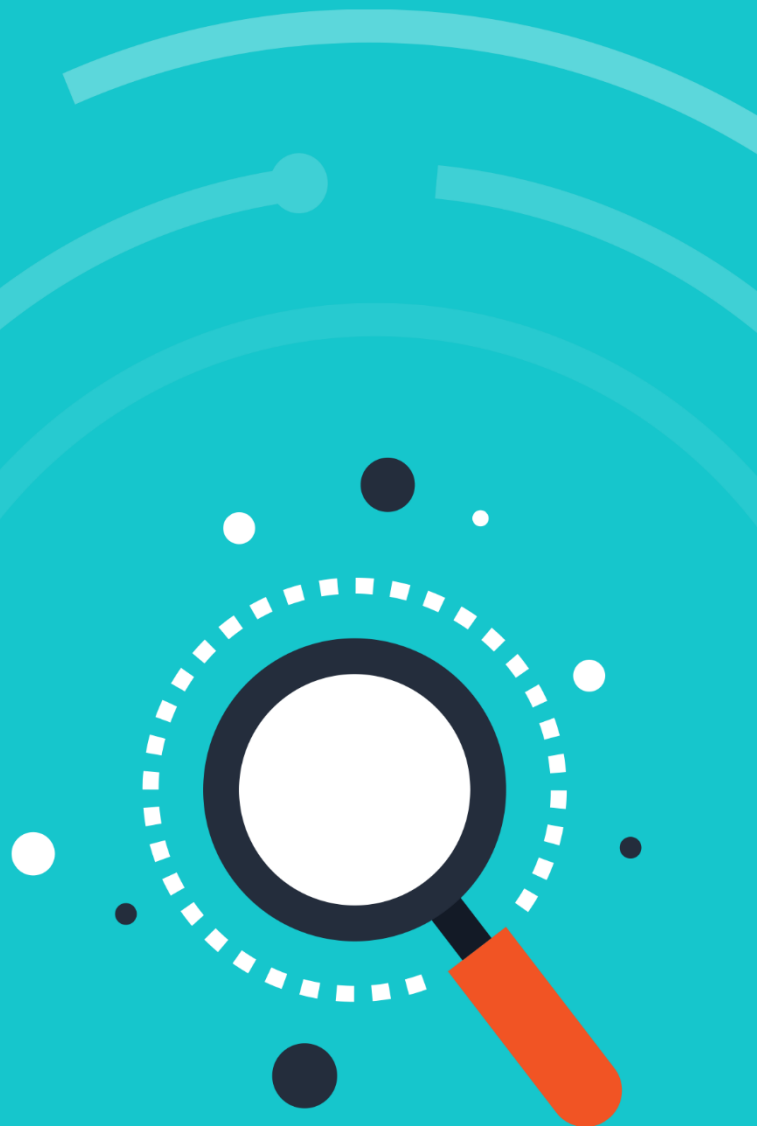


보안위협분석

DarkRace ransomware 분석

2024 년 09 월 30 일

(주)파이오링크 사이버위협분석팀

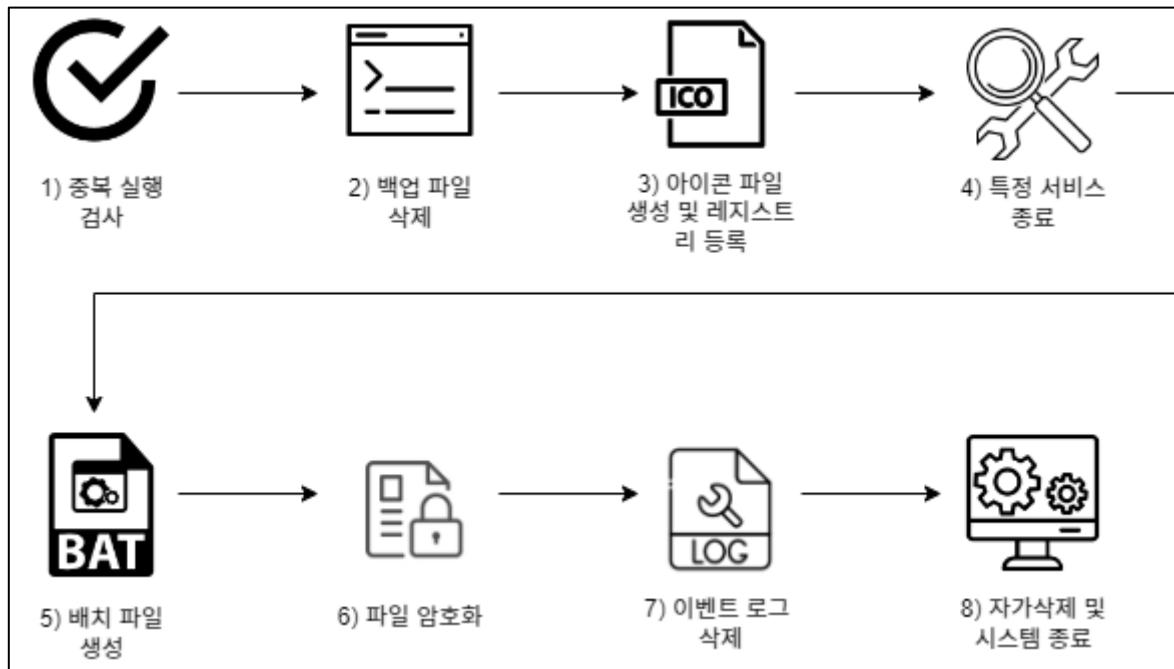


상세분석

1.1 분석 정보

74b5e2d90daaf96657e4d3d800bb20bf189bb2cf487479ea0facaf6182e0d1d3.bin			
MD5	cb1c423268b1373bde8a03f36f66b495		
SHA-256	74b5e2d90daaf96657e4d3d800bb20bf189bb2cf487479ea0facaf6182e0d1d3		
File Type	Win32 EXE	File Size	238.01 KB
주요 행위	파일 암호화 후 금전 요구		
드롭 파일	icon.ico 1.bat		

1.2 도식도



- 1) 악성코드 중복 실행 검사
- 2) 백업 파일 삭제
- 3) 아이콘 파일 생성 및 레지스트리 등록
- 4) 특정 서비스 종료
- 5) 배치 파일 생성
- 6) 파일 암호화
- 7) 이벤트 로그 삭제
- 8) 악성코드 자가 삭제 및 시스템 종료

DarkRace ransomware 분석

악성코드 실행 시 중복 실행 방지를 위해 뮤텍스를 생성한다.

003FF804	013D30E5	CALL to CreateMutexA from 74b5e2d9.013D30DF
003FF808	00000000	pSecurity = NULL
003FF80C	00000001	InitialOwner = TRUE
003FF810	013F94AC	MutexName = "CheckMutex"

[그림 1] 뮤텍스 생성

뮤텍스를 생성한 후 파일 복구를 방지하기 위해 총 2가지의 명령줄을 실행해 볼륨 새도우 카피를 삭제한다.

003FF7FC	013D328C	CALL to WinExec from 74b5e2d9.013D3286
003FF800	004EC658	CmdLine = "cmd /c "wmic shadowcopy delete /nointeractive""
003FF804	00000000	ShowState = SW_HIDE

[그림 2] 볼륨 새도우 카피 삭제

실행 명령어	
cmd /c "wmic shadowcopy delete /nointeractive"	볼륨 새도우 카피 삭제
cmd /c "vssadmin Delete Shadow /All /Quiet"	

아이콘 파일을 생성하며, 해당 아이콘을 레지스트리에 등록하여 암호화된 파일이 해당 아이콘으로 변경되도록 설정한다.

