

NoEscape Ransomware

사이버위협분석팀

목차

개요 3

상세분석 4

결론 15

1. 개요

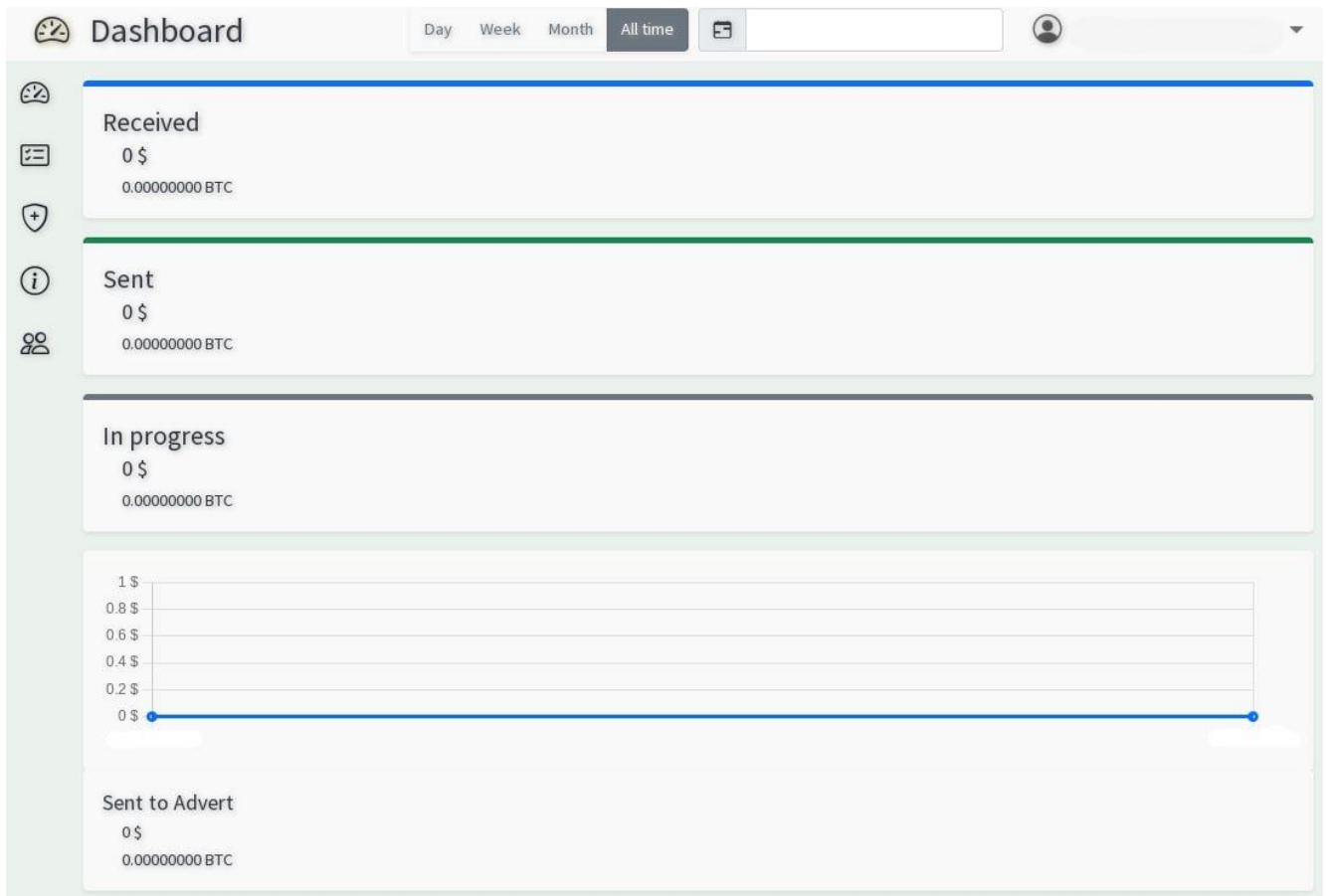
NoEscape 랜섬웨어는 2023 년 5 월에 등장하여 여러 산업분야에 공격을 진행하고 있다 서비스형 랜섬웨어(Ransomware-as-a-Service) 프로그램을 운영하며 개발자는 피해자의 데이터 유출, 파일 암호화 등의 악의적인 활동을 수행하는 데 필요한 악성코드를 생성하고 제공한다 이 그룹의 공격 대상은 국가 정부, 에너지 산업, 의료분야 등 다양한 산업분야를 대상으로 공격을 진행하고 있다. 현재는 존재하지 않는 Avaddon 랜섬웨어 그룹과 관련이 있는 것으로 추측하고 있다.

2. 상세분석

파일 이름	0073414c5a03b20f6f255f400291de67f2a7268c461f90ea6ff0355ca31af07a
운영체제	Windows
파일 타입	Executable
파일 크기	653 KB (669,184 bytes)
MD5	baa7c0e1d398cce0ebcfae8ce0aa0a0a
Sha256	0073414c5a03b20f6f255f400291de67f2a7268c461f90ea6ff0355ca31af07a
주요행위	파일 암호화 및 특정 서비스 및 프로세스 종료
특징	윈도우 및 리눅스, VMWare ESXi 서버에서 데이터를 암호화 한다

2.1 NoEscape 분석

NoEscape 랜섬웨어는 여러 산업 분야를 표적으로 삼고서 공격을 진행하는 악성코드이며 현재까지 정확한 감염 벡터는 밝혀지지 않았다 보안 기술 연구자인 EVIL RABBIT 의 트위터 게시물에는 Dashboard Panel 이미지와 Builder Page 이미지를 공유하고 있다.



