# 랜섬웨어 공격으로부터 살아남는 방법

랜섬웨어의 역사는 많은 사람이 생각하는 것보다 훨씬 오래되었으며, 그 기원은 1980년대로 거슬러 올라갑니다. 최초로 기록된 랜섬웨어 공격은 1989년 세계보건기구의 AIDS 컨퍼런스에서 플로피 디스크를 통해 배포된 AIDS 트로이 목마로, 주요 해킹 활동의 초기 사례 중 하나로 기록되었습니다.[1]

2000년대에 랜섬웨어의 진화가 가속화되었습니다. Archievus Trojan(Arhiveus Trojan이라고도 함)은 2006년에 등장한 최초의 랜섬웨어로, 고급 RSA 암호화를 사용하여 웹사이트와 스팸 이메일을 이용해 대량 배포되었습니다.[2] 이는 상당한 기술적 도약을 의미했지만, 통일된 복호화 방식으로 인해 그 영향은 제한적이었습니다. 2009년 1월에 공식 출시된 비트코인은 2008년에 등장하여 거래 추적을 어렵게 만드는 완전히 새로운 기능을 제공했고, 이로 인해 랜섬웨어의 급속한 성장이 촉진되었습니다.[3]

최근 공격에서는 점점 더 정교해지는 전술로 헤드라인을 장식하는 유명 랜섬웨어 그룹이 등장했습니다. 한때 랜섬웨어 서비스(RaaS) 모델로 유명했던 LockBit은 2024년 2월 국제 사법 집행 기관의 대규모 방해에 직면하기 전까지 중요 인프라, 의료 및 금융 부문을 표적으로 수많은 공격을 감행했습니다.[4]

Operation Cronos를 통해 소탕되었음에도 불구하고 이 그룹은 일주일 만에 다시 나타나 현대 랜섬웨어 작전의 회복력을 보여주었습니다.[5] RansomHub는 2024년에 주요 세력으로 부상했습니다. Palo Alto Networks의 위협 인텔리전스 및 컨설팅 부서인 Unit 42®는 RansomHub 랜섬웨어가 2025년 1월과 2025년 3월 사이에 가장 활동적인 랜섬웨어 변종이 되었음을 확인했습니다(그림 1).[6]

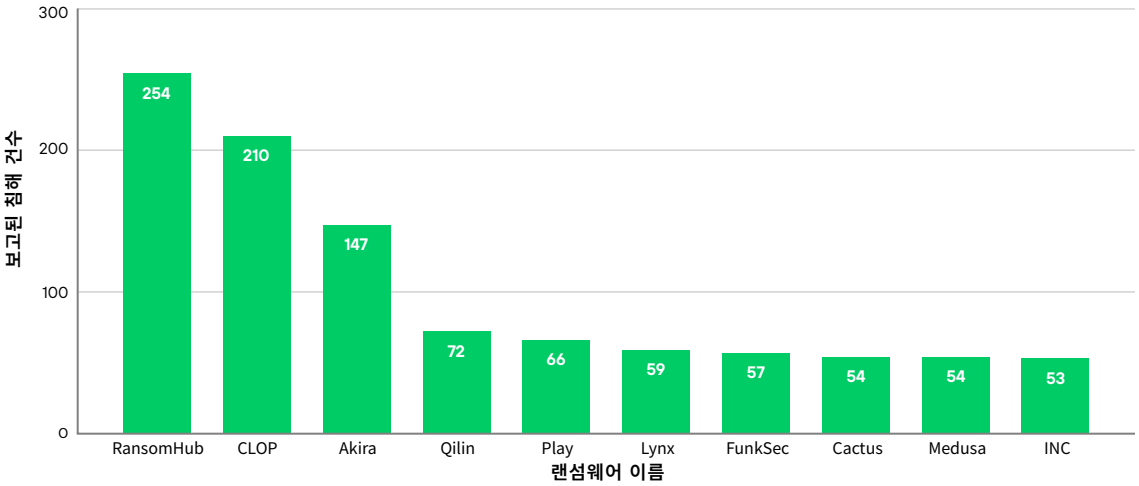


**그림 1.** 가장 활발한 랜섬웨어 유출 사이트 - 2025년 1월부터 2025년 3월까지

2024년에는 랜섬웨어 공격이 크게 증가했습니다. Unit 42의 인시던트 대응 사례 분석에 따르면, 업무 중단이 주요 공격 목표가 되었으며, 2024년 사고의 86%가 운영 중단, 평판 손상 또는 두 가지 모두와 관련이 있었습니다.[7] 같은 해에 몸값 지불액도 기록적으로 증가했습니다. Unit 42의 데이터에 따르면 2024년 초기 협박 요구액의 중간값이 전년 대비 약 80%나 급증해 125만 달러에 달했지만, 협상이 성공적으로 진행되면서 중간값 지불액은 267,500달러로 줄었습니다.[8]

1. Samantha Murphy Kelly, "랜섬웨어 발명가의 기이한 이야기", CNN Business, 2021년 5월 16일.
2. Joe Stewart, "위협 분석: Arhiveus 랜섬웨어 트로이 목마 분석," Secureworks, 2006년 5월 5일.
3. Terrence August, Duy Dao, Kihoon Kim 외, "사이버 보안에 대한 암호화폐의 영향," Institute for Operations Research and the Management Sciences, 2025년 3월 27일.
4. Jenna McLaughlin, "글로벌 법 집행 기관, LockBit 랜섬웨어 그룹에 대한 단속 강화," NPR, 2024년 2월 20일.
5. Ravie Lakshmanan, "법 집행 기관의 소탕 이후 LockBit 랜섬웨어 그룹이 다시 부상," The Hacker News, 2024년 2월 26일.
6. "2025년 1월-3월의 갈취 및 랜섬웨어 추세," Palo Alto Networks Unit 42, 2025년 4월 23일.
7. Ibid.
8. Ibid.


그림 2. 랜섬웨어: 과거(2017~2019년)와 현재(2020년 이후)

## 랜섬웨어 기본 사항

랜섬웨어는 악성 소프트웨어를 이용해 데이터를 인질로 잡고, 시스템을 잠그거나 암호화한 뒤 접근 권한을 복구해 주면 몸값을 요구하는 범죄 비즈니스 모델입니다. 점점 더 시급해지는 문제이기는 하지만 랜섬웨어는 예방할 수 있습니다. 적어도 적절한 교육, 현재 IT 환경에 대한 구체적인 튜닝, 고급 엔드포인트 기술 배포를 통해 피해를 최소화할 수 있습니다. 이 기술 배포에는 보안 스택에 확장된 탐지 및 대응(XDR)과 같은 솔루션을 추가하는 것이 포함됩니다.

랜섬웨어에는 두 가지 유형이 있습니다.

- **암호화 랜섬웨어는** 가장 일반적인 유형이며 파일과 데이터를 암호화합니다.
- **로커 랜섬웨어**는 컴퓨터나 기타 디바이스를 잠가 피해자가 사용하지 못하게 합니다.

암호화 랜섬웨어는 데이터를 암호화합니다. 멀웨어를 디바이스에서 제거하거나 저장 매체를 다른 디바이스로 옮기더라도 데이터에 접근할 수 없습니다. 일반적으로 암호화 랜섬웨어는 중요한 시스템 파일을 표적으로 삼지 않으므로, 감염되어도 디바이스는 계속 작동할 수 있습니다. 게다가 해당 디바이스는 몸값을 지불하는 데 필요할 수도 있습니다.

