



بیم‌الاعراض





snatch Ransomware

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو





فهرست مطالب

۴	مقدمه
۵	توضیحات اولیه
۶	دسترسی اولیه
۷	حرکت جانبی و ماندگاری (Lateral Movement and Persistence):
۱۰	اقدام بر روی اهداف (Action on Objectives):
۱۱	تیم Snatch
۱۱	بازیابی (Recovery)
۱۲	نتیجه گیری (Conclusion)
۱۲	تحلیل Safe.exe
۱۳	IOCs





مقدمه

حمله باج افزار Snatch نمونه‌ای روشن از این است که چطور یک اشتباه ظاهراً ساده – در معرض بودن RDP با رمز عبور ضعیف – می‌تواند ظرف چند ساعت به یک فاجعه سازمانی تبدیل شود. در این سناریو، مهاجم تنها در کمتر از پنج ساعت توانست از مرحله حدس زدن رمز عبور یک حساب Administrator از طریق حمله Brute Force روی RDP، به استقرار یک Meterpreter reverse shell، راه‌اندازی پروکسی RDP روی Tor، حرکت جانبی تا Domain Controller و نهایتاً رمزگذاری همه سیستم‌های عضو دامنه برسد.

این حمله نشان می‌دهد حتی مهاجمی که از نظر فنی چندان پیچیده نیست، اگر به سرعت و هدفمند عمل کند، می‌تواند در مدت زمانی بسیار کوتاه خسارتی سنگین به یک سازمان بزرگ وارد کرده و با حداقل سرمایه‌گذاری زمانی، به سود قابل توجهی از طریق باج‌گیری دست یابد.

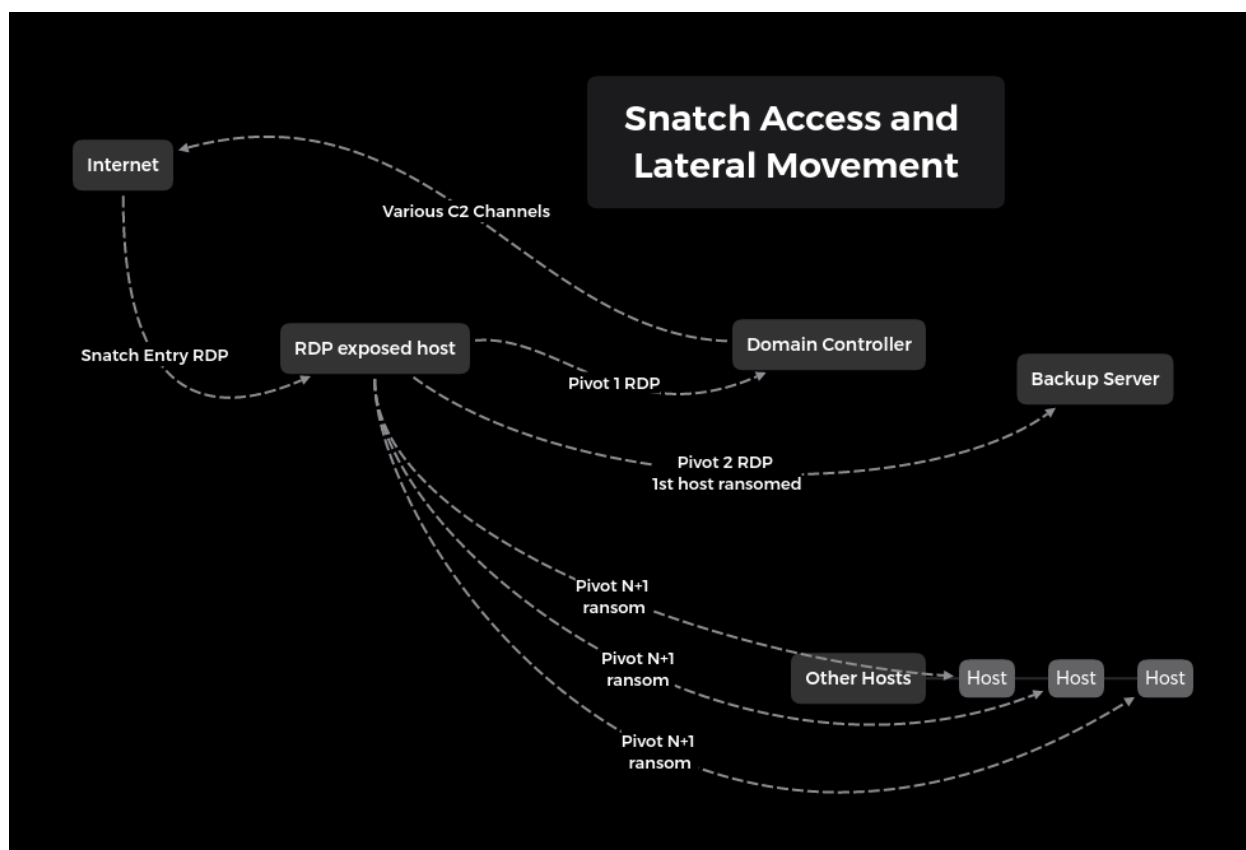
مطالعه این گزارش می‌تواند دید بهتری نسبت به رفتار مهاجمان، ابزارهای مورد استفاده و تکنیک‌های به‌کاررفته در چنین حملاتی ارائه دهد و به درک بهتر نحوه شناسایی و مقابله با این تهدیدات کمک کند.