[그림] 1 Dashboard Panel

제공된 이미지를 확인해보면 윈도우7 이상에서 사용할 수 있는 EXE 및 DLL 파일, DLL Injection, 윈도우XP 실행파일, Linux/ESXI 서버용 ELF 파일을 포함하여 다양한 빌드 기능을 제공하고 있으며 랜섬웨어 이름, 암호화 키, 랜섬 노트, 지불할 몸값, 타이머 등과 같은 기능도 제공하고 있다.

Locker build form

Locker name:

Key name:
 The name of the encryption key. You can create a build with an already existing key by specifying the key name.
 Don't use the same key for different companies!

Comment:

Price: \$
 Decryptor purchase price.

Timer type:
 You can use a timer to put extra pressure on the client. The timer can be omitted if you do not need it.
Double - after the time expires, the price will be doubled.
Leak - informs the client that his data has been stolen and will be published after the time expires

Here are the default settings for optimal Locker performance.
 Change these fields only if you clearly understand what you are doing!

Method: **All** Exe Dll Dllreflinj Xp Linux / ESXi
 You can create all lockers types with the same key by selecting **All**. May be useful for companies with different systems.
EXE - an executable file for operating systems Windows 7+.
DLL - Dll file for operating systems Windows 7+.

Primary paths:
 %ExchangeInstallPath%\Mailbox, %SYSTEMDRIVE%\Program Files (x86)\Microsoft SQL Server, %SYSTEMDRIVE%\Program Files (x86)\Microsoft\Exchange Server, %SYSTEMDRIVE%\Program Files

Preferred paths for encryption. These paths will be encrypted first. Separated by coma. **Available only for Windows.**

[그림] 2 Builder Page

악성코드는 악성 행위를 시작하기 전에 뮤텍스 값을 확인한다 뮤텍스 값은 운영체제 버전별로 다른 값을 확인하고 있다. ["Global\\W{3a26815b-763f-4659-b4f2-dca4e6dd3476}"]

0126CE9B	FF15 D8512A01	call dword ptr ds:[<&OpenMutexW>]	eax:L"Global\\{3a26815b-763f-4659-b4f2-dca4e6dd3476}"
0126CEA1	85C0	test eax, eax	
0126CEA3	75 18	jne escape.126CEC0	
0126CEA5	837E 14 08	cmp dword ptr ds:[esi+14], 8	esi:&L"Global\\{3a26815b-763f-4659-b4f2-dca4e6dd3476}";
0126CEA9	72 02	jb escape.126CEAD	esi:&L"Global\\{3a26815b-763f-4659-b4f2-dca4e6dd3476}";
0126CEAB	8B36	mov esi, dword ptr ds:[esi]	
0126CEAD	56	push esi	
0126CEAE	6A 00	push 0	
0126CEB0	6A 00	push 0	
0126CEB2	FF15 3C512A01	call dword ptr ds:[<&CreateMutexW>]	eax:L"Global\\{3a26815b-763f-4659-b4f2-dca4e6dd3476}";
0126CEB8	85C0	test eax, eax	
0126CEBA	74 04	je escape.126CEC0	esi:&L"Global\\{3a26815b-763f-4659-b4f2-dca4e6dd3476}";
0126CEBC	32C0	xor al, al	
0126CEBE	5E	pop esi	esi:&L"Global\\{3a26815b-763f-4659-b4f2-dca4e6dd3476}";
0126CEBF	C3	ret	
0126CEC0	B0 01	mov al, 1	esi:&L"Global\\{3a26815b-763f-4659-b4f2-dca4e6dd3476}";
0126CEC2	5E	pop esi	
0126CEC3	C3	ret	

[그림] 3 뮤텍스 확인

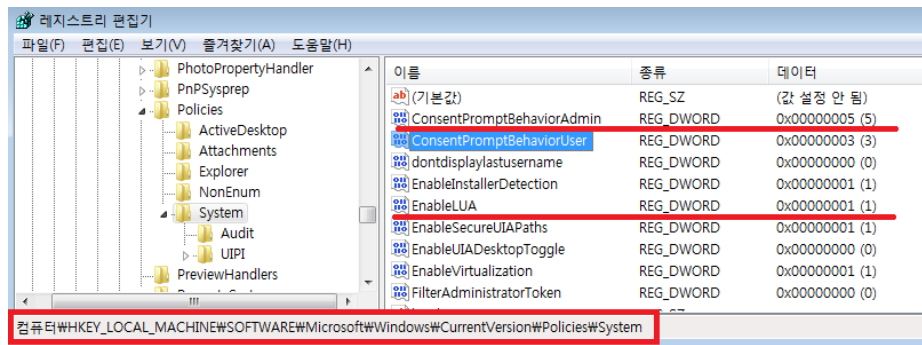
뮤텍스 값을 확인하여 기존 감염 여부를 확인하고 UAC를 비활성화하기 위해 레지스트리 값을 수정하게 된다.

