Keep up with Ransomware

피해자별 협상 채널 구축하는 DireWolf 랜섬웨어

■ 개요

2025 년 6 월 랜섬웨어 피해 사례 수는 지난 5 월(484 건)에 비해 소폭 증가한 505 건을 기록했다. 4 월 이후, 대형 랜섬웨어 그룹들의 해킹 피해와 활동 중단 사례가 잇따르고 있다. 이에 반해 한두 달간 짧게 활동하는 신규 랜섬웨어 그룹의 비중이 증가하는 추세다. 지속적인 법 집행 기관의 단속과, 피해 기업들의 몸값 지불 거부 등으로 장기 활동에 대한 부담이 커진 것으로 보인다. 따라서 랜섬웨어 그룹들은 서비스 형태의 랜섬웨어를 활용해 단기간에 집중적으로 활동하거나, 하나의 조직이 여러 랜섬웨어 프로젝트를 진행하는 경우, 그리고 리브랜딩을 통해 수시로 정체를 바꾸는 경향이 뚜렷해지고 있다.

이러한 흐름을 뒷받침하는 한 예로, Hunters 그룹이 7 월 초 공식적으로 랜섬웨어 활동 중단 선언을 했다. 7 월 3 일, 자신들의 다크웹 유출 사이트의 공지사항으로 "Hunters International 프로젝트를 종료하기로 결정했습니다." 라는 내용을 전달하며, 자신들의 행동이 미치는 영향을 잘 알고 있고 선의의 표시로 복호화 도구를 무료로 배포하겠다고 발표했다. 하지만 복호화 도구는 아직 공개되지 않았으며, 다크웹 유출 사이트에 모든 피해 기업 및 유출 데이터만 내려간 상태이다. 이들의 프로젝트 종료 움직임은 지난 24 년 11 월부터 있었다. Hunters 를 이용하는 제휴사의 패널에 랜섬웨어 프로젝트는 위험성이 높으나 수익성은 점점 낮아지고 있어 랜섬웨어 프로젝트를 종료할 것이라는 글을 업로드 했으며, 지난 1 월에는 데이터 탈취 만을 목적으로 하는 신규 프로젝트 World Leaks 를 내부적으로 공개하기도 했다. 이후 지난 5 월부터 World Leaks 활동을 시작했으며, 7 월에는 Hunters 프로젝트를 공식적으로 종료했다.

사이버 범죄 인프라 전반에서도 유의미한 변화가 이어지고 있다. 대표적인 해킹 포럼 중 하나인 BreachForums 의 주요 운영진들이 지난 2 월과 6 월에 프랑스 사이버 범죄 수사 부서(BL2C)에 체포되며, 포럼이 잠정 폐쇄된 것으로 확인됐다. 해킹 포럼 RaidForums(15 년 개설)을 대체하기 위해 2022 년에 만들어진 BreachForums 는 설립 이후에도 지속적으로 법 집행 기관의 감시를 받아왔다. 23 년에는 운영자 pompompurin 이 FBI 에 체포되어 사이트가 압수되었으며, 이어 24 년에 운영자 Baphomet 이 체포되면서 다시 폐쇄된 바 있다. 이후 포럼은 25 년 4 월에 다시 한번 폐쇄됐는데, 당시 운영진은 BreachForums 에서 사용하는 오픈 소스 포럼 소프트웨어 MyBB 의 제로데이 취약점을 통해 법 집행 기관이 접근할 수 있어, 포럼을 임시로 비활성화 한다고 설명했다. 발표에 따르면, BL2C 는 올해 2 월 주요 관계자 중 한명인 IntelBroker 를 체포했으며, 6 월에는 ShinyHunters, Hollow, Noct, Depressed 등 핵심 인물 4 명을 추가로 검거했다. 이 일련의 체포로 포럼 운영에 타격을 입으면서 BreachForums 는 현재까지도 운영되지 않고 있다. 다른 운영자들은 7 월에 BreachForums 복구를 예고했지만, 현재까지 공식적으로 복구된 사이트는 확인되지 않고 있다.

기존 그룹들의 활동 중단과 사이버 범죄자들의 체포 소식이 이어지는 가운데, 파트너를 모집하며 활동을 준비하는 그룹들도 확인됐다. 4 월에 RaLord 라는 이름으로 등장 후 5 월에 리브랜딩한 Nova 그룹이 6 월에는 RAMP 포럼에 홍보글을 업로드하며 활동에 박차를 가하고 있다. 기존에 자신들의 다크웹 유출 사이트에서 홍보하던 제휴 서비스는 물론이고, 랜섬웨어 기능을 상세하게 소개하며 랜섬웨어 서비스를 이용할 파트너를 모집하고 있다. 21 년부터 활동하고 있던 Chaos 그룹도 본격적으로 홍보를 시작했다. 이들은 별도의 다크웹 유출 사이트가 없이 활동하다가 25 년 4 월부터 다크웹 유출사이트도 운영하기 시작했으며, 6 월에는 RAMP 포럼에 홍보글을 게시하며 함께 일할 인원을 모집하고 있다. 그 외에도 6 월에 새로 등장한 WarLock 그룹도 RAMP 포럼에 새로운 파트너를 모집하는 글을 게시했으나, 현재 다크웹 유출 사이트에 접속이 불가능한 상태이다.

올해 상반기 기준 Clop 에 이어 다크웹에 두번째로 많은 피해자를 게시한 Qilin 그룹(333 건)이 5-6 월에 진행한 랜섬웨어 공격에 보안업체 Fortinet 의 보안 장비의 운영체제(FortiOS)의 취약점을 악용한 것으로 확인됐다. 공격에 사용된 취약점은 원격 코드 실행 취약점인 CVE-2024-21762 와 인증 우회 취약점 CVE-2024-55591 로, 두 취약점 모두 이미 패치가 배포된 상태다. 그러나 Qilin 은 여전히 패치되지 않은 취약한 시스템을 노리며 공격을 수행하고 있다. 이처럼 공격자들은 보안 업데이트가 적용되지 않은 취약한 시스템을 주요 표적으로 삼기 때문에, 소프트웨어와 보안 장비의 정기적인 패치 적용이 필수적이다

■ 랜섬웨어 뉴스

Hunters International, 랜섬웨어 프로젝트 종료

- 7월 3일 자신들의 DLS를 통해 랜섬웨어 활동을 종료한다고 공식적으로 발표
- 피해 기업과 모든 데이터는 DLS에서 더 이상 접근 불가능하며, 피해 기업에게 무료로 복호화 도구 배포 예정
- 내부적으로는 지난 1월부터 랜섬웨어 프로젝트 대신 데이터 탈취 프로젝트로 전환을 준비
- 해당 프로젝트는 5월에 등장한 World Leaks

