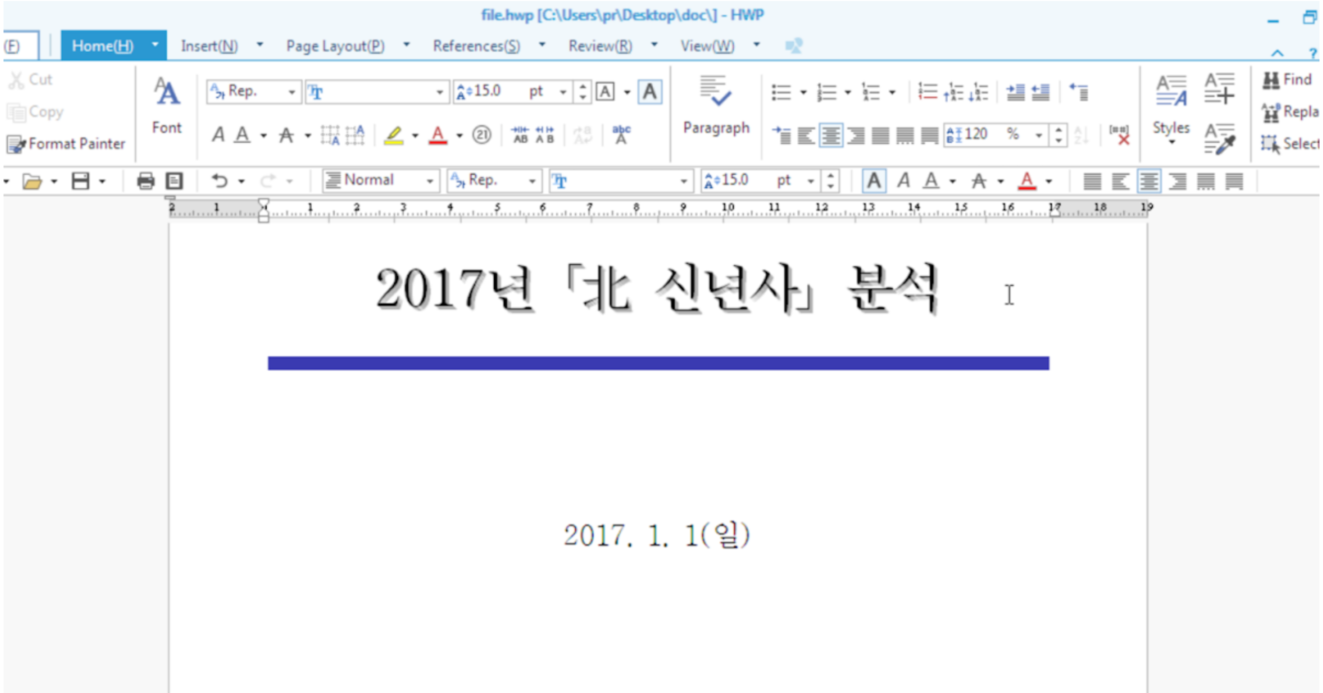
Korean MalDoc Drops Evil New Years Presents

blog.talosintelligence.com/2017/02/korean-maldoc.html



2017년「北 신년사」 분석

2017. 1. 1(일)

This blog was authored by Warren Mercer and Paul Rascagneres.

Executive Summary

Talos has investigated a targeted malware campaign against South Korean users. The campaign was active between November 2016 and January 2017, targeting a limited number of people. The infection vector is a Hangul Word Processor document (HWP), a popular alternative to Microsoft Office for South Korean users developed by Hancom.

The malicious document in question is written in Korean with the following title:

> 5170101-17년_북한_신년사_분석.hwp (translation: 5170101-17 __ North Korea _ New Year _ analysis .hwp)

This document was alleged to be written by the Korean Ministry of Unification and included their logo as a footer on the document.

An interesting twist also came within the analysed malicious document as it attempts to download a file from an official Korean government website: kgls.or.kr (Korean Government Legal Service). The file downloaded is a binary masquerading as a jpeg file that is later executed as part of the infection. It's likely that the website was compromised by the attackers to try and legitimise the HTTP GET attempts for the final payload, this traffic would potentially not have looked unfamiliar for any system administrators.

