Keep up with Ransomware

올해만 두 번, 국내 제조업체를 노린 Underground 랜섬웨어

■ 개요

2024 년 12 월 랜섬웨어 피해 사례 수는 지난 11 월(664 건)보다 9 건 증가한 673 건을 기록했다. 12 월에도 많은 피해가 발생한 이유는 12 월에 새로 등장한 FunkSec 그룹이 89 건의 피해자를 게시했고, Clop 그룹이 Cleo 사의 파일 공유 솔루션의 취약점을 악용해 66 건의 피해자를 발생시킨 사고가 있었기 때문이다.

Clop 이 악용한 취약점은 Cleo 사의 파일 전송 솔루션 Cleo Harmony, VLTrader, LexiCom 에서 발생한 파일 쓰기 취약점(CVE-2024-50623, CVE-2024-55956)이다. 특히 CVE-2024-50623 은 지난 10 월에 발견된 취약점으로 패치를 배포했지만 해당 패치로는 기존 취약점이 완전히 보완되지 않았으며, 두 달 뒤 파일 읽기만 가능한 새로운 취약점(CVE-2024-55956)까지 발생했다. Clop 은 공개된 두 취약점을 악용해 데이터 탈취 등의 악성 행위를 수행하는 JAVA 기반의 백도어[1] "Malichus"를 업로드해 공격을 수행했다. Clop 은 자신들의 다크웹 유출 사이트에 총 66 곳의 피해 기업명을 일부 필터링해 업로드했으며, 피해 기업들이 별다른 대응을 하지 않을 경우 25 년에 모든 피해 기업명을 공개할 예정이라고 밝혔다.

LockBit 의 범죄 인프라를 무력화하는 Cronos 작전 이후, 하락세를 걷고 있던 LockBit 그룹이 12 월 19 일 자신들의 다크웹 유출 사이트를 통해 LockBit 4.0 의 소식을 알리며 신규 파트너를 모집하기 시작했다. LockBit 그룹은 777 달러(한화 약 110 만원)을 암호화폐로 지불하면 관리 패널에 접근할 수 있으며, Windows·ESXi·Linux 버전의 랜섬웨어 생성은 물론 피해자 관리와 같은 인프라까지 즉시 제공한다고 홍보하고 있다. 다만, 아직 LockBit 4.0 에 대한 상세 정보는 공개되지 않아 지속적으로 지켜볼 필요가 있다.

랜섬웨어 위협이 지속되고 있는 가운데, 12 월에도 총 2 건의 국내 랜섬웨어 사고 사례가 확인됐다. RansomHub 그룹은 국내 특수 선재 제품 제조 업체를 공격해 데이터를 공개했으며, 공개된 데이터에는 재무·회계·보험 관련 정보들이 포함되어 있다. 또한 Underground 그룹은 다크웹 유출 사이트와 텔레그램을 통해서 국내 반도체 부품 제조 업체의 데이터 탈취 소식을 전했다. 이들은 피해자 공개 후 이틀 만에 직원 개인정보, 재무 문서가 포함된 745GB 크기의 전체 데이터를 공개했다.

[1] 백도어(Backdoor): 정상적인 인증 과정을 거치지 않고 시스템에 접근할 수 있는 악성코드

한편, 지난 10 월 네트워크 및 보안 서비스 제공 업체 Cisco 의 데이터 4.5TB 를 탈취한 뒤 BreachForums 에 판매 글을 업로드했던 IntelBroker 는 탈취한 데이터의 일부를 무료로 공개했다. 데이터 유출 경로 조사 결과, 소스코드, 스크립트 및 기타 콘텐츠를 얻을 수 있는 리소스 센터 DevHub 를 통해서 데이터를 탈취한 것으로 확인됐다. IntelBroker 는 탈취한 데이터에는 소스코드, 자격 증명, 여러 기업 문서 등이 포함되어 있다고 주장했으며 12 월 25 일에는 4.84GB 의 데이터를 무료로 공개했다.

랜섬웨어 뉴스

Clop 그룹, Cleo 취약점 악용한 대규모 공격

- Cleo의 파일 전송 솔루션 Cleo Harmony, VLTrader, LexiCom의 취약점(CVE-2024-50623, CVE-2024-55956) 악용
- 두 취약점은 파일 읽기/쓰기 취약점으로, 이를 활용해 JAVA 백도어 업로드 및 추가 악성 행위 수행
- 총 66개 기업의 데이터를 탈취했다고 주장
- 별다른 대응을 하지 않을 시, 25년에 모든 피해자 리스트 공개 예정

LockBit 4.0 공개

- LockBit 그룹이 자신들의 DLS에 LockBit 4.0 공개를 예고
- 예고글을 통해서 신규 파트너를 모집하고 있으며, 777 달러(한화 약 110만원)을 지불하면 랜섬웨어 및 패널 접근 가능

IntelBroker, Cisco 데이터 일부 무료 공개

- 지난 10월 탈취한 Cisco의 데이터 4.5TB 중 일부인 4.84GB 를 12월 25일 무료로 공개
- 데이터는 리소스 센터 DevHub를 통해서 탈취했다고 주장

RansomHub, 국내 선재 제조 업체 공격

- 12월 3일, 샘플 데이터와 함께 데이터 공개 협박글 게시
- 재무, 회계, 보험 관련 정보 등이 포함되어 있다고 주장
- 12월 10일, 약 58GB 크기의 데이터 전체 공개