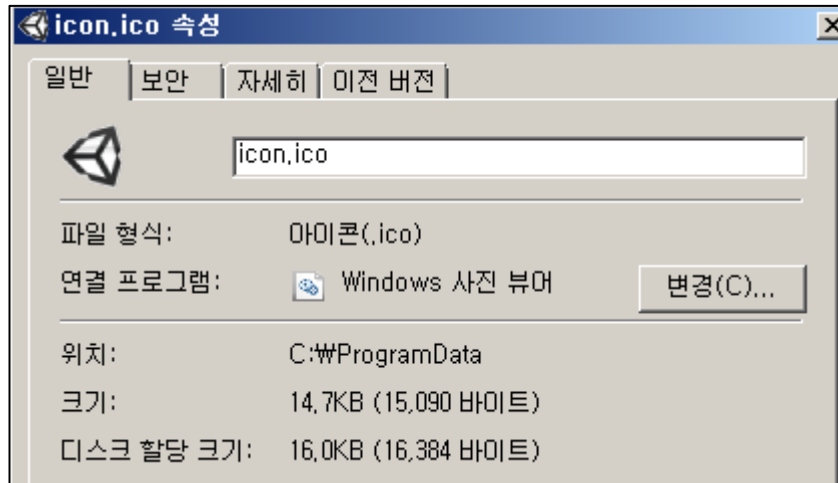
- 아이콘 파일 생성 경로 : "C:\WProgramData\icon.ico"

```

v0 = sub_4176F3("C:\WProgramData\icon.ico", &unk_42946C);
v1 = sub_4105B0(dword_43E0EC, dword_43E0EC, "ico", 0, 0, 1);
v2 = (const char *)sub_401990(v1);
sub_408A50(0, 0, &v11, v2, strlen(v2));
v3 = sub_401960(v11);
sub_408A50(v3, v11, &v11, v2, strlen(v2));
sub_417942(v3, 1, v11, v0);
sub_4175B2(v0);
sub_402680(&SubKey, ".%ls", (char)lpWideCharStr);
sub_402680(&Data, "%lsfile", lpWideCharStr);
RegCreateKeyExA(HKEY_CLASSES_ROOT, &SubKey, 0, 0, 0, 0xF003Fu, 0, &phkResult, &dwDisposition);
RegSetValueExA(phkResult, 0, 0, 1u, &Data, strlen((const char *)&Data));
RegCloseKey(phkResult);

```

[그림 3] 아이콘 생성



[그림 4] 생성된 아이콘

003FF6F8	013D3511	CALL to RegCreateKeyExA from 74b5e2d9.013D350F
003FF6FC	80000000	hKey = HKEY_CLASSES_ROOT
003FF700	003FF72C	Subkey = ".3fe57B660"
003FF704	00000000	Reserved = 0x0
003FF708	00000000	Class = NULL
003FF70C	00000000	Options = REG_OPTION_NON_VOLATILE
003FF710	000F003F	Access = KEY_ALL_ACCESS
003FF714	00000000	pSecurity = NULL
003FF718	003FF7F8	pHandle = 003FF7F8
003FF71C	003FF7F4	pDisposition = 003FF7F4

[그림 5] 레지스트리 등록

003FF6F8	013D358E	CALL to RegCreateKeyExA from 74b5e2d9.013D358C
003FF6FC	80000000	hKey = HKEY_CLASSES_ROOT
003FF700	003FF790	Subkey = "3fe57B660file\DefaultIcon"
003FF704	00000000	Reserved = 0x0
003FF708	00000000	Class = NULL
003FF70C	00000000	Options = REG_OPTION_NON_VOLATILE
003FF710	000F003F	Access = KEY_ALL_ACCESS
003FF714	00000000	pSecurity = NULL
003FF718	003FF7F8	pHandle = 003FF7F8
003FF71C	003FF7F4	pDisposition = 003FF7F4

