Keep up with Ransomware

국내 금융권을 공격한 Gunra 랜섬웨어

■ 개요

2025 년 7 월 랜섬웨어 피해 사례 수는 지난 6 월(512 건)에 비해 하락한 483 건을 기록했다. 피해 건수는 다소 감소했지만, 공격의 정교함과 전략적 다양성은 오히려 강화되는 양상을 보였다. 특히, 취약점을 악용한 침투, AI 기반 협상 자동화 시도, 그리고 법 집행과의 직접적 충돌 사례 등은 7 월의 주요 특징으로 분석된다.

지난 4 월 등장한 Gunra 그룹이 국내 금융기관을 대상으로 공격을 감행한 정황도 확인됐다. 피해 기관은 7 월 14 일 랜섬웨어 공격으로 인해 서비스 제공에 일시적인 차질을 빚었으며, 약 4 일 만에 복구를 완료하고 서비스를 재개했다. 그러나 피해는 서비스 중단에 그치지 않고 데이터 유출로 확산됐다. 공격자는 다크웹 유출 사이트에 해당 기관의 데이터베이스를 탈취했다고 주장하며, 함께 분석할 인원을 모집하는 메시지를 게시했다. 유출된 데이터는 총 13.2TB 분량의 압축 파일로 확인되었으며, 공격자는 순차적 공개를 예고하며 피해 기관에 대한 압박 수위를 높이고 있다.

Akira 그룹은 다중 인증(MFA)[1]이 적용된 환경에서도 패치가 적용된 SonicWall SSL-VPN[2] 장비를 통해 침투한 것으로 보인다. 이로 인해, 제로데이(Zero-Day) 취약점 존재 가능성에 대한 우려가 제기되고 있다. 이는 취약점이 공식적으로 공개되거나 패치되기 전까지 방어가 어려운 고도화된 위협이 여전히 존재함을 시사한다. 또 다른 사례로는 Microsoft SharePoint 의 ToolShell 취약점(CVE-2025-53770)을 악용한 Warlock 랜섬웨어의 확산이 확인되었다. 해당 공격은 미국 내 핵안보청(NNSA), 국립보건원(NIH) 등 주요 정부기관을 포함한 약 400 여 대의 서버에 피해를 입혔다.

공격자들은 기술적인 정교함뿐 아니라 운영 전략 측면에서도 진화를 거듭하고 있다. Global 그룹은 피해 기업과의 협상 과정에 AI 챗봇을 도입하여 인터페이스를 자동화하고, 협상 속도를 높이려는 시도를 보였다. 이러한 움직임은 서비스형 랜섬웨어 RaaS[3] 생태계의 서비스화와 자동화 트렌드를 반영하는 대표적 사례로 분석된다.

[1] MFA(Multi-Factor Authentication): 사용자가 계정에 접근할 때 두 가지 이상의 서로 다른 인증 요소를 요구해 보안을 강화하는 인증 방식

[2] SSL-VPN(Secure Sockets Layer Virtual Private Network): 인터넷을 통해 암호화된 채널로 내부 네트워크에 원격 접속할 수 있도록 하는 장비

[3] RaaS (Ransomware-as-a-Service): 랜섬웨어를 서비스 형태로 제공해서 누구나 쉽게 랜섬웨어를 만들고 공격할 수 있도록 하는 비즈니스 모델

공격자 활동에 대응하기 위한 법 집행 기관의 움직임도 더욱 강화되는 양상이다. 미국 연방수사국(FBI)은 Chaos 랜섬웨어 그룹 구성원이 보유한 약 240 만 달러 상당의 비트코인을 압수하기 위한 법적 절차에 착수했으며, 7 월 25 일에는 FBI, 유로폴(Europol), 독일 및 네덜란드 경찰 등 국제 수사기관이 협력해 BlackSuit 랜섬웨어 그룹의 다크웹 유출 사이트를 압수하는 데 성공했다. 해당 그룹은 180 건 이상의 피해자를 사이트에 게시했으며, 총 요구 금액은 약 5 억 달러(한화 약 6,948 억 원)에 달하는 것으로 알려졌다.

한편, 법 집행의 제재에도 불구하고 활동을 재개한 집단도 확인됐다. 지난 2 월과 6 월, 프랑스 사이버범죄수사국(BL2C)이 주요 운영자 5 명을 체포하며 폐쇄됐던 해킹 포럼 BreachForums 는 7 월 26 일 복구됐다. 운영자 공지에 따르면, 체포된 인물들은 실질적 관리자 권한이 없었으며, 실제 운영진의 신원을 숨기기 위한 역할로 직함만 부여된 인물이었다고 주장했다. 또한 지난 4 월, 포럼 소프트웨어인 MyBB 의 취약점으로 인해 일시적으로 운영을 중단한 것은 사실이나, 해당 취약점은 이미 해결되었으며 기존 도메인은 법 집행 기관의 요청에 따라 폐쇄했다고 덧붙였다.

반면, 러시아 해킹 포럼 XSS 는 여전히 폐쇄된 상태를 유지하고 있다. 유로폴을 포함한 국제 법 집행 기관은 7 월, 우크라이나에서 해당 포럼의 운영자로 추정되는 인물을 체포했다. 체포된 인물은 약 20 년간 사이버 범죄 생태계에서 활동하며, 광고 및 중개 수수료를 통해 약 700 만 유로(한화 약 80 억 원)를 벌어들인 것으로 확인되었다. 해당 체포 이후, XSS 포럼은 복구되지 않은 상태다.

■ 랜섬웨어 뉴스

Gunra 그룹, 국내 금융기관 대상 랜섬웨어·데이터 유출 공격

- 지난 7월 14일, 국내 금융기관 랜섬웨어 공격으로 서비스 중단 발생
- 서비스 재개에도 불구하고 데이터베이스(13.2TB) 유출 발생
- 탈취 자료 분석 완료 및 공개 예고

Chaos 그룹 대상 암호화폐 자산 압수 및 범죄 수익 회수 절차 추진

- 미국 FBI는 Chaos 랜섬웨어 그룹이 보유한 약 240만 달러 상당의 비트코인 자산에 대해 압수를 위한 법적 절차에 착수
- 해당 암호화폐는 랜섬웨어 피해자 지갑에서 이체된 자금으로, 미국 법무부는 몰수 추진
- 범죄 수익을 직접 겨냥한 이번 조치는 인프라 차단을 넘어선 법 집행의 확장 사례로 주목됨

BlackSuit 그룹에 대한 인프라 차단 및 국제 공조 작전

- FBI, 유로폴, 독일 및 네덜란드 경찰 등 국제 수사기관은 공조 작전을 통해 BlackSuit 그룹의 다크웹 유출 사이트를 압수
- 인프라를 직접 차단한 이번 조치는 랜섬웨어 생태계에 실질적 타격을 가한 사례로 주목받음