Underground, 국내 반도체 부품 제조 업체 공격

- 12월 17일 텔레그램과 다크웹 유출 사이트에 샘플 데이터 공개 및 협박글 게시
- 직원 개인정보 및 재무 문서 등 포함
- 12월 19일, 약 745GB 크기의 데이터 전체 공개
- 피해 기업은 11월에 공격 당했으며, 비용은 지불하지 않고 시스템을 복구했다고 주장

신규 LeakedData 그룹, 피해자 40건 게시

- 클리어넷에 데이터 유출 및 다운로드 사이트를 개설해 운영
- 피해자의 데이터 공개 전에는 이름을 필터링한 뒤, 일정 시간이 지나면 이름과 전체 데이터를 공개

신규 FunkSec 그룹, 피해자 89건 게시

- 12월 4일 발견됐으며, 다크웹 유출 사이트에 총 89건의 피해자 게시
- 랜섬웨어 및 데이터 공개 외에도, 추가적인 도구 및 서비스를 제공
- DDoS 공격, Gmail 탈취 도구, hVNC 도구 무료로 배포
- 유료 데이터 정렬 서비스를 파일 크기별로 제공

신규 BlueBox 그룹, 피해자 3건 게시

- 12월 10일 발견됐으며, 총 3건의 피해자를 게시
- 12월 25일부터 다크웹 유출 사이트에 접속이 불가능한 상태

■ 랜섬웨어 위협

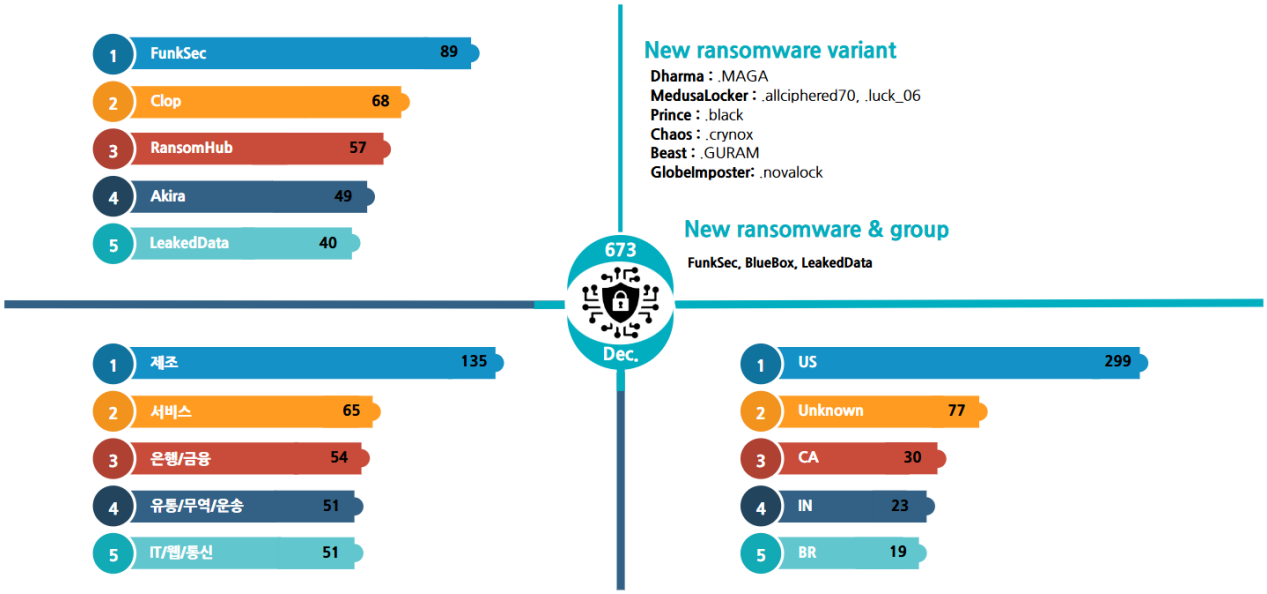


그림 2. 2024 년 12 월 랜섬웨어 위협 현황

새로운 위협

12 월에는 총 3 개의 신규 랜섬웨어 그룹이 발견됐다. BlueBox 그룹은 12 월 10 일 발견됐으며, 발견 당시 2 건의 피해자가 게시되어 있었다. 일주일 후 추가로 1 건을 더 게시했지만, 12 월 25 일부터는 다크웹 유출 사이트에 접속할 수 없는 상태다.

