우크라이나, 폴란드 운송 및 물류기관 공격
2월 우크라이나 인프라 파괴한 '허메틱와이퍼' 공격타깃과 일치

프레스티지 랜섬웨어

요약

1. **우크라이나, 폴란드 운송 및 물류 산업** 조직을 표적으로 랜섬웨어 배포
2. 2월 우크라이나 산업시설 공격한 **'허메틱 와이퍼' 피해대상과 동일** (링크)
3. '허메틱 와이퍼'는 주요 인프라 마비 목적으로 유포,
   '프레스티지'는 데이터 암호화를 통한 금전탈취 목적으로 유포
4. 정상파일로 위장하여 실행을 유도하는 것이 아닌
   내부 권한을 탈취한 후 랜섬웨어 유포
5. 스스로 **파일을 복구하지 못하도록**
   피해자 PC에 존재하는 **시스템 백업본 모두 삭제**

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. 비정상적인 프로세스 행위는 **실시간으로 모니터링**
3. 내부 데이터 보호를 위해 **업무망 망분리 수행**
4. 신뢰할 수 없는 메일의 **첨부파일은 실행금지** :
   메일 내용과 보내는이 계정에 연관성이 없거나 문법적으로 어색하고
   신뢰할 수 없는 링크 또는 첨부파일 클릭을 유도하는 메일
5. 비 업무 사이트 및 **신뢰할 수 없는 웹사이트 연결 차단**
6. OS 및 소프트웨어 보안 업데이트를 항상 최신형상으로 유지

목차

1. 개요

1.1 배경

2022년 10월 14일, MSTIC(Microsoft Threat Intelligence)는
우크라이나와 폴란드의 운송 및 물류 산업 조직을 표적으로 랜섬웨어를 배포하는
새로운 위협 그룹이 발견되었다고 전했다. [01]
MSTIC는 이 위협 그룹을 DEV-0960으로 이름 지었고,
공격자는 이 악성코드를 랜섬노트에 Prestige 랜섬웨어(이하 프레스티지) 라고 명시하였다.
프레스티지의 피해대상은 지난 2월 우크라이나를 대상으로 유포된 HermeticWiper와 겹친다고 전해진다.

그러나 PC가 부팅을 못하도록 MBR(Master Boot Record)과 MFT(Master File Table)를 덮어써서
주요 인프라를 마비시키는 것이 목적이었던 HermeticWiper와는 달리
프레스티지는 파일을 암호화하고 협박하여 금전적 이득을 취하고 있다.

이 랜섬웨어는 특정 조직을 대상으로 유포되었을 확률이 높다.
정상 파일로 위장하여 유포하는 것이 아니라,
도메인 관리자 등 높은 권한을 사전에 획득한 뒤 랜섬웨어를 유포했기 때문이다.
초기 침투 경로는 아직 알려지지 않았으며, 랜섬웨어를 유포하고 실행시킬 때
로컬 권한 상승과 원격 코드 실행을 보조하는 오픈소스 및 상용 도구를 적극 활용하였다.
SecureAuth에서 개발한 통신 도구 Impacket[02],
2021년 DEFCON에서 Mettle Security의 보안 연구원이 발표한
Windows 로컬 권한 상승 도구 winPEAS[03] 등이 사용되었다.

프레스티지 랜섬웨어는 C++로 작성되었으며
오픈소스 암호화 라이브러리인 CryptoPP[04] 를 정적 링킹하여 사용한다.
윈도우즈 환경에서 동작하는 랜섬웨어들은 마이크로소프트에서 제공하는
Win32 Cryptography API를 사용하거나 오픈소스를 가져와 사용하는 것이 일반적이다.
암호화 라이브러리를 정적 링킹하였기에 프레스티지 랜섬웨어는
추가적인 악성코드를 내장하지 않았음에도 불구하고 파일 크기가 1MB에 가까운 모습을 보인다.

소만사는 프레스티지 랜섬웨어에 대해 상세 분석을 진행하고 분석보고서를 작성하였다.

