

매그니베르 v2

랜섬웨어 “magniber (v2)”



융합보안학과 윤세영

유튜브 주소: <https://youtu.be/-GobfUCH7lc>

목차

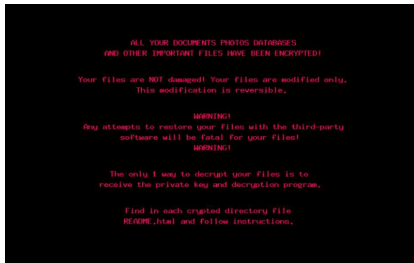
랜섬웨어 “magniber” 란? (v1과 v2)

진행했던 것

랜섬웨어 “magniber” 란?

랜섬웨어 "magniber" 란? (버전 1)

- magniber 랜섬웨어 -> 확장자명을 영문자로 변조 시킴
- 평균적으로 0.18 ~ 0.2 BTC 요구 BTC = 비트코인
- 배경화면 이미지를 변경하기도 함



| <input type="checkbox"/> 이름 | 수정된 날짜 | 유형 | 크기 |
|-----------------------------|--------------------|---------------------|----------|
| Field_49 File.bmp.sbqvowtn | 2022-10-28 오후 2:03 | S8QVOWTN 파일 | 2,701KB |
| Field_50 File.docx.sbqvowtn | 2022-10-28 오후 2:03 | S8QVOWTN 파일 | 102KB |
| Field_51 File.hwp.sbqvowtn | 2022-10-28 오후 2:03 | S8QVOWTN 파일 | 117KB |
| Field_52 File.jpg.sbqvowtn | 2022-10-28 오후 2:03 | S8QVOWTN 파일 | 65KB |
| Field_53 File.mp3 | 2019-06-08 오후 9:18 | MP3 파일 | 7,604KB |
| Field_54 File.pdf.sbqvowtn | 2022-10-28 오후 2:03 | S8QVOWTN 파일 | 2,937KB |
| Field_55 File.png.sbqvowtn | 2022-10-28 오후 2:03 | S8QVOWTN 파일 | 268KB |
| Field_56 File.pptx.sbqvowtn | 2022-10-28 오후 2:03 | S8QVOWTN 파일 | 1,328KB |
| Field_57 File.rtf.sbqvowtn | 2022-10-28 오후 2:03 | S8QVOWTN 파일 | 10KB |
| Field_58 File.txt | 2019-06-08 오후 6:00 | 텍스트 문서 | 6KB |
| Field_59 File.xlsx.sbqvowtn | 2022-10-28 오후 2:03 | S8QVOWTN 파일 | 217KB |
| Field_60 File.zip.sbqvowtn | 2022-10-28 오후 2:03 | S8QVOWTN 파일 | 11,381KB |
| README.html | 2022-10-28 오후 2:03 | Microsoft Edge H... | 17KB |

사진 출처: <https://blog.naver.com/checkmal/222913358453>

랜섬웨어 "magniber" 란?

1 BTC 87518799.38 24.05.06 KRW

Magniber 감염 후 바탕화면

MY DECRYPTOR

Your documents, photos, databases and other important files have been encrypted!

WARNING! Any attempts to restore your files with the third-party software will be fatal for your files! **WARNING!**

The only 1 way to decrypt your files is to receive the private key and decryption program.

[Click here for detailed instructions](#)

Magniber랜섬웨어에 감염되면
피해자에게 감염사실을 알리기위해
바탕화면에 창을 띄웁니다.

MY DECRYPTOR

[Home Page](#)

[Support](#)

[Decrypt 1 file for FREE](#)

[Refresh current page](#)

Your documents, photos, databases and other important files have been encrypted!

WARNING! Any attempts to restore your files with the third-party software will be fatal for your files! **WARNING!**

To decrypt your files you need to buy the special software - "My Decryptor"

All transactions should be performed via **BITCOIN** network.

Within 5 days you can purchase this product at a special price: **BTC 0.1800 (~ \$1960)**

After 5 days the price of this product will increase up to **BTC 0.3600 (~ \$3920)**

The special price is available:

05 . 00:14:28

Magniber 요구비용 홈페이지
요구 비트코인 :0.18BTC
일정시간 경과 후 :0.36BTC요구

사진 출처: 한국 랜섬웨어 침해 대응 센터

랜섬웨어 "magniber" 란?

Q. 감염은 어떻게 되나?

A. 제목에 payment, service 등의 단어를 넣고 송장 및 결제내역으로 교묘하게 위장하여 첨부파일을 다운로드하도록 유도함. (.wsf, .js, .hta, .zip, .pdf 등)

웹사이트에 게시된 광고 배너(광고 팝업이 많이 발생하는 뉴스나 블로그 등 주의), P2P를 이용한 다운로드로도 감염이 됨.



참고

Magniber의 공격 대상은
(한국어를 사용하는)
Windows 운영체제

내용 출처: 한국 랜섬웨어 침해 대응 센터

랜섬웨어 "magniber" 란?

Q. 감염되면 어떻게 되나?

A. 감염즉시 웹페이지와 함께 메모장이 뜬.

PC에서 접근할 수 있는 모든 저장소의 파일들이 암호화되어 파일을 열어볼 수 없음.

확장자명이 영문자로 변조됨. (외장하드가 연결되어 있거나 공유 폴더가 있었다면 전부 변조됨)

| 이름 | 수정된 날짜 | 유형 | 크기 |
|----------------------------|--------------------|---------------------|----------|
| Field_49 File.bmp.sbqvwtn | 2022-10-28 오후 2:03 | SBQVOWTN 파일 | 2,701KB |
| Field_50 File.docx.sbqvwtn | 2022-10-28 오후 2:03 | SBQVOWTN 파일 | 102KB |
| Field_51 File.hwp.sbqvwtn | 2022-10-28 오후 2:03 | SBQVOWTN 파일 | 117KB |
| Field_52 File.jpg.sbqvwtn | 2022-10-28 오후 2:03 | SBQVOWTN 파일 | 65KB |
| Field_53 File.mp3 | 2019-06-08 오후 9:18 | MP3 파일 | 7,604KB |
| Field_54 File.pdf.sbqvwtn | 2022-10-28 오후 2:03 | SBQVOWTN 파일 | 2,937KB |
| Field_55 File.png.sbqvwtn | 2022-10-28 오후 2:03 | SBQVOWTN 파일 | 268KB |
| Field_56 File.pptx.sbqvwtn | 2022-10-28 오후 2:03 | SBQVOWTN 파일 | 1,328KB |
| Field_57 File.rtf.sbqvwtn | 2022-10-28 오후 2:03 | SBQVOWTN 파일 | 10KB |
| Field_58 File.txt | 2019-06-08 오후 6:00 | 텍스트 문서 | 6KB |
| Field_59 File.xlsx.sbqvwtn | 2022-10-28 오후 2:03 | SBQVOWTN 파일 | 217KB |
| Field_60 File.zip.sbqvwtn | 2022-10-28 오후 2:03 | SBQVOWTN 파일 | 11,381KB |
| README.html | 2022-10-28 오후 2:03 | Microsoft Edge H... | 17KB |

내용 출처: 한국 랜섬웨어 침해 대응 센터

랜섬웨어 "magniber" 란? (버전 1)

```
MOV WORD PTR SS:[EBP-22],AX  
CALL DWORD PTR DS:[<&KERNEL32.GetSystemDefaultUILanguage  
MOVZX ECX,AX  
CMP ECX,412  
JE SHORT _00B7000.0124B47E
```

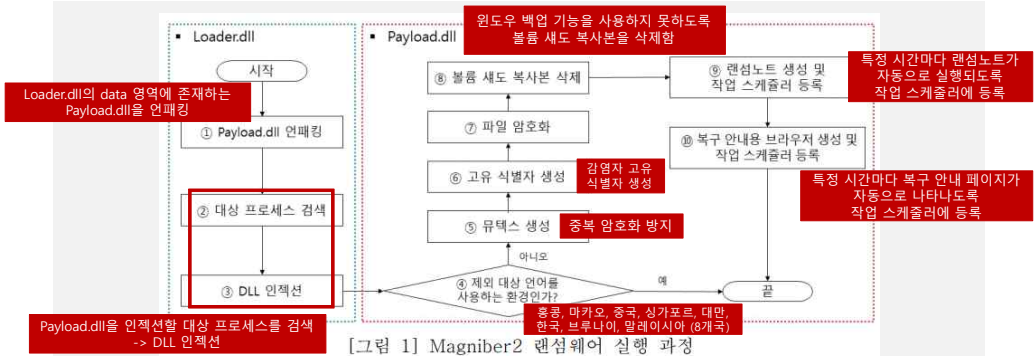
참고

Magniber는 우선 동작하는 PC의 운영체제를 파악한다.
GetSystemDefaultUILanguage를 통해 운영체제에서 한국어를 사용하는지 확인한다.
한국어를 사용할 경우에만 암호화를 진행한다.



