

THE DFIR REPORT

Real Intrusions by Real Attackers, The Truth Behind the Intrusion

REPORTS

ANALYSTS

SERVICES ▾

Thursday, October 31, 2024

ACCESS DFIR LABS

MERCHANDISE

SUBSCRIBE

CONTACT US

THREAT INTELLIGENCE

DETECTION RULES

DFIR LABS

MENTORING & COACHING PROGRAM

CASE ARTIFACTS

adfind

bazar

cobaltstrike

ransomware

rdp

ryuk

yara

Ryuk in 5 Hours

October 18, 2020

Intro

The Ryuk threat actors went from a phishing email to domain wide ransomware in 5 hours. They escalated privileges using Zerologon (CVE-2020-1472), less than 2 hours after the initial phish. They used tools such as Cobalt Strike, AdFind, WMI, and PowerShell to accomplish their objective.

Ryuk has been one of the most proficient ransomware gangs in the past few years, with the FBI claiming [\\$61 million USD](#) having been paid to the group as of February 2020. Earlier in the year, the group grew a little quiet, but that seems to have changed in the past few weeks, with incidents like what occurred at [UHS hospitals](#).

Case Summary

In our previous [Ryuk case](#), we saw the threat actors leverage access to an environment via the Bazar Loader malware. This time around, we saw them accomplish their objective faster, but the

general tactics and techniques stayed similar between incidents.

Bazar was introduced to the environment again with the delivery via phishing emails. For an in depth breakdown on this loader, see [this analysis](#) by Roman Marshanski & [Vitali Kremez](#). Bazar, once running, was seen again injecting into explorer.exe, svchost.exe, and spawning command shell processes.

From this loader we saw initial mapping of the domain, using built-in windows utilities such as Nltest. However, unlike the last case, the threat actors started at a lower privileged user and rather than proceed slowly or cautiously, they exploited the recently disclosed ZeroLogon vulnerability (CVE-2020-1472) to reset the machine password of the primary domain controller.

Lateral movement was initiated via SMB file transfers and WMI executions of Cobalt Strike Beacons. The network indicators align similarly to the prior campaign and were noted by [Kyle Ehmke](#) in response to our last post pivoting off the prior report's intel. From memory analysis, we were also able to conclude the actors were using a trial version of Cobalt Strike with the EICAR string present in the network configuration for the beacon. Both portable executable and DLL beacons were used.

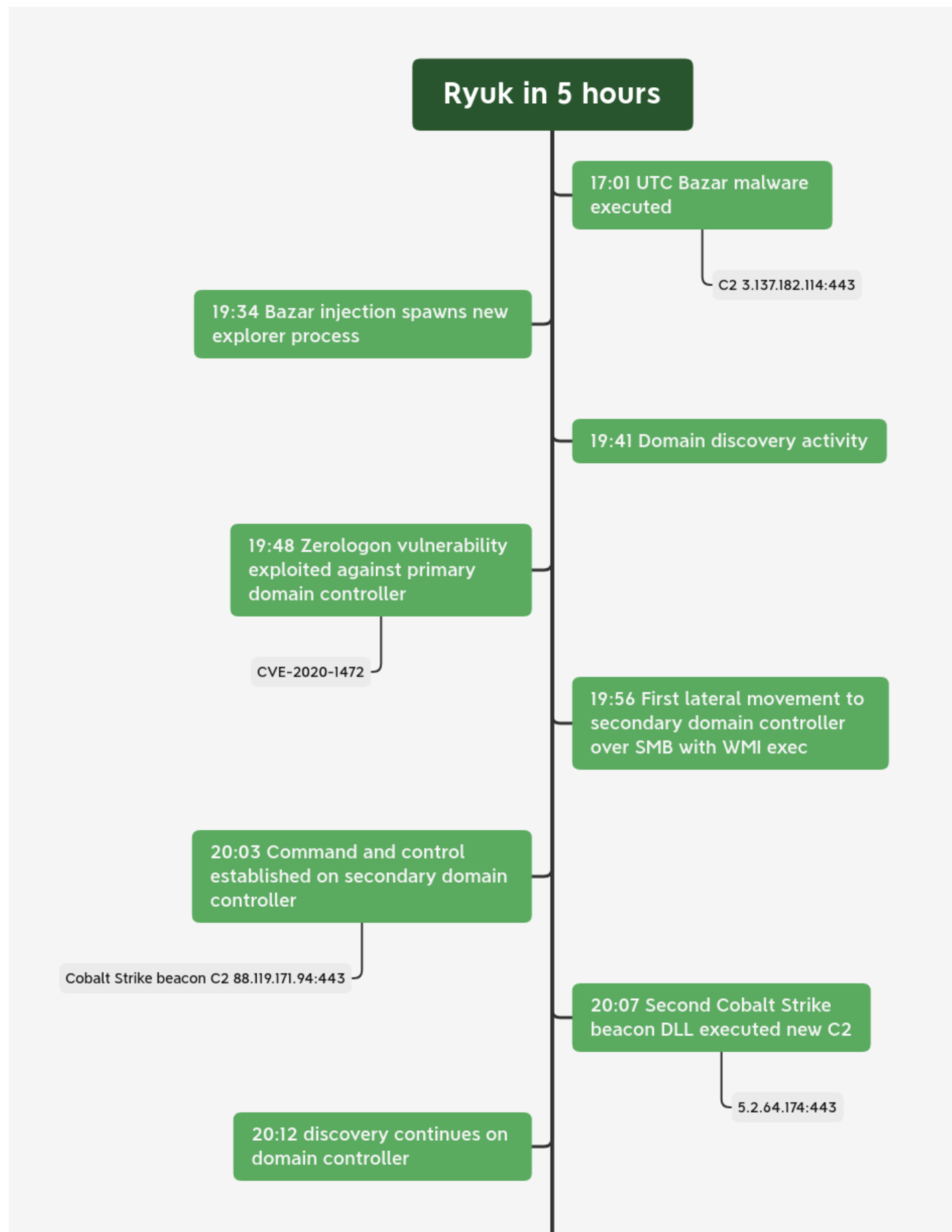
After moving laterally to the secondary domain controller, the threat actor started on more domain discovery via Net and the PowerShell Active Directory module. From there, the threat actors appeared to use the default named pipe privilege escalation module on the server. At this point, the threat actors used RDP to connect from the secondary domain controller, to the first domain controller, using the built in Administrator account.

