DoubleZero Wiper

우크라이나 주요기관 및 기업 인프라 파괴목적 삭제형 악성코드 감염시 수 초 내 시스템 파괴

목차

1. 개요

1.1 배경

러시아의 국가 해커들은
러시아와 우크라이나의 전면전과 함께 총성없는 사이버전을 수행하고 있다.
상대 국가의 주요 시스템을 파괴하는 악성코드를 제작 및 유포하고 있다.

이들은 우크라이나의 특정 기업과 기관을 상대로 악성코드를 제작하였으며,
이를 통한 감염으로 우크라이나의 주요 기관 및 기업 담당자 뿐만 아니라
PC를 사용하는 일반 사용자까지 시스템 파괴 공격을 받았다.
악성코드는 정상적인 파일로 위장되었으며,
공격 대상이 악성파일을 실행하면 시스템은 단 몇 초 내로 파괴된다.

DoubleZero Wiper는 감염 후 PC 내 모든 주요 정보, 부팅, 시스템 구성에 필요한 모든 데이터를
한 순간에 파괴한다. 이러한 공격을 수행하는 악성코드 그룹은 아래와 같다.

코드명	종류	유포 방식	주요 행위
Hermetic	Wiper	스피어 피싱	시스템 파괴
Isaac	Wiper	스피어 피싱	시스템 파괴
Caddy	Wiper	스피어 피싱	시스템 파괴
DoubleZero	Wiper	스피어 피싱	시스템 파괴

[표 1] 러시아 국가 해커의 시스템 파괴 악성코드 (Wiper)

국가 단위의 지원을 받는 해커들은 총과 칼이 아닌 총성 없는 사이버 전을 통해
지속적으로 주요 사회 기반 시설 및 기관과 기업을 대상으로 파괴 공작을 수행한다.
이들은 '금전이득'이 아닌 '파괴'가 목적이다.

2. 파일정보

2.1 파일정보

Name	[DoubleZero].exe (가칭)
Type	Portable Executable File
Behavior	System Destruction
SHA-256	30b3cbe8817ed75d8221059e4be35d5624bd6b5dc921d4991a7adc4c3eb5de4a

[파일 1] 주요 시스템 파일로 위장한 러시아 국가 해커의 DoubleZero Wiper 악성코드

3. 파일정보

3.1 파일정보

[그림 1] 우크라이나 정부 및 기관과 기업을 공격한 러시아 국가 해커

[주요 공격 흐름 : ①~③]

①	러시아 국가 해커의 DoubleZero Wiper 제작 러시아 국가 해커는 지속적으로 Wiper를 제작하였으며, 최근 본 보고서의 네 번째 DoubleZero Wiper를 제작했다.
②	주요 정부 기관 및 기업을 상대로 스피어 피싱 메일 발송 우크라이나의 주요 정부와 기관 및 기업을 상대로 스피어 피싱 메일을 발송하였으며, 발송한 메일 내에는 본 보고서의 DoubleZero Wiper가 첨부 되어있다.

③	**기관 및 기업의 주요 시스템 파괴** DoubleZero Wiper에 감염된 주요 시스템은 파괴되어 복구가 불가능하도록 변경된다. 해당 시스템 파괴 행위의 주요 흐름은 다음과 같다.
	1. 정상 시스템 파일 위장 2. 도메인 컨트롤러 여부 확인 3. 주요 대상 드라이브 목록 획득 4. 파괴 대상 폴더 및 파일 목록 열거 5. 중요도에 따라 우선순위를 정해 파일 제거 6. 레지스트리 파괴 7. 보안 강화 프로세스 종료 8. 부팅 및 시스템 유지가 불가능한 파괴