랜섬웨어 "magniber" 란? (버전 2)

Magniber v2 실행 과정



랜섬웨어 "magniber" 란? -> v1과 v2

Table 1. Comparison of Magniber version 1 and 2.

| Ransomware | Magniber v1 | Magniber v2 |
|------------------|---|--|
| Crypto system | AES128-CBC-PKCS7Padding | AES128-CBC-PKCS7Padding RSA2048-OAEP |
| Key generation | 1. Receive from C&C server 2. Fixed in code | Attacker's PRNG |
| Key management | None | Encrypted AES key with RSA stored in end of file |
| Key destruction | Yes | Yes |
| Decryption tool | Yes | No |
| Known extensions | kypmzmsw, owxpyzlj, prueitfik, rwithmoz, bnxzoucsx, tzdbkjry, iuoqetgb, pgvuuryti, zpnjelt, gnlnzhz, hssjfbf, ldofoxwu, zskgavp, gwinpyizt, hxzrvhh, cmjedin, dzvtwtqz, pxynindl, sqzprtt, etc. | fprgbk, ihsdj, kgpwwnr, vbdrj, skvtb, vpgvllkb, dlenggrl, dxjay, fbuvkngy, xhsptythxn, demffue, mftzmxqo, qmdjtc, wmfxdqz, ndpyhss, dyaaghemy, etc. |

진행했던 것

진행했던 것

- 진행 상황 – 가상환경 설치 및 사용법
- (1) 샘플 파일 압축 해제 후 스냅샷 촬영
- (2) “loader” 파일과 “payload” 파일 확인
- Loader 파일? : 랜섬웨어가 시스템에 침입하고 실행되기 위해 사용하는 코드나 모듈을 포함하고 있음.
- Payload 파일? : 데이터를 암호화하고 몸값을 요구하는 메시지를 표시하는 등의 악성 행위 수행.
- 로더가 시스템에 침입하여 환경을 조성 -> 페이로드가 해당 환경에서 악성 행위를 수행하는 방식



진행했던 것

ExeinfoPE를 이용해 패킹 확인




둘 다 패킹 안 되어 있음

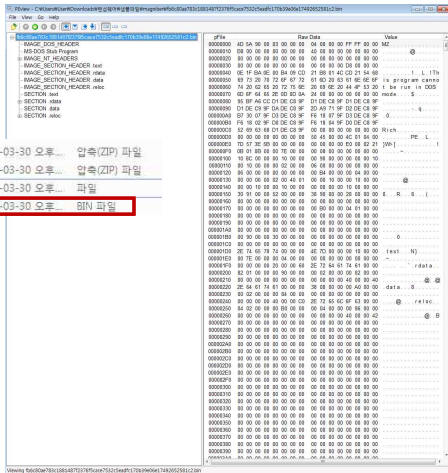


진행했던 것은 은수

- Payload 파일 분석 (PEview)
- 압축 해제 후 PEview 도구 사용

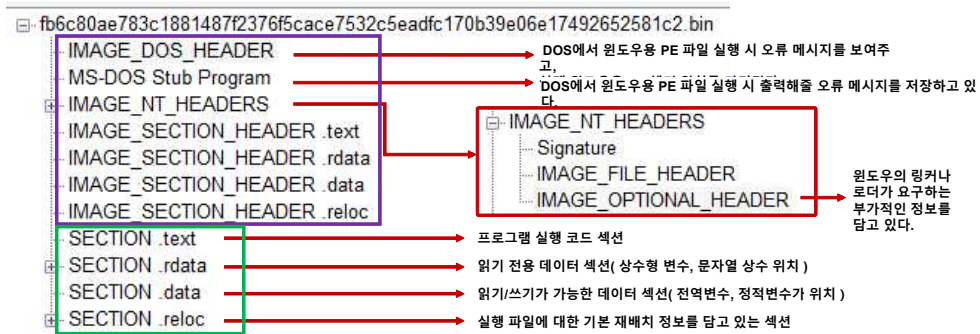
| | | | |
|--|---|------------------|------------|
|  | (loader)6e57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecdfeb293aa9dfc | 2023-03-30 오후... | 압축(ZIP) 파일 |
|  | (payload)fb6c80ae783c1881487f2376f5cace7532c5eadfc170b39e06e17492652581c2.bin | 2023-03-30 오후... | 압축(ZIP) 파일 |
|  | 6e57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecdfeb293aa9dfc | 2023-03-30 오후... | 파일 |
|  | fb6c80ae783c1881487f2376f5cace7532c5eadfc170b39e06e17492652581c2.bin | 2023-03-30 오후... | BIN 파일 |

bin 파일? : 바이너리 파일(이진 파일)



진행했던 것

- Payload 파일 분석 (PEview)



진행했던 것

- Payload 파일 분석 (PEview)
- IMAGE_DOS_HEADER

fb6c80ae783c1881487d2376f5cace7532c5eadfc170b39e06e17492652581c2.bin

- IMAGE_DOS_HEADER
- MS-DOS Stub Program
- + IMAGE_NT_HEADERS
 - IMAGE_SECTION_HEADER.text
 - IMAGE_SECTION_HEADER.rdata
 - IMAGE_SECTION_HEADER.data
 - IMAGE_SECTION_HEADER.reloc
- + SECTION.text
- + SECTION.rdata
- SECTION.data
- + SECTION.reloc

| pFile | Data | Description | Value |
|----------|------|------------------------------|------------------------|
| 00000000 | 5A4D | Signature | IMAGE_DOS_SIGNATURE MZ |
| 00000002 | 0090 | Bytes on Last Page of File | |
| 00000004 | 0003 | Pages in File | |
| 00000006 | 0000 | Relocations | |
| 00000008 | 0004 | Size of Header in Paragraphs | |
| 0000000A | 0000 | Minimum Extra Paragraphs | |
| 0000000C | FFFF | Maximum Extra Paragraphs | |
| 0000000E | 0000 | Initial (relative) SS | |
| 00000010 | 00B8 | Initial SP | |
| 00000012 | 0000 | Checksum | |
| 00000014 | 0000 | Initial IP | |
| 00000016 | 0000 | Initial (relative) CS | |

시그니처 MZ의 의미:
.exe 실행파일이라는 뜻

| pFile | Raw Data | Value |
|----------|---|-------------|
| 00000000 | 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 | MZ |
| 00000010 | B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 |@..... |
| 00000020 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | |

| | | |
|----------|----------|--------------------------|
| 00000028 | 0000 | Reserved |
| 0000002A | 0000 | Reserved |
| 0000002C | 0000 | Reserved |
| 0000002E | 0000 | Reserved |
| 00000030 | 0000 | Reserved |
| 00000032 | 0000 | Reserved |
| 00000034 | 0000 | Reserved |
| 00000036 | 0000 | Reserved |
| 00000038 | 0000 | Reserved |
| 0000003A | 0000 | Reserved |
| 0000003C | 000000D8 | Offset to New EXE Header |

진행했던 것

- Payload 파일 분석 (PEview)
- IMAGE_OPTIONAL_HEADER

fb6c80ae783c1881487f2376f5cace7532c5eadfc170b39e06e17492652581c2.bin

```

IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
  Signature
  IMAGE_FILE_HEADER
  IMAGE_OPTIONAL_HEADER
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .rdata
  IMAGE_OPTIONAL_HEADER
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .rdata
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER .reloc
SECTION .text
SECTION .rdata
SECTION .data
SECTION .reloc
  
