MALWARE ANALYSIS REPORT

No.16 | 2018 년 11 월

# Lazarus APT 분석

(주) 소만사 악성코드 분석 센터

# 목 차

# 1. 보도자료

## 또 등장한 라자루스, 최신 APT 작전 '배틀 크루저' 포착

2018-10-24

**보안·IT 전문 변호사 사칭 한글파일로 공격...정상적인 문서파일 출력해 위장**

[보안뉴스 원병철 기자] 지난 4월 라자루스의 최신 APT 공격으로 알려졌던 '배틀 크루저(Operation Battle Cruiser)'가 6개월 만에 재등장해 보안관계자들의 관심을 받고 있다.

지난 3월 달에 제작된 오퍼레이션 배틀 크루저의 다운로드 파일은 'battle32.avi', 'battle64.avi' 이름이 사용됐고, 4월 제작된 '오퍼레이션 스타 크루저'의 다운로드 파일명은 'star3.avi', 'star6.avi' 형태로 변경된 특징이 있다.

이번 10월 최신 공격에는 'akism1.pgi', 'akism2.pgi' 등으로 파일명과 확장자가 변경됐지만, 내부 익스포트 함수명은 3월과 동일한 'battle32.dll', 'battle64.dll' 이름이 그대로 사용됐다.

# 2. WebKeeper 대응

- 2018 년 10 월 N 일 NN 시 NN 분 파일 다운로드 링크 및 C2 서버 리스트 차단 완료 및 배포

[추가 파일 다운로드]

| | |
|---|---|
| OS - 32Bit | https://flydashi.com/wp-content/plugins/askism1.pgi |
| OS - 64Bit | https://flydashi.com/wp-content/plugins/askism2.pgi |

[C2 서버 리스트]

| | |
|---|---|
| 1. C2 | https://theinspectionconsultant.com/wp-content/plugins/akismet/index1.php |
| 2. C2 | http://danagloverinteriors.com/wp-content/plugins/jetpack/common.php |
| 3. C2 | https://as-brant.ru/wp-content/themes/shapely/common.php |

- 2018 년 10 월 N 일 웹키퍼 위클리를 통해 해당 내용 안내

# 3. 개 요

### 3.1 배 경

2018 년 4 월 Lazarus Group 의 최신 APT 공격으로 알려진
'작전명 스타 크루저(Operation Battle Cruiser)'가 6 개월 만에 다시 등장했다.
Lazarus 는 북한 정찰총국의 해커 부대로 소니 픽처스 공격의 주범이다.
최근 국내 특정 대상을 목표로 APT 공격을 수행 중이며,
악성코드가 들어있는 '한글'(HWP) 파일을
정상적인 '한글'(HWP) 파일로 위장해 이메일에 첨부, 발송한다.

### 3.2 파일 정보

| Name | **국가핵심인력등록관리제등검토요청(10.16)(김경환변호사).hwp** |
|---|---|
| Type | HWP (한글문서) |
| Behavior | Trojan.Exploit |
| SHA-256 | b2dd7f9bb24428b0e2ed30b9373fe033d981a29415576b4c654c0d999dd109e5 |
| Description | 악성 쉘 스크립트를 포함한 한글 문서 |

| Name | **akism1.pgi** |
|---|---|
| Type | PGI |
| Behavior | Backdoor |
| SHA-256 | 1ff597e8bd590896c17d856188d1f0950a5a4cf4e7d2c0b40a6c1eb95c9586b3 |
| Description | 악성코드 배포 서버로 부터 다운로드 되는 인코딩 된 악성코드 1 |

| Name | **akism2.pgi** |
|---|---|
| Type | PGI |
| Behavior | Backdoor |
| SHA-256 | 60b56eff7fbc2413d1b755e8b3f2f4e94d000448a3cd16965c9411d88a1ac935 |
| Description | 악성코드 배포 서버로 부터 다운로드 되는 인코딩 된 악성코드 2 |

