Keep up with Ransomware

Devman: 하나의 그룹, 여러 랜섬웨어

■ 개요

2025 년 5 월 랜섬웨어 피해 사례 수는 지난 4 월(550 건)에 비해 약 12% 감소한 484 건을 기록했다. 지난 3 월부터 매달 꾸준히 피해 사례 수가 감소하고 있는 추세지만, 5 월에 Vanhelsing 랜섬웨어의 소스코드가 공개돼 이를 악용한 변종이나 그룹이 등장할 가능성이 높아졌다.

5 월 초, LockBit 의 다크웹 유출 사이트가 "Don't do crime CRIME IS BAD xoxo from Prague"라는 문구와 함께 변조됐다. LockBit 의 경우 다크웹 유출 사이트가 변조뿐만 아니라 관리자 패널도 해킹을 당해 내부 데이터베이스 파일 일부가 유출됐다. 유출된 데이터베이스에는 가상화폐 지갑 주소, 랜섬웨어 버전 별 사용된 구성 정보, 제휴사 계정 정보, 채팅 내역 등이 포함되어 있었으며 복호화에 사용되는 개인키는 포함되어 있지 않았다. 이번 해킹 사태로 인해 평판이 훼손됐음은 물론, 6 월 초까지 다크웹 유출 사이트가 오픈 되지 않고 있는 상태로 보아 운영에 큰 차질이 생긴 것으로 보인다.

러시아 해킹 포럼 RAMP 에서 Vanhelsing 랜섬웨어의 소스코드가 공개됐다. 이전 멤버인 th30c0der 가 Vanhelsing 랜섬웨어의 소스코드를 판매한다는 글을 포럼 관련 사이트에 업로드한 것이다. Vanhelsing 운영진이 이를 인정하며 자신들의 기존 랜섬웨어와 패널 페이지 소스코드 일부를 공개했다. 하지만 th30c0der 는 자신이 패널부터 결제 시스템, 랜섬웨어를 개발한 핵심 인물이라고 소개하며, 공개된 코드가 전체 코드가 아니며 자신이 판매하고 있는 소스코드가 최신 버전이라고 주장하고 있다.

한편 Qilin 랜섬웨어의 복호화 도구로 추정되는 파일이 발견되기도 했다. 해당 샘플은 암호화된 파일을 AES 알고리즘이나 ChaCha20 알고리즘으로 복호화하는 기능을 제공한다. 다만, 모든 Qilin 랜섬웨어를 대상으로 복호화를 제공하진 않고, 특정 버전 혹은 특정 암호화 키로 암호화된 경우에만 정상적으로 복호화되는 것으로 확인됐다.

5 월에는 국내 침해 사례가 여러 건 확인됐다. RaLord 로 활동을 시작해 5 월에 리브랜딩한 Nova 그룹이 국내 대학교를 공격해 내부 문서, 보고서, 포털 사이트 소스코드, 데이터베이스, 학생 정보 등을 탈취했다고 주장했다. 6 월에는 탈취한 데이터가 공개됐으나, 개인 정보는 포함되지 않았으며, 포털 사이트 소스코드와 데이터베이스 관련 정보만 확인됐다.

TCR Team 은 국내 금융과 제조 분야의 기업 2 곳을 공격했다. 다크웹 유출 사이트에선 협상에 실패한 기업으로 분류되어 일부 데이터가 함께 공개됐다. 확보한 정보에는 내부 문서와 직원 개인 정보가 포함되어 있는 것으로 확인되었으나 약 2 주뒤에 공개된 데이터는 내려갔으며, 5 월 말에는 다크웹 유출 사이트가 비활성화 되어 접속이 불가능한 상태이다.

SAP 의 애플리케이션 통합 및 실행 플랫폼 NetWeaver 에서 발생한 파일 업로드 취약점(CVE-2025-31324)을 악용한 랜섬웨어 그룹이 확인됐다. 해당 취약점은 4 월 24 일 패치 됐으나 BianLian 그룹과 RansomEXX 그룹이 이를 악용한 정황이 확인됐다. 두 그룹 모두 랜섬웨어를 배포하진 않았으나, 취약점을 악용해 BianLian 의 C2[1] 서버와 통신하거나 RansomEXX 가 주로 사용하는 백도어[2] PipeMagic 을 배포하는 등의 행위가 포착됐다.

[1] C2: 악성코드에 감염된 PC 나 서버를 대상으로 공격자가 원하는 행위를 하도록 하는 명령을 하달하는 서버

[2] 백도어: 보안 시스템이나 인증 절차를 우회하여 대상 시스템에 접근할 수 있도록 하는 악성코드

■ 랜섬웨어 뉴스

LockBit 그룹, 내부 데이터베이스 유출

- 유출된 정보에 따르면 4월 말 해킹됐으며 5월 초 정보 공개
- “Don’t do crime CRIME IS BAD xoxo from Prague” 문구와 함께 내부 데이터베이스 일부 유출
- Everest 그룹의 해킹과 동일한 자의 소행으로 추정

Qilin 랜섬웨어 복호화 도구 발견

- Qilin 랜섬웨어로 암호화된 파일을 AES / ChaCha20 알고리즘 중 해당하는 알고리즘으로 복호화
- 모든 버전의 Qilin 랜섬웨어를 대상으로 복호화가 가능하진 않으며, 특정 버전 혹은 키에 해당하는 경우만 정상 동작

Vanhelsing 랜섬웨어 소스코드 공개

- “th30c0der”라는 유저가 5월에 RAMP 포럼에서 소스코드 판매
- Vanhelsing 운영진은 실제 함께 일한 유저임을 인정했으며, 자신들의 랜섬웨어 소스코드를 공개
- “th30c0der”는 공개된 코드가 v1에 해당하며, 자신은 최신 버전인 v2를 판매하고 있다고 주장

TCR Team 그룹, 국내 기업 2곳 공격

- 금융 및 제조업에 해당하는 기업을 공격해 데이터 탈취 및 공개
- 내부 문서와 직원 개인 정보가 포함된 데이터가 일부 공개
- 5월 말에 다크웹 유출 사이트가 비활성화되며 더 이상 접근 불가

Nova 그룹, 국내 대학교 공격

- 국내에 소재한 대학교를 공격해 내부 문서, 소스코드, 학생 정보 등을 탈취했다고 주장
- 6월 초 데이터가 공개됐으나 개인 정보는 포함되지 않았으며, 포털 사이트 소스코드와 데이터베이스가 포함

