



Operation LagTime IT: Colorful Panda Footprint

Virus Bulletin 2020 localhost

Sept 30 - Oct 2, 2020

Fumio Ozawa, Shogo Hayashi, Rintaro Koike



Fumio Ozawa

- SOC & malware analyst at NTT Security (Japan) KK
- Speaker at Japan Security Analyst Conference 2018

Shogo Hayashi

- SOC & malware analyst at NTT Security (Japan) KK
- Responding to EDR detections and creating IoCs
- Co-founder at SOCYETI

Rintaro Koike

- SOC & malware analyst at NTT Security (Japan) KK
- Founder & researcher at nao_sec

Introduction

TA428

- Chinese APT attack group
- Mainly targeting East Asian countries
- Recent operation : "LagTime IT"

Operation LagTime IT

- Attack campaign by TA428 since around March 2019
- Targeting East Asian governmental organizations
- Using Royal Road RTF Weaponizer, Poison Ivy and Cotx RAT

Operation LagTime IT by TA428 is an attack campaign

- Targeting governmental organization of East Asian countries
- Still in place and actively working as of 2020

The existing research deals with only the initial stages

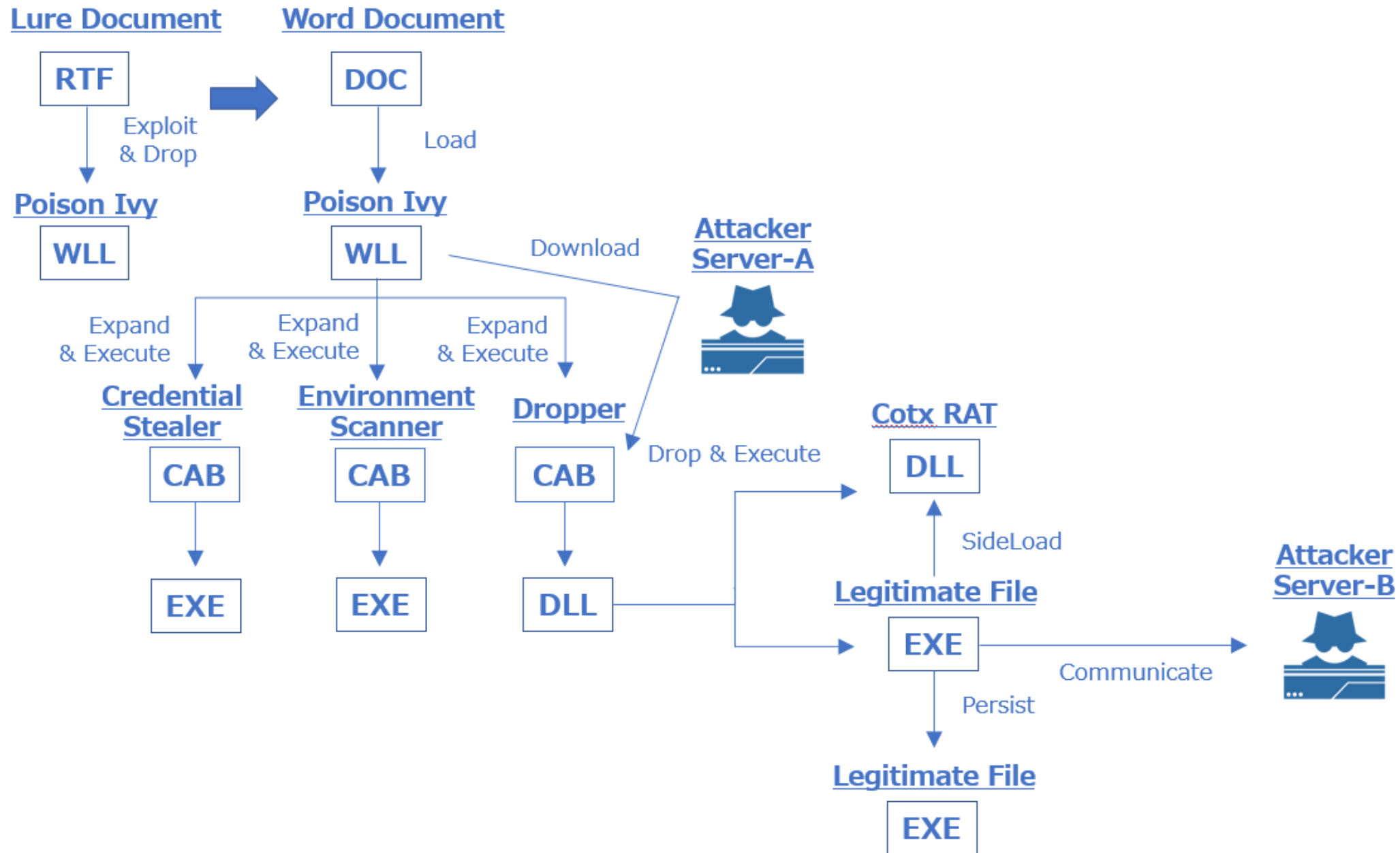
- Royal Road RTF Weaponizer, Poison Ivy and Cotx RAT
- Followed by complex attack with more malwares