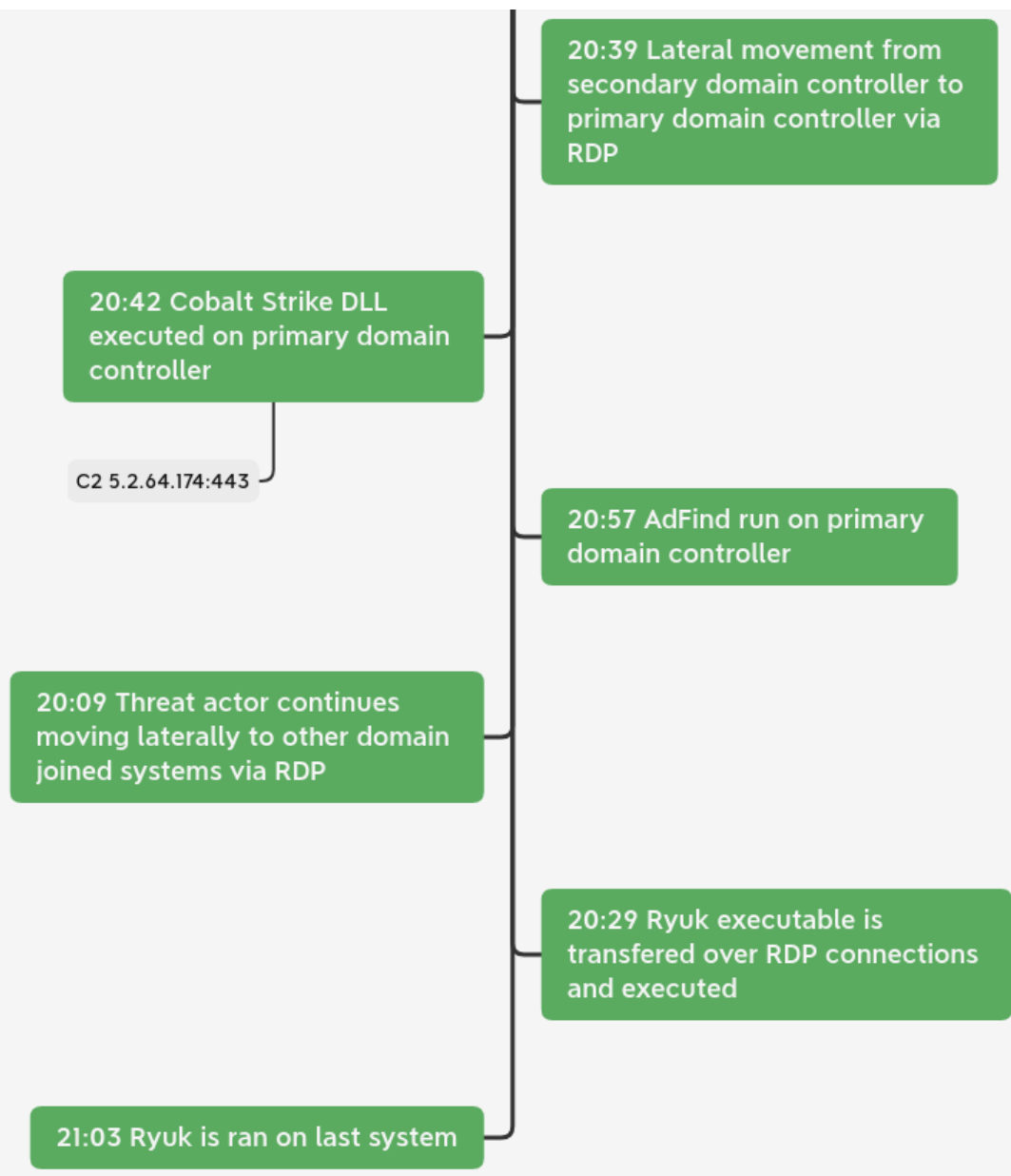
Once on the main domain controller, another Cobalt Strike beacon was dropped and executed. Then more domain reconnaissance was performed using [AdFind](#). Once this completed, at the four hour mark, the threat actors were ready for their final objective.

