Wipe系统中Shamoon攻击分析

Pinging / 2018-12-23 09:08:00 / 浏览数 2009 技术文章 翻译文章 顶(0) 踩(0)

前言

近些年以来，黑客攻击者多次使用具有破坏性的恶意软件对系统进行攻击。而这些攻击通常伴随某些针对性，其常常会被意识形态、政治目标甚至财务目标来影响。

这些具有破坏性的攻击由于会导致数据丢失或业务运营，所以对企业影响甚大。而若要恢复这些攻击造成的影响则要数周或数月，同时在修复过程中可能会造成企业利润已经

最近的一些攻击已经表明了攻击的伤害性有多大。去年，NotPetya攻击行为影响了全球多家公司。
去年2月，研究人员也发现了影响奥运会的`OlympicDestroyer`恶意攻击。

Shamoon是McAfee公司一直进行监控的具有破坏性恶意软件。 本月初，McAfee
Foundstone紧急事件响应团队对客户的被入侵行为做出了迅速反应并确定了攻击来自最新版本的恶意软件，也昭示了一波攻击浪潮的来袭。Shamoon于2012年袭击了中东

在过去的一周里，我们观察到一个新型的恶意手段攻击了几个部门，包括中东和南欧的石油，天然气，能源，电信和政府组织。

与之前的浪潮事件类似，Shamoon第3版使用几种机制作为规避技术来绕过安全，用以避免防御软件的分析。然而它的整体代码与以前的版本保持一致，这也使大多数反恶意

与以前的版本一样，Shamoon版本3安装了wiper组件的恶意服务。
一旦wiper运行，它会用垃圾内容覆盖所有文件并使系统重启，导致"蓝屏死机"或驱动程序错误的情况并使系统无法运行。
恶意软件还可以扫描本地网络，然而这个操作并没有被进一步利用。此版本的恶意软件有一些错误，表明此版本可能是测试阶段或测试阶段。

此版本与早期版本的主要区别在于最新的软件修改了"用于删除恶意文件的名称列表"以及将伪造的服务名称修改为"MaintenaceSrv"。wiper组件为使用以下选项定位系统上

- 用垃圾数据覆盖文件（在此版本和我们分析样本的相同）
- 用文件覆盖（在Shamoon版本1和2中使用）
- 加密文件和引导记录（此版本中未使用）

Shamoon是一种模块化恶意软件：wiper组件可以作为独立文件进行重用，此威胁也具有很高风险。该文章介绍了我们的研究结果，包括详细的分析和IOCs。

分析详情

Shamoon是一种包括三种功能的注入工具。注入前期需要收集相关设备信息并将恶意代码嵌入设备中，之后进行混淆，反调试的过程。而在运行此工具前，我们需要添加一

它会解密三个源码并将它们安装在■System■文件夹中。 之后创建用于运行wiper的服务--`MaintenaceSrv`。 服务名称中的拼写错误可以简化检测过程。

威胁研究团队在研究过程中也发现了这个工具多年来的发展情况，下面是各个版本的差别：

2016 Shamoon	
Service Name	NtsSrv
Display Name	Microsoft Network Realtime Inspection Service
Description	Helps guard against time change attempts targeting known and newly discovered vulnerabilities in network time protocols

2017 Shamoon	
Service Name	NtertSrv
Display Name	Extensible Remote Tab
Description	The Extensible Remote Tab manager service

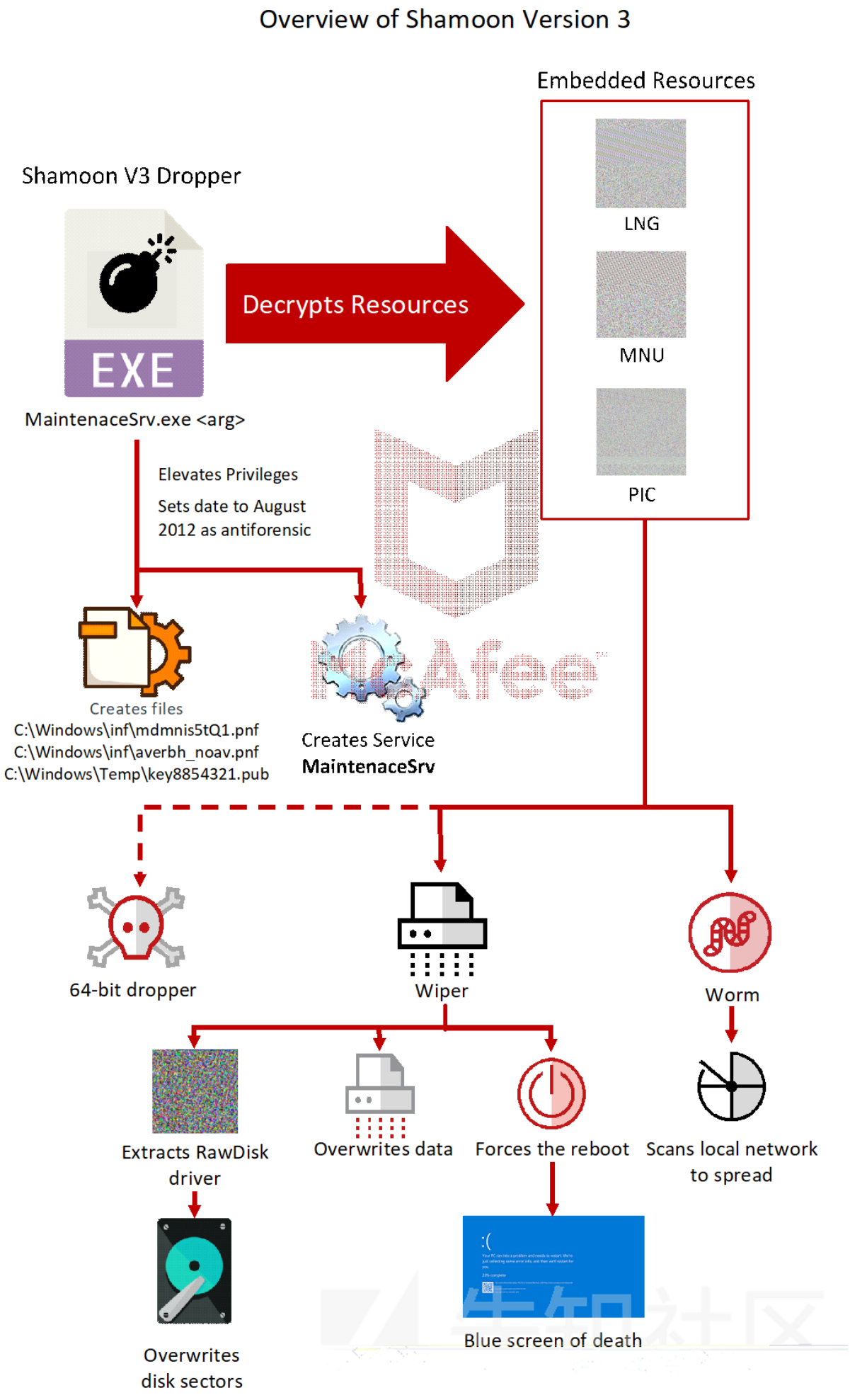
2018 Shamoon	
Service Name	MaintenaceSrv
Display Name	Maintenace Host Service