توضیحات اولیه

یک باج‌افزار دیگر مبتنی بر حمله Brute Force از طریق RDP دوباره حمله کرد — این بار تیم Snatch

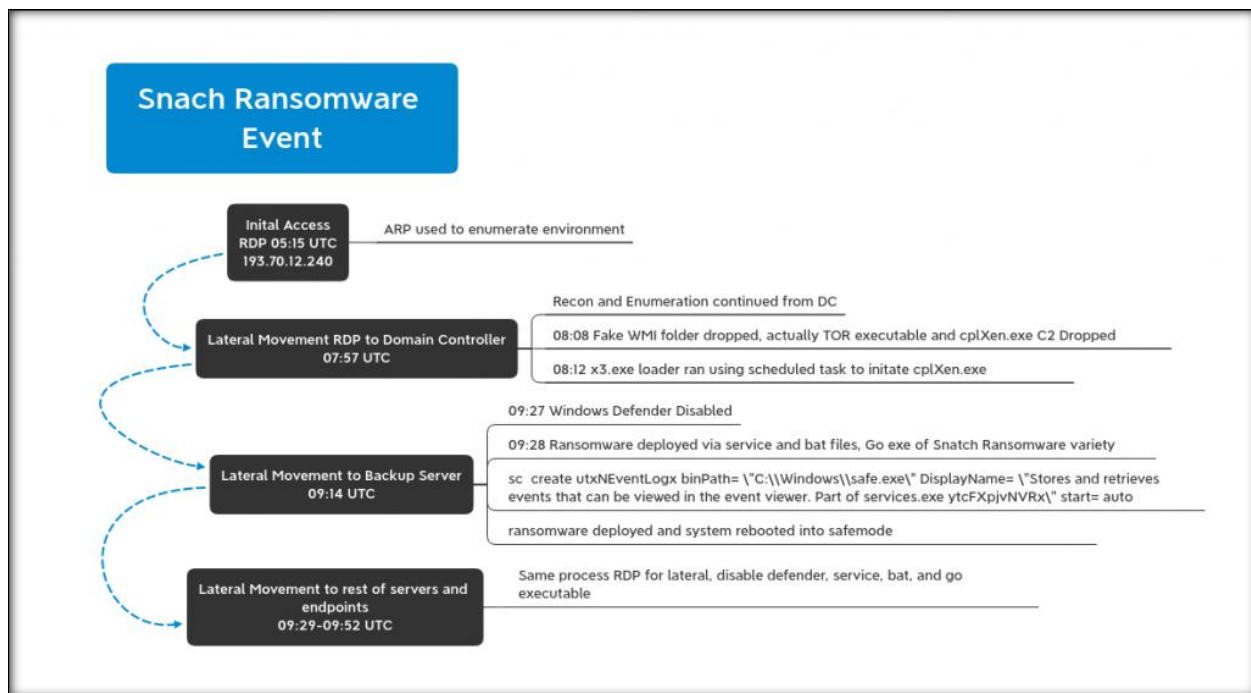


تیم Snatch توانست در مدت کمتر از ۵ ساعت، از مرحله حدس زدن رمز عبور یک حساب Administrator از طریق RDP، به اجرای یک Meterpreter reverse shell و همچنین یک پروکسی RDP از طریق شبکه Tor روی یک Domain Controller (DC) برسد، و در نهایت تمامی سیستم‌های عضو دامنه را رمزگذاری کند.

Snatch یک نمونه‌ی شناخته‌شده از باج‌افزار است که پیش از شروع فرآیند رمزگذاری، سیستم‌ها را به حالت Safe Mode ریبوت می‌کند.

تیم SophosLabs هم قبلاً یک تحلیل بسیار خوب درباره Snatch منتشر کرده که رفتار آن بسیار شبیه چیزی بود که ما مشاهده کردیم.





دسترسی اولیه

تیم Snatch حوالی ساعت ۰۵:۱۵ به وقت UTC از آی پی 193.70.12.240 وارد یک حساب Domain Administrator شد.

در ابتدا، پس از ورود، یک دستور ساده‌ی `arp -a` اجرا کردند.

در ساعت ۰۷:۵۳ UTC، مهاجمان مرحله بعدی را آغاز کردند و دستورات `ipconfig` و `quser` را اجرا کردند.

چند دقیقه بعد، حرکت جانبی را شروع کرده و یک نشست RDP با یک Domain Controller برقرار کردند.





حرکت جانبی و ماندگاری (Lateral Movement and Persistence):

پس از دسترسی به DC، عامل تهدید به سرعت وارد عمل شد و مجموعه‌ای از ابزارها را در مسیر C:\Windows مستقر کرد. این مجموعه شامل دو فایل اجرایی بود که خود را به صورت فایل‌های مربوط به WMI جا زده بودند. یکی از این فایل‌ها با پارامترهای دستوری زیر اجرا شد:

```
