우크라이나 주요 시설 파괴 악성코드
단순 구조로 변종생성 용이, 기존 안티바이러스 대응 한계

와이퍼 악성코드
시스템 파괴 방식과 대응

요약

1. 국가간 사이버 테러 목적으로 활발히 사용
   → **우크라이나 주요시설 파괴목적으로 러시아에서 사용**
2. 2010년대 1~2년 주기로 발생,
   2021년부터는 국가/조직적 성격을 띄며 활발하게 사용
   → **러시아의 경우 2022.01월부터 03월까지**
   최소 5개 이상의 와이퍼 변종을 통해 우크라이나 주요시설 파괴
3. 복구 자체가 불가능하도록 시스템 파괴
   → **금전 취득이 아닌 인프라 파괴 및 마비 목적**
4. 단순한 구조, 간단한 코드로 구성되어 변종 다수발견
   → **기존 시그니처 기반 탐지 안티바이러스 솔루션으로는 탐지 한계 발생**

대응 방안

1. Privacy-i EDR과 같은 EDR 솔루션의 **'행위기반 탐지엔진'으로 실행 차단**
   : 일반 Anti-Virus 솔루션에서도 대부분 차단 가능하나 최신 업데이트 필요
2. **주요 데이터는 주기적인 백업 수행:** 디스크 파괴 시에도 복구 가능하도록 대비
3. 비정상적인 프로세스 행위는 **실시간으로 모니터링**
4. 내부 데이터 보호를 위해 **업무망 망분리 수행** : 인가되지 않은 프로그램 실행 차단
5. 신뢰할 수 없는 메일의 **첨부파일은 실행금지** :
   메일 내용과 보내는 이 계정에 연관성이 없거나 문법적으로 어색하고
   신뢰할 수 없는 링크 또는 첨부파일 클릭을 유도하는 메일

목차

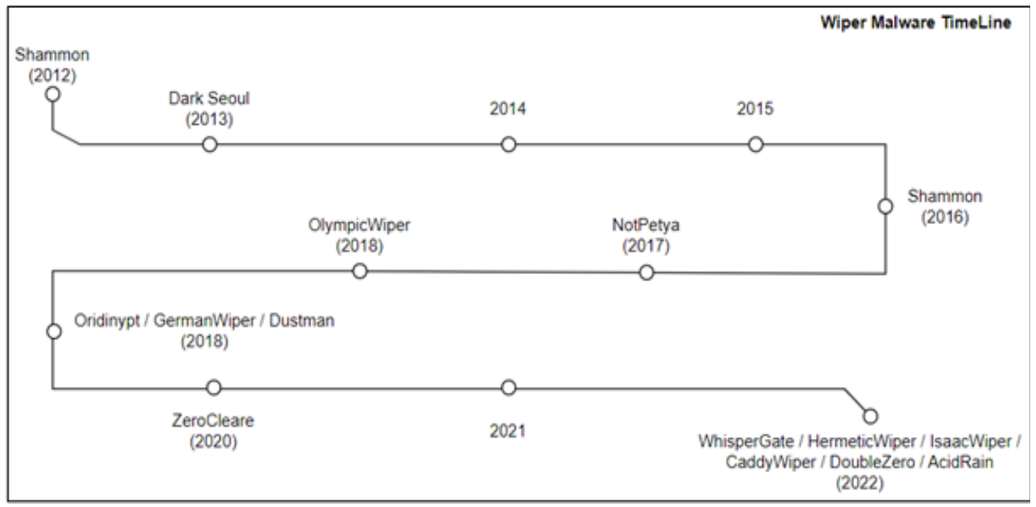
1. 개요

1.1 배경

와이퍼(Wiper) 악성코드(이하 와이퍼 악성코드)는 공격 대상의 시스템에 침투해
공격 대상의 시스템을 마비시키고 파괴하여 복구가 불가능한 피해를 입힌다.
우크라이나 주요시설 파괴목적으로 사용된 러시아의 악성코드도 와이퍼 악성코드였다.

와이퍼 악성코드는 공공, 민간기업과 군사시설 등 포괄적인 공격에 사용되고 있다.
주 목적은 침입 후 남은 흔적을 은폐하여 피해자의 대응능력을 약화시키는 것이다.
때로는 공격대상의 시스템 또는 기기 자체를 파괴하여 복구 불가능한 피해를 주기도 한다.