wiper使用`ElRawDisk.sys`访问用户的磁盘并覆盖所有文件夹和磁盘扇区中的数据，从而在重启系统之前感染计算机。

2017 Shamoon:	
ElRawDisk.sys key	8A6DB7D2-FECF-41ff-9A92-xxxxxxxxxxxx

2018 Shamoon:	
ElRawDisk.sys key	9A6DB7D2-FECF-41ff-9A92-xxxxxxxxxxxx

结果是蓝屏或驱动程序错误导致机器无法使用。

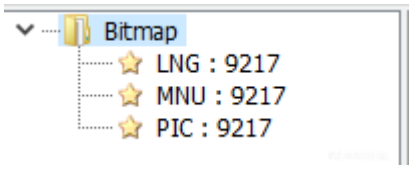

Overview of Shamoon Version 3
Embedded Resources
LNG
MNU
PIC
Shamoon V3 Dropper
EXE
Decrypts Resources
MaintenaceSrv.exe <arg>
Elevates Privileges
Sets date to August 2012 as antiforensic
Creates files
C:\Windows\inf\mdmnis5tQ1.pnf
C:\Windows\inf\averbh_noav.pnf
C:\Windows\Temp\key8854321.pub
Creates Service
MaintenaceSrv
64-bit dropper
Wiper
Worm
Extracts RawDisk driver
Overwrites data
Forces the reboot
Scans local network to spread
Overwrites disk sectors
Blue screen of death

注入工具的可执行摘要

Executable summary

File type	PE32 executable (console) Intel 80386, for Microsoft Windows
Filename	MaintenaceSrv32.exe
File size	1.8MB
Hash SHA-2	c3ab58b3154e5f5101ba74fccfd27a9ab445e41262cdf47e8cc3be7416a5904f
Compile time	2011-11-28 16:50:59
Import hash	53e316887bac4e36b2dfef0e711a3d8e

dropper包含许多恶意组件，这些组件使用嵌入在PE部分中的加密文件来进行隐藏。



这些资源由dropper工具解密，包含：

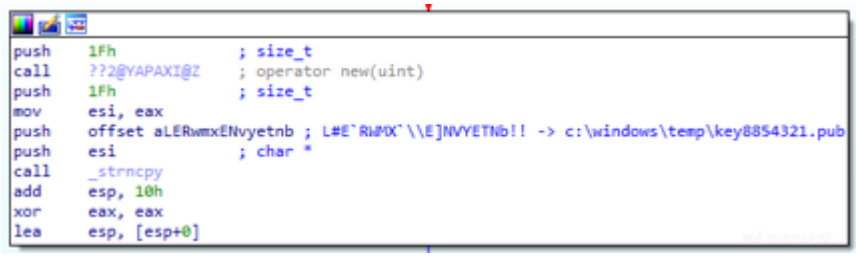
MNU：通信模块

LNG：wiper核心组件

PIC：64位版本的注入器

Shamoon 2018需要一个参数来运行攻击模块。 它解密内存中的几个字符串用于收集系统上的信息并确定是32位还是64位版本。

他会将key8854321.pub (MD5: 41f8cd9ac3fb6b1771177e5770537518)文件放在c:\Windows\Temp\key8854321.pub.中。



```
push    1Fh             ; size_t
call    ??2@YAPAXI@Z    ; operator new(uint)
push    1Fh             ; size_t
mov     esi, eax
push    offset aLERwmxENvyetnb ; L#E`RWMX`\\E]NVYETNb!! -> c:\windows\temp\key8854321.pub
push    esi             ; char *
call    _strncpy
add     esp, 10h
xor     eax, eax
lea     esp, [esp+0]
```

之后恶意软件会解密两个用户文件：

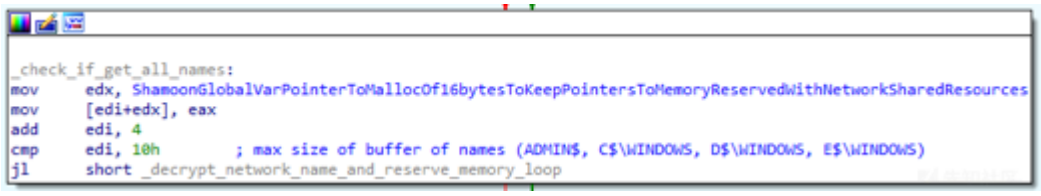
- C:\Windows\inf\mdmnis5tQ1.pnf
- C:\Windows\inf\averbh_noav.pnf

Shamoon启用RemoteRegistry■■，并允许程序远程修改注册表。 它还通过启用注册表项LocalAccountTokenFilterPolicy来禁用远程用户帐户控制。

```
call    _memset
lea     ecx, [ebp+var_634]
mov     ebx, 17h
mov     eax, offset aEBNv ; E\\b\\]NV -> \system32\kernel32.dll
mov     ShamoonGlobalVarPointerToMallocOf12bytesForNetworkSharedResourcesNames, ecx
call    ShamoonDecryptUnicodeString
mov     ShamoonGlobalVarPointerToMemoryWithStringOfKernelModule, eax
mov     ebx, 1Ah
mov     eax, offset a8ksuzk8kmoyzx_ ; 8KSUZK8KMOYZX_ -> RemoteRegistry
call    ShamoonDecryptUnicodeString
mov     ShamoonGlobalVarPointerToMemoryWithStringOfRemoteRegistry, eax
mov     ebx, 0FFFFFFF3h ; -0x0D
mov     eax, offset aYPnynpp ; Y|pnyNpp|? -> LocalAccountTokenFilterPolicy
call    ShamoonDecryptUnicodeString
mov     ShamoonGlobalVarPointerToMemoryWithStringOfLocalAccountTokenFilterPolicy, eax
mov     ebx, 0FFFFFFE9h ; -0x17
mov     eax, offset asc_423458 ; <? -> %s%s
mov     dword_43243C, offset a_exe ; ".exe"
call    ShamoonDecryptUnicodeString
```

