



Where is the cuckoo egg?

Virus Bulletin 2021 localhost

7-8 October, 2021

Ryuichi Tanabe, Hajime Takai & Rintaro Koike

Ryuichi Tanabe

- SOC & malware analyst at NTT Security (Japan) KK
- Responsible for EDR Detection in SOC

Hajime Takai

- SOC & malware analyst at NTT Security (Japan) KK
- Speaker of Japan Security Analyst Conference 2020, 2021

Rintaro Koike

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

We found an unknown malware (=Tmanger) in Operation LagTime IT

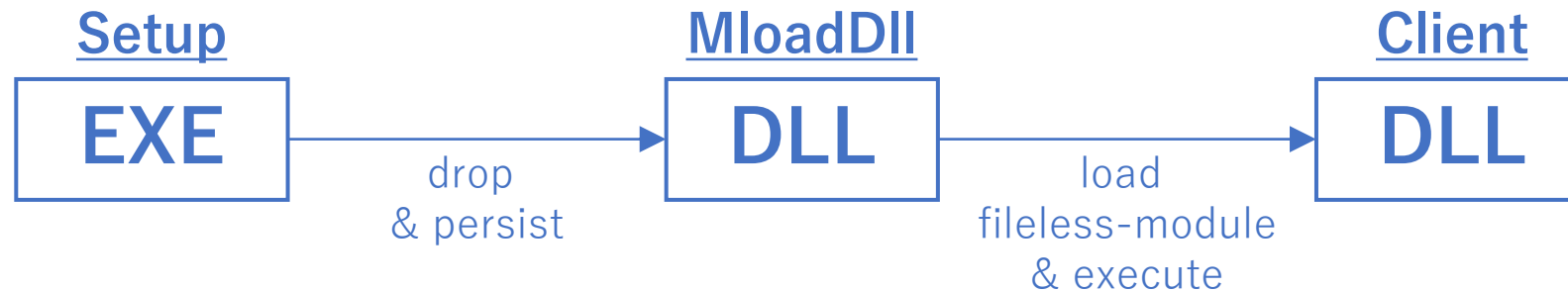
- Various versions and variants (Albaniiutas, Smanager, etc)
- Some APT groups seem to share them
- One of the most influential malware families in East and Southeast Asian countries.

Sharing information about Tmanger family

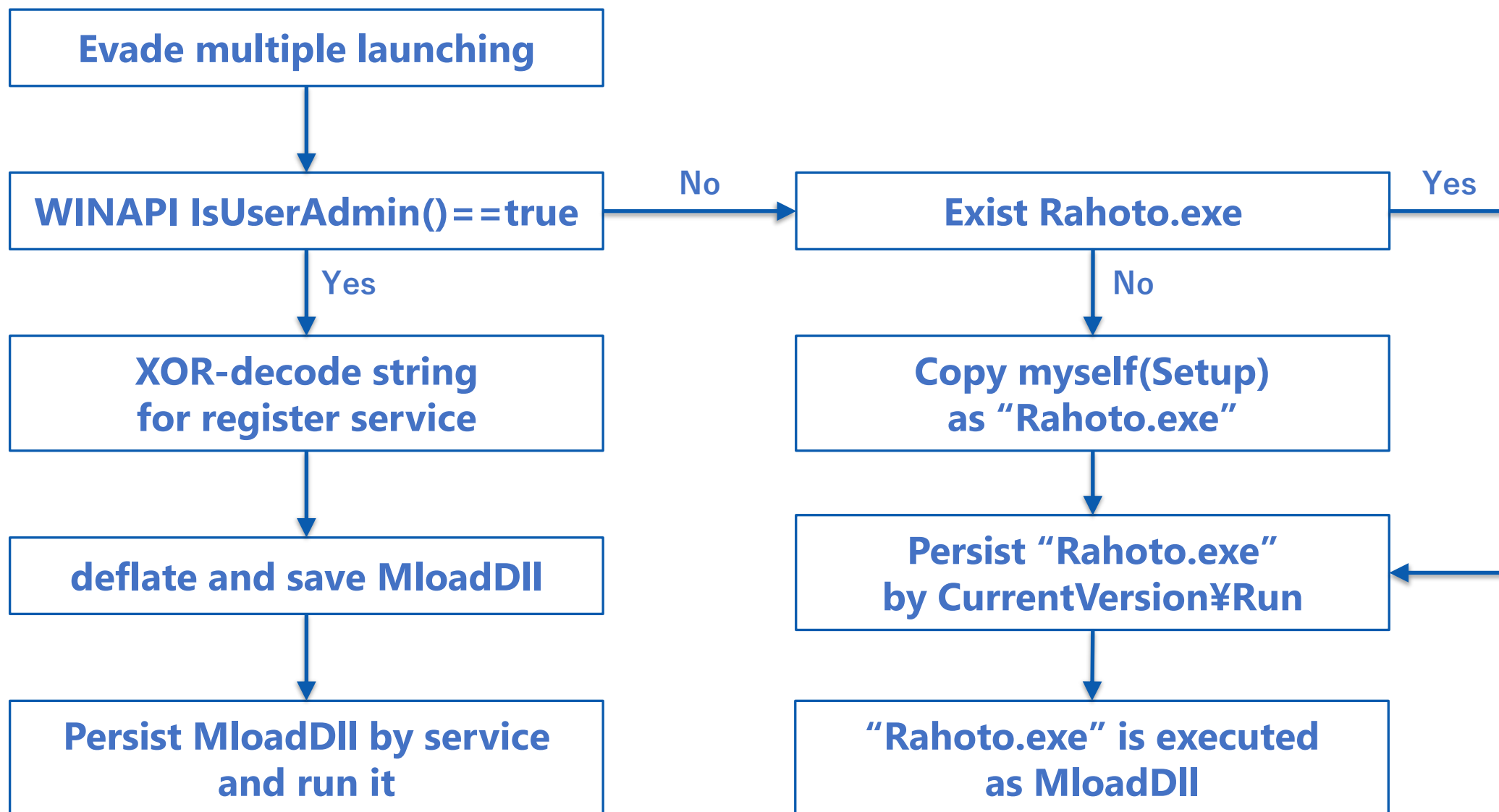
- Detailed analysis result (Tmanger, Albaniiutas and Smanager)
- Family Tree
- Attribution & relationship
- Hunting Tips (Especially APT groups may belong to China)

Malware Analysis

Tmanger family has 3 common elements

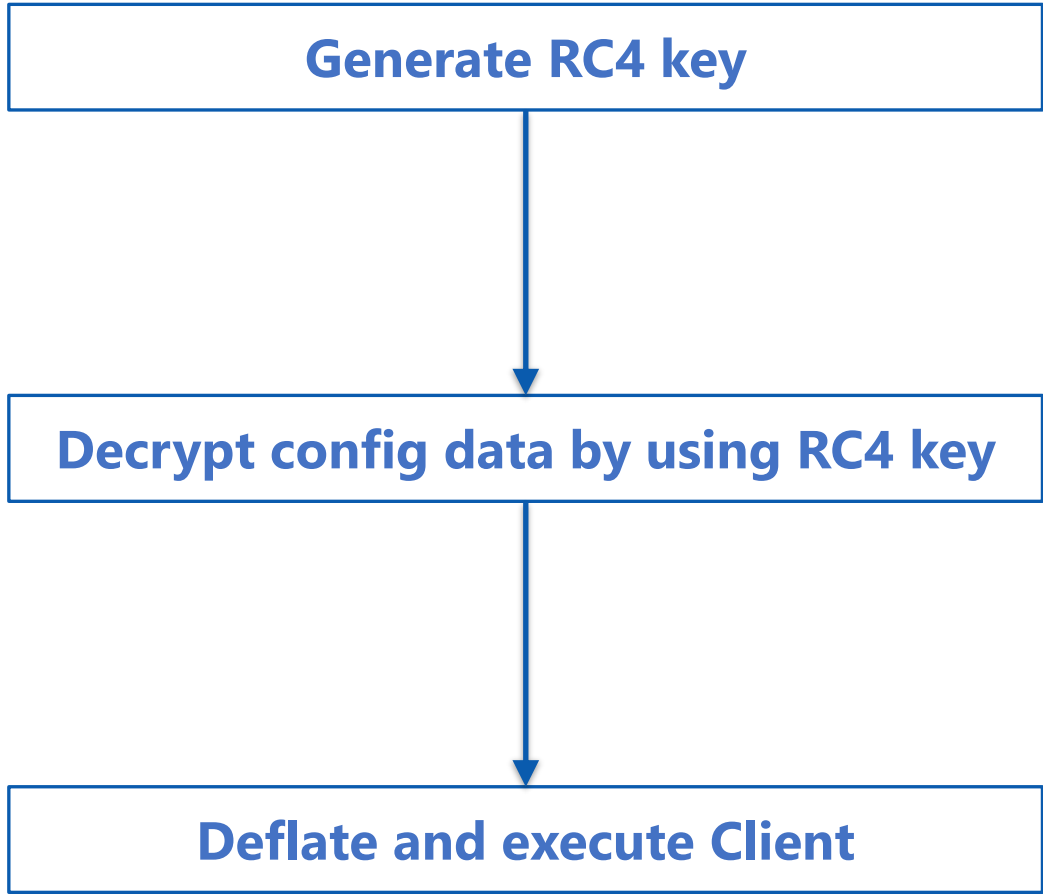


Classification of Tmanger	Description
SetUp	Open and execute MloadDII
MloadDII	Open and execute Client
Client	RAT



- Tmanger terminate Setup, if CreateEvent() is failed.
- Created event name fulfills following regex condition:

```
/[0-9a-f]{8}-[0-9a-f]{4}-4551-8f84-08e738aec[0-9a-f]{3}/
```