BreachForums 주요 관계자 체포 및 운영 중단

- 지난 2월 프랑스 사이버 범죄 수사 부서(BL2C)에 의해 IntelBroker 체포
- 6월에는 ShinyHunters, Hollow, Noct, Depressed 등 핵심 인물 4명 추가로 체포
- BreachForums는 지난 4월 MyBB 취약점으로 법 집행 기관이 접근할 수 있다며 사이트를 잠정 폐쇄
- 7월에 복구 예정이라 하였으나, 공식적으로 복구된 사이트는 확인되지 않음

Fortinet 취약점을 악용한 Qilin 그룹

- Qilin 그룹은 지난 5-6월 공격에 FortiOS의 취약점을 악용
- 사용한 취약점은 원격 코드 실행 취약점(CVE-2024-21762)과 인증 우회 취약점(CVE-2024-55591)
- 두 취약점 모두 패치가 배포됐지만, 아직 적용하지 않은 시스템을 표적으로 공격

신규 WarLock 그룹, DLS 소스코드에 한국어 발견

- 러시아 해킹 포럼 RAMP에 홍보글을 업로드하며 그룹 공개
- 공개 이전부터 피해자가 다수 게시된 것으로 보아, 6월 이전부터 활동한 것으로 추정
- 공개한 DLS에 한국어로 된 주석 발견


BlackLock과 Global 간의 연관성 확인
이전에 El Dorado, Mamona R.I.P를 운영한 BlackLock 그룹이 Global도 운영하는 것으로 추정
6월에 발견된 Global 그룹의 랜섬노트에 BlackLock DLS 포함
BlackLock의 운영자 $$$가 RAMP 포럼에 Global 홍보글 게시
다양한 신규 그룹의 등장
Akira의 DLS에 사용된 문구, 색상, 기능을 모방한 Kawa4096 그룹
협상중이거나 기한을 넘기지 않은 피해자명을 필터링해 업로드하는 W.A. 그룹
그 외 TeamXXX, Nemesis 그룹도 새롭게 등장

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

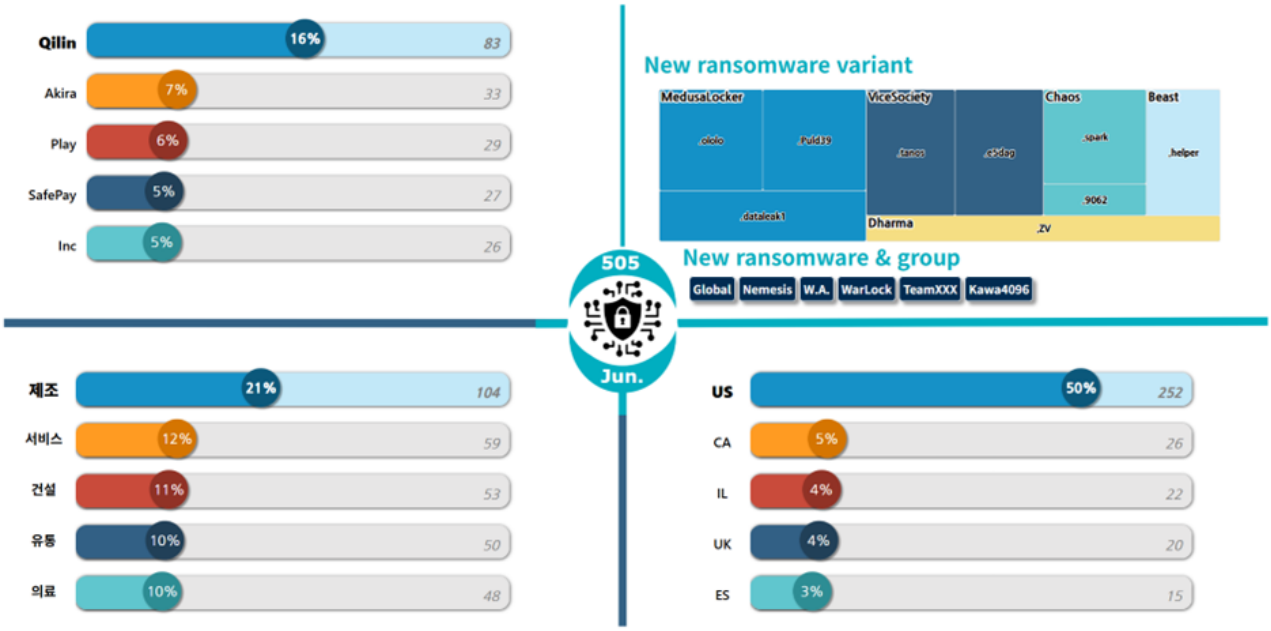

그림 2. 2025 년 6 월 랜섬웨어 위협 현황

새로운 위협

6 월에는 총 5 개의 신규 랜섬웨어 그룹이 등장했으며, 1 개의 그룹이 리브랜딩 후 활동을 재개했다. 신규 그룹 TeamXXX 는 6 월에 피해자 8 건을 게시했으며, 신규 그룹 W.A. 는 4 건을 게시했다. 특히 W.A. 그룹은 협상을 진행중이거나 아직 비용 지불 기한을 넘기지 않은 피해 기업의 이름을 필터링해 업로드하며, 협상에 실패하거나 기한을 넘기면 데이터와 기업명을 공개하는 모습을 보인다.

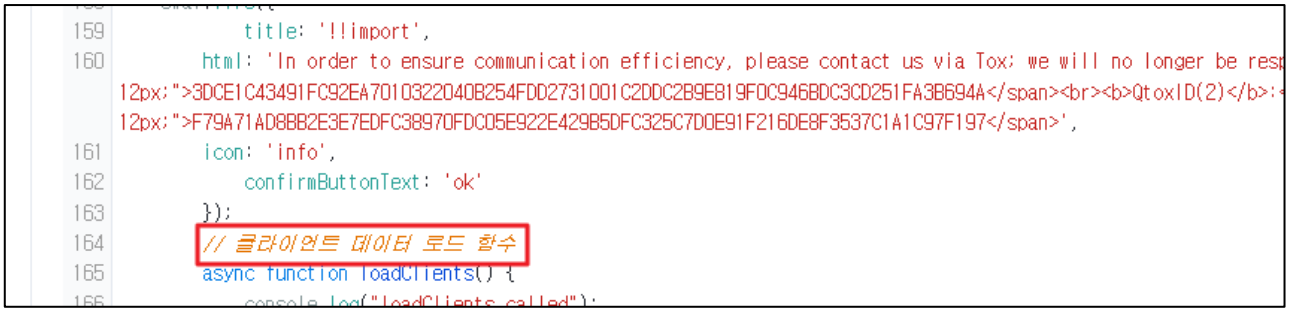

그림 3. WarLock DLS 페이지 소스코드

신규 그룹 WarLock 은 운영자로 추정되는 유저 cnkjasdfgd 가 러시아 해킹 포럼 RAMP 에 홍보글을 업로드하며 발견됐다. 이미 다크웹 유출 사이트에는 여러 피해자가 게시되어 있어 실제 활동을 6 월 이전부터 했을 것으로 추정된다. 또한 다크웹 유출 사이트 소스코드에 한국어로 된 주석이 달려있었으나, 현재는 폐쇄되어 접근이 불가능한 상태이다.