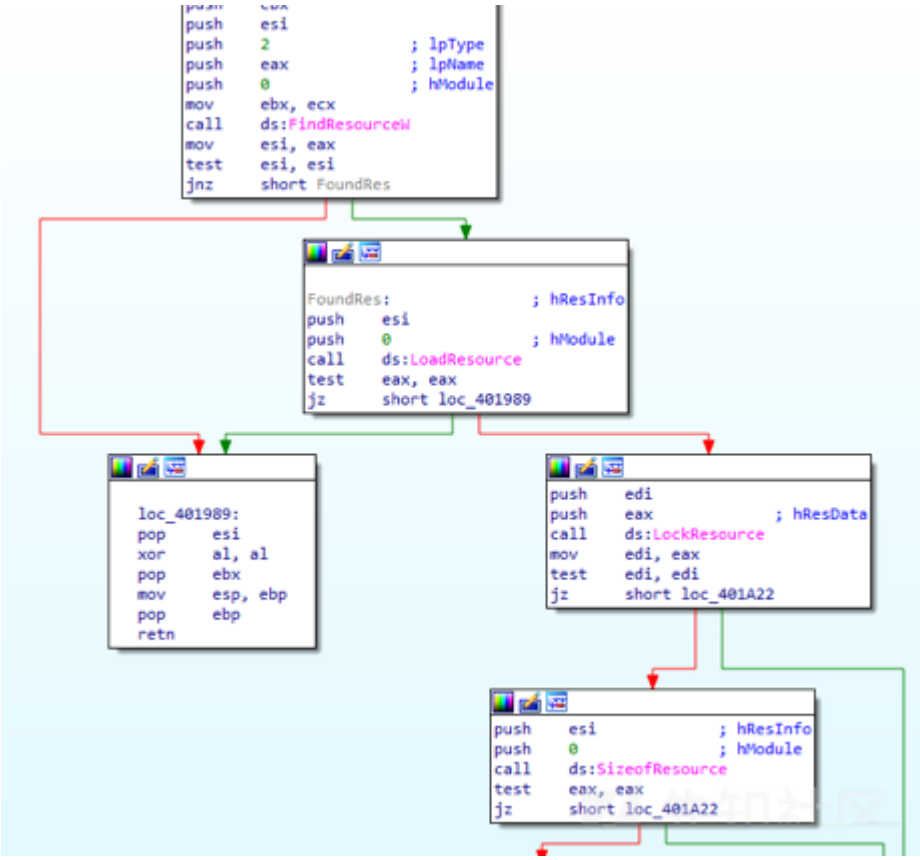
恶意软件会检查以下共享内容是否存在并将其复制进行病毒传播：

- ADMIN$
- C$\WINDOWS
- D$\WINDOWS
- E$\WINDOWS



Shamoon查询服务以检索与LocalService帐户相关的信息。

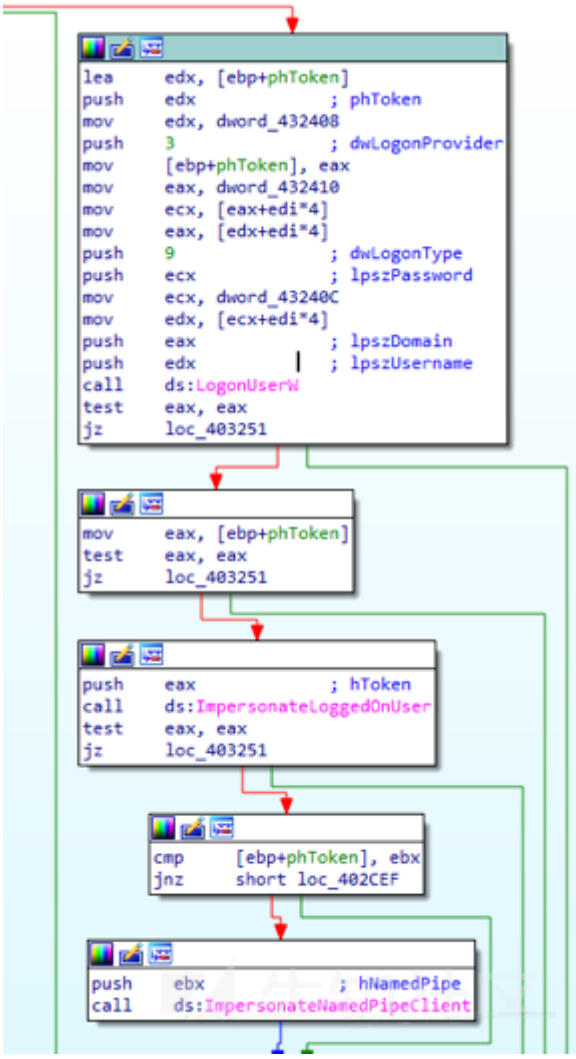
然后它会检索PE文件中的资源以删除组件。 查找资源的位置：



Shamoon创建文件并将时间设置为2012年8月（用于逃脱法律的制裁）。 它将此日期放在可以销毁的文件中。

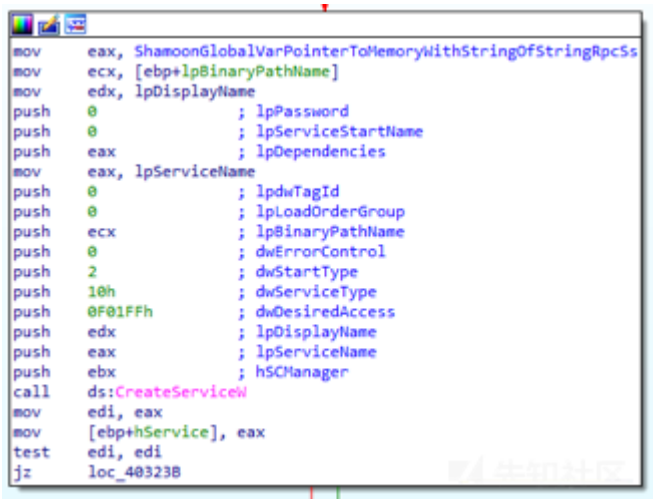
例如，修改时间可以用作基于时间线绕过检测的抗辩法技巧。 我们还观察到，在某些情况下，系统会简要修改日期，伪造每个文件的日期。
删除在系统上的文件存储在C：\ Windows \ System32 \中。