We succeeded in observing the subsequent attacks

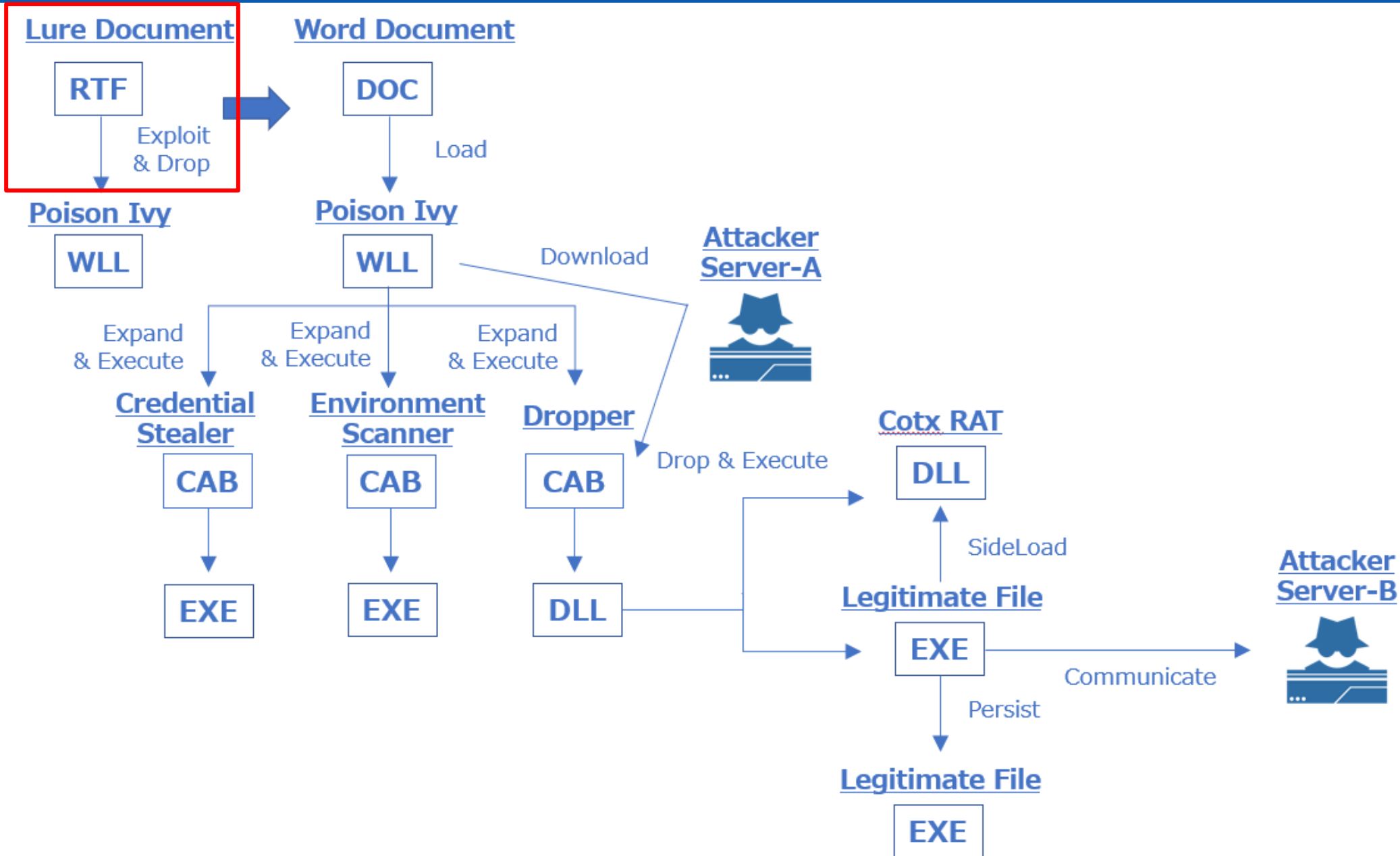
- Lateral movement
- Unknown malwares

Case 1

Attack Flow Case 1



Attack Flow Case 1



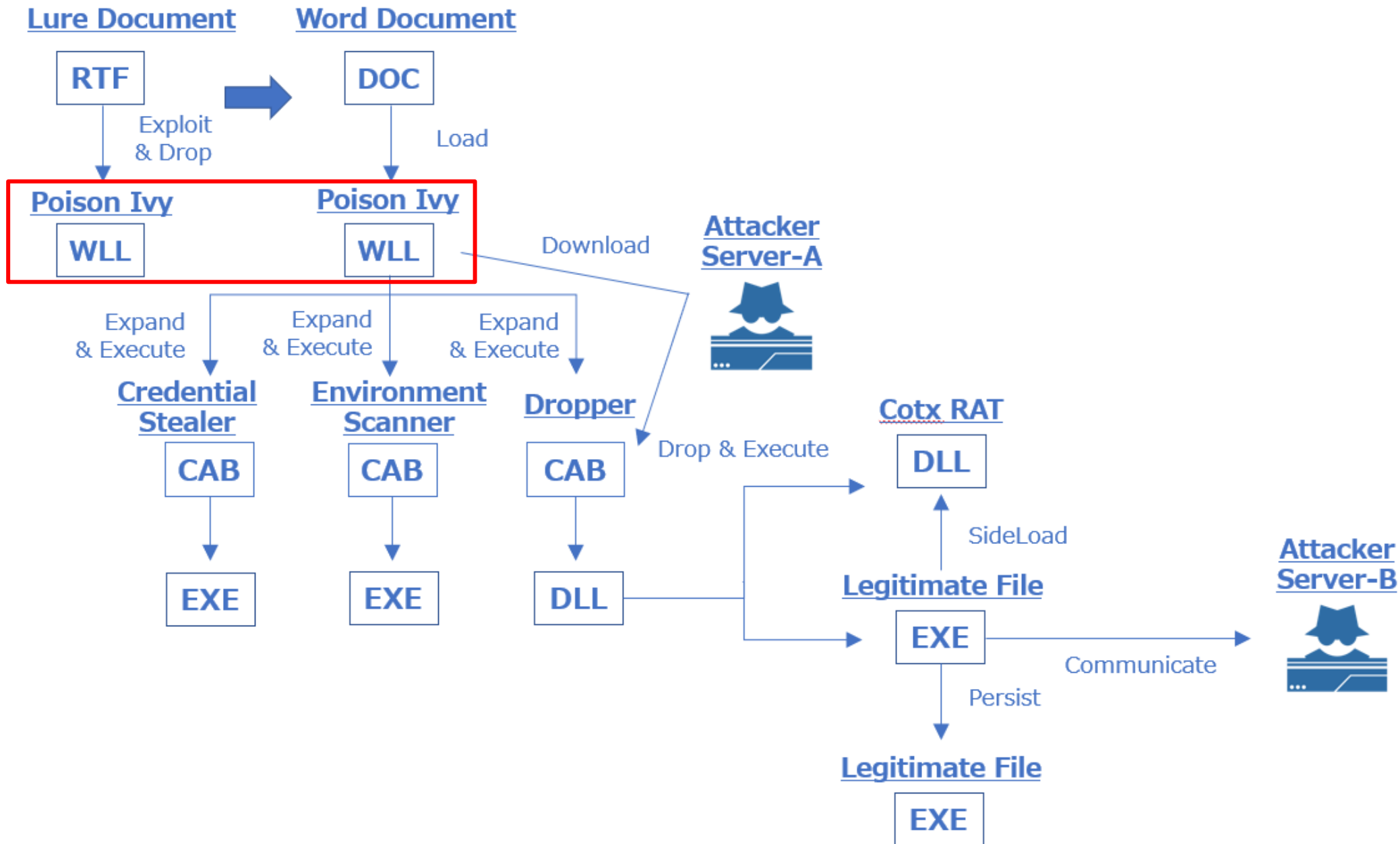
The lure document file is an RTF file

- Generated by Royal Road RTF Weaponizer
 - Exploits CVE-2018-0798
 - Executes 2byte-XOR-encoded shellcode
 - Decodes "8.t" object and writes to ".wll" file

```
0x0000006e    inc    edx
0x00000070    pop    rdi
0x00000071    add    edi, 0x1a
0x00000074    xor    ecx, ecx
0x00000076    mov    cx, 0x8ba
0x0000007a    cmp    word [rdi], 0
0x0000007e    je     0x85
0x00000080    xor    word [rdi], 0xc390
0x00000085    loop  0x7a
0x00000089    jns   0xad
0x0000008b    xchg  eax, edx
0x0000008c    ret
```

```
0x00000453    mov    eax, 0x48b53a6c
0x00000458    xor    edx, edx
0x0000045a    test   ebx, ebx
0x0000045c    jle   0x48e
0x0000045e    mov    esi, ebx
0x00000460    push  7
0x00000462    pop    rbx
0x00000463    mov    ecx, eax
0x00000465    shr   ecx, 0x1a
0x00000468    xor   ecx, eax
0x0000046a    shr   ecx, 3
0x0000046d    xor   ecx, eax
0x0000046f    add   eax, eax
0x00000471    and   ecx, 1
0x00000474    or    eax, ecx
0x00000476    jne   0x463
0x0000047a    mov   ecx, dword [rbp - 0xc]
0x0000047d    xor   byte [rdx + rcx], al
0x00000480    cmp   edx, esi
0x00000483    jl    0x460
0x00000485    mov   ebx, dword [rbp - 4]
0x00000488    lea  esi, [rdi + 0x2a5]
0x0000048e    xor   eax, eax
```

Attack Flow Case 1



The RAT has long been used by Chinese APT groups

Startup Sequence

- The Poison Ivy "useless.wll" placed in the Microsoft Word startup directory is automatically loaded and executed when Microsoft Word is started.
 - %APPDATA%\Microsoft\Word\STARTUP\useless.wll
- If command line string contains "WORD.EXE", the useless.wll runs the following command that calls function implemented on itself.
 - rundll32.exe %APPDATA%\Microsoft\Word\STARTUP\useless.wll,DllEntry10
- Function DllEntry10 decodes certain data with XOR and RC4 to restore main backdoor program and executes it.

Configuration

Decoded configuration data

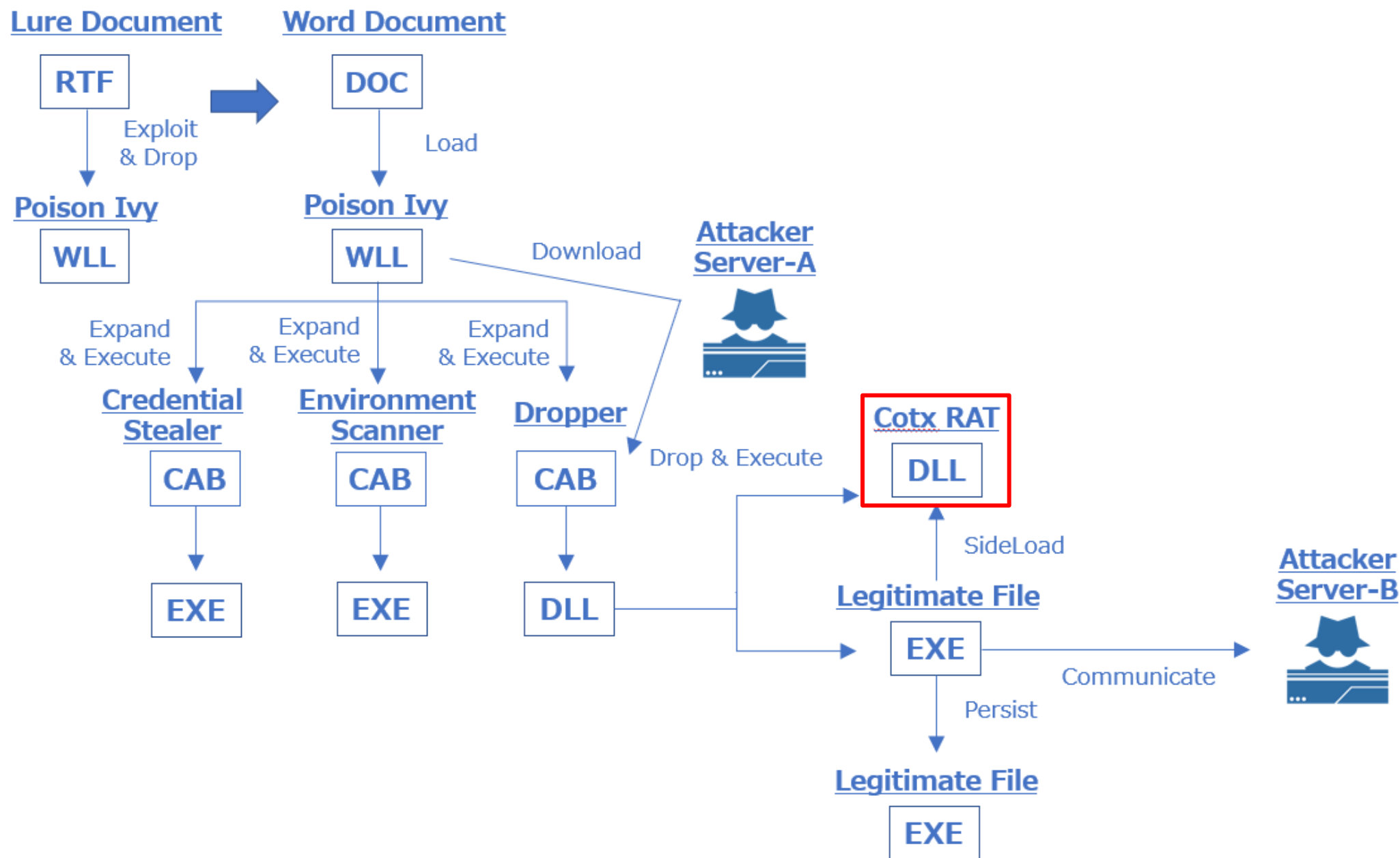
Item	Value
C&C Server	95[.]179.131.29:443
	95[.]179.131.29:8080
Campaign ID	hold
Group ID	hold
Mutex	99x7nmpWW
C&C Traffic Encryption Key (Camellia-256 in ECB mode)	3&U<9f*IZ>!MIQ

C&C Communication

- Same characteristics with the traffic generated by "SPIVY", Poison Ivy variant
 - <https://unit42.paloaltonetworks.com/unit42-new-poison-ivy-rat-variant-targets-hong-kong-pro-democracy-activists/>

Offset	Padding size	Padding data (random)	Padding end (size*2)	Encoded data
00000000	0b	f0 45 be 43 6a 89 34	22 9e 4e 55 16	27 a7 1c ..E.Cj.4 ".NU.'..
00000010	66 6a e4 41 1d 11 cf 7a	7a 7a ba db 86 bf a1 ad	fj.A...z zz.....	
00000020	61 c3 bb 1a 3e 4d 15 68	03 27 ba d1 68 9c 1d 11	a...>M.h .'..h...	
00000030	57 73 03 7c 22 7a 17 e4	ee 21 a4 e3 7f e3 74 66	Ws. "z.. !....tf	
00000040	87 f2 a9 b6 e1 c8 a8 29	a2 a4 6e cc ad 6c 43 8c) ..n..lC.	
00000050	19 bc 5e 34 96 7c 61 93	ba f8 40 8f 99 c2 62 c9	..^4. a. ..@...b.	
00000060	bf 5b ef ea 7b c9 8f 46	ec 6c 73 44 56 cd 1c 45	.[...{..F .lSDV..E	
00000070	87 25 38 14 0a b0 ab d2	39 f7 e3 4c 9a 1d 89 3a	.%8..... 9..L...:	
00000080	a5 78 42 a1 75 6c cf 99	26 3c 14 c3 7e e8 16 87	.xB.ul.. &<...~...	
00000090	11 e2 12 cb e8 b2 fc 04	95 65 46 b4 90 9b 07 f2eF.....	
000000A0	2b a8 2a 78 cb 07 3e 10	ad 9d 58 cd 42 74 d6 9f	+.*x...>. ..X.Bt..	
000000B0	8b 30 e5 fc 7f a8 a0 f4	d9 89 04 a3 c9 03 0d 13	.0.....	
000000C0	b8 1d 74 2e 82 d2 7d 86	f7 66 c2 e7 54 79 81 b4	..t...}. .f..Ty..	
000000D0	45 d8 80 b3 07 84 28 df	99 1c e3 19 2c aa f7 04	E.....(.,...	
000000E0	d3 f5 3d ca e2 6c e2 ee	0b f5 aa 1f 33 6b 5d cb	..=..l..3k].	
000000F0	f9 79 e0 50 0d b9 b8 63	3c 0b c8 07 28 ec f7 a4	.y.P...c <...(...	
00000100	ce 5f 2a d2 c6 7b 01 aa	1c bd 30 a7 22	._*...{.. ..0."	