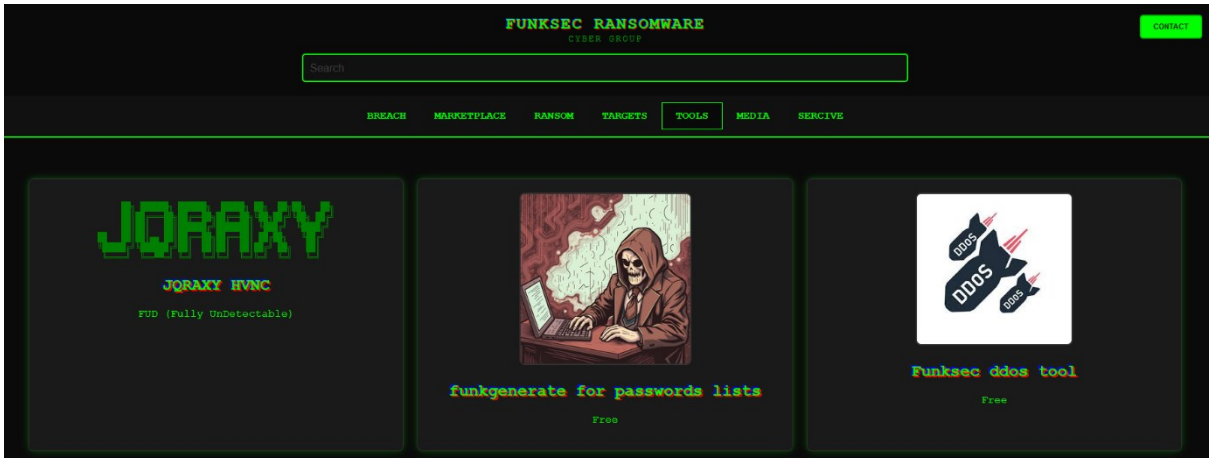


그림 3. FunkSec 다크웹 사이트

신규 랜섬웨어 그룹인 FunkSec 은 12 월 4 일 발견됐으며, 자신들의 다크웹 사이트를 통해서 피해 기업의 데이터를 게시하고 있다. 이들은 12 월에만 89 건의 신규 피해자를 게시했는데, 기업에서 탈취한 데이터뿐 아니라 출처가 불분명한 개인정보(여권, 계정정보 등) 또한 판매하고 있다. FunkSec 은 AES 알고리즘을

이용한 파일 암호화, 브라우저의 계정 데이터 탈취와 리버스 셸[2] 등의 기능을 가진 FunkLocker 를 홍보하고 있다. 뿐만 아니라 DDoS 공격 도구, Gmail 계정 탈취 도구, 가상 네트워크를 구축해 사용자 몰래 원격 접속이 가능한 hVNC 악성코드 등의 다양한 도구 및 서비스를 무료로 제공하고 있다.

그림 4. LeakedData 유출 사이트

한편, 클리어넷에서 활동하는 그룹도 확인됐다. LeakedData 그룹은 클리어넷을 통해 데이터를 공개하고 있으며, 이들은 12 월 한달 동안 총 40 명의 피해자를 업로드했다. 초반에는 공개 예정인 기업의 이름을 필터링했다가, 정해진 시간이 지나면 기업명과 전체 데이터의 다운로드 링크를 함께 공개한다.

Top5 랜섬웨어

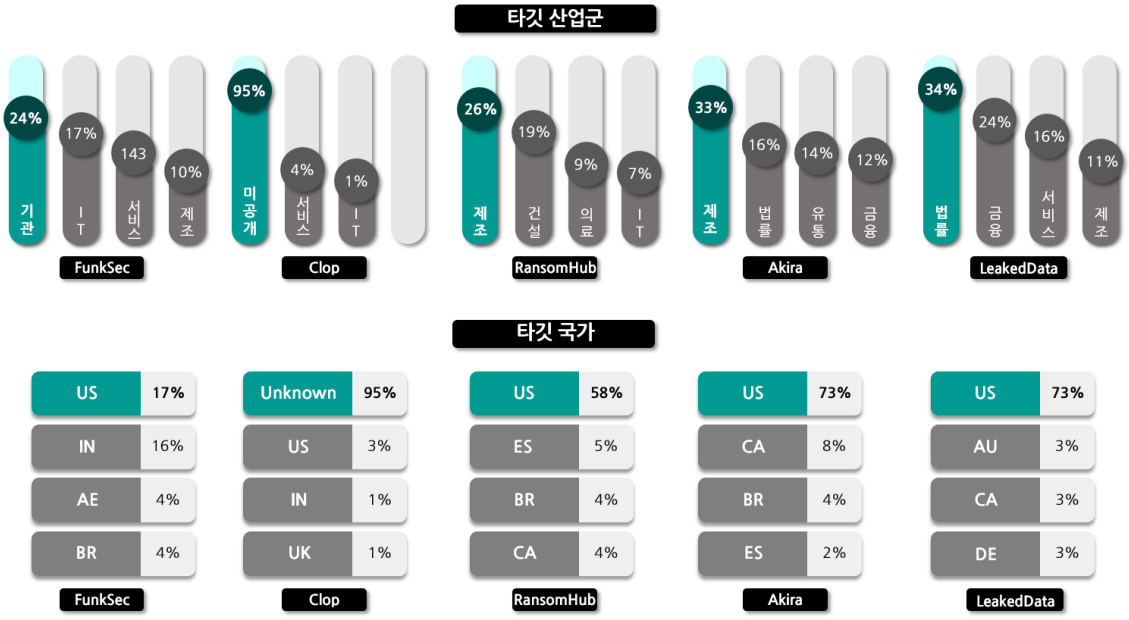


그림 5. 산업/국가별 주요 랜섬웨어 공격 현황

[2] 리버스 셸(Reverse Shell): 공격자가 사전에 설정한 수신 서버와 연결되어, 공격자가 시스템의 명령을 실행할 수 있는 악성코드

FunkSec 그룹은 12 월에 등장한 그룹임에도 89 건의 피해자를 게시하며 가장 활발히 활동했다. 이들은 기업의 데이터를 탈취해 판매하는 것뿐 아니라, 해당 기업의 인프라나 웹사이트 관리 페이지에 대한 액세스 권한과 특정 국적을 가진 개인 정보 등 다양한 데이터를 판매하고 있다. 이러한 데이터 판매 외에도 DDoS 공격, 계정 탈취, hVNC 와 같은 도구를 무료로 배포하고 있다. 또한 FunkSec 그룹이 공격한 기업 중 일부는 FunkSec 의 이미지가 삽입되어 디페이스[3] 된 경우도 존재한다.