01 https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/

02 https://github.com/SecureAuthCorp/impacket

03 https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS

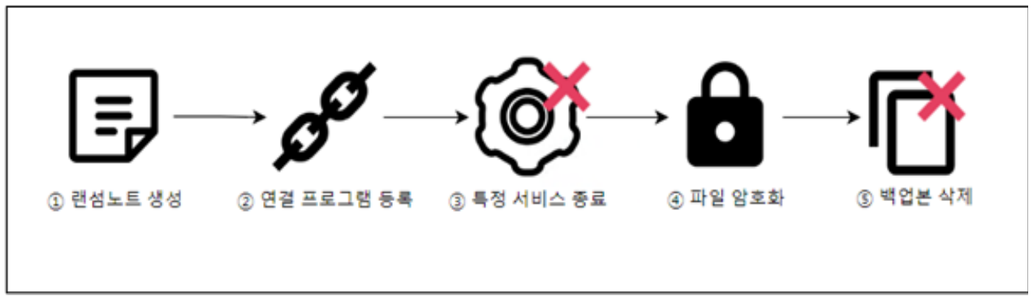
04 https://github.com/weidai11/cryptopp

1.2 파일 정보

Name	123.exe
Type	PE32
Behavior	Ransomware
SHA-256	5fc44c7342b84f50f24758e39c8848b2f0991e8817ef5465844f5f2ff6085a57

[파일 1] 프레스티지 랜섬웨어 실행 파일

2. 분석



[그림 1] 프레스티지 랜섬웨어 실행 흐름

①	랜섬노트 생성 피해자에게 메시지와 연락처를 전달하기 위해 랜섬노트를 생성한다.
②	연결 프로그램 등록 암호화된 파일을 실행하면 랜섬노트가 화면에 표시되도록 레지스트리에 키와 값을 추가한다.
③	특정 서비스 종료 파일을 암호화할 때 공유 위반이 발생하는 것을 방지하기 위해 특정 서비스를 종료한다.
④	파일 암호화 피해자의 시스템에 존재하는 파일들을 암호화시킨다. 암호화는 특정 확장자를 가진 파일만 대상으로 한다.
⑤	백업본 삭제 피해자가 스스로 파일을 복구하지 못하도록 시스템 백업본을 삭제한다.

2.1 랜섬노트 생성


README - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말
YOU PERSONAL FILES HAVE BEEN ENCRYPTED.

To decrypt all the data, you will need to purchase our decryption software.
Contact us Prestige.ranusomeware@Proton.me. In the letter, type your ID = 289B23AC.

* ATTENTION *
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Do not modify or rename encrypted files. You will lose them.

[그림 2] 프레스티지 랜섬웨어의 랜섬노트

랜섬노트는 공격자가 피해자에게 메시지와 연락처를 남기기 위한 수단이다.
파일 암호화 작업이 끝나고 생성되는 것이 일반적이지만,
프레스티지 랜섬웨어는 랜섬노트를 가장 먼저 생성한다.
위치는 사용자 공용 폴더인 C:\Users\Public에 README라는 이름으로 생성된다.

랜섬노트 본문에 포함된 ID는
랜섬웨어 실행 파일에 존재하는 공격자의 RSA 공개키에 대한 CRC-32 해시 값이다.
이와 비슷한 사례로 올해 4월에 발견된 REvil 랜섬웨어가 있다. [05] [06]
REvil은 피해자 PC의 NetBIOS 이름과 CPU 이름을 조합해
CRC-32 해시를 생성하고 이를 랜섬노트에 포함시켰다.
둘의 차이점은 REvil은 해시 값을 피해자의 고유 식별자로 사용했고,
프레스티지 는 해시 값을 공격자가 랜섬웨어의 버전 정보로 사용한다는 점이다.