Attack Flow Case 1



The original RAT used by TA428

Behavior

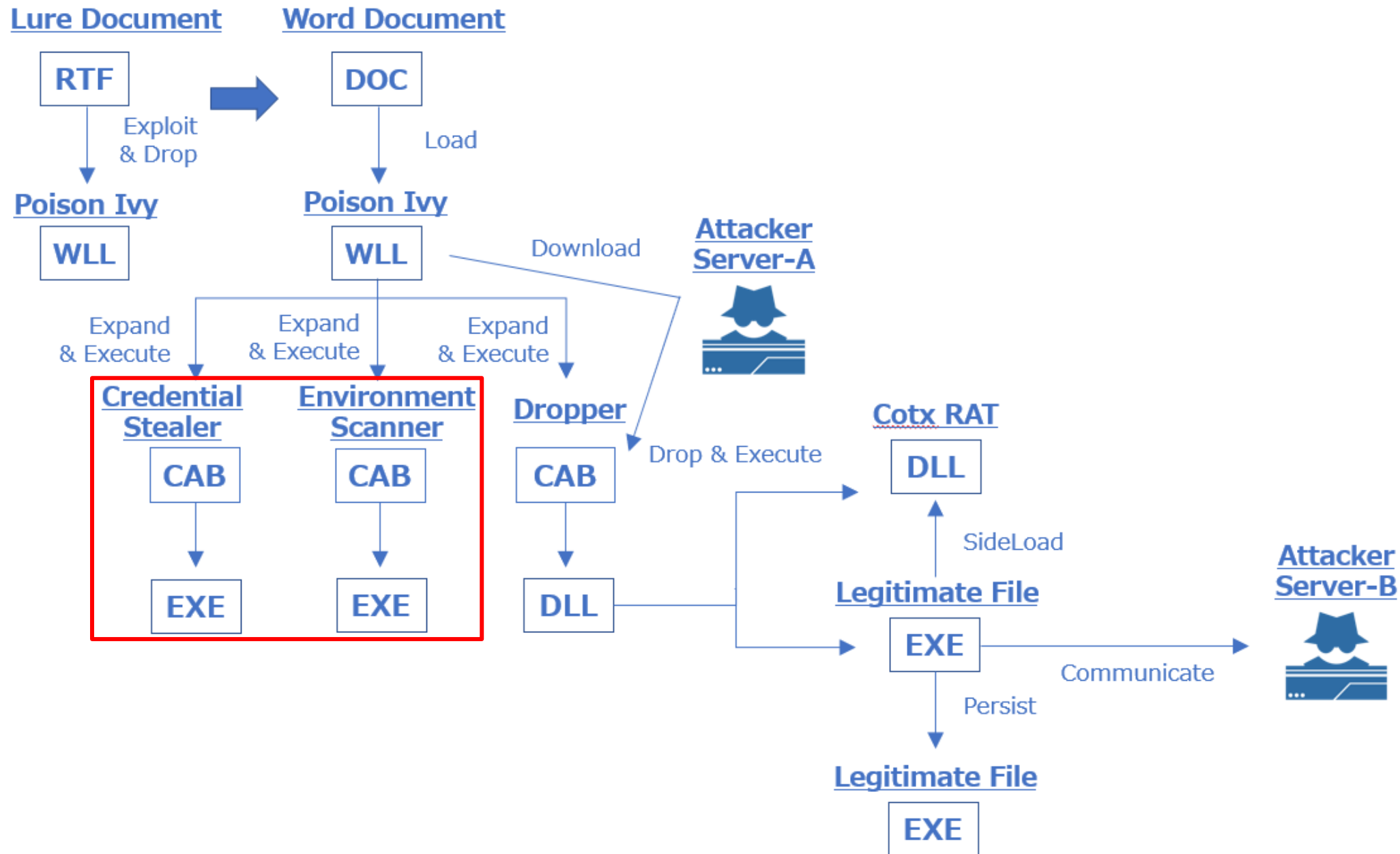
- Basically same characteristics as reported in the Proofpoint's blog
 - <https://www.proofpoint.com/us/threat-insight/post/chinese-apt-operation-lagtime-it-targets-government-information-technology>

Configuration

Decoded configuration data

Item	Value
C&C Server	mtanews.vzglagtime[.]net:443
"mark" field in the C&C beacon	1011_15
"passwd" field in the C&C beacon	P@SSaw1

Attack Flow Case 1



Outlook Password Dump v3.0

- Outlook Password Recovery Tool (The latest version is a commercial tool)
 - <https://securityxploded.com/outlook-password-dump.php>

```
$ o.exe

*****

Outlook Password Dump v3.0 by SecurityXploded

http://securityxploded.com/outlook-password-dump.php

*****

Email Address           Username           Password           Account Type       Email Server
=====
```

nbtscan 1.0.35

- NETBIOS nameserver scanner (public tool)
 - <http://www.unixwiz.net/tools/nbtscan.html>

```
$ n.exe
nbtscan 1.0.35 - 2008-04-08 - http://www.unixwiz.net/tools/

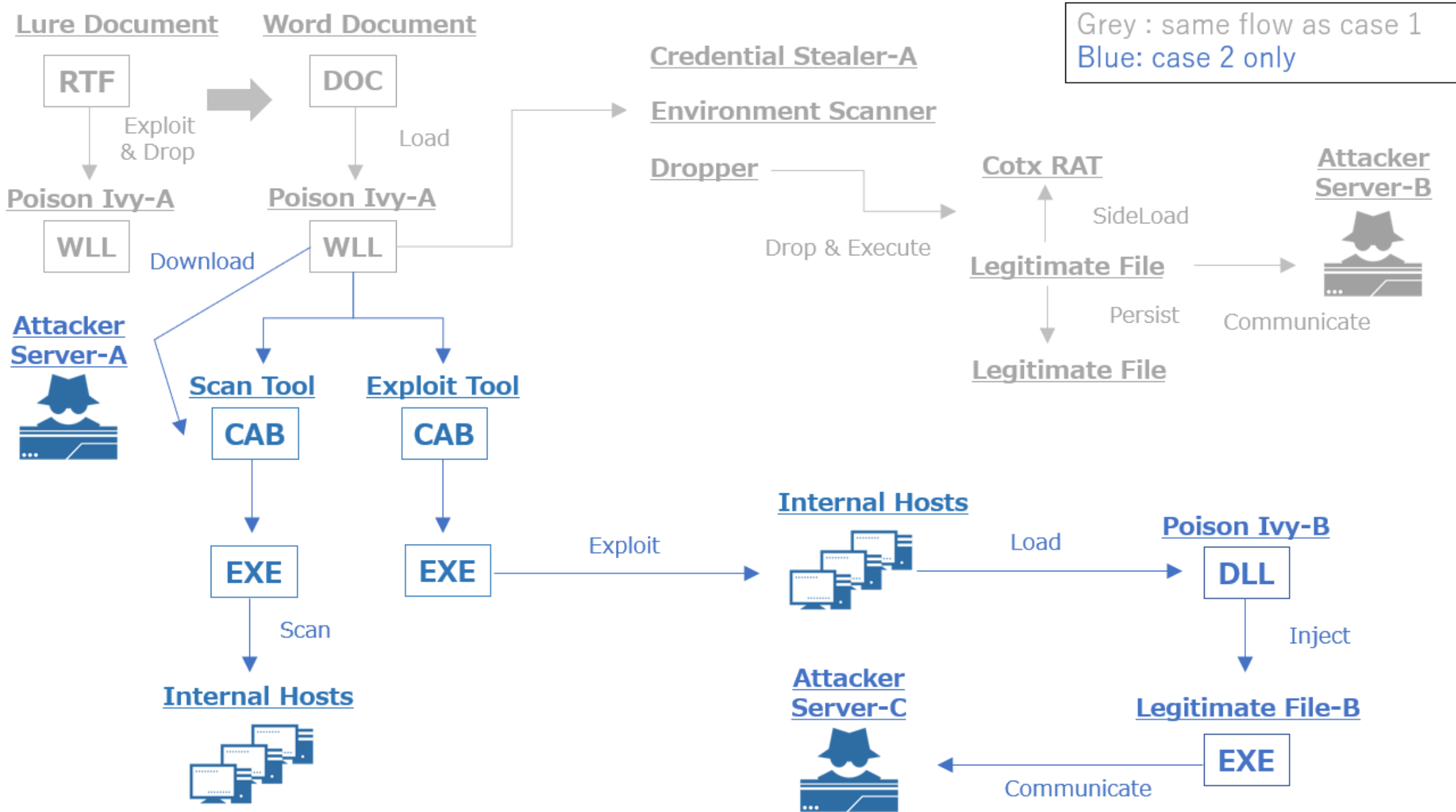
usage: n.exe [options] target [targets...]

Targets are lists of IP addresses, DNS names, or address
ranges. Ranges can be in /nbits notation ("192.168.12.0/24")
or with a range in the last octet ("192.168.12.64-97")

-V          show Version information
-f          show Full NBT resource record responses (recommended)
-H          generate HTTP headers
-v          turn on more Verbose debugging
-n          No looking up inverse names of IP addresses responding
-p <n>      bind to UDP Port <n> (default=0)
-m          include MAC address in response (implied by '-f')
-T <n>      Timeout the no-responses in <n> seconds (default=2 secs)
-w <n>      Wait <n> msecs after each write (default=10 ms)
-t <n>      Try each address <n> tries (default=1)
-l          Use Winsock 1 only
-P          generate results in perl hashref format
```