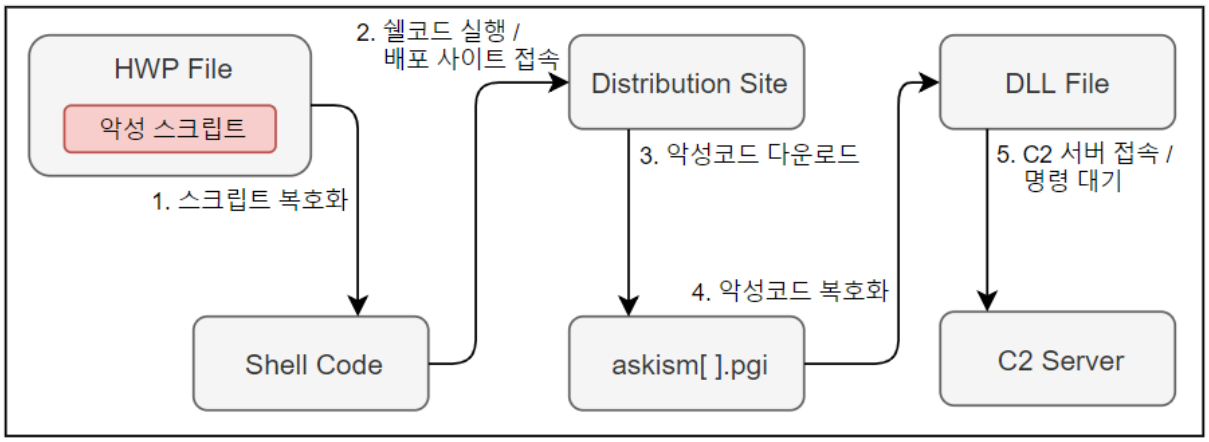
| Name | *가칭 [akism1].dll |
|---|---|
| Type | DLL |
| Behavior | Trojan.Generic |
| SHA-256 | eee38c632c62ca95b5c66f8d39a18e23b9175845560af84b6a2f69b7f9b6ec1c |
| Description | 디코딩 된 악성코드 바이너리 1 |

| Name | *가칭 [akism2].dll |
|---|---|
| Type | DLL |
| Behavior | Trojan.Generic |
| SHA-256 | f6e1a146543d2903146698da5698b2a214201720c0be756c6e8d2a2f27dcfaff |
| Description | 디코딩 된 악성코드 바이너리 2 |

# 4. 분 석

Lazarus Group 은 지난 3 월 파일명 'battle32.avi'와 'battle64.avi'로 APT 공격을 수행하였고,
4 월엔 변경된 파일명인 'star3.avi'와 'star6.avi'로 APT 공격을 수행하였다.
이번 10 월 발견된 최신 APT 공격은 'akism1.pgi'와 'akism2.pig'등으로
파일명과 확장자가 변경되었지만,
내부에 존재하는 익스포트 된 함수명이 지난 3 월과 동일한 'battle32.dll'과 'battle64.dll'이 사용되었다.

### 4.1. Lazarus APT 분석




[그림 1] Lazarus APT 프로세스

메일에 첨부되어 있는 HWP 파일 내부에는 악성 포스트 스크립트(Post Script)가 존재하며,

해당 포스트 스크립트(Post Script) 내부에 악성 쉘 코드가 포함되어 있다.
해당 파일이 실행되면 악성 포스트 스크립트(Post Script)가 실행되며,
배포 사이트로 접속 후 OS 버전에 따라 악성 파일 다운로드를 시도한다.
이후 HWP 문서 내용이 출력되며, 정상적인 문서 파일로 위장한다.

### 4.2. 제작일자

| Name | Size(B) | Created | Accessed | Modified |
|---|---|---|---|---|
| BinData | | 2018-10-21 오후 02:16... | 2018-10-21 오후 02:16:49 | 2018-10-21 오후 02:16:49 |
| BodyText | | 2018-10-21 오후 02:16... | 2018-10-21 오후 02:16:49 | 2018-10-21 오후 02:16:49 |
| DocOptions | | 2018-10-21 오후 02:16... | 2018-10-21 오후 02:16:49 | 2018-10-21 오후 02:16:49 |
| Scripts | | 2018-10-21 오후 02:16... | 2018-10-21 오후 02:16:49 | 2018-10-21 오후 02:16:49 |
| \|HwpSummaryInformation | 461 | 1601-01-01 오전 09:00... | 1601-01-01 오전 09:00:00 | 1601-01-01 오전 09:00:00 |
| DocInfo | 2589 | 1601-01-01 오전 09:00... | 1601-01-01 오전 09:00:00 | 1601-01-01 오전 09:00:00 |
| FileHeader | 256 | 1601-01-01 오전 09:00... | 1601-01-01 오전 09:00:00 | 1601-01-01 오전 09:00:00 |
| PrvImage | 33528 | 1601-01-01 오전 09:00... | 1601-01-01 오전 09:00:00 | 1601-01-01 오전 09:00:00 |
| PrvText | 2044 | 1601-01-01 오전 09:00... | 1601-01-01 오전 09:00:00 | 1601-01-01 오전 09:00:00 |