23 년 관리형 파일 전송(MFT) 도구인 MOVEit Transfer, MOVEit Cloud 의 SQL 인젝션 취약점(CVE-2023-34362)을 악용해 대규모 침해 사고를 발생시켰던 Clop 그룹이 24 년에도 MFT 도구의 취약점을 이용해 침해 사고를 일으켰다. 이들은 Cleo 사의 파일 전송 솔루션 Cleo Harmony, VLTrader, LexiCom 에서 발생한 파일 쓰기 취약점(CVE-2024-50623, CVE-2024-55956)을 악용해 공격했고, 66 개의 기업이 침해당했다. 처음 피해자 리스트를 공개할 때는 기업명이 필터링 된 상태로 공개됐으나, 협상에 진전이 없으면 25 년에 모든 기업 리스트를 공개할 것이라고 예고했다.

RansomHub 그룹은 12 월 5 일 국내 기업의 미국 자회사를 공격해 약 200GB 가량의 데이터를 탈취했다. 피해 기업은 2020 년 인수된 미국의 고압탱크 업체로, RansomHub 는 7 일 후인 12 월 12 일에 전체 데이터를 압축파일로 공개했다. 또한 미국의 의료 및 소비자 제품 업체 Tekni-Plex 를 공격해 약 420GB 가량의 민감한 데이터를 탈취했으며, 여러 계약서와 부동산 문서 등이 포함된 샘플을 공개했다. RansomHub 는 협상이 원활히 진행되지 않자 약 3 일 간격으로 탈취한 데이터의 일부 또는 협상 채팅 내역을 공개했으며, 최종적으로 12 월 23 일 전체 데이터를 공개했다.

지난 11 월, 74 건의 피해자를 공개하며 활동이 급증했던 Akira 그룹은 12 월에도 49 건의 피해자를 발생시키며 활발히 활동했다. Akira 그룹은 미국의 투자 회사인 Luxor Capital Group 을 공격해 의료 기록·여권·출생 증명서·기밀 서신·금융 정보·계약 관련 정보 등을 탈취했다.

12 월에 등장한 LeakedData 그룹은 40 건의 피해자를 공개하고, 클리어넷에서 운영 중인 자신들의 데이터 유출 사이트에 피해자를 게시했다. 이들은 신규 피해자 공개 시 협상 기간 동안에는 기업명을 필터링해 두었다가, 정해진 시간이 지나면 기업명과 전체 데이터를 공개하는 방식을 사용한다. 공개된 피해 기업 중 29 곳이 미국 소재이며, 대부분이 금융과 법률/세무 분야의 기업으로 확인됐다.

[3] 디페이스(Deface): 웹 사이트의 디자인은 해커의 의도대로 변경해 해킹에 성공했음을 알리는 공격 방식

■ 랜섬웨어 집중 포커스

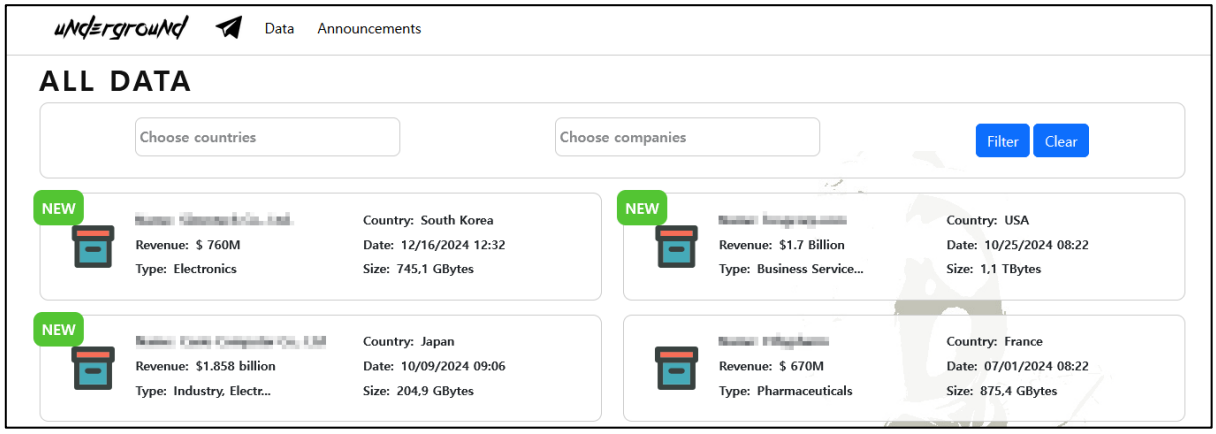
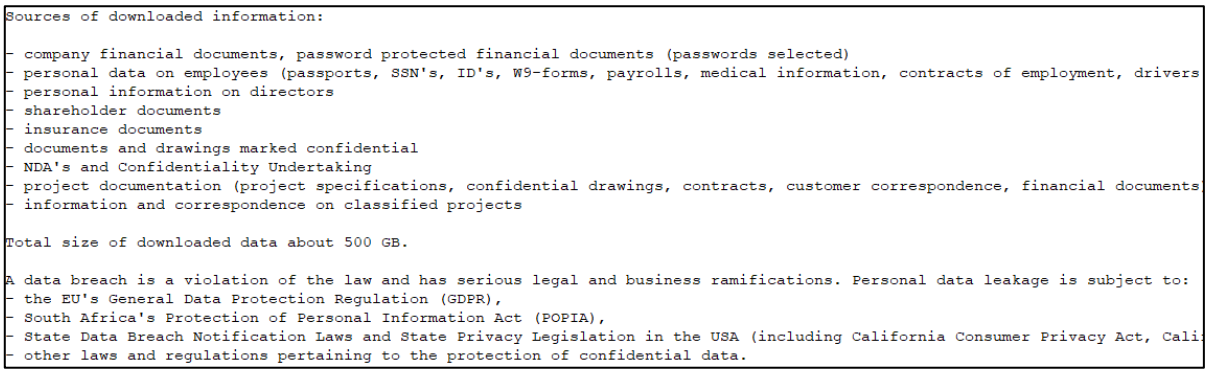