와이퍼 악성코드는 구조가 단순하고 복잡한 행위를 하지 않는 것이 특징인데,
단지 몇 줄에 불과한 코드로 위와 같은 파괴력과 위력을 낼 수 있다는 점이 특징으로 언급된다.
구조가 단순하기 때문에 변종 역시 손쉽게 제작된다.
방어하는 입장에서는 탐지 및 차단이 까다롭다.



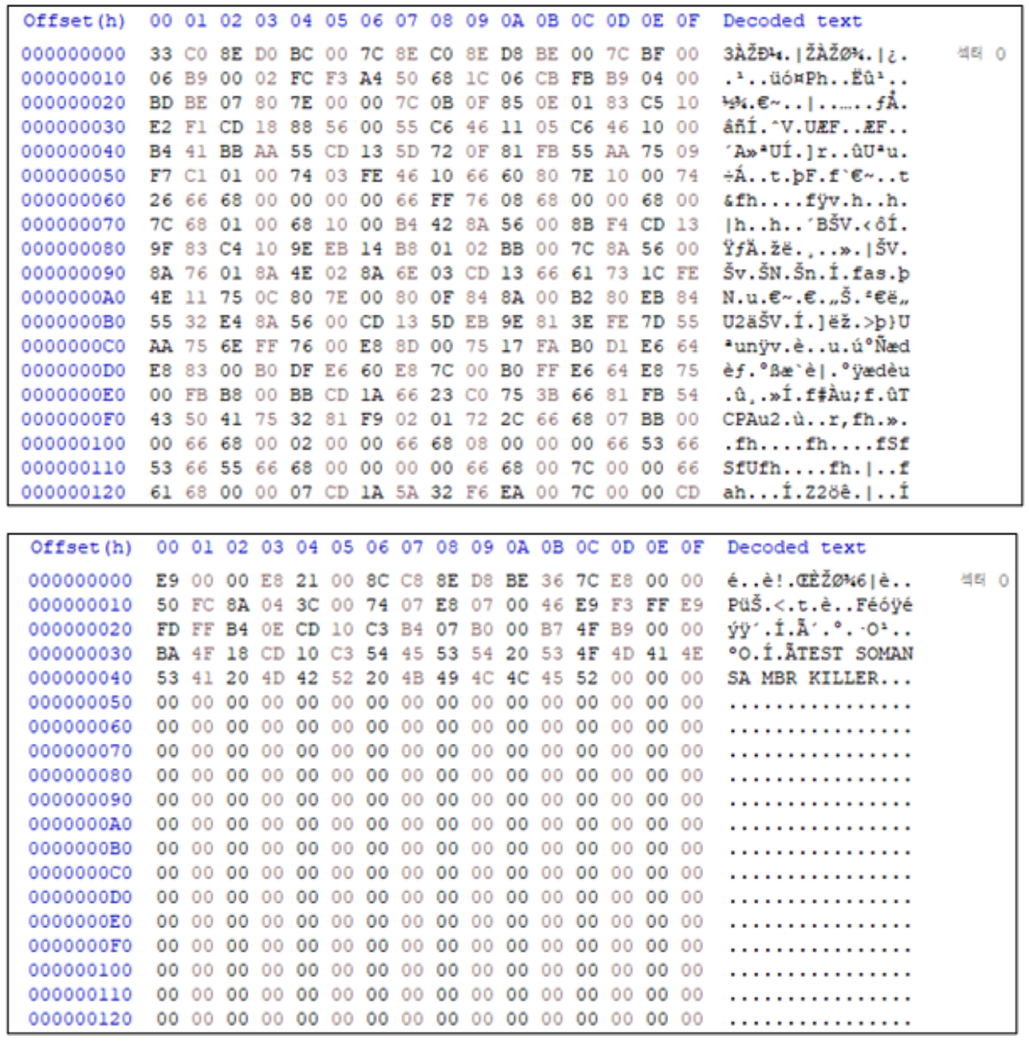
아래 사례는 실제 사용된 와이퍼 악성코드와 목적을 정의하고 있다.
이를 통해 지속적으로 정치 및 군사 목적으로 사용되고 있다는 것을 파악할 수 있다.
사이버전 또는 사이버 테러용 악성코드라고 불릴 정도로 활발히 진행되고 있다.