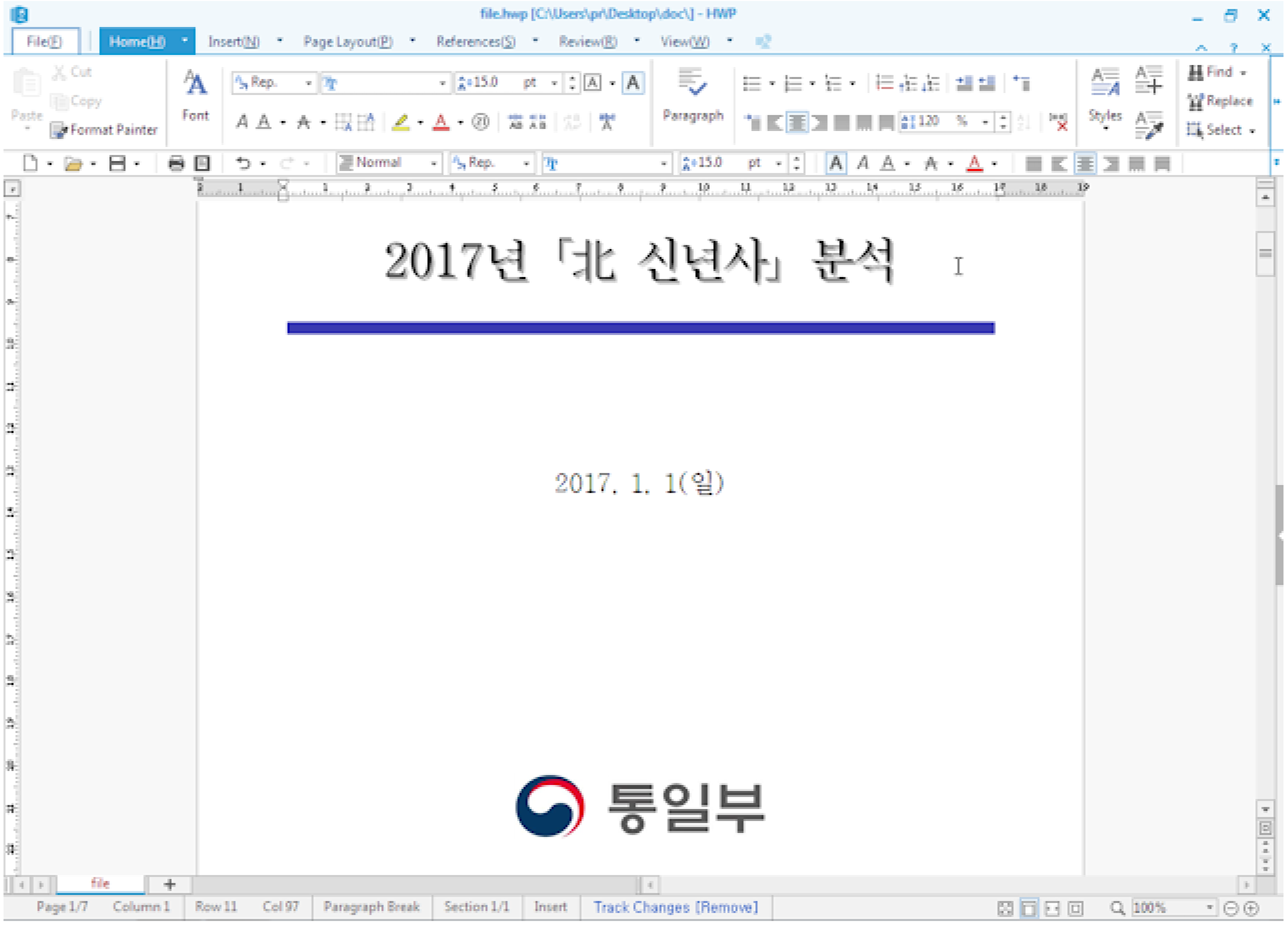
The attackers' infrastructure appeared to be up for a few days at a time with no observed infrastructure re-use occurring. Unfortunately, the compromised sites were all either cleaned or removed by the attackers and Talos were unable to obtain the final payload. This level of operational security is common for sophisticated attackers.

Due to these elements it's likely that this loader has been designed by a well-funded group in order to target public sector entities in South Korea. Many of these techniques fit the profile of campaigns previously associated with attacks by certain government groups.

Infection Vector: Hangul Word Processor

The infection vector identified by Talos is a HWP file. This is a fairly unusual choice as this software is rarely used outside of Korea, but it is known to be widely used within Korea, including use by the South Korean government. As a regional file format, many security devices are not equipped to process HWP files. This can allow an attacker a vector with a much lower risk of detection by any security scanning devices.