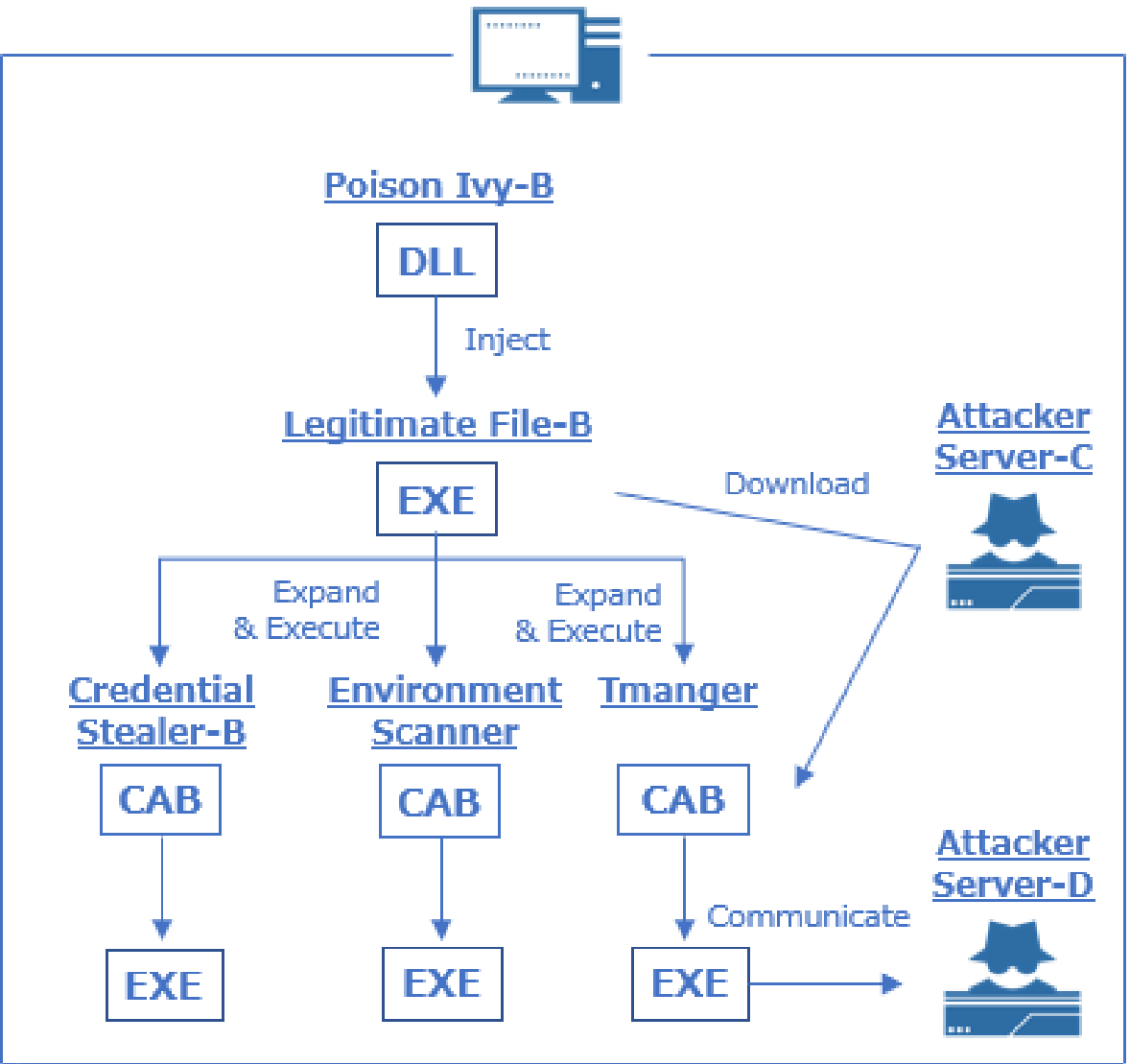
Case 2

Attack Flow Case 2

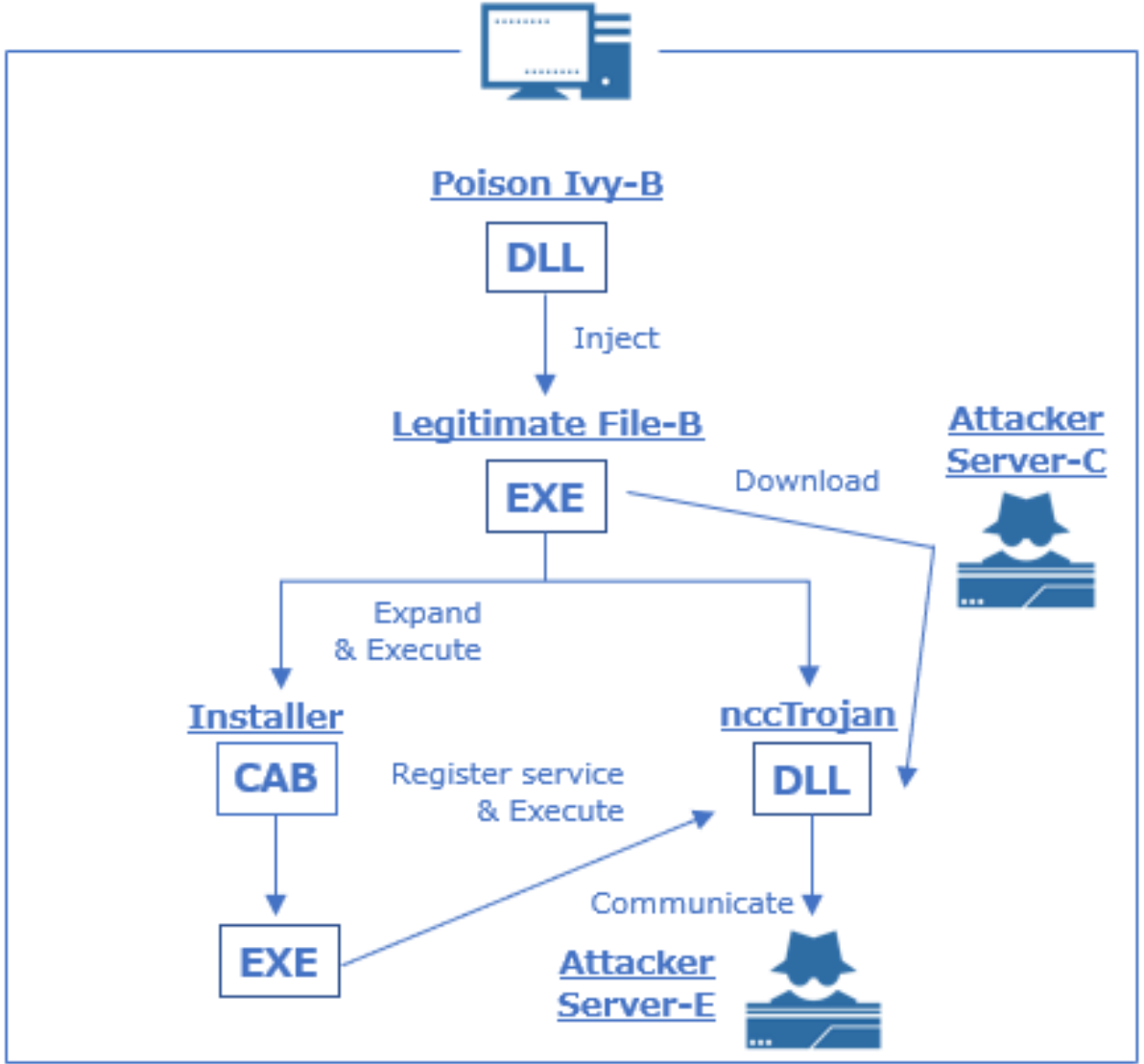


Attack Flow Case 2

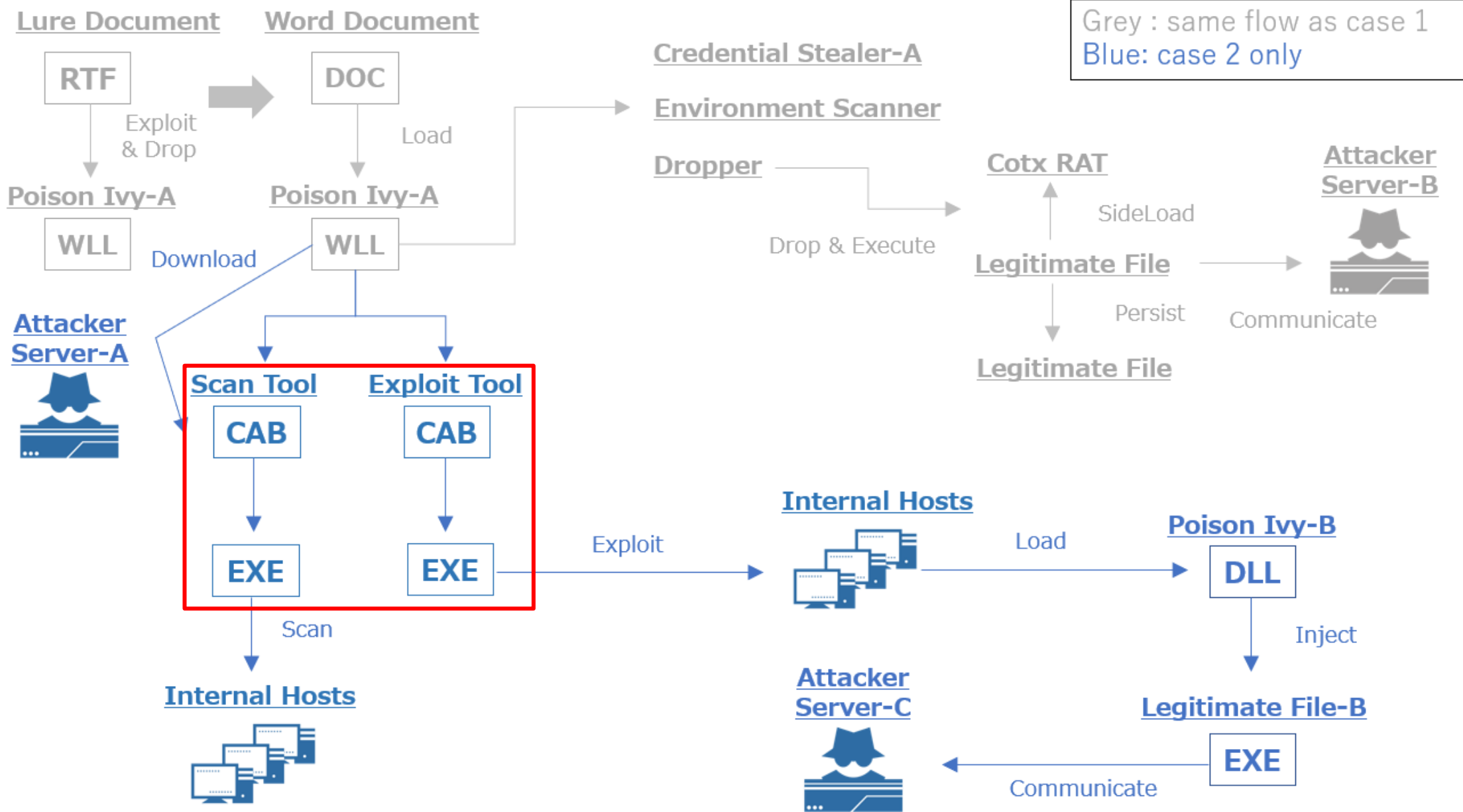
Internal Host-A



Internal Host-B



Attack Flow Case 2



Exploit Tool for MS17-010

- eternalblue.py

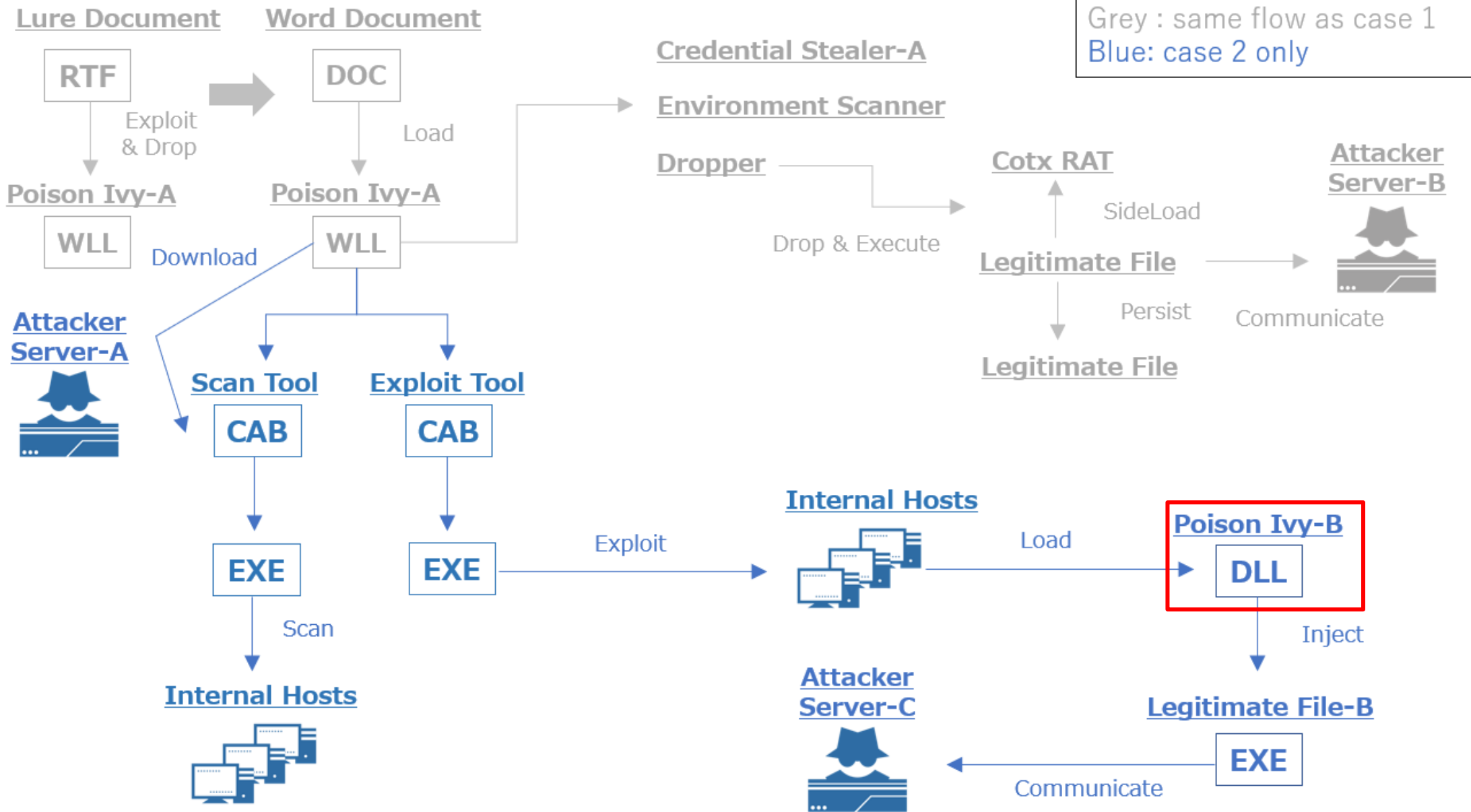
- <https://github.com/pythonone/MS17-010/blob/master/exploits/eternalblue/eternalblue.py>

```
$ w.exe
[1]-----check backdoor and system version-----
get_smb_signature 59437391
**** OS is Win 7 x86
**** backdoor is already installed!
[2]-----Inject dll -----
get_smb_signature 59437391
key 23f5a57b
dll_hex 200704
len_part: 204144
0 ----> 0x52
1 ----> 0x52
2 ----> 0x52

-- Snip --

49 ----> 0x52
50 ----> 0x52
**** dll is now injected!
```


Attack Flow Case 2



Startup Sequence

- Either one of the following DLL file (the Poison Ivy-B) is injected into lsass.exe on remote host by the MS17-010 exploiting tool and executed.
 - x86.dll: for 32bit environment
 - x64.dll: for 64bit environment
- The DLL file drops the following three files and executes PotPlayerMini.exe.
 - PotPlayerMini.exe: signed legitimate program
 - PotPlayer.dll: malware
 - PAME13.tmp: encoded configuration data
- The PotPlayerMini.exe loads PotPlayer.dll, and the PotPlayer.dll decodes PAME13.tmp to get configuration data and starts working as a RAT.