활동시기	이름	개발	대상	목적
2022.03	CaddyWiper	러시아	우크라이나	주요 기반 시설 내 시스템 파괴 목적
	IsaacWiper			
	DoubleZero			
2022.02	HermeticWiper			
2022.01	WhisperGate			
2021.07	MeteorWiper	미상	이란	국영 철도 시스템 파괴 목적
2021.05	ApostleWiper	이란	이스라엘	불특정 다수 대상 시스템 파괴 목적

[표 1] 와이퍼 공격 사례

공격받은 기업, 조직, 국가 대부분은 복구가 불가능한 수준의 피해를 겪은 것으로 알려졌다.
따라서 제작이 간편하지만 탐지하기 까다로운 와이퍼 악성코드를 통한 공격은 앞으로 활발해질 것으로 예상된다.

소만사는 와이퍼 악성코드에 대한 연구와 함께 공격기법 등을 지속적으로 모니터링했다.
이를 통해 공격원리와 함께 Privacy-i EDR을 통한 대응 및 방어방법에 대해
자세히 서술하여 피해를 최소화하고자 한다.



```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
000000000  33 C0 8E D0 BC 00 7C 8E C0 8E D8 BE 00 7C BF 00  3ÀŽÐ¼.|ŽÀŽØ¾.|¿.   섹터 0
000000010  06 B9 00 02 FC F3 A4 50 68 1C 06 CB FB B9 04 00  .¹..üó¤Ph..Ëû¹..
000000020  BD BE 07 80 7E 00 00 7C 0B 0F 85 0E 01 83 C5 10  ½¾.€~..|.....ƒÅ.
000000030  E2 F1 CD 18 88 56 00 55 C6 46 11 05 C6 46 10 00  âñÍ.ˆV.UÆF..ÆF..
000000040  B4 41 BB AA 55 CD 13 5D 72 0F 81 FB 55 AA 75 09  ´A»ªUÍ.]r..ûUªu.
000000050  F7 C1 01 00 74 03 FE 46 10 66 60 80 7E 10 00 74  ÷Á..t.þF.f`€~..t
000000060  26 66 68 00 00 00 00 66 FF 76 08 68 00 00 68 00  &fh....fÿv.h..h.
000000070  7C 68 01 00 68 10 00 B4 42 8A 56 00 8B F4 CD 13  |h..h..´BŠV.‹ôÍ.
000000080  9F 83 C4 10 9E EB 14 B8 01 02 BB 00 7C 8A 56 00  ŸƒÄ.žë.¸..».|ŠV.
000000090  8A 76 01 8A 4E 02 8A 6E 03 CD 13 66 61 73 1C FE  Šv.ŠN.Šn.Í.fas.þ
0000000A0  4E 11 75 0C 80 7E 00 80 0F 84 8A 00 B2 80 EB 84  N.u.€~.€.„Š.²€ë„
0000000B0  55 32 E4 8A 56 00 CD 13 5D EB 9E 81 3E FE 7D 55  U2äŠV.Í.]ëž.>þ}U
0000000C0  AA 75 6E FF 76 00 E8 8D 00 75 17 FA B0 D1 E6 64  ªunÿv.è..u.ú°Ñæd
0000000D0  E8 83 00 B0 DF E6 60 E8 7C 00 B0 FF E6 64 E8 75  èƒ.°ßæ`è|.°ÿædèu
0000000E0  00 FB B8 00 BB CD 1A 66 23 C0 75 3B 66 81 FB 54  .û¸.»Í.f#Àu;f.ûT
0000000F0  43 50 41 75 32 81 F9 02 01 72 2C 66 68 07 BB 00  CPAu2.ù..r,fh.».
000000100  00 66 68 00 02 00 00 66 68 08 00 00 00 66 53 66  .fh....fh....fSf
000000110  53 66 55 66 68 00 00 00 00 66 68 00 7C 00 00 66  SfUfh....fh.|..f
000000120  61 68 00 00 07 CD 1A 5A 32 F6 EA 00 7C 00 00 CD  ah...Í.Z2öê.|..Í

Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
000000000  E9 00 00 E8 21 00 8C C8 8E D8 BE 36 7C E8 00 00  é..è!.ŒÈŽØ¾6|è..   섹터 0
000000010  50 FC 8A 04 3C 00 74 07 E8 07 00 46 E9 F3 FF E9  PüŠ.<.t.è..Féóÿé
000000020  FD FF B4 0E CD 10 C3 B4 07 B0 00 B7 4F B9 00 00  ýÿ´.Í.Ã´.°.·O¹..