```

| pFile | Data | Description | Value |
|----------|----------|----------------------------|---|
| 000000F0 | 010B | Magic | IMAGE_NT_OPTIONAL_HDR32_MAGIC |
| 000000F2 | 0B | Major Linker Version | |
| 000000F3 | 00 | Minor Linker Version | |
| 000000F4 | 00007E00 | Size of Code | |
| 000000F8 | 00000800 | Size of Initialized Data | |
| 000000FC | 00000000 | Size of Uninitialized Data | |
| 00000100 | 00008C10 | Address of Entry Point | 프로그램이 실행되는 코드의 상대 주소(RVA = Relative Virtual Address, 상대주소)값 |
| 00000104 | 00001000 | Base of Code | |
| 000000FC | 00000000 | Size of Uninitialized Data | |
| 00000100 | 00008C10 | Address of Entry Point | |
| 00000104 | 00001000 | Base of Code | |
| 00000108 | 00009000 | Base of Data | |
| 0000010C | 10000000 | Image Base | 가상메모리에서의 PE파일이 로딩 되는 주소 |
| 00000110 | 00001000 | Section Alignment | |
| 00000114 | 00000200 | File Alignment | |
| 00000118 | 0006 | Major O/S Version | |
| 0000011A | 0000 | Minor O/S Version | |
| 0000011C | 0000 | Major Image Version | |

진행했던 것

- Payload 파일 분석 (x32dbg)

Process Explorer - Sysinternals: www.sysinternals.com [User-PC\User]

File Options View Process Find Users Help

<Filter by name>

| Process | CPU | Private Byt... | Working Set | PID | Description | Company Name |
|----------------------|--------|----------------|-------------|------|-----------------------------|----------------------------|
| VBoxService.exe | < 0.01 | 2,136 K | 4,552 K | 704 | VirtualBox Guest Additi... | Oracle and/or its affil... |
| svchost.exe | < 0.01 | 3,548 K | 6,648 K | 772 | Host Process for Windo... | Microsoft Corporation |
| svchost.exe | < 0.01 | 16,952 K | 15,512 K | 832 | Host Process for Windo... | Microsoft Corporation |
| audiodg.exe | | 15,900 K | 15,660 K | 2572 | | |
| svchost.exe | | 47,880 K | 50,580 K | 892 | Host Process for Windo... | Microsoft Corporation |
| dwm.exe | | 7,636 K | 9,420 K | 320 | 데스크톱 할 관리자 | Microsoft Corporation |
| svchost.exe | < 0.01 | 19,200 K | 28,504 K | 928 | Host Process for Windo... | Microsoft Corporation |
| svchost.exe | | 5,592 K | 10,436 K | 400 | Host Process for Windo... | Microsoft Corporation |
| svchost.exe | < 0.01 | 11,864 K | 10,616 K | 316 | Host Process for Windo... | Microsoft Corporation |
| spoolsv.exe | | 5,852 K | 7,224 K | 1152 | Spooler SubSystem App | Microsoft Corporation |
| svchost.exe | | 10,296 K | 8,360 K | 1196 | Host Process for Windo... | Microsoft Corporation |
| svchost.exe | | 4,572 K | 6,964 K | 1292 | Host Process for Windo... | Microsoft Corporation |
| taskhost.exe | | 7,324 K | 7,600 K | 1776 | Windows 작업을 위한 호... | Microsoft Corporation |
| sppsvc.exe | | 5,664 K | 7,644 K | 1928 | Microsoft 소프트웨어 보호... | Microsoft Corporation |
| SearchIndexer.exe | < 0.01 | 34,432 K | 31,572 K | 1756 | Microsoft Windows Sear... | Microsoft Corporation |
| SearchProtocolHo... | < 0.01 | 2,864 K | 8,232 K | 2516 | | |
| SearchFilterHoste... | | 2,620 K | 6,412 K | 2536 | | |
| svchost.exe | < 0.01 | 65,852 K | 26,000 K | 2080 | Host Process for Windo... | Microsoft Corporation |
| lsass.exe | < 0.01 | 3,848 K | 8,832 K | 520 | Local Security Authority... | Microsoft Corporation |
| lsmd.exe | | 2,332 K | 3,392 K | 528 | | |
| csrss.exe | < 0.01 | 12,776 K | 12,476 K | 416 | | |
| conhost.exe | < 0.01 | 2,400 K | 7,748 K | 2840 | 콘솔 할 호스트 | Microsoft Corporation |
| winlogon.exe | | 2,792 K | 5,508 K | 468 | | |
| explorer.exe | < 0.01 | 45,348 K | 58,424 K | 1768 | Windows 탐색기 | Microsoft Corporation |
| VBoxTray.exe | < 0.01 | 2,172 K | 6,608 K | 1640 | VirtualBox Guest Additi... | Oracle and/or its affil... |
| procexp64.exe | 0.77 | 16,340 K | 26,924 K | 2688 | Sysinternals Process E... | Sysinternals - www.s... |
| x32dbg.exe | < 0.01 | 31,332 K | 52,328 K | 2004 | x64dbg | |
| DLLLoader32_5CF7.exe | < 0.01 | 532 K | 2,356 K | 2416 | | |

CPU Usage: 0.77% Commit Charge: 17.02% Processes: 36 Physical Memory: 20.12%

진행했던 것

- Payload 파일 분석 (x32dbg)

The screenshot shows the x32dbg interface. On the left, the '모듈' (Modules) pane lists loaded DLLs. A red arrow points to 'lpk.dll' at address 75B40000. The main pane displays the disassembled code of 'dllloader32_sc7.exe' starting at address 003E1000. The code includes instructions for pushing the stack pointer, calculating offsets, and calling Windows API functions like GetCurrentProcessId, OpenFileMapping, and MapViewOfFile. A comment on the right side of the code indicates a path: '3EB188:L"Local\\szLibraryNamexx"'. The code ends at address 003E105F.

| 주소 | 모듈 | 코드 | 비고 |
|----------|---------------------|----|----|
| 003E0000 | dllloader32_sc7.exe | | |
| 75970000 | cryptbase.dll | | |
| 75980000 | sspicli.dll | | |
| 759F0000 | gdi32.dll | | |
| 75A80000 | msvcrt.dll | | |
| 75B40000 | lpk.dll | | |
| 75C30000 | sechost.dll | | |
| 76050000 | advapi32.dll | | |
| 76490000 | usp10.dll | | |

```

003E1000  55          push ebp
003E1001  8BEC       mov ebp,esp
003E1003  81EC 04020000 sub esp,204
003E1009  A1 00003F00 mov eax,dword ptr ds:[3F0000]
003E100E  33C5      xor eax,ebp
003E1010  8945 FC   mov dword ptr ss:[ebp-4],eax
003E1013  57        push edi
003E1014  FF15 00803E00 call dword ptr ds:[<GetCurrentProcessId>]
003E101A  50        push eax
003E101B  8D85 FCFDFFFF lea eax,dword ptr ss:[ebp-204]
003E1021  68 88B13E00 push d11loader32_sc7.3EB188
003E1026  50        push eax
003E1027  FF15 08B13E00 call dword ptr ds:[<wsprintfw>]
003E102D  83C4 0C   add esp,C
003E1030  8D85 FCFDFFFF lea eax,dword ptr ss:[ebp-204]
003E1036  50        push eax
003E1039  6A 00     push 0
003E103B  6A 04     push 4
003E103D  FF15 14803E00 call dword ptr ds:[<OpenFileMappingw>]
003E1043  8BF8     mov edi,eax
003E1045  85F6     test edi,edi
003E1047  74 34     je d11loader32_sc7.3E107B
003E1048  56        push esi
003E104A  68 00040000 push 400
003E104C  6A 00     push 0
003E104E  6A 00     push 0
003E1050  6A 04     push 4
003E1052  57        push edi
003E1054  FF15 08B03E00 call dword ptr ds:[<MapViewOfFile>]
003E105A  8BF0     mov esi,eax
003E105C  85F6     test esi,esi
003E105F  74 13     je d11loader32_sc7.3E1073
  
```

진행했던 것

- Payload 파일 분석 (x32dbg)

모르겠어요...