[표 2] DoubleZero Wiper의 시스템 파괴 흐름

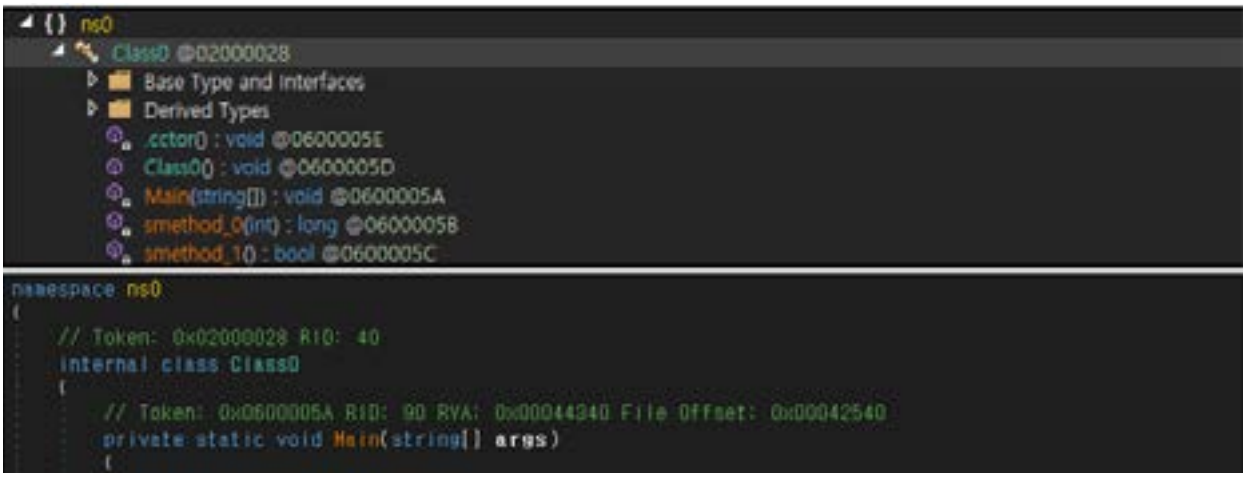
4. 파일정보

4.1 시스템 프로세스 위장과 난독화

[그림 2] CSRSS로 명명된 내부 명칭 및 난독화된 코드

DoubleZero Wiper는 CSRSS라는 내부 명칭으로 위장되어있다.
CSRSS는 윈도우 시스템에 기본으로 동작하는 프로세스로, 마이크로소프트의 클라이언트 서버 런타임이다.
DoubleZero Wiper는 위와 같이 CSRSS라는 명칭으로 위장하였으며,
내부 코드는 Main이 시작되는 진입점을 확인할 수 없을 정도로 복잡하게 난독화되어 있다.

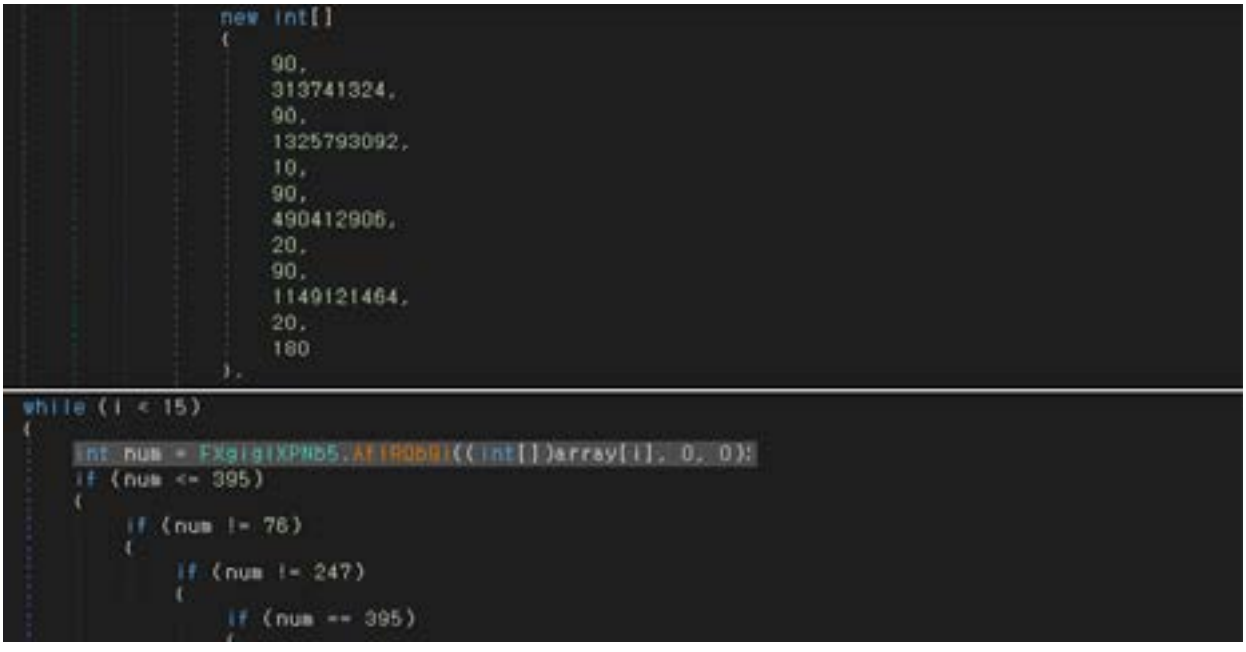
4.2 난독화 해제



[그림 3] 난독화가 해제된 DoubleZero Wiper 코드

DoubleZero Wiper의 난독화는 상용이 아닌 악성코드 제작자가 특수하게 만든 난독화 방식으로
이를 해제하면 위와 같이 .NET Class와 Main 등을 확인할 수 있다.