컴퓨터\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA

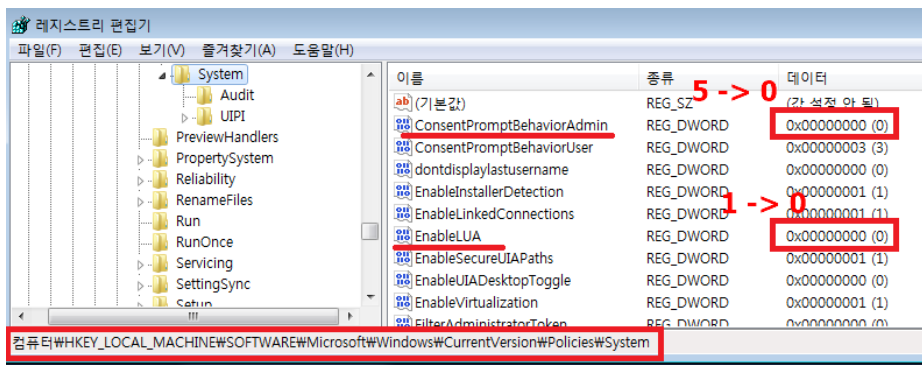
컴퓨터\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin

EnableLUA 데이터는 기본 1로 설정 되어 있으며 0으로 수정하여 UAC(사용자 계정 컨트롤)을 비활성화 한다.

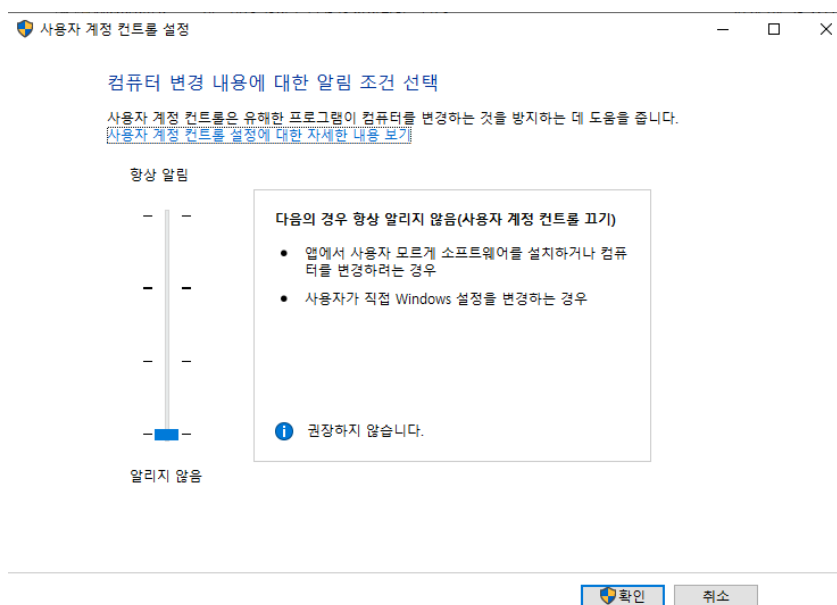
ConsentPromptBehaviorAdmin 데이터는 기본 5에서 0으로 수정 한다.