在创建服务之前，Shamoon通过系统token来提升其权限。
它首先使用`LogonUser`和`ImpersonateLoggedOnUser`，然后使用`ImpersonateNamedPipeClient`函数。 `Metasploit`也使用类似的技术来提升特权。



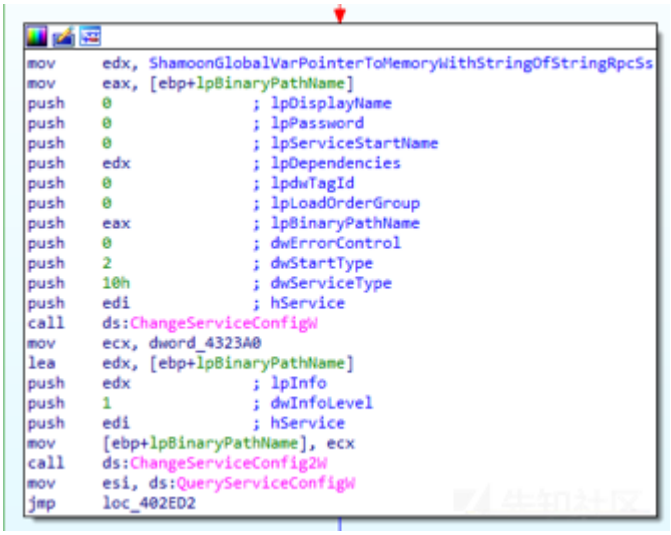
提升权限对于软件进一步执行恶意代码至关重要，然而这些修改通常会有许多限制。

Shamoon创建了新的恶意服务MaintenaceSrv。 它使用选项Autostart■StartType:2■创建服务，并使用自己的进程（ServiceType■0x10）运行服务：



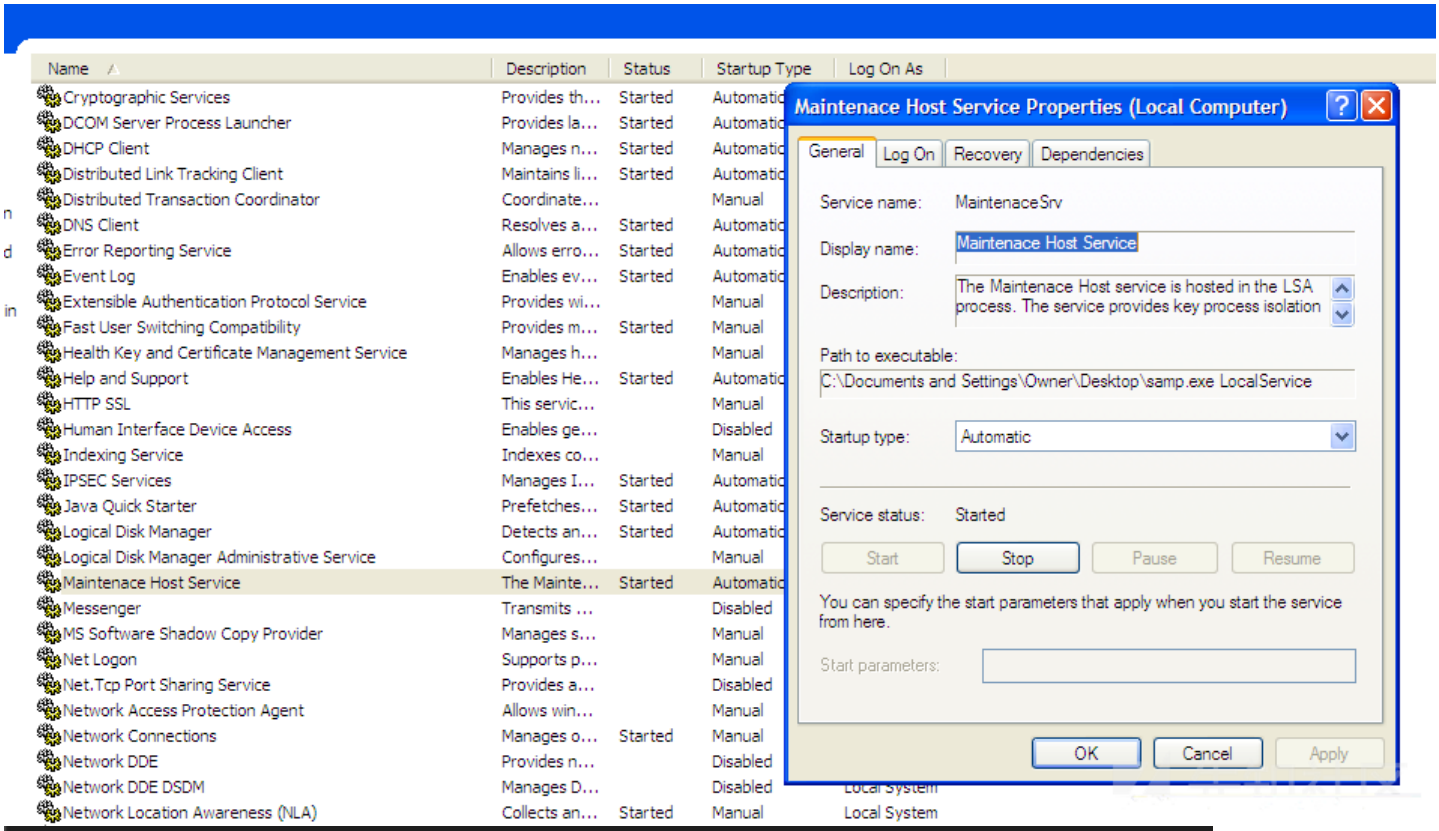
```
mov     eax, ShamoonGlobalVarPointerToMemoryWithStringOfStringRpcSs
mov     ecx, [ebp+lpBinaryPathName]
mov     edx, lpDisplayName
push    0               ; lpPassword
push    0               ; lpServiceStartName
push    eax             ; lpDependencies
mov     eax, lpServiceName
push    0               ; lpdwTagId
push    0               ; lpLoadOrderGroup
push    ecx             ; lpBinaryPathName
push    0               ; dwErrorControl
push    2               ; dwStartType
push    10h             ; dwServiceType
push    0F01FFh         ; dwDesiredAccess
push    edx             ; lpDisplayName
push    eax             ; lpServiceName
push    ebx             ; hSCManager
call    ds:CreateServiceW
mov     edi, eax
mov     [ebp+hService], eax
test    edi, edi
jz      loc_40323B
```