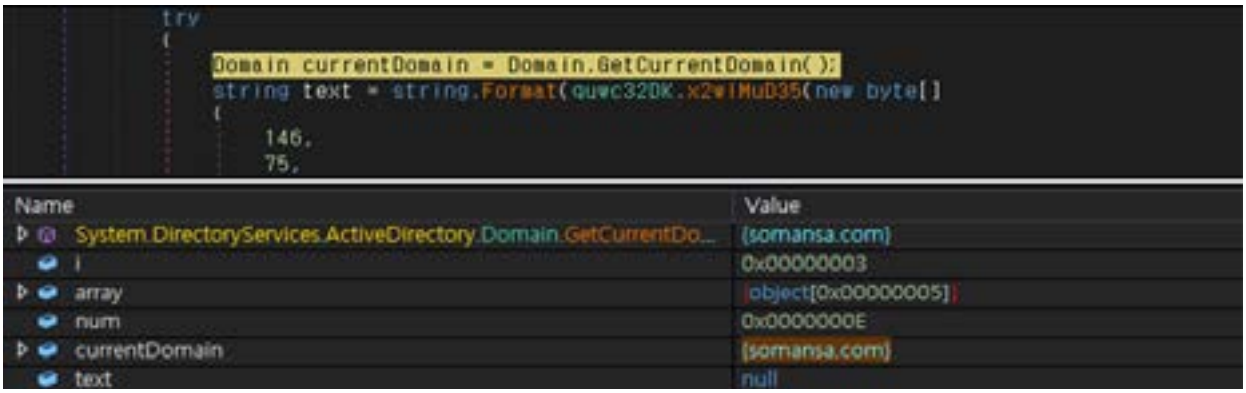
4.3 정수 배열을 통한 2차 난독화



[그림 4] 정수 배열을 통한 2차 난독화

정수 형태의 배열을 요소로 사용하여, 특정 메서드들을 호출한다.
해당 메서드 내부에는 실제 수행 시 사용되는 악의적인 행위들이 포함되어있다.
DoubleZero Wiper의 모든 악성 행위는 위와 같이 배열 내 정수를 통해
난독화된 코드를 난독화 해제를 수행하며 실행된다.

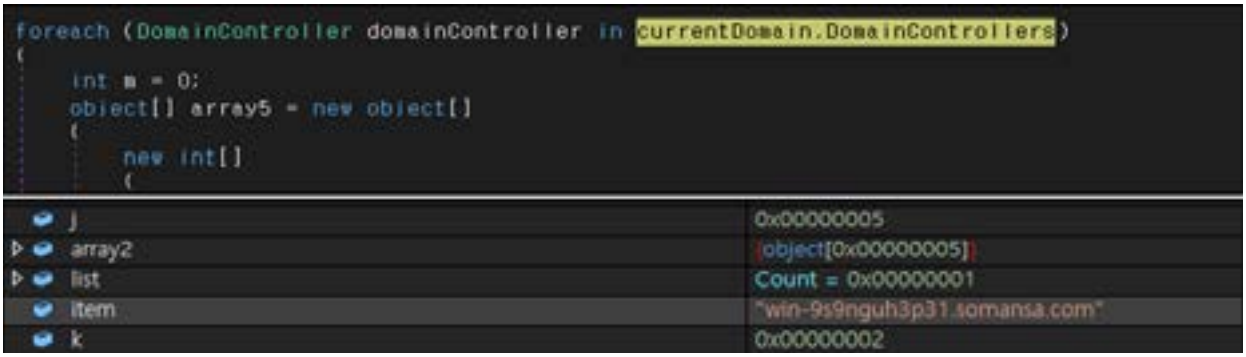
4.4 사용자 자격 증명에 대한 도메인 개체 확인



[그림 5] 사용자 자격 증명에 대한 도메인 개체 확인

.NET 메서드인 GetCurrentDomain을 호출하여 현재 사용자 자격 증명에 대한
도메인 컨트롤러 개체를 가져 온 후
이를 ActiveDirectory Domain Type의 currentDomain에 저장하여 결과를 확인한다.
이는 감염된 기기가 도메인 컨트롤러 중 하나인지 확인하고, 아니면 실행을 중지하는 행위이다.

