DOOSAN cybereason

2024 글로벌 랜섬웨어 설문조사 리포트

'랜섬웨어'라는 단어 하나만으로 기업이 입은 사이버 공격 피해를 설명할 수 없습니다.

'랜섬웨어'는 데이터를 암호화한 후 액세스 권한을 대가로 돈을 갈취하는 행위라는 단순한 개념에서 시작되었습니다. 그러나 2000년대 초반에 복잡한 혼합 공격 형태로 진화했고 이제 ChatGPT의 등장으로 빠르게 고도화되고 있습니다.

2023년 설문 조사에서 비영어권 국가(이탈리아, 독일, 프랑스, 일본)를 상대로 한 랜섬웨어 공격이 눈에 띄게 증가한 이유도 생성형 AI에 있습니다. 공격자들이 생성형 AI 도구로 랜섬웨어 현지화가 간편해지면서 더 빠르고 더 많은 규모로 공격이 가능해졌기 때문입니다.

공격자들은 AI 도구로 개인과 회사에 대한 정보를 수집하여 소셜 엔지니어링 공격에 활용했고, 생성형 AI로 공격을 간편하게 코드화했습니다. 특히 웜GPT와 같은 피싱 AI로 공격 자동화도 가능해졌습니다.

올해 연구에 따르면 대부분의 기업이 랜섬웨어 대응 전략을 수립했지만 여전히 많은 기업의 보안이 불완전합니다. 공격에 플랜대로 대응하지 못하거나 이를 수행할 수 있는 보안 담당자가 부족한 현실입니다. 그 결과, 많은 조직이 해결방안으로 몸값 지불을 선택하고 있습니다. 게다가 많은 기업이 사이버 보험을 가입했지만 랜섬웨어 공격에 대해 보험 적용 여부 및 범위를 명확히 파악하지 못하고 있다는 사실도 드러났습니다.

몸값을 지불하는 것은 해결책이 아닙니다.

몸값을 지불했다고 해서 데이터 손상 없이 온전히 돌려받을 것이라는 보장은 없습니다. 데이터 시스템이 손상되어 돌아올 수도 있고, 이미 암시장에서 데이터가 거래되었을 수도 있습니다. 또한 다시 공격의 대상이 되지 않을 것이라는 보장도 없습니다. 그리고 만약 이 돈이 테러 혹은 범죄 조직의 지원금으로 사용되었을 경우 형사 고발을 당할 수 있습니다.

그렇다면 2024년에 우리가 주목해야 할 시사점은 무엇일까요?

위협은 계속해서 빠른 속도로 진화하고 있으며 기업은 이에 대응하기 위해 고군분투하고 있다는 것입니다. 기업은 보안 역량을 테스트하고, 사이버보안을 비즈니스의 핵심 요소로 여겨 오늘날 공격 뿐만 아니라 미래 공격까지 대비해야 합니다.

그렉 데이
글로벌 필드 CISO, Cybereason 부사장

contents

랜섬웨어 침해 사고가 주는 교훈

**정교해진 랜섬웨어 공격이 빈번하게 발생하면서 수많은 기업이 피해를 받고 있습니다.
랜섬웨어 침해 사고를 겪은 기업은 다음 사이버 보안 공격을 어떻게 대비하고 있을까요?**

1,008명

엔터프라이즈 IT 전문가를 대상으로 4가지 항목에 대해 조사했습니다.

- 공격자가 네트워크에 침입한 방법
- 랜섬웨어 침입으로 공격자가 탈취한 정보
- 랜섬웨어 사고 해결 방법으로 몸값 지불을 택한 기업 수
- 몸값을 지불할 만한 가치가 있었는지의 여부

설문 조사 대상은 모두 사이버 보안 담당자였습니다.

지난 2년 간

모든 기업이 한 번 이상 공격을 받았습니다.

설문조사 결과과거에 공격 당한 조직은 여전히 위험에 처해 있으며그 중 대부분의 조직이 다음 랜섬웨어 공격에 대비하지 못하고 있습니다.