[그림 6] 레지스트리 등록

그 후 원활한 악성 행위를 위해 특정 서비스를 찾아 종료한다.

```

v1 = OpenSCManager(0, 0, 0xF003Fu);
hSCObject = v1;
if ( v1 || (result = OpenSCManager(0, 0, 5u), v1 = result, (hSCObject = result) != 0) )
{
    EnumServicesStatusExA(v1, 0, 0x30u, 3u, 0, 0, &pcbBytesNeeded, &ServicesReturned, 0, 0);
    v3 = pcbBytesNeeded + 44;
    lpServices = (LPBYTE)sub_416E4B(pcbBytesNeeded + 44);
    sub_413B10(lpServices, 0, v3);
    if ( EnumServicesStatusExA(v1, 0, 0x30u, 3u, lpServices, v3, &pcbBytesNeeded, &ServicesReturned, 0, 0) )
    {
        v4 = 0;
        if ( ServicesReturned )

```

[그림 7] 서비스 종료

종료 대상 서비스		
vss	sql	Svc\$
memtas	mepocs	msexchange
sophos	veeam	backup
GxVss	GxBlr	GxFWD
GxCVD	GxCIMgr	

서비스 종료 후 배치 파일을 생성하며, 해당 배치파일에는 특정 프로세스 종료를 위한 명령줄이 기록된다. 배치 파일을 생성한 후 WinExec 함수를 통해 실행한다.

- 배치파일 생성 경로 : "C:\ProgramData\W1.bat"

```

02A4F758 013F4C61 [CALL to CreateFileW from 74b5e2d9.013F4C5B
02A4F75C 005328B0   FileName = "C:\ProgramData\W1.bat"
02A4F760 40000000   Access = GENERIC_WRITE
02A4F764 00000003   ShareMode = FILE_SHARE_READ!FILE_SHARE_WRITE
02A4F768 02A4F7DC   pSecurity = 02A4F7DC
02A4F76C 00000002   Mode = CREATE_ALWAYS
02A4F770 00000080   Attributes = NORMAL
02A4F774 00000000   hTemplateFile = NULL

```

[그림 8] 배치 파일 생성

종료 대상 프로세스	
sql	Oracle
chrome	Veeam
mysql	firefox
excel	msaccess
onenote	outlook
powerpnt	winword
wuauclt	

명령줄
<pre>:start ping 127.0.0.1 -n 2 >nul & taskkill /f /im sql* & taskkill /f /im oracle* & taskkill /f /im mysq* & taskkill /f /im chrome* & taskkill /f /im veeam* & taskkill /f /im firefox* & taskkill /f /im excel* & taskkill /f /im msaccess* & taskkill /f /im onenote* & taskkill /f /im outlook* & taskkill /f /im powerpnt* & taskkill /f /im winword* & taskkill /f /im wuauc* goto start</pre>

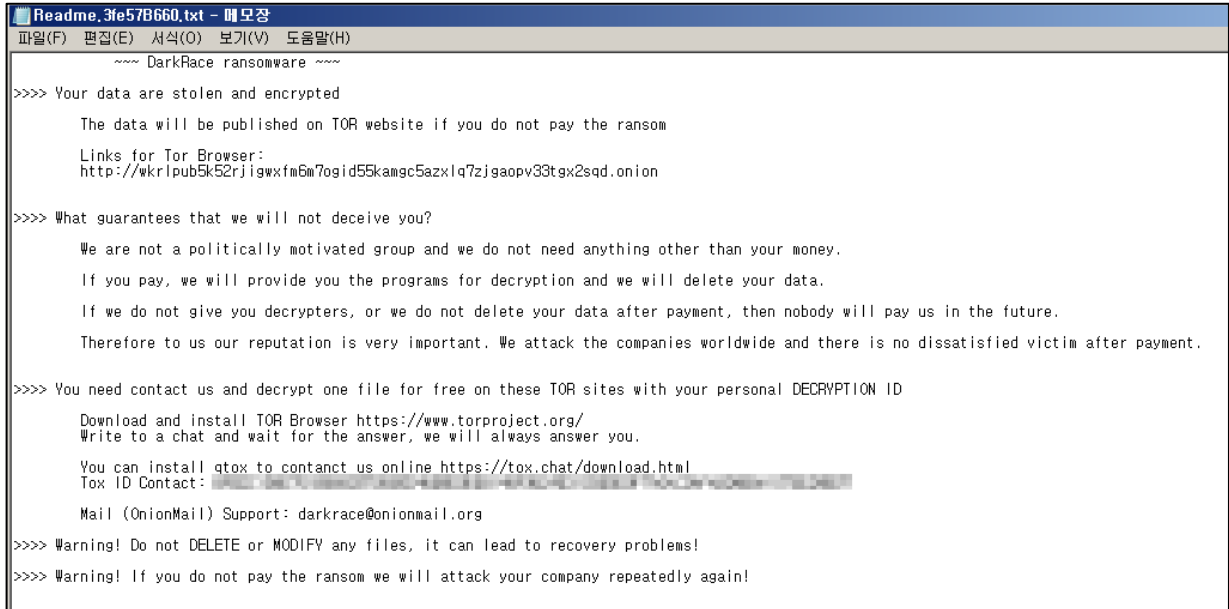
폴더 및 드라이브를 순회하며 암호화 대상 폴더인지, 암호화 대상 파일인지 비교하여 암호화를 진행하며 [원본 파일명].[원본 파일 확장자].3fe57B660 형식으로 파일명을 변경한다. 암호화된 파일은 이전에 생성한 아이콘 이미지로 아이콘이 변경된다. 크기가 큰 파일은 약 0x100000 영역까지만 부분 암호화된다.