Locker 랜섬웨어는 디바이스만 잠그고 디바이스에 저장된 데이터는 일반적으로 손상하지 않습니다. 따라서 멀웨어가 제거되어도 데이터는 영향을 받지 않습니다. 멀웨어를 쉽게 제거할 수 없더라도 저장 장치(일반적으로 하드 드라이브)를 다른 정상 작동하는 컴퓨터로 옮기면 데이터를 복구할 수 있는 경우가 많습니다.

9. "비트코인(BTC) 가격 예측 2025", CoinCodex, 2025년 7월.
10. CISO Advisory, "인공지능이 방어자에게 어려움을 주는 새로운 복잡한 사이버 공격 물결을 부추긴다," Cyber Security News, 2025년 5월 13일.
11. Konrad Martin, "AI 사이버 공격 통계 2025," Tech Advisors, 2025년 5월 27일.
12. *2025 Unit 42* 글로벌 사고 대응 보고서, Palo Alto Networks Unit 42, 2025년 2월.

## 일반적인 랜섬웨어 공격의 일반적인 단계

일반적인 랜섬웨어 공격은 공격이 완화되거나 피해자가 몸값 지불을 거부하지 않는 한 다음 단계로 구성됩니다.

### 1. 타협 및 시스템 장악

대부분의 공격은 피싱으로 시작됩니다. 피싱은 사용자에게 긴급하게 사기성 이메일을 보내 감염된 첨부 파일을 자신도 모르게 열도록 요구하는 것입니다. 첨부 파일을 열면 시스템에 문제가 발생합니다. 또는 공격자는 초기 접근을 위해 다른 형태의 유효한 자격 증명 남용을 시도할 수도 있습니다. 이는 컴퓨터나 모바일 디바이스 등 단일 호스트에 영향을 미칠 수 있습니다. 그러면 손상된 호스트는 명령 및 제어(C2) 서버와 통신을 설정합니다. 이 시점에서 공격자는 랜섬웨어 공격의 영향을 극대화하기 위해 초기 호스트에서 조직 내의 다른 시스템으로 측면 이동할 수 있습니다.

### 2. 귀중한 데이터의 발견 또는 빼내기

과거 랜섬웨어는 피해자에게 가치가 있을 만한 특정 파일 형식(예: .doc, .xls, .pdf와 같은 비즈니스 문서)을 식별하고 암호화하는 데 그쳤지만, 공격자는 진화했습니다. 이제 위협 행위자들은 고객 데이터나 지적 재산권 등 알려진 민감한 데이터를 은밀히 찾아내 더 높은 몸값을 요구하고 있습니다. 공격자는 다중 갈취 계획에 사용하기 위해 데이터를 빼내기도 합니다.

### 3. 시스템 접근 차단

공격자가 시스템을 감염시키면 데이터를 암호화하거나 잠금 화면이나 위협 전술을 통해 하나 또는 여러 시스템에 대한 액세스를 거부합니다.

### 4. 디바이스 소유자에게 침해 사실 및 몸값 금액 알림

이전 단계는 모두 랜섬웨어 공격의 실제 동작의 대부분을 나타냅니다. 숙련된 적이 이러한 동작을 행하면 피해자가 모르는 사이에 실행됩니다. 즉, 공격자가 피해자에게 자신의 존재를 알릴 때 공격은 완료됩니다. 이러한 알림은 대개 지불 지침과 디바이스 잠금 해제를 위한 추가 단계가 포함된 몸값 요구 메시지 형태로 제공됩니다.

### 5. 몸값 지불 수락

공격자는 법 집행 기관을 피하면서 몸값을 받을 방법이 있어야 합니다. 그들은 이러한 거래에 비트코인과 같은 익명의 암호화폐를 사용합니다.

### 6. 결제 수령 시 전체 액세스 권한 반환 약속

손상된 시스템을 복구하지 못하면 이 계획의 효과가 사라집니다. 소중한 자산이 반환될 것이라는 확신 없이 몸값을 지불하는 사람은 없기 때문입니다.

## 가속 위기

최근 랜섬웨어 공격은 속도가 엄청나게 빨라졌습니다. Unit 42 연구에 따르면 공격 타임라인이 극적으로 가속화되어 2021년 9일이었던 평균 유출 시간(MTTE)이 2023년에는 단 2일로 단축되었고, 일부 사건은 몇 시간 만에 발생했습니다.[13] 전문가들은 2025년까지 일부 사건의 MTTE가 25분까지 단축될 것으로 예측합니다. 이는 단 3년 만에 공격 속도가 100배 이상 빨라진다는 것을 의미합니다.[14] 이러한 가속화는 위협 환경을 근본적으로 변화시킵니다. 공격자가 30분 이내에 목표를 달성할 수 있게 되면, 인간의 분석과 수동 프로세스에 의존하는 기존의 탐지 및 대응 방법은 쓸모가 없어집니다.

13. "Unit 42가 예측하는 2025년의 혼란과 기타 주요 위협," Palo Alto Networks Unit 42, 2024년 11월 21일.
14. Ibid.

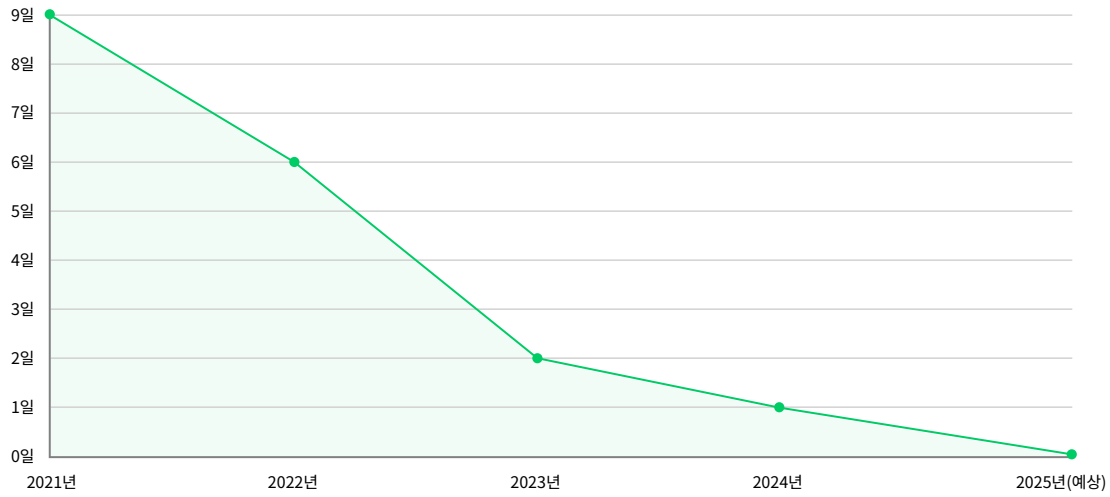


**그림 3.** 랜섬웨어 속도 위기: MTTE의 극적인 가속

## 일반적인 공격 방법

랜섬웨어를 효과적으로 예방하려면 공격자가 위협을 전달하는 데 사용하는 전략을 이해하는 것이 중요합니다. 여러 랜섬웨어 계열은 여러 공격 벡터를 통해 작동합니다. 예를 들어, 이러한 벡터는 네트워크, SaaS 애플리케이션을 통해 들어오거나 엔드포인트에 직접 도달할 수 있습니다. 이 정보를 활용하면 공격자가 가장 쉽게 악용할 수 있는 영역에 보안 제어를 집중하고 감염 위험을 줄일 수 있습니다.