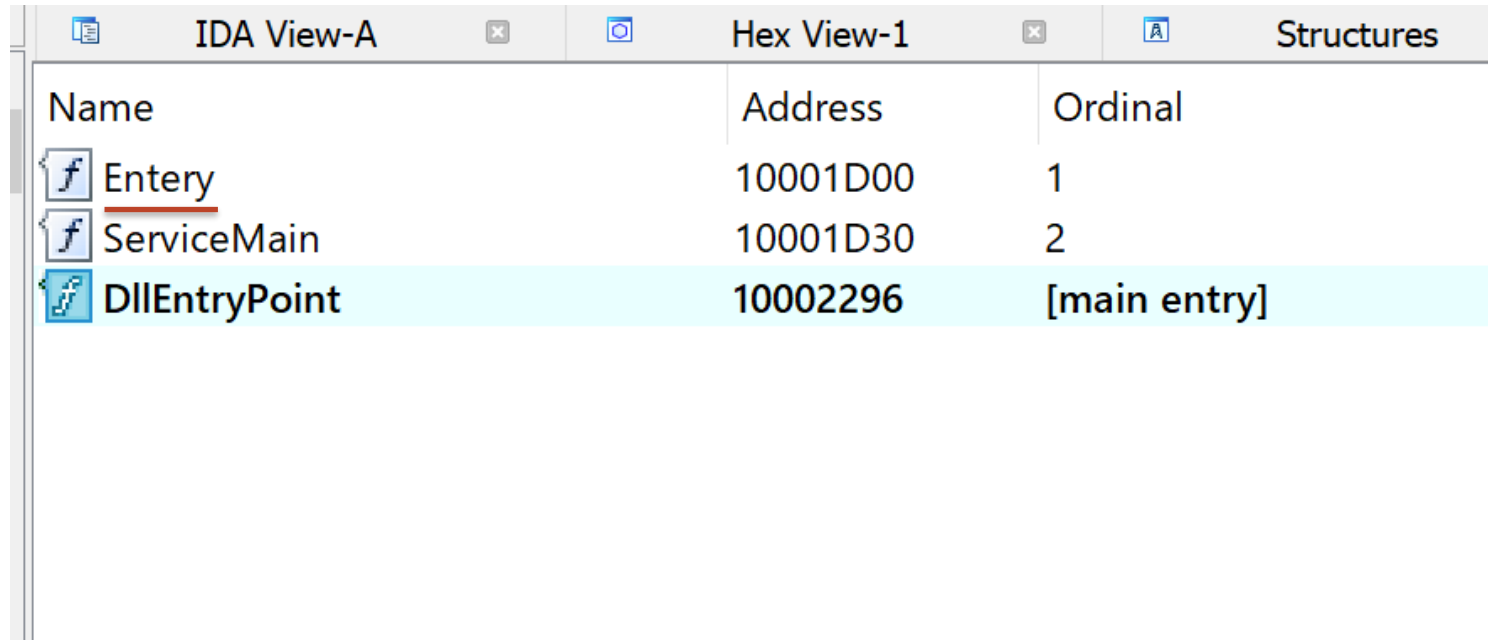
```
0x004010f0 movzx eax, byte [edx - 0x40]
0x004010f4 lea edx, [edx + 4]
0x004010f7 xor byte [edx - 4], al
0x004010fa movzx eax, byte [edx - 0x43]
0x004010fe xor byte [edx - 3], al
0x00401101 movzx eax, byte [edx - 0x42]
0x00401105 xor byte [edx - 2], al
0x00401108 movzx eax, byte [edx - 0x41]
0x0040110c xor byte [edx - 1], al
0x0040110f sub esi, 1
0x00401112 jne 0x4010f0
```




Fig.) RC4 key generation algorithm

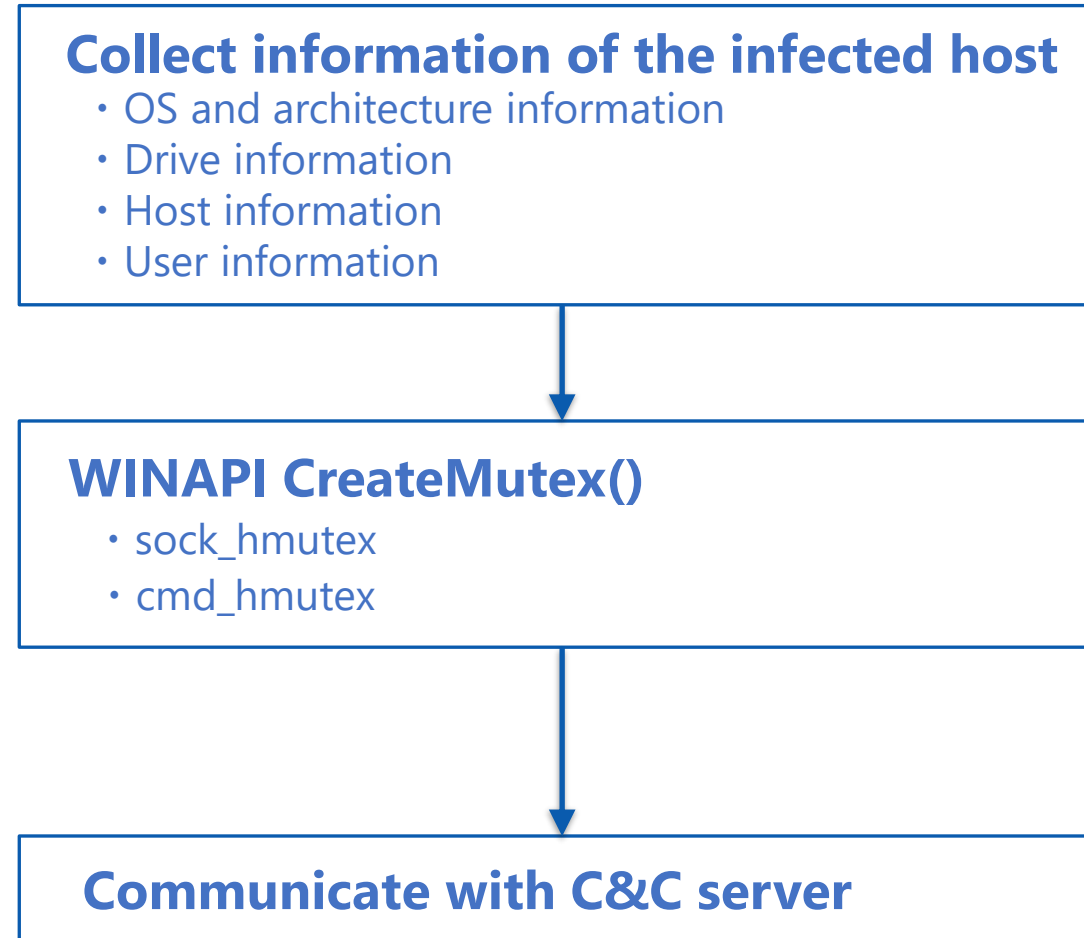
アドレス	Hex	ASCII
6F7BA770	31 37 32 2E 31 30 35 2E 33 39 2E 36 37 00 00 00	172.105.39.67...
6F7BA780	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
6F7BA790	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
6F7BA7A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
6F7BA7B0	38 30 00 00 00 00 00 00 00 00 00 00 00 00 00	80.....
6F7BA7C0	31 37 32 2E 31 30 35 2E 33 39 2E 36 37 00 00 00	172.105.39.67...
6F7BA7D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
6F7BA7E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
6F7BA7F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
6F7BA800	34 34 33 00 00 00 00 00 00 00 00 00 00 00 00	443.....
6F7BA810	31 37 32 2E 31 30 35 2E 33 39 2E 36 37 00 00 00	172.105.39.67...
6F7BA820	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
6F7BA830	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
6F7BA840	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
6F7BA850	35 32 32 32 00 00 00 00 00 00 00 00 00 00 00	5222.....

Fig.) decrypted config data(IP and port for Client)

- MloadDll implements an Export function named 'Entery'.
- `Entery` function is a characteristic name through Tmanger family



Name	Address	Ordinal
 Entery	10001D00	1
 ServiceMain	10001D30	2
 DllEntryPoint	10002296	[main entry]



Command ID	Description
1, 17	Start specific process
2	Get directory information
3, 19, 35	Upload file
4	Get file information
18	File delete
20, 52	Clean up memory etc
34	Start process by CreateProcess()
36	Download file
50	File copy
80, 81	Get keylog
96	Get screen capture
Others	Sleep

- Traffic Data was encrypted by RC4
- Head of Traffic Data(4 bytes) is an ID led from ProcessID
- Tmanger family use following calculation algorithm

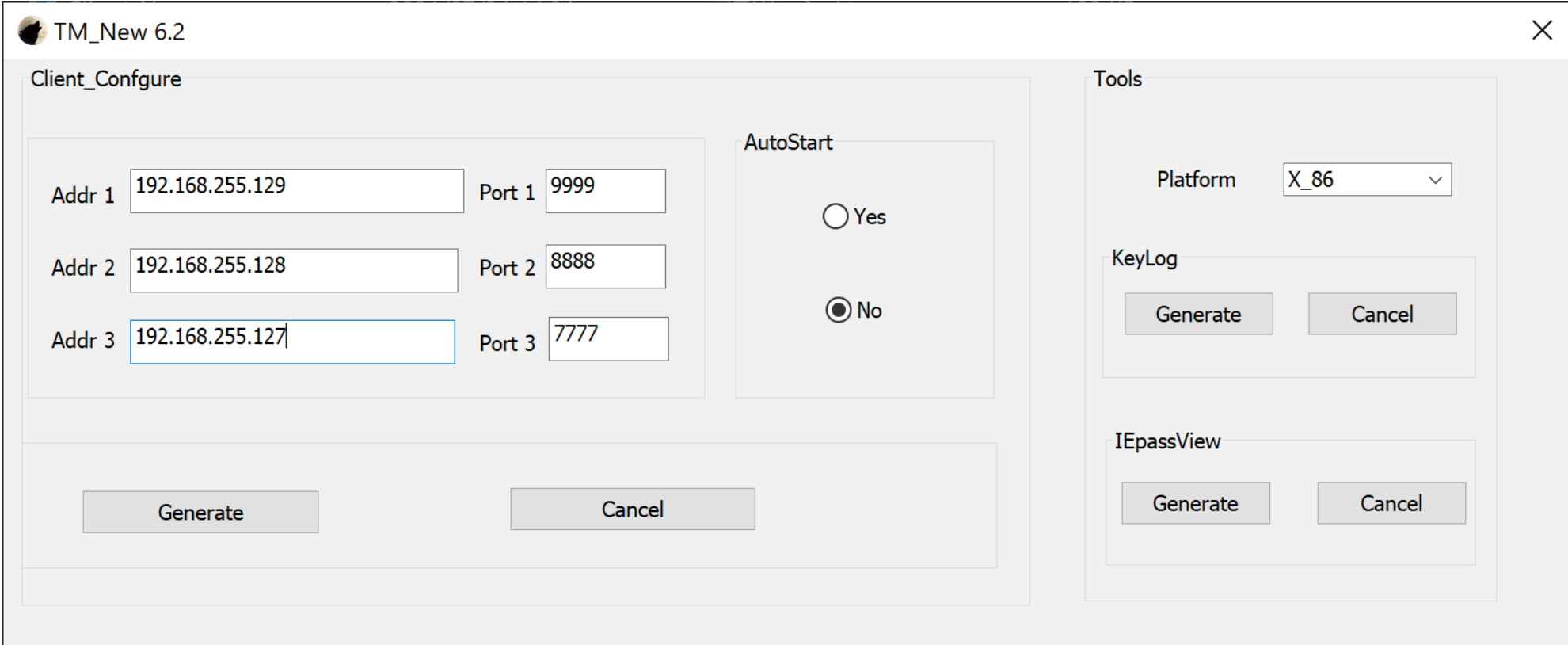
	Data Length	Encrypted Data
00000000	15 00 00 00	1b f5 42 5a 9e 55 92 03 7a 0e b8 b6
00000010	f8 8c 36 19	12 9e 54 62 56

↓ Decrypt(RC4)

	ID	Command
00000000	33 35 34 38	01 80 be 39 00 73 79 73 74 65 6d 69
00000010	6e 66	6f 0d 0a

$$\{(\text{ProcessID} \% 9) \times 1000\} + \{((\text{ProcessID} \% 1000) + 1000)\}$$

- Setting IPs and Ports of Client C&C server
- Generating MloadDlls
- Generated MloadDlls executes Client