[그림] 4 UAC 관련 레지스트리



[그림] 5 UAC 비활성화

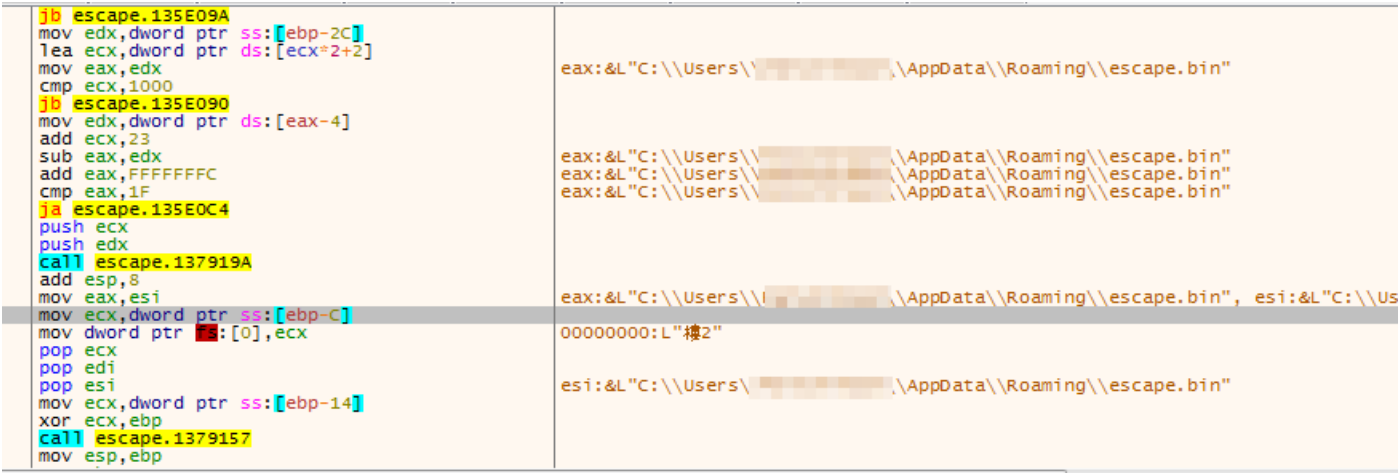


[그림] 5-1 UAC 비활성화

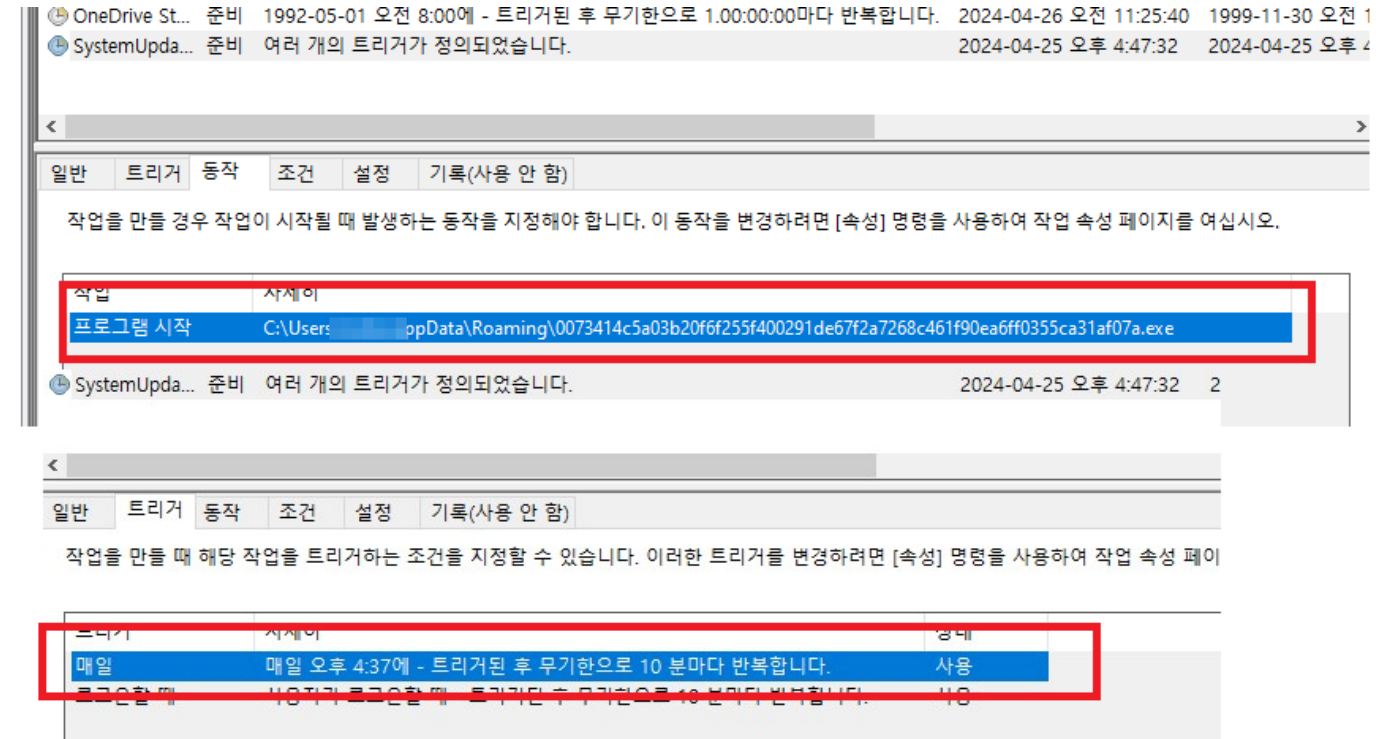
UAC를 비활성화 한 악성코드는 현재 실행되고 있는 경로에서 특정 경로로 악성코드를 복사하고 악성코드가 종료되더라도 계속해서 실행될 수 있도록 자동 스케줄러에 등록한다.

Path : "C:\Users\W[Users]\AppData\Roaming"

작업 스케줄러에 등록된 악성코드는 10분마다 반복 적으로 실행 되도록 설정되었다.



[그림] 6 파일 복사 이동



[그림] 7 작업스케줄러 등록

자동 스케줄러에 등록을 한 뒤에는 현재 실행되고 있는 프로세스 리스트를 검사하고 특정 프로세스가 실행되고 있다면 해당 프로세스를 종료시키는 행위를 하게 된다.



[그림] 8 프로세스 리스트 체크 및 종료

아래에 나열된 표에는 악성코드가 실행 중인 프로세스를 종료하는 상세 리스트이다.

360doctor	RAgui	ccleaner	infopath	mysqld-opt	powerpnt	sqlwriter	tomcat6	xfssvcccon
360se	RTVscan	ccleaner64	isqlplussvc	mysqld	procexp	steam	u8	vmcompute
Culture	agntsvc	dbeng50	java	ncsvc	qbupdate	supervise	ufida	vmwp
Defwatch	agntsgvcencsvc	dbsnmp	kingdee	ocautoupds	sqbcoreservice	synctime	visio	vmms
GDscan	agntsgvcisqlplussvc	encsvc	msaccess	ocomm	sql	taskkill	wdswfsafe	vds
MsDtSrvr	anvir	excel	msftesql	ocssd	sqlagent	tasklist	windord	
QBFCFMonitorService	anvir64	far	msspub	onedrive	sqlbrowser	tbirdconfig	wordpad	
QBDBMgr	apache	fdhost	mydesktopqos	onenote	sqlmangr	thebat	wuauclt	
QBIDPService	axlbridge	fdlauncher	mydesktopservice	oracle	sqlserver	thunderbird	wxServer	
QBW32	backup	httpd	mysqld-nt	outlook	sqlservr	tomcat	wxServerView	