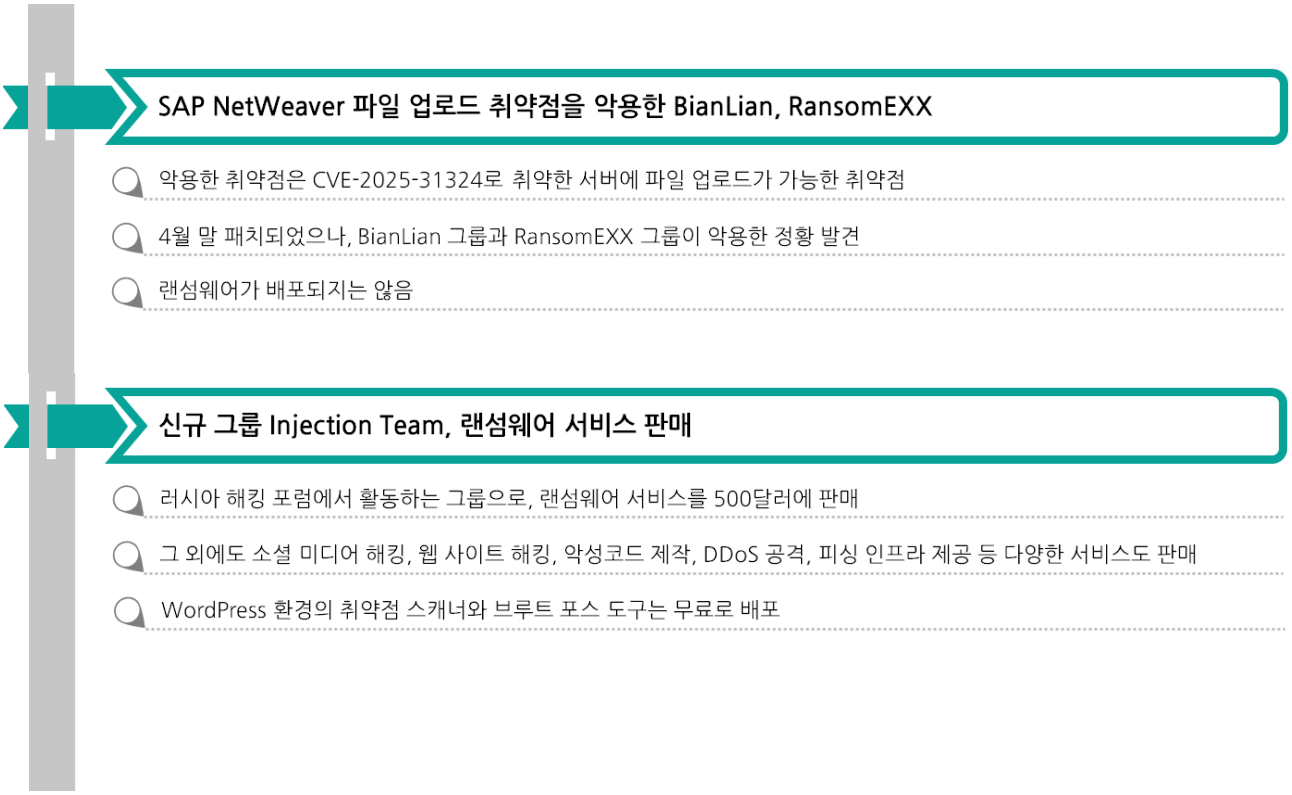
SAP NetWeaver 파일 업로드 취약점을 악용한 BianLian, RansomEXX
악용한 취약점은 CVE-2025-31324로 취약한 서버에 파일 업로드가 가능한 취약점
4월 말 패치되었으나, BianLian 그룹과 RansomEXX 그룹이 악용한 정황 발견
랜섬웨어가 배포되지는 않음
신규 그룹 Injection Team, 랜섬웨어 서비스 판매
러시아 해킹 포럼에서 활동하는 그룹으로, 랜섬웨어 서비스를 500달러에 판매
그 외에도 소셜 미디어 해킹, 웹 사이트 해킹, 악성코드 제작, DDoS 공격, 피싱 인프라 제공 등 다양한 서비스도 판매
WordPress 환경의 취약점 스캐너와 브루트 포스 도구는 무료로 배포

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

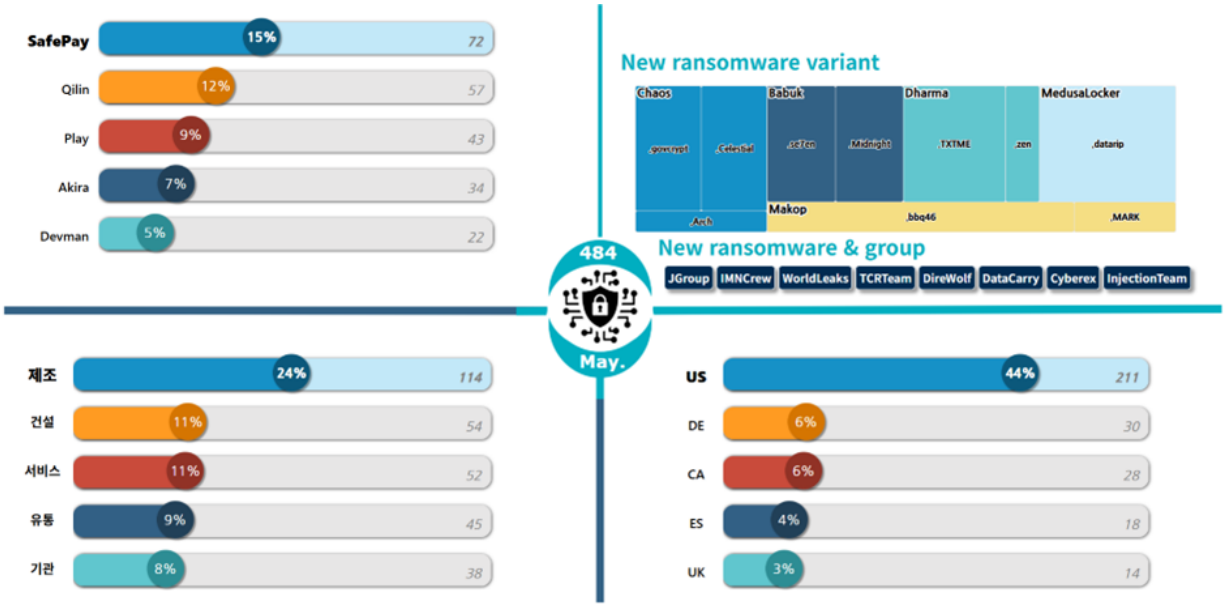

그림 2. 2025 년 5 월 랜섬웨어 위협 현황

새로운 위협

5 월에는 총 8 개의 신규 랜섬웨어 그룹이 확인됐다. JGroup 은 18 건, Imncrew 는 8 건, WorldLeaks 는 14 건, Direwolf 는 11 건, DataCarry 는 10 건 등 자체 다크웹 유출 사이트에 신규 피해자를 각각 업로드한 것이 확인됐다. 또한 Cyberex 그룹은 별도의 유출사이트를 운영하지 않고 채팅 사이트만 존재해, 감염된 피해자에게 몸값 협상을 진행하고 있다.