CommandLine=C:\Windows\wmis\WmiPrvSystemES.exe --nt-service -f C:\Windows\wmis\libey32.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
```

فایل dat. در واقع یک فایل پیکربندی (configuration file) بود و فایل اجرایی مربوطه، TOR بود که برای ایجاد یک تونل RDP استفاده می‌شد. (مگه این کار خیلی خیلی کند نیست؟)

```
HiddenServiceDir C:\Windows\wmis\CrashReporter
ClientOnly 1
ExitRelay 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/SeU8VFwzAdm8nDQ iat-mode=0
Bridge obfs4 185.198.57.215:443 9615531C2517AF54C44C99A69C4F69D053DAE585 cert=zNqqg8vzF7HnkhCc/mvPLXoaWlLumk2oYqsS2xYyStZi1A4i070iPqjtkPzdtSx95DKLrca iat-mode=0
```

فایل اجرایی دیگر در پوشه‌ی wmis یک فایل اجرایی نوشته‌شده با زبان Go بود که منبع آن مشخص نیست؛ احتمال داده می‌شود که به نوعی با قابلیت‌های مشابه uTorrent مرتبط باشد.

اقدام بعدی مهاجمان ایجاد یک reverse shell بود که احتمال می‌دهیم از نوع Meterpreter بوده باشد.





ارتباط با سرور C2 از طریق HTTPS روی پورت ۴۴۳ به آدرس 91.229.77.161 و با استفاده از فایل cplXen.exe برقرار شد.

وجود لاگ‌هایی که نشان‌دهنده استفاده از سرویس‌های Named Pipe هستند نیز احتمال استفاده از Meterpreter یا احتمالاً Cobalt Strike را افزایش می‌دهد.

برای این فعالیت هیچ امضای ET Pro فعال نشده، اما در آن زمان SSL inspection نیز فعال نبود، بنابراین ممکن است ترافیک رمزگذاری شده باعث عدم شناسایی شده باشد.

```
"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"
```

سپس یک فایل اجرایی جداگانه برای ماندگاری مخفیانه cplXen.exe روی سیستم قرار داده شد.