BreachForums, 법 집행 압박 속 재등장

- 운영자 체포로 폐쇄됐던 해킹 포럼 BreachForums, 7월 26일 복귀
- 운영자는 체포된 인물들이 실제 관리자 권한을 가진 적이 없으며, 주목을 끌기 위해 직함만 부여했다고 주장.
- 보안 취약점 패치·도메인 교체 완료 후 운영 재개

법 집행으로 폐쇄된 해킹 포럼 XSS

- 유로폴 등 법 집행기관, 7월 XSS 포럼 운영자 우크라이나서 체포
- 운영자는 20년간 활동하며 약 700만 유로(약 80억 원) 수익 올린 것으로 추정
- 체포 작전 이후 XSS 포럼 폐쇄 상태 지속


Akira 그룹 SonicWall SSL VPN 침해
Akira 랜섬웨어가 최신 펌웨어가 적용된 SonicWall SSL VPN 장비를 통해 내부망에 침투한 사례가 발견
MFA 설정이 활성화된 환경에서도 접근이 이루어진 정황이 있어, 알려지지 않은 취약점의 존재 가능성이 제기됨
공식적인 취약점(CVE)은 아직 공개되지 않음
SharePoint 취약점을 악용한 Warlock 랜섬웨어 배포
Storm-2603 으로 추정되는 공격자의 SharePoint 취약점(CVE-2025-53700) 악용
해당 취약점으로 Warlock 랜섬웨어 유포, 약 400대 서버 피해 발생
Global 그룹 협상 자동화를 위한 AI 챗봇 도입 시도
협상 인터페이스에 AI 챗봇을 도입해 피해 기업과의 소통을 자동화하는 시도 진행
협상 과정 단축 및 응답 속도 향상을 통해 금전 갈취 효율성 극대화 시도

그림 1. 랜섬웨어 동향

■ 랜섬웨어 위협

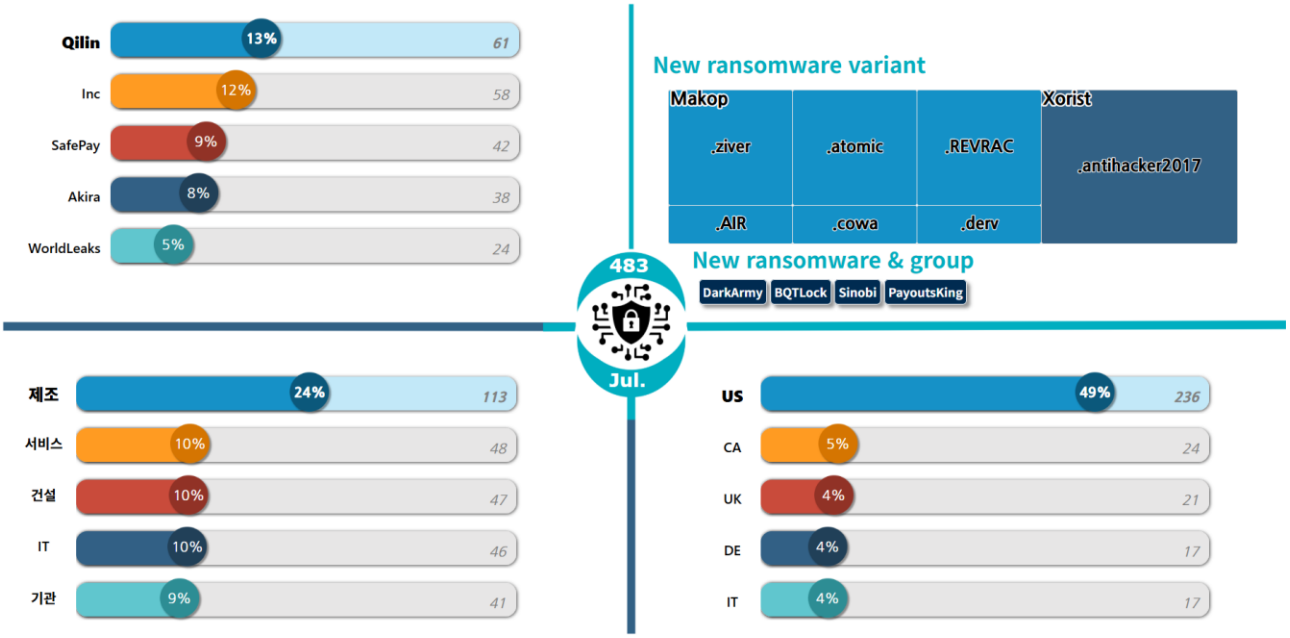

그림 2. 2025 년 7 월 랜섬웨어 위협 현황

새로운 위협

7 월 동안 총 483 건의 피해 사례가 확인됐으며, 이 기간 동안 신규 랜섬웨어 그룹 4 개가 새롭게 등장했다. 각 그룹은 자체 운영 중인 데이터 유출 사이트에 피해 사실을 게시했으며, 확인된 피해 규모는 DarkArmy 11 건, BQTLock 2 건, Sinobi 5 건, Payoutsking 18 건으로 집계됐다.

그림 3. DarkArmy 의 데이터 유출 사이트

DarkArmy 의 다크웹 데이터 유출 사이트 하단 배너에 睡觉的乌鸦(잠자는 까마귀)라는 중국어 표어와 연락 수단으로 QQ·위챗 계정이 병행 표기돼 있다. 종합적으로 추정하면, 개발·운영 주체가 중국어권일 가능성이 높다.