Four hours and 10 minutes in, the threat actors used the pivot from the primary domain controller to RDP into the Backup server. Backup servers were again targeted first for deployment of the ransomware executable, followed by servers and then workstations. The threat actors finished their objective by executing the ransomware on the primary domain controller, and at the 5 hour mark, the attack completed.

While last time we commented on the lead time between the first and second day to aid detection and response activity, this case goes to show that you can't count on that kind of timescale. You need to be ready to act in less than an hour, to make sure you can effectively disrupt the threat actor.

Timeline







MITRE ATT&CK

Initial Access

Access was initiated by a phishing email leading to the Bazar Loader malware executable.

Execution

Bazar relies on user execution of an executable to run. This user was a Domain User and did not have any other permissions.

Privilege Escalation

CVE-2020-1472 was used to reset the credentials on one of the domain controllers in the environment. After resetting the password, the threat actors then targeted a different domain controller, potentially due to breaking services by use of their exploit.

No.	Time	Source	Destination	Protocol	Length	Info
13610	105.683265	10.	10.	DCE/RPC	330	Bind: call_id: 2, Fragment: Single, 3 context items: RPC_NETLOGON V1.0 (32bit NDR), RPC_NETLOGON V1.0 (64bit NDR), RPC_NETLOGON V1.0 (6cb71c2c-9812-4540-0300-000000000000)
13613	105.683268	10.	10.	DCE/RPC	254	Bind ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 3 results: Provider rejection, Acceptance, Negotiate ACK
13614	105.683269	10.	10.	RPC_NETLOGON	322	NetServerReqChallenge request,
13615	105.683271	10.	10.	RPC_NETLOGON	286	NetServerReqChallenge response
13622	105.683316	10.	10.	DCE/RPC	330	Bind: call_id: 2, Fragment: Single, 3 context items: RPC_NETLOGON V1.0 (32bit NDR), RPC_NETLOGON V1.0 (64bit NDR), RPC_NETLOGON V1.0 (6cb71c2c-9812-4540-0300-000000000000)
13625	105.683319	10.	10.	DCE/RPC	254	Bind ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 3 results: Provider rejection, Acceptance, Negotiate ACK
13626	105.683320	10.	10.	RPC_NETLOGON	366	NetServerAuthenticate2 request
13627	105.683321	10.	10.	RPC_NETLOGON	210	NetServerAuthenticate2 response, STATUS_ACCESS_DENIED
13634	105.683346	10.	10.	DCE/RPC	330	Bind: call_id: 2, Fragment: Single, 3 context items: RPC_NETLOGON V1.0 (32bit NDR), RPC_NETLOGON V1.0 (64bit NDR), RPC_NETLOGON V1.0 (6cb71c2c-9812-4540-0300-000000000000)
13637	105.683364	10.	10.	DCE/RPC	254	Bind ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 3 results: Provider rejection, Acceptance, Negotiate ACK
13638	105.683365	10.	10.	RPC_NETLOGON	322	NetServerReqChallenge request,
13639	105.683366	10.	10.	RPC_NETLOGON	286	NetServerReqChallenge response
13646	105.683388	10.	10.	DCE/RPC	330	Bind: call_id: 2, Fragment: Single, 3 context items: RPC_NETLOGON V1.0 (32bit NDR), RPC_NETLOGON V1.0 (64bit NDR), RPC_NETLOGON V1.0 (6cb71c2c-9812-4540-0300-000000000000)
13649	105.683406	10.	10.	DCE/RPC	254	Bind ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 3 results: Provider rejection, Acceptance, Negotiate ACK
13650	105.683407	10.	10.	RPC_NETLOGON	366	NetServerAuthenticate2 request
13652	105.683425	10.	10.	RPC_NETLOGON	210	NetServerAuthenticate2 response, STATUS_ACCESS_DENIED
13660	105.683451	10.	10.	DCE/RPC	330	Bind: call_id: 2, Fragment: Single, 3 context items: RPC_NETLOGON V1.0 (32bit NDR), RPC_NETLOGON V1.0 (64bit NDR), RPC_NETLOGON V1.0 (6cb71c2c-9812-4540-0300-000000000000)
13663	105.683479	10.	10.	DCE/RPC	254	Bind ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 3 results: Provider rejection, Acceptance, Negotiate ACK
13664	105.683471	10.	10.	RPC_NETLOGON	322	NetServerReqChallenge request,
13665	105.683472	10.	10.	RPC_NETLOGON	286	NetServerReqChallenge response
13672	105.683487	10.	10.	DCE/RPC	330	Bind: call_id: 2, Fragment: Single, 3 context items: RPC_NETLOGON V1.0 (32bit NDR), RPC_NETLOGON V1.0 (64bit NDR), RPC_NETLOGON V1.0 (6cb71c2c-9812-4540-0300-000000000000)
13675	105.683497	10.	10.	DCE/RPC	254	Bind ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 3 results: Provider rejection, Acceptance, Negotiate ACK
13676	105.683498	10.	10.	RPC_NETLOGON	366	NetServerAuthenticate2 request
13677	105.683505	10.	10.	RPC_NETLOGON	210	NetServerAuthenticate2 response
13684	105.683541	10.	10.	DCE/RPC	330	Bind: call_id: 2, Fragment: Single, 3 context items: RPC_NETLOGON V1.0 (32bit NDR), RPC_NETLOGON V1.0 (64bit NDR), RPC_NETLOGON V1.0 (6cb71c2c-9812-4540-0300-000000000000)
13687	105.683544	10.	10.	DCE/RPC	254	Bind ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 3 results: Provider rejection, Acceptance, Negotiate ACK
13688	105.683560	10.	10.	RPC_NETLOGON	882	NetServerPasswordSet2 request(Malformed Packet)
13690	105.683562	10.	10.	RPC_NETLOGON	210	NetServerPasswordSet2 response(Malformed Packet)