인공지능(AI)으로 인해 공격이 점점 더 정교해지고 있습니다. AI가 생성한 텍스트는 합법적인 커뮤니케이션 스타일을 모방할 수 있으므로 악성 이메일과 진짜 이메일을 구별하기 어렵습니다. 2024년까지 피싱 이메일의 82.6%가 어떤 형태로든 AI 기술을 사용했으며, 78%의 사람들이 AI가 생성한 피싱 이메일을 열었습니다.[15] 이러한 공격의 정교화로 인해 더욱 진보된 탐지 방법과 사용자 교육이 필요해졌습니다.

### 악성 이메일 첨부 파일

지금까지 악성 이메일 첨부 파일을 통해 공격자는 인사부나 IT 부서 등 신뢰할 수 있는 출처에서 보낸 것처럼 이메일을 조작했습니다. 그런 다음 Portable Executable(PE) 파일, Word 문서, JS 파일 등의 악성 파일을 첨부했습니다. 수신자는 이메일이 신뢰할 수 있는 출처에서 전송되었다고 생각하고 첨부 파일을 엽니다. 그러면 랜섬웨어 페이로드가 수신자도 모르게 다운로드되고, 시스템이 감염되며, 파일은 인질로 잡히게 됩니다. 오늘날 악성 소프트웨어 감염은 공격자에게 랜섬웨어를 배포하는 데 사용되는 경우가 많습니다.

### 악성 이메일 링크

악성 이메일 첨부 파일과 마찬가지로 악성 이메일 링크는 이메일 본문에 있는 URL입니다. 이러한 이메일은 신뢰할 수 있는 출처라고 생각되는 개인이나 조직에서 보낸 것입니다. 이러한 URL을 클릭하면 웹을 통해 악성 파일이 다운로드되고, 시스템이 감염되며, 파일은 인질로 잡히게 됩니다.

15. Martin, "AI 사이버 공격 통계 2025."

### 취약한 자격 증명

랜섬웨어 운영자는 초기 침투 브로커(IAB)로부터 자격 증명을 구매하거나 비밀번호 관리가 취약한 점을 악용하여 피해자를 실제로 침해하는 전체 과정을 피할 수도 있습니다. IAB는 자격 증명을 수집하고 모아서 가장 높은 입찰자에게 판매하는 사람입니다. IAB가 랜섬웨어에만 사용되는 것은 아니지만, 랜섬웨어 운영자는 일반적으로 침입 라이프사이클의 시작 부분에서 이 시스템을 활용합니다. IAB는 정찰을 수행하여 가상 사설 통신망(VPN), 개방형 RDP 또는 노출된 소프트웨어 취약점이 있는 서버 등 취약한 애플리케이션이나 디바이스가 있는 네트워크를 식별합니다. 다중 인증(MFA) 및 추가 식별 메커니즘과 같은 견고한 모범 사례를 따르면 이러한 벡터를 피할 수 있습니다.

### CVE 익스플로잇

랜섬웨어 운영자는 알려진 CVE를 악용하여 대상 시스템에 처음으로 접근하는 경우가 많습니다. 이러한 공격은 운영 체제, 애플리케이션, 네트워크 인프라의 패치되지 않은 소프트웨어 취약점을 악용합니다. 공격자는 취약한 버전의 소프트웨어를 실행하는 시스템을 체계적으로 스캔한 다음 특정 CVE를 활용하기 위해 익스플로잇 코드를 배포합니다. 널리 알려진 보안 결함이 있는 웹 서버, VPN 어플라이언스, 이메일 서버, 원격 액세스 도구 등이 주요 타깃입니다.

공격이 성공적으로 이루어지면 공격자는 지속성을 확립하고 랜섬웨어 페이로드를 배포하거나 다른 위협 행위자에게 액세스 권한을 판매할 수 있습니다. 많은 조직이 포괄적인 패치 관리 프로그램을 유지하는 데 어려움을 겪고 있어 심각한 취약점이 장기간 노출되기 때문에 이러한 공격 벡터는 특히 효과적입니다. CVE가 공개된 후 광범위한 악용이 이루어지는 기간이 점점 줄어들고 있으며, 일부 취약점은 공개된 지 며칠 만에 적극적으로 악용되고 있습니다.

## 위험에 처해 있나요?

랜섬웨어는 대기업만 공격 대상으로 생각할 수 있지만, 중소기업도 랜섬웨어의 위협에서 자유롭지 않습니다. FBI는 의료 분야가 미국의 모든 중요 인프라 부문 중 랜섬웨어와 데이터 유출 공격을 가장 많이 경험했으며, 보고된 사건은 444건이라고 밝혔습니다.[16] 또한 설문 조사에 참여한 미국 의료 기관의 92%가 지난 12개월 동안 최소 한 번 이상의 사이버 공격을 경험했습니다.[17]

### 표적이 된 데이터의 보고

랜섬웨어 공격은 표적이 된 조직에 공개적으로 피해를 입힙니다. 최근 미국 전역의 병원을 대상으로 한 공격에서 알 수 있듯이 조직의 운영이 심각하게 저하되거나 완전히 중단될 수 있기 때문입니다. 개인식별정보(PII)는 다크웹에서 판매하거나 경매에 붙이는 사이버 도둑들에게는 엄청난 데이터의 보고입니다. 개인식별정보(PII)가 노출되면 소비자에게 영향을 미치는 신원 사기와 표적형 사기가 증가합니다.

범죄자들은 이것이 진입 장벽이 낮고 수익성이 좋은 사업이라는 것을 깨달았습니다. RaaS 모델을 사용하면 제휴사가 이미 개발된 랜섬웨어 도구를 사용하여 자체 랜섬웨어 공격을 실행할 수 있습니다. 결과적으로 랜섬웨어는 다른 사이버범죄 사업 모델을 대체하고 있습니다. 게다가 공격자들은 손상된 정보의 가치를 판단하고, 피해 조직의 지불 의사를 평가하고, 더 높은 몸값을 요구하는 능력이 점점 더 정교해지고 있습니다.

16. "보고서: 2024년에 가장 많은 사이버 위협을 겪은 보건 산업," American Hospital Association, 2025년 5월 12일.
17. Steve Adler, "92%의 미국 의료 기관, 지난해 사이버 공격 경험," The HIPAA Journal, 2024년 10월 9일.

### 취약한 다양한 플랫폼들

과거에는 공격자들이 주로 Microsoft Windows 시스템에만 집중했지만, Android, macOS, Linux를 노리는 랜섬웨어가 등장하면서 어떤 운영 체제도 이러한 공격에서 자유로울 수 없다는 사실이 드러났습니다. 인터넷에 연결된 거의 모든 컴퓨터나 디바이스는 랜섬웨어의 잠재적 피해자입니다. 이는 사물 인터넷(IoT) 디바이스의 확산과 더불어 최근에는 원격 근무 추세가 지속되면서 공격 표면이 확대되는 상황에서 제기되는 우려입니다.

## 공급망 및 교차점의 심각한 취약점

2024년에는 랜섬웨어 환경이 크게 변했으며, 공급망 공격과 심각한 취약점 악용이 랜섬웨어 활동 급증에 중심적인 역할을 했습니다.