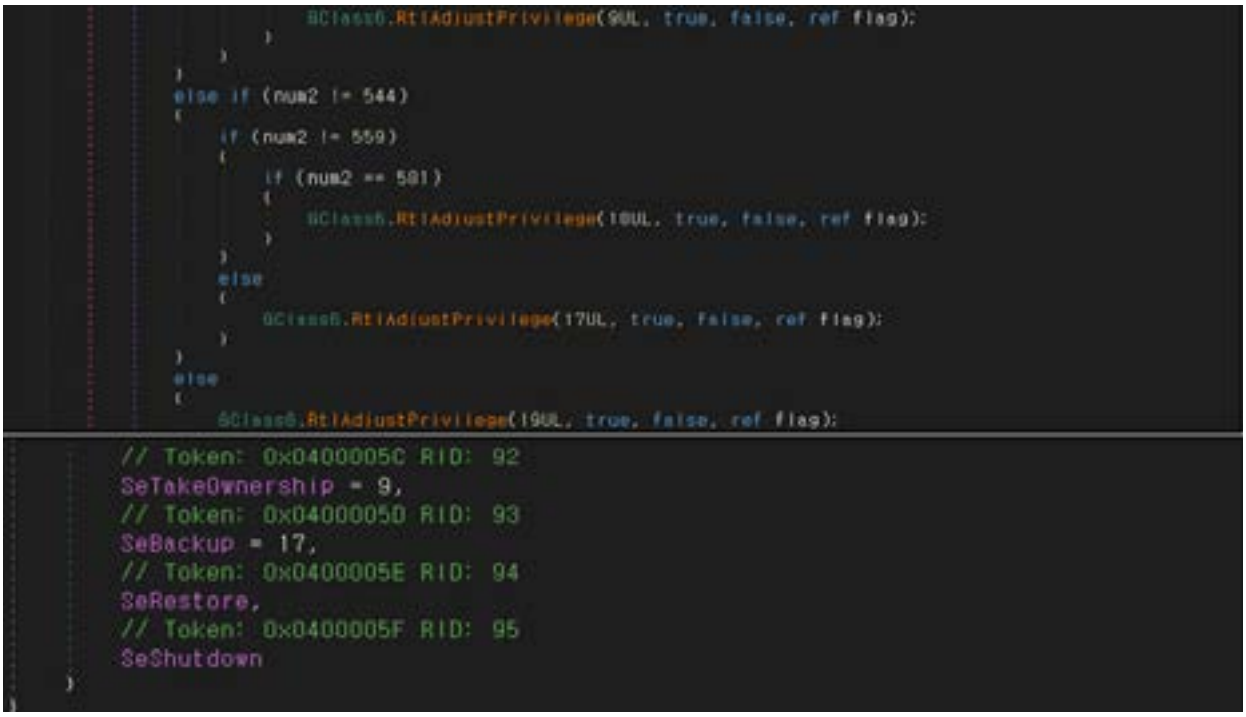
4.5 도메인 컨트롤러 열거 및 저장



[그림 6] 도메인 컨트롤러 열거 및 저장

획득한 도메인 컨트롤러 목록을 모두 열거하고 그 이름을 저장한다.
위 사진을 보면 해당 테스트를 위해 생성한 [*.somansa.com] 도메인 컨트롤러 목록을 확인할 수 있다.
이를 통해 도메인 컨트롤러를 획득한 DoubleZero Wiper는
획득한 모든 ActiveDirectory를 파괴하는 행위를 수행할 수 있다.

4.6 악성 행위에 필요한 권한 획득



[그림 7] 악성 행위에 필요한 권한 획득

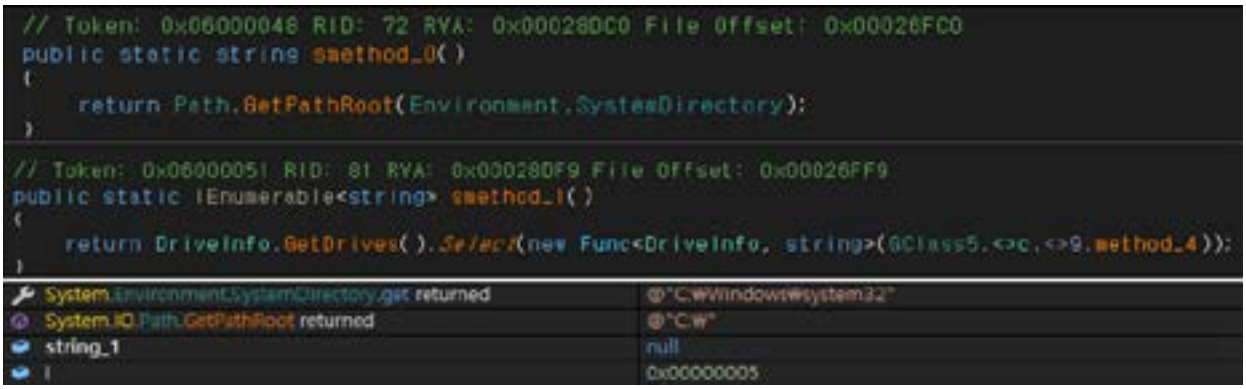
RtlAdjustPrivilege API를 호출한 후 악성 행위 수행에 필요한 네 가지 권한을 획득한다.
시스템을 손상 시키고 파일 및 폴더 등을 파괴하는 악성코드로서 아래와 같은 파일 권한 등을 획득한다.

SeBackupPrivilege	파일 및 폴더 백업
SeRestorePrivilege	파일 및 폴더 복원
SeShutdownPrivilege	시스템 종료
SeTakeOwnershipPrivilege	파일 또는 기타 개체의 소유권을 획득

[파일 3] 악성 행위에 필요한 권한

위 표의 권한은 파일 시스템에 관련된 권한으로서, DoubleZero Wiper의 시스템 파괴 행위에 필수이다.
위 권한들을 획득한 DoubleZero Wiper는
시스템 내 파일에 대한 제어권을 획득하여 삭제와 제어 및 조작 등을 할 수 있다.

4.7 주요 대상 드라이브 목록 획득



[그림 8] 주요 드라이브 목록 획득

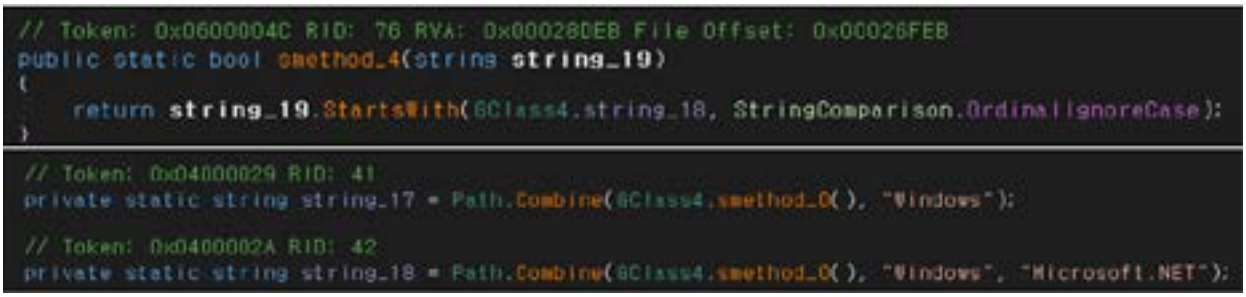
시스템 파괴에 앞서, GetPathRoot 메서드 및 GetDrives 메서드를 호출하여
시스템 내 주요 드라이브의 목록을 획득한다.
획득한 드라이브는 앞으로 DoubleZero Wiper의 주요 파괴 대상이 된다.