2.2 랜섬노트 연결 프로그램 등록

reg.exe는 윈도우즈의 레지스트리 편집기로 프레스티지는 이를 사용해 레지스트리에 키와 값을 추가한다.
이 프로그램은 콘솔 프로그램이기에 실행 시 명령 프롬프트 창이 화면에 표시되지만,
프레스티지는 창을 숨김 처리하여 피해자가 감염 사실을 도중에 파악하기 어렵도록 하였다.

```
C:\\Windows\\System32\\reg.exe add HKCR\\.enc /ve /t REG_SZ /d enc /f
```

[표 1] 확장자 정의를 위한 레지스트리 생성 명령

```
C:\\Windows\\System32\\reg.exe add HKCR\\enc\\shell\\open\\command /ve /t REG_SZ /d
\"C:\\Windows\\Notepad.exe C:\\Users\\Public\\README\" /f
```

[표 2] 확장자 처리기 등록을 위한 레지스트리 생성 명령

05 https://www.virustotal.com/gui/file/861e2544ddb9739d79b265aab1e327d11617bc9d9c94bc5b35282c33fcb419bc

06 https://www.somansa.com/security-report/security-note/2021kaseya/

[그림 3] HKCR 하이브에 저장된 확장자 이름

[그림 4] HKCR 하이브에 저장된 확장자 처리기

HKEY_CLASSES_ROOT(HKCR) 하이브는
확장자 이름과 해당 확장자를 가진 파일을 실행했을 때 이를 처리하는 실행 명령을 포함하고 있다.
해당 하이브에 레지스트리 키와 값을 추가하면
특정 확장자를 가진 파일을 실행했을 때 지정한 명령을 실행하도록 설정할 수 있다.
프레스티지는 .enc 확장자를 가진 파일을 실행하면
윈도우즈 기본 앱 중 하나인 메모장으로 랜섬노트를 열도록 명령한다.
.enc는 프레스티지 랜섬웨어가 암호화시킨 파일에 이어 붙이는 파일 확장자이다.
따라서 암호화된 파일을 실행하면 랜섬노트가 화면에 표시된다.

2.3 서비스 강제 종료

```
C:\\Windows\\System32\\net.exe stop MSSQLSERVER
```

[표 3] 서비스 강제 종료 명령

보다 많은 파일을 암호화시키기 위해선 파일을 사용 중인 프로세스가 적어야 한다.
파일을 암호화시키기 위해 접근했을 때,
다른 프로세스가 이미 해당 파일을 사용 중이면 공유 위반이 발생하여 접근이 불가하기 때문이다.
프레스티지는 마이크로소프트의 데이터베이스 서버 프로그램인 MSSQLSERVER 서비스를 강제로 종료시킨다.
종료 대상 서비스 목록은 랜섬웨어의 버전에 따라 상이할 수 있다.

2.4 파일 암호화 대상 선정

```
C:\\Windows
C:\\ProgramData\\Microsoft
```

[표 4] 파일 암호화 대상 제외 폴더 목록

일반적으로 랜섬웨어의 목적은 시스템 파괴가 아니라 돈을 버는 것이므로
감염 후에도 피해자에게 최소한의 가용성을 보장할 필요가 있다.
피해자가 운영체제를 실행할 수 있어야 암호화한 파일로 감염사실을 인지시키고,
랜섬노트를 통해 메시지와 연락처를 전달할 수 있기 때문이다.

따라서 시스템에게 잠재적인 위협을 끼칠 수 있는 파일들은 암호화 대상에서 제외시키는 것이 바람직하다.
프레스티지 랜섬웨어는 파일 암호화 작업을 하기 위해
접근 가능한 논리적 드라이브를 기준으로 하위의 모든 경로들을 수집한다.