[그림] 9 종료시키는 프로세스 리스트

악성코드는 실행 중인 프로세스뿐만 아니라 실행되고 있는 서비스 리스트도 확인하고 종료 시킨다.

```

v1 = lpServiceName;
v2 = 0;
if ( !*((_DWORD *)lpServiceName + 4) )
    return 0;
v3 = OpenSCManager(0, 0, 0xF003Fu);
v4 = v3;
if ( v3 )
{
    if ( *((_DWORD *)v1 + 5) >= 8u )
        v1 = *(LPCWSTR *)v1;
    v5 = OpenServiceW(v3, v1, 0x10020u);
    v6 = v5;
    if ( v5 )
    {
        v2 = DeleteService(v5) != 0;
        CloseServiceHandle(v6);
    }
    CloseServiceHandle(v4);
}
return v2;
}

```

W1*p.1...L...
 0.L...
 G.x.B.1.
 F...
 G.x.C.I.M.g.P...
 G.x.C.V.
 D...
 G.x.F.W.D...
 G.x.V.S.
 S...
 C.K...
 X.L...
 R.T.V.S.c.a.n...
 S.a.v.R.
 O.a.m...
 L...
 L...
 0.L...
 0.L...
 b.a.c.k.u.p...
 L...
 H.L...
 d.b.e.n...
 g.8...
 d.b.s.r.v.1.2...
 m.e.m.t...
 a.s...
 m.e.p.o.c.s...
 p.L...
 m.s.m.d.s.r.v...
 s.o.p.h...
 O.s...
 S.q.l...
 L...

[그림] 10 서비스 리스트 확인 및 종료

8	FF15 54503901	call dword ptr ds:[<&OpenServiceW>]	
E	88F0	mov esi,eax	esi:L"VMAuthdService"
0	85F6	test esi,esi	esi:L"VMAuthdService"
2	0F84 1E010000	je escape.1360106	
8	881D 5C503901	mov ebx,dword ptr ds:[<&QueryService>]	
E	8D45 F8	lea eax,dword ptr ss:[ebp-8]	
1	50	push eax	
2	6A 24	push 24	
4	8D45 D4	lea eax,dword ptr ss:[ebp-2C]	
7	C745 F4 00000000	mov dword ptr ss:[ebp-C],0	
E	50	push eax	
F	0F57C0	xorps xmm0,xmm0	
2	C745 F8 00000000	mov dword ptr ss:[ebp-8],0	
9	6A 00	push 0	
8	56	push esi	esi:L"VMAuthdService"
C	0F1145 D4	movups xmmword ptr ss:[ebp-2C],xmm0	
0	0F1145 E4	movups xmmword ptr ss:[ebp-1C],xmm0	
4	FFD3	call ebx	

[그림] 10-1 서비스 리스트 확인 및 종료

아래에 나열된 표에는 악성코드가 실행 중인 서비스를 종료하는 상세 리스트다.

Culserver	SavRoam	msexchange	tomcat6
DefWatch	VMAuthdService	msmdsrv	veeam
GxBlr	VMnetDHCP	sophos	vmware-converter
GxCIMgr	VMwareHostd	sql	vmware-usbarbiator64
GxCVD	backup	sqladhlp	vss
GxFWD	ccEvtMgr	sqlagent	
GxVss	dbeng8	sqlbrowser	
QBCFMonitorService	dbsrv12	sqlservr	
QBIDPService	memtas	sqlwriter	
RTVscan	mepocs	svc\$	

[그림] 10-2 종료 시키는 서비스 리스트

파일 암호화를 하기 전에 또 다른 디스크 볼륨이 있는지 확인하고 여러 경로에 "HOW_TO_RECOVER_FILES.txt" 파일을 생성한다.

```

a1[2] = 0;
sub_42B5D0(&v30, 0, 520);
v18 = FindFirstVolumeW((LPWSTR)&v30, 0x104u);
if ( v18 != (HANDLE)-1 )
{
    do
    {
        v4 = wcslen((const unsigned __int16 *)&v30);
        if ( v30 != 6029404 )
            break;
        if ( v31 != 63 )
            break;
        if ( v32 != 92 )
            break;
        v5 = 2 * v4 - 2;
        if ( *(_WORD *)((char *)&v39 + v5 - 544) != 92 )
            break;
        if ( v5 >= 0x208 )
        {
            sub_4292ED(v13);
LABEL_27:
            sub_42E4CF(v10, v13);
        }
        *(_WORD *)((char *)&v39 + v5 - 544) = 0;
        sub_42B5D0(&v29, 0, 520);
        v6 = QueryDosDeviceW((LPCWSTR)&v33, (LPWSTR)&v29, 0x104u);
        *(_WORD *)((char *)&v39 + v5 - 544) = 92;
        if ( v6 )
        {
            --