Here is a screenshot of the opened document:



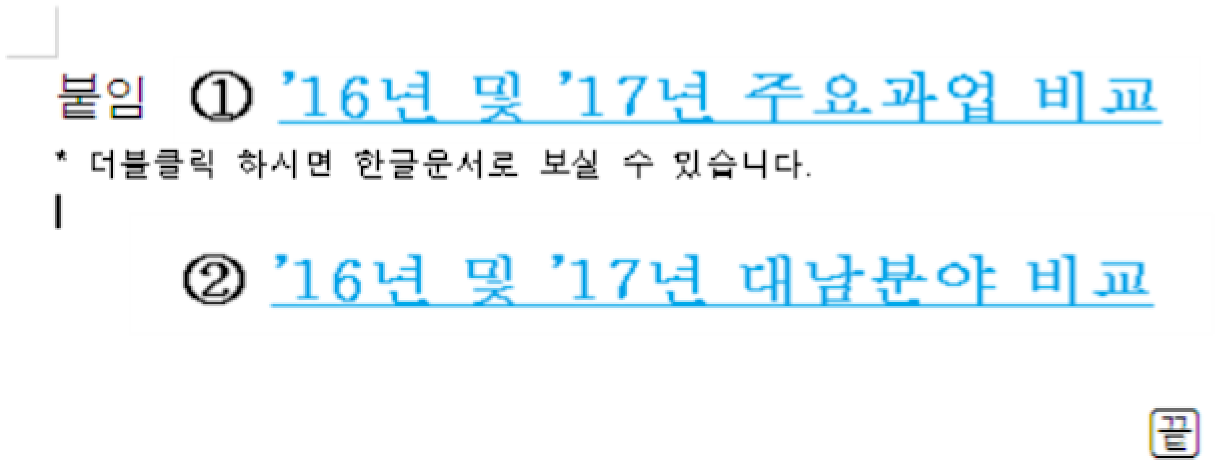
2017년 「北 신년사」 분석

2017. 1. 1(일)

통일부

The title of the document is "Analysis of "Northern New Year" in 2017". The logo at the bottom of the document in the logo of the Ministry Of Unification. This ministry is working towards the reunification of North & South Korea. The document describes information linked to the North Korean celebration of New Year.

At the end of the document are 2 links to additional documents. The malicious document mentions that users should double click in order to access to these documents, Document1 is identified as "Comparison of Major Tasks in '16 & '17" and the Document2 linked is identified as "Comparison between '16 & '17"