000000030  BA 4F 18 CD 10 C3 54 45 53 54 20 53 4F 4D 41 4E  °O.Í.ÃTEST SOMAN
000000040  53 41 20 4D 42 52 20 4B 49 4C 45 52 00 00 00 00  SA MBR KILLER....
000000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000000A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000000B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000000C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000000D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000000E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000000F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

[그림 1] 와이퍼 감염 전 디스크 (상) / 와이퍼 감염 후 파괴된 디스크 (하)

2. 정보

2.1 파일 정보

Name	[WhisperGate].exe
Type	Windows PE 실행 파일
Behavior	WhisperGate Wiper Malware
SHA-256	a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92

[파일 2] 우크라이나를 공격한 EXE 형태의 WhisperGate 와이퍼 악성코드

2.2 MBR(Master Boot Record)과 WhisperGate 와이퍼 악성코드

MBR이란 마스터 부트 레코드(Master Boot Record)의 약자로,
운영체제의 위치를 식별하여 PC의 주기억 장치에 적재될 수 있도록 하기 위한 정보이다.
하드 디스크 첫 번째 섹터에 저장되어 있다.
MBR은 파티션 섹터 또는 마스터 파티션 테이블이라고도 불린다.
하드 디스크가 포맷 될 때 나누어지는 각 파티션 위치 정보를 가지고 있기 때문이다.
즉, 파티션의 부트 섹터 레코드를 읽을 수 있는 프로그램을 포함하고 있다.

와이퍼 악성코드는 기술적으로 상기 서술한 MBR(Master Boot Record)를 파괴하여
운영 체제가 PC를 부팅할 수 없도록 손상시킨다.
PC 파티션 정보와 부팅에 필요한 부트 섹터 레코드를 제거하기 때문에 복구가 불가능하다.
와이퍼 악성코드는 치명적인 파괴력을 가지고 있지만 간단한 지식만으로도 만들 수 있는 단순한 악성코드다.
아래 API만을 가지고 빌드를 수행하면 만들 수 있다. 단 3가지의 API를 사용해 제작이 가능하다.

`Kernel32.CreateFile` (디스크의 MBR에 대한 접근 권한 획득)
`Kernel32.WriteFile` (MBR 덮어쓰기로 MBR 파괴)
`Kernel32.CloseHandle` (접근 권한 반환)

[그림 2] 와이퍼 감염 후 시스템 파괴 시연 / 와이퍼 악성코드 제작에 사용되는 API

기존 보안제품은 시그니처 기반으로 악성코드를 탐지하고 차단하기 때문에 변종대응에 한계가 있다.
와이퍼 악성코드는 변종 제작이 용이하기 때문에 신속하게 대응하는데 한계가 있었다.
그러나 Privacy-i EDR는 행위기반으로 탐지 및 차단을 수행하므로 실시간으로 보안위협을 탐지,
선제적으로 와이퍼 악성코드를 차단할 수 있게 되었다.

2.3 공격 방식

[그림 3] 와이퍼 악성코드 공격흐름

①	**해커의 와이퍼 악성코드 제작** 해커는 와이퍼 악성코드를 제작하고, 다양한 변종을 만들어 공격 대상을 탐색한다.
②	**감염 대상 국가, 시설, 시스템 침투** 감염 대상의 네트워크를 통해 시스템에 침투하여 와이퍼 악성코드 유포를 준비한다.
③	**와이퍼 악성코드 감염 및 실행** 파일을 암호화할 때 공유 위반이 발생하는 것을 방지하기 위해 특정 서비스를 종료한다.
④	**시스템은 파괴 및 복구 불가** 시스템은 와이퍼 악성코드에 의해 파괴되어 복구가 불가능한 피해를 입는다.

[그림 4] 페트야(Petya) 와이퍼 악성코드 감염 화면

해당 이미지는 페트야(Peyta) 와이퍼 악성코드 감염화면이다.
2016년 러시아 군사조직이 제작한 악성코드에 피해를 입은 우크라이나 PC에 나타한 이미지다.
단순한 구조를 통한 공격이었지만 복구가 불가능하도록 시스템을 파괴했기 때문에 산정 불가능한 피해를 입었다.

3. 분석

3.1 MBR(Master Boot Record) 접근 권한 획득