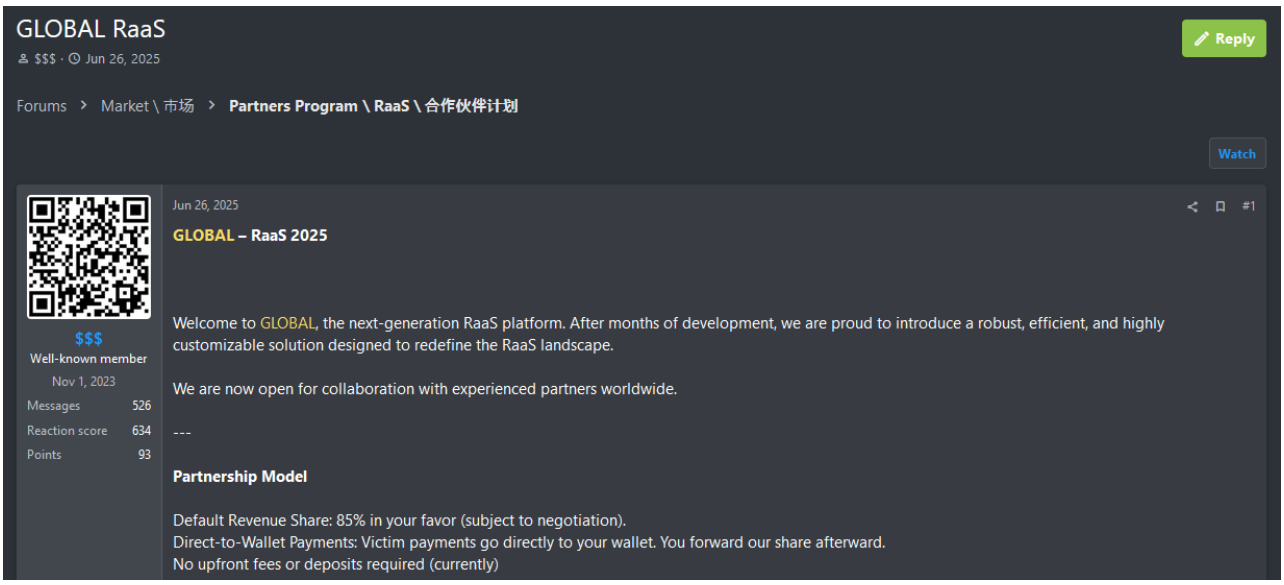

그림 4. Global RaaS 홍보글

신규 Global 그룹은 BlackLock 과 연관이 있는 것으로 확인됐다. 우선 6 월 초, BlackLock 의 또 다른 프로젝트였던 Mamona 랜섬웨어와 거의 동일한 버전의 Global 랜섬웨어가 발견됐다. 해당 랜섬웨어의 랜섬노트에 따르면 자신들을 Global 이라고 지칭하고 있지만, 랜섬노트에는 BlackLock 의 다크웹 유출 사이트 주소가 기재되어 있었다. 또한 협상 채팅에서는 Global 그룹의 다크웹 유출 사이트에서 피해 사실을 확인할 수 있다고 언급했다. 비슷한 시기에 BlackLock 의 운영진 $$$ 는 RAMP 에 작성했던 BlackLock 홍보 글과 프로필에서 BlackLock 대신 Global BlackLock 으로 명칭을 변경했으며, 6 월 말에는 $$$ 가 Global RaaS 를 직접 홍보하는 글을 업로드 하며 BlackLock 과 Global 의 연관성이 확인됐다.

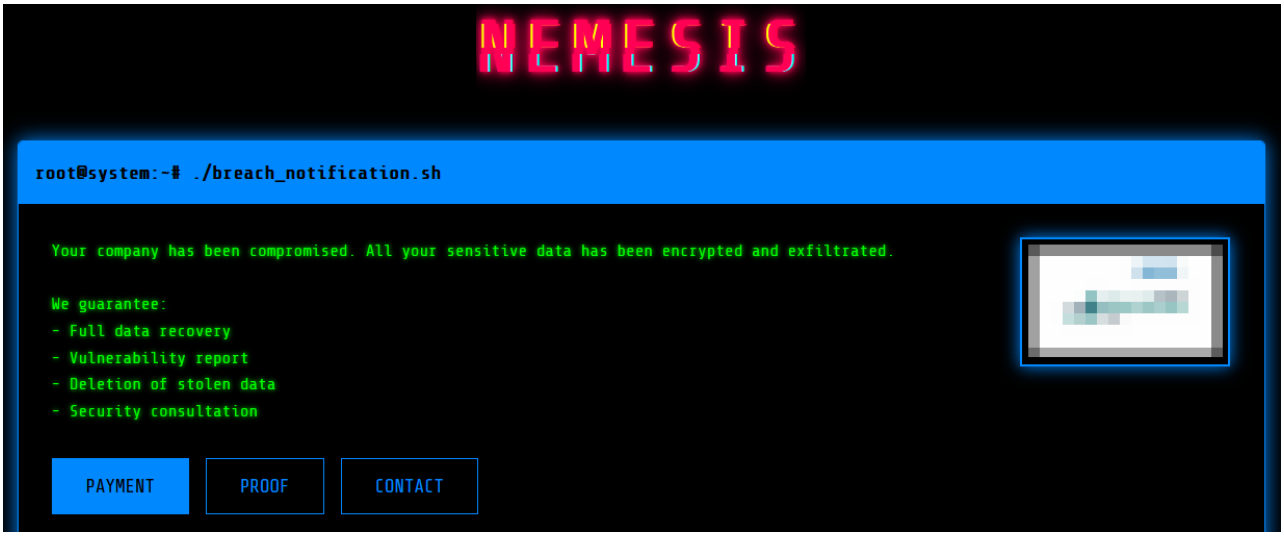

그림 5. Nemesis 협상 페이지

Nemesis 그룹은 탈취한 데이터를 공개하는 페이지는 아직 확인되지 않았다. 협상을 위한 채팅 페이지만 존재하거나, 피해자 및 유출 데이터를 한 곳에 모아 볼 수 있는 페이지가 있는 다른 그룹과는 달리, 랜섬노트에 피해자별로 별도의 토큰이 추가된 다크웹 페이지로 유도하고 있다. 이후 자신들이 탈취한 데이터의 샘플을 보여주고, 원하는 금액과 협상을 위한 메신저 ID 를 제공해 협상을 진행하고 있다.