Configuration

Decoded configuration data

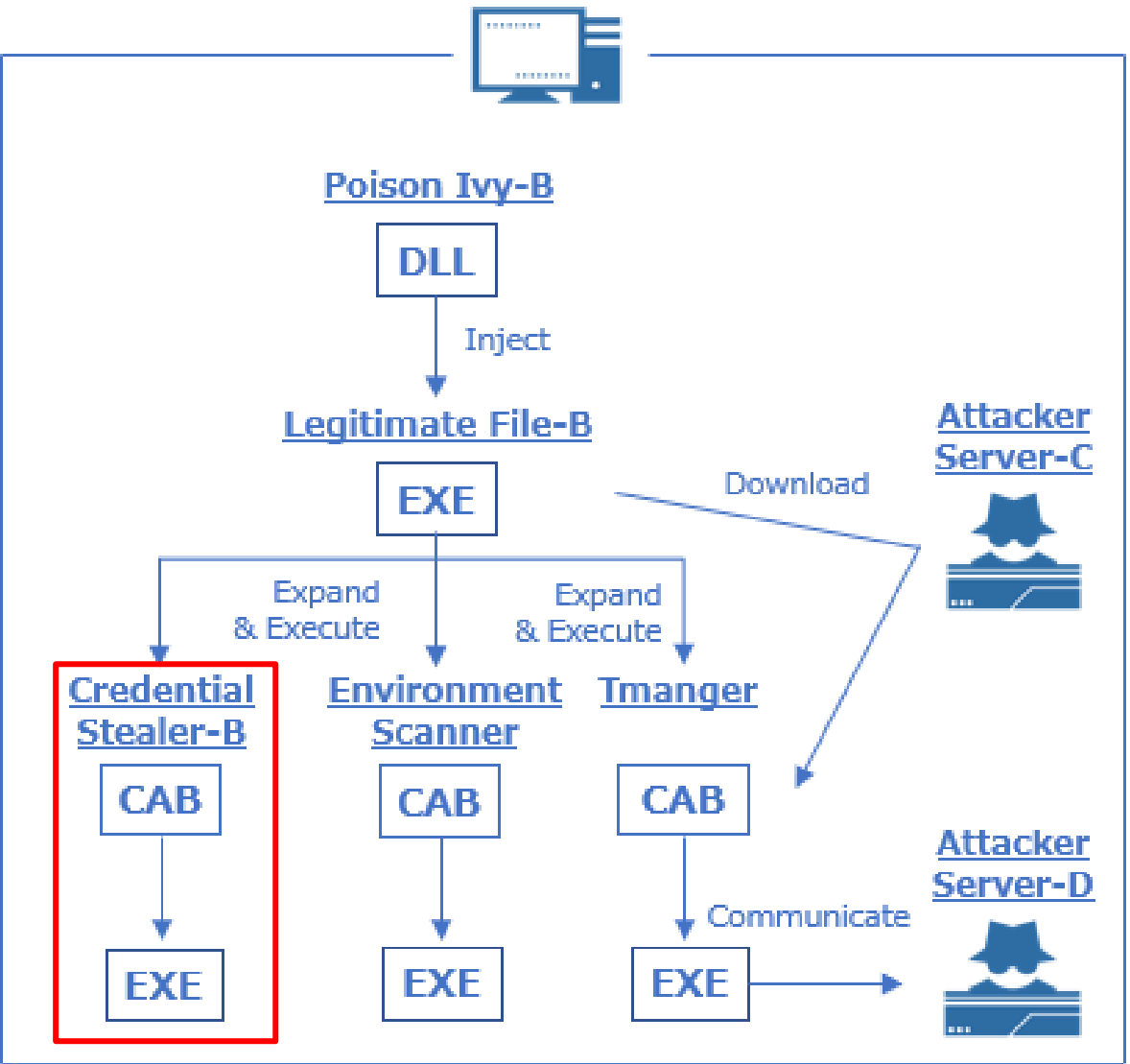
Item	Value
C&C Server	45[.]76.211.18:443
	45[.]76.211.18:8080
Campaign ID	TOEI
Group ID	TOEI
Mutex	G9u3cUoJs
C&C Traffic Encryption Key (Camellia-256 in ECB mode)	kos@On

C&C Communication

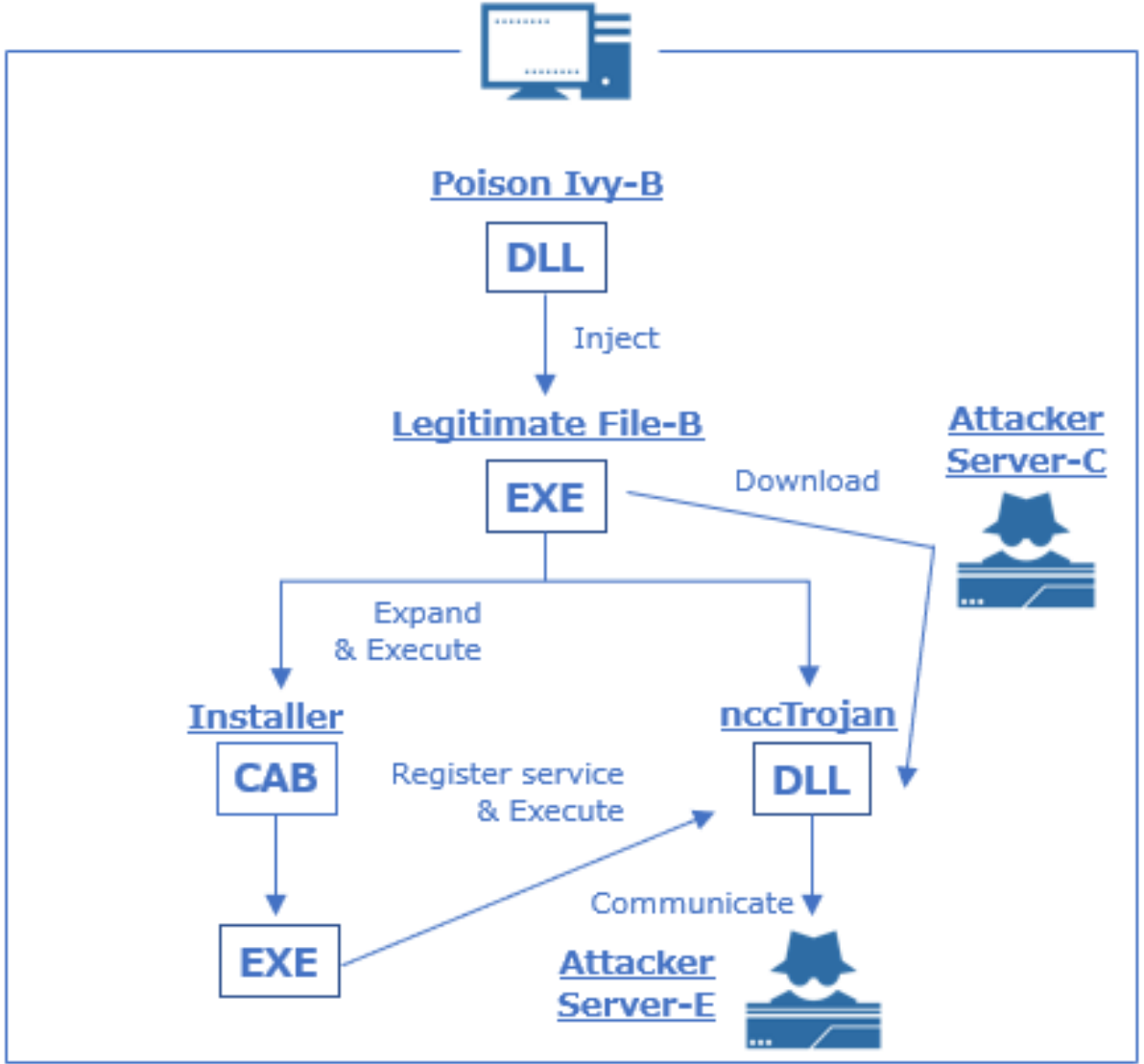
- Same characteristics with traffic by the Poison Ivy in Case 1

Attack Flow Case 2

Internal Host-A



Internal Host-B



show.exe

- Windows Credential Stealer (Original Tool)
 - Steal usernames, domain names and passwords from lsass.exe process.