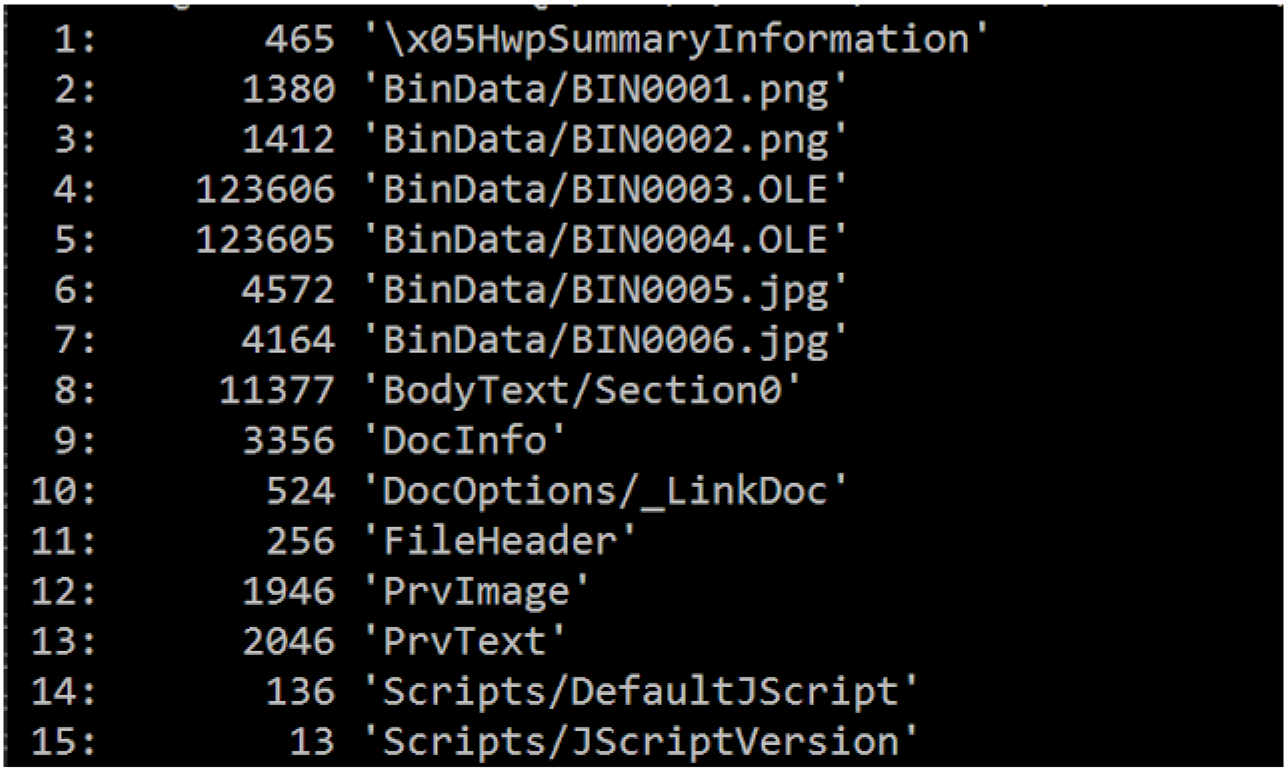
붙임 ① ’16년 및 ’17년 주요과업 비교

* 더블클릭 하시면 한글문서로 보실 수 있습니다.

② ’16년 및 ’17년 대남분야 비교

끝

The links point to 2 OLE objects embedded in the document (BIN0003.OLE and BIN004.OLE):



```
  1:       465 '\x05HwpSummaryInformation'
  2:      1380 'BinData/BIN0001.png'
  3:      1412 'BinData/BIN0002.png'
  4:    123606 'BinData/BIN0003.OLE'
  5:    123605 'BinData/BIN0004.OLE'
  6:      4572 'BinData/BIN0005.jpg'
  7:      4164 'BinData/BIN0006.jpg'
  8:     11377 'BodyText/Section0'
  9:      3356 'DocInfo'
 10:       524 'DocOptions/_LinkDoc'
 11:       256 'FileHeader'
 12:      1946 'PrvImage'
 13:      2046 'PrvText'
 14:       136 'Scripts/DefaultJScript'
 15:        13 'Scripts/JScriptVersion'
```

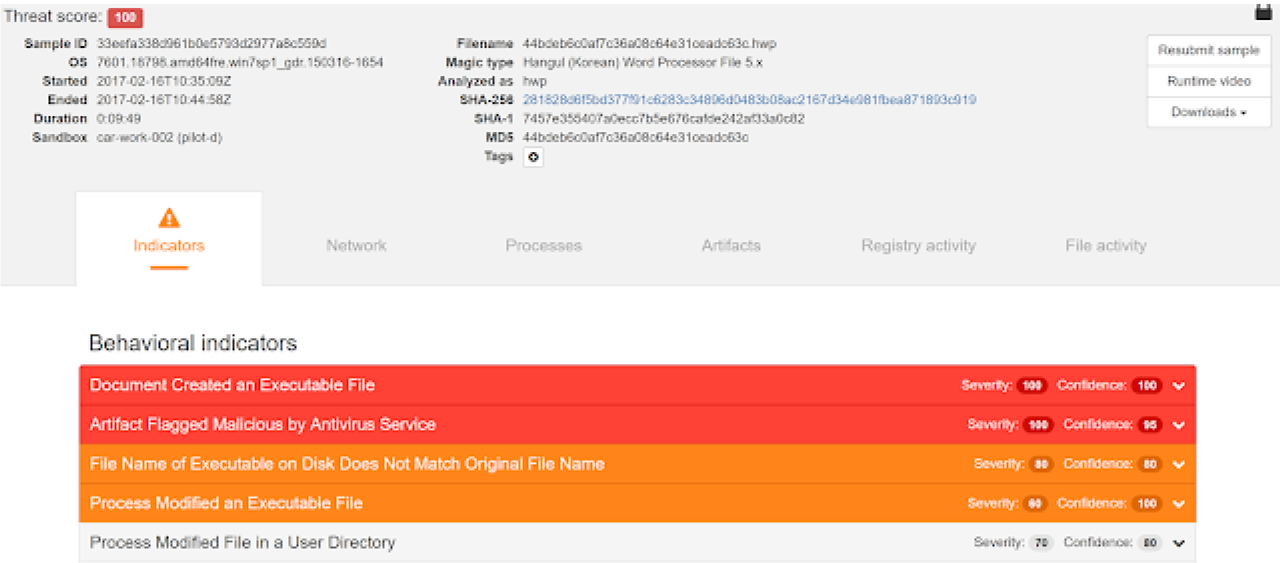
Once decompressed (zlib), we identified two PE32 files embedded within the 2 OLE files. If the targeted user double clicks on one of the links, a PE32 file is dropped and executed.

The 2 dropped binaries will be found and executed in this location during our analysis:

- C:\Users\ADMINI~1\AppData\Local\Temp\Hwp (2).exe
- C:\Users\ADMINI~1\AppData\Local\Temp\Hwp (3).exe

We can identify a JavaScript object in the document. This one does not contain malicious content, it's an object included by default.