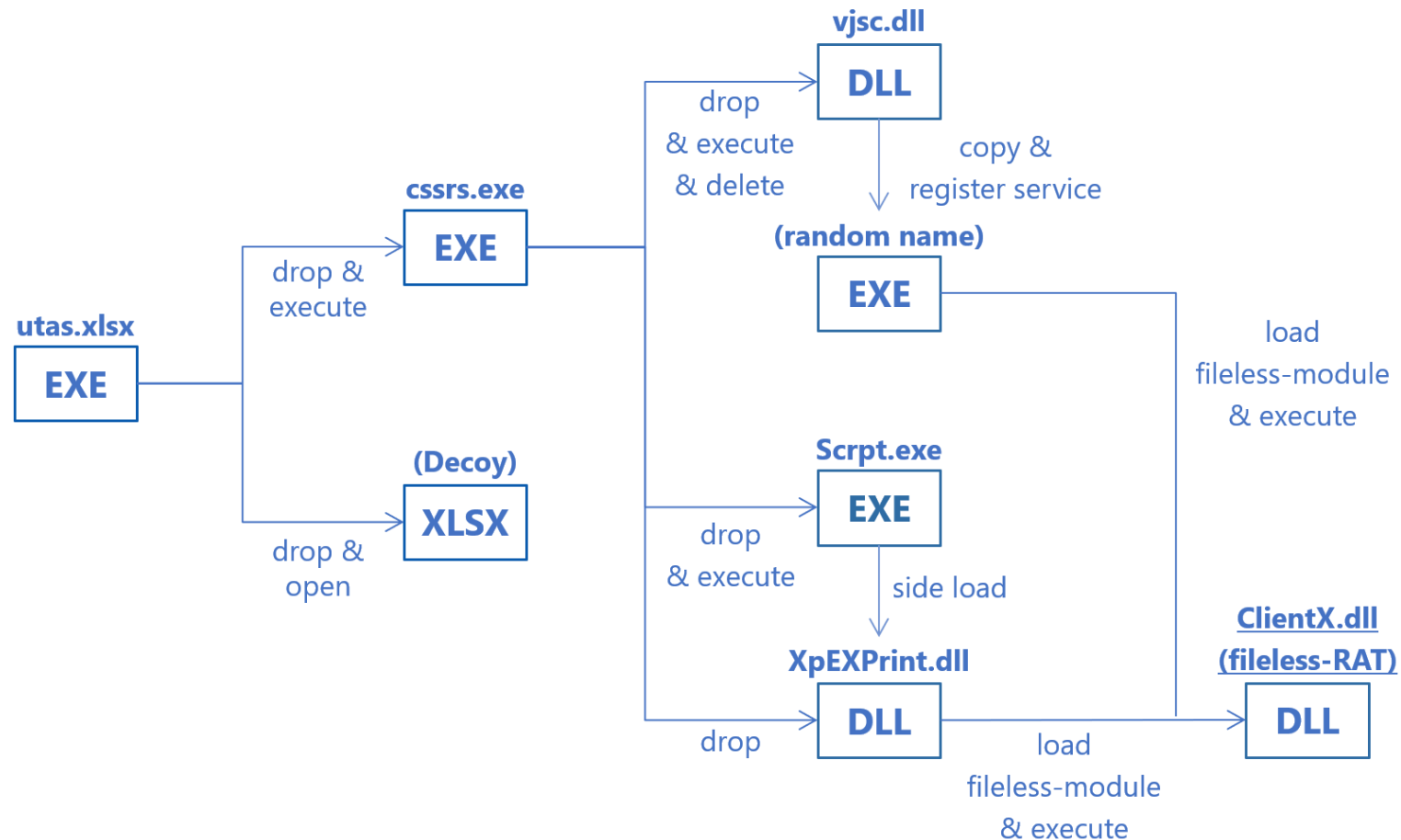
The screenshot displays the 'TM_New 6.2' application window, which is divided into two main sections: 'Client_Configure' and 'Tools'.

Client_Configure:

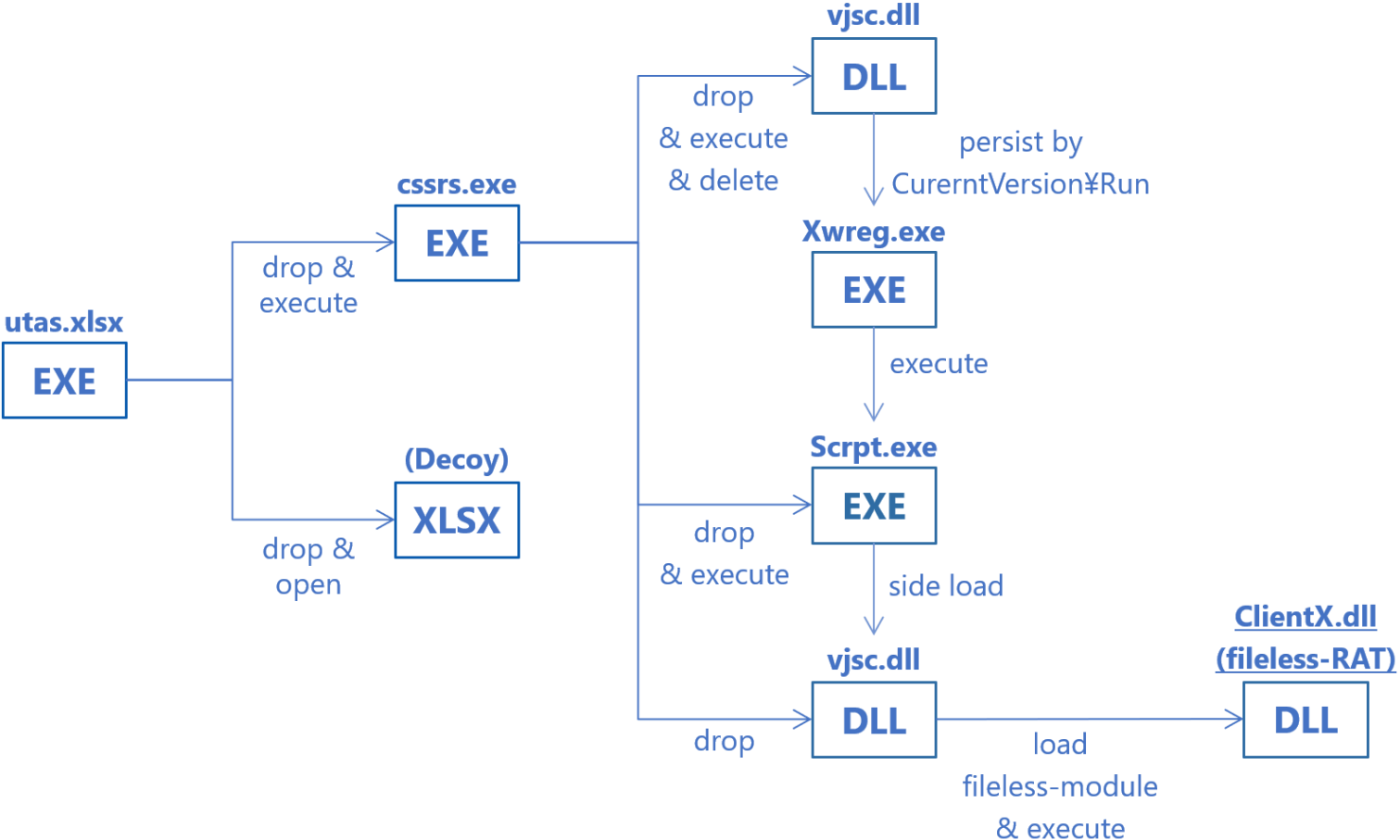
- Addr 1:** 192.168.255.129
- Port 1:** 9999
- Addr 2:** 192.168.255.128
- Port 2:** 8888
- Addr 3:** 192.168.255.127
- Port 3:** 7777
- AutoStart:** Radio buttons for 'Yes' (unselected) and 'No' (selected).
- Buttons:** 'Generate' and 'Cancel' buttons are located at the bottom of this section.

Tools:

- Platform:** A dropdown menu currently set to 'X_86'.
- KeyLog:** 'Generate' and 'Cancel' buttons.
- IEpassView:** 'Generate' and 'Cancel' buttons.



Classification of Tmanger	Albaniiutas
SetUp	cssrs.exe, vjsc.dll
MloadDll	(random name), XpEXPrint.dll
Client	ClientX.dll



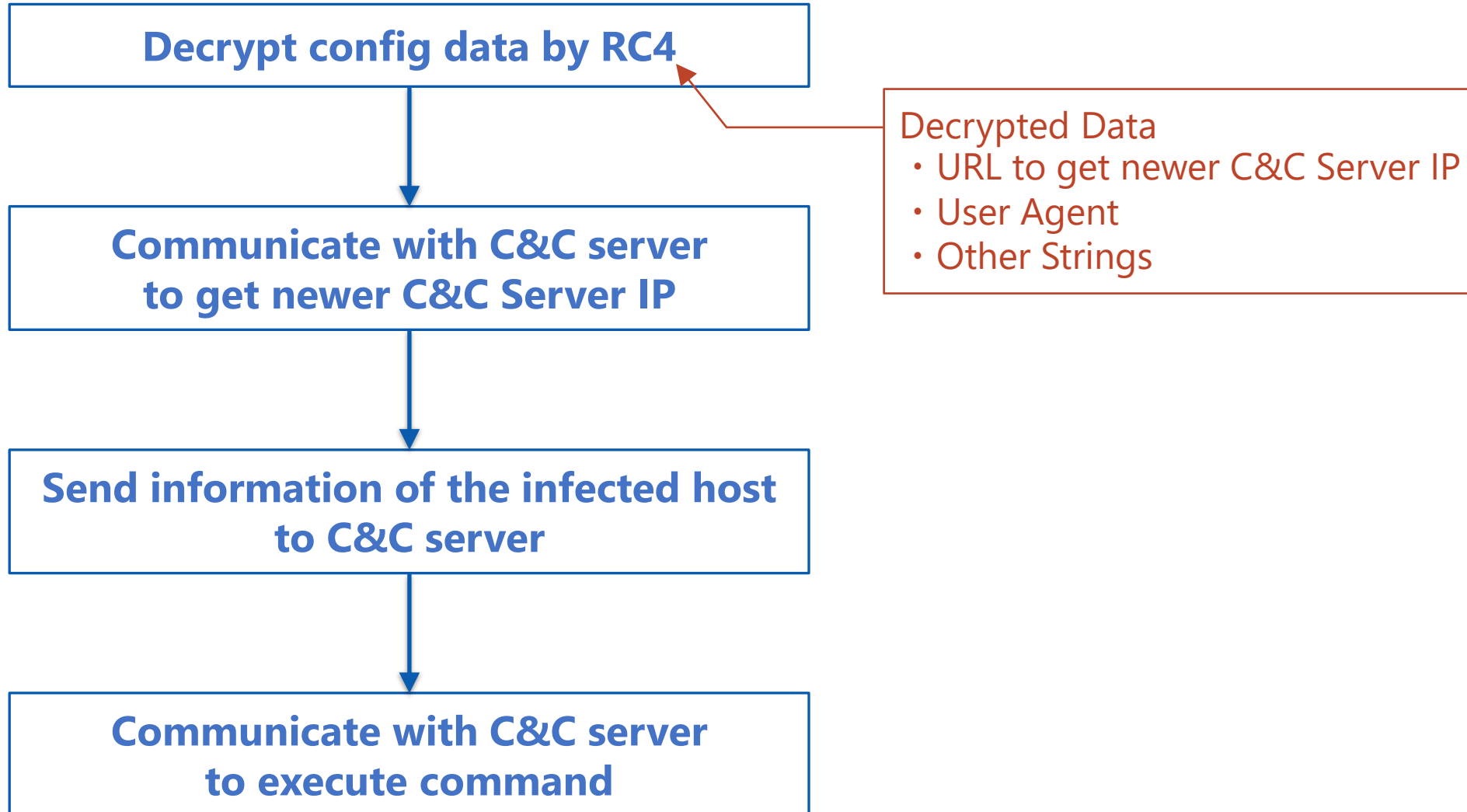
Classification of Tmanger	Albaniiutas
SetUp	cssrs.exe, vjsc.dll
MloadDll	Xwreg.exe, vjsc.dll
Client	ClientX.dll