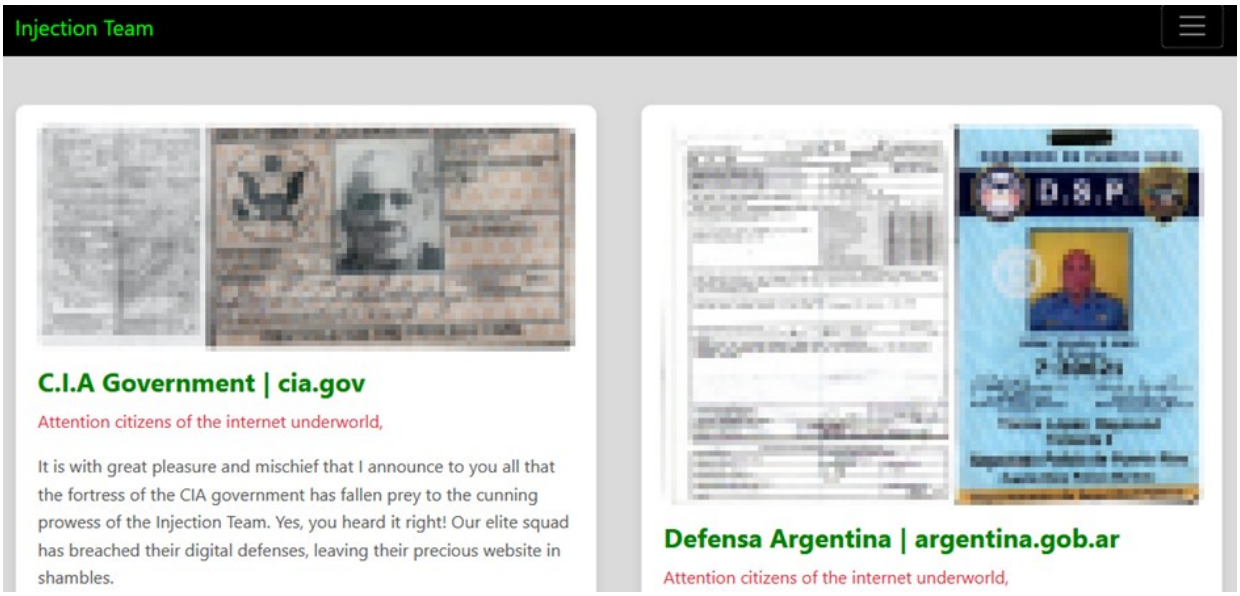

그림 3. InjectionTeam 다크웹 유출 사이트

신규 Injection Team 그룹은 러시아 해킹 포럼에서 자신들을 홍보하고 있는 그룹이다. 랜섬웨어 서비스는 물론 소셜 미디어 해킹, 웹 사이트 해킹, 악성코드 제작, DDoS[3] 공격, 피싱 인프라 제공 등의 각종 서비스를 1,000 달러 내외로 제공하고 있다. 이러한 유료 서비스 외에도 WordPress 환경의 취약점 스캐너와, 브루트 포스[4] 도구를 무료로 배포하고 있다.

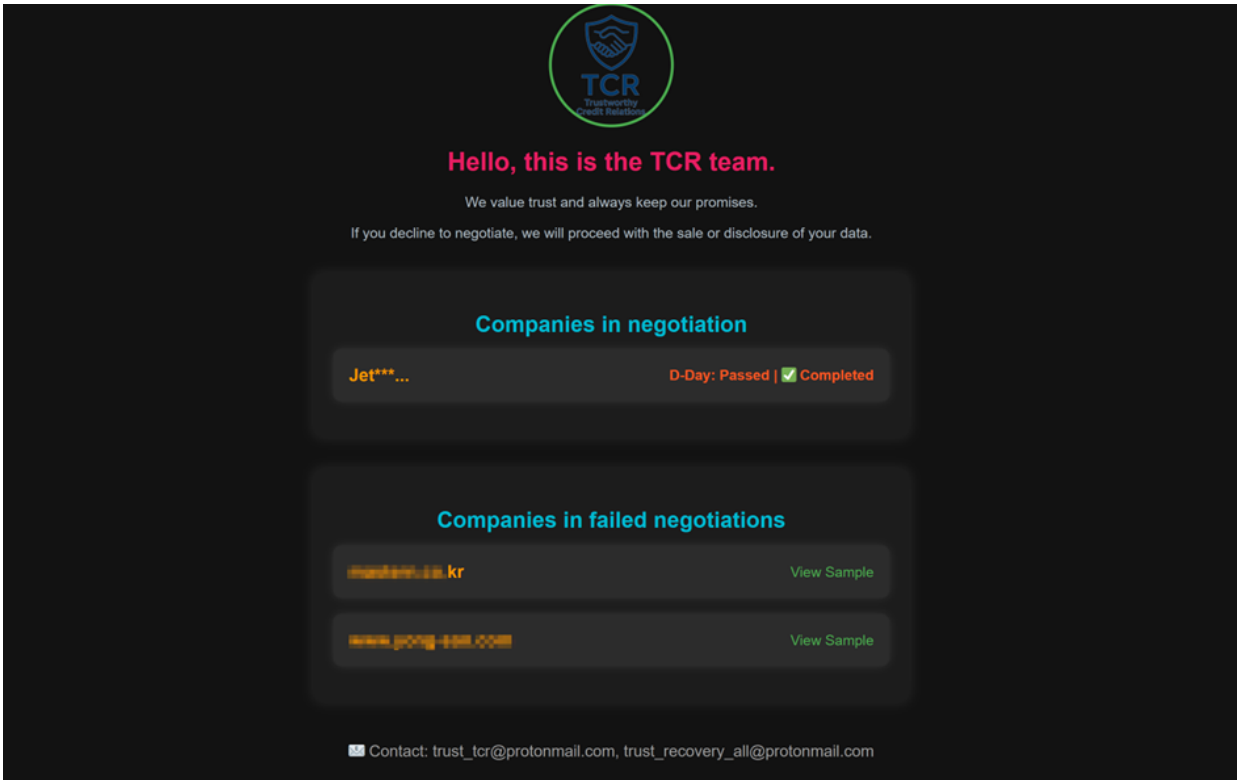

그림 4. TCR Team 다크웹 유출 사이트

국내를 공격한 신규 그룹도 확인됐다. TCR Team 그룹의 공격은 5 월 발견됐으며 국내 기업 2 곳을 공격해 일부 데이터를 공개했다. 피해 기업은 각각 금융 투자 기업과 자동차 부품 제조 기업으로 기업 내부 문서와, 직원 개인 정보가 포함된 문서들로 확인됐다. 5 월 말에는 샘플 데이터에 접근이 불가능해졌으며, 순차적으로 다크웹 유출 사이트 자체도 비활성화 됐다.

[3] DDoS (Distributed Denial of Service): 악의적으로 대상 네트워크, 서버, 온라인 서비스 등에 많은 트래픽을 발생시켜 해당 시스템의 기능을 정상적으로 사용하지 못하도록 하는 공격