```

[그림] 11 디스크 볼륨 검색

0F83 A1020000	jae escape.1263F5A	eax:L"Volume{3261f7b7-9c1c-11e7-a9de-806e6f6e6963}"
33C0	xor eax, eax	eax:L"Volume{3261f7b7-9c1c-11e7-a9de-806e6f6e6963}"
68 08020000	push 208	
50	push eax	
66:89843D E0FDFFFF	mov word ptr ss:[ebp+edi-220], ax	
8D85 D8FBFFFF	lea eax, dword ptr ss:[ebp-428]	
50	push eax	eax:L"Volume{3261f7b7-9c1c-11e7-a9de-806e6f6e6963}"
E8 F8780200	call escape.12885D0	
83C4 0C	add esp, C	
8D85 D8FBFFFF	lea eax, dword ptr ss:[ebp-428]	
68 04010000	push 104	eax:L"Volume{3261f7b7-9c1c-11e7-a9de-806e6f6e6963}"
50	push eax	
8D85 E8FDFFFF	lea eax, dword ptr ss:[ebp-218]	eax:L"Volume{3261f7b7-9c1c-11e7-a9de-806e6f6e6963}"
50	push eax	
FF15 70512A01	call dword ptr ds:[<&QueryDosDeviceW>]	
B9 5C000000	mov ecx, 5C	5C:'\'

[그림] 11-1 디스크 볼륨 검색

56	push esi	
FF15 10513901	call dword ptr ds:[<&CloseHandles>]	
8B40 CC	mov ecx, dword ptr ss:[ebp-34]	
83F9 08	cmp ecx, 8	
72 2E	jnb escape.136AC64	[ebp-48]:L"C:\\Users\\...\\Desktop\\HOW_TO_RECOVER_FILES.txt"
8B55 B8	mov edx, dword ptr ss:[ebp-48]	
8D0C4D 02000000	lea ecx, dword ptr ds:[ecx*2+2]	edx:L"C:\\Users\\...\\Desktop\\HOW_TO_RECOVER_FILES.txt"
8BC2	mov eax, edx	
81F9 00100000	cmp ecx, 1000	
72 10	jnb escape.136AC5A	edx:L"C:\\Users\\...\\Desktop\\HOW_TO_RECOVER_FILES.txt"
8B50 FC	mov edx, dword ptr ds:[eax-4]	
83C1 23	add ecx, 23	edx:L"C:\\Users\\...\\Desktop\\HOW_TO_RECOVER_FILES.txt"
2BC2	sub eax, edx	
83C0 FC	add eax, FFFFFFFC	
83F8 1F	cmp eax, 1F	
77 63	ja escape.136ACBD	
51	push ecx	edx:L"C:\\Users\\...\\Desktop\\HOW_TO_RECOVER_FILES.txt"
52	push edx	
E8 39E50000	call escape.137919A	
83C4 08	add esp, 8	
8B4D E4	mov ecx, dword ptr ss:[ebp-1C]	
83F9 08	cmp ecx, 8	

[그림] 12 랜섬노트 생성

악성코드가 파일을 암호화하기 전에 특정 프로세스 및 서비스를 종료 후에 파일 암호화를 시작하는데 특정 확장자와 특정 경로에 있는 파일들은 암호화에서 제외하고 있다.

.exe	.ini	.rdp	.dat	.msi
.bat	.lnk	.scr	.dll	.msp
.bin	.lock	.shs	.drv	.pif
.cmd	.log	.swp	.hta	.prf
.com	.mod	.sys		
.cpl	.msc	.theme		

[그림] 13 암호화 제외 확장자 리스트

\$recycle.bin	%SYSTEMDRIVE%\Users\AllUsers	ProgramData
\$windows.~bt	%SYSTEMDRIVE%\Windows	Tor Browser
\$windows.~ws	%SYSTEMDRIVE%\Windows	Boot
windows.old	%SYSTEMDRIVE%\WINDOW	Google
%PROGRAMFILE(x86)%	AppData	PerfLogs
%PUBLIC%	EFI	System Volume Information
%TMP%	Intel	
%ProgramData%	MSOCache	
%SYSTEMDRIVE%\Program Files	Mozilla	
%USERPROFILE%\AppData	Program Files	

[그림] 14 암호화 제외 폴더 리스트

파일 암호화를 수행하기 위해서 악성코드는 Microsoft Enhanced RSA 및 AES Cryptographic Provider 라이브러리를 사용하게 되는데 CryptoAPI의 다양한 기능을 활용하여 암호화를 진행한다.

```

F6BF6 74 1F jz cryptsp.70EF6C17
F6BF8 FF75 10 push dword ptr ss:[ebp+10]
F6BFB 8D45 C8 lea eax,dword ptr ss:[ebp-38]
F6BFE 50 push eax
F6BFF FF15 5411EF70 call dword ptr ds:[<&RtlInitUnicodeString>]
F6C05 6A 01 push 1
F6C07 8D45 C8 lea eax,dword ptr ss:[ebp-38]
F6C0A 50 push eax
F6C0B 8D45 D8 lea eax,dword ptr ss:[ebp-28]
F6C0E 50 push eax
F6C0F FF15 2411EF70 call dword ptr ds:[<&RtlUnicodeStringToAnsiString>]
F6C15 8BC8 mov ecx,eax
F6C17 3BCE cmp ecx,esi
F6C19 7C D4 jz cryptsp.70EF68EF
F6C1B FF75 18 push dword ptr ss:[ebp+18]
F6C1E FF75 14 push dword ptr ss:[ebp+14]
F6C21 FF75 DC push dword ptr ss:[ebp-24]
F6C24 FF75 E4 push dword ptr ss:[ebp-1C]
F6C27 FF75 08 push dword ptr ss:[ebp+8]
F6C2A E8 24DEFFFF call <&cryptsp.CryptAcquireContextA>
F6C2F 8BF8 mov eax,dword ptr ss:[ebp-20]
F6C31 8D45 E0 lea eax,dword ptr ss:[ebp-20]
F6C34 50 push eax
F6C35 8B35 2011EF70 mov esi,dword ptr ds:[<&RtlFreeUnicodeString>]
F6C38 FFD6 call esi
F6C3D 8D45 D8 lea eax,dword ptr ss:[ebp-28]
F6C40 50 push eax
F6C41 FFD6 call esi
F6C43 C745 FC FFFFFFFF mov dword ptr ss:[ebp-4],FFFFFFF
F6C4A 8BC7 mov eax,edi
F6C4C 75 28 jmp cryptsp.70EF6C76
F6C4E 8B45 EC mov eax,dword ptr ss:[ebp-14]
F6C51 8B00 mov eax,dword ptr ds:[eax]
```