Setup and MloadDll are almost like Tmanger

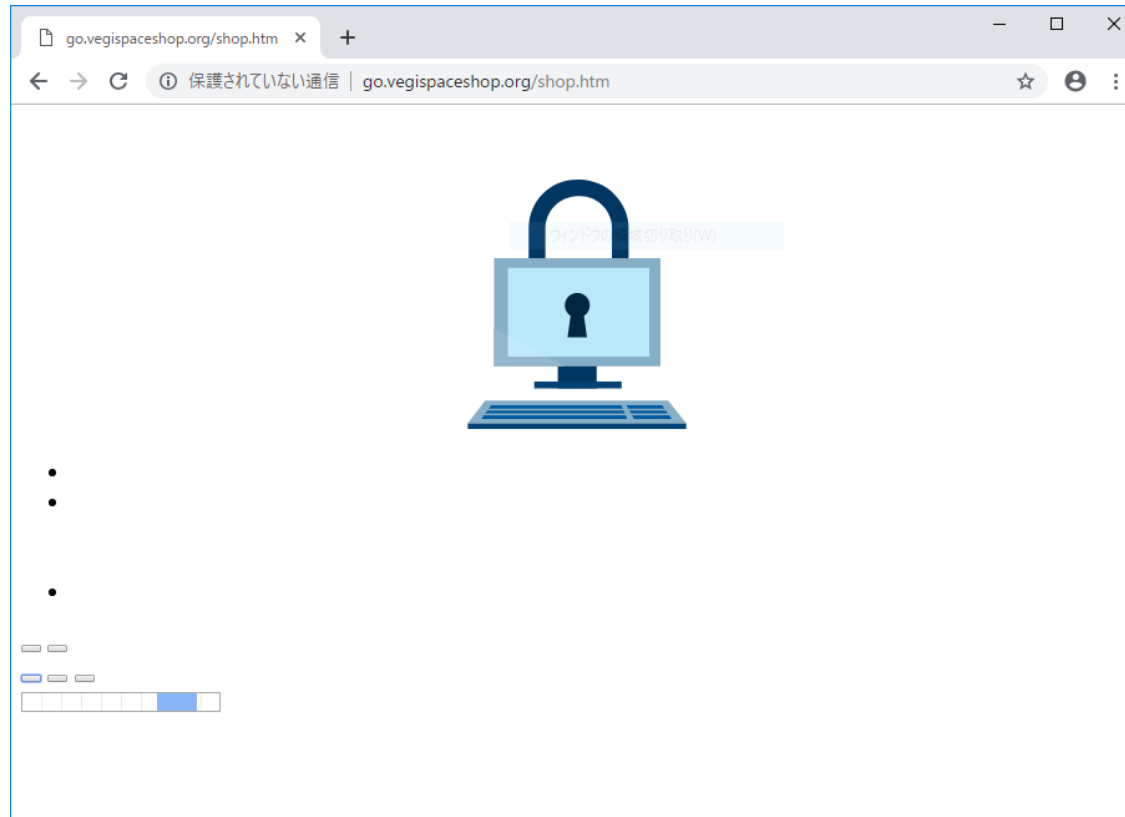
- Decrypting data in resource section
- Load and Execute Client on memory

But...

- MloadDll malware (XpEXPrint.dll and vjsc.dll) is side-loaded by a legitimate signed binary file
- That binary is a Visual J# command tool.



- Client downloads HTML file from C&C server
- HTML file includes encrypted data
- Encrypted data has new C&C server IP addresses



- Client sends host information in the path of URL to a new C&C server

http://199.247.6[.]37/home/1639/0108/

①

②

③

④

⑤

AES256 & Base64

- ① Newly obtained C&C server IP address
- ② Always same string "home"
- ③ Random value based on system time used by command execution
- ④ Numerical value of string length of ⑤
- ⑤ String encrypted by AES256 & Base64

result of
hostname command

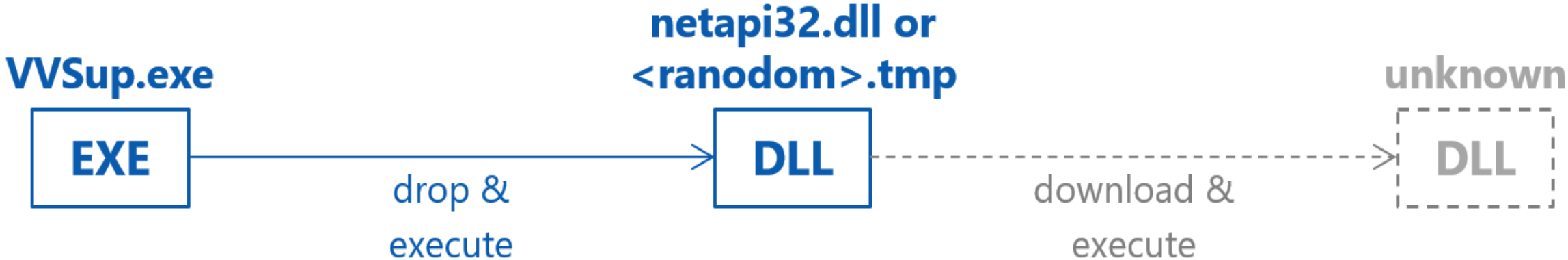
GUID created by
CoCreateGuid()

return value
of GetTickCount()

61	64	6d	69	6e	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
12	34	56	78	9a	bc	ed	f0	12	34	56	78	9a	bc	ed	f0
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
12	34	56	78	00	00	00	00	00	00	00	00	00	00	00	00

- Less command than Tmanger
- Seems minimum possible commands to run as a RAT.

Command ID	Option	Description
(command)	<ul style="list-style-type: none">● Argument(s)	Execute command by using cmd.exe and return the result to the C&C server
-upload	<ul style="list-style-type: none">● File Path of the infected host● Uploading path of the URL	Upload file
-download	<ul style="list-style-type: none">● Download URL● Stored file path	Download file
-exit		Do nothing



Classification of Tmanger	Smanager
SetUp	VVSup.exe
MloadDll	netapi32.dll or <random>.tmp
Client	unknown

Drop and decompress CAB file(MloadDll)

Overwrite config data of MloadDll

Dummy Data	Actual Config Data
192.168.0.107:8888	vgca.homeunix[.]org:443
(null)	office365.blogdns[.]com:443
(null)	unknown
f4f5276c00001ff5	f4f5276c00001ff5

WINAPI IsUserAdmin() == true

Table.) overwrite config data

Persist MloadDll by Service

Execute MloadDLL by WinExec

Connect to C&C server by
Microsoft Security Service Provider Interface

Execute command received from C&C server

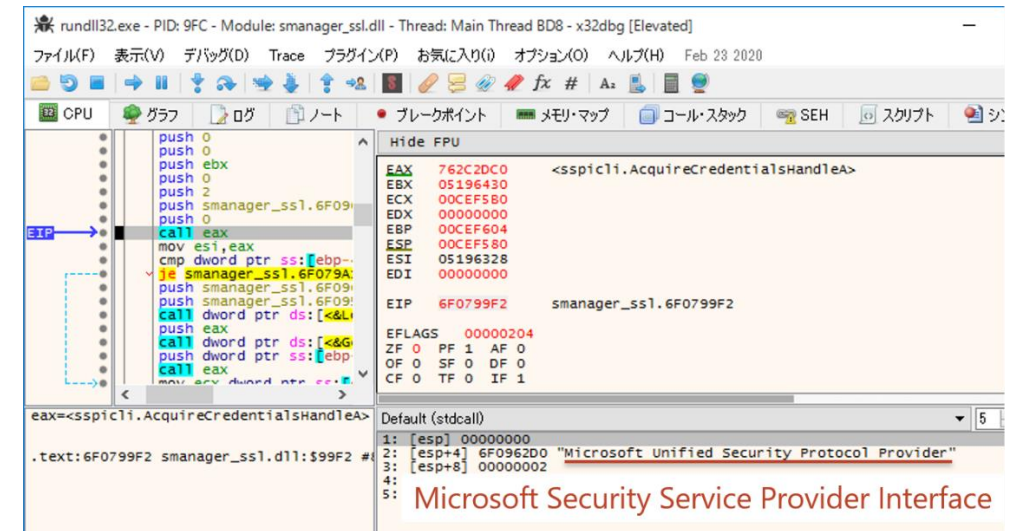


Fig.) connect to C&C server

Commands are only...

- Download an executable file and execute it
- Send the infected host information to the C&C server

Sending Information
Computer name
IP address
Language information
Default browser
Host name
OS version
Presence or absence of admin privileges
Username

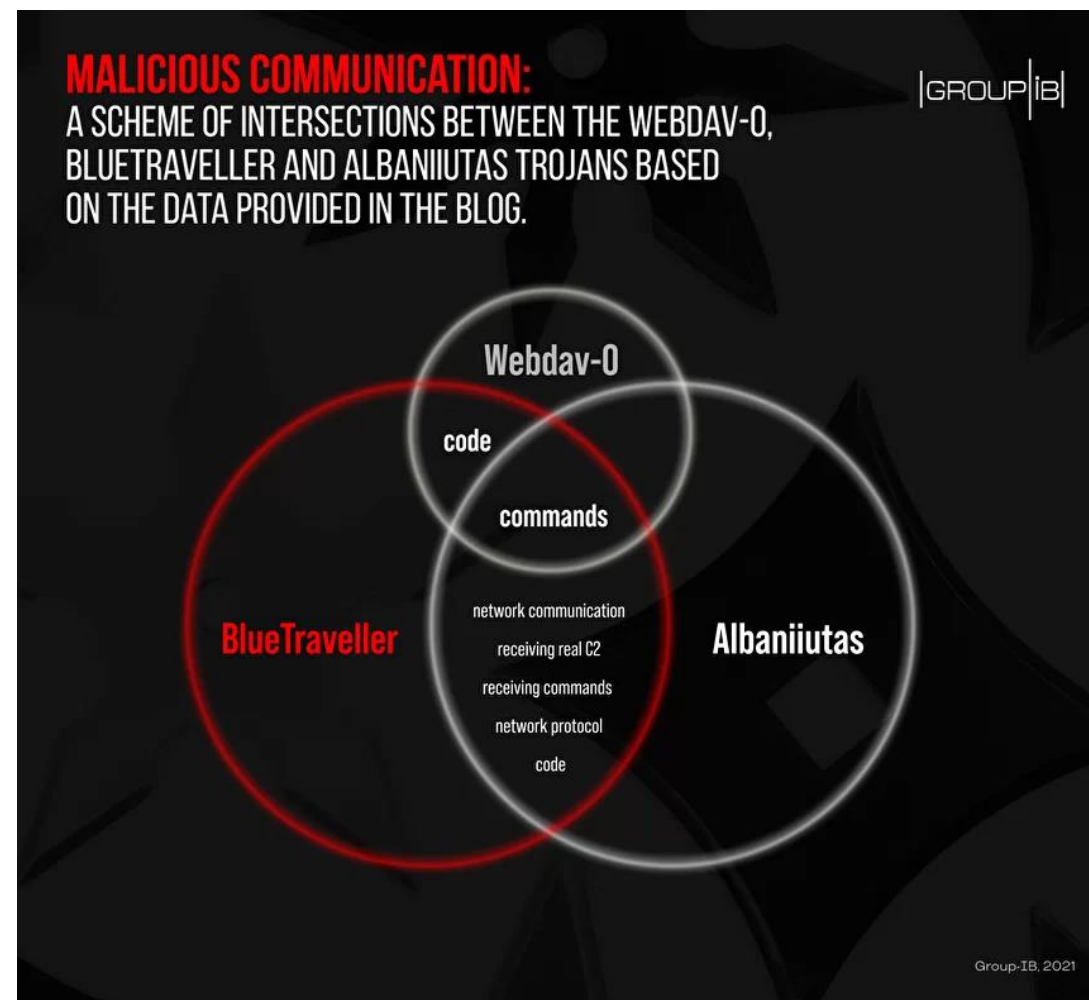
We haven't got a sample of Client but ...