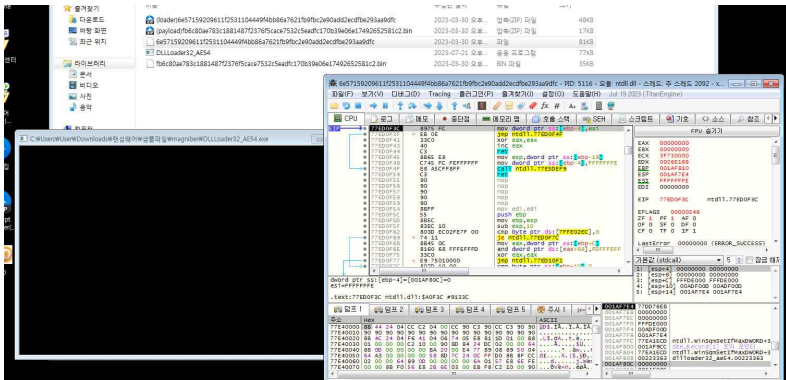


| 주소 | 디스어셈블리 | String A | 문자열 |
|----------|-------------------------------------|----------|---|
| 003E1021 | push d11loader32_5cf7.3EB688 | 003E6188 | "Local\\szLibraryNameEx" |
| 003E1108 | cmp dword ptr ds:[eax+3E0074],E | 003E6174 | "\\r\\n" |
| 003E1835 | push d11loader32_5cf7.3EB260 | 003E6260 | "L"mscoree.dll" |
| 003E1846 | push d11loader32_5cf7.3EB278 | 003E6278 | "CoExiitProcess" |
| 003E1884 | cmp dword ptr ds:[3EED00],0 | 003E6D00 | "잘>" |
| 003E1880 | push d11loader32_5cf7.3EED00 | 003E6D00 | "잘>" |
| 003E2158 | mov eax,dword ptr ds:[eax*8+3EB28C] | 003E629C | "&L"R6002\\r\\n- floating point support not loaded\\r\\n" |
| 003E22C4 | push d11loader32_5cf7.3EBC28 | 003E6C28 | "L"Runtime Error!\\n\\nProgram: " |
| 003E2205 | push d11loader32_5cf7.3EBC5C | 003E6C5C | "L"<program name unknown>" |
| 003E2230 | push d11loader32_5cf7.3EBC6C | 003E6C6C | "L"..." |
| 003E2266 | push d11loader32_5cf7.3EBC94 | 003E6C94 | "L"\\n\\n" |
| 003E229E | push d11loader32_5cf7.3EBCA0 | 003E6CA0 | "L"Microsoft Visual C++ Runtime Library" |
| 003E27CA | push d11loader32_5cf7.3EBC6C | 003E6C6C | "L"kernel32.dll" |
| 003E2700 | push d11loader32_5cf7.3EBD08 | 003E6D08 | "FlsAllLoc" |
| 003E27E8 | push d11loader32_5cf7.3EBD14 | 003E6D14 | "FlsFree" |
| 003E27FE | push d11loader32_5cf7.3EBD1C | 003E6D1C | "FlsGetValue" |
| 003E2811 | push d11loader32_5cf7.3EBD28 | 003E6D28 | "FlsSetValue" |
| 003E2824 | push d11loader32_5cf7.3EBD34 | 003E6D34 | "InitializeCriticalSectionEx" |
| 003E2837 | push d11loader32_5cf7.3EBD30 | 003E6D30 | "CreateEventEx" |
| 003E2844 | push d11loader32_5cf7.3EBD60 | 003E6D60 | "CreateSemaphoreEx" |
| 003E285D | push d11loader32_5cf7.3EBD74 | 003E6D74 | "SetThreadStackGuarantee" |
| 003E2870 | push d11loader32_5cf7.3EBD8C | 003E6D8C | "CreateThreadPoolTimer" |
| 003E2883 | push d11loader32_5cf7.3EBDA4 | 003E6DA4 | "SetThreadPoolTimer" |
| 003E2896 | push d11loader32_5cf7.3EBDB8 | 003E6DB8 | "WaitForThreadPoolTimerCallbacks" |
| 003E28A9 | push d11loader32_5cf7.3EBDB8 | 003E6DB8 | "CloseThreadPoolTimer" |
| 003E28B8 | push d11loader32_5cf7.3EBDF0 | 003E6DF0 | "CreateThreadPoolWait" |
| 003E28CF | push d11loader32_5cf7.3EBE08 | 003E6E08 | "SetThreadPoolWait" |
| 003E28E2 | push d11loader32_5cf7.3EBE1C | 003E6E1C | "CloseThreadPoolWait" |
| 003E28FA | push d11loader32_5cf7.3EBE30 | 003E6E30 | "FlushProcessWriteBuffers" |
| 003E2908 | push d11loader32_5cf7.3EBE4C | 003E6E4C | "FreeLibraryWhenCallbackReturns" |
| 003E2918 | push d11loader32_5cf7.3EBE6C | 003E6E6C | "GetCurrentProcessorNumber" |
| 003E292E | push d11loader32_5cf7.3EBE88 | 003E6E88 | "GetLogicalProcessorInformation" |
| 003E2941 | push d11loader32_5cf7.3EBEA8 | 003E6EA8 | "CreateSymbolicLink" |
| 003E2954 | push d11loader32_5cf7.3EBEBC | 003E6EBC | "SetDefaultDllDirectories" |
| 003E2967 | push d11loader32_5cf7.3EBED8 | 003E6ED8 | "EnumSystemLocalesEx" |
| 003E297A | push d11loader32_5cf7.3EBEBC | 003E6EBC | "CompareStringEx" |
| 003E298D | push d11loader32_5cf7.3EBEFC | 003E6EFC | "GetDateFormatEx" |
| 003E29A0 | push d11loader32_5cf7.3EBFOC | 003E6FOC | "GetLocaleInfoEx" |
| 003E29B3 | push d11loader32_5cf7.3EBF1C | 003E6F1C | "GetTimeFormatEx" |
| 003E29C6 | push d11loader32_5cf7.3EBF2C | 003E6F2C | "GetUserDefaultLocaleName" |
| 003E29D9 | push d11loader32_5cf7.3EBF48 | 003E6F48 | "IsValidLocaleName" |
| 003E29EC | push d11loader32_5cf7.3EBF5C | 003E6F5C | "LCMapStringEx" |
| 003E29FF | push d11loader32_5cf7.3EBF6C | 003E6F6C | "GetCurrentPackageId" |
| 003E2A12 | push d11loader32_5cf7.3EBF80 | 003E6F80 | "GetTickCount64" |
| 003E2A2A | push d11loader32_5cf7.3EBF90 | 003E6F90 | "GetFileInformationByHandleEx" |
| 003E2A38 | push d11loader32_5cf7.3EBFB0 | 003E6FB0 | "SetFileInformationByHandleEx" |
| 003E2E03 | cmp eax,d11loader32_5cf7.3F0180 | 003F0180 | "&sun" |
| 003E318D | mov eax,dword ptr ds:[3EC334] | 003EC334 | "L">ja-JP" |
| 003E3194 | mov eax,dword ptr ds:[3EC330] | 003EC330 | "L">ja-JP" |
| 003E3198 | mov eax,dword ptr ds:[3EC32C] | 003EC32C | "L">ja-JP" |

진행했던 것

- Magniber 감염 되어 보기

확장자 바꾸지 않으면 아무 일도 일어나지 않음



진행했던 것

- Magniber 감염 되어 보기

1. Loader 파일의 확장자를 (.cpl)로 변경



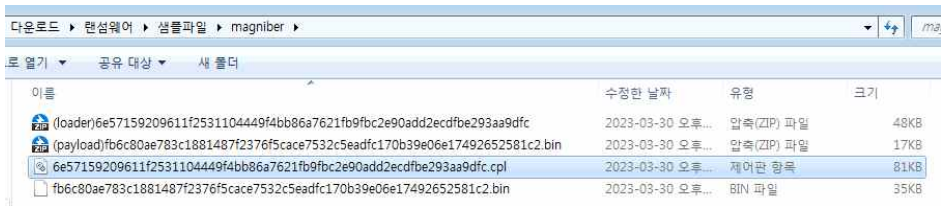
CPL 파일은 Control Panel File의 약자입니다. 이 파일은 Microsoft Windows 운영 체제의 제어판으로 열리는 바이너리 파일이며, 특히 마우스, 디스플레이, 네트워킹 등과 같이 제어판에서 사용할 수 있는 도구를 표시하고 여는 데 사용됩니다.