[그림] 15 파일 암호화

00F4F159	FF15 A050F700	call dword ptr ds:[<&MoveFileExw>]	
00F4F15F	888D 78FFFFFF	mov ecx, dword ptr ss:[ebp-88]	eax:L"C:\\87f315b3835d8e5314d75c2f005f0c51\\1029\\LocalizedData.xml"
00F4F165	85C0	test eax, eax	
00F4F167	0F95C0	setne al	
00F4F16A	8847 24	mov byte ptr ds:[edi+24], al	
00F4F16D	83F9 08	cmp ecx, 8	ecx:L"C:\\87f315b3835d8e5314d75c2f005f0c51\\1029\\LocalizedData.xml.HAFCIICJA"
00F4F170	72 35	jb escape.F4F1A7	[ebp-9C]:L"C:\\87f315b3835d8e5314d75c2f005f0c51\\1029\\LocalizedData.xml.HAFCIICJA"
00F4F172	8895 64FFFFFF	mov edx, dword ptr ss:[ebp-9C]	ecx:L"C:\\87f315b3835d8e5314d75c2f005f0c51\\1029\\LocalizedData.xml.HAFCIICJA"
00F4F178	8D0C4D 02000000	lea ecx, dword ptr ds:[ecx*2+2]	eax:L"C:\\87f315b3835d8e5314d75c2f005f0c51\\1029\\LocalizedData.xml"
00F4F17F	89C2	mov eax, edx	ecx:L"C:\\87f315b3835d8e5314d75c2f005f0c51\\1029\\LocalizedData.xml.HAFCIICJA"
00F4F181	81F9 00100000	cmp ecx, 1000	
00F4F187	72 14	jb escape.F4F190	
00F4F189	885D FC	mov edx, dword ptr ds:[eax-4]	ecx:L"C:\\87f315b3835d8e5314d75c2f005f0c51\\1029\\LocalizedData.xml.HAFCIICJA"
00F4F18C	83C1 23	add ecx, 23	eax:L"C:\\87f315b3835d8e5314d75c2f005f0c51\\1029\\LocalizedData.xml"
00F4F18F	28C2	sub eax, edx	eax:L"C:\\87f315b3835d8e5314d75c2f005f0c51\\1029\\LocalizedData.xml"
00F4F191	83C0 FC	add eax, FFFFFFFC	eax:L"C:\\87f315b3835d8e5314d75c2f005f0c51\\1029\\LocalizedData.xml"
00F4F194	83F8 1F	cmp eax, 1F	
00F4F197	0F87 B4000000	ja escape.F4F251	
00F4F19D	51	push ecx	ecx:L"C:\\87f315b3835d8e5314d75c2f005f0c51\\1029\\LocalizedData.xml.HAFCIICJA"
00F4F19E	52	push edx	
00F4F19F	E8 F69F0000	call escape.F5919A	
00F4F1A4	83C4 08	add esp, 8	

[그림] 15-1 파일 암호화

암호화를 진행하고 난 뒤에는 윈도우 명령어를 이용하여 시스템을 쉽게 복구하지 못하도록 하고 있다 vssadmin과 WMI를 이용하여 모든 볼륨 새도우 복사본을 제거하고 bcdedit을 이용하여 복구 모드로 부팅 되는 것을 막고 있다.