<pre>v38 = MapViewOfFile((HANDLE)pnProcInfo, 0xF001Fu, v33, v30, dwNumberOfBytesToMap); dwFileOffsetHigh = (DWORD)v38; if (!v38) goto LABEL_60; sub_4045F0(dword_43E0D8, 1, &v46, 0, v38, dwNumberOfBytesToMap); UnmapViewOfFile((LPCVOID)dwFileOffsetHigh); v32 = dwRebootReasons; v34 = HIWORD(v50) + 1; HIWORD(v50) = v34; } while (v34 < v52); v39 = dwFileOffsetLow; LODWORD(v40) = sub_412AB0(dwFileOffsetLow, a4, v50, 0); v41 = v40; if (v40) { if (SHIWORD(v40) < 0 SHIWORD(v40) <= 0 && !(_DWORD)v40) { v42 = 0; goto LABEL_59; } v42 = (char *)MapViewOfFile((HANDLE)pnProcInfo, 0xF001Fu, (__PAIR__(a4, v39) - v40) >> 32, v39 - v40, v40 + 512); if (v42) { memcpy(&v42[v41], lpBuffer, 0x200u); goto LABEL_59; } }</pre>
--

[그림 9] 파일 암호화

암호화 제외 확장자
386;adv;ani;bat;bin;cab;cmd;com;cpl;cur;deskthemepack;diagcab;diagcfg;diagpkg;dll;drv;exe;hlp;icl;icns;ico;ics;idx;lnk;mod;mpa;msc;msp;msstyles;msu;nls;no-media;ocx;prf;ps1;rom;rtp;scr;shs;spl;sys;theme;themepack;wpz;lock;key;hta;msi;pdb;search-ms
암호화 제외 파일
bootmgr;autorun.inf;boot.ini;bootfont.bin;bootsect.bak;desktop.ini;iconcache.db;ntldr;ntuser.dat;ntuser.dat.log;ntuser.ini;thumbs.db;GDIPFONTCACHEV1.DAT;d3d9caps.dat
암호화 제외 폴더

\$recycle.bin;config.msi;\$windows.~bt;\$windows.~ws;windows;boot;program files;program files (x86);programdata;system volume information;tor browser;windows.old;intel;msocache;perflogs;x64dbg;public;all users;default;microsoft;appdata