| | | | | 수정한 날짜 | 유형 | 크기 |
|--|---|------------------|------------|--------|----|----|
| | (loader)6e57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecdfe293aa9dfc | 2023-03-30 오후... | 압축(ZIP) 파일 | | | |
| | (payload)fb6c80ae783c1881487f2376f5cace7532c5eadfc170b39e06e17492652581c2.bin | 2023-03-30 오후... | 압축(ZIP) 파일 | | | |
| | 6e57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecdfe293aa9dfc | 2023-03-30 오후... | 파일 | | | |
| | fb6c80ae783c1881487f2376f5cace7532c5eadfc170b39e06e17492652581c2.bin | 2023-03-30 오후... | BIN 파일 | | | |
| | (loader)6e57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecdfe293aa9dfc | 2023-03-30 오후... | 압축(ZIP) 파일 | 48KB | | |
| | (payload)fb6c80ae783c1881487f2376f5cace7532c5eadfc170b39e06e17492652581c2.bin | 2023-03-30 오후... | 압축(ZIP) 파일 | 17KB | | |
| | 6e57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecdfe293aa9dfc.cpl | 2023-03-30 오후... | 제어판 항목 | 81KB | | |
| | fb6c80ae783c1881487f2376f5cace7532c5eadfc170b39e06e17492652581c2.bin | 2023-03-30 오후... | BIN 파일 | 35KB | | |

진행했던 것

- Magniber 감염 되어 보기

더블클릭으로는 아무 일도 일어나지 않음



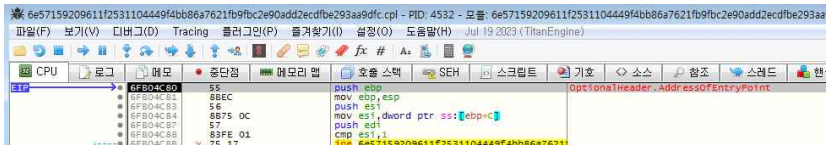
The screenshot shows a Windows File Explorer window with the address bar set to '다운로드 > 랜섬웨어 > 샘플파일 > magniber'. The file list contains four items, with the third item selected. The selected item is a file named '6e57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecdfe293aa9dfc.cpl' with a size of 81KB and a type of '제어판 항목' (Control Panel Item). The other items are ZIP files and a BIN file.

| 이름 | 수정한 날짜 | 유형 | 크기 |
|---|------------------|------------|------|
| (loader)6e57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecdfe293aa9dfc | 2023-03-30 오후... | 압축(ZIP) 파일 | 48KB |
| (payload)fb6c80ae783c1881487f2376f5cace7532c5eadfc170b39e06e17492652581c2.bin | 2023-03-30 오후... | 압축(ZIP) 파일 | 17KB |
| 6e57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecdfe293aa9dfc.cpl | 2023-03-30 오후... | 제어판 항목 | 81KB |
| fb6c80ae783c1881487f2376f5cace7532c5eadfc170b39e06e17492652581c2.bin | 2023-03-30 오후... | BIN 파일 | 35KB |

진행했던 것

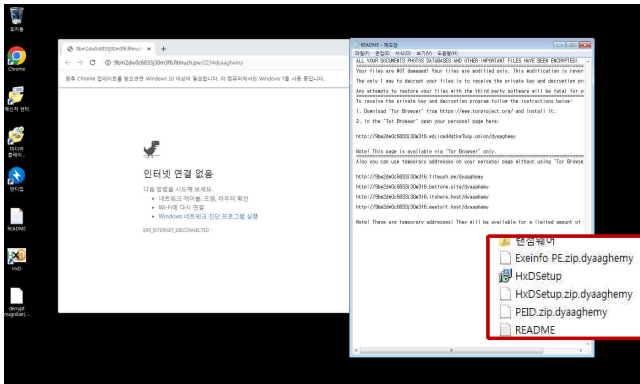
- Magniber 감염 되어 보기

x32dbg로 loader 파일 실행(F9)



진행했던 것

- Magniber 감염 되어 보기



감염되어 "README" txt 파일 및
팝업 등장
또한 기존의 파일들이
"dyaaghemy" 확장자 형태로 변경됨

| | | | |
|--------------------------|------------------|--------------|---------|
| 랜섬웨어 | 2024-05-14 오후... | 파일 폴더 | |
| Exeinfo.PE.zip.dyaaghemy | 2024-05-14 오후... | DYAAGHEMY 파일 | 1,228KB |
| HxDSetup | 2021-02-11 오전... | 응용 프로그램 | 3,365KB |
| HxDSetup.zip.dyaaghemy | 2024-05-14 오후... | DYAAGHEMY 파일 | 3,270KB |
| PEID.zip.dyaaghemy | 2024-05-14 오후... | DYAAGHEMY 파일 | 434KB |
| README | 2024-05-14 오후... | 텍스트 문서 | 2KB |

진행했던 것

해당 함수 실행 시 감염 됨

6e57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecd7be293aa9dfc.cpl - PID: 4040 - 모듈: 6e57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecd7be293aa9dfc.cpl - 스레드: 주 스레드 4140 - ...

파일(F) 보기(V) 디버거(D) Tracing 플러그인(P) 줄여보기(I) 설정(O) 도움말(H) Jul 19 2023 (TitanEngine)

CPU 로그 메모 중단점 메모리 맵 호출 스택 SEH 스크립트 기호 <> 소스 참조 스레드 행들 Trace

OptionalHeader.AddressOfEntryPoint

FPU 숨기기

| | | |
|------------|----------|---------------------|
| EAX | 00000000 | |
| EBX | 00000001 | |
| ECX | 77E63CA3 | ntdll.77E63CA3 |
| EDX | 00000000 | |
| EBP | 0042F39C | &"공B" |
| ESP | 0042F388 | |
| ESI | 00000001 | |
| EDI | 0042F46C | |
| EIP | 6FB04CAB | 6e57159209611f2531 |
| EFLLAGS | 00000212 | |
| ZF 0 | PF 0 | AF 1 |
| OF 0 | SF 0 | DF 0 |
| CF 0 | TF 0 | IF 1 |
| LastError | 00000000 | (ERROR_SUCCESS) |
| LastStatus | C0000139 | (STATUS_ENTRYPOINT) |
| G5 0028 | F5 0053 | |
| ES 0028 | DS 0028 | |
| CS 0023 | SS 0028 | |

6FB04C80 55
6FB04C81 8BEC
6FB04C83 56
6FB04C84 8B75 0C
6FB04C87 57
6FB04C88 83FE 01
6FB04C88 75 17
6FB04C8D E8 6E000000
6FB04C92 68 0490806F
6FB04C97 68 0090806F
6FB04C9C E8 7F000000
6FB04CA1 83C4 08
6FB04CA4 FF75 10
6FB04CA7 56
6FB04CA7 FF75 08
6FB04CAB E8 42C4FFFF
6FB04CB0 8BF8
6FB04CB2 85F6
6FB04CB4 75 05
6FB04CB6 E8 15000000
6FB04CB8 88C7
6FB04CBD 5F
6FB04CBE 5E
6FB04CBF 5D
6FB04CC0 C2 0C00
6FB04CC3 CC
6FB04CC4 CC
6FB04CC5 FF

push ebp
mov ebp,esp
push esi
mov esi,dword ptr ss:[ebp+C]
push edi
cmp esi,1
jne 6e57159209611f2531104449f4bb86a7621
call 6e57159209611f2531104449f4bb86a7621
push 6e57159209611f2531104449f4bb86a7621
push 6e57159209611f2531104449f4bb86a7621
call 6e57159209611f2531104449f4bb86a7621
add esp,8
push dword ptr ss:[ebp+10]
push esi
push dword ptr ss:[ebp+8]
call 6e57159209611f2531104449f4bb86a7621
mov edi,eax
test esi,esi
jne 6e57159209611f2531104449f4bb86a7621
call 6e57159209611f2531104449f4bb86a7621
mov eax,edi
pop edi
pop esi
pop ebp
ret C
int3
int3
int3