Frame 13688: 882 bytes on wire (7056 bits), 882 bytes captured (7056 bits)

Ethernet II, Src: [REDACTED]

Internet Protocol

Transmission Control Protocol, Src Port: 53837, Dst Port: 445, Seq: 563280, Ack: 451532, Len: 828

NetBIOS Session Service

SMB2 (Server Message Block Protocol version 2)

Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Request, Fragment: Single, FragLen: 704, Call: 2, Ctx: 1, [Resp: #13690]

Microsoft Network Logon, NetServerPasswordSet2

Operation: NetServerPasswordSet2 (30)

[Response in frame: 13690]

Server Handle

unknown string

Referent ID: 0x0000000000000000

Max Count: 0

Offset: 5

Actual Count: 4300080

[Malformed Packet: RPC_NETLOGON]

[Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]

[Malformed Packet (Exception occurred)]

[Severity level: Error]

[Group: Malformed]

Packet showing the zeroed out password.

Microsoft Network Logon, NetServerPasswordSet2
Operation: NetServerPasswordSet2 (30)
[Request in frame: 13688]
AUTHENTICATOR: return_authenticator
Referent ID: 0x727a324725c96601
Credential: 0000000000000000
[Malformed Packet: RPC_NETLOGON]
[Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
[Malformed Packet (Exception occurred)]
[Severity level: Error]
[Group: Malformed]

On one of the domain controllers we saw use of the Cobalt Strike named pipe escalation.

```
C:\Windows\system32\cmd.exe /c echo 92d8cc45954 > \\.\pipe\446b3c
```

Defense Evasion

On the first domain controller that the treat actors connected to after their initial connection, they dropped a DLL and executed it via rundll32.

```
C:\Windows\system32\cmd.exe /C rundll32 C:\Windows\system32\SQL.dll, StartW
```

Dropped via RDP and executed via rundll32 on the second domain controller.


```
rundll32 C:\PerfLogs\arti64.dll, rundll
```

Shortly after, the DLL was called again via regsrv32.

```
regsvr32 C:\PerfLogs\arti64.dll
```

Then a 2nd DLL was dropped and executed in a similar manner on the 2nd DC.

```
rundll32 C:\\PerfLogs\\socks64.dll, rundll
```

Discovery

Ran on the beachhead.

```
nltest /domain_trusts /all_trusts  
nltest /dclist:DOMAIN  
net group "Domain admins" /DOMAIN
```

Ran on a domain controller.

```
net group "enterprise admins" /domain  
nltest /domain_trusts /all_trusts  
nltest /dclist:"DOMAIN"  
ping DOMAINCONTROLLER  
cmd.exe /C time  
net user administrator /domain
```

Then they imported the PowerShell Active Directory module.