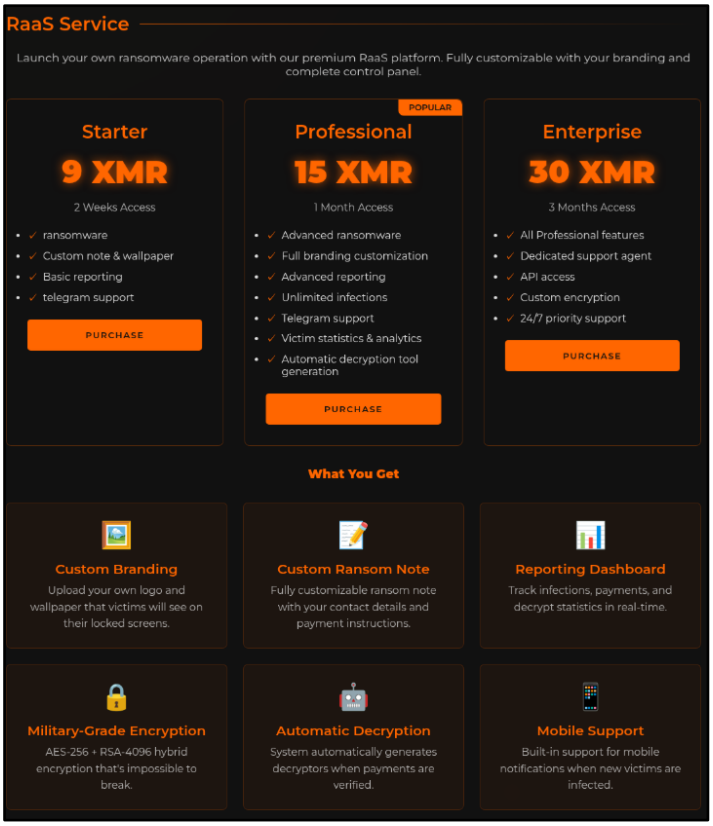

그림 4. BQTLock RaaS 대시보드

BQTLock 는 BQT RaaS 라는 자체 포털을 운영하며, 가입자에게 완전한 커스텀 빌더[4] 와 통계 대시보드를 제공한다. 포털에는 Starter, Professional, Enterprise 의 3 단계 요금제가 명시되어 있으며 각각 9XMR(한화 약 337 만원), 15XMR(한화 약 562 만원), 30XMR(한화 약 1,124 만원)의 비용을 요구한다. Professional 이상 구독 시 랜섬노트 브랜딩 커스터마이징, 피해자 통계·보고서, 자동 복호화 툴 생성 기능이 활성화된다. 이러한 원스톱 RaaS 플랫폼 구조는 비개발자 공격자까지 빠르게 랜섬웨어 캠페인을 구축·운영하도록 지원해 시장 확산을 가속화할 것으로 보인다.

[4] 빌더(builder): 공격자가 랜섬웨어의 암호화 방식, 몸값, 피해자 메시지, 타깃 경로 등 세부 옵션을 GUI 또는 명령형 인터페이스로 설정하고, 최종 실행 파일을 자동 생성해주는 도구

Top5 랜섬웨어

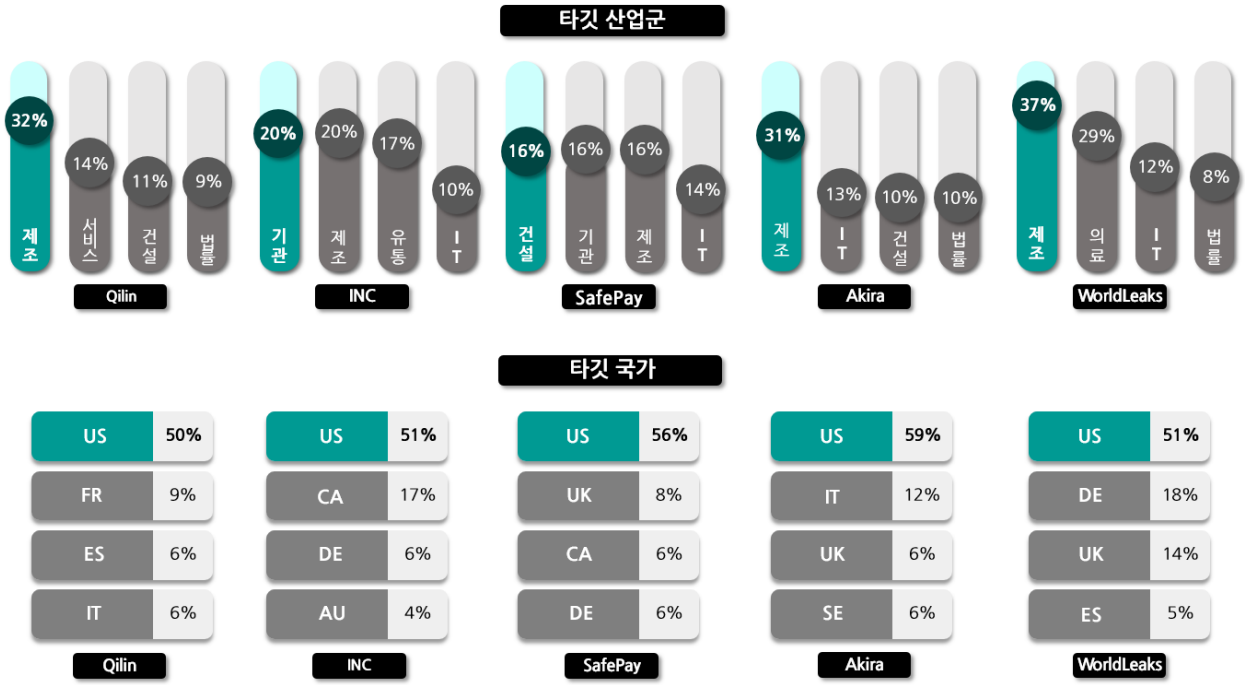

그림 5. 산업/국가별 주요 랜섬웨어 공격 현황

Qilin 그룹은 7 월 29 일 말레이시아의 식품 원료 제조업체 Custom Food Ingredients 를 공격해 핵심 제조 시스템에 침투하고 내부 데이터를 탈취했다고 주장했다. 이들은 다크웹 유출 사이트에 생산·운영 관련 문서 일부의 목록을 게시하며 피해 기업에 대한 압박 수위를 높였다.

Inc 그룹은 7 월 31 일 미국 웨스트 버지니아의 공공 의료기관 West Virginia Primary Care Association 에게 피해를 입혔다고 공개했다. 다크웹 유출 사이트에 피해 사실을 게시하고 연락을 요구했으며, 협상 불발 시 데이터를 공개하겠다고 경고했다. 또한 미국 버지니아주 Albemarle County 행정기관을 공격해 주민 및 직원의 이름, 주소, 사회보장번호(SSN), 운전면허번호 등 수천 건의 개인정보를 유출했다.

SafePay 그룹은 7 월 초 글로벌 IT 유통사 Ingram Micro 를 공격했다고 주장했다. 사건 직후 기업의 웹사이트와 주문 시스템이 일시 중단됐으며, 다크웹 유출 사이트에 피해 기업명을 등록하고 3.5TB 규모의 자료 공개를 예고했다. 이어 7 월 26 일에는 미국 피부과 병원 Southwest Florida Dermatology 를 공격해, 환자의 의료 기록을 포함한 민감한 내부 데이터를 유출했다고 밝혔다.