진행했던 것

- 감염 함수 분석 (call ~~~~. 6FB010F2)

The screenshot shows a debugger window with assembly code. A red arrow points from a question mark to a call instruction at address 6FB010F2. The assembly code is as follows:

```

6FB04CA4 FF75 10      push dword ptr ss:[ebp+10]
6FB04CA7 56          push esi
6FB04CA8 FF75 08      push dword ptr ss:[ebp+8]
6FB04CAB E8 42C4FFFF call 6E57159209611F2531104449F4bb86a7621fb9fbc2e90add2ecc
6FB04CB0 88F8        mov edi,eax
6FB04CB2 85F6        test esi,esi

6FB04CAB FF75 08      push dword ptr ss:[ebp+8]
6FB04CAB E8 42C4FFFF call 6E57159209611F2531104449F4bb86a7621fb9fbc2e90add2eccdfbe293aa9dfc.6FB010F2
6FB04CB0 88F8        mov edi,eax
6FB04CB2 85F6        test esi,esi
6FB04CB4 75 05      jne 6E57159209611F2531104449F4bb86a7621fb9fbc2e90add2eccdfbe293aa9dfc.6FB04CB8
6FB04CB6 call 6E57159209611F2531104449F4bb86a7621fb9fbc2e90add2eccdfbe293aa9dfc.6FB04CD0

6FB010F2 8B4424 08   mov eax,dword ptr ss:[esp+8]
6FB010F6 48         dec eax
6FB010F7 74 1A     jle 6E57159209611F2531104449F4bb86a7621fb9fbc2e90add2eccdfbe293aa9dfc.6FB01113
6FB010F9 83E8 05   sub eax,5
6FB010FC 75 0F     jne 6E57159209611F2531104449F4bb86a7621fb9fbc2e90add2eccdfbe293aa9dfc.6FB0110D
6FB010FE 8B4C24 0C mov ecx,dword ptr ss:[esp+C]
6FB01102 85C9     test ecx,ecx
6FB01104 74 07     jle 6E57159209611F2531104449F4bb86a7621fb9fbc2e90add2eccdfbe293aa9dfc.6FB0110D
6FB01106 A1 001D816F mov eax,dword ptr ds:[6FB11D00]
6FB01108 8901     mov dword ptr ds:[ecx],eax
6FB0110D 33C0     xor eax,eax
6FB0110F 40       inc eax
6FB01110 ret C
6FB01113 8B4424 04 mov eax,dword ptr ss:[esp+4]
6FB01117 A3 001D816F mov dword ptr ds:[6FB11D00],eax
6FB0111C E8 EF010000 call 6E57159209611F2531104449F4bb86a7621fb9fbc2e90add2eccdfbe293aa9dfc.6FB01310
6FB01121 6A 00     push 0
6FB01123 FF15 0080806F call dword ptr ds:[kExitProcess]
6FB01129 CC        int3
6FB0112A 83EC 24   sub esp,24
6FB0112D 53       push ebx
6FB0112F 54       push esi
  
```

진행했던 것

어떤 함수에서 감염이 일어나는지?

해당 함수 실행 시 감염 됨

The screenshot shows a debugger window with the following details:

- Assembly Code:** The code is in x86 assembly. The instruction at address 6FB04CAB is highlighted: `call 6e57159209611f2531104449f4bb86a7621`. This instruction is part of a sequence of operations including `push ebp`, `mov ebp, esp`, `push esi`, `mov esi, dword ptr ss:[ebp+c]`, `push edi`, `cmp esi, 1`, `jne 6e57159209611f2531104449f4bb86a7621`, `call 6e57159209611f2531104449f4bb86a7621`, `push 6e57159209611f2531104449f4bb86a7621`, `push 6e57159209611f2531104449f4bb86a7621`, `call 6e57159209611f2531104449f4bb86a7621`, `add esp, 8`, `push dword ptr ss:[ebp+10]`, `push esi`, `push dword ptr ss:[ebp+8]`, `mov edi, eax`, `test esi, esi`, `jne 6e57159209611f2531104449f4bb86a7621`, `call 6e57159209611f2531104449f4bb86a7621`, `mov eax, edi`, `pop edi`, `pop esi`, `pop ebp`, `ret 4`, `int3`, `int3`, `int3`.
- Registers:** The register window on the right shows the following values:
 - EAX: 00000000
 - EBX: 00000001
 - ECX: 77E63CA3
 - EDX: 00000000
 - ESP: 0042F39C
 - ESI: 00000001
 - EDI: 0042F46C
 - EIP: 6FB04CAB
- Trace:** The trace window shows the following information:
 - FFU 숨기기
 - EFLAGS: 00000212
 - ZF: 0 PF: 0 AF: 1
 - OF: 0 SF: 0 DF: 0
 - CF: 0 TF: 0 IF: 1
 - LastError: 00000000 (ERROR_SUCCESS)
 - LastStatus: C0000139 (STATUS_ENTRYPOINT)
 - GS: 0028 FS: 0053
 - ES: 0028 DS: 0028
 - CS: 0028 SS: 0028

감염(프로그램 종료) == DLL 인젝션 시작?

진행했던 것

어떤 함수에서 감염이 일어나는지?

```
70EE161D 8BF9 mov edi,ecx
70EE161F 56 push esi
70EE1620 57 push edi
70EE1621 FF15 580EE70 call dword ptr ds:[<vftua7A1ToCEx>]
70EE1627 8B08 mov ebx,eax
70EE1629 8B08 test ebx,ebx
70EE162B 74 34 je 6E57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecdfe293aa9dfc.70EE1661
70EE162D 56 push esi
70EE162E 55 push ebp
70EE162F 68 F090EE70 push 6E57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecdfe293aa9dfc.70EE90F0
70EE1634 55 push ebx
70EE1635 57 push edi
70EE1636 FF15 8C80EE70 call dword ptr ds:[<writeProcessMemory>]
70EE163C 85C0 test eax,eax
70EE163E 74 21 je 6E57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecdfe293aa9dfc.70EE1661
70EE1640 8B4424 18 mov eax,dword ptr ss:[esp+18]
70EE1644 56 push esi
70EE1645 56 push esi
70EE1646 56 push esi
70EE1647 03C3 add eax,ebx
70EE1649 50 push eax
70EE164A 56 push esi
70EE164B 56 push esi
70EE164C 57 push edi
70EE164D FF15 2880EE70 call dword ptr ds:[<createRemoteThread>]
70EE1653 85C0 test eax,eax
70EE1655 74 0A je 6E57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecdfe293aa9dfc.70EE1661
70EE1657 6A FF push FFFFFFFF
70EE1659 50 push eax
70EE165A 46 inc esi
70EE165B FF15 1880EE70 call dword ptr ds:[<waitForSingleObject>]
70EE1661 85FF test edi,edi
70EE1663 74 07 je 6E57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecdfe293aa9dfc.70EE166C
70EE1665 57 push edi
70EE1666 FF15 8080EE70 call dword ptr ds:[<closeHandle>]
70EE166C 5F pop edi
70EE166D 8BC6 mov eax,esi
```

타겟 프로세스의 메모리 공간 확보

인젝션할 DLL 경로 입력

← 뭐가 들어가는지
주시해봐야함

DLL 호출 (타겟 프로세스를 통해 호출함)