They then ran the following looking for host names, operating systems and last logon dates of all AD systems.

```
C:\Windows\system32\cmd.exe /C Get-ADComputer -Filter {enabled -eq $true} -p
```

After already completing the above discovery work and having already pivoted to their 2nd domain controller, the threat actors moved on to AdFind for further domain reconnaissance.

```
C:\Windows\Temp\adf\AdFind.exe  
C:\Windows\Temp\adf\adf.bat
```

Contents of the script ran the following with AdFind.

```
adfind.exe -f "(objectcategory=person) "  
adfind.exe -f "objectcategory=computer"  
adfind.exe -f "(objectcategory=organizationalUnit) "  
adfind.exe -sc trustdmp  
adfind.exe -subnets -f (objectCategory=subnet)  
adfind.exe -f "(objectcategory=group) "  
adfind.exe -gcb -sc trustdmp
```

The threat actor then ran this command a few times.

```
nltest /domain_trusts /all_trusts
```

Lateral Movement

The first lateral movement occurred to the domain controller not affected by the use of CVE-2020-1472. An executable was transferred to it via SMB using a domain administrator account.

After transferring the exe, the threat actors utilized WMI from the beachhead host to execute the file.

```
C:\Windows\system32\cmd.exe /C WMIC/node:"DC.DOMAIN.local" process call crea
```

The presence of the EICAR strings point to the Cobalt Strike software being used as a [trial version](#).

They accessed the GPO's for the domain but none were modified or added.

```
mmc.exe" "C:\Windows\System32\gpedit.msc"
```

Shortly there after we saw a Cobalt Strike DLL transferred via the RDP connection.

RDP was used to pivot from the main domain controller and distribute the final ransomware payload enterprise wide.

Command and Control

After our previous report, [@kyleehmke](#) pivoted off of our prior Ryuk report and used the network data to link several of these [domains](#) which we saw in this case.

Bazar:

Report_Print.exe

3.137.182.114:443

cstr3.com

Cobalt Strike:

servisses.exe

88.119.171.94:443

Certificate [[86:77:d8:5e:51:69:ac:e2:08:07:2e:b0:dc:6c:10:9e:25:80:70:a6](#)]

Not Before [2020/10/06 13:33:55 UTC](#)

Not After [2021/10/06 13:33:55 UTC](#)

Issuer Org [lol](#)

Subject Common [havemosts.com](#)

Subject Org [lol](#)

Public Algorithm [rsaEncryption](#)

JA3: 57f3642b4e37e28f5cbe3020c9331b4c

JA3s: e35df3e00ca4ef31d42b34bebaa2f86e

SQL.dll

5.2.64.174:443

Certificate [[36:d5:68:f9:be:2a:34:e1:76:3d:89:78:e5:62:4d:fc:ae:02:97:ad](#)]

Not Before [2020/10/02 16:45:57 UTC](#)

Not After [2021/10/02 16:45:57 UTC](#)

Issuer Org [lol](#)

Subject Common [quwasd.com](#)

Subject Org [lol](#)

Public Algorithm [rsaEncryption](#)

JA3: a0e9f5d64349fb13191bc781f81f42e1

JA3s: ae4edc6faf64d08308082ad26be60767

Impact

Starting around 4.5 hours after the initial Bazar malware was executed, the Ryuk threat actors acted on their final objectives and initiated RDP connections from the domain controller previously exploited, to the rest of the environment. This time they initiated the ransomware first on the secondary domain controller (their 1st pivot) and transferred the Ryuk executable over the RDP connection.

Enjoy our report? Please consider donating \$1 or more to the project using [Patreon](#). Thank you for your support!

We also have pcaps, files, memory images, Kape and Redline packages available [here](#).

IOCs

https://misppriv.circl.lu/events/view/80223 &
https://otx.alienvault.com/pulse/5f8cce76f5614d9b220181b6

Network

```
3.137.182.114:443
cstr3.com
88.119.171.94:443
havemosts.com
5.2.64.174:443
guwasd.com
```

File

```
servisses.exe
d971827d974effedaeaf7d62b619b1dd
c3a846eb04e2fe765e56fa15a0d5c1eb650ccba3
1d8b7faf5f290465cc742e07abca78fac419135b191071cc77912263cd1dde1d
socks64.dll
890206f0c506366d480e02fc9fed988a
ba1542d9b55fff21bda9495ed884404b0436cff2
feb8c2bcb71da02dbbeecb999869e053cf96af8cce6f9705cadca4338133d3b5
SQL.dll
3785d87f6995b4b95d9b55f8d2556237
9b44a8f0bb2d65fb19e7ca7bbd85b36c176f3d60
d67461ba45a4edf3b2a69b3e64303fda8130bd1fc7a1173f35c1fe67b40c9639
arti64.dll
3785d87f6995b4b95d9b55f8d2556237
9b44a8f0bb2d65fb19e7ca7bbd85b36c176f3d60
d67461ba45a4edf3b2a69b3e64303fda8130bd1fc7a1173f35c1fe67b40c9639
xxx.exe
5b8b66ddbfb1fd67211e9a4bf78c1700
```

```
cdb042dd8e9dc17f677c991b386f4cd242f2628d
ccde47a0d315dcd4740fccfe8e8110fbb1fd85bb305734fec409f52051790c98
```