단, 윈도우즈 구동에 필요한 중요 파일들이 위치한 경로는 수집 대상에서 제외시켜 최소한의 가용성을 확보한다.
뿐만 아니라, 해당 경로에 위치한 파일들의 개수가 결코 적지 않으므로
공격자는 파일 재귀 탐색 시 성능 상의 이점을 가져갈 수 있다.

```
.1cd .7z .abk .accdb .accdc .accde .accdr .alz .apk .apng .arc .asd .asf .asm .asx
.avhd .avi .avif .bac .backup .bak .bak2 .bak3 .bh .bkp .bkup .bkz .bmp .btr .bz
.bz2 .bzip .bzip2 .c .cab .cer .cf .cfu .cpp .crt .css .db .db-wal .db3 .dbf .der
.dmg .dmp .doc .docm .docx .dot .dotm .dotx .dpx .dsk .dt .dump .dz .ecf .edb
.epf .exb .ged .gif .gpg .gzi .gzip .hdd .img .iso .jar .java .jpeg .jpg .js .json
.kdb .key .lz .lz4 .lzh .lzma .mdmr .mkv .mov .mp3 .mp4 .mpeg .myd .nude .nvram
.oa .odf .ods .old .ott .ovf .p12 .pac .pdf .pem .pfl .pfx .php .pkg .png .pot
.potm .potx .pps .ppsm .ppsx .ppt .pptm .pptx .prf .pvm .py .qcow .qcow2 .r0 .rar
.raw .rz .s7z .sdb .sdc .sdd .sdf .sfx .skey .sldm .sldx .sql .sqlite .svd .svg
.tar .taz .tbz .tbz2 .tg .ti .tiff .trn .txt .txz .tz .vb .vbox .vbox-old .vbox-
prev .vdi .vdx .vhd .vhdx .vmc .vmdk .vmem .vmsd .vmsn .vmss .vmx .vmxf .vsd .vsdx
.vss .vst .vsx .vtx .wav .wbk .webp .wmdb .wmv .xar .xlm .xls .xlsb .xlsm .xlsx
.xlt .xltm .xltx .xlw .xz .z .zbf .zip .zipx .zl .zpi .zz
```

[표 5] 파일 암호화 대상 확장자 목록

또한 파일의 확장자를 검사하여 [표 5]에 포함되지 않는 확장자를 가진 파일들은 암호화 대상에서 제외시킨다.
[표 5]를 보면 암호화 대상으로 삼는 파일 확장자가 다양한데,
소스코드, 압축, 이미지, 동영상, 문서, 그리고 인증서 파일 등이 그 대상이다.

2.5 파일 암호화

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4mpkHWE1p0nefE0PL/Qk
gT7bjLTeJ9bpH6v41L1YGI688cwfEnjmIaDa0zwvHfbT8dn4o+Wh2iSpUZk0BYIi
Lw6u5+9nSd2UzD4sB+MY9dv6oVTHInxqp4VNLHR2nMjgIS4rFHYzNJ7Tsj/j3YJZ
dVPuPVCqbpZg5boXoSFbgLNIn6Mnr+vKc5tGh+pkGty0otyFd/ghM0b/xitowcvx
eqZezPO0YXmkjjeTi0jFa7E9IIP3Z/DMOR9r/oJR0NyEIs9HNKdFGTAjJKDAKWxu
1nEPXiZoPPHgS7fxqg40+ciCjj2i7eUwqVkop5PvwjqtqQ0TkIt8EqjvkmDtMrp8
ZQIDAQAB
-----END PUBLIC KEY-----
```

[표 6] 공격자의 RSA 공개키

프레스티지 랜섬웨어에는 공격자의 RSA 공개키가 하드코딩 되어 있다.
공격자는 오픈소스 암호화 라이브러리 CryptoPP를 사용해 각각의 파일을 AES로 암호화한다.

이름	수정한 날짜	유형	크기
sample1.docx	2022-05-11 오전 10:55	Microsoft Word ...	279KB
sample2.hwp	2022-05-11 오전 10:55	한컴오피스 한글 ...	416KB
sample3.pdf	2022-05-11 오전 10:55	Microsoft Edge P...	1,512KB
sample4.pptx	2022-05-11 오전 10:55	Microsoft PowerP...	182KB
sample5.txt	2022-05-11 오전 10:55	텍스트 문서	293KB
sample6.xlsx	2022-05-11 오전 10:55	Microsoft Excel ...	425KB
sample7.zip	2022-05-11 오전 10:55	압축(ZIP) 파일	1,229KB

[그림 5] 랜섬웨어 감염 전후 비교 (전)

이름	수정한 날짜	유형	크기
sample1.docx.enc	2022-10-28 오후 3:12	ENC 파일	279KB
sample2.hwp	2022-05-11 오전 10:55	한컴오피스 한글 ...	416KB
sample3.pdf.enc	2022-10-28 오후 3:12	ENC 파일	1,512KB
sample4.pptx.enc	2022-10-28 오후 3:12	ENC 파일	182KB
sample5.txt.enc	2022-10-28 오후 3:12	ENC 파일	294KB
sample6.xlsx.enc	2022-10-28 오후 3:12	ENC 파일	425KB
sample7.zip.enc	2022-10-28 오후 3:12	ENC 파일	1,229KB

[그림 6] 랜섬웨어 감염 전후 비교 (후)

[그림 5]와 [그림 6]은 랜섬웨어 감염의 전후 모습이다.
대부분의 문서파일과 압축파일은 암호화되었지만,
아래아한글 문서 파일은 암호화 대상 확장자에 포함되지 않기에 암호화되지 않았다.
암호화된 파일을 실행하면 랜섬노트가 메모장에 표시된다.

2.6 백업본 삭제