진행했던 것

Payload.dll PE 분석

| fb6c80ae783c1881487f2376f5cace7532c5eadfc170b39e06e17492652581c2.bin | | | | | | | | | | | | | | | | | |
|--|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------------|
| Offset(h) | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0A | 0B | 0C | 0D | 0E | 0F | Decoded text |
| 00000000 | 4D | 5A | 90 | 00 | 03 | 00 | 00 | 00 | 04 | 00 | 00 | 00 | FF | FF | 00 | 00 | MZ.....ÿÿ.. |
| 00000010 | B8 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 40 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |@..... |
| 00000020 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | |
| 00000030 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | DB | 00 | 00 | 00 |0... |
| 00000040 | 0E | 1F | BA | 0E | 00 | B4 | 09 | CD | 21 | B8 | 01 | 4C | CD | 21 | 54 | 68 | ..°..'í!..Lí!Th |
| 00000050 | 69 | 73 | 20 | 70 | 72 | 6F | 67 | 72 | 61 | 6D | 20 | 63 | 61 | 6E | 6E | 6F | is program canno |
| 00000060 | 74 | 20 | 62 | 65 | 20 | 72 | 75 | 6E | 20 | 69 | 6E | 20 | 44 | 4F | 53 | 20 | t be run in DOS |
| 00000070 | 6D | 6F | 64 | 65 | 2E | 0D | 0D | 0A | 24 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | mode....\$..... |
| 00000080 | 95 | BF | A6 | CC | D1 | DE | C8 | 9F | D1 | DE | C8 | 9F | D1 | DE | C8 | 9F | •¿;îÑpËYÑpËYÑpËY |
| 00000090 | D1 | DE | C9 | 9F | DA | DE | C8 | 9F | 2D | A9 | 71 | 9F | D2 | DE | C8 | 9F | ÑpËYÚpËY-@qYÓpËY |
| 000000A0 | B7 | 30 | 07 | 9F | D3 | DE | C8 | 9F | F6 | 18 | 07 | 9F | D3 | DE | C8 | 9F | ·0.YÓpËYø..YÓpËY |
| 000000B0 | F6 | 18 | 02 | 9F | D0 | DE | C8 | 9F | F6 | 18 | 04 | 9F | D0 | DE | C8 | 9F | ø..YðpËYø..YðpËY |
| 000000C0 | 52 | 69 | 63 | 68 | D1 | DE | C8 | 9F | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | RichÑpËY..... |
| 000000D0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 50 | 45 | 00 | 00 | 4C | 01 | 04 | 00 | PF T. |

진행했던 것

어떤 함수에서 감염이 일어나는지? – Loader.dll 분석, DLL 인젝션

DLL 인젝션 코드에서 WriteProcessMemory의 인자로 payload 파일(DLL)이 들어감을 확인

.bin Payload.dll PE

```

0F Decoded text
00 MZ.....YY..
00 .....@.....
00 .....
00 .....
68 ..°..'.i!..Li!Th
6F is program canno
20 t be run in DOS
00 mode....$......
9F *;INPEYNPÉYNPÉY
9F NPEYUPÉY-QqYOPÉY
9F *O.YOPÉYö..YOPÉY
9F ö..YOPÉYö..YOPÉY
00 RichNPÉY.....
00 DE T
        
```

```

6E57159209611F2531104449F4BB86A7621F09FC2E90ADD2ECDDBE293AA9DFC, 6FBC90F0
.text: 6FBC162F 6E57159209611F2531104449F4BB86A7621F09FC2E90ADD2ECDDBE293AA9DFC.cpl:1162F #A2F
        jmp     6E57159209611F2531104449F4BB86A7621F09FC2E90ADD2ECDDBE293AA9DFC
        
```

| 주소 | Hex | ASCII |
|----------|---|------------------|
| 6FBC90F0 | 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 | MZ.....YY.. |
| 6FBC9100 | B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 |@..... |
| 6FBC9110 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | |
| 6FBC9120 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | |
| 6FBC9130 | 0E 1F 8A 0E 00 84 09 CD 21 B8 01 4C CD 21 54 6E | ..°..'.i!..Li!Th |
| 6FBC9140 | 69 73 20 70 72 6F 67 72 61 60 20 63 63 6E 6E 6E | is program canno |
| 6FBC9150 | 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 | t be run in DOS |
| 6FBC9160 | 60 6F 64 65 2E 00 00 04 00 00 00 00 00 00 00 00 | mode....\$...... |
| 6FBC9170 | 95 BF A6 CC D1 DE C8 9F D1 DE C8 9F D1 DE C8 9F | *;INPEYNPÉYNPÉY |
| 6FBC9180 | D1 DE C9 9F DA DE C8 9F 20 A9 71 9F D2 DE C8 9F | NPEYUPÉY-QqYOPÉY |
| 6FBC9190 | 87 30 0F 9F D3 DE C8 9F F6 18 07 9F D3 DE C8 9F | *O.YOPÉYö..YOPÉY |
| 6FBC91A0 | F6 18 02 9F D0 DE C8 9F F6 18 04 9F D0 DE C8 9F | ö..YOPÉYö..YOPÉY |
| 6FBC91B0 | 52 69 63 68 D1 DE C8 9F 00 00 00 00 00 00 00 00 | RichNPÉY..... |
| 6FBC91C0 | 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00 | DE T |
| 6FBC91D0 | 7D 57 3E 58 00 00 00 00 00 00 00 00 00 00 00 00 | |
| 6FBC91E0 | 08 01 08 00 00 7E 00 00 00 00 00 00 00 00 00 00 | |

진행했던 것

x32dbg를 이용한 동적 분석

이 구간이 반복해서 실행됨

| | | | |
|-----|----------|---------------|--|
| EIP | 6FBC1405 | 3098 F090BC6F | xor byte ptr ds:[eax+6FBC90F0],b1 |
| | 6FBC1408 | 43 | inc ebx |
| | 6FBC140C | 81FB FF000000 | cmp ebx,FF |
| | 6FBC1412 | 0F44DE | cmovbe ebx,esi |
| | 6FBC1415 | 40 | inc eax |
| | 6FBC1416 | 3D 008A0000 | cmp eax,8A00 |
| | 6FBC141B | 72 E8 | jb 6e57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecdfeb293aa9dfc.6FBC1405 |

| | | | |
|-----|----------|---------------|--|
| EIP | 6FBC1405 | 3098 F090BC6F | xor byte ptr ds:[eax+6FBC90F0],b1 |
| | 6FBC1408 | 43 | inc ebx |
| | 6FBC140C | 81FB FF000000 | cmp ebx,FF |
| | 6FBC1412 | 0F44DE | cmovbe ebx,esi |
| | 6FBC1415 | 40 | inc eax |
| | 6FBC1416 | 3D 008A0000 | cmp eax,8A00 |
| EIP | 6FBC141B | 72 E8 | jb 6e57159209611f2531104449f4bb86a7621fb9fbc2e90add2ecdfeb293aa9dfc.6FBC1405 |

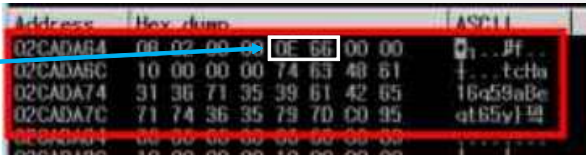


진행했던 것

AES-128로 암호화됨

Algorithm IDs - integer identifier of the encryption algorithm from the following range

- 0x6601 - DES
- 0x6602 - RC2 (version needed to extract < 5.2)
- 0x6603 - 3DES 168
- 0x6609 - 3DES 112
- 0x660E - AES 128
- 0x660F - AES 192
- 0x6610 - AES 256
- 0x6702 - RC2 (version needed to extract >= 5.2)
- 0x6720 - Blowfish
- 0x6721 - Twofish
- 0x6801 - RC4
- 0xFFFF - Unknown algorithm



| Address | Hex dump | ASCII |
|----------|-------------|-----------|
| 02CADA64 | 0E 66 00 00 | 01...H... |
| 02CADA6C | 10 00 00 00 | +...tctha |
| 02CADA74 | 31 36 71 35 | 16a59aBe |
| 02CADA7C | 71 74 36 35 | at65y)적 |
| 02CADA84 | 00 00 00 00 | |
| 02CADA8C | 10 00 00 00 | |

진행했던 것

복호화

→ KISA에는 v1 복호화 도구만 공개됨

→ v2 복호화 관련 논문은 있음

Magniber v2 Ransomware Decryption: Exploiting the Vulnerability of a Self-Developed Pseudo Random Number Generator

by Sehoon Lee ¹ ✉, Myungseo Park ^{1,*} ✉ and Jongsung Kim ^{1,2} ✉

¹ Department of Financial Information Security, Kookmin University, Seoul 02707, Korea

² Department of Information Security, Cryptology and Mathematics, Kookmin University, Seoul 02707, Korea

* Author to whom correspondence should be addressed.