```
00403B93    C74424 18 00000000  mov dword ptr ss:[esp+18],0
00403B9B    C74424 14 00000000  mov dword ptr ss:[esp+14],0
00403BA3    C74424 10 03000000  mov dword ptr ss:[esp+10],3
00403BAB    C74424 0C 00000000  mov dword ptr ss:[esp+C],0
00403BB3    C74424 08 03000000  mov dword ptr ss:[esp+8],3
00403BBB    C74424 04 00000010  mov dword ptr ss:[esp+4],10000000
00403BC3    C70424 64704000     mov dword ptr ss:[esp],whispergate.407064   [esp]:L"\\\\.\\PhysicalDrive0"
00403BCA    E8 71FFFFFF         call <JMP.&CreateFileW>
00403BCF    89C6                mov esi,eax
00403BD1    8D85 E8DFFFFF       lea eax,dword ptr ss:[ebp-2018]
00403BD7    83EC 1C             sub esp,1C
00403BDA    893424              mov dword ptr ss:[esp],esi                  [esp]:L"\\\\.\\PhysicalDrive0"
00403BDD    C74424 10 00000000  mov dword ptr ss:[esp+10],0
00403BE5    C74424 0C 00000000  mov dword ptr ss:[esp+C],0
00403BED    C74424 08 00020000  mov dword ptr ss:[esp+8],200
00403BF5    894424 04           mov dword ptr ss:[esp+4],eax
```

[그림 5] MBR 접근권한 획득

WhisperGate 와이퍼 악성코드는 사용자에 의해 실행되면
즉시 시스템 파괴를 위해 CreateFileW API를 호출하여
물리디스크(\\\\.\\PhysicalDriver0)의 접근 권한을 획득한다.

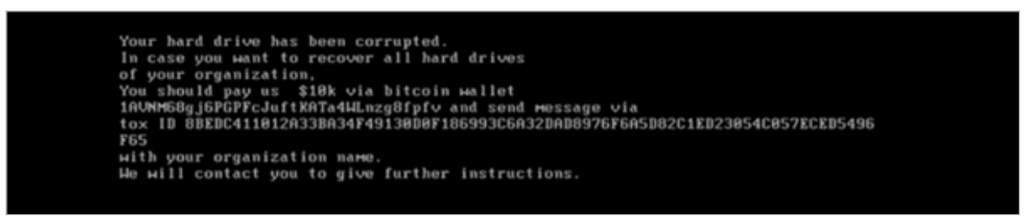
3.2 MBR(Master Boot Record) 파괴

```
00403BD7    83EC 1C             sub esp,1C
00403BDA    893424              mov dword ptr ss:[esp],esi
00403BDD    C74424 10 00000000  mov dword ptr ss:[esp+10],0
00403BE5    C74424 0C 00000000  mov dword ptr ss:[esp+C],0
00403BED    C74424 08 00020000  mov dword ptr ss:[esp+8],200
00403BF5    894424 04           mov dword ptr ss:[esp+4],eax
00403BF9    E8 AAFEFFFF         call <JMP.&WriteFile>
00403BFE    83EC 14             sub esp,14
00403C01    893424              mov dword ptr ss:[esp],esi
00403C04    E8 3FFFFFFF         call <JMP.&CloseHandle>
00403C09    50                  push eax
00403C0A    8D65 F4             lea esp,dword ptr ss:[ebp-C]
00403C0D    31C0                xor eax,eax
00403C0F    59                  pop ecx
00403C10    5E                  pop esi
00403C11    5F                  pop edi                                     edi:", "
00403C12    5D                  pop ebp
00403C13    8D61 FC             lea esp,dword ptr ds:[ecx-4]
00403C16    C3                  ret