- Too few commands to run as a RAT
- It has a command to download and execute an executable file.
- Tmanger family has a RAT function malware 'Client'
- Smanager should also have 'Client' and it may be downloaded file.

Family Tree

Tmanger family have some aliases

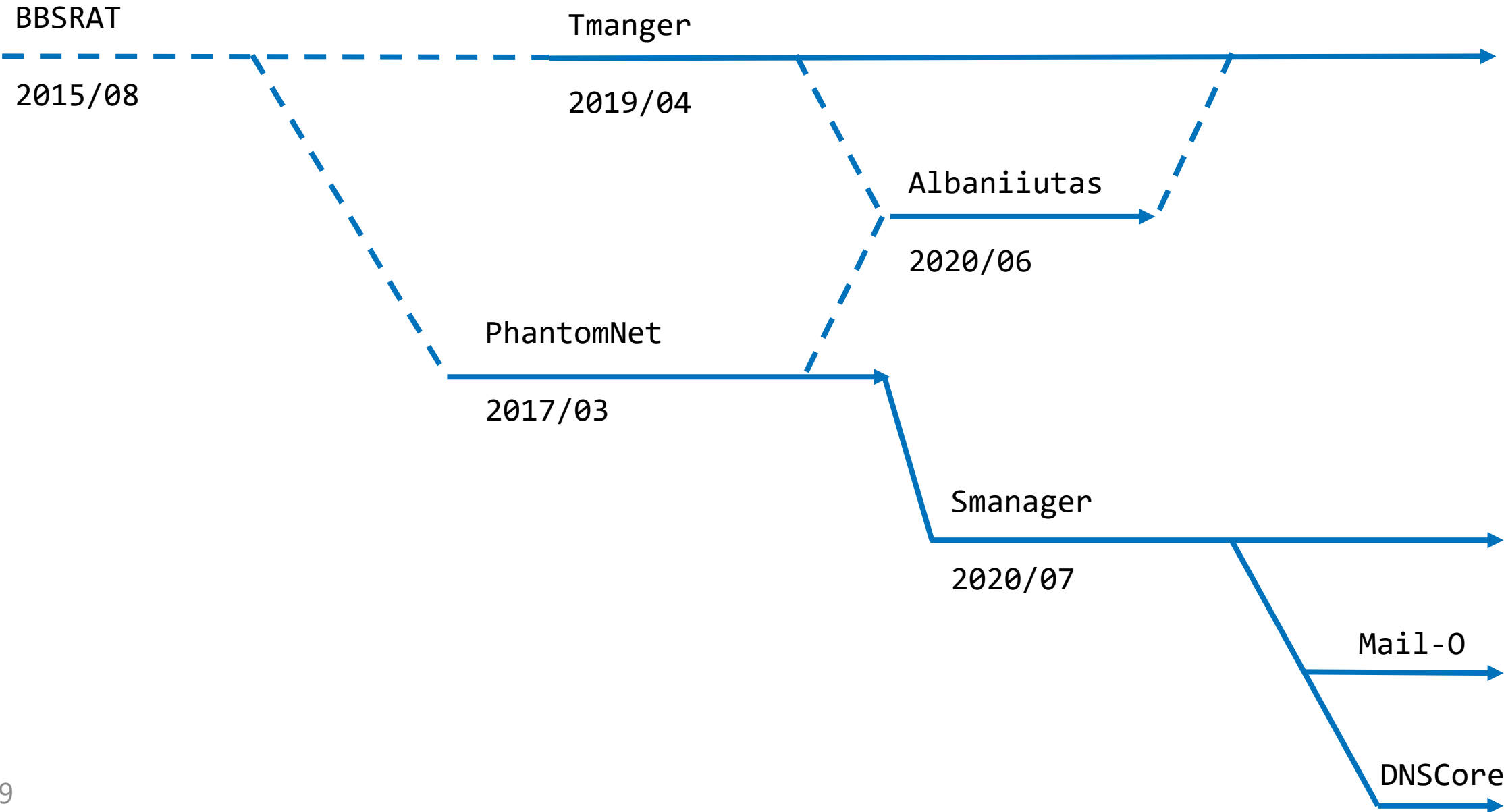
Our Definition	Alias
Tmanger	LuckyBack
Albaniiutas	(BlueTraveller*)
Smanager	PhantomNet, CoughingDown

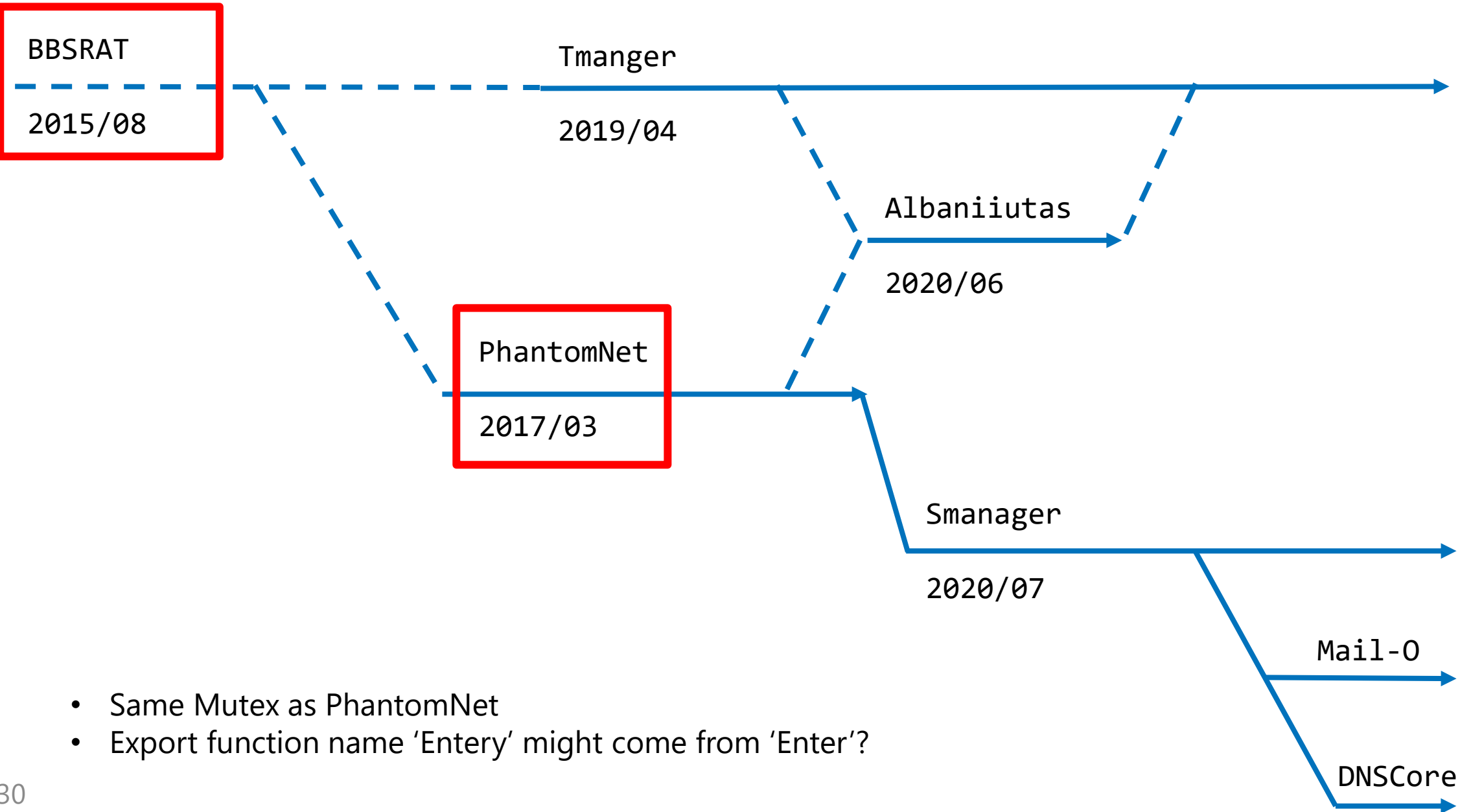


(<https://blog.group-ib.com/task>)