### 2024년 공격에 대한 주요 조사 결과

- **악용된 심각한 취약점:** CVE-2024-3400(Palo Alto Networks 방화벽) 및 기타 중요 인프라 구성 요소와 같은 취약점을 표적으로 삼는 제로데이 공격으로 인해 방어자가 취약한 소프트웨어를 업데이트하기 전에 랜섬웨어 감염이 급증했습니다.[18]
- **공급망 영향:** 공급망 침해는 두 번째로 흔한 공격 벡터(15%)가 되었고, 악의적인 내부 위협(491만 달러)에 이어 두 번째로 비용이 많이 드는 공격 벡터(491만 달러)가 되었습니다.[19] Unit 42의 연구에 따르면 소프트웨어 공급망 및 클라우드 공격은 빈도와 정교함이 모두 증가하고 있으며, 위협 행위자는 잘못 구성된 환경에 숨어들어 광대한 네트워크를 스캔하여 귀중한 데이터를 찾습니다. Unit 42가 기록한 한 캠페인에서 공격자는 민감한 정보를 얻기 위해 2억 3천만 개 이상의 고유한 대상을 스캔했습니다.[20]
- **새로운 위협:** 새로운 랜섬웨어 그룹이 계속해서 등장하고 있어 랜섬웨어가 수익성 있는 범죄 활동으로 여전히 인기를 끌고 있습니다.
- **산업 초점:** 2024년에는 헬스케어가 가장 많이 표적이 되는 산업 중 하나가 되었습니다. Unit 42 사고 대응 데이터에 따르면 가장 많이 표적이 된 6개 산업은 전문 및 법률 서비스, 첨단 기술, 제조, 의료, 금융, 도소매였습니다. 이들은 모두 전체 사례의 63%를 차지했습니다.[21]

### 전술의 진화

랜섬웨어 그룹은 영향력과 이익을 극대화하기 위해 전략을 변경했습니다.

- **다단계 공격:** 일부 그룹은 랜섬웨어를 주의를 돌리는 수단이나 더 복잡한 공급망을 손상시키기 위한 자금원으로 사용합니다.
- **데이터 유출:** RansomHub와 다른 주요 공격 조직은 암호화하기 전에 정교한 데이터 도용을 포함하도록 전략을 업데이트하여 갈취 활동의 효율성을 높였습니다.
- **중요 인프라를 표적으로 삼기:** 랜섬웨어 운영자들은 의료, 제조, 에너지 등 가동 중지 허용도가 낮은 분야에 집중적으로 공격을 가했습니다.
- **AI 강화 작업:** Unit 42에서 2024년에 실시한 연구에서는 위협 행위자가 GenAI 도구를 사용하여 멀웨어를 생성하는 방법을 조사했습니다. 초기 시도에서는 기본적인 코드가 생성되었지만 MITRE ATT& CK®와 같은 프레임워크를 사용하는 보다 체계적인 접근 방식이 기능적인 결과를 낳았습니다.[22] Unit 42는 2025년을 내다보며 GenAI 기능이 랜섬웨어 개발 및 배포의 일부를 자동화하여 자동 암호화, 피해자 타겟팅 및 정찰 기능을 갖춘 맞춤형 랜섬웨어 키트 및 빌더를 만드는 데 도움이 될 것으로 예측합니다.[23]

18. Deeba Ahmed, "RansomHub: 랜섬웨어의 새로운 왕? 2024년까지 600개 기업 표적," HackRead, 2025년 2월 14일.
19. *2025*년 데이터 유출의 총 비용 *AI* 감독 격차, IBM 및 Ponemon Institute, 2025년 7월 31일.
20. *2025*년 *Unit 42* 글로벌 인시던트 대응 보고서.
21. *Unit 42* 공격 표면 위협 보고서, Palo Alto Networks, 2025년 5월 6일.
22. *Unit 42* 위협의 최전선*:* 새로운 *AI* 위험에 대비하기, Palo Alto Networks, 2024년 10월 16일
23. "혁신의 해."

## 사법 집행 기관 및 사이버 보안 대응

2024년에는 국제법 집행 기관의 노력이 강화되었습니다. Operation Cronos는 한때 세계에서 가장 활발하게 랜섬웨어를 퍼뜨렸던 LockBit를 붕괴시켰습니다.[24] 그러나 작전이 중단된 지 일주일 만에 이 단체가 빠르게 다시 활동하면서 현대 랜섬웨어 작전의 회복력이 입증되었습니다.[25] 이러한 활동은 사이버 보안 분야에서의 글로벌 협력의 성공과 과제를 모두 반영합니다.

### 미래 트렌드 및 예측

앞으로 Unit 42는 2025년 위협 환경을 재편할 몇 가지 주요 사건을 예측합니다.[26]

- **GenAI는 사이버 공격을 최대 100배까지 가속화합니다.** 위협 행위자가 AI를 사용하여 정찰, 고도로 개인화된 피싱, 네트워크 전반의 빠른 측면 이동을 자동화함에 따라 공격 속도가 며칠에서 단 25분으로 단축될 수 있습니다.
- **RaaS는 AI로 강화될 것입니다.** GenAI의 역량은 랜섬웨어 개발 및 배포를 자동화하고, 위협 행위자로부터 훈련을 받은 LLM이 맞춤형 랜섬웨어 키트와 챗봇을 만들어 몸값 요구를 협상할 수 있도록 만듭니다.
- **중요 인프라는 국가적 공격의 증가에 직면하게 될 것입니다.** 지정학적 긴장이 고조됨에 따라 적대 세력이 전략적 거점을 노리고 에너지, 물, 교통, 의료 등 필수 서비스를 겨냥한 공격적인 사이버 캠페인이 늘어날 것입니다.
- **공급망의 취약성은 더욱 심화될 것입니다.** 조직은 복잡한 소프트웨어 종속성으로 어려움을 겪을 것이고, 지능형 지속 위협 그룹은 단일 침해를 통해 영향을 극대화하기 위해 점점 더 타사 공급업체와 주요 클라우드 서비스 공급업체를 표적으로 삼을 것입니다.

랜섬웨어 공격은 계속해서 진화하고 있으므로 조직에서는 이러한 위협의 기술적 측면과 평판 손상 가능성을 모두 해결하기 위해 방어 수단을 조정해야 합니다. 또한 기업은 점점 더 복잡해지는 공격의 표적이 될 수 있는 직원, 고객, 파트너를 보호해야 합니다.

# 다중 갈취의 진화

랜섬웨어 운영자들은 피해자들에게 돈을 지불하도록 압력을 가하기 위해 여러 가지 갈취 기법을 점점 더 많이 사용하고 있습니다. 이러한 다중 협박 추세는 2021년 이후 크게 진화했으며, 위협 행위자들은 지불 가능성을 최대화하기 위해 다양한 전략을 구사하고 있습니다. Unit 42에서는 이러한 진화를 몸값을 요구하는 전통적인 암호화, 데이터 도난과 암호화를 결합한 이중 갈취, 운영에 미치는 영향을 극대화하기 위해 고안된 최신의 의도적인 비즈니스 방해의 세 가지 흐름으로 정의합니다.[27]

## 일반적으로 사용되는 랜섬웨어 기술

4중 갈취의 증가는 우려스러운 추세 중 하나를 보여줍니다. 랜섬웨어 운영자들은 이제 피해자들에게 압력을 가하기 위해 일반적으로 최대 4가지 기술을 사용합니다.

- **암호화:** 피해자는 암호화된 데이터와 손상된 컴퓨터 시스템에 다시 접근하기 위해 비용을 지불합니다.
- **데이터 도난:** 해커들은 피해자가 몸값을 지불하지 않으면 민감한 정보를 공개하겠다고 위협합니다.