0060DF80  00 00 41 41 41 41 00 59 6F 75 72 20 68 61 72  ..AAAAA.Your har
0060DF90  64 20 64 72 69 76 65 20 68 61 73 20 62 65 65 6E  d drive has been
0060DFA0  20 63 6F 72 72 75 70 74 65 64 2E 0D 0A 49 6E 20   corrupted...In
0060DFB0  63 61 73 65 20 79 6F 75 20 77 61 6E 74 20 74 6F  case you want to
0060DFC0  20 72 65 63 6F 76 65 72 20 61 6C 6C 20 68 61 72   recover all har
0060DFD0  64 20 64 72 69 76 65 73 0D 0A 6F 66 20 79 6F 75  d drives..of you
0060DFE0  72 20 6F 72 67 61 6E 69 7A 61 74 69 6F 6E 2C 0D  r organization,.
0060DFF0  0A 59 6F 75 20 73 68 6F 75 6C 64 20 70 61 79 20  .You should pay
0060E000  75 73 20 20 24 31 30 6B 20 76 69 61 20 62 69 74  us  $10k via bit
0060E010  63 6F 69 6E 20 77 61 6C 6C 65 74 0D 0A 31 41 56  coin wallet..1AV
0060E020  4E 4D 36 38 67 6A 36 50 47 50 46 63 4A 75 66 74  NM68gj6PGPFcJuft
0060E030  4B 41 54 61 34 57 4C 6E 7A 67 38 66 70 66 76 20  KATa4WLnzg8fpfv
0060E040  61 6E 64 20 73 65 6E 64 20 6D 65 73 73 61 67 65  and send message
0060E050  20 76 69 61 0D 0A 74 6F 78 20 49 44 20 38 42 45   via..tox ID 8BE
0060E060  44 43 34 31 31 30 31 32 41 33 33 42 41 33 34 46  DC411012A33BA34F
0060E070  34 39 31 33 30 44 30 46 31 38 36 39 39 33 43 36  49130D0F186993C6
0060E080  41 33 32 44 41 44 38 39 37 36 46 36 41 35 44 38  A32DAD8976F6A5D8
0060E090  32 43 31 45 44 32 33 30 35 34 43 30 35 37 45 43  2C1ED23054C057EC
0060E0A0  45 44 35 34 39 36 46 36 35 0D 0A 77 69 74 68 20  ED5496F65..with
0060E0B0  79 6F 75 72 20 6F 72 67 61 6E 69 7A 61 74 69 6F  your organizatio
0060E0C0  6E 20 6E 61 6D 65 2E 0D 0A 57 65 20 77 69 6C 6C  n name...We will
0060E0D0  20 63 6F 6E 74 61 63 74 20 79 6F 75 20 74 6F 20   contact you to
0060E0E0  67 69 76 65 20 66 75 72 74 68 65 72 20 69 6E 73  give further ins
0060E0F0  74 72 75 63 74 69 6F 6E 73 2E 00 00 00 00 55 AA  tructions.....U*

