尸网络 |
| 189.134.4.209 | 墨西哥墨西哥州诺凯潘 | telmex.com | 僵尸网络 |
| 1.32.54.12 | 马来西亚吉隆坡联邦直辖区 | tm.com.my | 僵尸网络 |
| 172.105.213.30 | 日本东京都东京 | linode.com | 僵尸网络 |
| 69.30.205.162 | 美国密苏里州堪萨斯城 | wholesaleinternet.net | 僵尸网络 |
| 50.63.13.135 | 美国亚利桑那州凤凰城 | godaddy.com | 僵尸网络 |
| 192.161.190.171 | 美国德克萨斯州达拉斯 | quadranet.com | 僵尸网络 |
| 190.5.162.204 | 阿根廷 | megacable.com.ar | 僵尸网络 |
| 50.116.78.109 | 美国德克萨斯州休斯顿 | websitewelcome.com | 僵尸网络 |
| 210.224.65.117 | 日本广岛县 | kddi.com | 僵尸网络 |
| 186.215.101.106 | 巴西 | telefonica.com | 僵尸网络 |
| 5.189.148.98 | 德国巴伐利亚州纽伦堡 | contabo.de | 僵尸网络 |
| 81.82.247.216 | 比利时弗拉芒大区西弗兰德 | telenet.be | 僵尸网络 |
| 139.162.185.116 | 德国黑森州法兰克福 | linode.com | 僵尸网络 |
| 172.104.70.207 | 日本东京都品川区 | linode.com | 僵尸网络 |
| 143.95.101.72 | 美国德克萨斯州达拉斯 | athenixinc.com | 僵尸网络 |
| 190.189.79.73 | 阿根廷 | cablevision.com.ar | 僵尸网络 |
| 83.110.107.243 | 阿联酋 | etisalat.ae | 僵尸网络 |
| 82.79.244.92 | 罗马尼亚 | rcs-rds.ro | 僵尸网络 |
| 195.201.56.68 | 德国萨克森州法尔肯施泰因 | hetzner.de | 僵尸网络 |
| 181.197.108.171 | 巴拿马 | cableonda.com | 僵尸网络 |
| 157.7.164.178 | 日本东京都东京 | gmo.jp | 僵尸网络 |
| 83.99.211.160 | 拉脱维亚里加 | balticom.lv | 僵尸网络 |
| 46.17.6.116 | 荷兰北荷兰省哈勒姆 | flexwebhosting.nl | 僵尸网络 |
| 216.75.37.196 | 美国加利福尼亚州圣地亚哥 | cari.net | 僵尸网络 |
| 138.197.140.163 | 加拿大安大略省多伦多 | digitalocean.com | 僵尸网络 |
| 51.38.134.203 | 波兰马佐夫舍省华沙 | ovh.com | 僵尸网络 |
| 211.218.105.101 | 韩国江原道 | kt.com | 僵尸网络 |
| 103.122.75.218 | 孟加拉 | sktraderss.com | 僵尸网络 |
| 198.57.217.170 | 美国犹他州普若佛 | unifiedlayer.com | 僵尸网络 |
| 172.90.70.168 | 美国加利福尼亚州圣安娜 | twcc.com | 僵尸网络 |
| 41.218.118.66 | 安哥拉 | -------------- | 僵尸网络 |
| 195.191.107.67 | 英国西米德兰兹郡考文垂 | glidegroup.co.uk | 僵尸网络 |
| 189.225.211.171 | 墨西哥墨西哥州塔兰潘特拉 | telmex.com | 僵尸网络 |
| 80.93.48.49 | 俄罗斯圣彼得堡 | peterhost.ru | 僵尸网络 |
| 45.129.121.222 | 土耳其 | hayalnet.com.tr | 僵尸网络 |
| 23.253.207.142 | 美国伊利诺伊州芝加哥 | rackspace.com | 僵尸网络 |
| 81.213.145.45 | 土耳其 | turktelekom.com.tr | 僵尸网络 |
| 181.44.166.242 | 阿根廷 | telecentro.com.ar | 僵尸网络 |
| 187.177.155.123 | 墨西哥哈利斯科州瓜达拉哈拉 | axtel.mx | 僵尸网络 |
| 189.180.105.125 | 墨西哥克雷塔罗州克雷塔罗 | telmex.com | 僵尸网络 |
| 182.176.116.139 | 巴基斯坦 | ptcl.com.pk | 僵尸网络 |
| 186.66.224.182 | 厄瓜多尔 | grupotvcable.com | 僵尸网络 |
| 212.112.113.235 | 吉尔吉斯斯坦 | aknet.kg | 僵尸网络 |
| 212.129.14.27 | 法国法兰西岛大区 | online.net | 僵尸网络 |
| 119.159.150.176 | 巴基斯坦 | ptcl.com.pk | 僵尸网络 |