[그림 2] 악성파일 제작일자

HWP 문서 파일의 제목은 10 월 16 일자 제작으로 명시되었지만,
실제 해당 HWP 문서 파일은 10 월 21 일 제작된 것으로 확인된다.

### 4.3. 악성 포스트 스크립트(Post Script)

1) BIN0001.ps

| | | | |
|---|---|---|---|
| BIN0001.id0 | 2018-10-30 오전... | ID0 파일 | 16KB |
| BIN0001.id1 | 2018-10-30 오전... | ID1 파일 | 0KB |
| BIN0001.nam | 2018-10-30 오전... | NAM 파일 | 0KB |
| BIN0001.ps | 2018-10-29 오후... | PS 파일 | 19KB |
| BIN0001.til | 2018-10-30 오전... | TIL 파일 | 1KB |

[그림 3] 악성 PS 파일

HWP 문서 파일 내부에는 악성 포스트 스크립트(Post Script)인 'BIN0001.ps'가 포함되어있다.

2) BIN0001.ps 내부 쉘 코드

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000   CD BD DB AE 05 39 72 1D F8 2B F5 07 66 92 4C 5E  Í½Û®.9r.ø+õ.f'L^
00000010   00 C1 40 5E C8 7F D0 E3 8C D4 B2 1F 06 1E 63 2C  .Á@^È.ÐãŒÔ²...c,
00000020   19 02 0C FF FB C4 5A 11 64 32 F7 3E A7 54 1A CF  ...ÿûÄZ.d2÷>§T.Ï
00000030   83 81 46 77 75 E5 D9 99 4C 32 2E 2B 56 5C F2 3F  ƒ.FwuåÙ™L2.+V\ò?
00000040   FC FD E6 B6 3F FE CE 1F 57 B8 B7 BA E5 50 EB 5E  üýæ¶?þÎ.W¸·ºåPë^
00000050   EE 5C 53 49 DB 7D E7 A3 6E C7 7E A5 C4 EB BE 6E  î\SIÛ}ç£nÇ~¥Äë¾n
00000060   DB 59 DB 7E 76 77 F8 D3 87 A3 B4 76 6F E7 DE BD  ÛYÛ~vwøÓ‡£´voçÞ½
00000070   F3 FB B9 9F B5 F8 E4 4B 76 67 6F 67 3F 7D F6 1F  óû¹ŸµøäKvgog?}ö.
00000080   BF 8F B8 7F E9 DB D1 C2 E1 8F CD 7F 5E DF E5 BA  ¿.¸.éÛÑÂá.Í.^ßå°
00000090   97 EB BD C7 33 35 97 E3 D1 BA DC DD 9D D9 F9 74  —ë½Ç35—ãÑ°ÜÝ.Ùùt
000000A0   9C B7 2B 5B F2 D7 B9 B5 9E BB 6B DD F9 CB B5 DB  œ·+[ò×¹µž»kÝùËµÛ
```

[그림 4] BIN0001.ps 내장 압축 코드

BIN0001.ps 내부에는 위와 같은 압축된 코드가 존재하며, 이는 이후 실행될 악성 쉘 코드이다.

3) BIN0001.ps 내부 쉘 코드 압축 해제

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000   2F 59 31 30 31 20 3C 32 41 43 33 44 31 39 31 37  /Y101 <2AC3D1917
00000010   33 39 39 35 38 44 37 39 36 38 36 31 44 44 37 41  39958D796861DD7A
00000020   39 31 41 35 43 36 36 32 41 43 33 44 32 39 31 31  91A5C662AC3D2911
00000030   42 39 45 35 42 46 30 41 32 42 32 33 41 38 45 45  B9E5BF0A2B23A8EE
00000040   44 31 42 35 46 32 30 32 35 42 35 42 39 38 32 36  D1B5F2025B5B9826
00000050   32 38 37 30 42 46 45 42 46 42 32 37 32 44 37 41  2870BFEBFB272D7A
00000060   39 31 41 35 43 36 36 32 41 43 33 44 34 39 31 37  91A5C662AC3D4917
00000070   33 38 46 31 41 45 33 41 32 41 31 32 32 44 37 41  38F1AE3A2A122D7A
00000080   39 31 41 35 43 36 36 32 41 43 33 44 35 39 31 37  91A5C662AC3D5917
00000090   32 38 46 31 46 46 34 42 36 45 30 37 34 41 45 46  28F1FF4B6E074AEF
000000A0   42 35 46 30 42 37 30 32 36 41 42 44 30 38 31 36  B5F0B7026ABD0816
000000B0   32 43 42 31 45 46 37 46 30 45 46 30 32 43 30 45  2CB1EF7F0EF02C0E
```