如果服务已被创建，则会使用先前的配置更改服务的参数。



```
mov     edx, ShamoonGlobalVarPointerToMemoryWithStringOfStringRpcSs
mov     eax, [ebp+lpBinaryPathName]
push    0               ; lpDisplayName
push    0               ; lpPassword
push    0               ; lpServiceStartName
push    edx             ; lpDependencies
push    0               ; lpdwTagId
push    0               ; lpLoadOrderGroup
push    eax             ; lpBinaryPathName
push    0               ; dwErrorControl
push    2               ; dwStartType
push    10h             ; dwServiceType
push    edi             ; hService
call    ds:ChangeServiceConfigW
mov     ecx, dword_4323A0
lea     edx, [ebp+lpBinaryPathName]
push    edx             ; lpInfo
push    1               ; dwInfoLevel
push    edi             ; hService
mov     [ebp+lpBinaryPathName], ecx
call    ds:ChangeServiceConfig2W
mov     esi, ds:QueryServiceConfigW
jmp     loc_402ED2
```

它最后完成MaintenaceSrv的创建：




```
SERVICE_NAME: MaintenaceSrv
DISPLAY_NAME: Maintenace Host Service
The Maintenace Host service is hosted in the LSA process. The service provides key process isolation to private keys
and associated cryptographic operations as required by the Common Criteria. The service stores and uses long-lived keys
in a secure process compl0
        TYPE               : 10 WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0 ms
```

wiper模块可以为以下任何一个名称：

samp.exe	3456	CreateFile	C:\WINDOWS\system32_wialx002.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32__wiaca00a.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\tsprint_jbv.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\acpipmi2z.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\pmlx00ctl.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\pmgt6_4.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\arcx6u0.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32_tdibth.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\pmcaz90x.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\mdmgcs_8.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\mdmusrk1g5.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\netbxndxlg2.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\pmsv0_56.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\af0038bdax.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\averfix2h826d_noaverir.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\megasasop.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\hidirkbdmvs2.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\vsmxraid.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\mdamx_5560.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\wiacnt7001.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\mdmusrk1g5.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32_wialx002.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32__wiaca00a.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\tsprint_jbv.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\acpipmi2z.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\pmlx00ctl.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\pmgt6_4.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\arcx6u0.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32_tdibth.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\pmcaz90x.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\mdmgcs_8.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\mdmusrk1g5.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\netbxndxlg2.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\pmsv0_56.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\af0038bdax.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\averfix2h826d_noaverir.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\megasasop.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\hidirkbdmvs2.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\vsmxraid.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\mdamx_5560.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\wiacnt7001.exe
samp.exe	3456	CreateFile	C:\WINDOWS\system32\mdamx_5560.exe

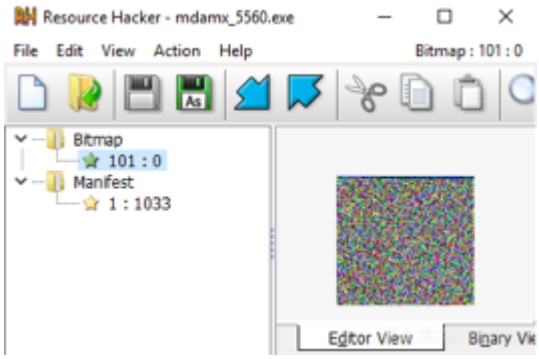
接下来，wiper运行以销毁数据。

Wiper组件解析

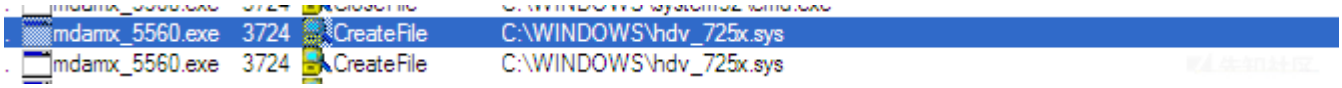
wiper组件被放入System32文件夹中并 需要一个参数才能运行。 Wiper驱动程序嵌入其资源中。

File type	PE32 executable (console) Intel 80386, for Windows
Filename	netbxndxlg2.exe
File size	1.8MB
Hash SHA-2	391e7b90bf3f0bfeb2c2602cc65aa6be4dd1c01374b89c4a48425f2d22fe231c
Compile time	2011-11-28 15:52:52
Import hash	4767fbf3ade8812b0583b2b20cb6dd46

我们可以在此屏幕截图中看到工具对资源101进行加密：



驱动程序`ElRawDisk.sys`被用于解密资源，之后擦除磁盘内容。



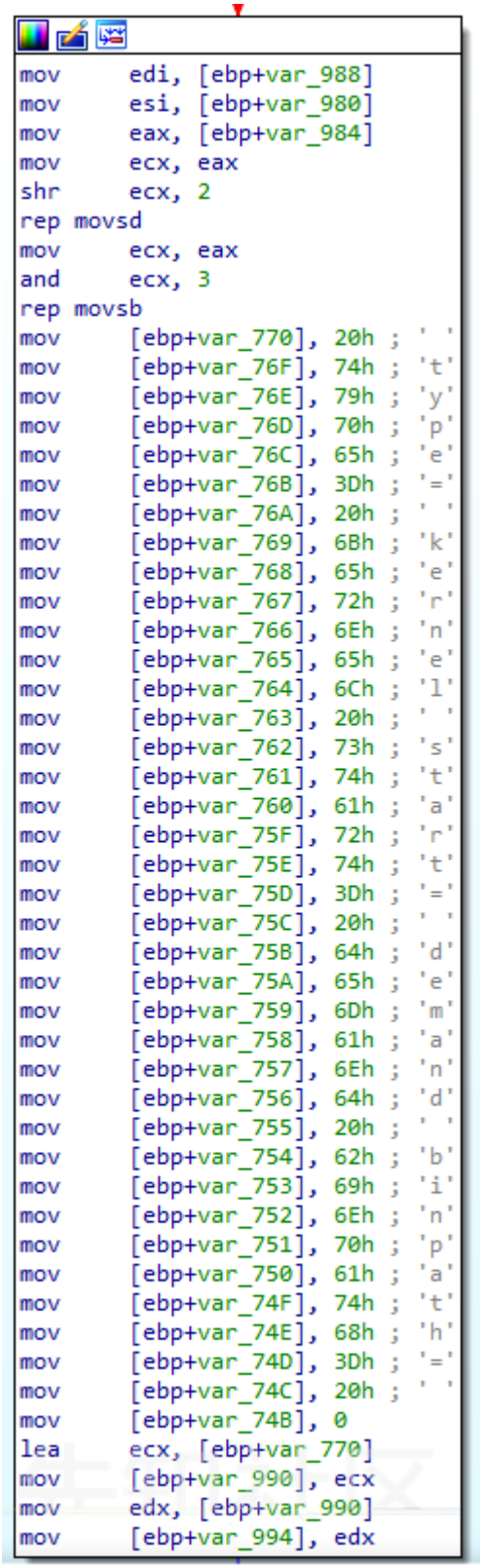
提取资源：

File type	PE32 executable (native) Intel 80386, for Windows
Filename	hdv_725x.sys
File size	27KB
Hash SHA-2	6985ef5809d0789eeff623cd2436534b818fd2843f09fa2de2b4a6e2c0e1a879
Compile time	2011-12-28 17:51:24
Import hash	c94e5ad0f33374535392364a5a193253