24. Kate Whiting, "LockBit: 국제 작전이 '세계에서 가장 해로운 사이버 범죄 집단'을 장악한 과정," World Economic Forum, 2024년 2월 21일.
25. Lakshmanan, "사법 집행 기관의 소탕 이후 LockBit 랜섬웨어 그룹이 다시 등장하다."
26. "혁신의 한 해."
27. Ibid.

- **서비스 거부:** 랜섬웨어 갱단은 피해자의 공개 웹사이트를 차단하는 DoS 공격을 실행합니다.
- **괴롭힘:** 사이버 범죄자들은 고객, 사업 파트너, 직원, 언론사에 연락해 해킹 사실을 알리고 피해 조직에 압력을 가합니다.

Unit 42의 2024년 사고 대응 데이터에 따르면 협박 공격의 92%에서 암호화가 가장 흔히 사용되는 전술로 나타났고, 그 다음으로는 데이터 도난이 60%로 나타났습니다.[28]

| 갈취 전술 | 2021년 | 2022년 | 2023년 | 2024년 |
|---|---|---|---|---|
| **암호화** | 96% | 90% | 89% | 92% |
| **데이터 도난** | 53% | 59% | 53% | 60% |
| **괴롭힘** | 5% | 9% | 8% | 13% |

출처: *Unit 42 사고 대응 보고서 2024년*, Palo Alto Networks

**그림 4.** 갈취 관련 사건에서의 갈취 전술의 유행

그러나 중요한 발견은 현재 사고의 86%가 운영 다운타임, 평판 손상 또는 둘 다에 걸친 비즈니스 중단과 관련이 있다는 것입니다.[29] 한 조직이 네 가지 기술 모두에 피해를 입는 경우는 드물지만, 공격자는 목표를 달성하기 위해 여러 방법을 점점 더 많이 사용하고 있다는 추세를 보여줍니다.

2024년에 검토한 사례 중 Unit 42는 중간 초기 협박 요구액이 125만 달러에 달했으며, 이는 피해 조직의 연간 수익 추정치의 약 2%에 해당한다고 밝혔습니다.[30] 협상을 통해 피해 조직은 초기 요구액에서 중간값 50% 이상의 감소를 달성했습니다.[31] 사이버 범죄 집단이 피해자에게 돈을 지불하도록 강요하는 전술을 더욱 다듬고 공격을 더욱 파괴적으로 만드는 새로운 접근 방식을 개발함에 따라 랜섬웨어 위기는 계속해서 확산되고 있습니다.

### 암호화 없는 갈취의 증가세

과거 전략과 달리, 협박과 관련된 사고 대응 사안의 약 10%는 암호화와 관련이 없습니다.[32] 이러한 사례는 데이터 도난에만 의존하는 경우가 많으며, 일부 위협 행위자는 조직의 데이터를 암호화하는 대신 완전히 삭제하기도 합니다. 개선된 백업 관행에도 불구하고 Unit 42의 데이터에 따르면 영향을 받은 피해자의 거의 절반(49.5%)이 2024년에 백업에서 복구할 수 있었으며, 이는 2022년에 백업에서 복구할 수 있었던 비율이 11%에 불과했던 것에 비해 약 5배나 높습니다.[33] 따라서 조직은 데이터 액세스가 끊어지지 않은 경우에도 랜섬웨어 공격자가 몸값 지불을 강요하기 위해 다른 형태의 압력을 가할 수 있다는 사실에 대비해야 합니다.

랜섬웨어 집단이 계속해서 전략을 발전시키고 있기 때문에 조직은 다양한 압박 방법에 대처하기 위해 방어 체계를 조정해야 합니다. 현대의 사고 대응 계획에서는 기술적 측면과 조직의 평판을 보호하는 측면을 모두 고려해야 합니다. 또한 점점 더 공격적인 갈취 전술의 표적이 될 수 있는 직원, 고객, 파트너를 보호하기 위한 조치도 고려해야 합니다.

## 준비 및 예방

랜섬웨어는 빠르게 작동합니다. 감염 후 몇 분 만에 공격이 시작되는 경우도 있습니다. 따라서 랜섬웨어 공격을 완화하거나 예방하는 제어 기능을 구축하는 것이 중요합니다. AI 기반 공격, 다중 협박 계획, 공급망 침해가 증가함에 따라 조직에서는 최신 위협 벡터를 처리하는 포괄적인 방어 전략이 필요합니다.

28. *Unit 42 사고 대응 보고서 2024*, Palo Alto Network, 2024년 2월.
29–33. Ibid.

## 랜섬웨어 공격의 영향을 완화하기 위한 권장 사항

### AI 인식, 최종 사용자 인식 프로그램 개발 및 실행

현재 피싱 이메일의 82.6%가 AI 기술을 사용하고 있어[34] 기존의 인식 교육으로는 부족합니다. 딥페이크 오디오 및 비디오 인식을 포함하여 AI가 생성한 콘텐츠 감지를 특별히 다루는 분기별 교육을 구현하세요. 특히 금융 거래나 신원 정보 요청의 경우 대체 커뮤니케이션 채널을 통해 요청을 확인하도록 사용자를 교육하세요. 사용자가 AI가 생성한 사회 공학적 시도를 의심하는 경우 명확한 보고 절차를 수립하세요.

### Zero Trust 백업 및 복구 아키텍처 구현

3-2-1-1 백업 전략을 구현하세요. 두 가지 다른 미디어 유형에 데이터 사본 3개를 저장하고, 한 사본은 오프사이트에 보관하고, 다른 사본은 오프라인 또는 변경할 수 없도록 보관해야 합니다. 매월 백업 복원 절차를 테스트하고 중요 시스템에 대한 문서화된 복구 시간 목표(RTO)와 복구 지점 목표(RPO)를 유지 관리하세요.

Unit 42 데이터는 백업 관행 개선의 효과를 보여줍니다. 2024년에 피해자의 절반(49.5%)이 백업에서 데이터를 복원할 수 있었습니다. 이는 2022년 대비 5배 증가한 수치입니다.[35] 백업 시스템에 별도의 인증 자격 증명이 필요하고 프로덕션 네트워크에서 액세스할 수 없도록 하세요.

### 종합 권한 관리 구축

관리 기능에 대해 JIT(Just-In-Time) 액세스를 구현하여 필요할 때만 권한이 있는 계정이 활성화되도록 하세요. 모든 관리 활동을 모니터링하고 기록하는 권한 있는 액세스 관리(PAM) 솔루션을 배포하세요. 사용자 역할에 따라 네트워크 액세스를 세분화하고 마이크로 세분화를 구현하여 측면 이동을 제한해야 합니다.

정기적으로 불필요한 권한을 감사하고 취소하며, 권한 상승 시도에 대한 자동 알림을 설정하세요. 권한이 있는 계정에 대한 비밀번호와 API 키를 정기적으로 순환하는 자동화된 자격 증명 재활용 정책을 구현하여 공격 표면을 줄이고 자격 증명 채우기 공격이나 장기적인 자격 증명 손상으로 인한 위험을 완화하세요.

### 다 갈취 사고 대응 절차

최신 랜섬웨어는 데이터 도난, 괴롭힘, DoS 공격을 포함한 여러 가지 압박 전술을 사용합니다. 법적 통지 요구 사항, 영향을 받는 당사자와의 의사소통 전략, 법 집행 기관과의 협력을 포함하여 각 협박 유형을 처리하기 위한 구체적인 절차를 문서화하세요.