4.8 파괴 대상 드라이브 목록 열거

[그림 9] 파괴 대상 드라이브 목록 열거

이전에 획득한 주요 대상 드라이브 목록을 통해 파괴 대상 드라이브 목록을 열거한다.

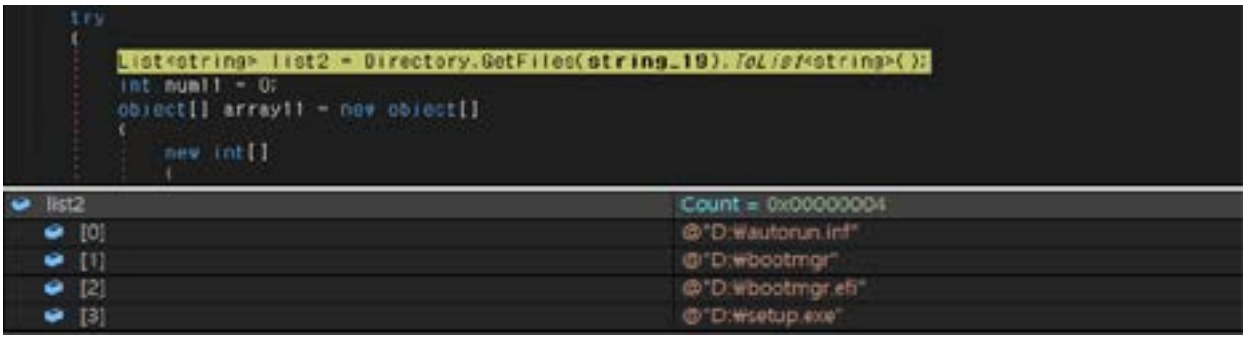
4.9 파괴 대상 폴더 목록 획득



[그림 10] 파괴 대상 폴더 목록 획득

DoubleZero Wiper는 각 드라이브의 폴더 목록을 재귀하며 찾는다.
이 때, 각 드라이브의 폴더 목록의 경로에 StartsWith 메서드를 호출한다.
특정 문자열이 포함되어 있을 시 이를 파괴 대상으로 저장한다.

4.10 파괴 대상 폴더 내 파일 목록 획득



[그림 11] 파괴 대상 폴더 내 파일 목록 획득

이전에 획득한 파괴 대상 폴더 내의 파일 목록을 획득한다.
해당 파일들은 향 후 DoubleZero Wiper에 의해 파괴가 수행된다.

4.11 현재 사용자에 로컬 시스템 계정의 모든 권한 부여

[그림 12] 로컬 시스템 계정 보안 식별자 부여

현재 사용자에 로컬 시스템 계정 (WellKnownSidType.LocalSystemSid) 보안 식별자를 부여하여
향후 파일에 대한 접근 제어를 변경할 수 있도록 한다.

4.12 파일에 대한 접근 제어 변경

[그림 13] 파일에 대한 접근 제어 변경

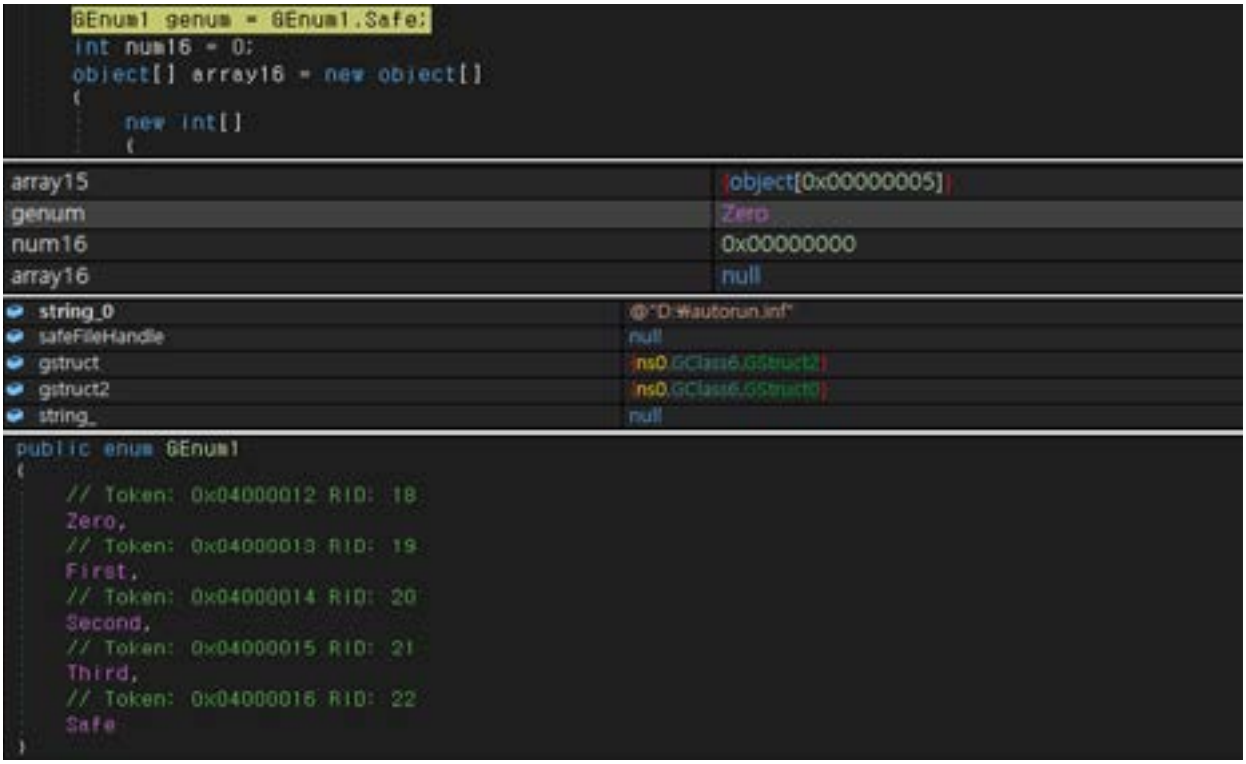
GetAccessControl 메서드를 호출하여 파일에 대한 현재 접근 제어 권한을 확인한 후,
이전에 획득한 로컬 시스템 계정 보안 식별자를 사용하여
SetOwner 및 SetAccessControl 메서드를 호출한 뒤 접근 제어 권한을 변경한다.
이 때, FILE_ACCESS_ACCESS (0x001F01FF) 권한을 사용한 AddAccessRule 메서드가 사용되며
변경 후 GetAccessControl 메서드로 다시 한번 변경한 제어 권한을 확인한다.
파괴 대상 폴더 목록은 아래의 표와 같다.