[그림 5-1] 압축 해제된 쉘 코드

```
0000C3B0   20 64 65 66 20 30 20 31 20 59 31 30 31 20 6C 65   def 0 1 Y101 le
0000C3C0   6E 67 74 68 20 31 20 73 75 62 20 7B 20 2F 59 31  ngth 1 sub { /Y1
0000C3D0   38 20 65 78 63 68 20 64 65 66 20 59 31 30 31 20  8 exch def Y101
0000C3E0   64 75 70 20 2F 59 31 30 32 20 38 20 64 65 66 20  dup /Y102 8 def
0000C3F0   59 31 38 20 67 65 74 20 3C 30 35 39 41 45 30 42  Y18 get <059AE0B
0000C400   31 34 32 41 46 37 42 39 31 44 30 43 30 35 42 46  142AF7B91D0C05BF
0000C410   37 43 44 37 46 33 41 34 36 3E 20 59 31 38 20 31  7CD7F3A46> Y18 1
0000C420   35 20 61 6E 64 20 2F 59 31 30 34 20 38 20 64 65  5 and /Y104 8 de
0000C430   66 20 67 65 74 20 2F 59 31 30 35 20 34 20 64 65  f get /Y105 4 de
0000C440   66 20 78 6F 72 20 59 31 38 20 65 78 63 68 20 2F  f xor Y18 exch /
0000C450   59 31 30 33 20 38 20 64 65 66 20 70 75 74 7D 20  Y103 8 def put}
0000C460   66 6F 72 20 59 31 30 31 20 63 76 78 20 65 78 65  for Y101 cvx exe
0000C470   63                                               c
```

[그림 5-2] 압축 해제된 쉘 코드

압축 해제 시 쉘 코드를 확인할 수 있으며,
해당 쉘 코드는 '0x46, 0x3A, 0x7F, 0xCD, 0xF7, 0x5B, 0xC0, 0xD0, 0x91, 0x7B, 0xAF, 0x42, 0xB1, 0xE0, 0x9A, 0x05'의 16 바이트로 XOR 암호화가 되어 있음을 확인할 수 있다.