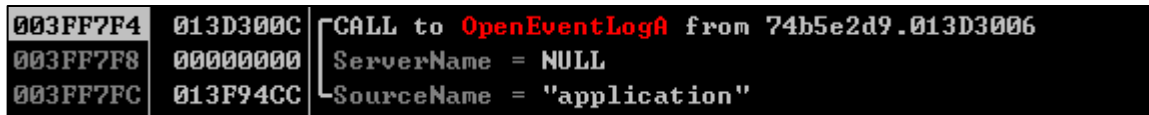


[그림 10] 랜섬노트

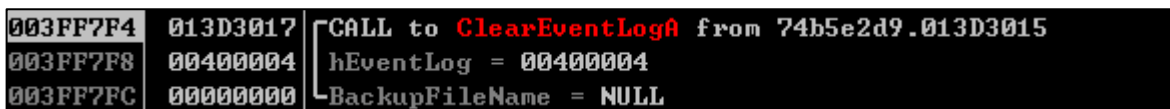
🔍 _bsddb.pyd, 3fe57b660	2024-09-26 오후 ...	3FE57B660 파일	989KB
🔍 _ctypes.pyd, 3fe57b660	2013-11-10 오후 ...	3FE57B660 파일	86KB
🔍 _ctypes_test.pyd, 3fe57b660	2024-09-26 오후 ...	3FE57B660 파일	16KB
🔍 _elementtree.pyd, 3fe57b660	2024-09-26 오후 ...	3FE57B660 파일	126KB
🔍 _hashlib.pyd, 3fe57b660	2024-09-26 오후 ...	3FE57B660 파일	351KB
🔍 _msi.pyd, 3fe57b660	2024-09-26 오후 ...	3FE57B660 파일	48KB
🔍 _multiprocessing.pyd, 3fe57b660	2024-09-26 오후 ...	3FE57B660 파일	27KB
🔍 _socket.pyd, 3fe57b660	2024-09-26 오후 ...	3FE57B660 파일	44KB
🔍 _sqlite3.pyd, 3fe57b660	2024-09-26 오후 ...	3FE57B660 파일	47KB

[그림 11] 변경된 아이콘

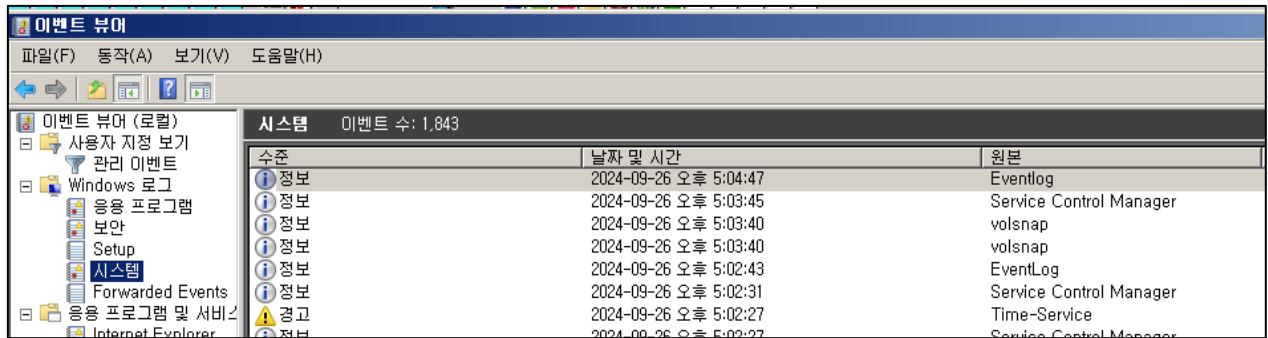
암호화를 완료한 후 악성행위를 숨기기 위해 이벤트로그를 차례로 삭제한다.