Detections

Network

```
GPL NETBIOS SMB-DS IPC$ share access
ET POLICY SMB2 NT Create AndX Request For a DLL File - Possible Lateral Move
ET POLICY SMB2 NT Create AndX Request For an Executable File
```

Sigma

https://github.com/Neo23x0/sigma/blob/master/rules/windows/malware/win_mal_ryuk.yml

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

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

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

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

Detects AdFind usage from a past case:

```
title: AdFind Recon
description: Threat Actor using AdFind for reconnaissance.
author: The DFIR Report
date: 2019/8/2
references:
```



```
- https://thedfirreport.com/2020/08/03/dridex-from-word-to-domain-domina
tags:
- attack.remote_system_discovery
- attack.T1018
logsource:
  category: process_creation
  product: windows
detection:
  selection_1:
    CommandLine|contains:
      - adfind -f objectcategory=computer
  selection_2:
    CommandLine|contains:
      - adfind -gcb -sc trustdmp
  condition: selection_1 or selection_2
falsepositives:
  - Legitimate Administrator using tool for Active Directory querying
level: medium
status: experimental
```

Yara

```
/*
YARA Rule Set
Author: The DFIR Report
Date: 2020-10-13
Identifier: Case 1006 Ryuk
Reference: https://thedfirreport.com
*/

/* Rule Set -----

import "pe"
```

```

rule ryuk_1006_servisses_procdump {
meta:
description = "files - file servisses-procdump.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2020-10-13"
hash1 = "387894a0b404c67e722799308b12ff2be31d2e8ce798aa53d971f0c13805d54d"
strings:
$s1 = "c:/crossdev/src/winpthreads-svn6233/src/mutex.c" fullword ascii
$s2 = "mutex_global_shmem" fullword ascii
$s3 = "mutex_global_static_shmem" fullword ascii
$s4 = "_pthread_key_dest_shmem" fullword ascii
$s5 = "_pthread_key_sch_shmem" fullword ascii
$s6 = "_pthread_key_max_shmem" fullword ascii
$s7 = "_pthread_key_lock_shmem" fullword ascii
$s8 = "cannot find name of executable" fullword ascii
$s9 = "tiles32.png" fullword ascii
$s10 = "GetModuleFileName: %s" fullword ascii
$s11 = "IP_DEST_HOST_UNREACHABLE (11003)" fullword ascii
$s12 = "This program requires Windows NT!" fullword ascii
$s13 = "SNMP INVALID_SESSION" fullword ascii
$s14 = "SNMP TRAP_ERRORS" fullword ascii
$s15 = "SNMP SELECT_FDERRORS" fullword ascii
$s16 = "Some different radices: %d %x %o %#x %#o " fullword ascii
$s17 = "c:/crossdev/src/winpthreads-svn6233/src/rwlock.c" fullword ascii
$s18 = "_pthread_tls_shmem" fullword ascii
$s19 = "IP_DEST_PORT_UNREACHABLE (11005)" fullword ascii
$s20 = "pthr_root_shmem" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 2000KB and
( pe.imphash() == "a90d500745a1ce2417c01fecefbcb2851" or 8 of them )
}

rule ryuk_1006_files_socks64 {
meta:
description = "files - file socks64.dll"
author = "The DFIR Report"
reference = "https://thedfirreport.com"

```

```

date = "2020-10-13"
hash1 = "feb8c2bcb71da02dbbeecb999869e053cf96af8cce6f9705cadca4338133d3b5"
strings:
$x1 = "C:\\Users\\Izidu\\Desktop\\2019\\WindowsSDK7-Samples-master\\WindowsS
$s2 = "C:\\Users\\Izidu\\Desktop\\2019\\WindowsSDK7-Samples-master\\WindowsS
$s3 = "PluginSample.dll" fullword ascii
$s4 = "AppPolicyGetProcessTerminationMethod" fullword ascii
$s5 = "luginSample.pdb" fullword ascii
$s6 = "rundll" fullword ascii
$s7 = "AcquireSamplePlugin::DisplayConfigureDialog" fullword wide
$s8 = "AppPolicyGetThreadInitializationType" fullword ascii
$s9 = "`template-parameter-" fullword ascii
$s10 = "operator<=>" fullword ascii
$s11 = "operator co_await" fullword ascii
$s12 = "AppPolicyGetWindowingModel" fullword ascii
$s13 = "Transfer Completed Successfully!" fullword wide
$s14 = "AppPolicyGetShowDeveloperDiagnostic" fullword ascii
$s15 = "noexcept" fullword ascii
$s16 = "Read-Only Photo Acquire Plugin" fullword wide
$s17 = "api-ms-win-appmodel-runtime-l1-1-2" fullword wide
$s18 = "Software\\Microsoft\\Windows\\CurrentVersion\\Photo Acquisition\\Plu
$s19 = ".?AUIUserInputString@@" fullword ascii
$s20 = "g0DVNrB\\\"Rtf#" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 2000KB and
( pe.imphash() == "0fd22f187f22ab4ec2eb55f91ccefa7a" and ( pe.exports("SGeru
}

rule ryuk_1006_Report_Print {
meta:
description = "files - file Report_Print.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2020-10-13"
hash1 = "23ac461f9b5128841cafabb4282432252ea7b57874595cf6fe8457fc1ac65007"
strings:

```

```

$s1 = "kErNe132.Dll" fullword wide
$s2 = "DOOKOL.exe" fullword ascii
$s3 = "c:/crossdev/src/winpthreads-svn6233/src/mutex.c" fullword ascii
$s4 = "hmutex" fullword ascii
$s5 = "._FindPESectionExec" fullword ascii
$s6 = "mutex_global_shmem" fullword ascii
$s7 = "processthreadsapi.h" fullword ascii
$s8 = "mutex_global_static_shmem" fullword ascii
$s9 = "TargetIp" fullword ascii
$s10 = "c:\\crossdev\\gccmaster\\build-tdm64\\gcc\\x86_64-w64-mingw32\\libgc
$s11 = "h:\\crossdev\\gccmaster\\build-tdm64\\runtime\\mingw-w64-crt" fullwc
$s12 = "J__mingw_winmain_lpCmdLine" fullword ascii
$s13 = "GNU C 4.8.1 -mtune=generic -march=x86-64 -g -O2 -O2 -O2 -fbuilding-1
$s14 = "GNU C 4.8.1 -mtune=generic -march=x86-64 -g -O2 -O2 -O2 -fbuilding-1
$s15 = "GNU C 4.8.1 -m64 -mtune=generic -march=x86-64 -g -O2 -std=gnu99" ful
$s16 = "GNU C 4.8.1 -mtune=generic -march=x86-64 -g -O2 -O2 -O2 -fbuilding-1
$s17 = "9lpszCommandLine" fullword ascii
$s18 = "=__mingw_GetSectionForAddress" fullword ascii
$s19 = "__mingw_winmain_lpCmdLine" fullword ascii
$s20 = "%Target" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 3000KB and
( pe.imphash() == "8f0088451a1156246379abc67514cacf" and pe.exports("CSBhvSW
}

rule ryuk_1006_files_xxx {
meta:
description = "files - file xxx.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2020-10-13"
hash1 = "ccde47a0d315dcd4740fccfe8e8110fbb1fd85bb305734fec409f52051790c98"
strings:
$s1 = "DOOKOL.exe" fullword ascii
$s2 = "c:/crossdev/src/winpthreads-svn6233/src/mutex.c" fullword ascii
$s3 = "hmutex" fullword ascii
$s4 = "mutex_global_shmem" fullword ascii
$s5 = "processthreadsapi.h" fullword ascii

```

```

$s6 = "mutex_global_static_shmem" fullword ascii
$s7 = "fake_get_output_format" fullword ascii
$s8 = "&rvaTarget" fullword ascii
$s9 = "h:\\crossdev\\gccmaster\\build-tdm64\\runtime\\mingw-w64-crt" fullwor
$s10 = "c:\\crossdev\\gccmaster\\build-tdm64\\gcc\\x86_64-w64-mingw32\\32\\1
$s11 = "E__mingw_winmain_lpCmdLine" fullword ascii
$s12 = "GNU C 4.8.1 -m32 -mtune=generic -march=x86-64 -g -O2 -O2 -O2 -fbuild
$s13 = "GNU C 4.8.1 -m32 -mtune=generic -march=x86-64 -g -O2 -O2 -O2 -fbuild
$s14 = "GNU C 4.8.1 -m32 -mtune=generic -march=x86-64 -g -O2 -O2 -O2 -fbuild
$s15 = "GNU C 4.8.1 -m32 -mtune=generic -march=x86-64 -g -O2 -std=gnu99" ful
$s16 = "__mingw_winmain_lpCmdLine" fullword ascii
$s17 = "Npthead_getspecific" fullword ascii
$s18 = "__gthread_getspecific" fullword ascii
$s19 = "__mingw_GetSectionForAddress" fullword ascii
$s20 = "4lpszCommandLine" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 2000KB and
( pe.imphash() == "00f3261b5b33a9b1e8b6003f4056a885" and pe.exports("CSBhvSW
}

rule ryuk_1006_servisses {
meta:
description = "files - file servisses.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2020-10-13"
hash1 = "1d8b7faf5f290465cc742e07abca78fac419135b191071cc77912263cd1dde1d"
strings:
$s1 = "DOOKOL.exe" fullword ascii
$s2 = "c:/crossdev/src/winpthreads-svn6233/src/mutex.c" fullword ascii
$s3 = "mutex_global_shmem" fullword ascii
$s4 = "mutex_global_static_shmem" fullword ascii
$s5 = "_pthread_key_dest_shmem" fullword ascii
$s6 = "_pthread_key_max_shmem" fullword ascii
$s7 = "_pthread_key_sch_shmem" fullword ascii
$s8 = "_pthread_key_lock_shmem" fullword ascii