Here is the execution of the HWP file in Cisco AMP Thread Grid:



Threat score: 100

Sample ID	33eefa338d961b0e5793d2977a8c559d	Filename	44bdeb6c0af7c36a08c64e31ceadc63c.hwp
OS	7601.18798.amd64fre.win7sp1_gdr.150316-1654	Magic type	Hangul (Korean) Word Processor File 5.x
Started	2017-02-16T10:35:09Z	Analyzed as	hwp
Ended	2017-02-16T10:44:58Z	SHA-256	281828d6f5bd377f91c6283c34806d0483b08ac2167d34e981fbea871893c919
Duration	0:09:49	SHA-1	7457e355407a0ecc7b5e676cafde242af33a0c82
Sandbox	car-work-002 (pilot-d)	MD5	44bdeb6c0af7c36a08c64e31ceadc63c
		Tags	

Behavioral indicators

Document Created an Executable File	Severity: 100	Confidence: 100
Artifact Flagged Malicious by Antivirus Service	Severity: 100	Confidence: 95
File Name of Executable on Disk Does Not Match Original File Name	Severity: 80	Confidence: 80
Process Modified an Executable File	Severity: 60	Confidence: 100
Process Modified File in a User Directory	Severity: 70	Confidence: 80

Dropped files

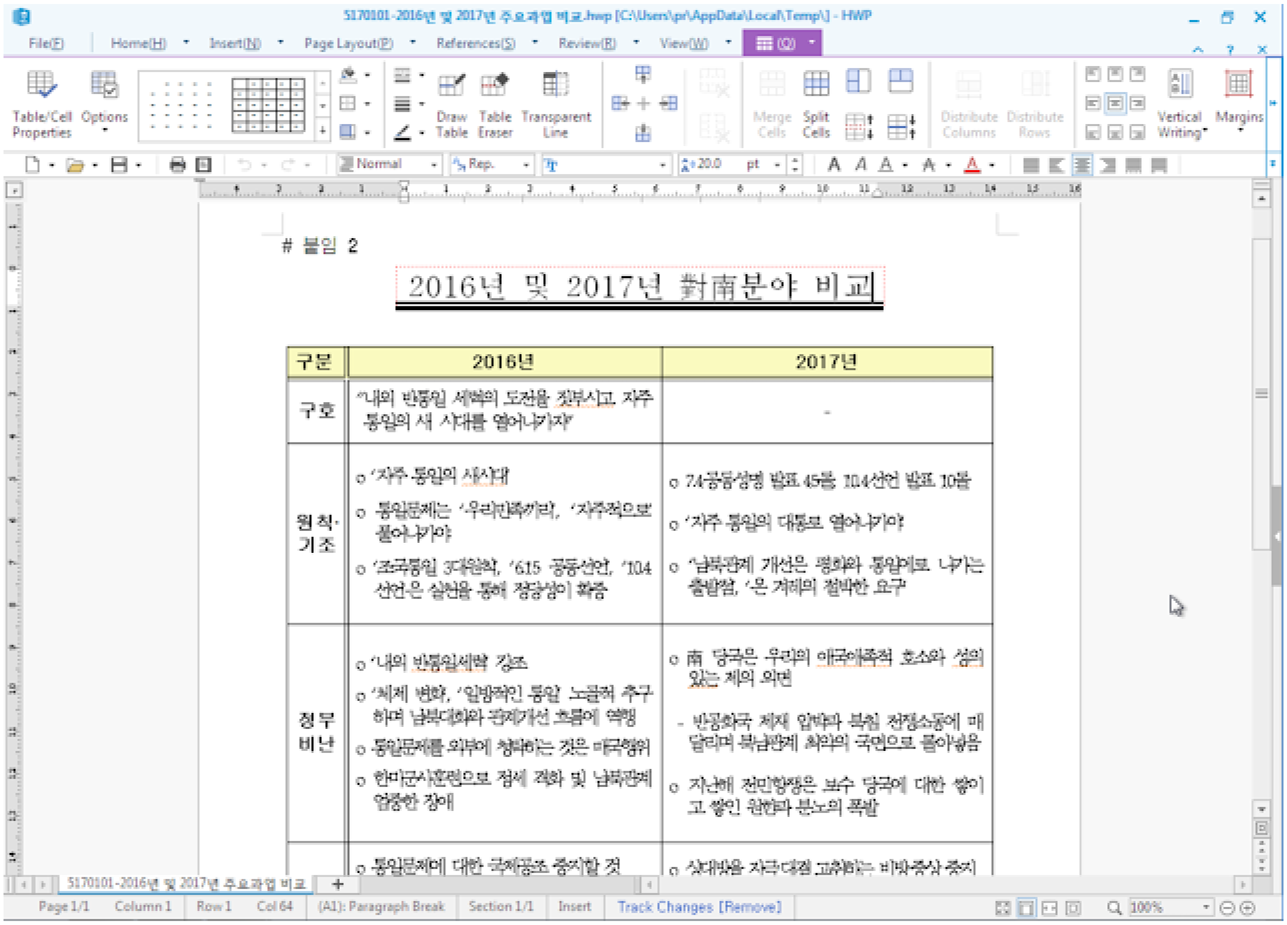
The compilation path of the binaries was not removed which allows us to determine the working space and environment used for this attack.