4). 쉘 코드 복호화

```
00000FB0  68 74 74 70 73 3A 2F 2F 66 6C 79 64 61 73 68 69  https://flydashi
00000FC0  2E 63 6F 6D 2F 77 70 2D 63 6F 6E 74 65 6E 74 2F  .com/wp-content/
00000FD0  70 6C 75 67 69 6E 73 2F 61 6B 69 73 6D 31 2E 70  plugins/akism1.p
00000FE0  67 69 00 4B E0 F7 E9 9E D9 30 81 A4 32 17 D2 28  gi.Kà÷éžÙ0.¤2.Ò(
00000FF0  2D F6 A1 72 FE 69 FF 0E A2 7B 2C A2 D7 AE 33 D1  -ö¡rþiÿ.¢{,¢×®3Ñ
00001000  D4 70 A6 B7 1B EC 08 B8 B5 F6 59 AD F5 04 C0 59  Ôp¦·.ì.¸µöY.õ.ÀY
00001010  89 C5 35 AC D4 54 64 2D 5A ED 39 5E ED 49 BE 34  ‰Å5¬ÔTd-Zí9^íI¾4
00001020  88 DC BE 71 EF B7 8D 04 9A A0 5D 1F CF B5 2D 36  ˆÜ¾qï·..š ].Ïµ-6
00001030  83 53 77 04 58 7F B4 B3 CB 73 04 24 B5 5B 27 90  ƒSw.X.´³Ës.$µ['.
00001040  4F 5E 54 08 AC 25 AB 35 02 95 29 02 D5 DA E9 E5  O^T.¬%«5.•).ÕÚéå
00001050  2E CC 4D 2C 28 2A 9D 02 EC 16 2D 5C 79 84 DF F3  .ÌM,(*..ì.-\y„ßó
00001060  79 EE 9F 88 A1 3F 61 2C 16 E1 3A EC DC CB E2 4F  yîŸˆ¡?a,.á:ìÜËâO
00001070  69 FB D4 78 06 5F 37 1A 76 CB A9 B1 11 AB 71 24  iûÔx._7.vË©±.«q$
00001080  D6 66 21 96 42 59 5D 22 8B BF 30 2D 22 6C 27 F6  Öf!–BY]"‹¿0-"l'ö
00001090  92 85 98 C7 42 2C ED 63 C4 F2 DA 78 6E 7A EA 46  '…˜ÇB,ícÄòÚxnzêF
000010A0  CE 99 59 74 12 92 4B A9 6E A4 16 22 D6 AB 63 6A  Î™Yt.'K©n¤."Ö«cj
000010B0  3D A1 0C C7 68 74 74 70 73 3A 2F 2F 66 6C 79 64  =¡.Çhttps://flyd
000010C0  61 73 68 69 2E 63 6F 6D 2F 77 70 2D 63 6F 6E 74  ashi.com/wp-cont
000010D0  65 6E 74 2F 70 6C 75 67 69 6E 73 2F 61 6B 69 73  ent/plugins/akis
000010E0  6D 32 2E 70 67 69 00 27 BF 3B AF EE CD EF 05 5E  m2.pgi.'¿;¯îÍï.^
```

[그림 6] 배포 서버 URL

쉘 코드 복호화 시 위와 같은 배포 서버 URL 을 확인할 수 있으며,

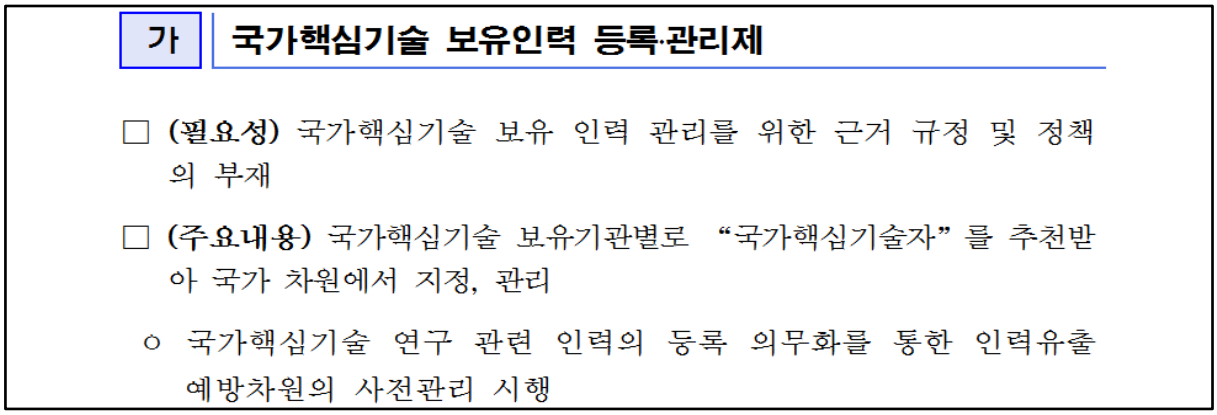
쉘 코드가 실행되면 접속을 시도한 후 OS 버전에 따라 상이한 이름의 추가 파일 다운로드를 시도한다.