[4] 브루트 포스(BruteForce): 조합 가능한 모든 경우의 수를 대입해보는 공격 기법

Top5 랜섬웨어

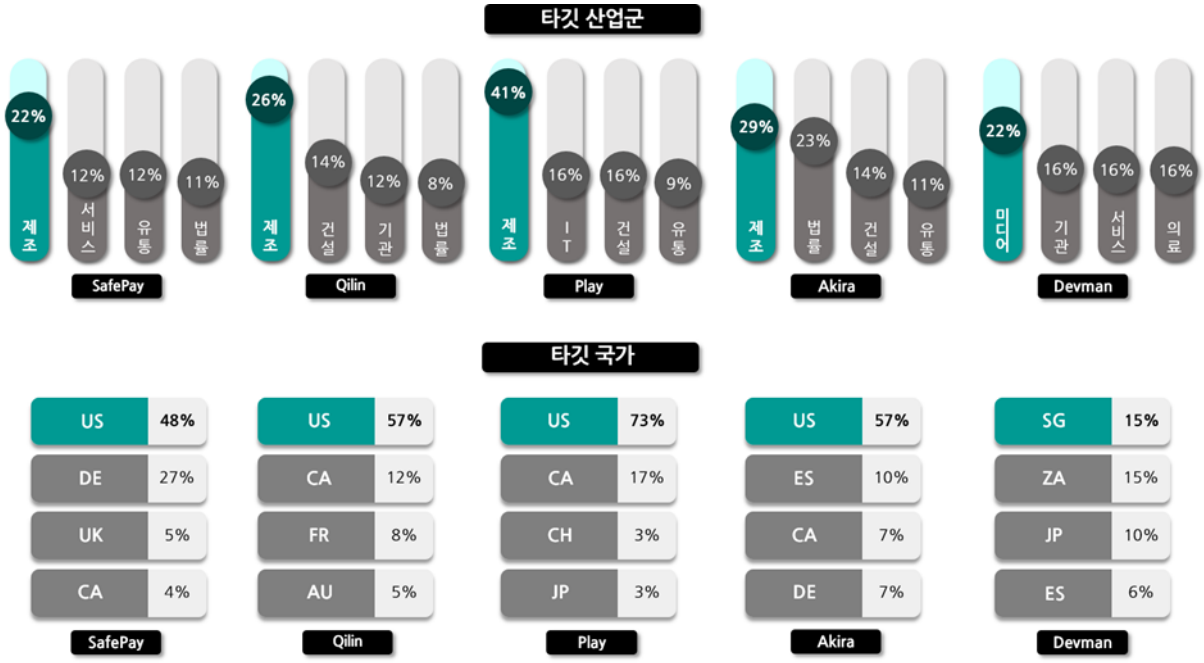

그림 5. 산업/국가별 주요 랜섬웨어 공격 현황

SafePay 그룹은 체코에 위치한 공립 고등학교 Gymnázium a Jazyková škola Zlín 을 공격해 30GB 가량의 내부 데이터를 공개했다. 해당 데이터에는 학교 내부 기록은 물론 학생의 정보가 일부 포함되어 있었다. 또한 호주의 법률 회사 RTB Legal 을 공격해 200GB 규모의 데이터를 탈취했으며, 이로 인해 법원 문서, 고객 정보, 이메일, 계약서, 유언장 등 다양한 법률 및 행정 문서가 유출됐다.

Qilin 그룹은 미국 조지아주 Cobb 카운티 정부를 공격해 약 150GB 크기의 40 만개의 문서를 탈취했다. 탈취한 데이터에는 주민 및 공무원 개인정보는 물론 사망자 이미지가 포함되어 있었다. 또한 미국의 컨트리 클럽 Army Navy Country Club 을 공격해 300GB 규모의 데이터를 탈취했으며, 이로 인해 회원의 이름, 주소, 신용카드 정보, 자격증명 등 민감 정보가 유출됐다.

Play 그룹은 미국의 기업을 집중적으로 공격하는 모습을 보이고 있다. 5 월에는 미국의 건설업체 W.E. Bowers 를 공격해 고객 문서, 예산, 급여 명세서, 회계 자료, 신분증, 재무 정보 등 다양한 데이터를 유출했으며, 구체적인 피해 규모는 공개되지 않았다. 또 다른 미국 건설업체 Greater Seattle Concrete 도 공격당했으며, 이로 인해 내부 문서와 기밀 정보가 포함된 데이터가 5 월 말 공개됐다.

Akira 그룹은 미국 에너지업체 Pacific Summit Energy 를 공격해 약 160GB 규모의 데이터를 탈취했다. 직원 개인 정보, 재무 감사 자료, 내부 업무 문서 등이 포함되어 있으며, 해당 데이터는 전부 공개됐다. 또한 미국의 금융 기관 Flagship Bank 를 공격해 고객 정보, 세부 재무 자료, 계약서 등이 포함된 40GB 규모의 데이터를 탈취해 공개했다.

4 월에 등장한 신규 그룹 Devman 은 케냐의 공공 연금 기구 NSSF Kenya 를 공격해 2.5TB 가량의 데이터를 탈취했다고 주장하고 있다. 자신의 X(트위터)를 통해서 인증 스크린샷을 지속적으로 업로드하고 있으며, 다크웹 유출 사이트에 정찰, 데이터 탈취, 파일 암호화 방식을 설명하기도 했다. 탈취한 데이터에는 이름, 주소, 사회보장번호와 같은 개인정보가 포함되어 있으며 몸값으로는 450 만 달러(한화 약 61 억원)을 요구하고 있다. 필리핀 매체 GMA Network 도 내부 서버가 암호화됐으며 65GB 가량의 데이터가 유출됐다. 몸값으로는 250 만 달러(한화 약 34 억원)을 요구하였으나 GMA Network 는 유출 데이터에 민감 정보나 개인 정보가 포함되지 않았다고 주장했다.

■ 랜섬웨어 집중 포커스

Welcome to Devman's Place

Soon there will be some news. Thanks for waiting.

WE ARE ACTIVELY BUYING ACCESS TO COUNTRIES(UK, FRANCE, CANADA). THESE COUNTRIES ARE OUR MAIN PRIORITY.

P.S sorry for being offline

My Victims

Company	Status	Ransom Amount
Doumen.fr(QILIN)	Negotiating	800k USD
Optimax Technology(QILIN)	Whaitng	590k USD
Texas Construction Firm(QILIN)	Pending	Amount TBD
Tawasol (APOS Attack)	Pedning	150k USD
Feel Four (QILIN Attack)	Pedning	60k USD
China Harbour (s) Engeneiring Company (Dragon Force Attack) FILE SAMPLE 1 avaliable /CHEC/CHECsample.zip	Ecnrypted(we encrypted every signle device on the network and downloaded 50gb of sensitive files)	450k USD
Honk Kong Victim (To be discoled)	(To be discoled)	(To be discoled)

그림 6. Devman 다크웹 유출 사이트

Devman 그룹은 25 년 4 월부터 활동을 시작한 그룹으로, 지금까지 총 44 건의 피해자를 게시했다. 처음 등장했을 때에는 “My Writeups” 페이지에 공격에 사용한 소프트웨어 취약점이나 취약한 패스워드 등을 공격 단계별로 상세하게 설명하는 독특한 모습을 보였다. 또한 자체 랜섬웨어가 아니라 다른 그룹의 랜섬웨어를 공격에 적극적으로 활용하며, 피해자가 Devman 유출 사이트뿐만 아니라 다른 랜섬웨어 그룹의 유출 사이트에도 함께 게시되기도 했다. 공격에 활용한 다른 그룹의 랜섬웨어는 Apos, Qilin, DragonForce, RansomHub 가 있으며, 5 월부터는 자체 랜섬웨어인 Devman 랜섬웨어를 악용한 피해자를 게시하기 시작했다.

Devman 그룹은 주로 X(트위터)에서 활동한다. 개발중인 랜섬웨어 서비스 페이지나, 공격 예고 글, 자체 제작 랜섬웨어 테스트 동영상 등 자신들을 과시하기 위한 용도로 주로 활용하고 있다. 또한 유출 규모가 큰 기업의 경우, 피해자의 X 계정을 직접적으로 언급하면서 확보한 샘플 이미지를 공개하거나 침투한 환경의 스크린샷을 공개하며 조롱하고 협박하는 모습도 확인됐다.