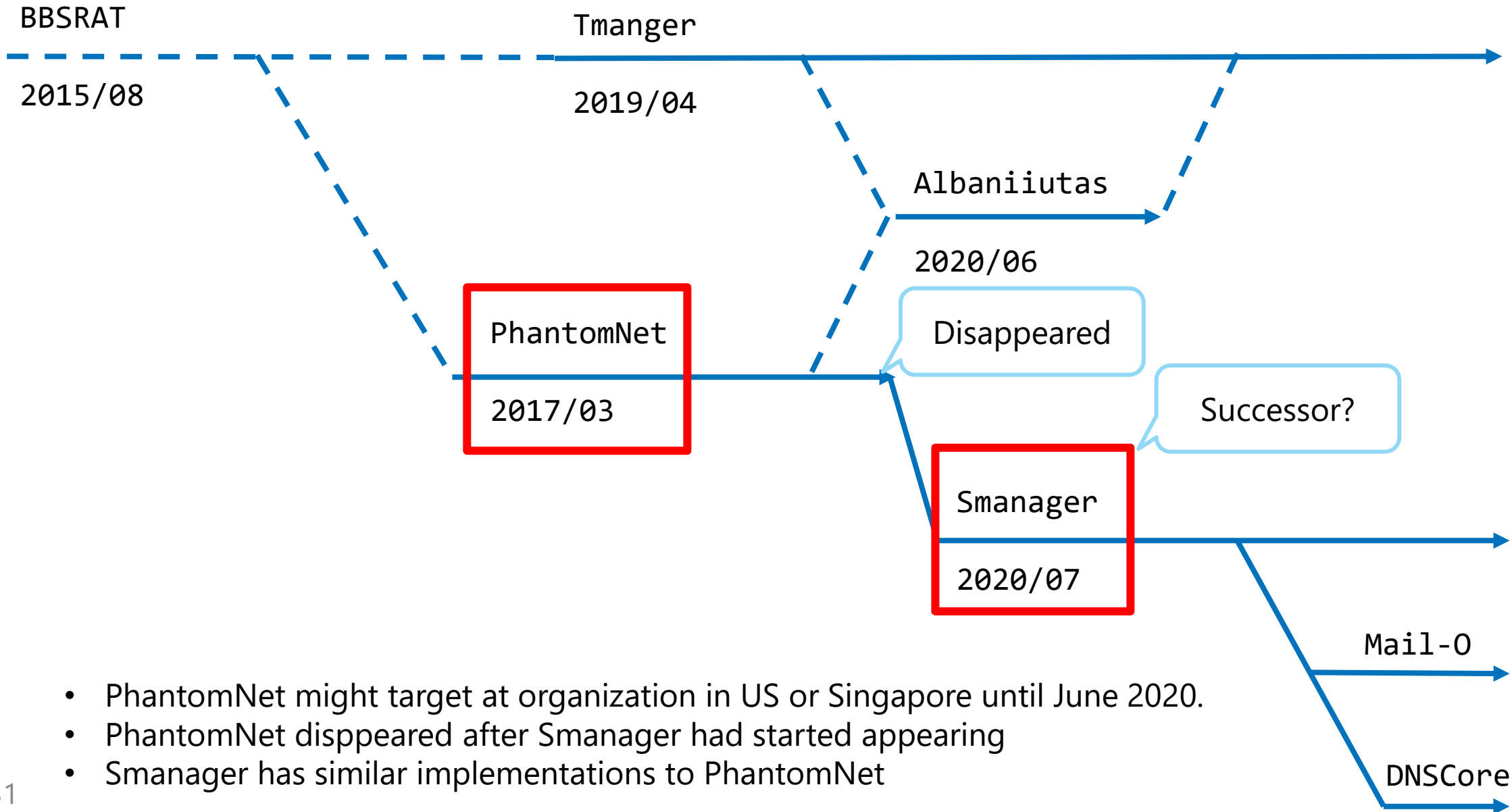
	Tmanger	Albaniutas	Smanager
Common items through multi part			
Target	Mongolia	Mongolia	Vietnam
Output of debug message	True	True	True
Compile time is around 2025	True	True	False
Include 'Waston' in user path	True	True	False
Overwrite config data	True	True	True
Setup			
Check admin privileges	True	True	True
Compression algorithm	Deflate	Deflate	Cab
String to generate encrypt key	N/A	Including '276c00001ff5'	Including '276c00001ff5'
MloadDll			
Function 'Entery' is exported	True	True	True
Call export function 'GetPluginObject' from Client	False	True	True

Overview of Tmanger Family Tree

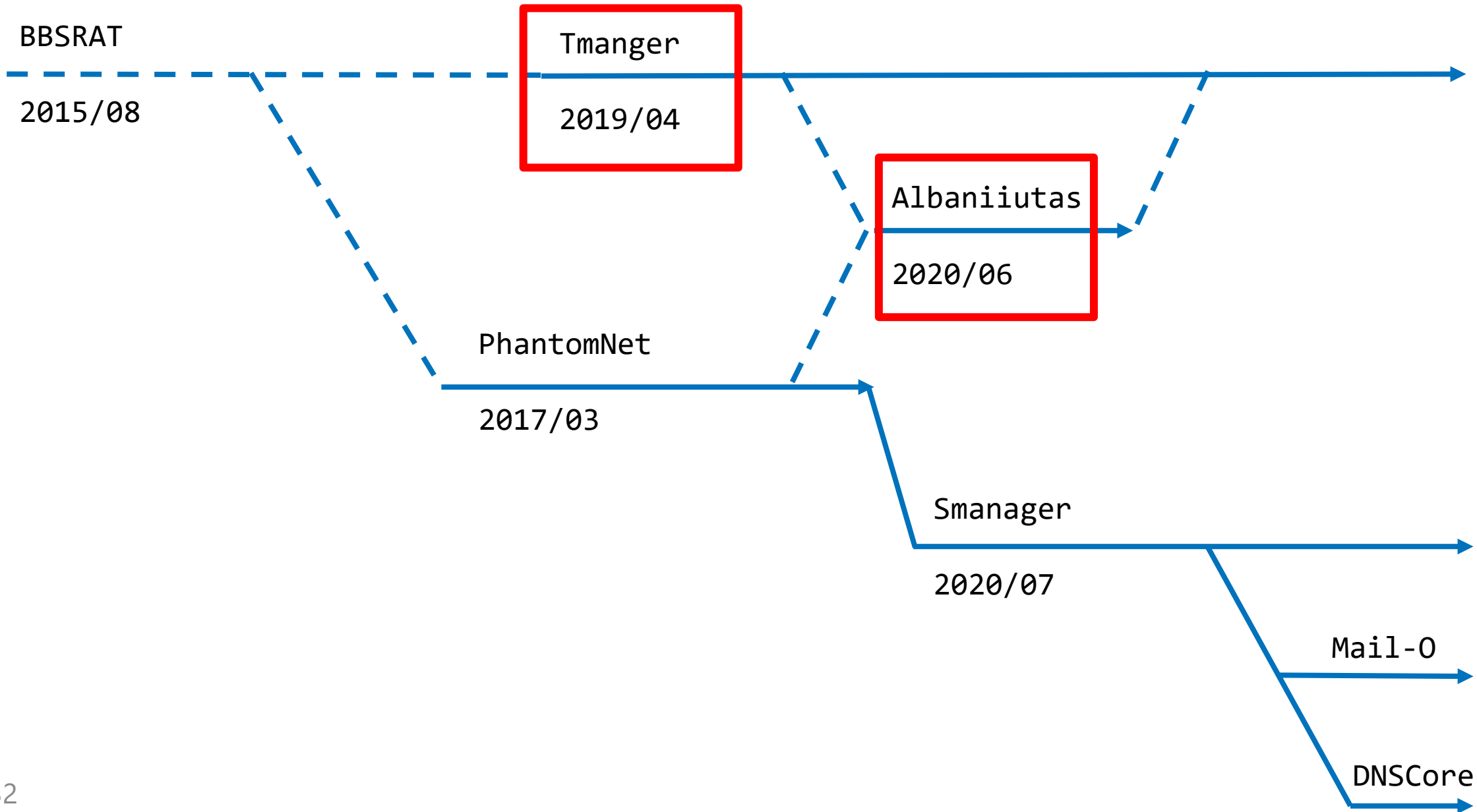




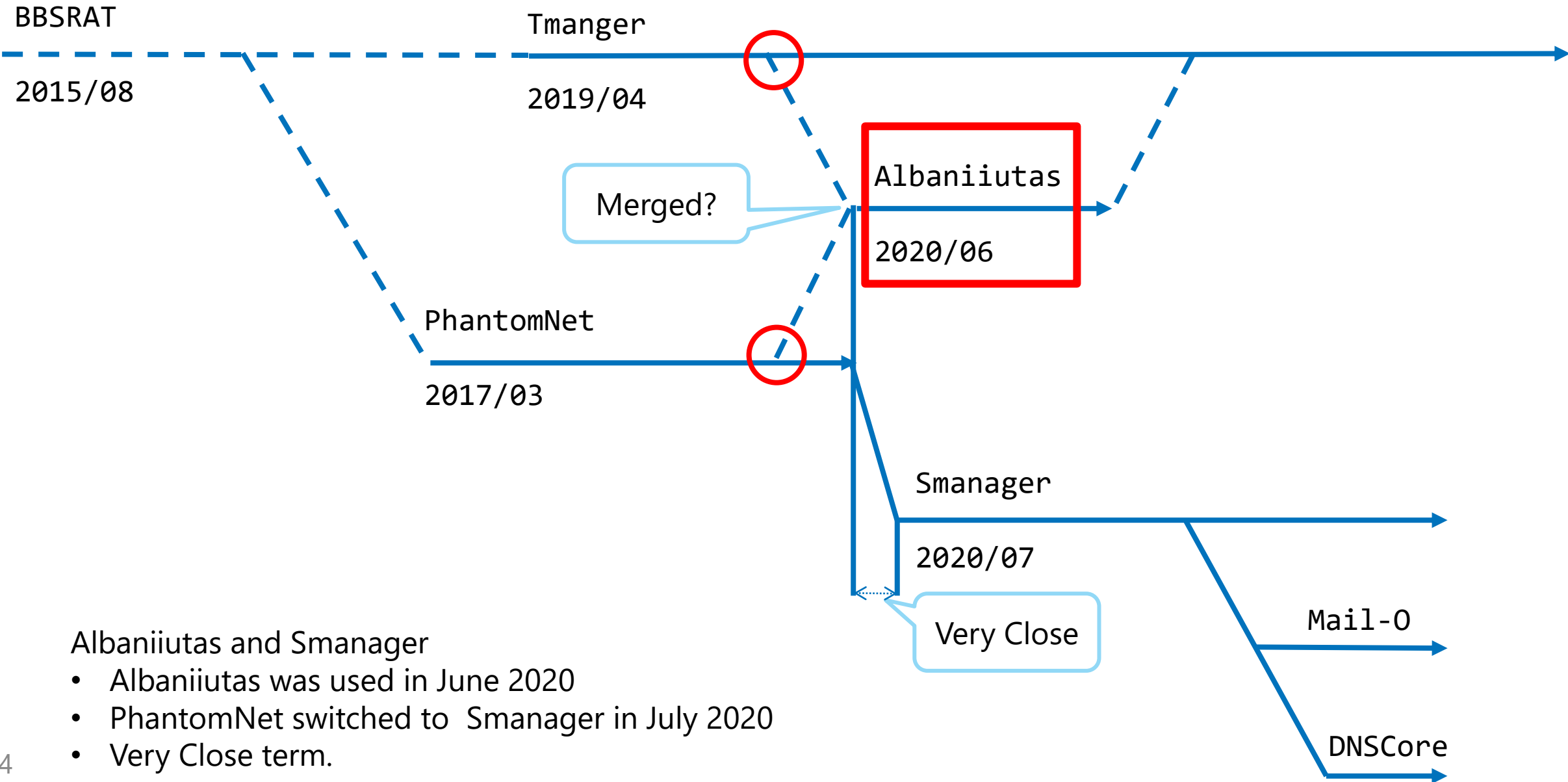
- Same Mutex as PhantomNet
- Export function name 'Entery' might come from 'Enter'?