88F7	6666:0F1F8400 00000000	mov esi, edi	
8D8D	24FFFFFF	nop word ptr ds:[eax+eax], ax	
E8 35300000		lea ecx, dword ptr ss:[ebp-DC]	[ebp-DC]:L"SHADOWCOPY DELETE /nointeractive"
83EE 01		call escape.1360830	
		sub esi, 1	
75 F0		jne escape.135D7F0	
8D8D	3CFFFFFF	lea ecx, dword ptr ss:[ebp-C4]	[ebp-C4]:L"wmic SHADOWCOPY DELETE /nointeractive"
E8 A52B0000		call escape.1360380	
8D8D	54FFFFFF	lea ecx, dword ptr ss:[ebp-AC]	[ebp-AC]:L"wbadmin DELETE SYSTEMSTATEBACKUP -deleteoldest"
E8 9A2B0000		call escape.1360380	
8D8D	6CFFFFFF	lea ecx, dword ptr ss:[ebp-94]	[ebp-94]:L"wbadmin DELETE SYSTEMSTATEBACKUP -keepversions:0"
E8 8F2B0000		call escape.1360380	
8D4D	84	lea ecx, dword ptr ss:[ebp-7C]	[ebp-7C]:L"wbadmin DELETE BACKUP -deleteoldest"
E8 872B0000		call escape.1360380	
8D4D	9C	lea ecx, dword ptr ss:[ebp-64]	[ebp-64]:L"wbadmin DELETE BACKUP -keepversions:0"
E8 7F2B0000		call escape.1360380	
8D4D	B4	lea ecx, dword ptr ss:[ebp-4C]	[ebp-4C]:L"vssadmin Delete Shadows /All /Quiet"
E8 772B0000		call escape.1360380	
8D4D	CC	lea ecx, dword ptr ss:[ebp-34]	[ebp-34]:L"bcdedit /set {default} recoveryenabled No"
E8 6F2B0000		call escape.1360380	
8D4D	E4	lea ecx, dword ptr ss:[ebp-1C]	[ebp-1C]:L"bcdedit /set {default} bootstatuspolicy ignoreallfailures"
E8 672B0000		call escape.1360380	
83EF 01		sub edi, 1	
75 B2		jne escape.135D800	
884D F8		mov ecx, dword ptr ss:[ebp-8]	
83F9 08		cmp ecx, 8	
72 32		jb escape.135D888	
8855 E4		mov edx, dword ptr ss:[ebp-1C]	
8D0C4D 02000000		lea ecx, dword ptr ds:[ecx*2+2]	
88C2		mov eax, edx	

[그림] 16 복구 옵션 및 백업 삭제

다음으로는 SHEmptyRecycleBinW API를 이용하여 윈도우 휴지통을 비우고 있다.

0	6A 07	push 7	
2	6A 00	push 0	
4	6A 00	push 0	
6	FF15 F0520900	call dword ptr ds:[<&SHEmptyRecycleBinw>]	
C	C3	ret	
D	CC	int3	
E	CC	int3	
F	CC	int3	

[그림] 17 휴지통 삭제

파일이 암호화되고 나면 이 악성코드는 바탕화면 이미지를 변경하고 랜섬 노트를 실행하여 피해자가 랜섬웨어에 감염된 것을 알려주고 공격자에게 연락할 수 있는 Tor 주소를 알려주며 접속을 유도하고 있다. 바탕화면 이미지 파일은 악성코드 복사본의 경로와 동일 한 위치에 존재한다.

Path : "C:\Users\W[Users]\AppData\Roaming"

결론

해당 랜섬웨어는 감염 벡터가 정확히 밝혀지지 않았다 기존 랜섬웨어들과 마찬가지로 파일 암호화를 진행하고 감염된 피해자에게 몸값을 요구하며 시스템을 복구할 수 없도록 하고 있다 윈도우는 기본이고 리눅스 버전에서도 동작하는 형태이며 RaaS(Ransomware-as-a-Service) 서비스형 랜섬웨어로 타겟 대상에 따라 공격 기능이 달라질 수 있다 이메일에 매크로가 포함된 파일을 첨부하여 배포될 수 있으니 첨부파일이 포함된 이메일을 확인할 때는 각별한 주의가 필요하다.

IOC 정보

Windows

07c70968c66c93b6d6c9a90255e1c81a3b385632c83f53f69534b3f55212ced9
68e5caa3f0fd4adc595b1163bf0dd30ca621c5d7a6ad0a20dfa1968346daa3c8
0073414c5a03b20f6f255f400291de67f2a7268c461f90ea6ff0355ca31af07a
2020cae5115b6980d6423d59492b99e6aaa945a2230b7379c2f8ae3f54e1efd5
4175dae9b268fe5b4f96055ea0376417b5ddc2518d3bd11e20f0f8255bb4621e
4d7da1654f9047b6c6a9d32564a66684407ed587cbaffa54ec1185fd73293d3e
5300d7456183c470a40267da9cd1771d6147445b203d8eb02437348bf3169e0d
53f5c2f70374696ff12adcaaf1bbbe0e5dd1b1995d98f2e876b0671888b43128
62205bf0a23e56524f2f1c44897f809457ad26bc70810008ec5486e17c7e64e2
68bce3a400721d758560273ae024f61603b8a4986440a8ec9e28305d7e6d02b0
68ff9855262b7a9c27e349c5e3bf68b2fc9f9ca32a9d2b844f2265dccc2bc0d8
73c19eab8d2ae58db3968dd7de0e745db2d7709859305b113b748bb02494465e
831a2409d45d0c7f15b7f31eddbbdfef7d58414499e81b3da7d9fdee28fafe646
8dd64ea7f226d3eb1e857b0086c0668542652cb37f8142dc000272dbd9569e31
91c515d55fae6d21b106c8c55067ce53d42bef256bd5a385cadd104cf68f64ff
9d346518330eeefbf288aeca7b2b6243bc158415c7fee3f2c19694f0e5f7d51c

linux

21162bbd796ad2bf9954265276bfebea8741596e8fe9d86070245d9b5f9db6da
aa5a487db37ce176e17c7abbb2b1d460ba926344e46737f2f64b65bf5a4a3e58
16d9e969457a76874e7452e687a7b6843c65ef75d1a4404d369074ad389f6c38
c34c5dd4a58048d7fd164e500c014d16befa956c0bce7cae559081d57f63a243
46f1a4c77896f38a387f785b2af535f8c29d40a105b63a259d295cb14d36a561
10d2b5f7d8966d5baeb06971dd154dc378496f4e5faf6d33e4861cd7a26c91d7