TBD GREECE	ALL FILES ENCRYPTED 120gb of data stollen	NEGOTIATION STARTED
TBD HONK KONG	ALL FILES ENCRYPTED	PAYED
TBD KOREA	ALL FILES ENCRYPTED	PAYED

그림 7. 일부 정보만 공개된 피해자 리스트

이들은 피해자를 공개할 때, 기업명을 바로 공개하지 않고 기업의 소속 국가나, 어떤 분야의 기업인지 우선적으로 공개하고 있다. 그 중에는 국내 기업도 포함되어 있으나, 정확한 피해 규모나 요구한 몸값은 공개되지 않고 이미 비용을 지불한 것으로 확인된다.

5 월에는 Devman 그룹의 자체 랜섬웨어로 추정되는 샘플이 발견됐으며, Devman 그룹이 자신들의 X 계정을 통해 해당 랜섬웨어가 v1 버전임을 인정하기도 했다. 다만 랜섬웨어가 지난 3 월 해킹당한 Mamona 랜섬웨어와 매우 유사해 비교 분석한 결과, 일부 기능이 추가된 버전으로 확인됐다. 6 월부터는 자체 랜섬웨어 서비스를 공개해 활동이 더 왕성해질 것으로 보여 이에 대비하고자 Devman 랜섬웨어를 분석한 내용을 공유하고자 한다.

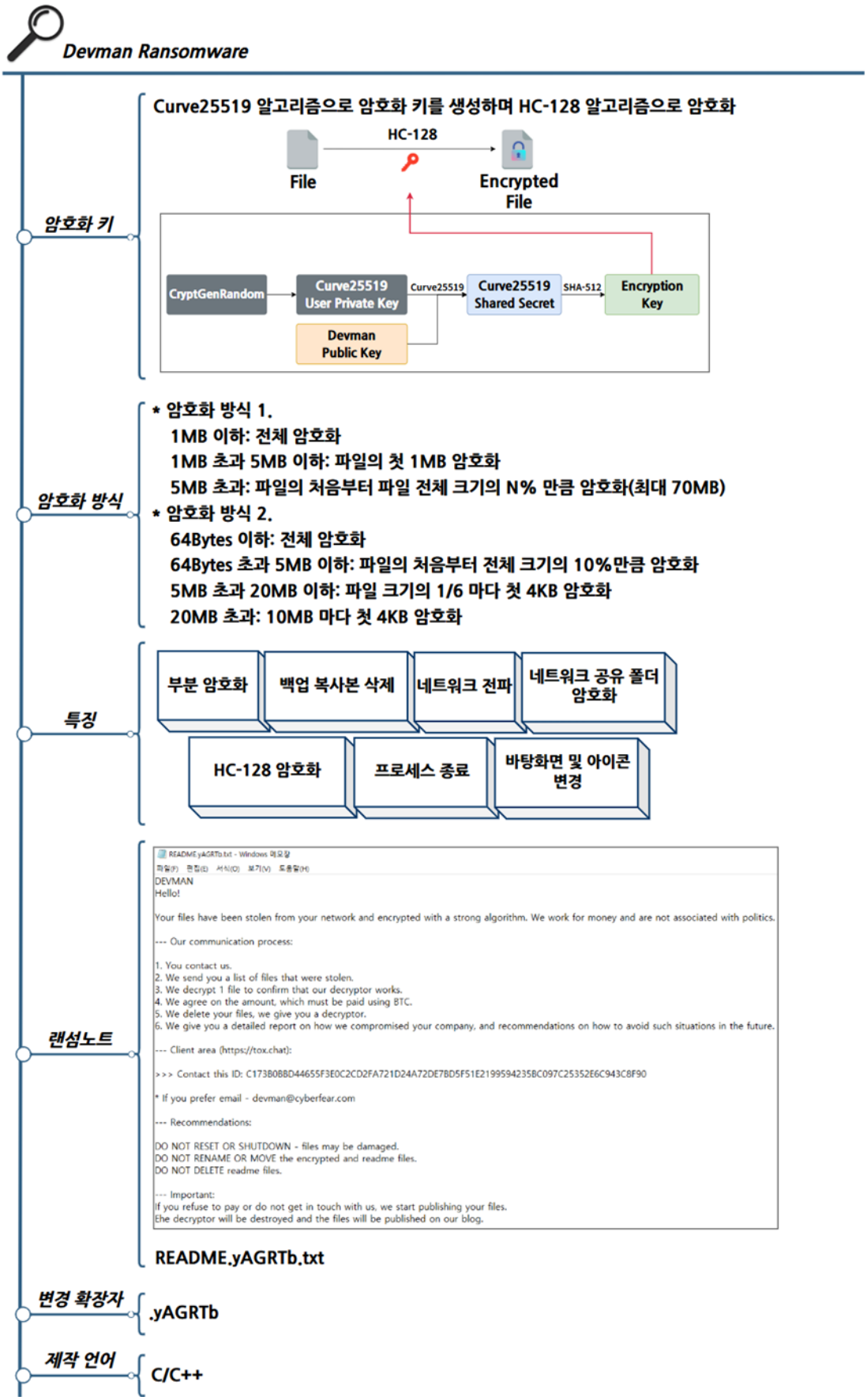

그림 8. Devman 랜섬웨어 개요

Devman 랜섬웨어 전략

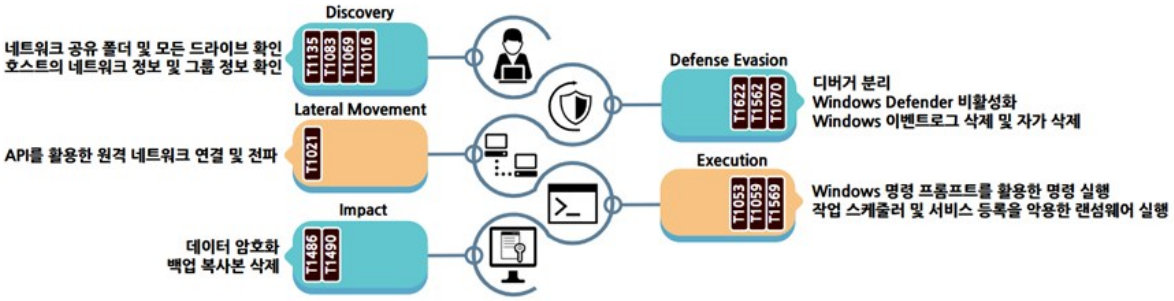

그림 9. Devman 랜섬웨어 공격 전략

Devman 랜섬웨어는 Mamona 랜섬웨어와 대부분의 기능이 동일하다. 차이점이 있다면 아이콘을 지정한 이미지 파일로 변경하거나, 디버거 분리를 위해 랜섬웨어를 재실행하는 기능 추가 그리고 대폭 개선된 네트워크 전파 부분이다. 변경점은 실행 인자에도 일부 반영됐다. Mamona 버전에서는 네트워크 인증을 위해서 NTLM[5] 해시를 전달하기 위한 인자 -H 가 Devman 버전에서는 삭제됐다. 또한 네트워크 전파 활성화를 위한 -ldap 인자와 네트워크 전파 대상을 지정하기 위한 -host, 디버거 분리 기능을 비활성화 하기 위한 -detached 인자가 함께 추가됐다.