Akira 그룹은 7 월 25 일 미국 오클라호마시티에 위치한 지식재산 전문 로펌 Dunlap Codding 의 자료를 탈취했다고 주장했다. 다크웹 유출 사이트에는 고객 파일, 재무 자료, 특허 및 법원 관련 문서 등 약 19GB 규모의 자료 공개 예고문이 게시되었다. 또한 스페인의 온라인 뷰티 유통업체 Druni 역시 공격을 받아, 직원 신분증, 재무 기록, 고객 정보 등이 포함된 40GB 분량의 데이터가 유출되었다.

WorldLeaks 그룹은 7 월 21 일 미국의 엔지니어링 서비스 기업 Proactive Engineering Consultants 를 공격했다고 주장했다. 이후 다크웹 유출 사이트를 통해 피해 사실을 공개하고, 5.3TB 에 달하는 설계 및 프로젝트 관련 자료를 유출했다. 이어 미국 건설사 Thomas Bennett & Hunter 를 공격해 사내 프로젝트 및 운영 관련 데이터를 공개했다.

■ 랜섬웨어 집중 포커스

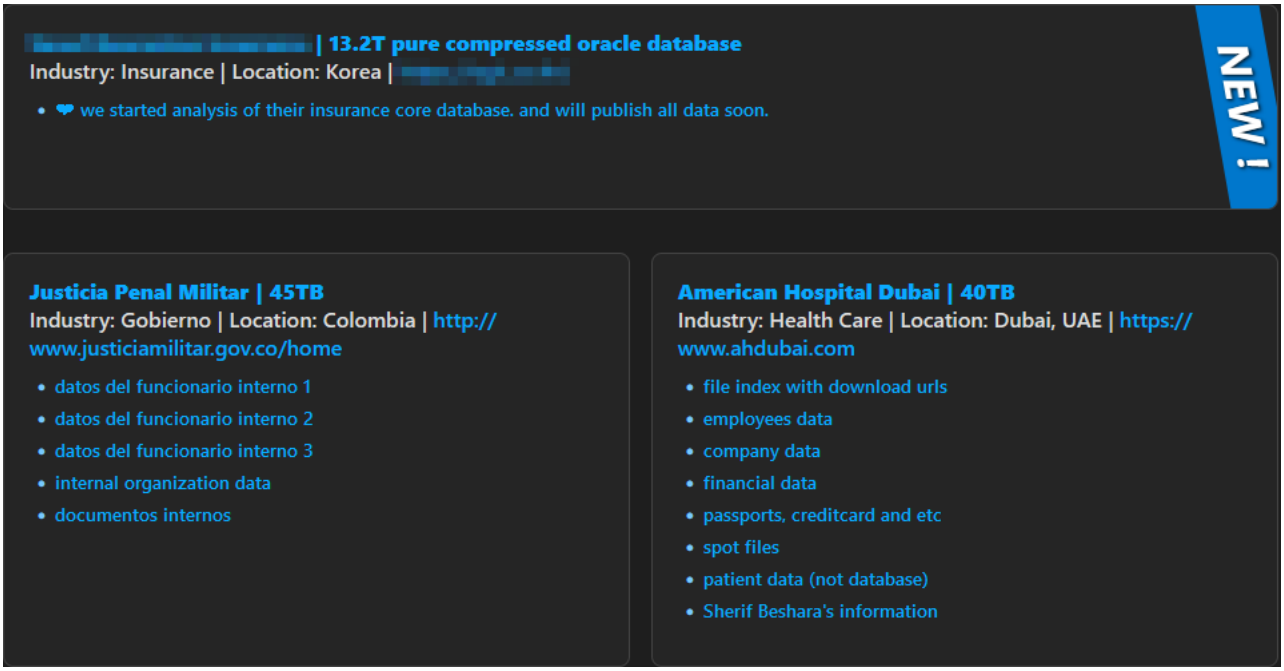

그림 6. Gunra 다크웹 유출 사이트

Gunra 랜섬웨어 그룹은 2025 년 4 월 처음 확인되었으며, 현재까지 총 16 건의 피해자를 전용 데이터 유출 사이트에 게시했다. 전용 사이트는 Tor 네트워크에서 운영되며, 피해자별 기업명·산업·국가와 함께 탈취한 데이터의 종류, 게시 일시, 협상 마감 시한을 명시한다. 이들은 피해자별로 탈취한 데이터의 종류와 게시 일시를 공개하고, 협상이 결렬되거나 정해진 기한이 지나면 해당 자료를 다크웹에 전면 공개하는 방식을 사용한다.

이들은 짧은 협상 기한 설정과 다중 익명 채널 활용이 특징이며, 랜섬노트에는 피해자가 5 일 이내에 연락해야 한다는 기한 강조 문구와 함께 Tox ID 와 메일 주소를 기재해 피해자와 접촉한다. 초기에는 일부 파일의 무료 복호화를 제안한 후, 응답이 없으면 유출 사이트에 피해자 정보를 게시한 뒤 탈취 자료 일부를 공개하며 압박 수위를 높인다. 협상이 장기화하면 추가 데이터를 공개하거나 자료 전체 유출을 경고하는 등 단계적으로 피해자를 위협한다. 게시된 피해자 중에는 2025 년 7 월 발생한 국내 금융권 기업도 포함되어 있으며, 피해 기업의 자료 공개를 예고하며 강도 높은 압박을 가했다.

현재까지 확인된 Gunra 랜섬웨어는 Windows 와 Linux 두 버전이 존재한다. Windows 버전은 암호화 후 디렉터리별로 랜섬 노트를 남기며, Linux 버전은 랜섬 노트를 생성하지 않고, 실행 인자로 지정된 경로와 확장자, 암호화 비율을 바탕으로 파일을 선별해 암호화한다. 두 버전 모두 파일 크기나 유형에 따라 전체 또는 부분 암호화를 적용해 효율성과 속도를 높이는 것이 특징이다. 본 보고서에서는 두 버전을 분석해, Gunra 의 활동 방식과 기술적 특징을 정리함으로써 랜섬웨어 위협에 효과적으로 대비할 수 있도록 하고자 한다.