e:\Happy\Work\Source\version 12\T+M\Result\DocPrint.pdb

The two dropped malware files have a different hash but their purpose is the same:

- Open a HWP document (to respond to the double click in the previous document)
- Download a payload from a compromised host/C2.

The opened document is embedded in the PE (in a resource named 'DOC'):



붙임 2

2016년 및 2017년 對南분야 비교

구분	2016년	2017년
구호	"내외 반통일 세력의 도전을 짓부시고 자주통일의 새 시대를 열어나가자"	-
원칙·기조	○ '자주 통일의 새시대' ○ 통일문제는 '우리민족끼리', '자주적으로 풀어나가야' ○ '조국통일 3대원칙, '6.15 공동선언, '10.4 선언'은 실천을 통해 정당성이 확증	○ 7.4공동성명 발표 45돌 10.4선언 발표 10돌 ○ '자주 통일의 대통로 열어나가야' ○ '남북관계 개선은 평화와 통일에로 나가는 출발점, '은 겨레의 절박한 요구
정부비난	○ '내외 반통일세력' 강조 ○ '체제 변화, '일방적인 통일' 노골적 추구하며 남북대화와 관계개선 흐름에 역행 ○ 통일문제를 외부에 청탁하는 것은 매국행위 ○ 한미군사훈련으로 정세 격화 및 남북관계 엄중한 장애	○ 南 당국은 우리의 애국애족적 호소와 성의 있는 제의 외면 - 반공화국 제재 압박과 북침 전쟁소동에 매달리며 북남관계 최악의 국면으로 몰아넣음 ○ 지난해 전민항쟁은 보수 당국에 대한 쌓이고 쌓인 원한과 분노의 폭발
	○ 통일문제에 대한 국제공조 중지할 것	○ 상대방을 자극대결 고취하는 비방중상 중지

Like the previous document, this one speaks of the relation between North Korea and South Korea, and is seemingly written by a native Korean speaker due to the specific language used.

The second stage of the binary executes wscript.exe and injects shellcode into the process. The shellcode is embedded in a resource called 'BIN'. The purpose of this shellcode is to unpack a second PE32 in the legitimate wscript.exe process and execute it. The injection is perform by the classic:
VirtualAllocEx(), WriteProcessMemory() and CreateRemoteThread() APIs.

The unpacked binary is used to collect information on the infected system, and to attempt to communicate with the C2 in order to download the final payload. The information collected was:

- The computer name
- The username
- The execution path of the sample
- The BIOS model by analysing the HKLM\System\CurrentControlSet\Services\mssmbios\Data\SMBiosData registry key. This information allows the attackers to identify Virtual Machine (on VirtualBox the model is "innotek GmbH VirtualBox")

- An ID randomly generated to identify the system

This information could be used as a reconnaissance phase to determine if there was a suitable platform to deliver the final payload and to avoid sending the final payload to sandbox systems.

The analysed sample performed network connections to these 2 URLs in this order:

- www.kgls.or.kr/news2/news_dir/index.php (where the collected information is sent)
- www.kgls.or.kr/news2/news_dir/02BC6B26_put.jpg

The beginning of the jpg document (02BC6B26) is the ID previously generated. We think that the jpg file is automatically generated by the index.php file if the collected data is relevant. The content of the jpg file is saved in a file called 'officepatch.exe'. Finally, this new file is executed and the unpacked executable terminates itself.

The website kgls.or.kr is the web site of the Korean Government Legal Service. Talos can only assume that this website was compromised in order to deliver the final stage malware, the jpg file. All the infrastructure was down during our analysis, which meant we were unable to analyse the payload directly.