구분	설명
-log	로그 출력
-keep	자가 삭제 비활성화
-skip-net	로컬 디스크만 암호화
-skip-local	네트워크만 암호화
-code {32Bytes key}	랜섬웨어 실행에 필요한 비밀번호
-sub {subnet}	네트워크 암호화 대상 네트워크 대역
-p {password}	네트워크 로그인 비밀번호
-u {username}	네트워크 로그인 이름
-time {HH:MM}	지정한 시각(HH:MM)까지 대기 후 실행
-delay {ss}	지정한 시간동안 대기 후 실행
-threads {int}	암호화 스레드 수 설정
-path {path}	특정 폴더 암호화
-host {ip_addr}	**특정 호스트 암호화**
-ldap	**네트워크 전파 활성화**
-detached	**랜섬웨어 재실행 비활성화**

표 1. Devman 랜섬웨어 실행 인자

[5] NTLM: 보안 인증 프로토콜 중 하나로, 인증을 위해 실제 암호 대신 해시를 전달해 권한 부여 및 인증을 제공하는 기능

Devman 랜섬웨어는 실행인자 외에도 암호화 관련 설정이나, 랜섬노트 내용, 키 생성에 필요한 공개키 등 각종 정보를 암호화한 채로 특정 세션에 저장하고 있으며, 이를 복호화해 사용한다. 확인된 정보는 아래와 같다.

오프셋	설명
config[0]	부분 암호화 비율
config[4]	랜섬노트 내용
config[2056]	자가 삭제 여부
config[2057]	이벤트 로그 삭제 여부
config[2058]	서비스 종료 여부
config[2059]	프로세스 종료 여부
config[2060]	랜섬웨어 비밀번호 검증 여부
config[2061]	암호화 모드 설정
config[2062]	랜섬노트 프린터 출력 여부
config[2064]	아이콘 변경 여부
config[2065]	네트워크 공유 자원 마운트 여부
config[2066]	랜섬웨어 비밀번호 (32Bytes)
config[2098]	암호화 확장자
config[2114]	Curve25519 공개키 (32Bytes)

표 2. Devman 랜섬웨어 설정값

랜섬웨어는 또한 복구 방지와 분석 방해를 위해 각종 기록이나 흔적을 삭제한다. 휴지통에 있는 데이터를 모두 삭제하며, 설정 값에 따라 Windows 환경의 모든 이벤트 로그를 삭제한다. 또한 명령 프롬프트 명령어를 활용해 백업 복사본을 삭제하며, 모든 파일 암호화가 끝난 뒤에는 랜섬웨어를 자체적으로 삭제한다.

명령어	설명
cmd.exe /c vssadmin delete shadows /all /quiet	백업 복사본 삭제
cmd.exe /C ping 127.0.0.7 -n 3 > Nul & Del /f /q \"%s\	자가 삭제

표 3. 삭제 관련 명령어

설정값에 서비스 종료나 프로세스 종료 관련 설정이 되어 있다면 원활한 파일 암호화를 위해 특정 서비스와 프로세스를 우선적으로 종료한다. 종료 대상 서비스 및 프로세스는 아래 표와 같다.

서비스	프로세스
WinDefend, SecurityHealthService, wscsvc, Sense, WdNisSvc, WdNisDrv, WdFilter, WdBoot, wdnisdrv, wdfilter, wdboot, mpssvc, mpsdrv, BFE, MsMpSvc, SepMasterService, wscsvc, SgrmBroker, SgrmAgent, EventLog	MsMpEng.exe, NisSrv.exe, SecurityHealthService.exe, smartscreen.exe, SecHealthUI.exe, MpCmdRun.exe, MSASCui.exe, MpUXSrv.exe, SgrmBroker.exe, MsSense.exe, SenseIR.exe, SenseCE.exe, SenseSampleUploader.exe, SenseNdr.exe,

표 4. 종료 대상 서비스 및 프로세스

서비스와 프로세스를 종료한 이후에는 네트워크에 랜섬웨어를 전파한다. 이는 -ldap 인자를 사용해야 실행되며, 추가적으로 -host 인자를 사용해 특정 호스트에만 전파를 시도하거나 -sub 인자를 사용해 특정 서브넷 대역의 모든 호스트에 전파할 수 있다. 기존 Mamona 버전에서는 IPC$[6] 를 통해서 네트워크 연결을 시도하며, 이를 위해서 -u, -H, -p 인자에 각각 로그인 아이디와 인증용 NTLM 해시, 로그인 비밀번호를 입력받는다. -H 로 인증용 해시 값을 받지만 실제 NTLM 인증은 진행하지 않으며, -u 인자와 -p 인자를 통해서 로그인을 시도한다. 만약 접속이 가능하다면, 별도의 랜섬웨어 전파 없이 해당 네트워크 공유 자원에 있는 파일을 암호화하는 방식을 사용한다.

```
  if ( log_flag )
  {
    print_log_sub_402730(Format: L"attempting hash auth to %s with user %s", v10, v11 + 568);
    v13 = v11 + 1608;
  }
  if ( !auth_ntlm_sub_406570(v10, lpUserName: (v11 + 568), v13) )
  {
    if ( log_flag )
      print_log_sub_402730(Format: L"hash auth failed, trying password auth");
LABEL_20:
    lpUserName = (v11 + 568);
    if ( !*(v11 + 568) || (lpPassword = (v11 + 1088), !*lpPassword) )
    {
      lpPassword = 0;
      lpUserName = 0;
    }
    if ( WNetAddConnection2W(lpNetResource: &cp, lpPassword: lpPassword, lpUserName: lpUserName, dwFlags: 0) )
      return HeapFree_wrp(lpMem: *(v1 + 4));
    WNetCancelConnection2W(lpName: Name, dwFlags: 0, fForce: 1);
  }
  if ( log_flag )
    print_log_sub_402730(Format: L"found accessible host: %s", *(v1 + 4));
```

그림 10. Mamona 랜섬웨어의 네트워크 인증 방식

[6] IPC$: 네트워크를 통해 다른 컴퓨터에 접근하려 할 때, 인증을 수행하기 위한 제어용 공유 폴더

Devman 랜섬웨어에서는 IPC$를 통해 네트워크 암호화를 시도하는 것이 아니라, LDAP[7] 을 활용해서 랜섬웨어를 전파하는 방식을 사용한다. -u 인자로 전달받은 로그인 아이디가 id@domain 형태라면 여기서 도메인 정보를 추출해서 사용하며, 해당 도메인 정보를 기반으로 AD[8] 에 연결된 모든 호스트의 정보를 가져온다. 이후 각 호스트에 -u 인자의 아이디와 -p 인자의 비밀번호로 인증이 가능한지 확인한 후, 인증된 모든 호스트에 랜섬웨어를 전파한다.

```
vsprintf_sub_409070(NewFileName, 260, L"%s\\Temp\\cleanup.exe", Name);
NetResource.dwType = 1;
NetResource.dwScope = 0;
memset(&NetResource.dwDisplayType, 0, 12);
NetResource.lpComment = 0;
NetResource.lpProvider = 0;
NetResource.lpRemoteName = Name;
if ( log_flag )
  print_log_sub_409040("[+] Connecting to share: %ws\n", Name);
v6 = WNetAddConnection2W(lpNetResource: &NetResource, lpPassword: lpPassword, lpUserName: lpUserName, dwFlags: 0);
if ( v6 )
{
  if ( log_flag )
    print_log_sub_409040("[!] Failed to connect to share: %ws (Error: %d)\n", Name, v6);
  return 0;
}
if ( log_flag )
  print_log_sub_409040("[+] Connected to share, copying binary\n");
if ( CopyFileW(lpExistingFileName: Filename, lpNewFileName: NewFileName, bFailIfExists: 0) )
{
  TickCount = GetTickCount();
  vsprintf_sub_409070(sc_name, 32, L"Radio_%d", TickCount);
  vsprintf_sub_409070(
    CommandLine,
    520,
    L"sc \\\\%s create %s binPath= \"%%windir%%\\Temp\\cleanup.exe %s\" start= demand",
```