此前曾有一个文件不是恶意文件，但由于它是原始驱动程序，因此被认为是具有风险性的。

Wiper使用以下命令创建驱动程序：

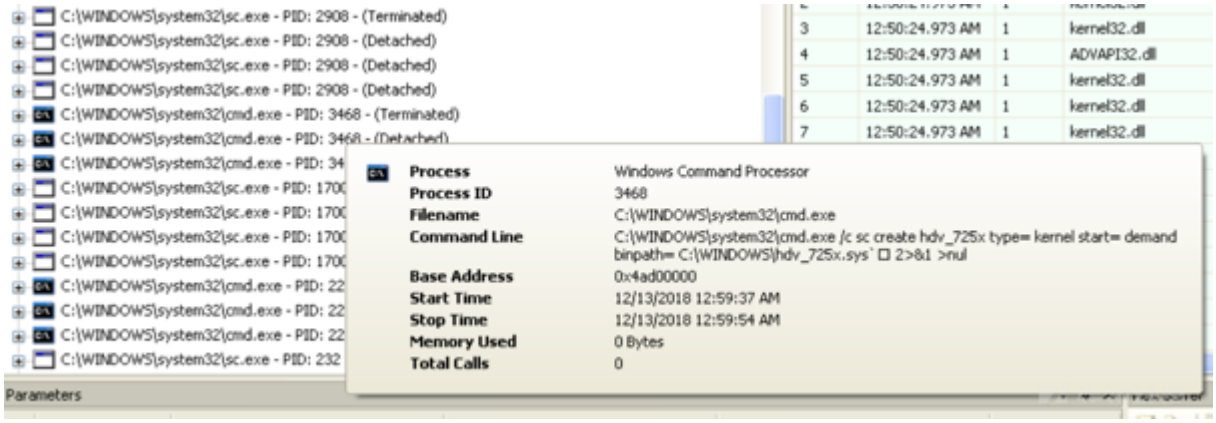
```
sc create hdv_725x type= kernel start= demand binpath= WINDOWS\hdv_725x.sys 2>&1 >nul
```



```
mov     edi, [ebp+var_988]
mov     esi, [ebp+var_980]
mov     eax, [ebp+var_984]
mov     ecx, eax
shr     ecx, 2
rep movsd
mov     ecx, eax
and     ecx, 3
rep movsb
mov     [ebp+var_770], 20h ; ' '
mov     [ebp+var_76F], 74h ; 't'
mov     [ebp+var_76E], 79h ; 'y'
mov     [ebp+var_76D], 70h ; 'p'
mov     [ebp+var_76C], 65h ; 'e'
mov     [ebp+var_76B], 3Dh ; '='
mov     [ebp+var_76A], 20h ; ' '
mov     [ebp+var_769], 6Bh ; 'k'
mov     [ebp+var_768], 65h ; 'e'
mov     [ebp+var_767], 72h ; 'r'
mov     [ebp+var_766], 6Eh ; 'n'
mov     [ebp+var_765], 65h ; 'e'
mov     [ebp+var_764], 6Ch ; 'l'
mov     [ebp+var_763], 20h ; ' '
mov     [ebp+var_762], 73h ; 's'
mov     [ebp+var_761], 74h ; 't'
mov     [ebp+var_760], 61h ; 'a'
mov     [ebp+var_75F], 72h ; 'r'
mov     [ebp+var_75E], 74h ; 't'
mov     [ebp+var_75D], 3Dh ; '='
mov     [ebp+var_75C], 20h ; ' '
mov     [ebp+var_75B], 64h ; 'd'
mov     [ebp+var_75A], 65h ; 'e'
mov     [ebp+var_759], 6Dh ; 'm'
mov     [ebp+var_758], 61h ; 'a'
mov     [ebp+var_757], 6Eh ; 'n'
mov     [ebp+var_756], 64h ; 'd'
mov     [ebp+var_755], 20h ; ' '
mov     [ebp+var_754], 62h ; 'b'
mov     [ebp+var_753], 69h ; 'i'
mov     [ebp+var_752], 6Eh ; 'n'
mov     [ebp+var_751], 70h ; 'p'
mov     [ebp+var_750], 61h ; 'a'
mov     [ebp+var_74F], 74h ; 't'
mov     [ebp+var_74E], 68h ; 'h'
mov     [ebp+var_74D], 3Dh ; '='
mov     [ebp+var_74C], 20h ; ' '
mov     [ebp+var_74B], 0
lea     ecx, [ebp+var_770]
mov     [ebp+var_990], ecx
mov     edx, [ebp+var_990]
mov     [ebp+var_994], edx
```

```
mov     [ebp+var_3F8], 0
mov     [ebp+var_77C], 73h ; 's'
mov     [ebp+var_77B], 63h ; 'c'
mov     [ebp+var_77A], 20h ; ' '
mov     [ebp+var_779], 63h ; 'c'
mov     [ebp+var_778], 72h ; 'r'
mov     [ebp+var_777], 65h ; 'e'
mov     [ebp+var_776], 61h ; 'a'
mov     [ebp+var_775], 74h ; 't'
mov     [ebp+var_774], 65h ; 'e'
mov     [ebp+var_773], 20h ; ' '
mov     [ebp+var_772], 0 ; sc create
lea     ecx, [ebp+var_77C]
mov     [ebp+var_958], ecx
mov     edx, [ebp+var_958]
mov     [ebp+var_95C], edx
```