그림 6. Underground 다크웹 유출 사이트

Underground 그룹은 23 년 7 월 발견된 그룹이다. 이들은 활동 초기에 별도의 다크웹 유출 사이트는 운영하지 않았으며, 랜섬노트에 기재된 채팅 사이트를 통해서 몸값 협상을 진행하는 방식을 사용했다. 24 년 5 월에는 피해 기업으로부터 탈취한 데이터를 게시하는 신규 다크웹 유출 사이트가 발견됐으며, 이를 통해 24 년 12 월까지 총 19 건의 피해자를 게시했다. 게시한 피해자 중 2 곳은 국내 제조 업체로 확인됐으며, 각각 3 월과 12 월에 탈취한 데이터가 업로드됐다.

그림 7. Underground 그룹 텔레그램 채널

이들은 또한 24 년 3 월부터 텔레그램 채널을 운영하기 시작했으며, 채널을 통해서 신규 피해 기업 추가 소식과 샘플 데이터를 공유하는 것뿐 아니라 온라인 저장소 서비스인 MEGA 에 전체 데이터를 업로드 한 뒤 이를 텔레그램에 공유하는 모습도 확인됐다.



```
Sources of downloaded information:

- company financial documents, password protected financial documents (passwords selected)
- personal data on employees (passports, SSN's, ID's, W9-forms, payrolls, medical information, contracts of employment, drivers
- personal information on directors
- shareholder documents
- insurance documents
- documents and drawings marked confidential
- NDA's and Confidentiality Undertaking
- project documentation (project specifications, confidential drawings, contracts, customer correspondence, financial documents
- information and correspondence on classified projects

Total size of downloaded data about 500 GB.

A data breach is a violation of the law and has serious legal and business ramifications. Personal data leakage is subject to:
- the EU's General Data Protection Regulation (GDPR),
- South Africa's Protection of Personal Information Act (POPIA),
- State Data Breach Notification Laws and State Privacy Legislation in the USA (including California Consumer Privacy Act, Cali
- other laws and regulations pertaining to the protection of confidential data.
```

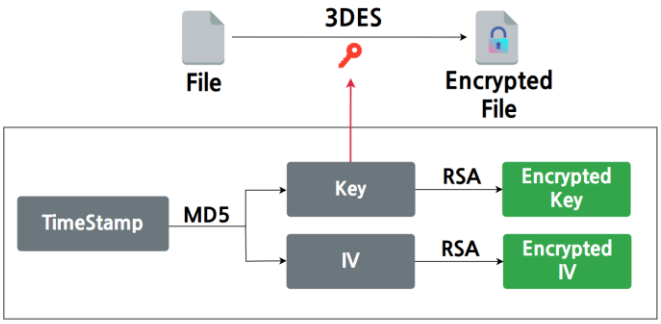
그림 8. Underground 랜섬노트

Underground 그룹은 공격 대상별로 랜섬노트를 수정한 뒤 사용한다. 랜섬노트에는 기업으로부터 탈취한 데이터의 리스트와 총 크기가 적혀 있으며, 데이터 유출로 발생할 수 있는 법률 위반 사항을 추가해 피해자를 협박하는 모습을 보이고 있다. 또한 랜섬노트에 다크웹 채팅 사이트의 주소와 접속에 필요한 ID, PW 를 제공해서 피해자가 직접 협상할 수 있도록 유도하고 있다.

Underground Ransomware

암호화 키

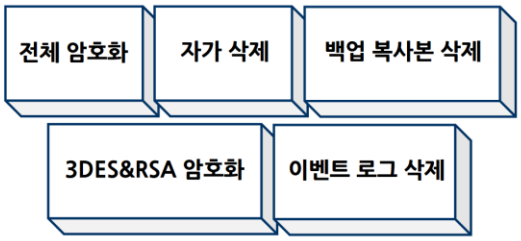
3DES 알고리즘으로 파일 암호화를 하고 RSA 알고리즘으로 키와 IV를 보호



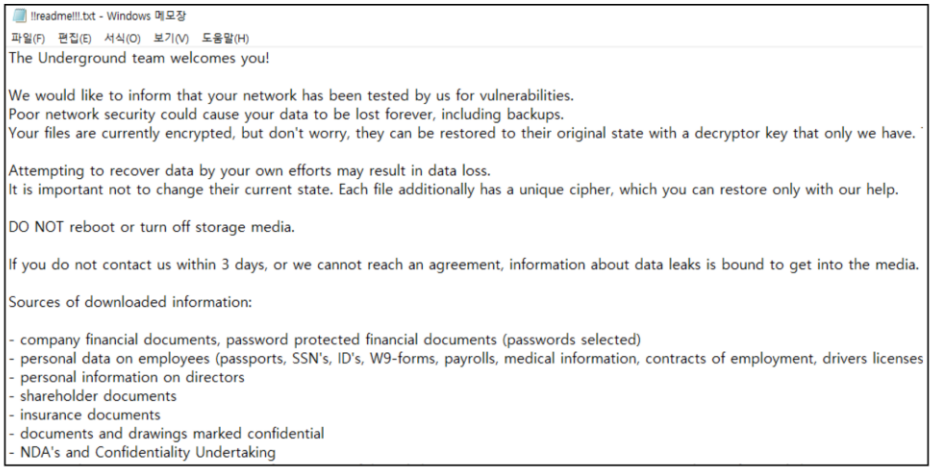
암호화 방식

파일 전체 암호화

특징



랜섬노트



!!readme!!!.txt - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

The Underground team welcomes you!