그림 6. 다크웹 유출 사이트(상: Akira, 하: Kawa4096)

신규 Kawa4096 그룹의 다크웹 유출 사이트는 Akira 그룹의 다크웹 유출 사이트와 매우 유사한 디자인을 가지고 있다. 사용된 문구와 컬러는 물론이고, 콘솔 창처럼 보이는 디자인에 명령어를 직접 입력해야 다른 데이터에 접근할 수 있는 방식 등 많은 부분에서 유사점을 보이고 있다. 다만, 그룹 간에 직접적인 관계나 연관성이 없더라도 다크웹 유출 사이트의 디자인이나 문구 등을 모방하는 사례는 드물지 않기 때문에 두 그룹간의 관계를 더 지켜볼 필요가 있다.

Top5 랜섬웨어

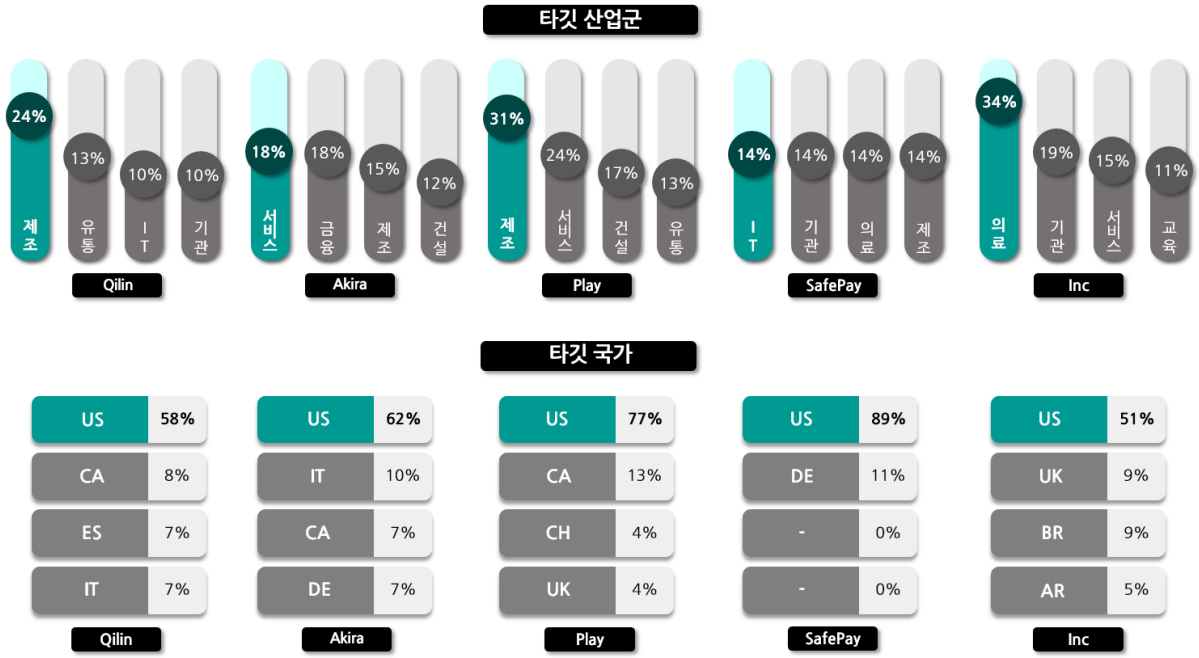

그림 7. 산업/국가별 주요 랜섬웨어 공격 현황

Qilin 그룹은 6 월 24 일 미국의 의료기관 Covenant Health 를 공격해 내부 문서를 유출했다. 유출된 자료에는 환자 의료 정보, 계약서, 세금 문서, 직원을 식별할 수 있는 파일 등이 포함됐다. 또한 6 월 23 일 미국 물류업체 Estes Forwarding Worldwide 가 공격당했으며, 여권 스캔본, 운전면허증, 직원 정보 스프레드시트 등이 샘플로 다크웹에 게시됐다. 영국의 스프링 제조업체 Airedale Springs Ltd.도 6 월 말 공격을 받아 내부 운영 문서, 공급망 관련 문서가 일부 유출됐다.

Akira 그룹은 6 월 초 미국의 사교 클럽 Sleepy Hollow Country Club 을 공격해 약 14GB 가량의 내부 데이터를 탈취했다. 이들은 6 월 말 모든 데이터를 공개했으며, 데이터에는 직원의 여권, 주민번호와 같은 개인정보는 물론 계약서, 재무제표 등이 포함되어 있다. 또한 아웃소싱 기업 Datrose 를 공격해 약 5GB 의 데이터를 탈취했다. 여기에는 이메일, 주소 등이 포함된 개인정보와 비밀 유지 계약서, 재무제표 등이 포함된 것으로 확인됐다.

Play 그룹은 미국 펜실베이니아의 운송업체 S&H Express 를 공격해 데이터를 탈취했다. 유출된 샘플에는 계약서, 고용 관련 문서, 세금 파일, 운전면허증 사본 등이 포함되었다. 또한 6 월 27 일 캐나다의 통신 장비 유통 기업 Cartel Communication Systems 도 공격을 받아 고객 명단, 내부 프로젝트 문서, 공급사 계약서, 일부 기술 문서가 다크웹에 게시됐다.

SafePay 그룹은 미국 오하이오주 Liberty Township 교육청을 공격해 일부 내부 재무자료, 운영 문서, 교직원 관련 문서가 포함된 48GB 의 데이터를 탈취했다. 또한 독일의 IT 서비스업체 MCSL GmbH 도 공격을 받아 고객 보고서, 프로젝트 문서, 내부 커뮤니케이션 파일이 유출되었으며, 미국의 차고 문 제조업체 The Overhead Door Company 역시 공격을 당해 기술 문서, 회계 기록, 고용 계약서 등이 포함된 내부 자료가 노출됐다.

Inc 그룹은 독일의 통신기기 제조업체 funktel GmbH 의 3.5TB 가량의 데이터를 탈취했다고 주장하며, 주요 제품의 설계도, 내부 메일, 급여 명세서, 운영 계획서 등 다양한 문서를 샘플로 공개됐다. 또한 미국의 의료 업체 Medical Center of Marin 을 공격해 환자 개인정보가 포함된 설문지나 의료 소견서, 환자의 신분증 등 환자의 정보가 유출됐다.