전문 사이버보안 법률 회사와 협력하고 사이버 보험사에 통보하는 절차를 수립하고, 사전 협상된 보수 계약을 유지하여 신속한 대응과 적절한 보장 조정을 보장하는 것을 고려하세요. 이해관계자, 고객, 미디어를 대상으로 사전 승인된 커뮤니케이션 템플릿을 수립해야 합니다. 임원 및 직원을 대상으로 하는 괴롭힘 캠페인을 처리하기 위해 특정 팀원을 지정하세요. 디지털 포렌식 회사와 위기 커뮤니케이션 전문가와 계약을 맺어 대응 노력을 신속히 진행하는 것을 고려하세요.

### 공급망 보안 프로토콜 개발

제3자에 의한 침해가 데이터 침해의 상당 부분을 차지하므로, 온보딩 전에 사이버 보안 태세를 평가하는 공급업체 위험 평가 프로그램을 구현하세요. 주요 공급업체로부터 보안 인증과 정기적인 침투 테스트 보고서를 요구하세요. 사고 알림 일정 및 책임 조건을 포함한 계약상의 보안 요구 사항을 수립해야 합니다. 타사의 시스템 접근을 모니터링하고 공급업체 연결에 대한 네트워크 분할을 구현하세요. 여기에는 타사가 위험 허용 범위를 벗어나는 경우 지속적인 위험 평가 및 완화 프로토콜을 수행하는 것도 포함됩니다.

34. "모든 피싱 이메일의 82%, AI 활용하다." Security Magazine, 2025년 3월 24일.
35. 글로벌 사고 대응 보고서.

### 확실한 규제 준수 준비

2022년 중요 인프라에 대한 사이버 사고 보고법(CIRCIA, 72시간 사고 보고용), 디지털 운영 복원력법(DORA, 금융 서비스 복원력용) 및 새로운 주 개인정보 보호법 등의 규정에 대비하세요. 보고 요구사항을 충족하기 위해 모든 사이버 보안 사고를 타임스탬프와 영향 평가와 함께 문서화해야 합니다. 사이버보안법을 전문으로 하는 법률 고문과 관계를 구축하고 포렌식 회사와 사고 대응 계약을 맺으세요.

## 랜섬웨어 감염을 예방하기 위한 상위 권장 사항

### AI 기반 위협 탐지 및 대응 구현

랜섬웨어 활동을 나타내는 비정상적인 동작 패턴을 감지하기 위해 AI를 활용하는 보안 솔루션을 구축하세요. 비정상적인 액세스 패턴이나 데이터 이동을 식별하기 위해 사용자 및 엔터티 동작 분석(UEBA)을 구현해야 합니다. 악성 AI 도구에서 생성된 것을 포함하여 정교한 피싱 시도를 탐지할 수 있는 AI 강화 이메일 보안을 사용하세요. 공격 체인의 초기 단계에서 측면 이동을 감지하기 위해 허니팟을 생성하는 기만 기술을 배포하세요.

전 세계 네트워크에서 관찰되는 침해 및 공격 패턴에 대한 공유 지표를 통해 조기 경보 시스템을 제공하고 위협 탐지를 가속화하기 위해 글로벌 위협 인텔리전스 피드와 솔루션을 통합해야 합니다. 24시간 연중 무휴 관리형 탐지 및 대응(MDR) 전문가로 SOC를 강화하면 팀이 랜섬웨어 공격을 더 빠르게 탐지, 추적하고 대응하여 운영 중단이나 평판 손상을 방지할 수 있습니다.

엔드포인트, 네트워크, 클라우드, 이메일, ID 등 더 광범위한 보안 계층의 데이터를 분석하기 위해 AI를 통합하고 사용하는 Cortex XDR®과 같은 XDR 플랫폼을 고려해 보세요. 이러한 플랫폼은 위협에 대한 보다 전체적인 관점을 제공하고 다단계 공격을 탐지하는 향상된 기능을 제공합니다.

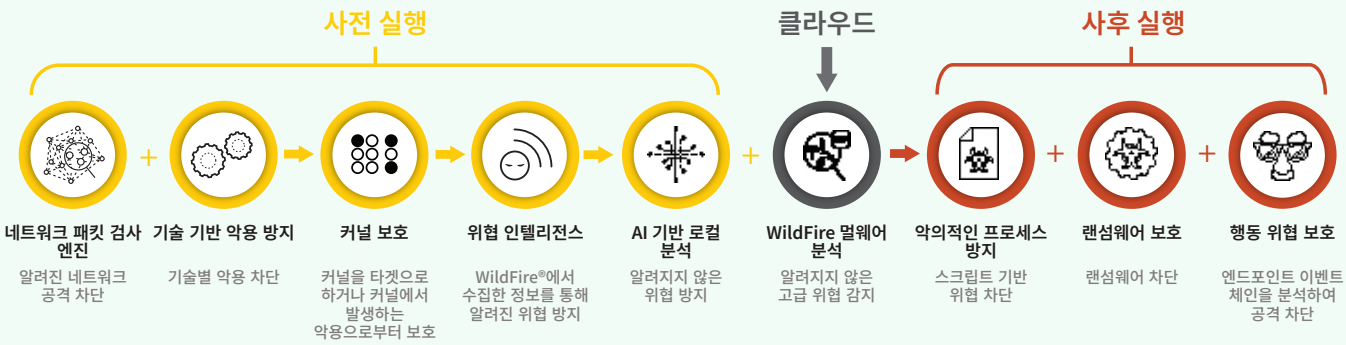


그림 5. Cortex XDR Agent는 효과적인 랜섬웨어 방어를 위해 여러 가지 위협 방지 방법을 계층화합니다.

### 제로 트러스트 네트워크 아키텍처 구축

경계 기반 보안에서 모든 사용자와 디바이스를 검증한 후 액세스를 허용하는 제로 트러스트 모델로 전환하세요. 시스템 간 랜섬웨어 확산을 제한하기 위해 네트워크 마이크로세그먼테이션을 구현해야 합니다. 기존 VPN 대신 원격 액세스를 위해 소프트웨어 정의 경계(SDP)를 배포하세요. 모든 네트워크 연결을 지속적으로 모니터링하고 검증하며, 내부 트래픽을 잠재적으로 적대적인 것으로 간주하세요.

### 보안 원격 근무 정책 개발

기존 VPN 대신, 제로 트러스트 네트워크 액세스(ZTNA) 솔루션을 통해 안전한 원격 액세스를 구축하세요. 모든 회사 디바이스에 모바일 디바이스 관리(MDM)를 구현하고 BYOD(Bring Your Own Device)를 활용하세요. 위치에 관계없이 원격 근무자를 보호하는 클라우드 기반 보안 서비스를 구축해야 합니다. 안전한 재택근무 환경 설정 및 개인 디바이스 사용에 대한 정책을 수립하세요.

## 랜섬웨어 감염 방지를 위한 상위 권장 사항(계속)

### 위협 헌팅 기능 수립

최첨단 지속 위협과 랜섬웨어 지표를 사전에 검색하는 전담 위협 사냥팀을 배치하세요. 암호화가 시작되기 전에 미묘한 침해 징후를 감지할 수 있는 행동 분석을 구현해야 합니다. 내부 이벤트와 글로벌 위협 데이터를 연관시키는 위협 인텔리전스 플랫폼을 활용하세요. 보안 제어를 검증하기 위해 정기적인 침투 테스트와 레드팀 훈련을 실시하세요.