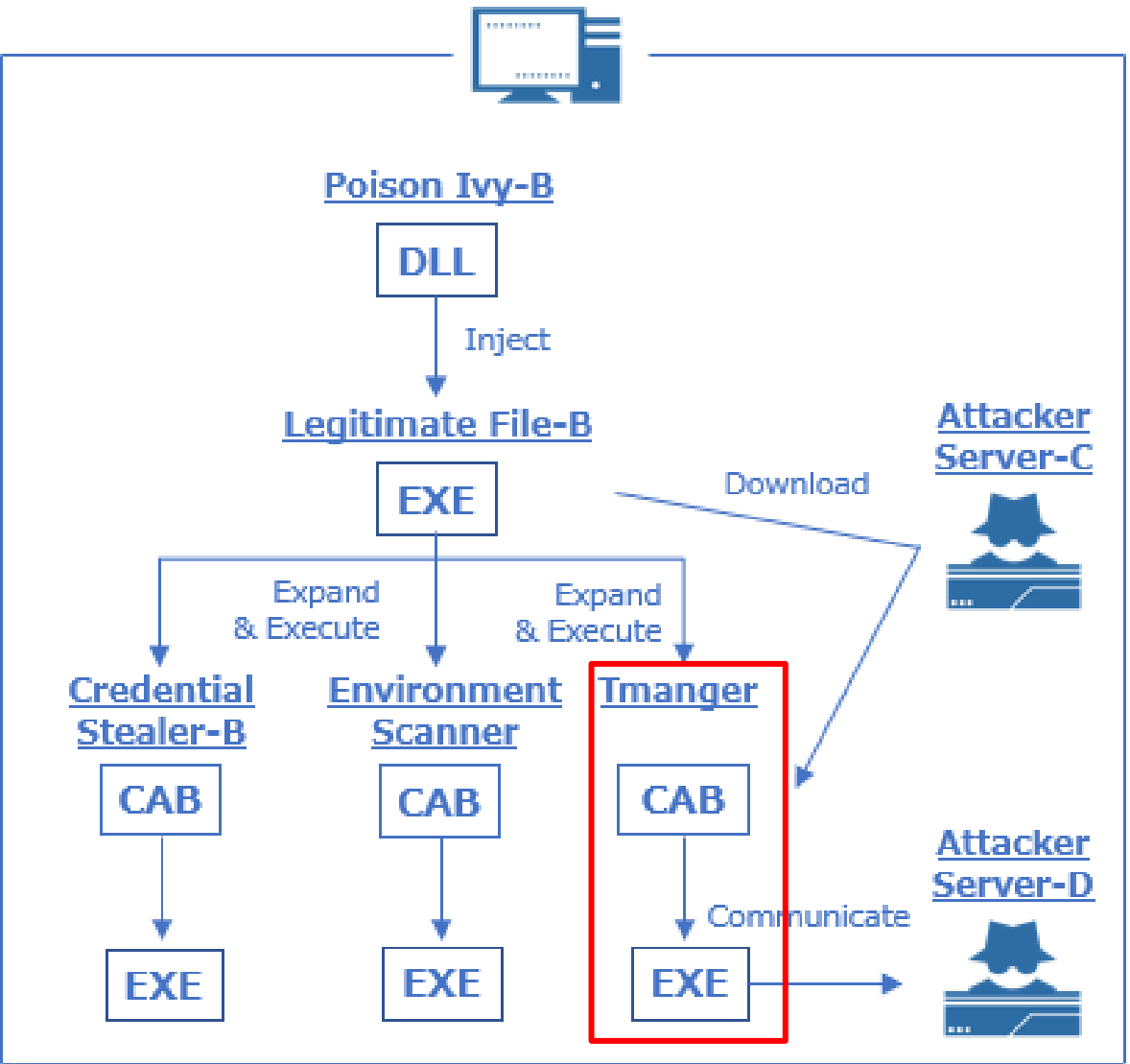
```
$ show.exe
U: Administrator
DO: [Reducted]
ps: [Reducted]

U: ANONYMOUS LOGON
DO: NT AUTHORITY
Specific LUID NOT found

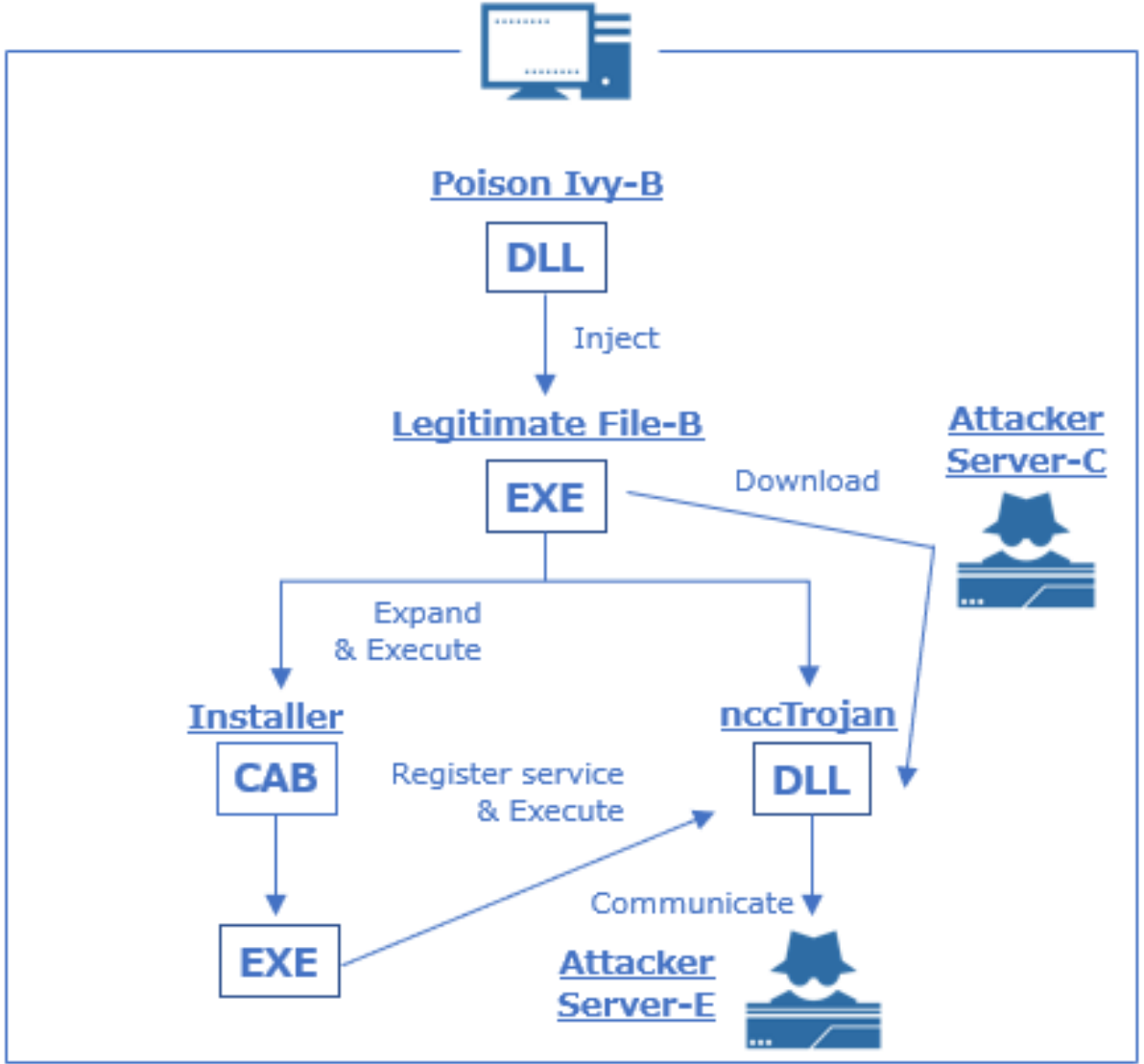
U: LOCAL SERVICE
DO: NT AUTHORITY
ps:
```

Attack Flow Case 2

Internal Host-A



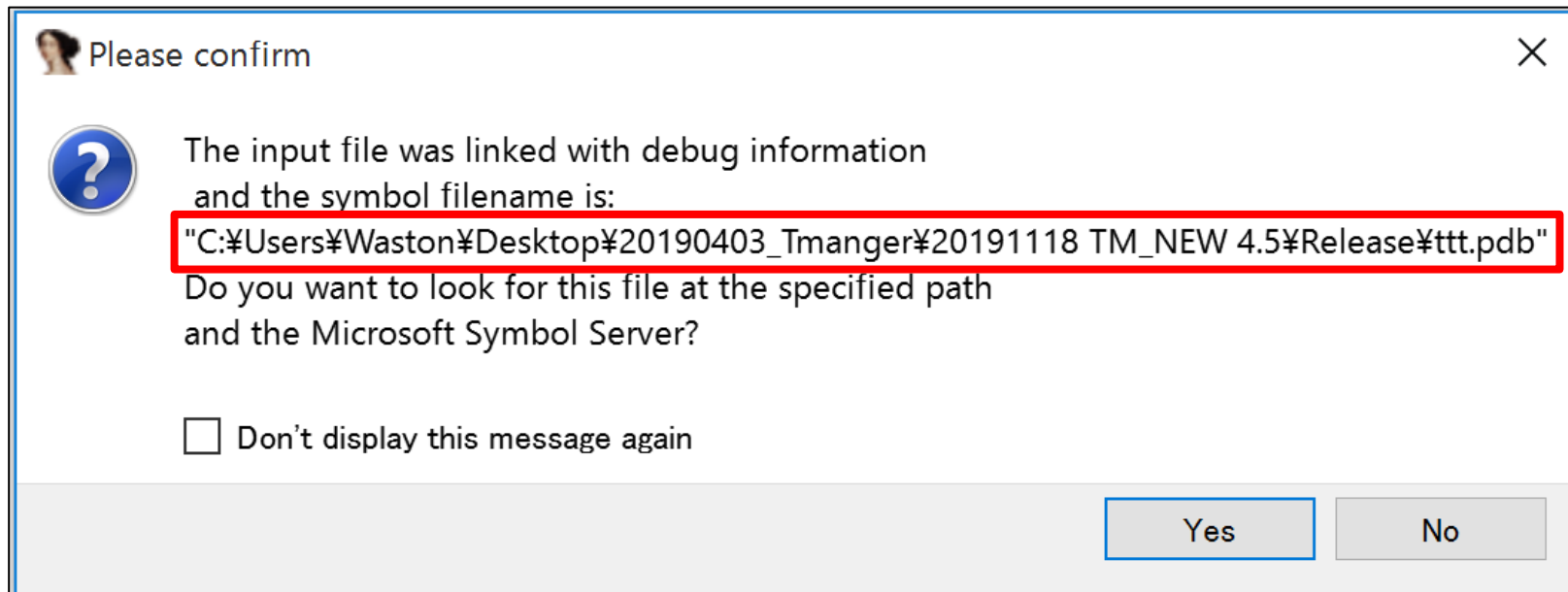
Internal Host-B



Evidence

- PDB File Path

- Found string "Tmanger" in directory name that would represent this RAT



Startup Sequence and Persistence

- Tmanger "dwm.exe" is placed and executed by Poison Ivy-B.
- dwm.exe drops test.dll by extracting data from its resource section and expands it.
 - %Temp%\test.dll
- The dwm.exe drops master.exe by copying itself.
 - %Temp%\master.exe
- The dwm.exe executes the following command.
 - rundll32.exe %Temp%\test.dll,Entry
- The test.dll creates the following registry key and starts working as a RAT.

The registry key (Persistence)

Key	Value
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Master	%Temp%\master.exe

Configuration

- Three destinations with the same IP address but different port numbers
- If the first port is unable, Tmanger tries to connect to the second port.

The decoded configuration data

Item	Value
C&C Server	172[.]105.39.67:80
	172[.]105.39.67:443
	172[.]105.39.67:5222

C&C Communication

- TCP Payload

- Data Size (4 Bytes) + Encrypted Data

	Data Size	Encrypted Data	
00000000	15 00 00 00	1b f5 42 5a 9e 55 92 03 7a 0e b8 b6BZ .U..z...
00000010		f8 8c 36 19 12 9e 54 62 56	..6...Tb V

- Encryption

- Algorithm: RC4
- Key (512 bits):

アドレス	Hex	ASCII
0093C970	00 0C 7C 17 A7 1C D2 07 DA 9E EE C5 8B 0B D7 86	.. .§.ò.ú.îÀ..x.
0093C980	AB 7E 5E 1C 55 C5 6E 2E 75 10 A0 FC C2 C8 7A 99	«~^.UÀn.u. üÅÈZ.
0093C990	DB 6C 5C B5 2A C6 32 EE 03 C5 4C A4 4D 0A 20 24	0T\μ*Æ2î.ÀL♠M. \$
0093C9A0	92 CD D9 CB 8C 89 81 80 A5 90 D1 AF 02 B6 5F 15	.íÙÈ....¥.Ñ¯.¶_.