■ 랜섬웨어 집중 포커스

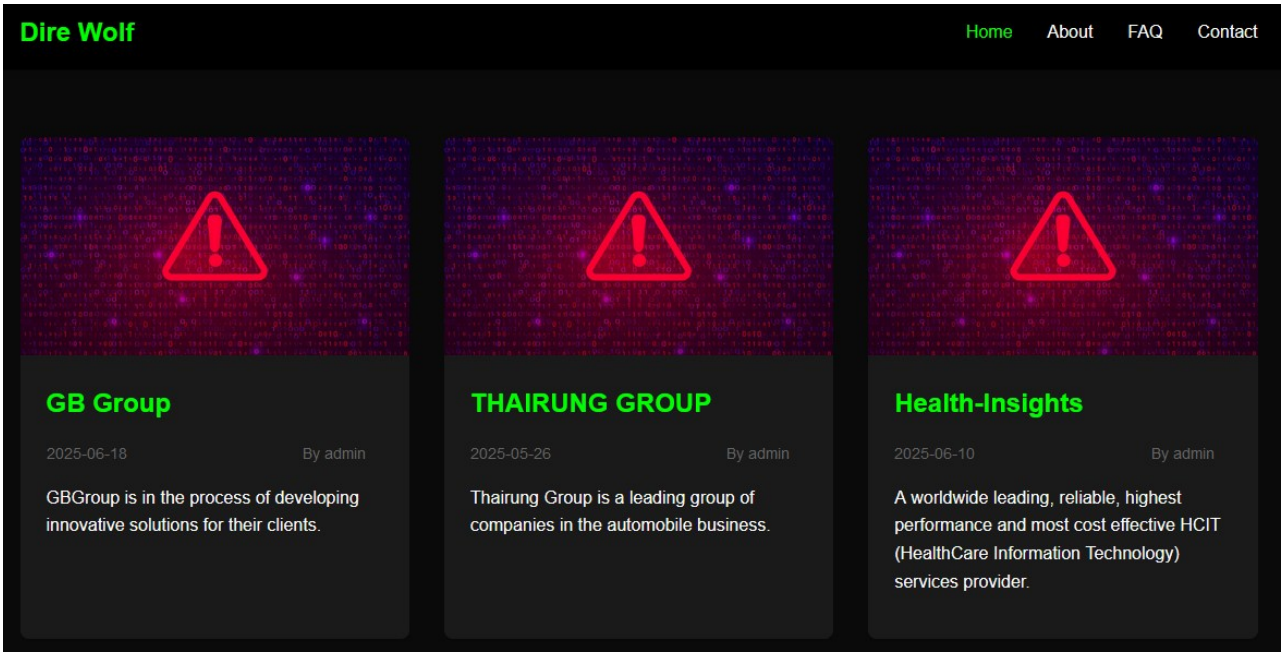

그림 8. DireWolf 다크웹 유출 사이트

25 년 5 월부터 활동을 시작한 DireWolf 그룹은 지금까지 총 16 건의 피해자를 게시했다. 각 피해자 마다 어떤 파일을 탈취했는지, 언제 업로드 했는지를 기록한 뒤, 협상에 실패하거나 일정 기간이 지나면 모든 사용자가 접근할 수 있도록 다크웹에 게시하고 있다.

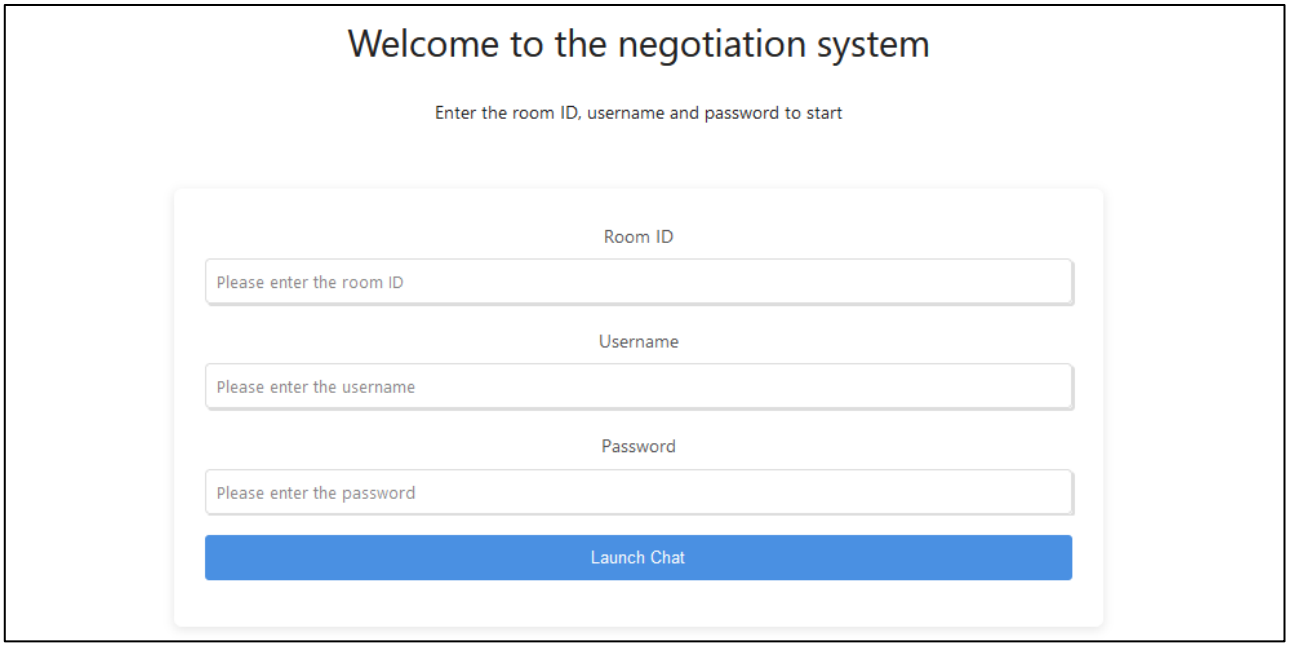

그림 9. DireWolf 다크웹 협상 페이지

랜섬노트에는 위 다크웹 유출 사이트 주소는 물론, 협상을 진행할 다크웹 채팅 사이트 주소와, 접속에 필요한 Room ID, Username, Password 를 함께 제공한다. 또한 자신들이 데이터를 탈취했음을 증명하기 위한 샘플 데이터를 다크웹에 업로드하는 것이 아니라, 이를 압축해 클라우드 스토리지 GoFile에 업로드하고 그 링크를 랜섬노트에 첨부해 피해자만 확인할 수 있도록 한다.

샘플 데이터가 업로드된 클라우드 링크를 제공하는 점과, 협상 페이지에 접속하기 위한 정보를 전달하는 점으로 미루어 보아, 이들은 각 피해자 별로 일부 수정된 랜섬웨어를 배포하고 있을 확률이 높다. 단순히 랜섬노트 내용만 변경한 뒤 배포할 수 있으며, 그 외의 기능도 맞춤으로 수정해 배포하고 있을 수 있다. 현재는 1 개의 피해자를 대상으로 하는 랜섬웨어만 확인됐으며, 이를 분석한 내용을 공유해 앞서 다가올 랜섬웨어 위협에 쉽게 준비할 수 있도록 하고자 한다.