| 176.58.93.123 | 荷兰北荷兰省阿姆斯特丹 | netactuate.com | 僵尸网络 |
| 187.233.220.93 | 墨西哥阿瓜斯卡达特斯州  阿瓜斯卡达特斯 | telmex.com | 僵尸网络 |
| 124.150.175.133 | 新西兰奥克兰大区奥克兰 | fastcom.co.nz | 僵尸网络 |
| 83.156.88.159 | 法国普罗旺斯阿尔卑斯  蓝色海岸大区马赛 | free.fr | 僵尸网络 |
| 60.53.3.153 | 马来西亚西马 | tm.com.my | 僵尸网络 |
| 110.142.161.90 | 澳大利亚维多利亚州墨尔本 | telstra.com | 僵尸网络 |
| 174.57.150.13 | 美国新泽西州尤宁 | comcast.com | 僵尸网络 |
| 95.216.212.157 | 芬兰新地区赫尔辛基 | hetzner.de | 僵尸网络 |
| 197.90.159.42 | 南非 | optinet.net | 僵尸网络 |
| 37.59.24.25 | 法国大东部大区斯特拉斯堡 | ovh.com | 僵尸网络 |
| 201.196.15.79 | 哥斯达黎加 | grupoice.com | 僵尸网络 |
| 221.154.59.110 | 韩国京畿道富川市 | kt.com | 僵尸网络 |
| 187.250.92.82 | 墨西哥下加利福尼亚州提华纳 | telnor.com | 僵尸网络 |
| 78.46.87.133 | 德国萨克森州法尔肯施泰因 | hetzner.de | 僵尸网络 |
| 85.105.183.228 | 土耳其布尔萨省 | turktelekom.com.tr | 僵尸网络 |
| 201.183.251.100 | 厄瓜多尔 | claro.com.ec | 僵尸网络 |
| 123.142.37.165 | 韩国京畿道 | uplus.co.kr | 僵尸网络 |
| 172.245.13.50 | 美国纽约州布法罗 | colocrossing.com | 僵尸网络 |
| 72.69.99.47 | 美国纽约州纽约 | verizon.com | 僵尸网络 |
| 177.103.201.23 | 巴西 | telefonica.com | 僵尸网络 |
| 124.150.175.129 | 新西兰奥克兰大区奥克兰 | fastcom.co.nz | 僵尸网络 |
| 190.161.67.63 | 智利 | vtr.com | 僵尸网络 |
| 192.163.221.191 | 美国犹他州普若佛 | unifiedlayer.com | 僵尸网络 |
| 80.102.124.98 | 西班牙加泰罗尼亚自治区  巴塞罗那 | orange.es | 僵尸网络 |
| 95.216.207.86 | 芬兰新地区赫尔辛基 | hetzner.de | 僵尸网络 |
| 190.101.87.170 | 智利 | vtr.com | 僵尸网络 |
| 72.27.212.209 | 牙买加 | discoverflow.co | 僵尸网络 |
| 163.172.97.112 | 法国法兰西岛大区巴黎 | online.net | 僵尸网络 |
| 191.100.24.201 | 厄瓜多尔 | etapa.net.ec | 僵尸网络 |
| 46.105.131.68 | 法国上法兰西大区鲁贝 | ovh.com | 僵尸网络 |
| 188.230.134.205 | 斯洛文尼亚 | t-2.net | 僵尸网络 |
| 193.33.38.208 | 乌克兰伊万诺  弗兰科夫斯克州卡卢什 | itlux.if.ua | 僵尸网络 |
| 192.241.220.183 | 美国加利福尼亚州旧金山 | digitalocean.com | 僵尸网络 |
| 189.236.4.214 | 墨西哥墨西哥州诺凯潘 | telmex.com | 僵尸网络 |
| 162.144.46.90 | 美国犹他州普若佛 | unifiedlayer.com | 僵尸网络 |
| 210.111.160.220 | 韩国仁川广域市 | nibtv.co.kr | 僵尸网络 |
| 113.52.135.33 | 中国香港 | ximbo.com | 僵尸网络 |
| 89.215.225.15 | 保加利亚普罗夫迪夫州  普罗夫迪夫 | a1.bg | 僵尸网络 |
| 200.71.112.158 | 委内瑞拉 | -------------- | 僵尸网络 |
| 78.186.102.195 | 土耳其迪亚巴克尔省 | turktelekom.com.tr | 僵尸网络 |
| 152.169.32.143 | 阿根廷 | cablevision.com.ar | 僵尸网络 |
| 192.210.217.94 | 美国加利福尼亚州洛杉矶 | colocrossing.com | 僵尸网络 |
| 142.93.87.198 | 美国加利福尼亚州旧金山 | digitalocean.com | 僵尸网络 |
| 122.11.164.183 | 新加坡 | starhub.com | 僵尸网络 |