- PhantomNet might target at organization in US or Singapore until June 2020.
- PhantomNet disappeared after Smanager had started appearing
- Smanager has similar implementations to PhantomNet



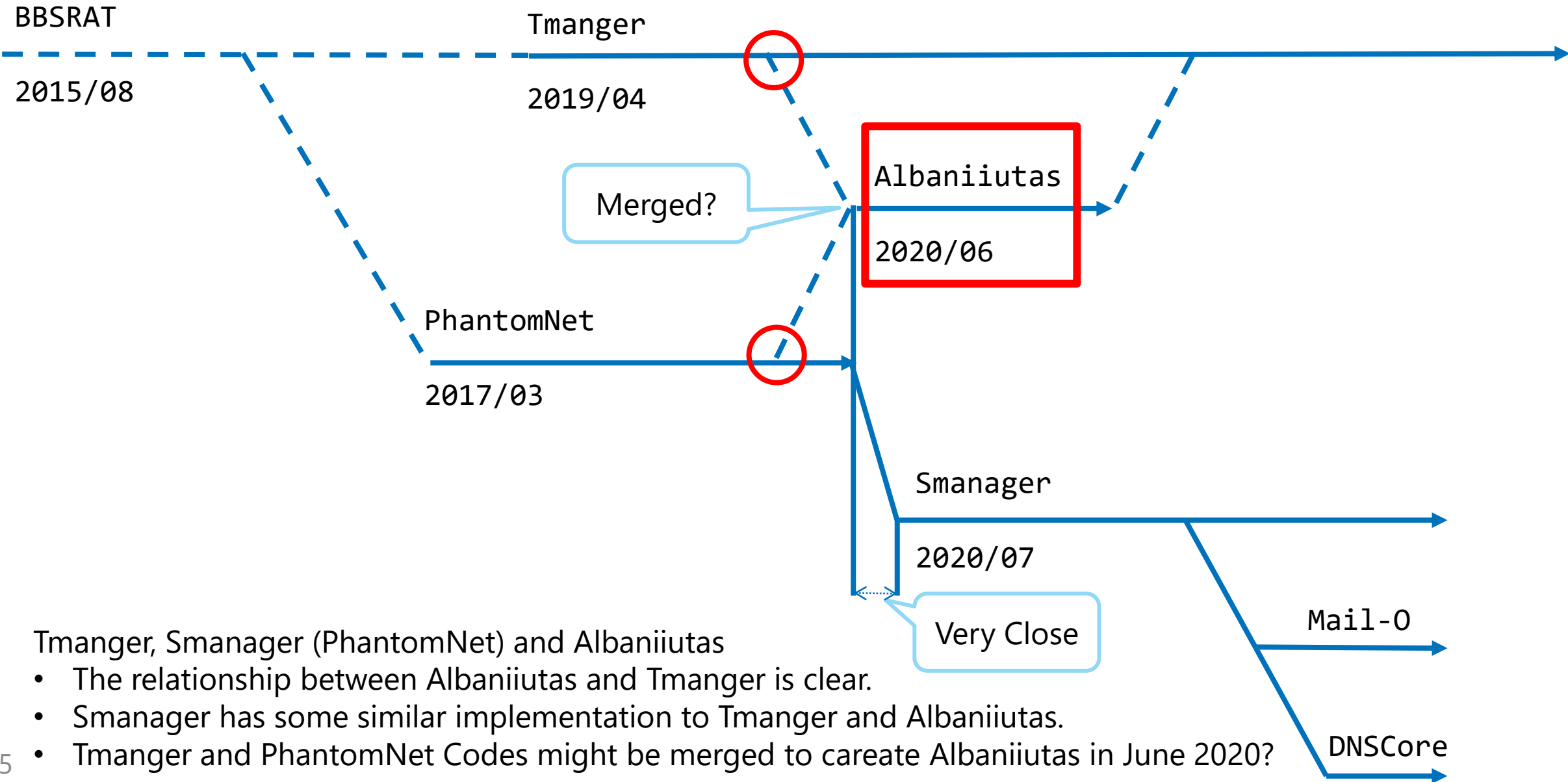
Name	Timestamp	Version	PDB
Tmanger	2025-08-19	1.0	C:\Users\Waston\Desktop\20190403_Tmanger\20191118 TM_NEW 1.0\Release\MloadDll.pdb
Tmanger	2025-10-05	4.4	C:\Users\Waston\Desktop\20190403_Tmanger\20191118 TM_NEW 4.4\Release\MloadDll_REG.pd
Tmanger	2025-10-06	4.5	C:\Users\Waston\Desktop\20190403_Tmanger\20191118 TM_NEW 4.5\Release\MloadDll_REG_DLL.pdb
Tmanger	2020-03-16	4.5	C:\Users\sxpolaris\Desktop\2020\TM VS2015\TM_NEW 4.5\ Release\MloadDll.pdb
Albaniutas	2025-12-10		
Tmanger	2026-04-23	6.2	



Albaniiutas and Smanager

- Albaniiutas was used in June 2020
- PhantomNet switched to Smanager in July 2020
- Very Close term.

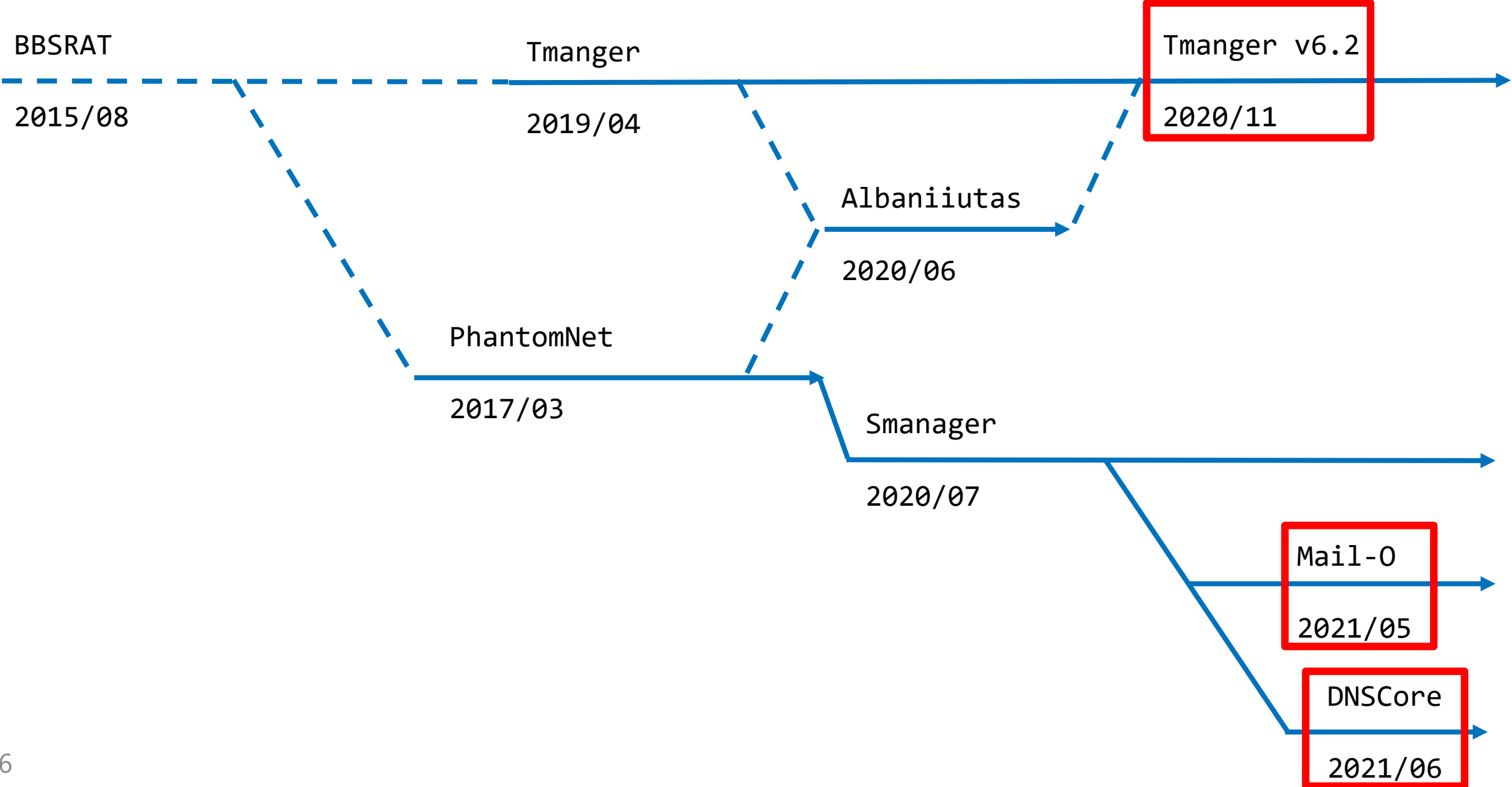
Origin of Albaniiutas



Tmanger, Smanager (PhantomNet) and Albaniiutas

- The relationship between Albaniiutas and Tmanger is clear.
- Smanager has some similar implementation to Tmanger and Albaniiutas.
- Tmanger and PhantomNet Codes might be merged to create Albaniiutas in June 2020?

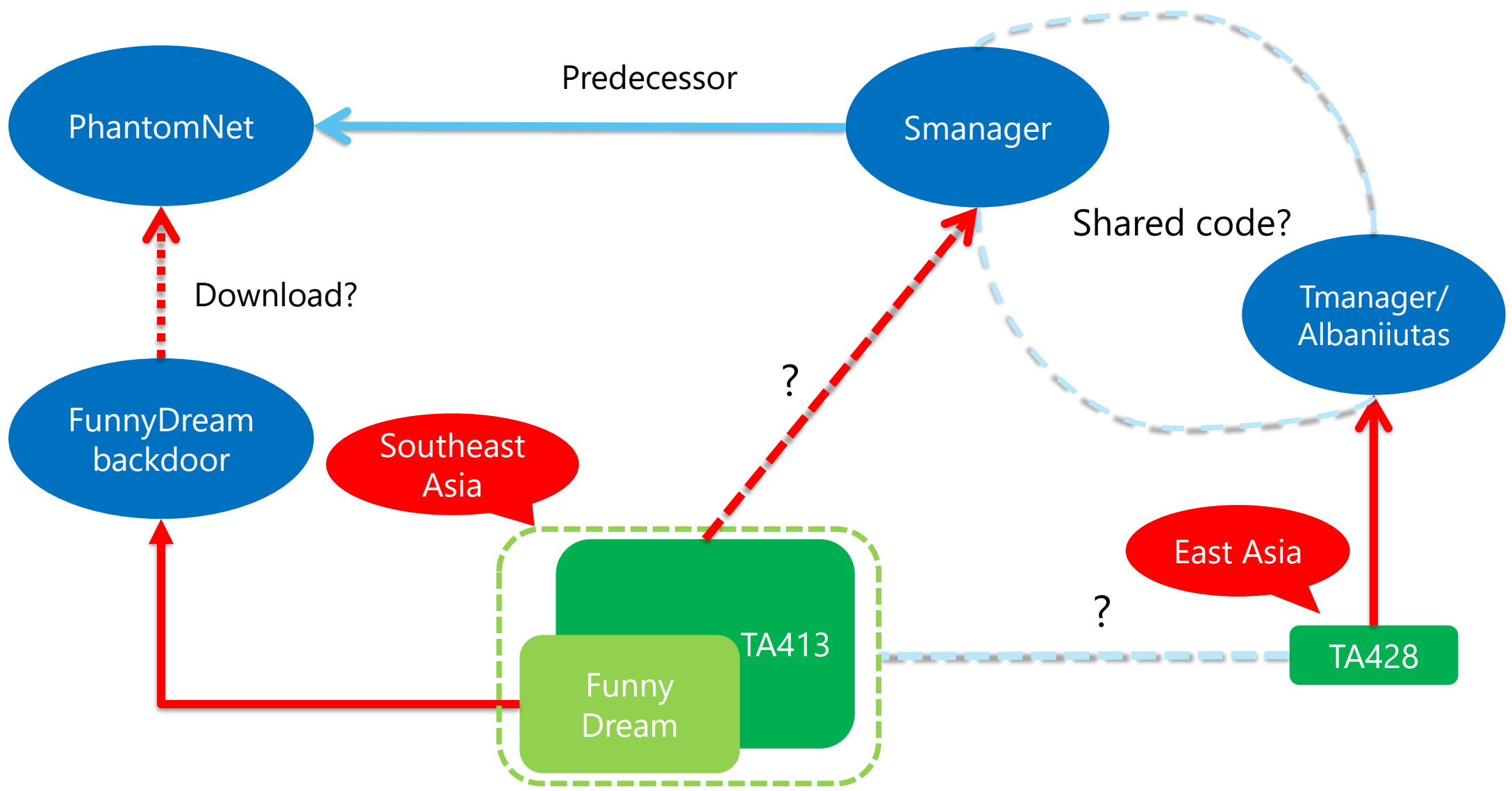
Tmanger nowadays...