그림 11. Devman 랜섬웨어 전파 및 실행

연결된 호스트의 임시 폴더에 cleanup.exe 파일명으로 랜섬웨어를 복제하며, 서비스로 등록하거나 작업 스케줄러로 랜섬웨어를 실행한다. 또한, 같은 네트워크에서 전파가 여러 번 시도되는 것을 방지하기 위해 원격 호스트에서는 -skip-net 인자를 추가하여 랜섬웨어를 실행한다. 사용하는 명령어는 아래 표와 같다.

명령어	설명
sc \\{host_ip} create Radio_[0-9]{32} binPath= "%%windir%%\\Temp\\cleanup.exe -skip-net" start= demand	원격 호스트에 서비스 생성
sc \\{host_ip} start Radio_[0-9]{32}	서비스 실행
schtasks /create /s {host_ip} /u {username} /p {password} /tn "CoolTask" /tr "%%windir%%\Temp\cleanup.exe -skip-net" /sc once /st 00:00	작업 스케줄러 작업 생성
schtasks /run /s {host_ip} /u {username} /p {password} /tn	작업 스케줄러 작업 실행
schtasks /delete /s {host_ip} /u {username} /p {password} /tn	작업 스케줄러 작업 삭제

표 5. 종료 대상 서비스 및 프로세스

[7] LDAP: 네트워크 상에서 사용자, 그룹, 장비, 인증 정보 등의 데이터를 저장하고 조회 가능하게 하는 프로토콜

[8] AD (Active Directory): LDAP 기반의 Windows 통합 디렉터리 시스템으로 사용자와 컴퓨터를 일괄적으로 관리 가능

네트워크 전파 이후에는 현재 로컬 시스템 암호화를 진행한다. -skip-local 을 사용하면 네트워크 공유 폴더만 암호화하며, -skip-net 을 사용하면 로컬 디스크만 암호화한다. 또한 -path 인자를 사용하면 특정 디렉터리와 그 하위 디렉터리만 암호화한다. 암호화 대상을 설정했으면, 각 디렉터리를 순회해 예외 항목에 해당하는지 확인한다. Devman 버전의 예외 확장자에 .bin 이 추가된 것을 제외하고, 두 버전의 암호화 예외 대상이 동일하다. 확인하는 암호화 예외 대상은 아래 표와 같다.

폴더명	확장자 및 파일명
Windows, Program Files, Program Files (x86), AppData, ProgramData, All Users, NETLOGON, SYSVOL	PrintMe22.pdf, .exe, .dll, .msi, .sys, .ini, .ink, .bin

표 6. 암호화 예외 대상

파일 암호화 방식은 설정값에 따라 두가지 암호화 모드로 구분된다. 설정값에는 암호화 모드를 결정하는 값과, 부분 암호화 비율을 결정하는 두 개의 옵션이 존재한다. 첫 번째 방식은 크기가 큰 파일의 경우 앞부분 일부만 암호화하는 방식이다. 1MB 이하의 파일은 전체 암호화를 진행하며, 5MB 이하의 파일은 처음 1MB 만큼만 암호화한다. 5MB 보다 큰 파일은 공격자가 지정한 비율만큼 파일의 첫 부분을 암호화하는데, 그 크기가 최대 70MB 로 제한되어 있다.

그림 12. 크기 별 파일 암호화 방식 - 1

두 번째 방식은 크기가 큰 파일의 경우 일정 간격마다 암호화하는 방식이다. 64Bytes 이하의 파일은 전체 암호화를 하며, 5MB 이하의 파일은 전체 크기의 10%만큼만 암호화한다. 20MB 이하의 파일은 전체 크기의 1/6 만큼 구간을 나누어 각 구간의 첫 4KB 만 암호화하고, 20MB 보다 큰 파일은 10MB 마다 처음 4KB 를 암호화한다.

그림 13. 크기 별 파일 암호화 방식 - 2

두 암호화 방식 모두 동일한 알고리즘을 사용한다. 암호화 키는 Curve25519 를 통해서 생성한 공유 비밀을 이용한다. 각 파일마다 랜덤한 개인키를 하나 생성한 다음, 하드코딩된 Devman 의 공개키를 사용해 공유 비밀을 생성할 수 있다. 자신의 개인키와 상대방의 공개키로 만든 공유 비밀이 자신의 공개키와 상대방의 개인키로 만든 공유 비밀과 동일한 값을 가지는 Curve25519 의 특성을 이용한 것이다. 해당 공유 비밀을 SHA-512 알고리즘으로 해시를 생성해 해쉬의 뒷 32 바이트를 키로 이용해 HC-128 알고리즘으로 파일을 암호화한다. 파일의 끝에는 키 복구에 필요한 Curve25519 공개키를 함께 저장한다.

파일 암호화가 끝나면, 각 암호화 대상 경로에 랜섬노트를 생성한다. 만약 랜섬노트를 출력하는 옵션이 활성화되어 있다면, 랜섬노트 내용을 PDF 형태로 저장한 뒤, 이를 연결된 모든 프린터에 출력한다. 랜섬노트는 임시폴더에 PrintMe22.pdf 이름으로 저장된다.