\Microsoft	Windows 주요 시스템 관련 폴더
\Windows	Windows 운영체제 관련 폴더
\drivers	Windows 주요 시스템 드라이버 관련 폴더
\NTDS	ActiveDirectory의 데이터베이스 파일 저장 관련 폴더
\Microsoft.NET	Microsoft .NET 관련 폴더
\Fonts	시스템 글꼴 관련 폴더
\Documents and Settings	보호된 운영 체제 파일 관련 폴더
\ProgramData	Windows 주요 시스템 관련 폴더
\Application Data	각 프로그램이 생성한 데이터 저장 관련 폴더
\Users	Windows 사용자 계정 관련 폴더
\All Users	Windows 공용 사용자 계정 관련 폴더

\Default User	Windows 기본 사용자 계정 관련 폴더
\AppData	사용자 별 설정 저장 관련 폴더
\Local	고유한 단일 시스템 데이터 저장 관련 폴더
\Roaming	북마크 및 기타 데이터 관련 폴더
\Local Settings	시스템 설정 관련 폴더
\Start Menu	시작 프로그램 관련 폴더
C:\Windows	Windows 운영체제 관련 폴더
C:\Windows\Microsoft.NET	Microsoft .NET 관련 폴더

[파일 4] 파괴 대상 폴더 목록

4.13 파일 파괴 과정 (1.1) – 시스템 파일



[그림 14] 주요 시스템 파일 삭제 전 확인 작업

부팅, 시스템 관리와 드라이버 파일 등 주요 시스템을 관리하는 파일에 대해서는
위와 같이 단계 별로 나누어 파괴 과정을 달리한다.
파괴 우선 순위에 따라 위와 같이 [Zero ~ Safe] 단계로 나누어 파괴 시
지속적인 악성 행위에 있어 안전한 파일인지, 파괴를 후순위로 밀어
다른 악성 행위 및 파괴 행위를 다 마친 후 파괴할 것인지를 판단한다.

4.14 파일 파괴 과정 (1.2) – 시스템 파일

[그림 15] 주요 시스템 파일 삭제 작업

주요 시스템 파일에 대해서는 NtOpenFile API를 호출한 후,
GetFileSizeEx API를 호출하여 대상 파일 핸들과 크기를 확인한다.
이후 NtFsControlFile API라는 비문서화된 API를 호출하는데,
이는 디스크의 직접적인 작업을 수행하도록 하는 API이다.
이를 FSCTL_SET_ZERO_DATA (0x980C8)을 인자로 주어 호출하면
대상 파일은 모두 0으로 채워져 파괴된다.

4.15 파일 파괴 과정 (2.1) – 일반 파일

[그림 16] 일반 파일 삭제 작업

일반 파일의 경우, FileStream 클래스의 Write 메서드를 사용하여
대상 파일에 대한 덮어쓰기를 수행한 후 파일 파괴 작업을 수행한다.
이를 통해 파일은 복구 불가능하도록 파괴된다.

4.16 레지스트리 파괴 과정 (1)

```
RegistrySecurity registrySecurity = new RegistrySecurity();
int i = 0;
object[] array4 = new object[]
{
    new int[]
    {
        90,
        199025202,
int num3 = K5SaFfdCXPYvOd0.ZaS941dK((int[])array11[num11], 0, 0);
if (num3 != 87 && num3 == 160)
{
    securityIdentifier = new SecurityIdentifier(WellKnownSidType.LocalSystemSid, null);
}
num3 = num11;
num11 = num3 + 1;

OpenSubKey(string_0 ?? "", RegistryKeyPermissionCheck.ReadWriteSubTree, RegistryRights.TakeOwnership);
```

[그림 17] 로컬 시스템 계정 권한의 레지스트리 접근 권한 부여

현재 사용자에 로컬 시스템 계정 (WellKnownSidType.LocalSystemSid) 보안 식별자를 부여하여
향후 레지스트리에 대한 시스템 계정 수준의 접근 제어를 변경할 수 있게 한다.