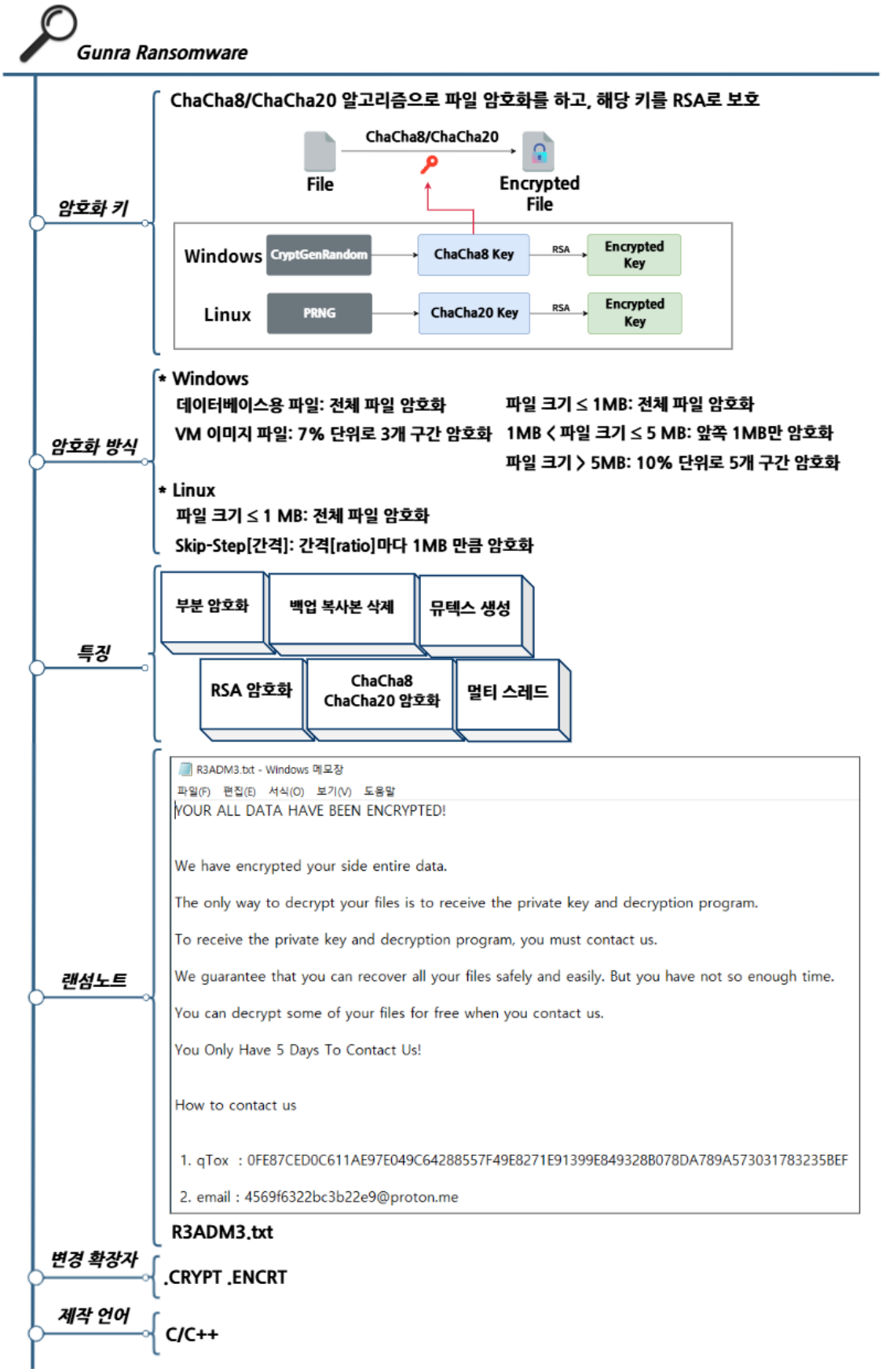

그림 7. Gunra 랜섬웨어 개요

Gunra 랜섬웨어 전략

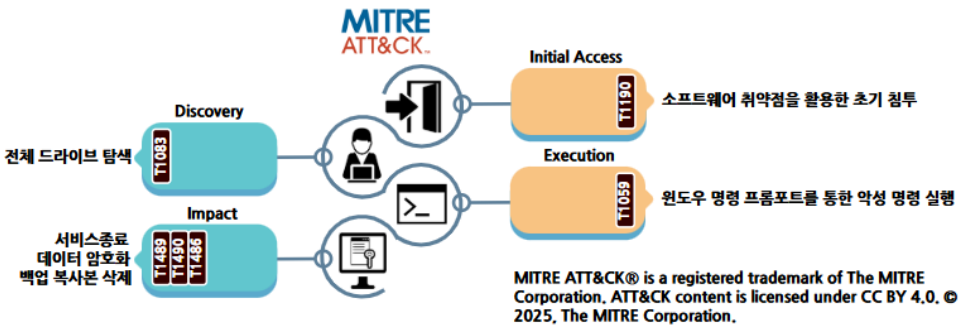

그림 8. Gunra 랜섬웨어 공격 전략

Gunra 랜섬웨어 (Linux 버전)

Gunra 랜섬웨어의 Linux 버전은 다양한 실행 인자를 통해 암호화 동작을 정밀하게 제어할 수 있도록 설계되어 있어, 공격자는 목표 파일의 위치, 확장자, 암호화 강도, 암호화 키 저장 방식 등을 유연하게 설정할 수 있다. Linux 버전의 인자와 기능은 아래 표와 같다.

구분	설명
--threads / -t	파일 암호화 스레드 개수 지정
--path / -p	암호화 대상 지정
--exts / -e	암호화 대상 파일의 확장자 지정(all: 모든 파일, disk: 블록 디바이스)
--ratio / -r	암호화 간격 설정 (MB)
--keyfile / -k	RSA 공개키 파일(.pem) 경로
--store / -s	암호화 키 저장 경로
--limit / -l	최대 암호화 크기 (GB, 0: 전체 파일 암호화)

표 1. Gunra 랜섬웨어 Linux 버전 실행 인자

Linux 버전의 경우 -p 인자를 통해 암호화 대상 파일 또는 경로를 지정한다. 함께 입력한 대상이 단일 파일일 경우 해당 파일에 대해서 암호화를 수행하며, 디렉터리일 경우 해당 디렉터리와 하위 디렉터리를 탐색해 암호화 대상 파일을 암호화한다.

-e 옵션은 암호화 대상 파일의 확장자를 지정하며, 이 옵션이 없거나 'all'로 설정된 경우 파일 내부에 명시된 예외 확장자를 제외한 모든 파일이 암호화 대상이 된다. 또한 'disk'로 설정된 경우 시스템에 존재하는 블록 디바이스 파일만 암호화한다. 암호화 예외 대상 파일 확장자에는 이미 암호화 완료된 파일의 확장자인 .ENCRT 와 랜섬 노트 파일인 R3ADM3.txt 가 포함된다.