```
C:\\Windows\\System32\\wbadmin.exe delete catalog -quiet
```

[표 7] wbadmin을 사용한 백업본 삭제 명령

```
C:\\Windows\\System32\\vssadmin.exe delete shadows /all /quiet
```

[표 8] vssadmin을 사용한 백업본 삭제 명령

마지막으로 스스로 파일을 복구하지 못하도록 피해자 PC에 존재하는 시스템 백업본을 모두 삭제한다.
32비트 실행 파일은 WoW64 파일 시스템 리다이렉션에 의해
64비트 윈도우즈에서 System32 폴더에 접근을 시도하는 경우
SysWoW64 폴더로 리다이렉션되는 것이 윈도우즈의 기본 정책이다.

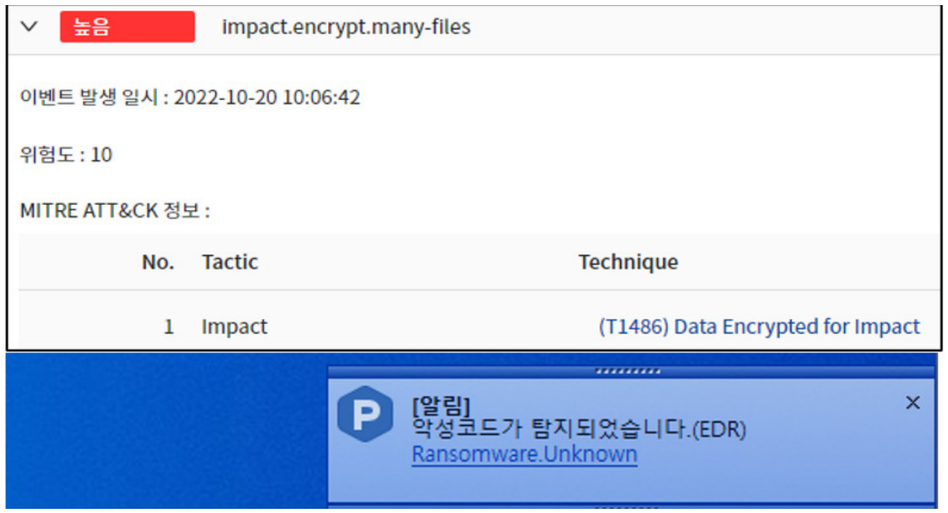
그러나 프레스티지 랜섬웨어는 이를 일시적으로 비활성화시키고 System32 폴더에 접근한다.
시스템 백업본을 삭제할 수 있는 기본 프로그램인 wbadmin.exe와 vssadmin.exe 파일이
64비트 윈도우즈에선 System32 경로에만 존재하기 때문이다.

4. Privacy-i EDR 탐지 정보

3.1 랜섬웨어 탐지 정보

[그림 7] Privacy-i EDR의 행위탐지 및 경고정보

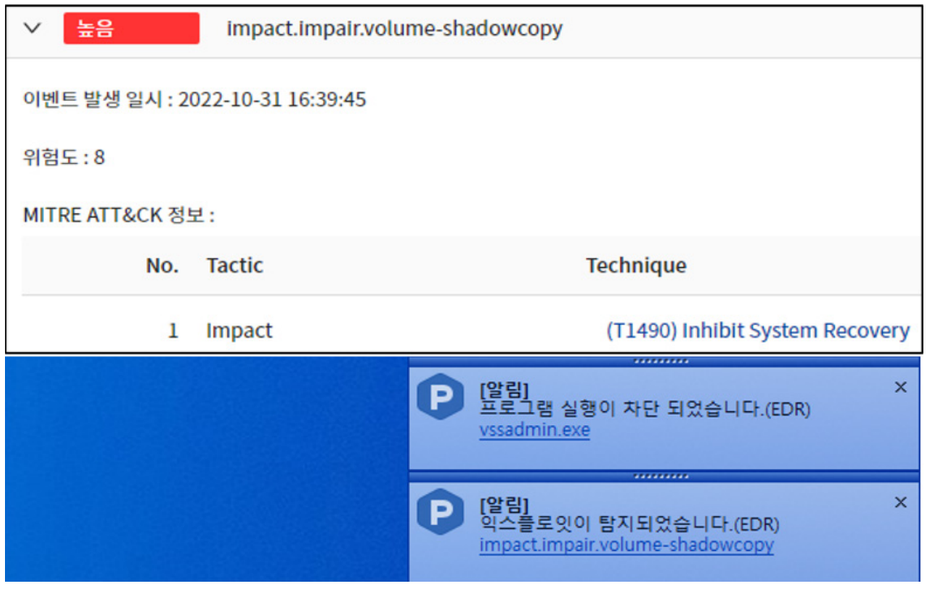
3.2 파일 암호화 행위



[그림 8] Privacy-i EDR 파일 암호화 탐지 정보

Privacy-i EDR은 프레스티지 랜섬웨어를 Ransomware.Unknown으로 탐지하고 있다.