4.17 레지스트리 파괴 과정 (2)

```
    else
    {
        registryKey.SetAccessControl(registrySecurity);
    }
}
else
{
    registrySecurity.SetAccessRuleProtection(false, false);
}
num5 = n;
n = num5 + 1;
int num5 = K5SaFfdCXPYvOd0.ZaS941dK((int[])array16[num16], 0, 0);
if (num5 != 74 && num5 == 147)
{
    registryKey.DeleteSubKeyTree(OqA84Tq0.CxOrebi251W(new byte[]
    {
        200,
```

[그림 18] 레지스트리 파괴 (삭제)

이전에 획득한 레지스트리 접근 권한을 바탕으로 SetAccessControl 메서드를 호출하여
대상이 되는 레지스트리에 대한 접근 권한을 변경한다.

이후 DeleteSubKeyTree 메서드를 호출하여 레지스트리를 파괴 (삭제) 하는데, 그 대상은 다음과 같다.

HKLM(HKEY_LOCAL_MACHINE), HKCU(HKEY_CURRENT_USER), HKU(HKEY_USERS)

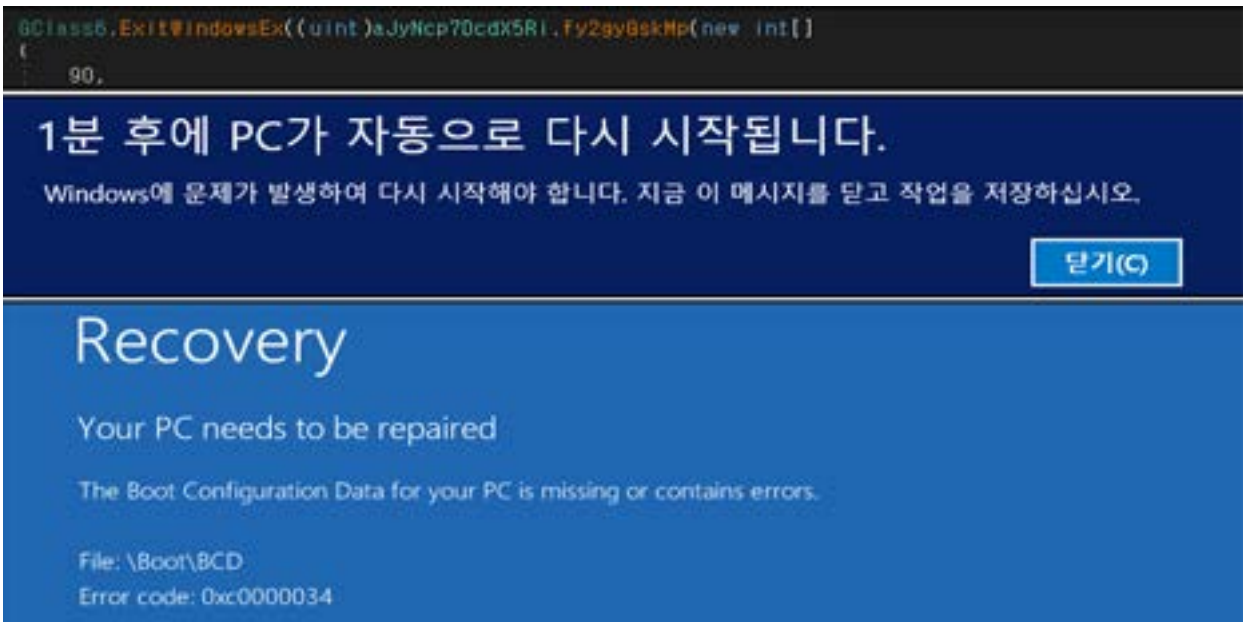
4.18 LSASS.EXE 프로세스 종료

```
Process[] processesByName = Process.GetProcessesByName(string_0);
int i = 0;
foreach (Process process in processesByName)
{
// ns0.GClass5
// Token: 0x04000033 RID: 51
private const string string_0 = "lsass";
                    else
                    {
                        process.Kill();
                    }
                    num6++;
```

[그림 19] LSASS.EXE 프로세스 종료 과정

DoubleZero Wiper는 작업을 마치기에 앞서, LSASS.EXE 프로세스를 종료시킨다.
이는 LSASS.EXE 프로세스가 시스템에 접속하는 유저들의 로그인을 검사하고,
비밀번호 변경 및 액세스 토큰 생성 등 시스템의 보안 정책을 강화하는 역할을 하기 때문이다.
즉, 마지막까지 시스템의 주요 보안을 담당하는 프로세스를 종료시키는 행위이다.