Attribution & Relationship

When	Group	Campaign	Target	Attack Vector	Malware
February 2020	TA428	Operation Lag Time IT	Mongolia	Spear Phishing -> Royal Road RTF Weaponizer	<u>Tmagner</u>
June 2020	LuckyMouse	N/A	Mongolia	Spear Phishing -> fake software	<u>Tmanger</u> , Albaniitutas
June 2020	LuckyMouse	Operation StealthyTrident	Mongolia	Supply Chain	<u>Tmanger</u>
July 2020	N/A	Operation SignSight	Vietnam	Supply Chain	Smanager

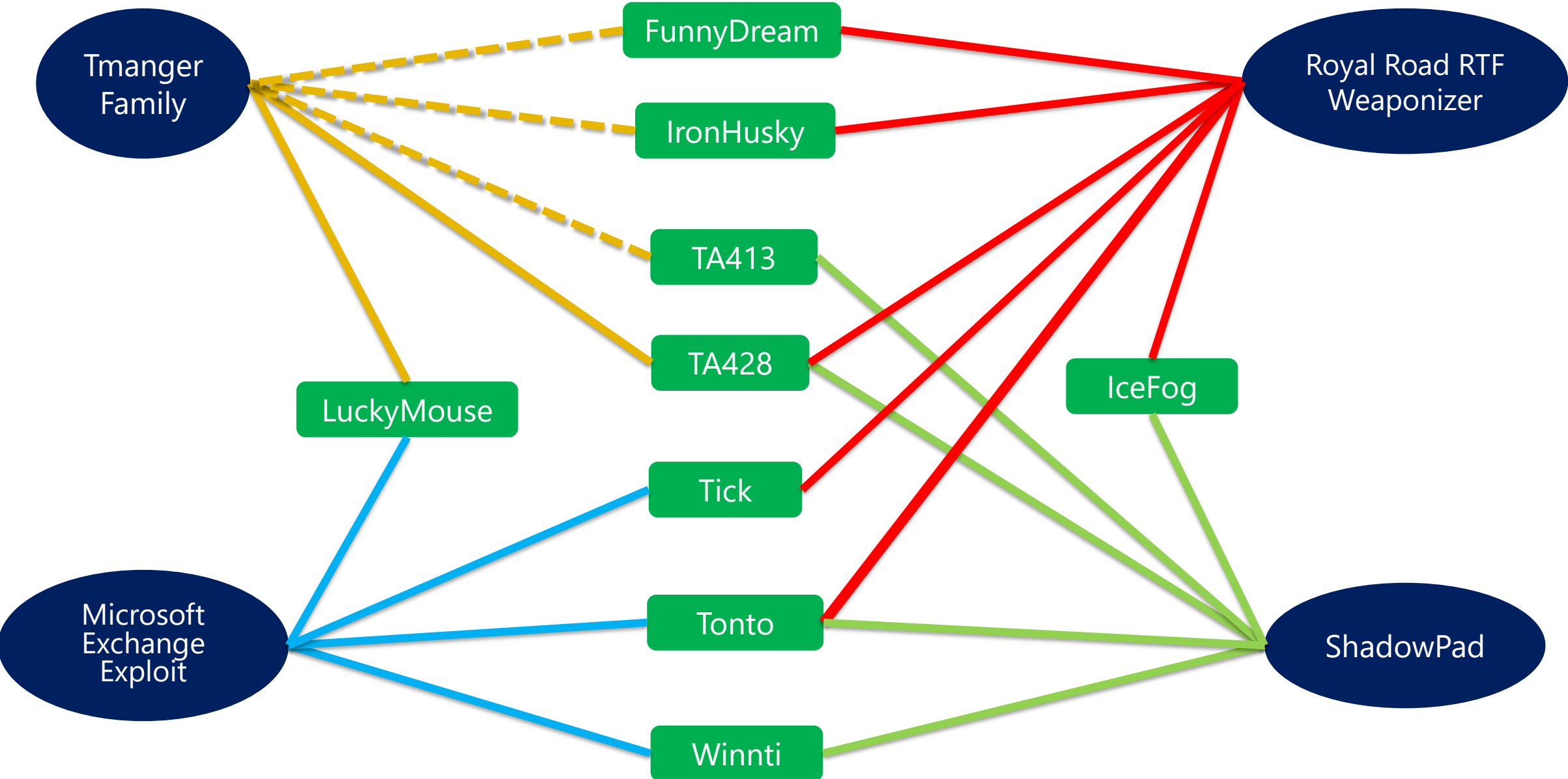
When	Group	Campaign	Target	Attack Vector	Malware
February 2020	TA428	Operation Lag Time IT	Mongolia	Spear Phishing -> Royal Road RTF Weaponizer	Tmagner
June 2020	LuckyMouse	N/A	Mongolia	Spear Phishing -> fake software	Tmanger, Albaniitutas
June 2020	LuckyMouse	Operation StealthyTrident	Mongolia	Supply Chain	Tmanger
July 2020	N/A	Operation SignSight	Vietnam	Supply Chain	Smanager



Roaming Tiger may be close to TA428

- BBSRAT has same mutex with old PhantomNet
- 'Entery' may come from BBSRAT 'Enter'
- Both targets are East Asian countries (Russia, Mongolia, etc.)

```
int32_t main (void) {
    a1 = fcn_00402b80 ();
    if (a1 == 0) {
        goto label_1;
    }
    eax = uint32_t (*CreateMutexA)(void, void, char*) (0, 0, "Global\\GlobalAcprotectMutex");
    if (eax == 0) {
        goto label_1;
    }
    eax = uint32_t (*GetLastError)() ();
    if (eax == 0xb7) {
        goto label_1;
    }
}
```



Wrap-up

Pay attention to Supply Chain attack cases

- Check carefully limited specific software
- Region-specific supply chain is also an important check point.

Focus on the attributes (Especially Chinese APT groups)

- Check the shared tools like Tmanger and Royal Road RTF Weaponizer

Research carefully following points

- Debug strings, Event names, Path names, Encryption keys, Export functions, Load process of additional modules

Analysis results of Tmanger family

- Three common elements (Setup, MloadDll and Client)
- Characteristic implementations (privilege check, 'Entery', ID calculation algorithm...)
- Characteristic Meta information (Compile time around 2025, 'Waston' pdb path...)

Researching Tmanger family and its attribution & relationship

- Past and current Tmanger family (From BBSRAT to Mail-O/DNSCore)
- Several Chinese APT groups may use and share Tmanger family
- Relationship between APT groups through Tmanger family
- Tmanger family seems to be developing day by day

Thank you

Appendix

Tmanger

- 977bd4b7e054b84b4b62e84875ff3277dd8c039cf3ee0ded435b41025d0d2b21
- 88ffb081f6924261df32322f343ccb9078ee45eaa369660892585037baf59078
- 8987b9587c1d4f6fbf2fa49eb11bb20b8b30b82d5bc988f5c882501b1f76b82a
- 85a53a2525643a84509b10d439734509203a2a74e1a167d5c3494e37a47c8c8c
- 86297be195acaa36ec042523a5484d9e14fd9fb4cbd977f709e75207358a3f86
- 5d3db73458eeeb6439ab921159ba447b01c7a12f7291eb4b5cf510e29a8137c6
- ebe05801d32985dc954e754aed63b5cee6e889f26533b1635c1f47e42bcb483a
- c60490f6fbda0a2cf1a8cd401b2f3ce9262e600268264229122a4d80e327ed4b
- 6fdd004d0835577749e8742c91e9f1720953faa8ecd55d3b203edddd4d6db5568

Tmanger

- 71fe3edbee0c27121386f9c01b723e1cfb416b7af093296bd967bbabdc706393
- 8109a33c573e00e7849ba2d63714703e2e7bd65dee1c2c6454951f7fc4b2f275
- 7807c0177cf37bce6e38ef534f804935f505a24d735baa53a18e2da766ec136b
- 4fcb79a73f5286ed8f2bc671b64c76dac4971a0cce10936f63d210e8e17c5fd5
- e494c8916e93295338a7368f86c42fce0916b559e63d462bd1b3265b6009bf9b
- d4b339f502119d4cf10d48c8c7297bbaebb22387eb7cc4447540b666d27ba166
- 078498d02775b64c5660ccbdfd12f31f3b810ed612e10c3dd50660cfa03ad470
- afd457592715bdef21d02c4e4d0e80dd70cf801a9d4d9afed795494012994372
- 772e69b3d66ef5b4fdda49d3ca39a5459b8c3afce77c24ebda698aef5bdbbc5c3
- 8e9fc7bd0673a88a04583dda7d42f278013aa7abc4e26de86e953cc4a6825708
- 2999e5209cf1d7fb484832278e11e4c4950ef40e8f52a44329ed4230135f9b64

Albaniutas

- 5eb4a19fbd25ecdabf2a456a23251f13fa938400cb32cfe87a62e8c168f9b841
- 29152de94199d77b0da9fc89d5b80bd4692f4aadf9e8362a2aee0a3b455c4e76
- fd43fa2e70bcc3b602363667560494229287bf4716638477889ae3f816efc705
- cf36344673a036f5a96c1c63230c9c15bb5e4f440eafd4ba0dc01d44bb1df3bf
- d94f404b2b5bafa0d9ce66219b2684186715f5ef20a69f036a06d465177d5769
- 71750c58eee35107db1a8e4d583f3b1a918dbffbd42a6c870b100a98fd0342e0

Smanager / PhantomNet

- f659b269fbe4128588f7a2fa4d6022cc74e508d28eee05c5aff26cc23b7bd1a5
- 1d9bc6939e2eceb3e912f158e05e04cadc1965849c4eb2c96e37e51a7d4f7aa5
- 97a5fe1d2174e9d34cee8c1d6751bf01f99d8f40b1ae0bce205b8f2f0483225c
- 02f1244310dd527d407ebcef07c5431306c56c1b28272b8d4e59902b3df537c8
- c129d892a5e2d17c38950fdf77a0838edc1fa297a4787414e90906f7cb8f43b8
- 1fff4faa83678564aefb30363f0cbe2917d2a037d3d8e829a496e8fd1eca24c9

Smanager / PhantomNet

- 58012504861dee4663ecaa4f2b93ca245521103f4c653b2dd0032a583db8f0af
- 17bc9b7c7df4acd42e795591731e568cb040d6908d892f853af777d5f05c8806
- 338502691f6861ae54e651a25a08e62eeca9febc6830978a670d44caf3d5d056
- d5f96b3b677ac68e45d4297e392b14a52678c2758a4030d2f6ad158027508c6d
- 00badf016953ec740b61f4ba27c5886a6460f6abba98819e00bde51574e0ebf4
- e8156ec1706716cada6f57b6b8ccc9fb0eb5debe906ac45bdc2b26099695b8f5
- feaba29072531b312e3bd0152b9c17c48901db7c8d31019944e453ca9b1572e2