C&C Communication

- Decrypted Data

- Encoded PID (4 Bytes) + Command (1 Byte) + Content

```
          Encoded PID  Command
00000000  33 35 34 38 01 80 be 39 00 73 79 73 74 65 6d 69 |3548...9.systemi|
00000010  6e 66 6f 0d 0a                                     |nfo..|
00000015
```

- Encoded PID

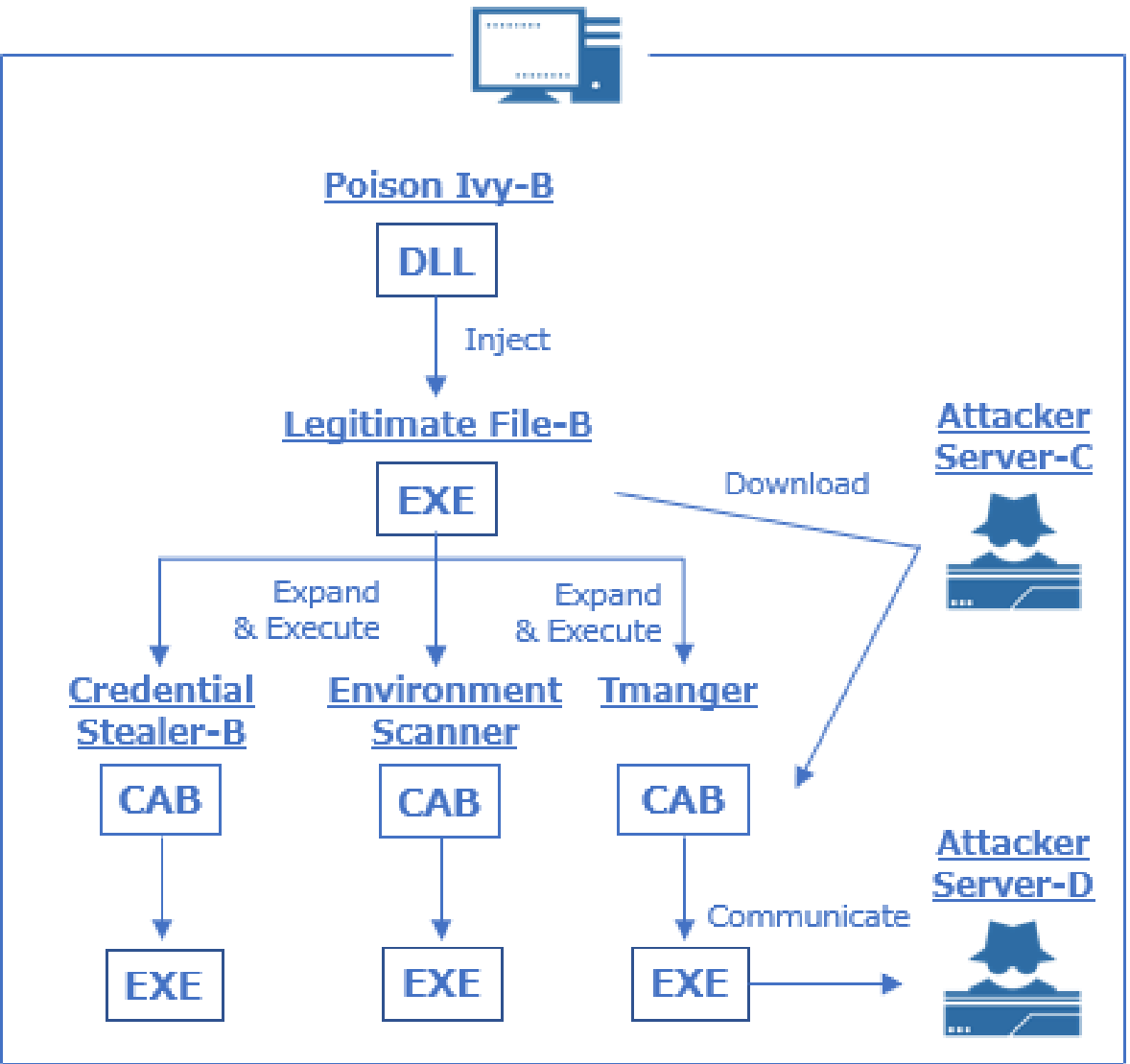
$$\text{Encoded PID} = ((\text{PID} \% 9) \times 1000) + ((\text{PID} \% 1000) + 1000)$$

Command and Control

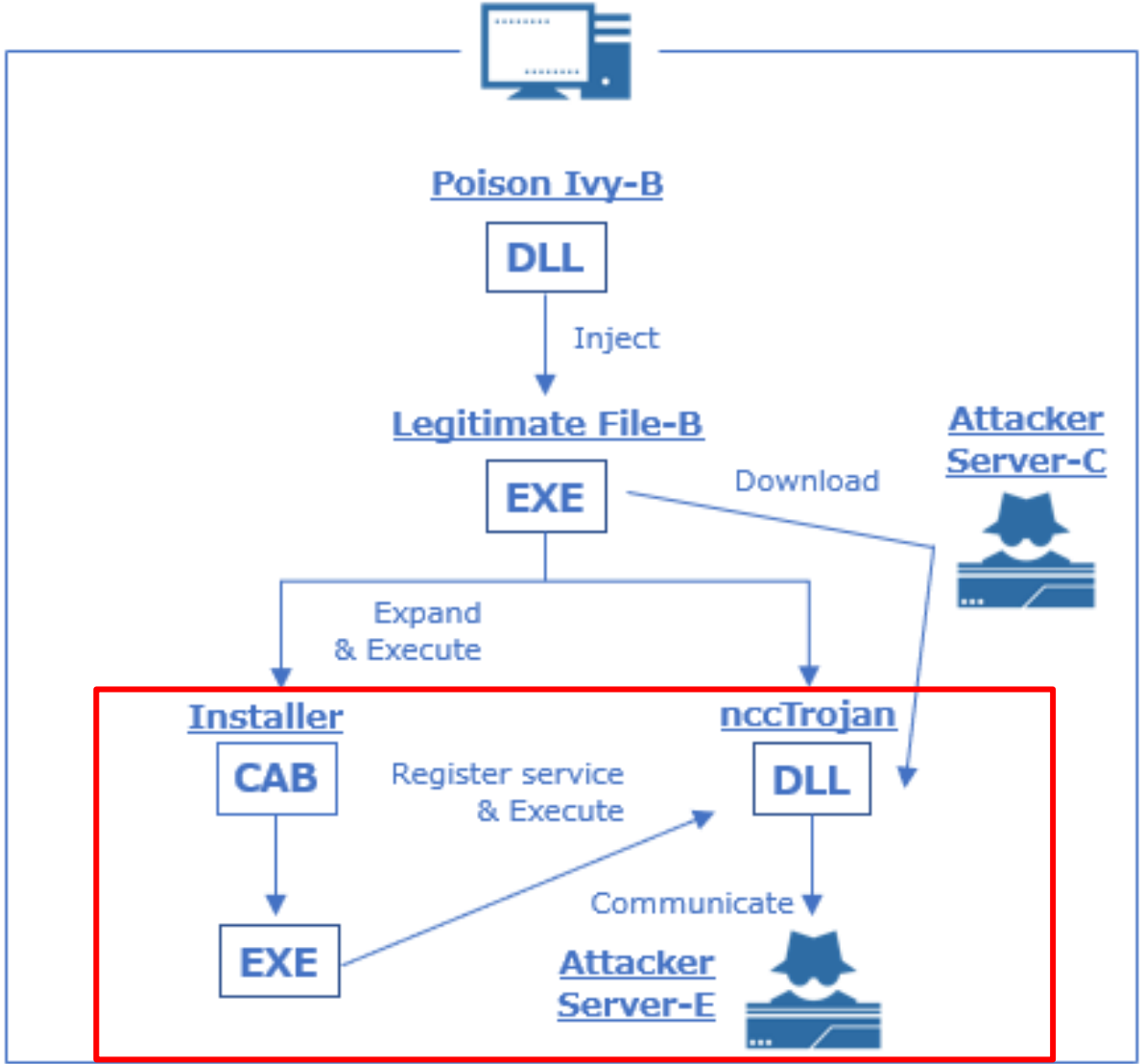
- Tmanger has following functions:
 - Remote Shell (cmd.exe)
 - Remote Shell (powershell.exe)
 - Send Host Information
 - Send File Contents
 - Send Screen Capture Images
 - Delete Files
 - Keylogger

Attack Flow Case 2

Internal Host-A

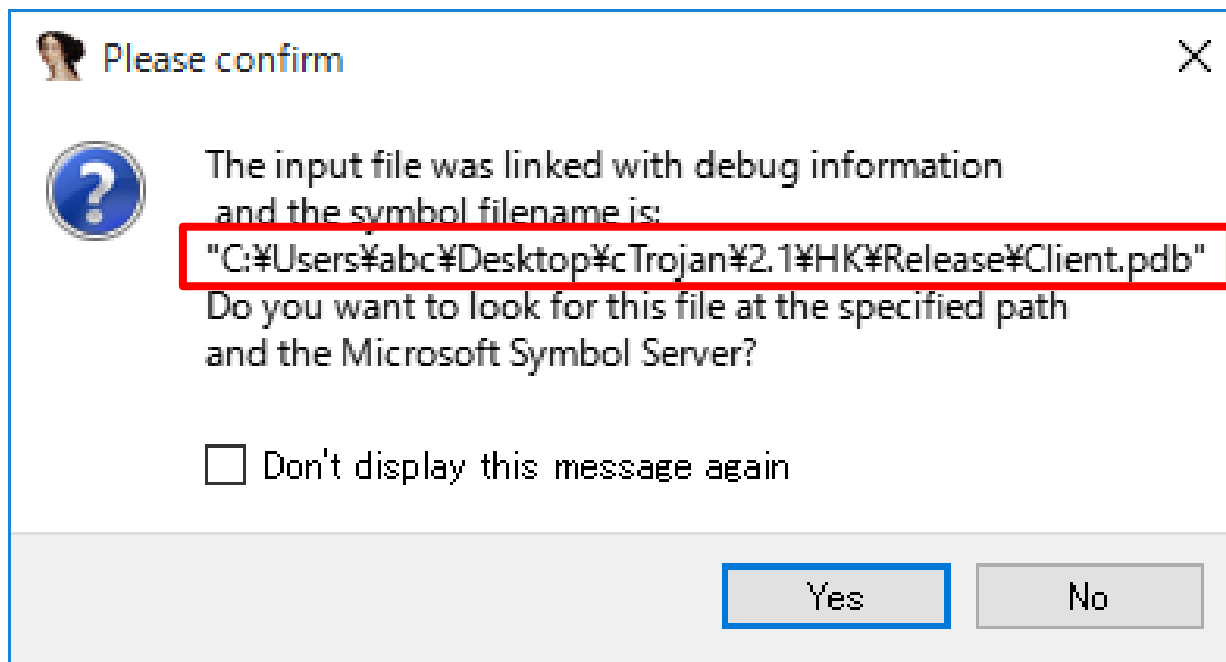


Internal Host-B



Evidence

- PDB File Path



Startup Sequence and Persistence

- Poison Ivy-B places the installer "Instsrv.exe" and nccTrojan "WindowsResKits.dll" on "C:\ProgramData\Microsoft\Crypto", then launches Instsrv.exe.
- Instsrv.exe copies WindowsResKits.dll to following system directories.
 - %SYSTEMROOT%\System32\WindowsResKits.dll (in 32-bit environment)
 - %SYSTEMROOT%\SysWOW64\WindowsResKits.dll (in 64-bit environment)
- Instsrv.exe creates and start following fake service.