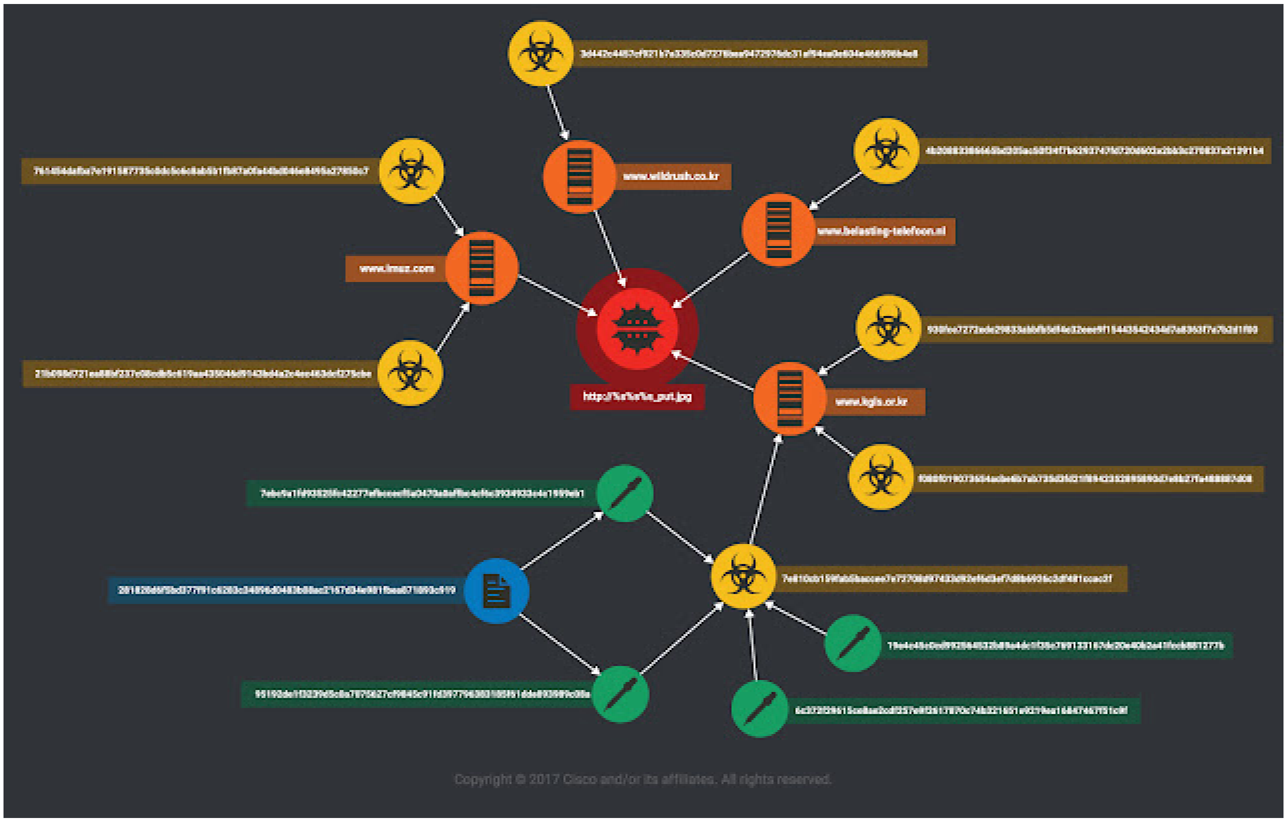
The collected binaries are compiled between 22:43:05 UTC and 4:55:18 UTC (the 3 files at 22:00:00 are the binaries dropped by the HWP document and the other files are the unpacked payload) - Time Stamp artifacts can be easily faked and can be deployed as a false flag mechanism to make the researcher believe the compiled code came from a certain Time Zone - this should not be trusted as an indicator of where the attack or attacker originated from.

Command & Control infrastructure

During our investigation we were able to identify additional Command and Control infrastructure used by this actor. The four C2s were based in the following countries:

- 3 C2 in South Korea
- 1 C2 in the Netherlands

Here is a global map of the identified infrastructure:


www.wildrush.co.kr
www.imuz.com
www.belasting-telefoon.nl
http://%s%s%s_put.jpg
www.kgls.or.kr
Copyright © 2017 Cisco and/or its affiliates. All rights reserved.

Colour Key:

- Red: the '_put.jpg' binary (final payload)
- Orange: C2 infrastructure used by the attackers
- Yellow: the unpacked samples that perform the connection to download the final malware (the green bubbles share 90% of similar codes)
- Green: the dropped executable by the HWP document (the orange bubbles share 90% of similar codes)
- Blue: the HWP document

Conclusion

This actor appears to have made intentional decisions to limit the attack surface by using Hangul. This allowed them to evade some security devices as this format is not frequently processed.