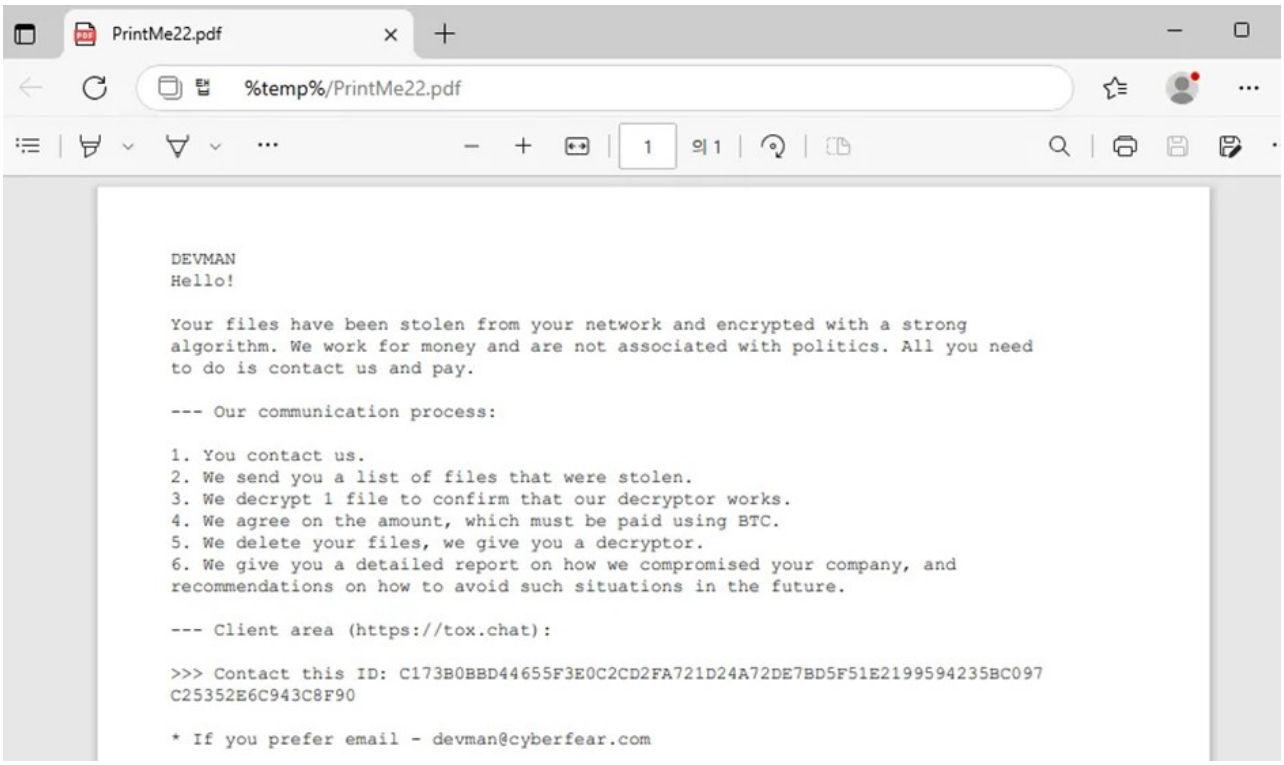

그림 14. 출력용 랜섬노트

그 외에도 암호화된 파일의 아이콘을 변경하기 위해 Base64 형태로 저장된 아이콘 이미지 파일을 임시폴더에 저장한 후, 레지스트리 설정 변경을 통해서 아이콘을 임의로 변경한다. 또한 “YOUR FILES HAVE BEEN ENCRYPTED! CHECK README.yAGRTb.txt” 라는 문구가 적힌 이미지로 배경화면을 변경한다.

그림 15. 변경된 배경화면

DragonForce 랜섬웨어 대응방안

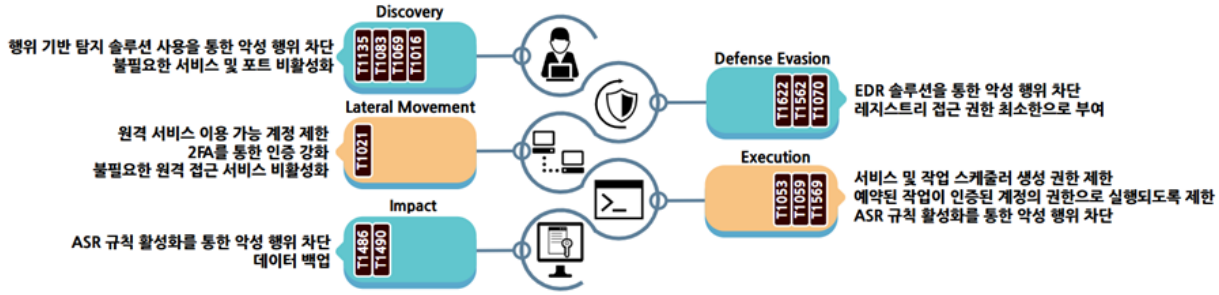

그림 16. Devman 랜섬웨어 대응방안

Devman 랜섬웨어는 파일 암호화 및 네트워크 전파를 위해서 네트워크 공유 폴더나 시스템이 속한 도메인 등 각종 정보를 활용한다. 따라서 행위 기반 탐지 솔루션을 사용해 악성 행위를 차단할 수 있으며, 불필요한 네트워크 서비스를 제거하거나 비활성화해 네트워크로 피해가 확산되지 않게 할 수 있다.

랜섬웨어의 악성 행위가 탐지되는 것을 회피하기 위해 Windows Defender 를 비활성화하며, 디버거를 분리하고 각종 이벤트 로그를 삭제한다. EDR[9] 솔루션을 사용해 Windows Defender 비활성화나 이벤트 로그 삭제와 같은 악성 행위를 차단할 수 있다. 특히 이벤트 로그 삭제의 경우 레지스트리에 접근이 필요한데, 레지스트리 접근 권한을 최소한으로 부여하면 공격자가 임의로 이벤트 로그를 삭제하지 못하게 할 수 있다.

또한 네트워크 환경으로 랜섬웨어를 전파하기 위해서 로그인 ID 와 비밀번호를 이용해 네트워크 환경에 접근을 시도한다. 별도의 ID 및 비밀번호 수집 과정은 확인되지 않았으나, 공격 준비 과정에서 계정 정보를 수집하거나 유출 혹은 취약한 계정을 악용할 수 있기 때문에 2FA[10] 를 이용해 인증을 강화해야 한다. 또한 원격 서비스를 이용할 수 있는 계정을 제한하거나 불필요한 원격 서비스 자체를 비활성화해 공격자가 네트워크 환경에 접근하지 못하도록 할 수 있다.

앞서 설명한 악성 행위는 대부분 Windows 명령 프롬프트를 활용하거나 작업 스케줄러 및 서비스 등록을 통해 이루어진다. 따라서 ASR[11] 규칙 활성화로 비정상적인 프로세스를 차단해 악성 행위를 막을 수 있다. 또한 랜섬웨어에 저장된 프로그램을 임시 폴더에 저장하거나 작업 등록을 위해 랜섬웨어를 특정 위치에 복제하기 때문에 Anti-Virus 를 활용하여 의심스러운 파일 격리도 가능하다. 그 외에도 서비스 및 작업 스케줄러의 생성 권한을 제한하여 복제된 랜섬웨어가 원격으로 실행되지 않도록 제한해야 하며, 예약된 작업이 실행되더라도 인증된 계정의 권한으로 실행되도록 설정하여 피해를 최소화할 수 있다.

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

[10] 2FA (2-factor Authentication): ID/PW 인증 외에도 휴대전화나 OTP 등을 활용한 추가 인증 수단으로 인증하는 방식

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

암호화된 파일을 사용자가 임의로 복구하는 것을 방지하기 위해서는 시스템에 존재하는 모든 백업 복사본을 삭제한 뒤 파일을 암호화한다. ASR 규칙 활성화를 통해서 백업 복사본을 삭제하는 프로세스와 파일을 암호화는 것을 차단할 수 있다. 뿐만 아니라 백업 복사본을 별도의 네트워크나 저장소에 소산 백업하여, 시스템이 암호화되더라도 복구할 수 있도록 조치해야 한다.

IoCs

Hash(SHA-256)
1f6640102f6472523830d69630def669dc3433bbb1c0e6183458bd792d420f8e
c5f49c0f566a114b529138f8bd222865c9fa9fa95f96ec1ded50700764a1d4e7

■ 참고 사이트

• GMA Network (https://www.gmanetwork.com/news/topstories/nation/945481/gma-network-statement-on-cybersecurity-incident)

• RELIAQUEST (https://reliaquest.com/blog/threat-spotlight-reliaquest-uncovers-vulnerability-behind-sap-netweaver-compromise/)