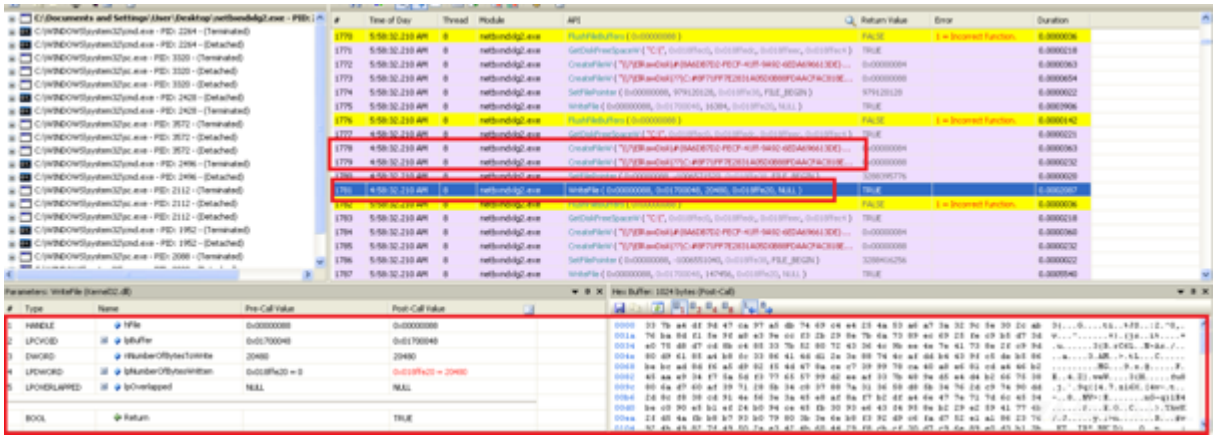
下面的截图显示了命令的执行过程：



恶意软件会覆盖掉`c:\Windows\System32`中的所有文件，并使计算机严重瘫痪。从而使计算机中所有的文件均被覆盖。

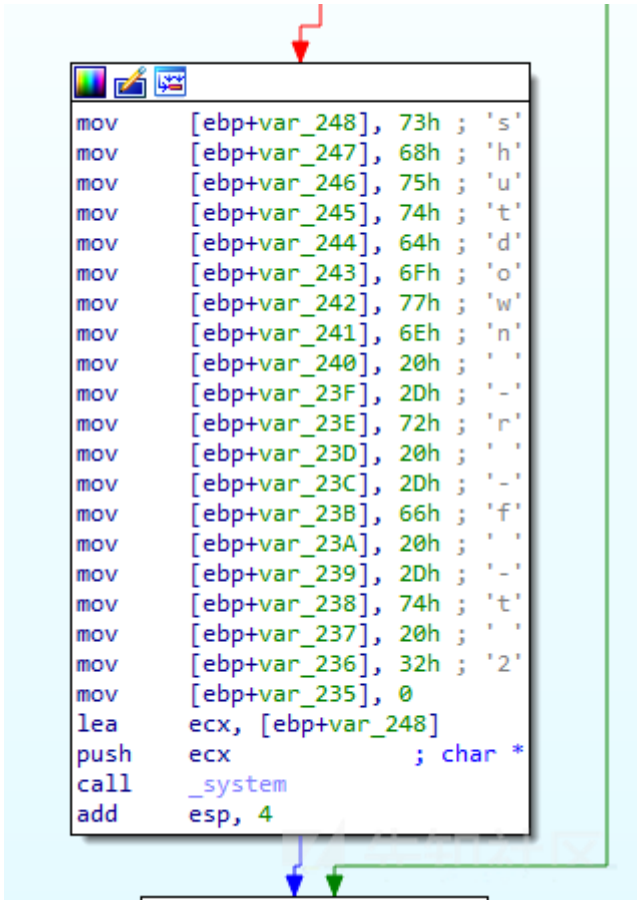
e	3724	CloseFile	C:\
e	3724	CreateFile	C:\WINDOWS\system32\drivers\acpi.sys
e	3724	QueryStandardI...	C:\WINDOWS\system32\drivers\acpi.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\acpi.sys
e	3724	FlushBuffersFile	C:\WINDOWS\system32\drivers\acpi.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\acpi.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\acpi.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\acpi.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\acpi.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\acpi.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\acpi.sys
e	3724	CloseFile	C:\WINDOWS\system32\drivers\acpi.sys
e	3724	CreateFile	C:\WINDOWS\system32\drivers\acpi.sys
e	3724	QueryAttributeT...	C:\WINDOWS\system32\drivers\acpi.sys
e	3724	SetDispositionI...	C:\WINDOWS\system32\drivers\acpi.sys
e	3724	CloseFile	C:\WINDOWS\system32\drivers\acpi.sys
e	3724	CreateFile	C:\
e	3724	QuerySizeInfor...	C:\
e	3724	CloseFile	C:\
e	3724	CreateFile	C:\WINDOWS\system32\drivers\acpiec.sys
e	3724	QueryStandardI...	C:\WINDOWS\system32\drivers\acpiec.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\acpiec.sys
e	3724	FlushBuffersFile	C:\WINDOWS\system32\drivers\acpiec.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\acpiec.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\acpiec.sys
e	3724	CloseFile	C:\WINDOWS\system32\drivers\acpiec.sys
e	3724	CreateFile	C:\
e	3724	QuerySizeInfor...	C:\
e	3724	CloseFile	C:\
e	3724	CreateFile	C:\WINDOWS\system32\drivers\afd.sys
e	3724	QueryStandardI...	C:\WINDOWS\system32\drivers\afd.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\afd.sys
e	3724	FlushBuffersFile	C:\WINDOWS\system32\drivers\afd.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\afd.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\afd.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\afd.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\afd.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\afd.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\afd.sys
e	3724	CloseFile	C:\WINDOWS\system32\drivers\afd.sys
e	3724	CreateFile	C:\
e	3724	QuerySizeInfor...	C:\
e	3724	CloseFile	C:\
e	3724	CreateFile	C:\WINDOWS\system32\drivers\AGP440.SYS
e	3724	QueryStandardI...	C:\WINDOWS\system32\drivers\AGP440.SYS
e	3724	WriteFile	C:\WINDOWS\system32\drivers\AGP440.SYS
e	3724	FlushBuffersFile	C:\WINDOWS\system32\drivers\AGP440.SYS
e	3724	WriteFile	C:\WINDOWS\system32\drivers\AGP440.SYS
e	3724	WriteFile	C:\WINDOWS\system32\drivers\AGP440.SYS
e	3724	CloseFile	C:\WINDOWS\system32\drivers\AGP440.SYS
e	3724	CreateFile	C:\
e	3724	QuerySizeInfor...	C:\
e	3724	CloseFile	C:\
e	3724	CreateFile	C:\WINDOWS\system32\drivers\amdk6.sys
e	3724	QueryStandardI...	C:\WINDOWS\system32\drivers\amdk6.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\amdk6.sys
e	3724	FlushBuffersFile	C:\WINDOWS\system32\drivers\amdk6.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\amdk6.sys
e	3724	WriteFile	C:\WINDOWS\system32\drivers\amdk6.sys
e	3724	CloseFile	C:\WINDOWS\system32\drivers\amdk6.sys