Electronics **2021**, *10*(1), 16; <https://doi.org/10.3390/electronics10010016>

Submission received: 28 November 2020 / Revised: 18 December 2020 / Accepted: 20 December 2020 /
Published: 24 December 2020

진행했던 것

복호화

공격자의 PRNG 생성 취약점을 이용하여 복호화 시도



| Offset(d) | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | Decoded text |
|-----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------------|
| 00000000 | 66 | 0D | 14 | 91 | 07 | 03 | 92 | B7 | 00 | 25 | E7 | 27 | CD | FF | 75 | 4B | f...'.tq'iyuK |
| 00000016 | D6 | 65 | FD | 4A | B0 | 7B | 72 | 72 | 50 | 61 | 7A | FD | 28 | C8 | 51 | 2E | YeyJ*(xrPazY(EQ. |
| 00000032 | 30 | 3C | A1 | 96 | 82 | 3A | 5C | 6D | C6 | 08 | FA | 35 | 25 | B2 | E1 | 9A | O< -,:mE.ú5%*áá |
| 00000048 | 5E | 2E | 5C | A8 | 5B | C0 | 27 | 9E | 41 | 4B | 02 | EF | 00 | E6 | C4 | F2 | ^.\'[A'EAK.1.mAó |
| 00000064 | D0 | CD | EC | 49 | DD | 6D | 8E | F5 | D8 | C3 | FC | FA | 45 | 99 | 44 | 18 | BiliYmZSoAúóE*D. |
| 00000080 | D6 | F5 | 11 | FD | B2 | D7 | 5A | C2 | 08 | F0 | D1 | D8 | 04 | B0 | 65 | 39 | Óó.y*ZA.óNó.*e9 |
| 00000096 | 40 | 35 | B2 | 07 | CB | A4 | 02 | F1 | 70 | B3 | 00 | 0E | 28 | 09 | 4A | CF | @5*.Ew.áp*..(JUI |
| 00000112 | E5 | 70 | 6E | DA | 58 | F8 | 4D | CE | 9E | 96 | 15 | FC | 8B | 36 | 1C | 58 | ápnUXeMiz-.ú<6.X |
| 00000128 | B7 | 8D | E5 | E9 | 3A | EB | 19 | CE | 05 | C5 | 04 | 94 | 78 | 4D | F7 | 3F | ...é:e.I.Á."xM+? |
| 00000144 | 96 | 11 | 43 | 57 | 0C | 6A | E1 | C4 | 44 | E2 | 11 | 88 | 5D | BE | 7A | AF | -.CW.úáADá."jMz- |
| 00000160 | 36 | 9E | 42 | 97 | D6 | C5 | AB | EF | F2 | 2A | 34 | 1B | D9 | D1 | 3B | 94 | 6zB-ÓúAúó*4.ÚN;" |
| 00000176 | 48 | 1C | 5C | 20 | 1D | DB | E1 | 15 | A4 | 37 | 7A | 5E | B8 | 02 | 85 | 91 | H.\.ÚÁ.w7z^....' |
| 00000192 | 3C | BA | 35 | 5B | 7E | AC | 03 | B8 | 98 | 01 | F5 | 33 | 3F | FA | 6D | 7E | <*5[-...".ó3?úm- |
| 00000208 | 3D | 34 | D4 | CA | 2B | 9E | E4 | B3 | CA | B1 | 33 | 61 | 2D | A0 | 0C | 16 | =4óE+úá'Eú3.-.. |
| 00000224 | F1 | 04 | 75 | 4A | A4 | 4C | 2F | 36 | B0 | 3C | A9 | 98 | 2A | D0 | 95 | FE | ñ.uJ=L/6°<@°*B*ó |
| 00000240 | 63 | 18 | 33 | 4F | 4C | FC | C0 | C6 | EA | 9E | D2 | 1B | 58 | AA | 65 | A3 | c.3oLuAúóó.X*ef |
| 00000256 | 42 | 1C | DE | D3 | 22 | 90 | 1D | 0C | 6C | DA | 75 | 54 | 88 | DA | FD | 95 | B.óó"...10ut'Úy. |
| 00000272 | E7 | 5B | 73 | 30 | 65 | 4B | 50 | 6F | 1C | A5 | 53 | 82 | C6 | 61 | 72 | 92 | q[úóeKPo.YS,Ear' |

(a)

a

b

c

| Offset(d) | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | Decoded text | |
|-----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------------------|------------------|
| 00000000 | FF | D8 | FF | E1 | 01 | 60 | 45 | 78 | 69 | 66 | 00 | 00 | 49 | 49 | 2A | 00 | y09á.'Exif..II*. | |
| 00000016 | 08 | 00 | 00 | 00 | 10 | 00 | 9A | 82 | 0A | 00 | 01 | 00 | 00 | 00 | CE | 00 |s.....i. | |
| 00000032 | 00 | 00 | 10 | 01 | 02 | 00 | 0A | 00 | 00 | 00 | D6 | 00 | 00 | 00 | 00 | 01 |ó..... | |
| 00000048 | 03 | 00 | 01 | 00 | 00 | 00 | 40 | 10 | 00 | 00 | 9D | 82 | 0A | 00 | 01 | 00 |8..... | |
| 00000064 | 00 | 00 | E0 | 00 | 00 | 00 | 03 | A4 | 03 | 00 | 01 | 00 | 00 | 00 | 00 | 00 | ..á...w..... | |
| 00000080 | 00 | 00 | 09 | 92 | 03 | 00 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 0F | 01 | ...'...... | |
| 00000096 | 02 | 00 | 10 | 00 | 00 | 00 | E8 | 00 | 00 | 00 | 27 | 88 | 08 | 00 | 01 | 00 |é...'...... | |
| 00000112 | 00 | 00 | FA | 00 | 00 | 00 | 0A | 92 | 05 | 00 | 01 | 00 | 00 | 00 | 00 | F8 | 00 | ..ú...'......s. |
| 00000128 | 00 | 00 | 08 | 92 | 03 | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 12 | 01 | ...'...... |
| 00000144 | 03 | 00 | 01 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 07 | 92 | 03 | 00 | 01 | 00 | 00 | |
| 00000160 | 00 | 00 | FF | FF | FF | FF | 01 | 01 | 03 | 00 | 01 | 00 | 00 | 00 | 00 | 24 | 09 | ..TTTT.....s. |
| 00000176 | 00 | 00 | 32 | 01 | 02 | 00 | 14 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 00 | 25 | 88 | ..2.....%* |
| 00000192 | 04 | 00 | 01 | 00 | 00 | 00 | 14 | 01 | 00 | 00 | 69 | 87 | 04 | 00 | 01 | 00 | 00 |i\$..... |
| 00000208 | 00 | 00 | 3A | 01 | 00 | 00 | 00 | 00 | 00 | 00 | 2A | 00 | 00 | 00 | 00 | E8 | 03 |*.....é. |
| 00000224 | 00 | 00 | 4C | 47 | 2D | 46 | 34 | 36 | 30 | 4C | 00 | 00 | 18 | 00 | 00 | 00 | 00 | ...LG-F460L..... |
| 00000240 | 0A | 00 | 00 | 00 | 4C | 47 | 20 | 45 | 6C | 65 | 63 | 74 | 72 | 6F | 6E | 69 | 00 | ...LG Electroni |
| 00000256 | 63 | 73 | 00 | 00 | 8D | 01 | 00 | 00 | 64 | 00 | 00 | 00 | 32 | 30 | 31 | 35 | 00 | cs.....d...2015 |
| 00000272 | 3A | 31 | 31 | 3A | 32 | 35 | 20 | 32 | 30 | 3A | 32 | 38 | 3A | 33 | 33 | 00 | 00 | :11:25 20:28:33. |

(b)



감사합니다