فایل X3.exe یک Loader است که از سه فایل DLL (که در واقع فایل‌های ini هستند) استفاده می‌کند تا cplXen.exe را اجرا کند.

D...	Location	Label	Code Unit	String View
			CALL dword ptr [EAX + 0x7c]	"Q!ntFD"
			PUSH EAX	"PhpGD"
			PUSH EAX	"PhpGD"
		u_kb05987631s.dll_0044...	unicode u"kb05987631s.dll"	u"kb05987631s.dll"
		u_fw0a53482aa.dll_0044...	unicode u"fw0a53482aa.dll"	u"fw0a53482aa.dll"
		u_jd4ob7162ns.dll_0044...	unicode u"jd4ob7162ns.dll"	u"jd4ob7162ns.dll"
		u_/K_schtasks/Create/R...	unicode u"/K_schtasks /Create /RU SYSTEM /SC ONSTART /TN \"Regular Idle Maintenance\" /TR \"	u"/K_schtasks /Create /RU SYSTE...
		u_&&_exit_0044473c	unicode u" && exit"	u" && exit"
		u_cmd.exe_00444750	unicode u"cmd.exe"	u"cmd.exe"
		u_/K_schtasks/Create/R...	unicode u"/K_schtasks /Create /RU SYSTEM /SC DAILY /ST 00:00 /TN \"Regular Idle Maintenance\" /TR \"	u"/K_schtasks /Create /RU SYSTE...
		s_Error_00445780	ds "Error"	"Error"
		s_Runtime_error_at_000...	ds "Runtime error at 00000000"	"Runtime error at 00000000"
		s_oleaut32.dll	ds "oleaut32.dll"	"oleaut32.dll"
		s_SysFreeString	ds "SysFreeString"	"SysFreeString"
		s_SysReAllocStringLen	ds "SysReAllocStringLen"	"SysReAllocStringLen"

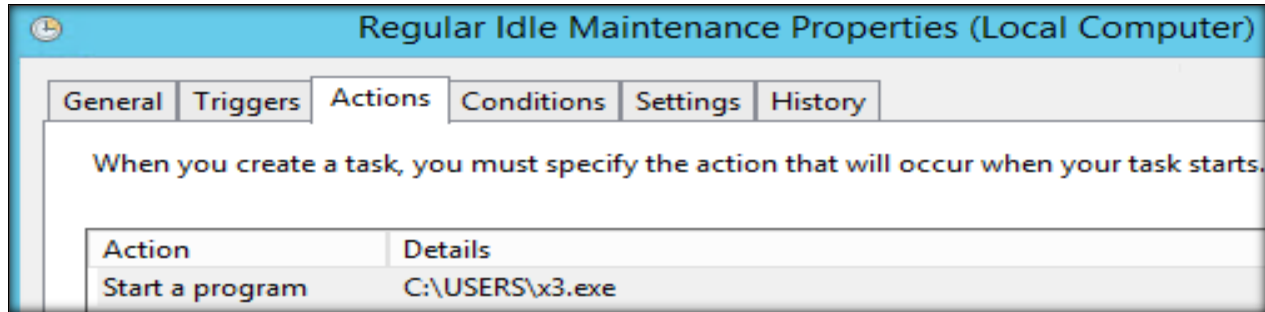
jd4ob7162ns.dll: C:\windows\system32\cplXen.exe /F

fw0a53482aa.dll: 443

kb05987631s.dll: 91.229.77.161

دو Scheduled Task ایجاد شد تا Loader (X3.exe) را اجرا کند، و این Loader به نوبه خود باعث ماندگاری و اجرای مداوم cplXen.exe روی سیستم می‌شود.





فایل X3.exe نسبت به ویروس تیوتور (VT) نسبتاً کم‌تر شناخته شده بود. اگر کسی می‌خواهد بیشتر در این مورد تحقیق کند، خوشحال می‌شویم که با ما تماس بگیرد تا فایل را دریافت کند یا آن را در MISP/VT پیدا کند.