00401288    89C3                mov ebx,eax
0040128A    E8 F9270000         call <JMP.&_cexit>
0040128F    891C24              mov dword ptr ss:[esp],ebx
00401292    E8 91280000         call <JMP.&ExitProcess>
```

[그림 6] MBR 파괴

이전의 CreateFileW API 호출로 얻은 핸들로 WriteFile API를 호출하는데,
MBR(Master Boot Record) 영역인 512Byte 만큼을 덮어씌운다.
즉, MBR 영역을 파괴하여 공격자가 작성한 데이터로 덮어씌워
시스템을 파괴하고 복구가 불가능하도록 변경한다.

3.3 MBR(Master Boot Record) 파괴에 의한 시스템 파괴

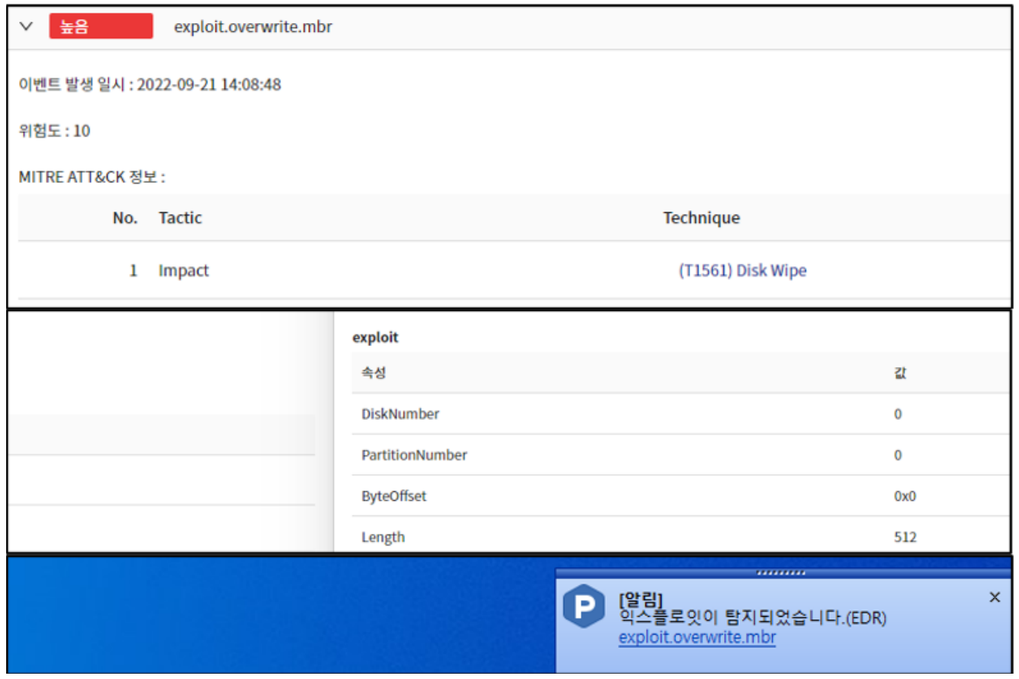


[그림 7] MBR 파괴에 의한 시스템 파괴 및 부팅 메시지

마지막으로 MBR이 파괴되어 정상적인 부팅되지 않으며 러시아 군사조직이 작성한 문구를 확인할 수 있다.
내용상으로는 비트코인을 요구하고 있으나
실제로는 우크라이나 주요 시설을 파괴하기 위한 목적으로 제작된 와이퍼 악성코드다.

4. Privacy-i EDR 탐지 정보

4.1 취약점 공격 방지 기능을 통한 탐지 및 차단



[그림 8] Privacy-i EDR의 MBR 파괴 행위 탐지 및 차단

Privacy-i EDR은 WhiperGate의 MBR 파괴 행위를 행위 기반 취약점 보호 기능으로 탐지 및 차단한다.
탐지 로그를 통해 관리자는 파괴시도를 위해 MBR 위치와 디스크 접근이 수행된 정보까지 확인할 수 있다.

4.2 취약점 공격 방지 기능을 통한 시스템 보호

[그림 9] Privacy-i EDR의 MBR 파괴 행위 탐지 및 차단 후 정상 부팅이 된 모습

그러나 Privacy-i EDR의 취약점 공격 방지 기능을 통해
악성코드가 실행되어 디스크 접근까지 수행되었음에도 불구하고 시스템은 성공적으로 부팅되었다.
Privacy-i EDR이 WhisperGate의 MBR 접근까지 파악한 후
파괴 전 단계에서 선제적으로 탐지/대응했기 때문이다.

이와 같이 Privacy-i EDR은 MBR을 파괴하는 와이퍼 형태의 악성코드 행위에 대해
실시간 보호와 함께 보안담당자의 개입없이 엔드포인트 자체에서 선제적으로 악성코드를 차단한다.

5. 대응 방안

1. Privacy-i EDR과 같은 EDR 솔루션의 **'행위기반 탐지엔진'으로 실행 차단**
   : 일반 Anti-Virus 솔루션에서도 대부분 차단 가능하나 최신 업데이트 필요
2. **주요 데이터는 주기적인 백업 수행:** 디스크 파괴 시에도 복구 가능하도록 대비
3. 비정상적인 프로세스 행위는 **실시간으로 모니터링**
4. 내부 데이터 보호를 위해 **업무망 망분리 수행** : 인가되지 않은 프로그램 실행 차단
5. 신뢰할 수 없는 메일의 **첨부파일은 실행금지** :
   메일 내용과 보내는 이 계정에 연관성이 없거나 문법적으로 어색하고
   신뢰할 수 없는 링크 또는 첨부파일 클릭을 유도하는 메일

궁금하신 점이나 문의사항은 malware@somansa.com 으로 문의주십시오