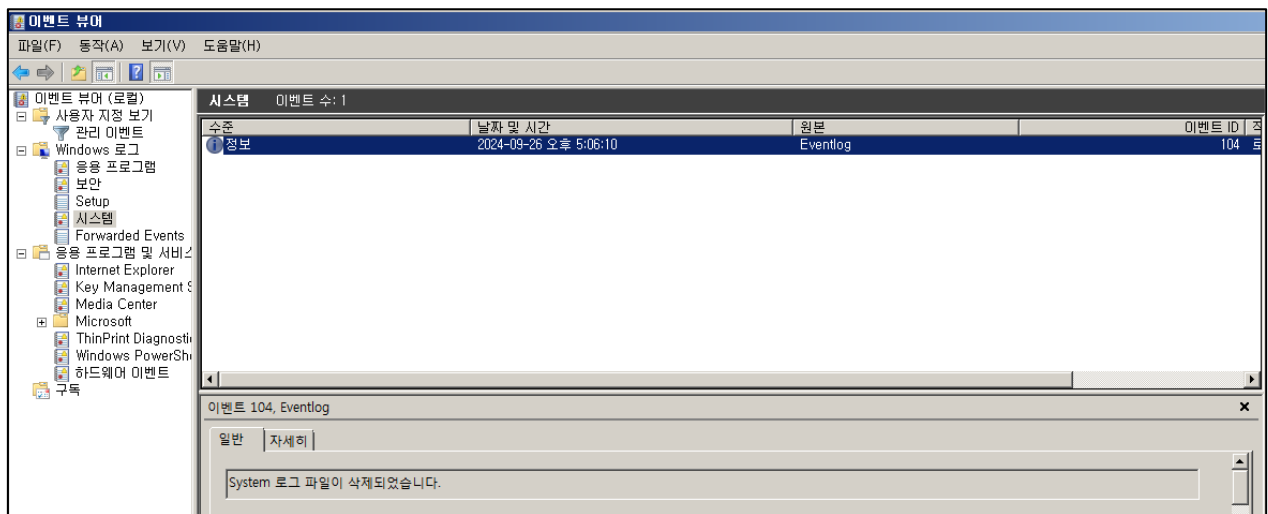
[그림 12] 이벤트 로그 오픈



[그림 13] 이벤트 로그 삭제



[그림 14] 로그 삭제 전



[그림 15] 로그 삭제 후 (system 로그 파일 삭제 로깅)

이벤트 로그를 삭제한 후 생성한 배치 파일 및 악성코드를 자가 삭제한 후 재부팅한다.

```
003FF7F4 013D30BF CALL to WinExec from 74b5e2d9.013D30BD
003FF7F8 012987D0 CmdLine = "cmd /c "ping 127.0.0.1 & del C:\ProgramData\1.bat & del C:\
003FF7FC 00000000 ShowState = SW_HIDE
```

[그림 16] 삭제 및 재부팅 명령줄 실행

실행 명령줄
cmd /c "ping 127.0.0.1 & del C:\ProgramData\1.bat & del C:\Users\Administrator\Desktop\74b5e2d90daaf96657e4d3d800bb20bf189bb2cf487479ea0facaf6182e0d1d3.bin.sample & shutdown -r -f -t 0"

결론

2022년 4월에 최초로 등장한 것으로 추측되는 DarkRace 랜섬웨어는 이후 많은 리브랜딩을 거쳐 현재는 DoNex라는 이름의 랜섬웨어로 활동하고 있다.

DarkRace 랜섬웨어는 암호화 파일 아이콘 변경, 프로세스 종료를 위한 배치파일 생성 등 Lockbit 3.0과 매우 유사한 부분이 있으며, 일부 샘플에서는 랜섬노트에 Lockbit 3.0 사칭하기도 한다. 계속해서 리브랜딩을 해 활동하는 만큼 새로운 기능들이 추가될 수 있어 주의가 필요하다.

해당 악성코드의 감염을 막기 위해 Windows 업데이트와, 사용 중인 백신의 버전을 최신으로 유지할 것을 권고한다.

IoC

- 74b5e2d90daaf96657e4d3d800bb20bf189bb2cf487479ea0facaf6182e0d1d3
- 0e60d49a967599fab179f8c885d91db25016be996d66a4e00cbb197e5085efa4
- 0adde4246aaa9fb3964d1d6cf3c29b1b13074015b250eb8e5591339f92e1e3ca
- 6d6134adfdf16c8ed9513aba40845b15bd314e085ef1d6bd20040afd42e36e40
- b32ae94b32bcc5724d706421f915b7f7730c4fb20b04f5ab0ca830dc88dcce4e