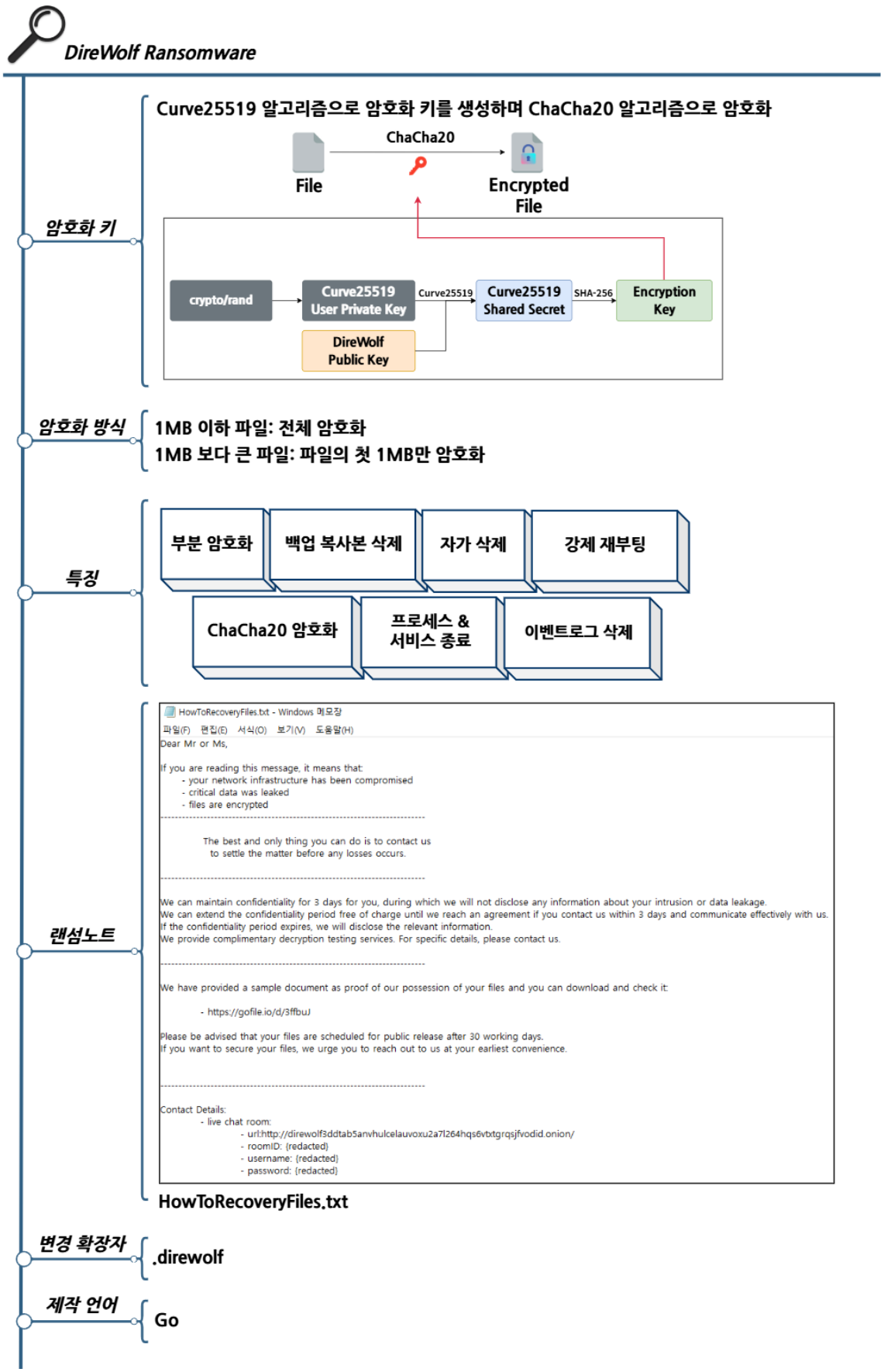

그림 10. DireWolf 랜섬웨어 개요

DireWolf 랜섬웨어 전략

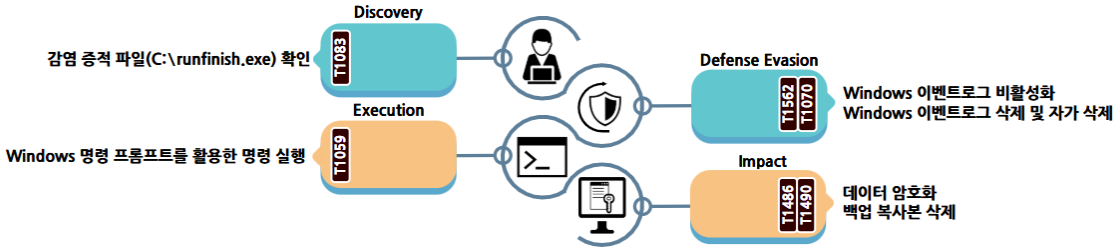

그림 11. DireWolf 랜섬웨어 공격 전략

DireWolf 는 별도의 설정 파일이 없으며, 2 개의 실행 인자를 사용해 기능을 제어할 수 있다. -h 인자를 사용해 실행 인자 설명을 볼 수 있으며, -d 인자를 사용해 특정 디렉터리만 암호화하도록 설정할 수 있다.

구분	설명
-h	실행 도움말 출력
-d <path>	특정 경로만 암호화

표 1. DireWolf 실행 인자

DireWolf 는 중복으로 실행되는 것을 방지하기 위해 뮤텍스[1] 를 활용한다. 랜섬웨어가 실행되면 “Global\direwolfAppMutex”라는 이름으로 뮤텍스를 생성하고, 이를 종료 직전에 해제한다. 만약 동일한 뮤텍스가 이미 생성되어 있다면 동일한 랜섬웨어가 이미 실행 중이므로 현재 프로세스를 종료해 중복 실행을 방지한다. 또한 DireWolf 랜섬웨어는 대상 시스템을 모두 암호화 한 뒤 C:\runfinish.exe 경로에 빈 파일을 생성하는데, 랜섬웨어 시작 시 해당 파일이 존재하는지 확인해 이미 암호화된 시스템을 중복으로 탐색하고 암호화하는 것을 차단한다. 만약 뮤텍스나 runfinish.exe 파일이 존재하는 경우, 랜섬웨어 종료는 물론 아래 명령어를 사용해 자가 삭제를 진행한다.

```
cmd /C timeout /T 3 & del /f /q <path> & exit
```

표 2. 자가 삭제 명령어

자가 삭제 외에도 복구 방지는 물론 분석 방해와 탐지 회피를 위해 각종 기록이나 흔적을 삭제한다. 실행중인 Windows 이벤트 로그 프로세스는 종료하고, Windows 환경의 기본 이벤트 로그를 삭제한다. 또한 명령 프롬프트를 활용해 백업 복사본 삭제는 물론 복구 환경 비활성화나 복구 모드 진입 방지도 함께 진행한다.