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





اقدام بر روی اهداف (Action on Objectives):

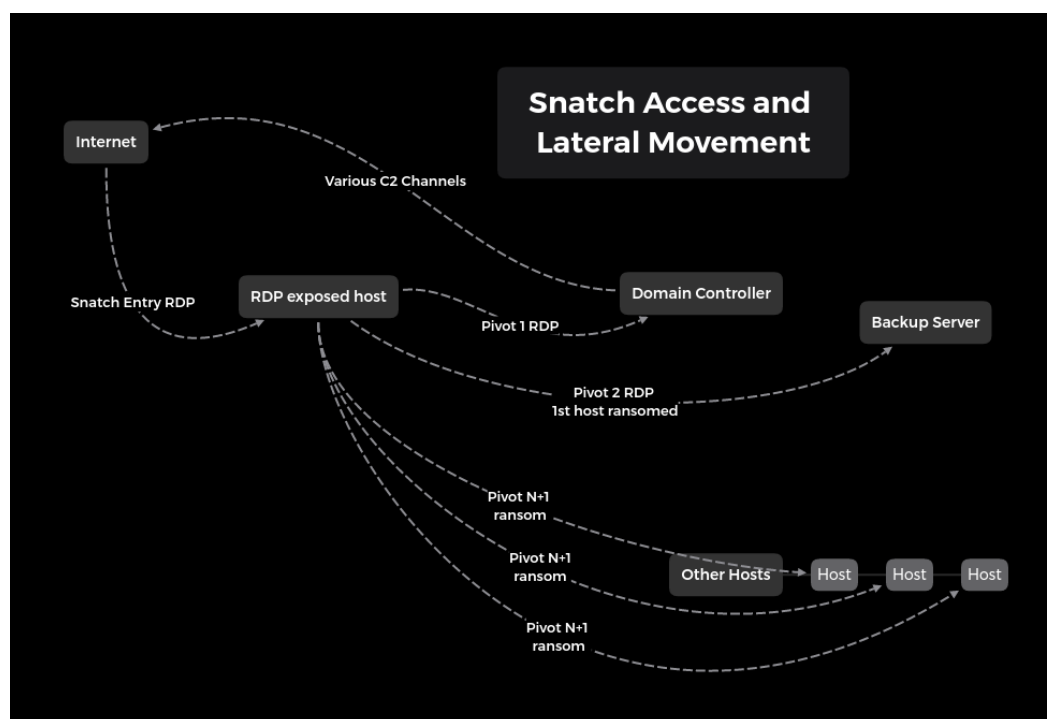
حدود نیم ساعت پس از برقراری موفق ارتباط با سرور C2، این مورد را مشاهده کردیم:

```
eventdata.data esentutl, 1424, 2, C:\Users\
00, [8] 0.000, [9] 0.000, [10] 0.000, [11] 0.000, [12] 0.000., 1 0
\\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
system.channel Application
system.computer
system.eventID 326
system.eventRecordID 4000
system.keywords 0x8000000000000000
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
```

می‌توان نتیجه گرفت که ditsnap به احتمال زیاد روی Domain Controller اجرا شد تا با ایجاد یک snapshot یک نسخه از فایل ntds.dit به دست آورده شود.

چهل و پنج دقیقه بعد، تیم Snatch اولین موفقیت خود را ثبت کرد. آن‌ها با RDP وارد سرور بکاپ شدند، Windows Defender را غیرفعال کردند و فایل safe.exe را اجرا کردند. آن‌ها، این کار را برای همه سیستم‌های دامنه انجام دادند و ظرف ۱۵ دقیقه، تمامی ماشین‌ها (including DC) رمزگذاری شدند.

تمامی سیستم‌ها پیش از شروع رمزگذاری، به حالت Safe Mode ریبوت شدند که باعث شد همه‌ی لاگ‌ها و ابزارهای راه دور از کار بیفتند (لعنت بر حالت Safe Mode!).





روی تمامی سیستمها، موارد زیر باقی مانده‌اند:

```

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.