### DNS 보안 조치 구현


알려진 악성 도메인과 공격에 사용되는 새로 등록된 도메인에 대한 액세스를 차단하는 DNS 필터링 서비스를 배포하세요. DNS 모니터링을 구현하여 데이터 유출 시도와 C2 통신을 감지해야 합니다. 조작 및 모니터링을 방지하기 위해 DNS 쿼리를 암호화하는 안전한 DNS 서비스를 사용하세요.

### 보안 클라우드 및 하이브리드 환경

클라우드 구성을 지속적으로 모니터링하고 개선하기 위해 클라우드 보안 포스처 관리(CSPM) 도구를 구현하세요. SaaS 애플리케이션 사용을 제어하고 모니터링하기 위해 클라우드 액세스 보안 브로커(CASB)를 배포하세요. 모든 클라우드 서비스에서 전송 중인 데이터와 저장 중인 데이터를 모두 암호화해야 합니다. 모든 클라우드 리소스에 대해 강력한 인증 및 최소 권한 적용을 통해 최신 IAM을 구현하세요. 특히 서비스 계정, API 키, 토큰, 자동화된 스크립트와 같은 비인간적 엔터티를 보호하는 것이 중요합니다.

### 고급 엔드포인트 보호 기능 수립

행동 분석과 머신 러닝을 활용하여 알려지지 않은 위협을 탐지하는 차세대 바이러스 백신 솔루션을 구축하세요. 실시간 모니터링과 자동 대응을 제공하는 엔드포인트 탐지 및 대응(EDR) 기능을 구현해야 합니다. 허가되지 않은 소프트웨어 실행을 방지하는 애플리케이션 제어 기술을 배포하세요. 모든 엔드포인트에 출시 후 72시간 이내에 보안 업데이트를 적용하는 자동 패치 시스템이 있는지 확인하세요.

### AI 생성 위협에 대한 이메일 보안 강화

AI가 생성한 텍스트 패턴에 따라 메시지 내용을 분석하는 고급 이메일 필터링을 구현하세요. 이메일 스푸핑을 방지하기 위해 도메인 기반 메시지 인증, 보고 및 준수(DMARC), 메일서버등록제(SPF), 도메인키 인증 메일(DKIM)을 포함한 이메일 인증 프로토콜을 배포하세요. 지나치게 완벽한 문법, 특이한 응답 패턴, 정상적인 비즈니스 프로세스를 우회하는 요청 등 AI가 생성한 피싱 지표를 인식하도록 사용자를 교육하세요. 최종 사용자에게 전달하기 전에 모든 첨부 파일과 링크에 대한 이메일 샌드박싱을 구현하세요.

### 취약성 관리 프로그램 강화

활성 위협 정보를 기반으로 자동화된 취약성 스캐닝 및 우선순위 지정을 수립하세요. 즉시 업데이트할 수 없는 중요 시스템에는 가상 패치를 구현해야 합니다. 공격이 성공하기 전에 침해 징후를 사전에 검색하는 위협 사냥 프로그램을 배포하세요. Unit 42 분석에 따르면 5건 중 1건 가까이에서 데이터 유출이 침해 후 1시간 이내에 발생했으며, 이는 신속한 탐지 및 대응의 필요성을 강조합니다.[36] 클라우드 리소스, IoT 장치, 섀도 IT 시스템을 포함한 실시간 자산 인벤토리를 유지 관리하세요.

### 종합 보안 모니터링 생성

24시간 연중무휴 모니터링 기능과 MDR 전문가를 팀의 확장 구성원으로 갖춘 보안 정보 및 이벤트 관리(SIEM) 시스템을 구현하세요. 보안 오케스트레이션, 자동화 및 대응(SOAR) 플랫폼을 구축하여 사고 대응 및 자동 수정을 가속화해야 합니다. 새로운 랜섬웨어 캠페인에 대한 실시간 정보를 제공하는 위협 인텔리전스 피드를 구축하세요. 탐지 후 몇 분 내에 위협을 억제할 수 있는 자동화된 사고 대응 플레이북을 만드세요.

36. 글로벌 사고 대응 보고서.

## 랜섬웨어 사례 2건은 Palo Alto Networks의 신속한 대응 역량을 보여줍니다.

인프라 제조업체가 Black Basta와 LockBit 공격을 두 번이나 받았고, 통신 서비스 제공업체가 13시간 동안 공격을 받아 운영의 50%가 중단되었을 때, Unit 42는 신속하게 봉쇄하고 위협을 근절하고 운영을 복구했습니다.

**사례 연구 | 인프라 제조업체**

**73 퍼센트**
전문가 협상으로 몸값 지불 감소

**<5 일**
최초 감염자를 식별하고, 데이터 유출 범위를 파악하며, 알려진 모든 랜섬웨어 IoC를 차단하는 일수

**250 만 이상**
협상을 통해 노출 방지된 파일 수

**사례 연구 | 통신 제공업체**

**3 일**
50K 엔드포인트 환경에서 공격 벡터를 결정하는 일수

**80 퍼센트**
전문가 협상을 통한 몸값 감면

**2 일**
위협을 억제하고 비즈니스 운영의 연속성을 보장하는 일수

Unit 42는 광범위한 원격 측정, 최소한의 방해로 더 빠른 위협 제거, 연간 1,000건 이상의 사건에 대한 전문가 대응을 통해 조사를 가속화했습니다. 두 조직 모두 몸값 협상 지원을 받으면서 통제권을 회복하고 중요한 운영을 복구했습니다.

**다음 스토리에서 자세한 내용을 확인하세요.**

- 통신사, Black Basta 공격 억제 및 운영 재개
- 인프라 제조업체, 이중 랜섬웨어 공격 후 통제권을 되찾다

# Cortex가 랜섬웨어 공격을 예방, 탐지 및 차단하는 방법

Cortex XDR과 Cortex XSIAM®을 사용하면 모든 사용자나 자산을 표적으로 삼는 첨단 랜섬웨어 공격을 하나의 플랫폼과 하나의 콘솔에서 모두 탐지하고 차단할 수 있습니다. 분석가는 시행 지점과의 긴밀한 통합을 통해 멀웨어 확산을 신속하게 막고, 디바이스에서 발생하는 네트워크 활동을 제한하고, 악성 도메인 등의 위협 예방 목록을 업데이트할 수 있습니다. Unit 42에 따르면 사고의 70%가 3개 이상의 공격 표면에 걸쳐 발생하므로 Cortex®가 제공하는 종단 간 가시성은 사치가 아닌 필수입니다.[37]

Cortex 플랫폼을 사용하면 다음과 같은 작업을 수행할 수 있습니다.

- Cortex XDR 에이전트를 사용하면 초기 공격부터 파일 분석 및 동작 보호까지 공격 주기의 모든 단계에서 랜섬웨어 공격을 차단할 수 있습니다.
- AI와 교차 데이터 분석을 통해 은밀한 공격을 찾아내세요.
- 근본 원인 분석을 통해 신속하게 조사하세요.
- 조정된 대응으로 모든 위협을 봉쇄하세요.

XDR 에이전트는 랜섬웨어에 대한 매우 효과적인 방어를 위해 여러 가지 위협 방지 방법을 계층화합니다.

Cortex XDR 및 XSIAM의 대응 옵션은 다음과 같습니다.