The infection process was a MalDoc with multiple droppers (identical in their execution) and then C2 communication to obtain the final payload. The use of decoy documents is very common and shows that the attacker wanted to use a social engineering / enticement aspect to encourage the users to open the file.

This campaign has clearly targeted at a specific group of users, this rings true with the use of such specific file formats. Steps were clearly taken to limit the ability of security products to detect the threat as well as adherence to a strict timeline to prevent the malicious files from being discovered. The attackers were careful to remove their malicious payloads and not re-use their infrastructure.

We believe this is a targeted attack aimed at South Korean users in the public sector conducted by a sophisticated threat actor with access to native Korean speakers. Attacks on these individuals may be an attempt to gain a foothold into assets which can be deemed extremely valuable.

IOC

HWP File:

5170101-17년_북한_신년사_분석.hwp:
281828d6f5bd377f91c6283c34896d0483b08ac2167d34e981fbea871893c919

Dropped files:

95192de1f3239d5c0a7075627cf9845c91fd397796383185f61dde893989c08a
7ebc9a1fd93525fc42277efbccecf5a0470a0affbc4cf6c3934933c4c1959eb1
6c372f29615ce8ae2cdf257e9f2617870c74b321651e9219ea16847467f51c9f
19e4c45c0cd992564532b89a4dc1f35c769133167dc20e40b2a41fccb881277b
3a0fc4cc145eafe20129e9c53aac424e429597a58682605128b3656c3ab0a409
7d8008028488edd26e665a3d4f70576cc02c237fffe5b8493842def528d6a1d8

Unpack related samples:

7e810cb159fab5baccee7e72708d97433d92ef6d3ef7d8b6926c2df481ccac2f
21b098d721ea88bf237c08cdb5c619aa435046d9143bd4a2c4ec463dcf275cbe
761454dafba7e191587735c0dc5c6c8ab5b1fb87a0fa44bd046e8495a27850c7
3d442c4457cf921b7a335c0d7276bea9472976dc31af94ea0e604e466596b4e8
930fce7272ede29833abbfb5df4e32eee9f15443542434d7a8363f7a7b2d1f00
4b20883386665bd205ac50f34f7b6293747fd720d602e2bb3c270837a21291b4
f080f019073654acbe6b7ab735d3fd21f8942352895890d7e8b27fa488887d08

Network:

www.imuz.com/admin/data/bbs/review2/board/index.php
www.imuz.com/admin/data/bbs/review2/board/123.php
www.imuz.com/admin/data/bbs/review2/board/02BC6B26_put.jpg (where 02BC6B26 is randomly generated)

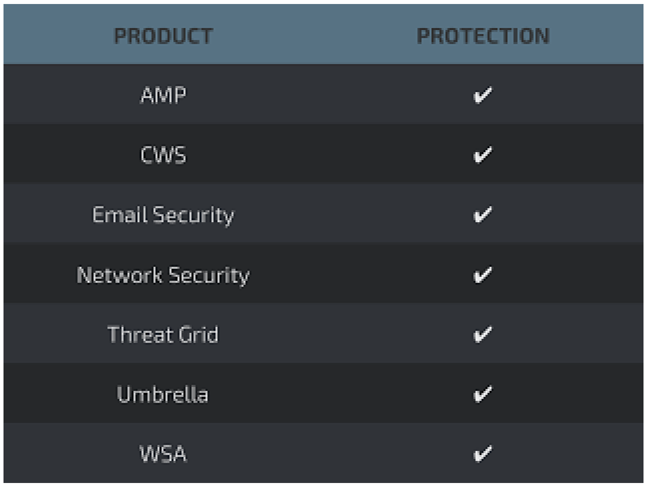
www.wildrush.co.kr/bbs/data/image/work/webproxy.php
www.wildrush.co.kr/bbs/data/image/work/02BC6B26_put.jpg (where 02BC6B26 is randomly generated)

www.belasting-telefoon.nl//images/banners/temp/index.php
www.belasting-telefoon.nl//images/banners/temp/02BC6B26_put.jpg (where 02BC6B26 is randomly generated)

www.kgls.or.kr/news2/news_dir/index.php
www.kgls.or.kr/news2/news_dir/02BC6B26_put.jpg (where 02BC6B26 is randomly generated)

Coverage

Additional ways our customers can detect and block this threat are listed below.



PRODUCT	PROTECTION
AMP	✔
CWS	✔
Email Security	✔
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

CWS orWSA web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

The Network Security protection ofIPS andNGFW have up-to-date signatures to detect malicious network activity by threat actors.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella prevents DNS resolution of the domains associated with malicious activity.