```

تیم Snatch

تیم Snatch برای ابزار رمزگشا (decryptor)، مبلغ ۴۰ هزار دلار درخواست کرد، اما با مذاکره موفق شدیم مبلغ را به کمتر از ۱۵ هزار دلار کاهش دهیم.

بازیابی (Recovery)

بیاپید یک لحظه تصور کنیم بازیابی در یک سازمان بزرگ چگونه خواهد بود:

تمام سرورها و ماشین‌های آنلاین قبل از شروع رمزگذاری، به حالت Safe Mode بدون شبکه ریپوت شدند، که باعث از دست رفتن دید کامل روی سیستمها می‌شود. این وضعیت خیلی سریع در دسترس‌ساز می‌شود.





نتیجه گیری (Conclusion)

همان طور که بارها دیده ایم، RDP به روش Brute Force هدف قرار می گیرد تا به شبکه دسترسی پیدا شود و سپس عامل تهدید سریعاً Lateral Movement انجام می دهد و باج افزار را نصب می کند.

با وجود آن که انتظار می رفت مهاجمان برای توزیع باج افزار از روش های متمرکزتری مانند GPO یا ابزارهایی نظیر PsExec استفاده کنند، مشاهده کردیم که آن ها به صورت دستی و سیستم به سیستم وارد عمل شدند. این رویکرد در نگاه اول نشانه ای از پیچیدگی فنی پایین تر به نظر می رسد، اما در عمل نشان داد که کارآمدی همیشه وابسته به پیشرفته بودن ابزارها نیست. مهاجمان با سرعت، تمرکز و حداقل اتکا به تکنیک های پیچیده، توانستند عملیات خود را با موفقیت کامل اجرا کنند.

نتیجه این رویکرد ساده اما مؤثر، رمزگذاری کامل دامنه در کمتر از پنج ساعت و مطالبه ۴۰ هزار دلار باج بود؛ رقمی که اگر به زمان اجرای حمله تقسیم شود، معادل حدود ۸ هزار دلار در ساعت خواهد بود. این موضوع به خوبی نشان می دهد که در بسیاری از موارد، سرعت عمل و دسترسی اولیه موفق، می تواند حتی بیش از مهارت های پیشرفته فنی تعیین کننده باشد.

تحلیل Safe.exe

Safe.exe یک فایل اجرایی نوشته شده با زبان Go است که چهار فایل bat ایجاد می کند و سپس فرآیند باج گیری را شروع می کنند. در ادامه یک سرویس جدید برای اجرای safe.exe می سازد.

سپس سیستم را تنظیم می کند تا در بوت بعدی به حالت Safe Mode برود و به سرعت سیستم را خاموش می کند. وقتی سیستم دوباره بالا می آید، در حالت Safe Mode بدون شبکه قرار دارد.

<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

b93d633d379052f0a15b0f9c7094829461a86dbb

3160b4308dd9434ebb99e5747ec90d63722a640d329384b1ed536b59352dace6

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

x3.exe

1422dae0330c713935d50773680fcb39

d5a0c796032eda2fe20d1f39bae3fbc4e6407e8c

b9e4299239880961a88875e1265db0ec62a8c4ad6baf7a5de6f02ff4c31fadb1

<https://www.virustotal.com/gui/file/b9e4299239880961a88875e1265db0ec62a8c4ad6baf7a5de6f02ff4c31fadb1/details>