- **직접 엔드포인트에 액세스할 수 있는 라이브 터미널에는** 그래픽 작업 관리자와 파일 관리자가 포함되어 있어 프로세스를 보고 종료하고, 파일을 삭제하거나 다운로드하고, 명령을 실행하는 등의 작업을 수행할 수 있습니다.
- **수색 및 파괴** 조직의 모든 엔드포인트에 있는 모든 파일을 인덱싱하여 실시간으로 악성 파일을 찾아 삭제합니다.

37. 글로벌 인시던트 대응 보고서.

- 관리 콘솔에서 **스크립트를 실행**해 하나의 엔드포인트, 엔드포인트 그룹 또는 모든 엔드포인트에서 사실상 모든 Python 스크립트를 실행할 수 있습니다.
- **엔드포인트를 복구**하여 악의적인 활동으로 인해 엔드포인트에 적용된 변경 사항을 복원하고 되돌립니다.

당사의 수정 제안을 통해 멀웨어를 삭제하고, Windows 섀도 복사본을 사용하여 파일을 복원하고, 레지스트리 키 변경 사항을 제거할 수 있습니다. 이러한 기능은 격리, 네트워크 격리, 파일 차단과 같은 보다 전통적인 대응 옵션에 추가됩니다.

Cortex XSIAM은 랜섬웨어 조사 및 대응을 한 단계 더 발전시켜 전체 보안 스택으로 적용 범위를 확장합니다. 위협 인텔리전스로 이벤트를 강화하고, 손상된 사용자 계정을 비활성화하고, 방화벽에서 네트워크 액세스를 차단하여 랜섬웨어를 차단하고 환경에서 적을 근절할 수 있습니다. 그리고 강력하고 즉시 사용 가능한 워크플로우를 통해 랜섬웨어 복구에 대한 추측이 불필요해집니다.

또한 Cortex XDR 및 Cortex XSIAM에 대한 사전 예방적 방어 솔루션인 Unit 42 MDR은 Cortex 기반의 전문가가 관리하는 AI 기반 방어 기능으로 SOC 팀을 강화하여 공격 표면 전체에서 24시간 내내 위협을 차단할 수 있습니다.

당사의 사전적 위협 탐지 담당자, 분석가 및 대응자는 Cortex와 Unit 42의 독점 AI를 활용하여 신뢰성 높은 위협 인텔리전스를 제공하고 탐지, 조사 및 대응을 가속화합니다. 그 결과 MTTD와 MTTR이 최대 90%까지 감소했습니다. Cortex XDR 및 XSIA은 둘 다 문제를 진단하고 해결합니다. 맞춤형 임원 보고, 지속적인 태세 최적화, 공격 표면에 대한 통합된 보기를 통해 완벽한 가시성, 더 빠른 보호, 그리고 첨단 위협보다 앞서 나갈 수 있는 자신감을 얻을 수 있습니다.

## 공격을 받았다면 꼭 해야 할 일 5가지

1. **네트워크를 분리하세요**. 손상된 디바이스에 대한 네트워크 액세스를 비활성화하세요.
2. **재부팅하기 전에** 공격 정보의 위치를 신중하게 고려하세요. 때로는 메모리에서 암호화 키와 기타 공격 정보를 찾을 수도 있습니다.
3. **적절한 데이터 백업을 확인**하고 몸값을 지불하지 않을 경우 **조직에 발생할 수 있는 전반적인 위험을 파악하세요**.
4. No More Ransom 웹사이트(https://www.nomoreransom.org)에서 검색하여 **복호화 도구가 있는지 확인하세요**.
5. **사고 대응 계획(IRP)을 실행하거나 Palo Alto Networks Unit 42와 같은 IR 팀에 문의하세요**. Unit 42는 업계 최고의 위협 인텔리전스를 제공한다는 명성을 얻은 사이버 연구원과 사고 대응자로 구성된 엘리트 그룹입니다. 침해를 당했다고 생각되거나 긴급한 문제가 있는 경우 unit42-investigations@paloaltonetworks.com으로 이메일을 보내거나 아래 전화번호로 연락해 Unit 42 사고 대응팀에 문의하세요.
   - 북미 무료 전화: +1.866.486.4842 (+1.866.4.UNIT42)
   - EMEA: +31.20.299.3130
   - APAC: +65.6983.8730
   - 일본: +81.50.1790.0200

### 당장 랜섬웨어 방어 구축 시작하기

랜섬웨어 공격을 예방하고 침해가 발생했을 때 피해를 최소화하는 방법에 대한 자세한 내용을 알아보려면 온디맨드 웨비나 랜섬웨어 차단을 위한 모범 사례를 시청하고 2025년 1월~3월의 갈취 및 랜섬웨어 동향을 다운로드하세요.

랜섬웨어 공격에 대한 방어는 계획부터 시작됩니다. 랜섬웨어 준비성 평가를 통해 이 과정을 시작해 보세요.

## 최신정보 받아보기

앞서 살펴본 것처럼 랜섬웨어를 예방하려면 첨단 기술, 사전 예방 전략, 지속적인 경계를 결합한 다면적인 접근 방식이 필요합니다. AI 기반 공격, 정교한 다중 갈취 계획, 중요 인프라를 표적으로 삼는 점점 더 표적화된 캠페인 등으로 위협 환경은 계속해서 빠르게 진화하고 있습니다.

Cortex XDR 및 Cortex XSIAM에 대한 자세한 내용은 다음 리소스를 참조하세요.

### Cortex XDR

- 당사 웹페이지를 방문하세요.
- XDR For Dummies 가이드를 다운로드하세요.
- MITRE ATT&CK Enterprise 평가에서 당사의 탁월한 성과에 대해 알아보세요.

### Cortex XSIAM

- 당사 웹페이지를 방문하세요.
- 당사의 전자책 'Cortex XSIAM: 반응형 보안을 넘어선 AI 기반 SecOps 플랫폼'을 다운로드하세요.
- XSIAM 제품 투어를 둘러보세요.

Cortex 솔루션 포트폴리오에 대해 자세히 알아보려면 홈페이지를 방문하세요 .

### Unit 42 MDR

- 당사 웹페이지를 방문하세요.
- *2025 Frost Radar™: 글로벌 관리형 탐지 및 대응(MDR)* 보고서를 다운로드하세요.
- MDR 전문가와의 상담 전화 일정을 잡으세요.

## Cortex 소개

Palo Alto Networks의 Cortex는 조직에서 최신 보안 운영 센터(SOC) 환경을 제공할 수 있도록 보안 운영 솔루션을 새롭게 정의했습니다. Cortex는 머신 러닝과 Unit 42® 위협 인텔리전스를 기반으로 하는 통합 플랫폼에서 동급 최고의 위협 탐지, 예방, 공격 표면 관리 및 보안 자동화를 제공합니다. 전 세계 기업의 신뢰를 받고 주요 분석가 기업의 인정을 받은 Cortex XDR, Cortex XSOAR®, Cortex Xpanse® 및 Cortex XSIAM은 스탠드얼론 솔루션으로 검증된 보호 기능을 제공하며, SOC 전반에 걸쳐 역량 증폭기 역할로 함께 원활하게 작동합니다. Cortex에 대해 자세히 알아보려면 www.paloaltonetworks.com/cortex 사이트를 방문하세요.

3000 Tannery Way
Santa Clara, CA 95054

대표 전화: +1.408.753.4000
판매 문의: +1.866.320.4788
지원 문의: +1.866.898.9087

www.paloaltonetworks.com



cortex_wp_what-you-need-to-know-to-surve-ransomware_082225