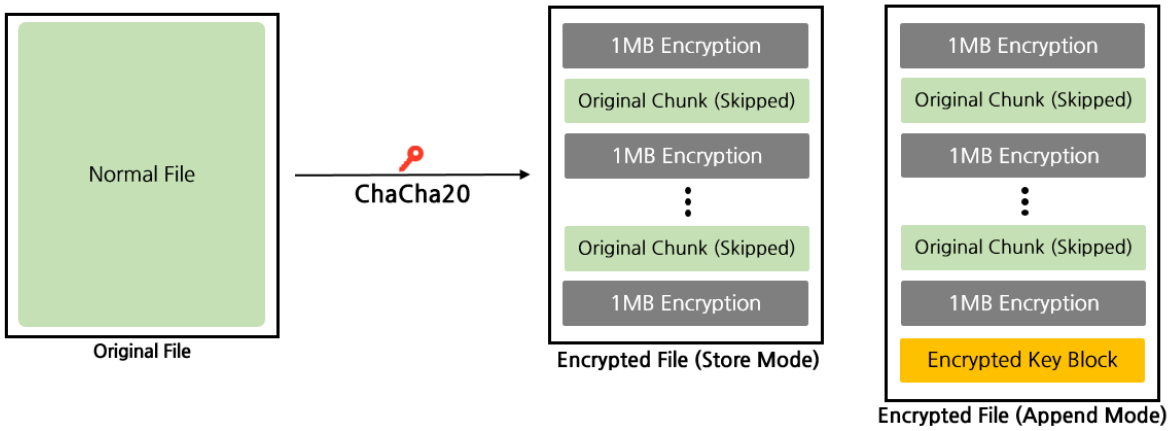

그림 9. Gunra 랜섬웨어 리눅스 버전 암호화

Gunra 랜섬웨어의 리눅스 버전은 파일 암호화에 ChaCha20 알고리즘을 사용한다. 암호화 대상 파일은 –p, -e 인자로 지정한 경로와 확장자에 따라 선정되며, 암호화는 -r 인자값에 기반한 부분 암호화 방식으로 진행된다. Gunra 는 모든 파일을 1MB 단위로 암호화하며, -r 인자를 사용해 1MB 로 암호화 이후 건너뛸 구간의 크기를 설정한다. 예를 들어 -r=5 의 경우, 1MB 를 암호화한 뒤 5MB 를 건너뛰고, 다시 1MB 를 암호화하는 방식으로 반복 수행된다. 이때 건너뛰는 간격만 달라질 뿐, 모든 암호화 구간의 크기는 고정적으로 1MB 이다. 또한 -l 인자를 사용해 GB 단위로 최대 암호화 크기를 지정할 수 있다. 파일 암호화 후, ChaCha20 에 사용된 키, Nonce[5] , -r, -l 인자를 따로 저장하는데, -s 인자의 유무에 따라 저장 방식이 달라진다.

-s 인자를 사용하면 Store Mode 가 적용되어 암호화된 키 블록이 지정한 디렉터리에 별도로 저장된다. 이 과정에서 랜섬웨어는 해당 경로가 존재하는지 확인한 뒤, 원본 파일명을 기반으로 [Filename].keystore 형태의 키 파일을 생성한다. -s 인자를 사용하지 않았다면 Append Mode 가 적용되어 암호화된 키 블록이 암호화된 파일의 끝부분에 추가된다.

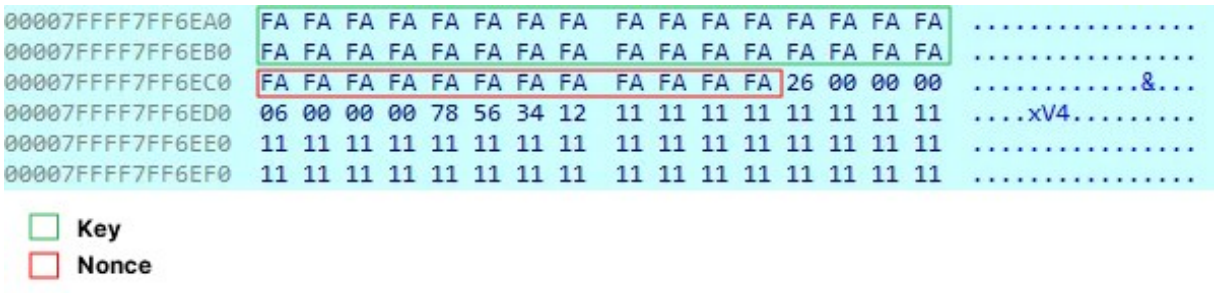

그림 10. Gunra 랜섬웨어 Linux 버전의 취약한 키 생성

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

추가로, Linux 버전에서는 암호화 키 생성 과정 중 설계상 취약점이 확인됐다. 일반적으로는 암호화 키와 Nonce 를 예측할 수 없도록 충분히 랜덤한 값을 생성하고, 이를 비대칭 키로 암호화해 공격자만 복호화할 수 있게 한다. 그러나 Gunra 의 Linux 버전은 1Byte 단위로 랜덤 값을 생성해 이어 붙이는 비효율적인 방식을 사용한다. 이 과정에서 매 바이트마다 time(0) 함수를 호출해 초 단위의 현재 시간을 시드(seed)로 설정하는데, 32Byte 키와 12Byte Nonce 를 생성하는 데 1 초도 걸리지 않아 동일한 시드로 생성된 값이 반복될 가능성이 높다. 만약 생성 도중 시간이 바뀌더라도 시드 변화 폭이 작아, 공격자가 비교적 쉽게 키와 Nonce 를 예측할 수 있는 상황이 발생한다.

Gunra 랜섬웨어 (Windows 버전)

Gunra 랜섬웨어 Windows 버전은 Linux 버전과 달리 별도의 실행 인자 없이 동작하도록 설계되어 있으며, 실행 중 중복 감염을 방지하기 위한 뮤텍스 이름이나, 암호화에 사용한 키를 보호하기 위한 RSA 공개키 등의 중요한 값들이 내부에 포함되어 있다.

랜섬웨어가 실행되면 중복 실행 방지를 위해 '375345635adfwef39'이라는 이름의 뮤텍스를 생성한다. 이후 시스템 전체 드라이브를 순차적으로 탐색해 랜섬노트를 생성하고, 암호화 대상을 확인한다. 이 때, C 드라이브 내 사용자 폴더와 그 하위 폴더만 탐색하고 나머지 드라이브는 최상위 디렉터리부터 탐색을 진행한다. 암호화 과정에서 특정 폴더명과 확장자 및 파일명은 제외하고 암호화하며, 확인된 예외 대상은 아래 표와 같다.