We would like to inform that your network has been tested by us for vulnerabilities.
Poor network security could cause your data to be lost forever, including backups.
Your files are currently encrypted, but don't worry, they can be restored to their original state with a decryptor key that only we have.

Attempting to recover data by your own efforts may result in data loss.
It is important not to change their current state. Each file additionally has a unique cipher, which you can restore only with our help.

DO NOT reboot or turn off storage media.

If you do not contact us within 3 days, or we cannot reach an agreement, information about data leaks is bound to get into the media.

Sources of downloaded information:

- company financial documents, password protected financial documents (passwords selected)
- personal data on employees (passports, SSN's, ID's, W9-forms, payrolls, medical information, contracts of employment, drivers licenses
- personal information on directors
- shareholder documents
- insurance documents
- documents and drawings marked confidential
- NDA's and Confidentiality Undertaking

!!readme!!!.txt

변경 확장자

확장자 변경 없음

제작 언어

C/C++

그림 9. Underground 랜섬웨어 개요

Underground 랜섬웨어 전략

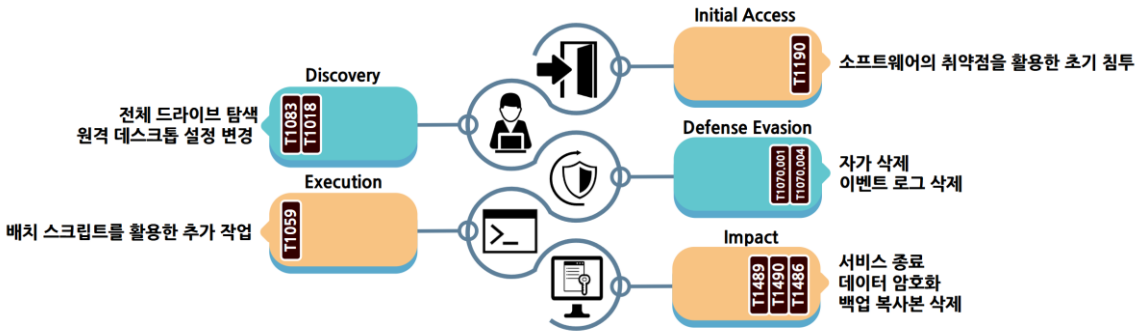


그림 10. Underground 랜섬웨어 공격 전략

Underground 랜섬웨어는 우선 Windows 명령어를 활용해 백업 복사본을 삭제하고 실행 중인 MS SQL 서버를 중지시킨다. 또한 레지스트리를 수정해 원격 접속에 사용되는 원격 데스크톱의 최대 유지 시간을 14 일로 변경한다. 사용하는 전체 명령어는 아래 표와 같다.

명령어	설명
vssadmin.exe delete shadows /all /quiet	백업 복사본 삭제
reg.exe add HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services / v MaxDisconnectionTime / t REG_DWORD / d 1209600000 / f	Remote Desktop 최대 연결 시간 변경(14일)
net.exe stop MSSQLSERVER /f /m	MS SQL 서버 종료

표 1. 실행 명령

이후 본격적으로 암호화 과정을 진행하는데, 만약 인자로 별도의 암호화 대상 경로를 입력했다면 해당 경로와 하위 경로에 존재하는 파일만 암호화를 진행한다. 인자를 입력하지 않았다면 전체 드라이브를 탐색해 암호화를 진행해야 한다. 또한 내부에 저장된 예외 항목을 확인해, 일부 디렉터리와 확장자를 가진 파일은 암호화를 진행하지 않는다. 예외 항목은 아래 표와 같다.

디렉터리	확장자
Windows Microsoft google\chrome mozilla\firefox opera	.sys, .exe, .dll, .bat, .bin, .cmd, .com, .cpl, .gadget, .inf1, .ins, .inx, .isu, .job, .jse, .lnk, .msc, .msi, .mst, .paf, .pif, .ps1, .reg, .rgs, .scr, .sct, .shb, .shs, .u3p, .vb, .vbe, .vbscript, .ws, .wsh, .wsf

표 2. 암호화 예외 대상

```
*lDistanceToMove = 0i64;
*FileSize = v20 - 4;
*DistanceToMoveHigh = 0i64;
SetFilePointer(FileW, v20 - 4, &FileSize[1], 0);
ReadFile(FileW, v15, 4u, &NumberOfBytesWritten, 0i64);// read last 4Bytes
v26 = *FileSize + 4i64;
*FileSize += 4i64;
if ( *v15 == 0x31415926 )            // Check Last 4Bytes of the file
  goto LABEL_63;
```

그림 11. 암호화 여부 확인

디렉터리를 순회하며 암호화 대상 파일에 하나씩 접근한 뒤, 해당 파일이 이미 암호화된 파일인지 확인한다. Underground 랜섬웨어는 파일 암호화 이후 파일 확장자 변경을 하지 않기 때문에 암호화된 파일의 끝에 4Bytes 의 시그니처(0x31415926)를 추가해 암호화 여부를 식별한다. 따라서 암호화를 진행하기 전에 파일 끝의 4Byte 를 확인해 파일의 암호화 여부를 확인한다.