```

```

$s9 = "cannot find name of executable" fullword ascii
$s10 = "tiles32.png" fullword ascii
$s11 = "GetModuleFileName: %s" fullword ascii
$s12 = "IP_DEST_HOST_UNREACHABLE (11003)" fullword ascii
$s13 = "This program requires Windows NT!" fullword ascii
$s14 = "SNMP INVALID_SESSION" fullword ascii
$s15 = "SNMP TRAP_ERRORS" fullword ascii
$s16 = "SNMP SELECT_FDERRORS" fullword ascii
$s17 = "Some different radices: %d %x %o %#x %#o " fullword ascii
$s18 = "c:/crossdev/src/winpthreads-svn6233/src/rwlock.c" fullword ascii
$s19 = "_pthread_tls_shmem" fullword ascii
$s20 = "IP_DEST_PORT_UNREACHABLE (11005)" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 2000KB and
( pe.imphash() == "a90d500745a1ce2417c01fecefbcb2851" and pe.exports("KADWEGA
}

rule ryuk_1006_files_SQL {
meta:
description = "files - file SQL.dll"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2020-10-13"
hash1 = "d67461ba45a4edf3b2a69b3e64303fda8130bd1fc7a1173f35c1fe67b40c9639"
strings:
$s1 = ".data$_ZN12_GLOBAL__N_110fake_mutexE" fullword ascii
$s2 = ".data$_ZZN12_GLOBAL__N_116get_static_mutexEvE4once" fullword ascii
$s3 = "DOOKOL.dll" fullword ascii
$s4 = "_ZN12_GLOBAL__N_110fake_mutexE" fullword ascii
$s5 = "_ZZN12_GLOBAL__N_116get_static_mutexEvE4once" fullword ascii
$s6 = ".data$_ZN12_GLOBAL__N_115emergency_mutexE" fullword ascii
$s7 = ".data$_ZN12_GLOBAL__N_1L12static_mutexE" fullword ascii
$s8 = "__shmem_winpthreads_grabber_mutex_global_shmem" fullword ascii
$s9 = "__shmem_winpthreads_init_mutex_global_shmem" fullword ascii
$s10 = "__shmem_winpthreads_ptr_mutex_global_shmem" fullword ascii
$s11 = "c:/crossdev/src/winpthreads-svn6233/src/mutex.c" fullword ascii
$s12 = "pthread_mutex_lock_intern" fullword ascii
$s13 = "__shmem_winpthreads_init_mutex_global_static_shmem" fullword ascii

```

```
$s14 = "__shmem_winpthreads_grabber_mutex_global_static_shmem" fullword ascii
$s15 = "__shmem_winpthreads_ptr_mutex_global_static_shmem" fullword ascii
$s16 = "_Z7ExecutePv" fullword ascii
$s17 = "hmutex" fullword ascii
$s18 = "._FindPESectionExec" fullword ascii
$s19 = "_ZN9__gnu_cxx17__recursive_mutex6unlockEv" fullword ascii
$s20 = ".text$_ZN9__gnu_cxx17__recursive_mutex6unlockEv" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 2000KB and
( pe.imphash() == "d16819dafefb97404d0d0e42adb82e5c" and ( pe.exports("CSBhv
}
```

If you have detections you would like to add to this section, please contact us and we will credit you.

MITRE

Spearphishing Link – T1192

🌐 Remote Desktop Protocol – T1076

🌐 Remote File Copy – T1105

🌐 Windows Management Instrumentation – T1047

🌐 Command-Line Interface – T1059

🌐 Domain Trust Discovery – T1482

🌐 Remote System Discovery – T1018

🌐 System Time Discovery – T1124

🌐 Data Encrypted for Impact – T1486

🌐 Commonly Used Port – T1043

🌐 Standard Application Layer Protocol – T1071

🌐 Standard Cryptographic Protocol – T1032

🌐 User Execution – T1204

🌐 Valid Accounts – T1078

🌐 Exploitation for Privilege Escalation – T1068

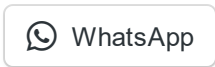
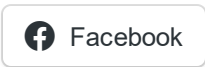
🌐 Signed Binary Proxy Execution – T1218

🌐 Rundll32 – T1085

🌐 Regsvr32 – T1117

(internal case 1006)

Share this:



adfind _ bazar _ cobalt strike _ kegtap _ malspam _ ryuk

« RYUK'S RETURN

RYUK SPEED RUN, 2 HOURS TO RANSOM »

Search

Type your email...

Subscribe



Register For Our Next CTF



Reports



Threat Intelligence



Detection Rules



DFIR Labs



Mentoring and Coaching