Fake service

Name	Image path
Microsoft Windows Resource Kits	%SYSTEMROOT%\System32\svchost.exe -k WindowsResKits

Configuration

Decoded configuration data

Item	Value
C&C Server	45[.]77.129.213:443
Version Information	v2.1[exe]
Activation Code	ncc

Activation

- If the data received from C&C server includes activation code "ncc", nccTrojan activates its C&C functions.
- We call the new RAT "**nccTrojan**" because the activation code is characteristics for this RAT.

C&C Communication

- TCP Payload

- SIZE Field (8 Bytes) + Encrypted DATA Field
- The SIZE field expresses data size in decimal and unused digits are filled with invalid character "x".

	SIZE Field								Encrypted DATA Field								
	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F	0123456789ABCDEF
000000	78	78	78	78	78	78	34	38	-53	EA	92	51	39	C5	1B	D4	xxxxxx48S..Q9...
000010	93	E4	E3	41	B3	6E	E7	38	-DC	6B	8F	50	BB	72	0E	08	...A.n.8.k.P.r..
000020	BB	2A	93	F1	83	F6	D6	CC	-54	B0	AC	CA	6E	EA	F8	E1	.*.....T...n...
000030	2F	E5	92	57	74	B7	89	44	-								/..Wt..D

C&C Communication

- Encryption

- Algorithm: AES-256 in CFB mode
- Key (256 bits) / Initialization Vector (128 bits):

The encryption key and initialization vector

Item	Value
Key (hex-encoded)	981511371412780969AFC3AB2072018709A83A3332466A8B56FF 3FAB8E6C3DAA
IV (hex-encoded)	2042123224315117031B1A0A3CCDA53F

C&C Communication

● Decrypted DATA Field

- Size (8 Bytes) + Command (1 Byte) + Content + Padding
- Size = length(Command + Content)
- The format of Size field is as same as that in TCP payload.

	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F	0123456789ABCDEF
000000	78	78	78	78	78	78	33	35	03	6E	65	74	20	67	72	6F	xxxxxx35.net gro
000010	75	70	20	22	44	6F	6D	61	69	6E	20	43	6F	6E	74	72	up "Domain Contr
000020	6F	6C	6C	65	72	73	22	20	2F	64	6F	00	00	00	00	00	ollers" /do.....
000030	█																█

Size (points to bytes +0 to +7)
Command (points to byte +8)
Content (points to bytes +9 to +F)
Padding (points to bytes +C to +F)

Command and Control

- nccTrojan has following functions:
 - Remote Shell
 - Send Disk Information
 - Send File List
 - Send Process List
 - Download File (Read File)
 - Upload Files
 - Operate Files (Copy, Move, Delete)
 - Kill Process

Wrap up

Royal Road RTF Weaponizer

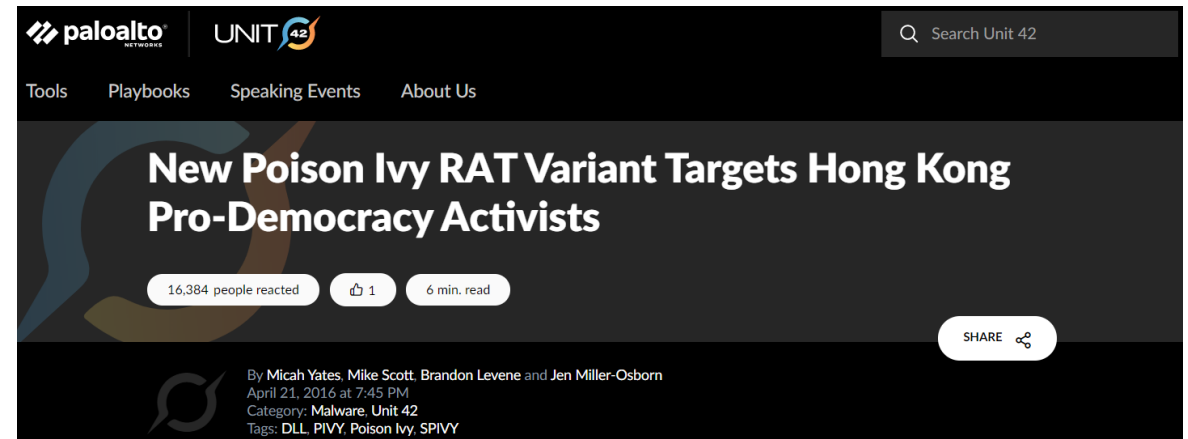
- Used by Chinese APT groups
 - Temp.Trident, Tick and Tonto
 - Mainly targeting East Asian countries

Poison Ivy

- SPIVY
 - Modified traffic structure
 - Previously used in Hong Kong in March 2016
 - Used same DLL Side-loading technique "RasTls.dll"



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



paloalto NETWORKS | **UNIT 42** | Search Unit 42

Tools | Playbooks | Speaking Events | About Us

New Poison Ivy RAT Variant Targets Hong Kong Pro-Democracy Activists

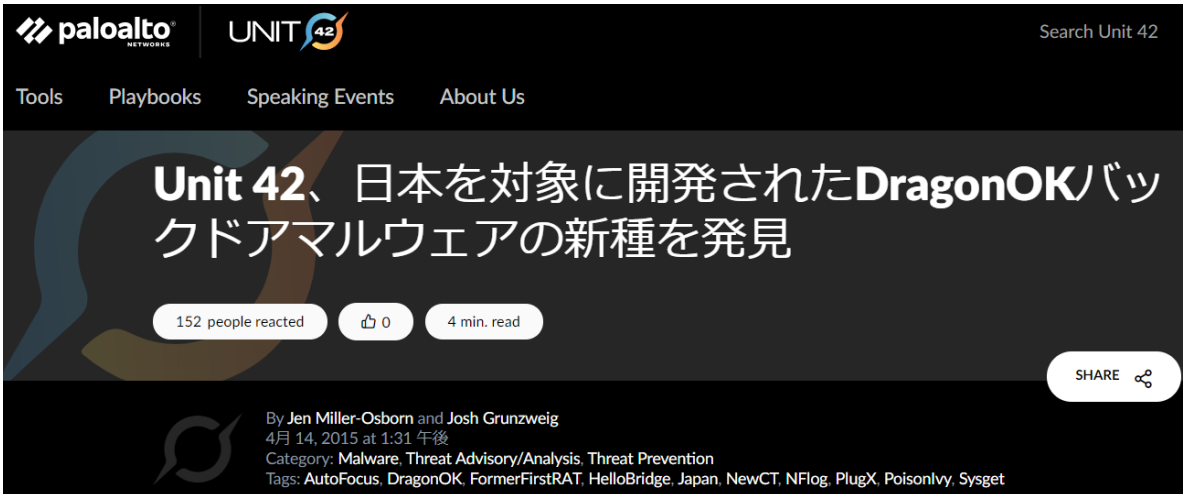
16,384 people reacted | 1 | 6 min. read

By Micah Yates, Mike Scott, Brandon Levene and Jen Miller-Osborn
April 21, 2016 at 7:45 PM
Category: Malware, Unit 42
Tags: DLL, PIVY, Poison Ivy, SPIVY

<https://unit42.paloaltonetworks.com/unit42-new-poison-ivy-rat-variant-targets-hong-kong-pro-democracy-activists/>

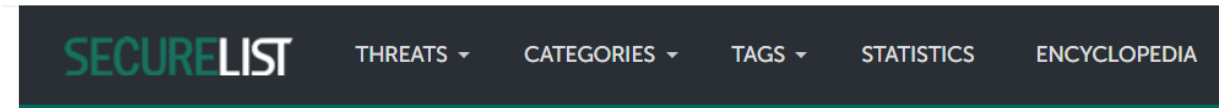
DLL Side-Loading

- PotPlayerMini
 - Previously used by DragonOK
 - DragonOK targets East Asian countries



The screenshot shows a blog post on the Palo Alto Networks Unit 42 website. The title is "Unit 42、日本を対象に開発されたDragonOKバックドアマルウェアの新種を発見" (Unit 42 discovers a new variant of DragonOK backdoor malware developed against Japan). The post is by Jen Miller-Osborn and Josh Grunzweig, dated April 14, 2015. The category is Malware, Threat Advisory/Analysis, Threat Prevention. Tags include AutoFocus, DragonOK, FormerFirstRAT, HelloBridge, Japan, NewCT, NFlag, PlugX, PoisonIvy, Sysget.

<https://unit42.paloaltonetworks.jp/unit-42-identifies-new-dragonok-backdoor-malware-deployed-against-japanese-targets/>



The screenshot shows the navigation bar of the SecureList website. It includes the "SECURELIST" logo and several menu items: THREATS, CATEGORIES, TAGS, STATISTICS, and ENCYCLOPEDIA.

PUBLICATIONS

CVE-2015-2545: overview of current threats

By **GREAT** on May 25, 2016. 10:56 am

<https://securelist.com/cve-2015-2545-overview-of-current-threats/74828/>

As a result of analyzing the observed attack cases, we found the following:

- Operation LagTime IT has been observed since at least around March 2019 and its TTPs hasn't changed for more than a year
- Used a tool to exploit MS17-010 for lateral movement, NETBIOS scanner for environmental investigations, tools to steal credentials and new RATs such as Tmanger or nccTrojan
- Colorful Panda Footprint (the TTPs of these attack cases overlap with those of several Chinese APT groups)
 - Tick, Tonto, DragonOK

Traffic Decryption Tools for Tmanger & nccTrojan

- Later, we will announce the download site on our Twitter account
 - @GlobalNTT_JP (https://twitter.com/globalntt_jp)



Case 1

- MD5

- f1b21f5f9941afd9eec0ab7456ec78b8 (Lure Document)
- b26b60c8ba87df6322fa48916b7ba86d (Poison Ivy)
- 8fa6b43e35675b05bd4cbe8a9e9413b8 (Credential Stealer)
- f01a9a2d1e31332ed36c1a4d2839f412 (Environment Scanner)
- 11b2e94fdac1ff94899debbcf63c33aa (Cotx RAT)

- Domain

- news.vzglagtime[.]net (Attacker Server-A)
- mtanews.vzglagtime[.]net (Attacker Server-B)

Case 2

- MD5

- 60ec80e7e72afa9a24c48517d9e97f4c (Lure Document)
- 7372101f6423ee4226b83cca12b13bb9 (Poison Ivy-A)
- 8fa6b43e35675b05bd4cbe8a9e9413b8 (Credential Stealer-A)
- f01a9a2d1e31332ed36c1a4d2839f412 (Environment Scanner)
- 11b2e94fdac1ff94899debbcf63c33aa (Cotx RAT)
- d00d8f1c6ee37d86dd78bbbbee328878c (Scan Tool)
- 78ea3649a05f241516288603e5305a79 (Exploit Tool)
- bcfd4ebf4856ae2eeba1604fd243d522 (Poison Ivy-B x86.dll)
- 7dfae85cb034a2ee5c715530e163b35d (Poison Ivy-B x64.dll)
- 4993e67fcabaf949380196fabe004fd4 (Credential Stealer-B)
- 8a79aeaed654e96d86fbe1bbc1e9de84 (Tmanger)
- c999b26e4e3f15f94771326159c9b8f9 (Installer)
- 54816d2dcc0275e30c615cc44f52df6b (nccTrojan)

Case 2

- Domain & IP
 - 95[.]179.131.29 (Attacker Server-A)
 - mtanews.vzglagtime[.]net (Attacker Server-B)
 - 45[.]76.211.18 (Attacker Server-C)
 - 172[.]105.39.67 (Attacker Server-D)
 - 45[.]77.129.213 (Attacker Server-E)

Thank you