覆盖程序如下：



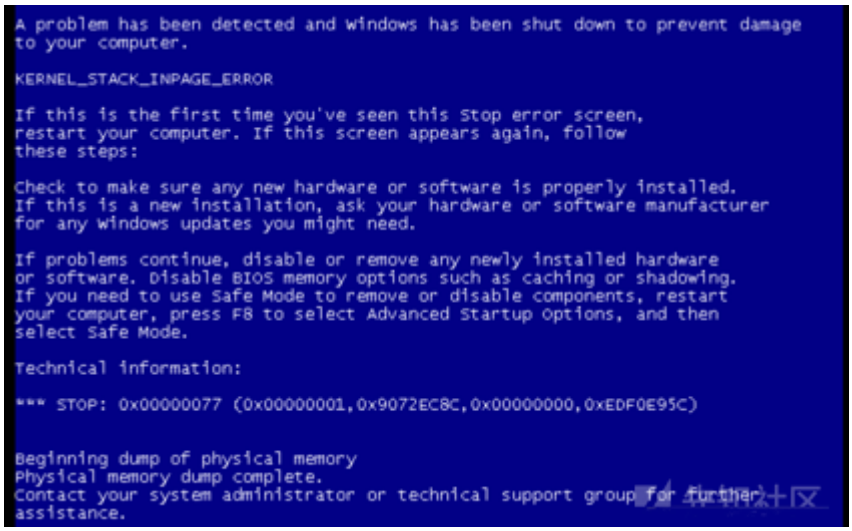
最后，它使用以下命令强制重新启动：

```
Shutdown -r -f -t 2
```



```
mov     [ebp+var_248], 73h ; 's'
mov     [ebp+var_247], 68h ; 'h'
mov     [ebp+var_246], 75h ; 'u'
mov     [ebp+var_245], 74h ; 't'
mov     [ebp+var_244], 64h ; 'd'
mov     [ebp+var_243], 6Fh ; 'o'
mov     [ebp+var_242], 77h ; 'w'
mov     [ebp+var_241], 6Eh ; 'n'
mov     [ebp+var_240], 20h ; ' '
mov     [ebp+var_23F], 2Dh ; '-'
mov     [ebp+var_23E], 72h ; 'r'
mov     [ebp+var_23D], 20h ; ' '
mov     [ebp+var_23C], 2Dh ; '-'
mov     [ebp+var_23B], 66h ; 'f'
mov     [ebp+var_23A], 20h ; ' '
mov     [ebp+var_239], 2Dh ; '-'
mov     [ebp+var_238], 74h ; 't'
mov     [ebp+var_237], 20h ; ' '
mov     [ebp+var_236], 32h ; '2'
mov     [ebp+var_235], 0
lea     ecx, [ebp+var_248]
push    ecx             ; char *
call    _system
add     esp, 4
```

系统重启后会显示蓝屏：



```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

KERNEL_STACK_INPAGE_ERROR

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000077 (0x00000001,0x9072EC8C,0x00000000,0xEDF0E95C)


Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.
```

Worm组件详情

蠕虫组件是从droper的资源中提取出来的。 破坏性恶意软件通常使用传播技术感染机器。

File type	PE32 executable (console) Intel 80386, for Windows
Filename	averfx2swtvZ.exe
File size	261KB
Hash SHA-2	0694bdf9f08e4f4a09d13b7b5a68c0148ceb3fcc79442f4db2aa19dd23681afe
Compile time	2011-11-28 15:53:13
Import hash	bc0eba48e65cc3ae72091c76f068f3e5

蠕虫组件可以使用以下名称：

mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\netnbdrve.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\pmod802.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\netmdiscnt.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\netrtl42l.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\mdmadccnt.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\pmca00.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\bth2bht_jbv32.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\cxfalcon_jbL32.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\mdmsupr30.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\digitalmediadevicectl.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\mdmetech2dmv.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\netb57vxx.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\winwsdprint.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\pmkwy005.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\composite005.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\mdmar1_jbv32.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\pmle444.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\kscaptur_jbv32.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\mdmzyxlga.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\usbvideob.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\input_jbv48.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\pmok002_jbv.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\averfx2swtvZ.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\wpdmtp_jbv32.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\mdmti_jbv32.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\printupg_jbv32.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\wiabr788.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\WINDOWS\System32\MaintenaceSrv32.exe
mdamx_5560.exe	3724	CreateFile	C:\?
mdamx_5560.exe	3724	CreateFile	C:C:\Documents and Settings\Owner\Desktop\mdamx_5560.exe

我们注意到该组件拥有扫描本地网络并连接到控制服务器的能力：

虽然蠕虫组件可以传播dropper并连接到远程服务器，但该版本中未使用该组件。

总结

除了恶意软件可能造成的破坏之外，Wiper组件可以独立于droper使用。 2018 Shamoon改进版的功能表明该应用使用了模块化进行开发。
这使wiper同样可以被Shamoon以外的恶意软件下载使用。

Shamoon正显示出不断改进的迹象; 但是，这些改变并没有逃脱McAfee DAT的检测。我们预计这些攻击者会在中东（及其他地区）进行更多的攻击。
我们将继续对其进行监控，并在我们了解更多信息时更新此分析。

IOCs

```
df177772518a8fcedbbc805ceed8daecc0f42fed                    Original dropper x86
ceb7876c01c75673699c74ff7fac64a5ca0e67a1                    Wiper
10411f07640edcaa6104f078af09e2543aa0ca07                   Worm module
43ed9c1309d8bb14bd62b016a5c34a2adbe45943                key8854321.pub
bf3e0bc893859563811e9a481fde84fe7ecd0684                   RawDisk driver
```

McAfee 检测

- Trojan-Wiper!DE07C4AC94A5
- RDN/Generic.dx
- Trojan-Wiper

■■■■■■■■■■■https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/shamoon-returns-to-wipe-systems-in-middle-east-europ

上一篇：WebAssembly的安全性问题... 下一篇：flask之ssti模版注入从零到入门

1. 0 条回复
   - 动动手指，沙发就是你的了！

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