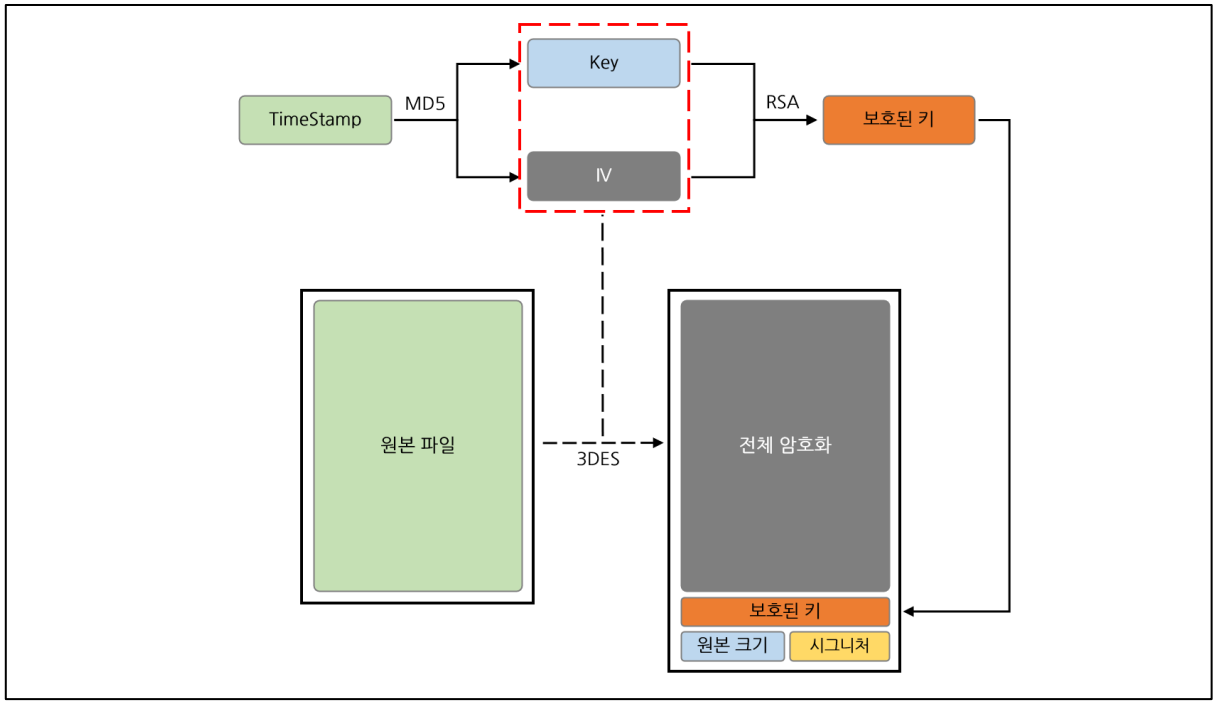


그림 12. 암호화 로직

시그니처가 없는 암호화 대상 파일이라면 암호화를 진행해야 한다. 파일마다 현재 시간을 나타내는 타임스탬프 값을 가져온 뒤, 이를 기반으로 MD5 해시를 2 개 생성한다. 첫 번째 MD5 해시 값의 앞 8Bytes 는 IV 로 사용하며, 두 번째 MD5 의 해시 값의 앞 24Bytes 는 암호화 키로 사용한다. 이후 파일 전체를 3DES 알고리즘을 사용해 암호화를 진행한다. 파일 암호화에 사용한 키와 IV 값은 RSA 알고리즘을 통해 암호화한 뒤 파일의 맨 뒤에 추가하며, 원본 파일 사이즈와 암호화된 파일임을 나타내기 위한 시그니처(0x31415926)를 파일의 맨 끝에 추가하고 암호화를 종료한다. 파일 암호화 이후에는 모든 디렉터리에 랜섬노트를 생성한다.

```
FileW = CreateFileW(L"temp.cmd", 0x40000000u, 1u, 0i64, 2u, 0x80u, 0i64);
if ( FileW != -1i64 )
{
  strcpy(
    String,
    "@Echo off\r\n"
    ":rep\r\n"
    "del %1\r\n"
    "if not errorlevel 0 goto rep\r\n"
    "for /F \"tokens=*\" %%1 in ('wevtutil.exe el') DO wevtutil.exe cl \"%%1\"\r\n"
    "del %0\r\n");
  NumberOfBytesWritten = 0;
  memset(Filename, 0, sizeof(Filename));
  memset(CommandLine, 0, sizeof(CommandLine));
  v7 = lstrlenA(String);
  WriteFile(FileW, String, v7, &NumberOfBytesWritten, 0i64);
  CloseHandle(FileW);
  ModuleHandleA = GetModuleHandleA(0i64);
  GetModuleFileNameA(ModuleHandleA, Filename, 0x400u);
  wsprintfA(CommandLine, "temp.cmd %s", Filename);
  StartupInfo.cb = 104;
  memset(&StartupInfo.cb + 1, 0, 100);
  memset(&ProcessInformation, 0, sizeof(ProcessInformation));
  CreateProcessA(0i64, CommandLine, 0i64, 0i64, 0, 0, 0i64, 0i64, &StartupInfo, &ProcessInformation);// self delete
```

그림 13. 자가 삭제 및 이벤트 로그 삭제

암호화 과정이 끝나고 나면, Windows 배치 스크립트를 이용해 랜섬웨어와 Windows 이벤트 로그를 삭제한다. 하드코딩된 자가 삭제 및 이벤트 로그 삭제 명령어를 temp.cmd 파일에 저장하고, 이를 실행한 뒤 종료한다.