4.19 파괴 작업 완료 후 자가 종료

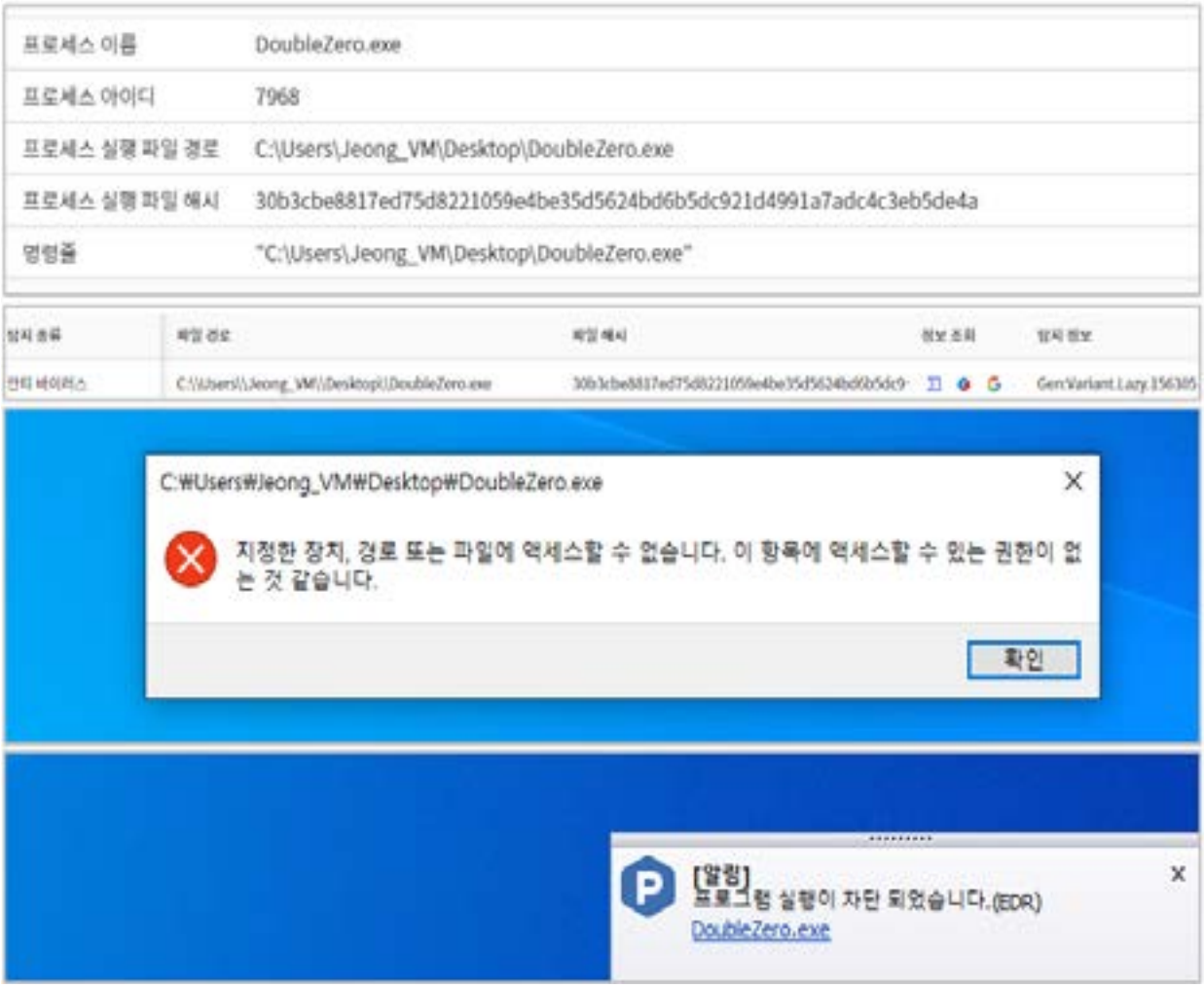


[그림 20] 자가 종료 및 시스템 파괴

시스템 파괴가 끝나면, 자가 종료를 수행하며 시스템은 더 이상 유지되지 못하고 파괴되어
복구가 불가능한 상태로 변경된다.
시스템을 유지하는 파일 및 레지스트리와 중요 시스템은 모두 파괴되어
더 이상 정상적으로 동작할 수 없다.

5. Privacy-i EDR 탐지 정보

5.1 탐지 정보 (Gen:Variant.Lazy.156305)



[그림 21] Privacy-i EDR 탐지 정보

Privacy-i EDR의 DoubleZero Wiper 탐지는
실시간으로 파일을 모니터링 하는 안티바이러스 엔진에서 탐지 되었으며
DoubleZero Wiper 실행 시, 파일 정보 획득과 동시에 파일 격리 및 차단이 이루어진다.
또한 DoubleZero Wiper에 대해 Gen:Variant.Lazy.156305로 탐지하고 대응한다.

6. 대응

1. Privacy-i EDR의 악성코드 탐지 기능을 통해 악성코드 실행을 사전에 방지한다.
2. OS 및 소프트웨어 보안 업데이트를 항상 최신으로 유지한다.
3. 주요 문서는 주기적으로 백업하고 물리적으로 분리하여 관리한다.
4. 신뢰 할 수 없는 메일의 첨부파일은 실행을 금지한다.
5. 비 업무 사이트 및 신뢰 할 수 없는 웹사이트의 연결을 차단한다.

궁금하신 점이나 문의사항은 malware@somansa.com 으로 문의주십시오