cplXen.exe

c9a728aa3f5b6f48b68df4bb66b41a5c

90035ab418033b39d584c7bc609cab1664460069





c305b75a4333c7fca9d1d71b660530cc98197b171856bf433e4e8f3af0424b11

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

116EBE27202905AFFB94F5C1597D511ABCB5B381411431956A03E47B388582BF.bat

1f7b17cacb0263b84cf3e9d4a5429ef9

14b2948a28d16c05fa7237dd8823592a735ef43f

116ebe27202905affb94f5c1597d511abcb5b381411431956a03e47b388582bf

2155A029A024A2FFA4EFF9108AC15C7DB527CA1C8F89CCFD94CC3A70B77CFC57.bat

6d9d31414ee2c175255b092440377a88

c24aee8fa0a81a82fe73bf60e0282b1038d6ea80

2155a029a024a2ffa4eff9108ac15c7db527ca1c8f89ccfd94cc3a70b77cfc57

3295F5029F9C9549A584FA13BC6C25520B4FF9A4B2FEB1D9E935CC9E4E0F0924.bat

3d33a19bb489dd5857b515882b43de12

0882f2e72f1ca4410fe8ae0fa1138800c3d1561d

3295f5029f9c9549a584fa13bc6c25520b4ff9a4b2feb1d9e935cc9e4e0f0924

251427C578EAA814F07037FBE6E388B3BC86ED3800D7887C9D24E7B94176E30D.bat

3e36d3dc132e3a076539acc9fcd5535c

89be35c19a65b9e6f7a277e1a9f66ab76d024378

251427c578eaa814f07037fbe6e388b3bc86ed3800d7887c9d24e7b94176e30d

safe.exe

2bbff2111232d73a93cd435300d0a07e

b93d633d379052f0a15b0f9c7094829461a86dbb





3160b4308dd9434ebb99e5747ec90d63722a640d329384b1ed536b59352dace6

6C9D8C577DDDF9CC480F330617E263A6EE4461651B4DEC1F7215BDA77DF911E7.bat

54fe4d49d7b4471104c897f187e07f91

18f963dbee830e64828991d26a06d058326c1ddb

6c9d8c577ddf9cc480f330617e263a6ee4461651b4dec1f7215bda77df911e7

A80C7FE1F88CF24AD4C55910A9F2189F1EEDAD25D7D0FD53DBFE6BDD68912A84.bat

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 = "b9e4299239880961a88875e1265db0ec62a8c4ad6baf7a5de6f02ff4c31fcdb1"  
  
  strings:  
  
    $s1 = "jd4ob7162ns.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
```





```
$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]Zlo" 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 = "spdelt" 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\"></requestedExecutionLevel></requeste" ascii
```

```
$s3 = "AppPolicyGetProcessTerminationMethod" fullword ascii
```

```
$s4 =
```

```
"hemas.microsoft.com/SMI/2005/WindowsSettings\">true</dpiAware></windowsSettings></application></assembly>" fullword ascii
```

```
$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=\"urn:schemas-microsoft-com:asm.v3" ascii
```

```
$s11 = "vileges<>/security></trustInfo><application xmlns=\"urn:schemas-microsoft-com:asm.v3\"><windowsSettings><dpiAware xmlns=\"http://" ascii
```

```
$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 = ">6?V?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-config, or --key-expiration) in NT s" ascii
    $x2 = "Unsupported command (--list-fingerprint, --hash-password, --keygen, --dump-config,
--verify-config, or --key-expiration) in NT s" ascii
    $x3 = "Tor is currently configured as a relay and a hidden service. That's not very secure: you
should probably run your hidden service" ascii
    $x4 = "Failed to open handle to monitored process %d, and error code %lu (%s) is not
'invalid parameter' -- assuming the process is sti" ascii
    $x5 = "Failed to open handle to monitored process %d, and error code %lu (%s) is not
'invalid parameter' -- assuming the process is sti" ascii
    $x6 = "Unable to parse descriptor of type %s with hash %s and length %lu. Descriptor not
dumped because it exceeds maximum log size all" ascii
    $x7 = "Unable to parse descriptor of type %s with hash %s and length %lu. Descriptor not
dumped because it exceeds maximum log size all" ascii
    $s8 = "Doesn't look like we'll be able to create descriptor dump directory %s; dumps
will be disabled." fullword ascii
    $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)." fullword ascii

\$s12 = "Unable to parse descriptor of type %s with hash %s and length %lu. Descriptor not
dumped because the sandbox is configured" fullword ascii

\$s13 = "You are running a new relay. Thanks for helping the Tor network! If you wish to
know what will happen in the upcoming weeks rega" ascii

\$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'. Malformed hidden service descriptor?" fullword ascii

\$s16 = "Uploading hidden service descriptor: http status %d (%s) response unexpected
(server '%s:%d')." fullword ascii