[추가 파일 다운로드]

| | |
|---|---|
| OS - 32Bit | https://flydashi.com/wp-content/plugins/askism1.pgi |
| OS - 64Bit | https://flydashi.com/wp-content/plugins/askism2.pgi |

### 4.4. HWP 문서 파일 위장

1) 정상적인 문서 내용 출력




[그림 7] 문서 내용 출력

악성 스크립트 및 쉘 코드가 실행된 후

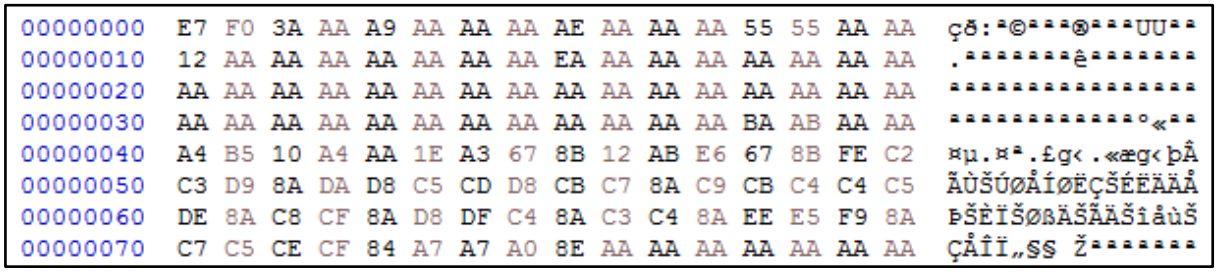
HWP 문서 파일의 내용을 출력하여 정상 HWP 문서 파일로 위장한다.

### 4.5. 악성 파일

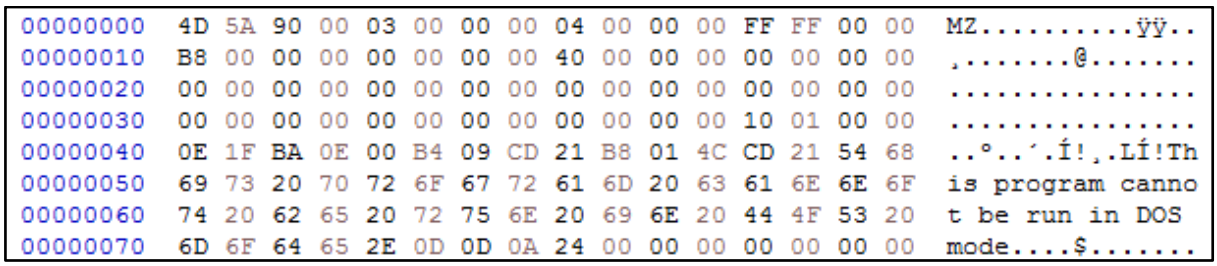
1) 악성 파일


[그림 8] 다운로드 된 악성 파일

배포 서버로부터 다운로드된 악성 파일은 OS 버전에 따라 위와 같이 상이하게 다운로드 된다.



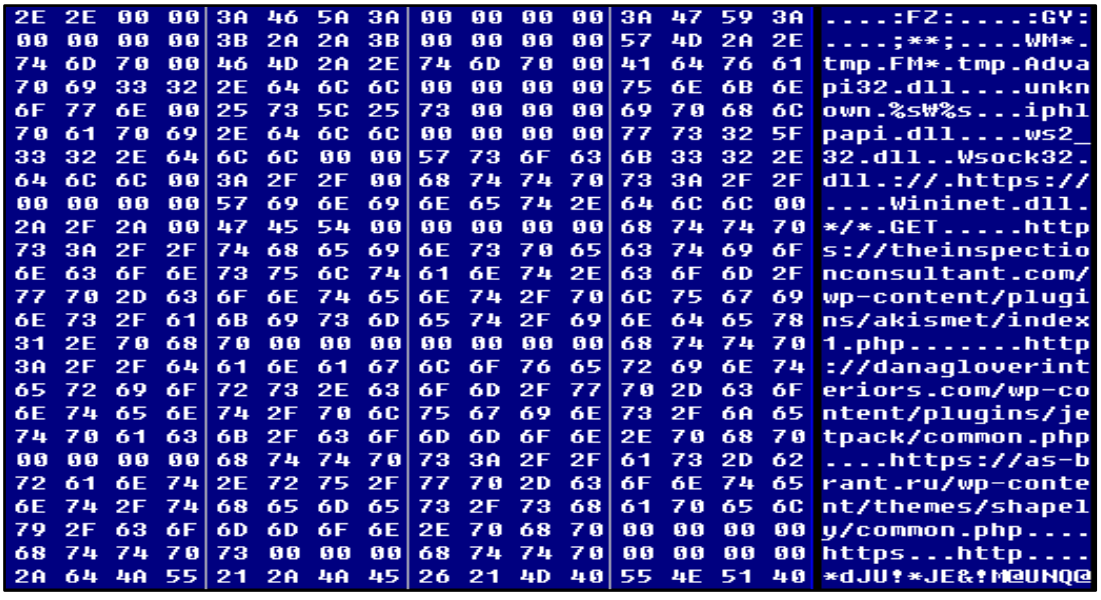

[그림 9-1] '0xAA'로 암호화




[그림 9-2] '0xAA'로 복호화

배포 서버로부터 다운로드된 악성 파일은 '0xAA'로 XOR 암호화 되어있으며,
복호화 시 DLL 파일임을 확인할 수 있다.
쉘 코드 명령에 의해 복호화가 수행되며, 이후 악성 파일이 실행된다.