[1] 뮤텍스(Mutex): 여러 프로세스 혹은 스레드가 동일한 자원을 동시에 접근하지 못하도록 하는 보호 기법

명령어	설명
Get-WmiObject -Class win32_service -Filter "name = 'eventlog'" | select -exp ProcessId exp ProcessId	이벤트 로그 프로세스 ID 확인
Get-WmiObject -Class win32_service -Filter "name = 'eventlog'" | select -	이벤트 로그 프로세스 ID 확인
taskkill /f /pid <PID>	이벤트 로그 프로세스 종료
vssadmin delete shadows /all /quiet	복원 지점 제거
wmic shadowcopy delete /nointeractive	복원 지점 제거
wbadmin stop job -quiet	실행중인 백업 작업 중단
wbadmin disable backup -quiet	예약된 백업 작업 중단
wbadmin delete backup -keepVersions:0 -quiet	모든 백업 버전 삭제
wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:0 -quiet	시스템 상태 백업 삭제
wbadmin delete catalog -quiet	백업 메타데이터 삭제
bcdedit /set {default} recoveryenabled No	복구 환경(WinRE) 비활성화
bcdedit /set {default} bootstatuspolicy ignoreallfailures	복구 모드 진입 방지
wevtutil cl Application	Application 로그 삭제
wevtutil cl system	System 로그 삭제
wevtutil cl security	Security 로그 삭제
wevtutil cl setup	Setup 로그 삭제

표 3. 백업 및 이벤트 로그 삭제 명령어

원활한 파일 암호화를 위해 특정 프로세스와 서비스를 우선적으로 종료한다. 종료 대상 프로세스 및 서비스는 아래 표와 같다.

프로세스
wxServerView.exe, sqlmangr.exe, RAgui.exe, supervise.exe, Culture.exe, Defwatch.exe, httpd.exe, wsa_service.exe, synctime.exe, vxmon.exe, sqlbrowser.exe, memtas.exe, tomcat6.exe, Sqlservr.exe, agntsvc.exe, dbeng50.exe, dbsnmp.exe, dbsrv12.exe, encsvc.exe, excel.exe, firefox.exe, vss.exe, infopath.exe, isqlplussvc.exe, msaccess.exe, mspub.exe, mydesktopqos.exe, mydesktopservice.exe, ocautoupds.exe, ocomm.exe, ocssd.exe, onenote.exe, oracle.exe, outlook.exe, powerpnt.exe, sqbcoreservice.exe, sql.exe, steam.exe, tbirdconfig.exe, thebat.exe, thunderbird.exe, visio.exe, WinSAT.exe, winword.exe, wordpad.exe, onedrive.exe, wrapper.exe, xfssvccon.exe, sqlservr.exe, sqlagent.exe, sqlwriter.exe, MSExchangeIS.exe, MSExchangeTransport.exe, MSExchangeMailboxAssistants.exe, MSExchangeRepl.exe, MSExchangeRPC.exe, MSExchangeServiceHost.exe, notepad++.exe, notepad.exe

표 4. 종료 대상 프로세스

서비스
AcrSch2Svc, backup, BackupExecAgentAccelerator, BackupExecAgentBrowser, BackupExecDiveciMediaService, BackupExecJobEngine, BackupExecManagementService, BackupExecRPCService, BackupExecVSSProvider, CAARCUpdateSvc, CASAD2DWebSvc, ccEvtMgr, ccSetMgr, DefWatch, GxBlr, GxCIMgr, GxCVD, GxFWD, wuauserv, GxVss, Intuit.QuickBooks.FCS, memtas, mepocs, PDVFSService, QBCFMonitorService, QBFCService, QBIDPService, RTVscan, SavRoam, sophos, sql, stc_raw_agent, veeam, VeeamDeploymentService, VeeamNFSSvc, VeeamTransportSvc, VSNAPVSS, vss, YooBackup, YooIT, zhudongfangyu, SQLPBDMS, SQLPBENGINE, MSSQLFDLauncher, SQLSERVERAGENT, MSSQLServerOLAPService, SSASTELEMETRY, SQLBrowser, SQLServerDistributedReplayClient, SQLServerDistributedReplayController, MsDtsServer150, SSISTELEMETRY150, SSISScaleOutMaster150, SSISScaleOutWorker150, MSSQLLaunchpad, SQLWriter, SQLTELEMETRY, MSSQLSERVER, BackExecRPCService, bedbg, Culserver, dbeng8, MSExchange, msftesql-Exchange, msmdsrv, MSSQL, sqladhlp, SQLADHLP, sqlagent, SQLAgent, SQLAgent$SHAREPOINT, tomcat6, vmware-converter, vmware-usbarbitator64, WSBExchange

표 5. 종료 대상 서비스

대상 서비스와 프로세스를 종료한 이후에는 암호화를 진행한다. -d 인자를 사용하면 특정 디렉터리와 그 하위 디렉터리만 암호화하며, -d 인자를 사용하지 않으면 CD/ROM 을 제외한 연결된 모든 드라이브를 암호화한다. 암호화 대상을 설정했으면, 각 디렉터리를 순회해 예외 항목에 해당하는지 확인하고 랜섬노트를 생성한다. 확인하는 암호화 예외 대상은 아래 표와 같다.

폴더명	확장자 및 파일명
AppData, Boot, C:\Windows, SYSVOL, Tor Browser, Internet Explorer, Google, Opera, Opera Software, Mozilla, Mozilla Firefox, $Recycle.Bin, ProgramData, All Users, bootmgr, system volume information, inte, msocache, perflogs, ntldr, Program Files, Program Files (x86), #recycle, $windows.~bt, ntuser.dat, NTUSER.DAT	HowToRecoveryFiles.txt, .exe, .dll, .sys, .drv, .bin, .tmp, .iso, .img, .direwolf

표 6. 암호화 예외 대상

파일 암호화는 파일의 크기에 따라 전체 암호화와 부분 암호화로 구분한다. 1MB 이하의 파일은 전체 데이터를 암호화하고, 1MB 보다 큰 파일은 파일의 첫 1MB 만 암호화한다. 각 암호화 대상 마다 랜덤한 개인키를 생성하고, 하드코딩된 DireWolf 의 공개키를 사용해 Curve25519 공유 비밀을 만들어 암호화에 활용한다. 해당 공유 비밀은 SHA-256 해시 알고리즘으로 해싱되어 암호화 키로 사용된다. 이 키는 다시 SHA-256 으로 해싱되며, 해당 해시의 일부를 nonce[2] 로 활용하여 ChaCha20 알고리즘으로 파일을 암호화한다. 파일의 끝에는 키 복구에 필요한 Curve25519 공개키와 함께 6 바이트 크기의 임의의 데이터(0xAB 0xBC 0xCD 0xDE 0xEF 0xF0)를 함께 저장한다.