\$s17 = "Your server (%s:%d) has not managed to confirm that its DirPort is reachable. Relays
do not publish descriptors until their ORPo" ascii

\$s18 = "Your server (%s:%d) has not managed to confirm that its ORPort is reachable. Relays
do not publish descriptors until their ORPor" ascii

\$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 overlapcrypto/des: invalid buffer" ascii
```

```
$x2 = "> (den<<shift)/2unexpected end of JSON inputunexpected protocol version cannot be converted to type %s(%s) - handshake failed: " ascii
```

```
$x3 = "sync: WaitGroup misuse: Add called concurrently with Waittls: Ed25519 public keys are not supported before TLS 1.2tls: peer does" ascii
```

```
$x4 = "slice bounds out of range [:%x] with length %ystopTheWorld: not stopped (status != _Pgcstop)tls: ECDSA signing requires a ECDSA " ascii
```

```
$x5 = "Pakistan Standard TimeParaguay Standard TimePrint version and exitSakhalin Standard TimeTOR_PT_SERVER_BINDADDRTasmania Standard " ascii
```

```
$x6 = "0123456789ABCDEFGHIJKLMNQRSTUUV28421709430404007434844970703125: day-of-year does not match dayABCDEFGHIJKLMNQRSTUUVWXYZ234567" ascii
```

```
$x7 = "unknown network workbuf is emptywww-authenticate initialHeapLive= sp  
inningthreads=%%!%c(big.Int=%s)0123456789ABCDEFX0123456789ab" ascii
```

```
$x8 = "unixpacketunknown pcuser-agentws2_32.dll of size (targetpc= ErrCode=%v [scrubbed] a.npages= b.npages= gcwaiting= gp.status=" ascii
```

```
$x9 = "attempt to execute system stack code on user stackcrypto/cipher: incorrect nonce length given to GCMcryptobyte: attempted write " ascii
```

```
$x10 = "streamSafe was not resetstructure needs cleaningtext/html; charset=utf-8unexpected buffer len=%vunexpected exponent baseunexpected" ascii
```

```
$x11 = "100-continue152587890625762939453125:key_extractBidi_ControlCIDR addressCONTINUATIONContent TypeContent-TypeECDSA-SHA256ECDSA-SH" ascii
```

```
$x12 = "IP addressKeep-AliveKharoshthiLockFileExManichaeenMessage-IdNo ContentOld_ItalicOld_PermicOld_TurkicOther_MathPOSTALCODEParseFlo" ascii
```

```
$x13 = "tls: ECDSA signature contained zero or negative values  
tls: client indicated early data in second ClientHello  
tls: failed to creat" ascii
```

```
$x14 = "to unallocated span%!%c(*big.Float=%s)37252902984619140625Arabic Standard TimeAzores Standard TimeBUG: Failed HKDF: %sCertOpenS" ascii
```

```
$x15 = "CertEnumCertificatesInStoreDATA frame with stream ID 0Easter Island Standard TimeG waiting list is corruptedTOR_PT_EXTENDED_SERV" ascii
```





```
$x16 = ".lib section in a.out
corrupted11368683772161602973937988281255684341886080801486968994140625CLIENT_
HANDSHAKE_TRAFFIC_SECRETCent" ascii

$x17 = "Saint Pierre Standard TimeSouth Africa Standard
TimeTOR_PT_EXIT_ON_STDIN_CLOSEW. Australia Standard TimeWest Pacific Standard Ti" ascii

$x18 = "Temporary
RedirectUNKNOWN_SETTING_%dVariation_Selectorajax.aspnetcdn.combad Content-
Lengthbad manualFreeListbufio: buffer fullco" ascii

$x19 = "request rejected because the client program and identd report different user-idstls:
either ServerName or InsecureSkipVerify mus" ascii

$x20 = "invalid network interface nameinvalid pointer found on stacklooking for beginning
of valuemeeek_lite: protocol negotiatedmime: du" ascii

condition:
uint16(0) == 0x5a4d and filesize < 26000KB and
( pe.imphash() == "f0070935b15a909b9dc00be7997e6112" or 1 of ($x*) )
}
```

منبع:

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