2) DLL 악성 파일



[그림 10] C2 서버 URL

로드된 내부 DLL 악성 파일은 C2 서버로 접속하여 악성 행위를 위해 공격 명령을 기다린다.

[C2 서버 리스트]

| | |
|---|---|
| 1. C2 | https://theinspectionconsultant.com/wp-content/plugins/akismet/index1.php |
| 2. C2 | http://danagloverinteriors.com/wp-content/plugins/jetpack/common.php |
| 3. C2 | https://as-brant.ru/wp-content/themes/shapely/common.php |

### 4.6. Lazarus Group 과의 연관성

1) 내부 파일명

```
.rdata:1001D650 ;
.rdata:1001D650 ; Export directory for battle32.dll
.rdata:1001D650 ;
.rdata:1001D650                 dd 0                    ; Characteristics
.rdata:1001D654                 dd 5BC9866Ah            ; TimeDateStamp: Fri Oct 19 07:23:22 2018
.rdata:1001D658                 dw 0                    ; MajorVersion
.rdata:1001D65A                 dw 0                    ; MinorVersion
.rdata:1001D65C                 dd rva aBattle32Dll     ; Name
.rdata:1001D660                 dd 1                    ; Base
.rdata:1001D664                 dd 1                    ; NumberOfFunctions
.rdata:1001D668                 dd 1                    ; NumberOfNames
.rdata:1001D66C                 dd rva off_1001D678     ; AddressOfFunctions
.rdata:1001D670                 dd rva off_1001D67C     ; AddressOfNames
.rdata:1001D674                 dd rva word_1001D680    ; AddressOfNameOrdinals
.rdata:1001D680 word_1001D680   dw 0                    ; DATA XREF: .rdata:1001D674↑o
.rdata:1001D682 aBattle32Dll    db 'battle32.dll',0     ; DATA XREF: .rdata:1001D65C↑o
.rdata:1001D68F aCheckself      db 'CheckSelf',0        ; DATA XREF: .rdata:off_1001D67C↑o
```

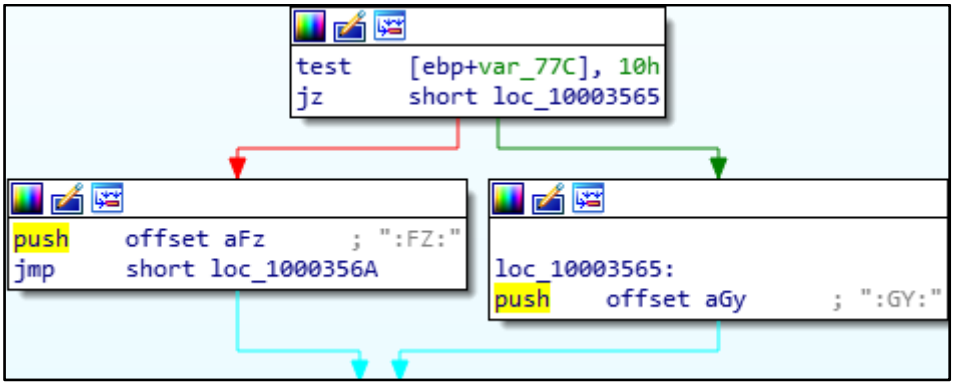
[그림 11] 'battle32.dll'

지난 3 월 '작전명 배틀크루저(Operation Battle Cruiser)'에 사용된 동일한 내부 파일명인 'battle32.dll'과 'battle64.dll'을 확인할 수 있다.