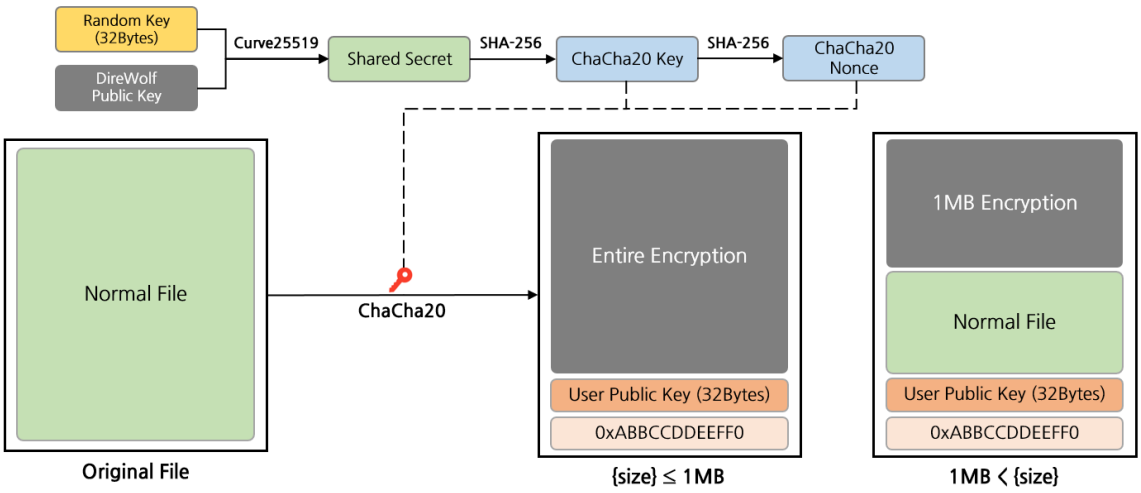

그림 12. 파일 암호화 방식

파일 암호화가 끝나면 C:\runfinish.exe 경로에 빈 파일을 생성하고 10 초 뒤 재부팅을 시도한다. 만약 재부팅에 실패하면 자가 삭제를 진행한 뒤 종료하고, 재부팅에 성공하면 자가 삭제는 진행되지 않는다. 사용하는 재부팅 명령어는 아래 표와 같다.

cmd /c start shutdown -r -f -t 10

표 7. 재부팅 명령어

[2] Nonce: 암호화에서 보안성과 고유성을 위해 사용되는 임의의 값

DireWolf 랜섬웨어 대응방안

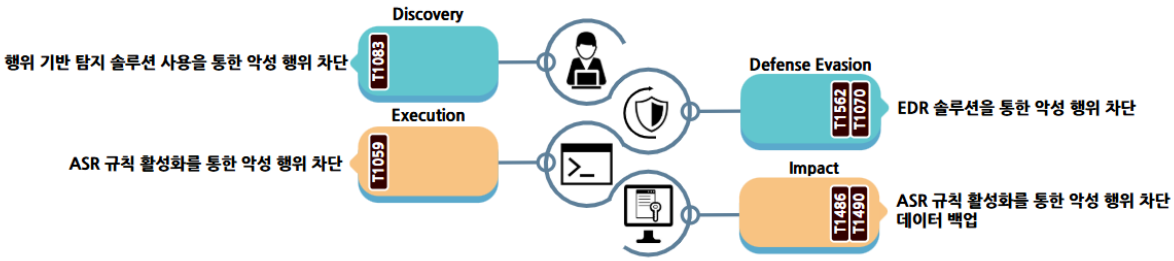

그림 13. DireWolf 랜섬웨어 대응방안

DireWolf 랜섬웨어는 중복 실행 방지를 위해서 실행 종료 시 runfinish.exe 라는 이름의 빈 파일을 생성하고, 실행 시에는 해당 파일이 시스템에 존재하는지 확인해 동일한 시스템을 중복으로 암호화하는 것을 방지하고 있다. 특정 경로의 파일을 검사하기 때문에 행위 기반 탐지 솔루션을 사용해 악성 행위를 탐지하고 차단할 수 있다.

악성 행위가 탐지되는 것을 회피하기 위해 이벤트 로그 프로세스를 중지하고 Windows 의 기본 이벤트 로그를 삭제한다. EDR[3] 솔루션을 사용해 특정 프로세스의 비활성화나 이벤트 로그 삭제와 같은 악성 행위를 차단할 수 있다. 또한, 분석 방지를 위해 자가 삭제 기능이 존재하는데, 이 역시도 EDR 솔루션을 사용해 악성 행위를 차단할 수 있다.

또한 앞서 설명한 DireWolf 랜섬웨어의 악성 행위는 Windows 명령 프롬프트를 활용해서 실행된다. 따라서 ASR[4] 규칙 활성화를 통해서 비정상적인 프로세스를 차단해 악성 행위를 막을 수 있다. 또한 암호화된 파일을 사용자가 임의로 복구하는 것을 방지하기 위해 총 9 개의 명령어를 활용해 시스템에 존재하는 모든 백업 복사본을 삭제하고, 복구 옵션을 비활성화한다. ASR 규칙 활성화로 파일 암호화는 물론 백업 복사본을 삭제하는 것을 차단할 수 있다. 또한, 백업 복사본을 별도의 네트워크나 저장소에 소산 백업하여, 시스템이 암호화되더라도 복구할 수 있도록 조치해야 한다.

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

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

IoCs

Hash(SHA-256)
8fdee53152ec985ffeeeda3d7a85852eb5c9902d2d480449421b4939b1904aad
27d90611f005db3a25a4211cf8f69fb46097c6c374905d7207b30e87d296e1b3
b6fa7a34b57803d2b80f3f484656d34997231597b6c1aa7fc8a386d6474c8afe

■ 참고 사이트

• Group-IB (https://www.group-ib.com/blog/hunters-international-ransomware-group/)

• LE Parisien (https://www.leparisien.fr/high-tech/la-police-interpelle-cinq-hackers-francais-de-haut-vol-derriere-un-celebre-forum-de-vol-de-donnees-25-06-2025-QJTPFTDPQZAP7B25MF24YLHU6E.php)

• BleepingComputer (https://www.bleepingcomputer.com/news/security/critical-fortinet-flaws-now-exploited-in-qilin-ransomware-attacks/)