행위 기반 탐지 엔진에서 랜섬웨어의 파일 암호화 행위를 탐지하고 차단하였다.

3.3 볼륨 섀도 복사본 삭제 행위



[그림 9] Privacy-i EDR 볼륨 섀도 복사본 삭제 탐지 정보

프레스티지 랜섬웨어는 파일 암호화 작업을 마치고 볼륨 섀도 복사본 삭제 행위를 수행하기 때문에
Privacy-i EDR에서 프레스티지 랜섬웨어를 탐지하고 해당 행위를 수행하기 전에 프로세스를 차단한다.

하지만 위협 행위 탐지 및 대응 테스트를 위하여
Privacy-i EDR의 정책에서 프로세스 차단을 비활성화 한 경우에는
프레스티지 랜섬웨어는 볼륨 섀도 복사본 삭제를 시도한다.
그러나 Privacy-i EDR은 볼륨 섀도 복사본 삭제행위 역시 탐지하고 차단한다.

4. 대응

1. Privacy-i EDR과 같은 EDR 솔루션의 **'행위기반 탐지엔진'으로 실행 차단**
   : 일반 Anti-Virus 솔루션에서도 대부분 차단 가능하나 최신 업데이트 필요
2. 비정상적인 프로세스 행위는 **실시간으로 모니터링**
3. 내부 데이터 보호를 위해 **업무망 망분리 수행**
4. 신뢰할 수 없는 메일의 **첨부파일은 실행금지** :
   메일 내용과 보내는이 계정에 연관성이 없거나 문법적으로 어색하고
   신뢰할 수 없는 링크 또는 첨부파일 클릭을 유도하는 메일
5. 비 업무 사이트 및 **신뢰할 수 없는 웹사이트 연결 차단**
6. OS 및 소프트웨어 보안 업데이트를 항상 최신형상으로 유지

궁금하신 점이나 문의사항은 malware@somansa.com 으로 문의주십시오