폴더명	확장자 및 파일명
tmp, winnt, temp, thumb, $Recycle.Bin, $RECYCLE.BIN, System Volume Information, Boot, Windows, Trend Micro	.exe, .dll, .lnk, .sys, msi, R3ADM3.txt, CONTI_LOG.txt

표 2. Gunra 랜섬웨어 Windows 버전 암호화 예외 대상

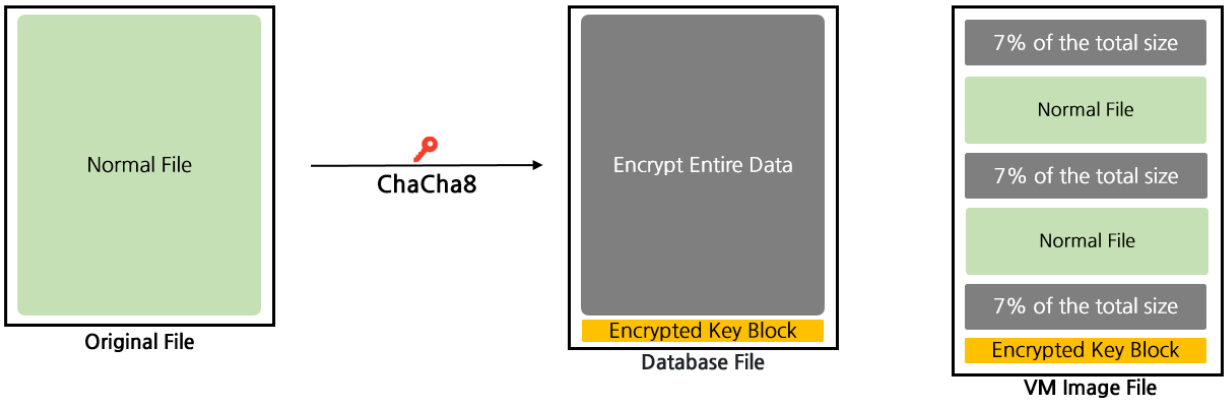

그림 11. Gunra 랜섬웨어 Windows 버전 암호화 방식(파일 확장자 기준)

파일 암호화 방식은 파일의 확장자와 크기에 따라 결정된다. 데이터베이스와 관련된 파일은 크기와 무관하게 전체를 암호화하며, 가상 머신(VM) 이미지와 관련된 파일은 크기와 관계없이 파일의 맨 앞과 뒤, 그리고 중간을 각각 전체 크기의 7% 만큼씩 암호화해 총 21%만 암호화한다. 각각 해당하는 파일 확장자는 아래 표와 같다.

데이터베이스 관련 확장자	VM 관련 확장자
.4dd, .4dl, .accdb, .accdc, .accde, .accdr, .accdt, .accft, .adb, .ade, .adf, .adp, .arc, .ora, .alf, .ask, .btr, .bdf, .cat, .cdb, .ckp, .cma, .cpd, .dacpac, .dad, .dadiagrams, .daschema, .db, .db-shm, .db-wal, .db3, .dbc, .dbf, .dbs, .dbt, .dbv, .dbx, .dcb, .dct, .dcx, .ddl, .dlis, .dp1, .dqy, .dsk, .dsn, .dtsx, .dxl, .eco, .ecx, .edb, .epim, .exb, .fcd, .fdb, .fic, .fmp, .fmp12, .fmpsl, .fol, .fp3, .fp4, .fp5, .fp7, .fpt, .frm, .gdb, .grdb, .gwi, .hdb, .his, .ib, .idb, .ihx, .itdb, .itw, .jet, .jtx, .kdb, .kexi, .kexic, .kexis, .lgc, .lwx, .maf, .maq, .mar, .mas, .mav, .mdb, .mdf, .mpd, .mrg, .mud, .mwb, .myd, .ndf, .nnt, .nrmlib, .ns2, .ns3, .ns4, .nsf, .nv, .nv2, .nwdb, .nyf, .odb, .oqy, .orx, .owc, .p96, .p97, .pan, .pdb, .pdm, .pnz, .qry, .qvd, .rbf, .rctd, .rod, .rodx, .rpd, .rsd, .sas7bdat, .sbf, .scx, .sdb, .sdc, .sdf, .sis, .spq, .sql, .sqlite, .sqlite3, .sqlitedb, .te, .temx, .tmd, .tps, .trc, .trm, .udb, .udl, .usr, .v12, .vis, .vpd, .vvv, .wdb, .wmdb, .wrk, .xdb, .xld, .xmlff, .abcddb, .abs, .abx, .accdw, .adn, .db2, .fm5, .hjt, .icg, .icr, .kdb, .lut, .maw, .mdn, .mdt	.vdi, .vhd, .vmdk, .pvm, .vmem, .vmsn, .vmsd, .nvram, .vmx, .raw, .qcow2, .subvol, .bin, .vsv, .avhd, .vmrs, .vhdx, .avdx, .vmcx, .iso

표 3. 데이터베이스 및 VM 관련 확장자

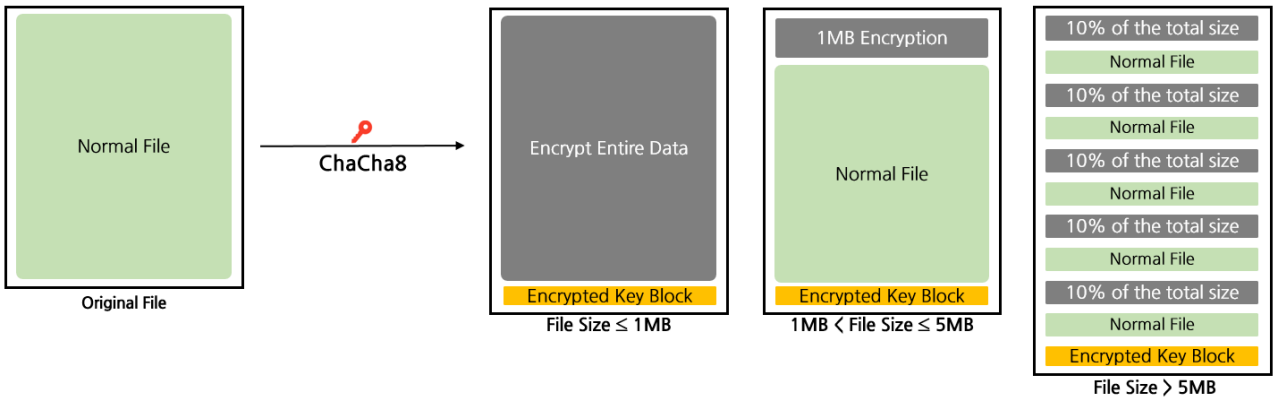

그림 12. Gunra 랜섬웨어 윈도우 버전 암호화 방식

가상머신과 데이터베이스 관련 파일을 제외한 나머지 파일은 크기에 따라 암호화를 수행한다. 파일 크기가 1MB 이하인 경우 전체 파일을 암호화하고, 1MB 를 초과하면서 5MB 이하인 경우에는 파일의 상위 1MB 만 암호화한다. 5MB 를 초과하는 파일은 전체 파일을 10% 크기의 블록으로 나누어 홀수 번째 블록만 암호화한다.