[내부 파일명]

| | |
|---|---|
| OS - 32Bit | battle32.dll |
| OS - 64Bit | battle64.dll |

2). 소니 픽처스(Sony Pictures) 공격 코드



```
.rdata:1001CA18 aFz             db ':FZ:',0             ; DATA XREF: sub_10003250+30E↑o
.rdata:1001CA1D                 align 10h
.rdata:1001CA20 ; CHAR aGy[]
.rdata:1001CA20 aGy             db ':GY:',0             ; DATA XREF: sub_10003250:loc_10003565↑o
.rdata:1001CA25                 align 4
.rdata:1001CA28 ; CHAR asc_1001CA28[]
.rdata:1001CA28 asc_1001CA28    db ';**;',0             ; DATA XREF: sub_10003250:loc_10003601↑o
.rdata:1001CA2D                 align 10h
.rdata:1001CA30 aWmTmp          db 'WM*.tmp',0          ; DATA XREF: StartAddress+1AE↑o
.rdata:1001CA30                                         ; sub_10006C60:loc_10006D05↑o
.rdata:1001CA38 aFmTmp          db 'FM*.tmp',0          ; DATA XREF: StartAddress+1B8↑o
.rdata:1001CA38                                         ; sub_10006C60+B4↑o
```

[그림 12] 소니 픽쳐스(Sony Pictures) 공격 코드

악성 파일은 지난 소니 픽쳐스(Sony Pictures) 공격 때 사용하였던
메타 데이터와 함수를 사용하고 있다.

3). *dJU!*JE&!M@@UNQ@' 코드

```
dword_1001F61C = sub_10001050(&String2, v8, v30, v23);
if ( !dword_1001F61C )
  goto LABEL_30;
dword_1001F610 = rand() % 10000;
if ( !sub_10001370(0, dword_1001F610, "*dJU!*JE&!M@UNQ@", 0) )
  goto LABEL_30;
v15 = dword_1001F61C;
v16 = LoadLibraryA("Winhttp.dll");
v17 = GetProcAddress(v16, "WinHttpWriteData");
if ( !*(_DWORD *)(v15 + 12)
  || (sub_10001010(&v27, "\r\n--%s--\r\n", v15 + 792),
      ((void (__stdcall *)(_DWORD, char *, unsigned int, _DWORD))v17)(*(_DWORD *)(v15 + 12), &v27, strlen(&v27), 0),
      v18 = dword_1001F61C,
      !*(_DWORD *)(dword_1001F61C + 12))
  || (v19 = LoadLibraryA("Winhttp.dll"),
      v20 = GetProcAddress(v19, "WinHttpReceiveResponse"),
      !((int (__stdcall *)(_DWORD, _DWORD))v20)(*(_DWORD *)(v18 + 12), 0))
  || !sub_10001E50(&v37, 4u, 0) )
```

[그림 13] *dJU!*JE&!M@@UNQ@' 코드 사용

지난 상반기에 발생한 Lazarus Group 의 APT 공격에 사용되었던 *dJU!*JE&!M@@UNQ@' 코드가
이번 10 월 APT 공격에도 지속적으로 사용되고 있음을 확인하였다.

### 4.7. 분석 결과

1). 결론

북한 정찰총국의 해커부대로 알려진 Lazarus 그룹은
지난 3 월과 4 월에 이어 10 월, 다시 한번 국내 특정 대상을 목표로
지속적인 APT 공격을 시도하고 있다.
이번 10 월 발생한 APT 공격의 배후가 Lazarus 그룹임은 다양한 단서로 확인할 수 있으며,
특징은 다수에게 변호사를 사칭하는 메일을 발송하여
정상적인 HWP 문서 파일로 위장하는 사회공학적 기법의 공격을 통해 악성 파일을 유포하고,
C2 서버와의 통신을 유지하는 것이다. 해당 그룹은 현재까지도 활동이 지속적으로 발견되어
각별한 주의가 필요하며, 한컴오피스의 한글 프로그램을 최신 버전으로 업데이트 하여야 한다.

# 5. 대 응

1. MS 제공하는 보안 업데이트를 자동으로 설정한다.
2. 사용중인 소프트웨어 최신 업데이트 유지한다.
3. 백신 최신 업데이트 유지한다.
4. 주요 문서는 주기적으로 백업하고 물리적으로 분리하여 관리한다.
5. 신뢰할 수 없는 메일의 첨부파일은 실행을 금지한다.
6. 비 업무 사이트 및 신뢰할 수 없는 웹사이트의 연결을 차단한다.