Underground 랜섬웨어 대응방안

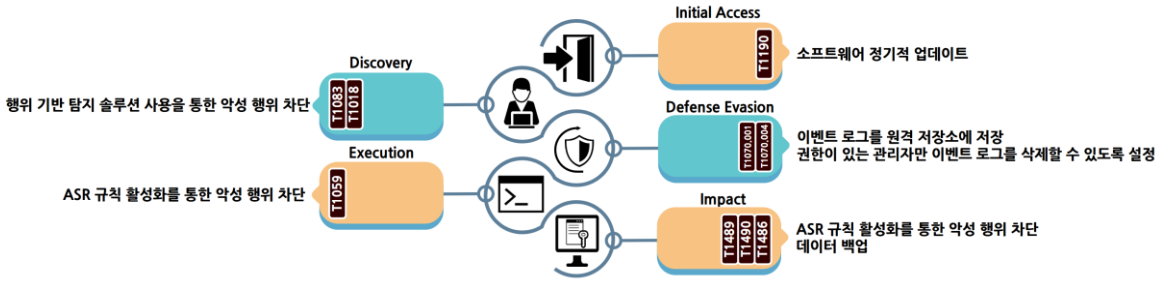


그림 14. Underground 랜섬웨어 대응방안

Underground 랜섬웨어는 소프트웨어의 취약점을 악용해 배포하는 것으로 알려져 있다. 따라서 사용하는 소프트웨어를 정기적으로 점검하고 최신 업데이트를 유지해 소프트웨어의 취약점을 통한 침입을 최소화해야 한다. 이외에도 피싱 메일의 링크나 첨부파일을 통해 침투를 시도할 수 있기 때문에 Anti-Virus 를 이용해 악성 파일 다운로드나 실행을 방지한다. Email Threat Detection & Response 와 같이 가상 환경에서 메일을 검역하는 솔루션을 사용해 피해를 최소화해야 한다.

랜섬웨어가 실행되면 Windows 명령어를 활용해 원격 접속 세션의 연결 유지 시간을 변경하고 특정 서비스를 종료한 후 저장된 백업 복사본을 삭제한다. 행위 기반 탐지 솔루션을 통해 레지스트리 경로에 비정상적인 접근 시도나 서비스 종료와 같은 악성 행위를 차단할 수 있다. 랜섬웨어가 작동해 파일이 암호화될 경우를 대비해 시스템 복구를 위한 백업 및 복사본을 별도의 네트워크나 저장소에 해 놔야 한다.

또한 배치 스크립트를 이용해 랜섬웨어 파일을 자가 삭제 및 Windows 이벤트 로그를 삭제한다. 파일 암호화 등을 방지하기 위해 ASR[4] 규칙을 활성화하거나 EDR[5] 솔루션을 활용해 공격자가 사용하는 특정 프로세스를 차단해 악성 행위를 막을 수 있다. 이외에도 이벤트 로그를 권한이 있는 사용자만 접근할 수 있도록 사전에 설정해 두거나, 이벤트 로그를 원격 저장소에 별도로 저장해 보존할 수 있다.

[4] ASR (Attack Surface Reduction): 공격자가 사용하는 특정 프로세스와 실행 가능한 프로세스를 차단하는 보호 기능

[5] EDR (Endpoint Detection and Response): 컴퓨터와 모바일, 서버 등 단말기에서 발생하는 악성 행위를 실시간으로 감지하고 분석 및 대응하여 피해 확산을 막는 솔루션

Indicator Of Compromise

Underground(SHA-256)

d4a847fa9c4c7130a852a2e197b205493170a8b44426d9ec481fc4b285a92666

cc80c74a3592374341324d607d877dcf564d326a1354f3f2a4af58030e716813

9d41b2f7c07110fb855c62b5e7e330a597860916599e73dd3505694fd1bbe163

eb8ed3b94fa978b27a02754d4f41ffc95ed95b9e62afb492015d0eb25f89956f

f1b6738897b0856d21367f47666aee3679cdf1cd41569bc9277b4f2604c09279

cc80c74a3592374341324d607d877dcf564d326a1354f3f2a4af58030e716813

9f702b94a86558df87de316611d9f1bfe99a6d8da9fa9b3d7bb125a12f9ad11f

9d41b2f7c07110fb855c62b5e7e330a597860916599e73dd3505694fd1bbe163

File Name

enc_getswin_x64.exe

참고 사이트

• CyberPress (https://cyberpress.org/microsoft-office-zero-day-to-spread-ransomware/)

• BleepingComputer 공식 홈페이지 (https://www.bleepingcomputer.com/news/security/clop-ransomware-is-now-extorting-66-cleo-data-theft-victims/)

• BleepingComputer 공식 홈페이지 (https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-cleo-data-theft-attacks/)

• Qualys 위협 분석 보고서 (https://threatprotect.qualys.com/2024/12/03/zyxel-firewall-directory-traversal-vulnerability-exploited-in-ransomware-attack-cve-2024-11667/)

• Security Week (https://www.securityweek.com/hacker-leaks-cisco-data/)

• KBS 뉴스 (https://news.kbs.co.kr/news/pc/view/view.do?ncd=8133787)

• BleepingComputer 공식 홈페이지 (https://www.bleepingcomputer.com/news/security/us-charges-russian-israeli-as-suspected-lockbit-ransomware-coder/)

• 보안뉴스 (https://www.boannews.com/media/view.asp?idx=135211)

• 뉴스 저널리즘 (https://www.ngetnews.com/news/articleView.html?idxno=516169)