파일 암호화 후 파일의 맨 뒤에 복구에 필요한 데이터를 추가한다. 암호화에 사용한 ChaCha8 키, Nonce, 원본 파일 크기는 물론 어떤 방식으로 암호화를 진행했는지 구분하기 위한 2Bytes 크기의 식별자를 공격자의 RSA 공개키로 암호화한 뒤 추가한다.

Gunra 랜섬웨어는 시스템 복원 기능을 무력화해 사용자의 복구 가능성을 차단한다. 이를 위해 VSS(Volume Shadow Copy Service) 목록을 조회한 뒤 각 항목을 삭제하는 작업을 수행한다. 이 과정에서 랜섬웨어는 WMI[6] 를 통해 SELECT * FROM Win32_ShadowCopy 쿼리를 실행하여 시스템 내 모든 볼륨 섀도 복사본을 검색하고, 조회 결과에서 각 볼륨 섀도 복사본의 고유 ID 값을 추출한다. 이후 해당 ID 값을 이용해 다음 명령어를 생성·실행하여 해당 섀도 복사본을 삭제한다.

```
cmd.exe /c C:\Windows\System32\wbem\WMIC.exe shadowcopy where "ID='%s'" delete
```

표 4. VSC 삭제 명령어

[6] WMI(Windows Management Instrumentation): 윈도우 운영체제의 구성 요소, 상태, 동작 정보를 표준화된 방식으로 조회·관리할 수 있도록 하는 관리 인터페이스

Gunra 랜섬웨어 대응방안

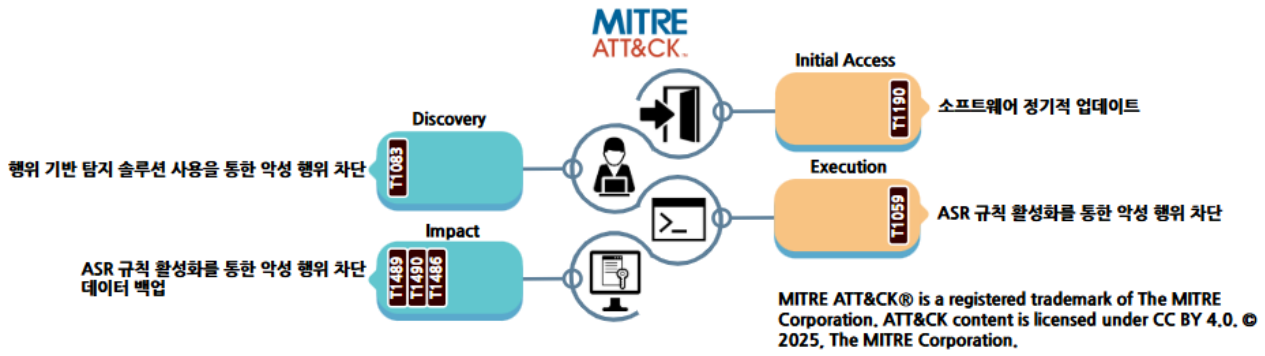

그림 13. Gunra 랜섬웨어 대응방안

Gunra 랜섬웨어의 Windows 버전은 Windows 명령 프롬프트를 활용해 시스템 내 백업 복사본을 삭제한 뒤 파일 암호화를 수행한다. 이에 따라 ASR 규칙을 활성화하면, 백업 삭제 및 암호화와 관련된 비정상적인 프로세스를 사전에 차단하여 악성 행위를 효과적으로 방지 가능하다. 특히, 시스템 복원 지점 삭제와 같은 행위를 탐지·차단할 수 있는 환경 구성이 중요하다. 사전에 정책을 정교하게 설정하고, 불필요한 스크립트 실행 시도를 즉시 차단하는 것도 피해 예방에 큰 도움이 된다.

또한 EDR 솔루션을 도입하고 최신 보안 패치를 적용하여, 알려진 취약점 악용을 통한 침투나 로컬 실행 기반의 비정상적인 동작을 신속히 식별·차단할 수 있도록 해야 한다. 이를 통해 파일 암호화 과정에서 발생하는 행위 기반 패턴을 실시간으로 탐지하고, 악성 프로세스의 실행을 중단할 수 있다. 더불어, EDR·백신·로그 분석 시스템을 연계하여 경고 이벤트를 중앙에서 모니터링하면, 다수의 단말에서 동시다발적으로 발생하는 공격에도 신속한 대응 체계를 갖추게 된다.

아울러, 백업 복사본을 별도의 네트워크 구간이나 외부 저장소, 오프라인 매체에 주기적으로 분산 백업해 두면, 시스템이 암호화되더라도 데이터 복구가 가능하다. 이때 백업 장치 접근 권한을 최소화하고, 정기적으로 복구 테스트를 실시하여 백업 데이터의 무결성을 보장하는 것이 중요하다. 추가로 별도의 네트워크나 저장소의 데이터를 분산해 백업하거나 백업 스케줄과 보관 주기를 다양화해 랜섬웨어의 삭제 시도를 피하는 것도 효과적인 방법이다.

이러한 대응 전략은 Windows 환경뿐 아니라 Linux 버전의 Gunra 랜섬웨어에도 동일하게 적용 가능하다. Linux 환경에서는 서버 등 핵심 인프라를 직접 노리는 경우가 많으므로, OS 특성에 맞는 접근 제어 정책과 서비스 포트 제한, 관리자 계정 관리 강화가 필수적이다. 운영체제와 관계없이 다계층 보안 체계를 적용하면, 랜섬웨어 감염 시 피해를 최소화하고 신속한 복구를 보장할 수 있다.

IoCs

Hash(SHA-256)
91F8FC7A3290611E28A35A403FD815554D9D856006CC2EE91CCDB64057AE53B0
22C47EC98718AB243F2F474170366A1780368E084D1BF6ADCD60450A9289E4BE

■ 참고 사이트

• ArcticWolf (https://arcticwolf.com/resources/blog/arctic-wolf-observes-july-2025-uptick-in-akira-ransomware-activity-targeting-sonicwall-ssl-vpn/)

• Microsoft (https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/)

• Thehackernews (https://thehackernews.com/2025/07/newly-emerged-global-group-raas-expands.html)

• Securit affairs (https://securityaffairs.com/180578/cyber-crime/fbi-seizes-20-btc-from-chaos-ransomware-affiliate.html)