설문 결과 한 눈에 보기

설문 결과 랜섬웨어를 경험한 보안 담당자 중 대다수는 아직 기업이 다음 랜섬웨어 공격에 대응하기에 보안 인력과 플랜이 부족하다고 밝혔습니다.

공격은 계속해서 진화합니다

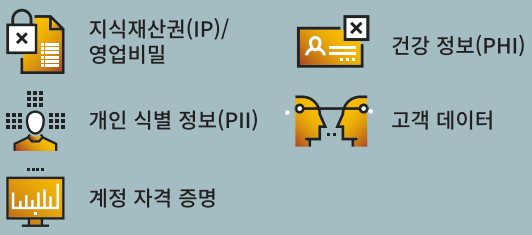
랜섬옵스의 더 복잡해진 로우 앤 슬로우 공격(매우 느린 속도로 트래픽 혹은 HTTP를 요청해 정상인 것처럼 위장해 탐지를 회피하는 공격)은 최대한 많은 네트워크를 손상시킨 후 높은 몸값을 요구합니다.

*랜섬옵스: 초기 침투부터 공격 이동, 페이로드 암호화까지 표적화해 공격하는 다단계 랜섬웨어

공격받은 기업 56% 는

3개월에서 길게는 1년까지 침해를 감지하지 못했습니다.

랜섬웨어로 공격자가 탈취한 정보



공격자는 어떻게 침입했을까요?

41% 공급망 파트너를 통해 들어왔고

24% 직접 침입했으며

22% 내부자의 도움을 받았습니다

몸값을 지불하는 것은 해결책이 아닙니다

대부분의 피해 기업이 몸값을 지불했지만 데이터 손상 없이 돌려받은 기업은 절반에 미치지 못합니다. 그리고 이 중 대부분은 1년 내에 다시 랜섬웨어 공격을 받았습니다.

84% 가 몸값을 지불했습니다.

그러나

47% 만이 데이터 및 서비스 손상 없이 돌려 받았습니다.

기업들은 왜 몸값을 지불했을까요?

이후

78% 는 다시 랜섬웨어 공격을 받았습니다.

그리고 그 중

63% 는 두번째 공격에서 더 많은 비용 지불 요구를 받았습니다.

82%는 1년 이내에 다시 침해를 당했습니다.
36%는 동일한 공격자에게 다시 침해 당했으며
42%는 새로운 공격자에게 공격받았습니다

DOOSAN

cybereason

기업이 겪는 진짜 피해는 막대합니다

공격자가 요구하는 높은 몸값 요구는 실제로 기업이 받는 피해의 빙산의 일각에 불과합니다.

46% 는

100만달러에서 1,000만 달러 사이의 피해를 받았습니다.

16% 는

1,000만 달러 이상의 손실을 입었습니다.

지난 24개월 간 지불된 국가별 평균 금액

미국	140만 달러
프랑스	100만 달러
독일	76.2만 달러
영국	42.3만 달러

아래 항목을 포함한 실제 피해는 막대합니다.

- 브랜드 가치 하락
- 매출 손실
- 비즈니스 임시 중단
- 고위 경영진의 사직
- 해고

기업은 보안 강화에 더 노력해야 합니다

대부분의 기업은 침해 이후 사이버 보안에 대한 투자를 늘렸지만 보안취약점은 여전히 존재합니다. 심지어 다음 공격에 잘 대비하고 있다고 답한 보안팀은 절반도 되지 않습니다.

87% 는

사이버 보안 관련 투자를 늘렸습니다.

그러나 **41%** 만이

보안 전문가를 확보했고 다음 공격에 대한 대응 플랜이 준비되어 있다고 답했습니다.

37% 는

보안 전문가는 있지만 수립된 보안 플랜이 없으며

18% 는

올바른 대응 플랜을 가지고 있지만 보안 담당자가 부족하다고 답했습니다.

기업은 다음 분야에 투자하고 있습니다.

1. 사이버 보안 전문가 확보
2. 보안 인식 교육
3. 최신 보안 기술 도입
   (예: 엔드포인트 기술 및 ID 서비스)
4. 내부/공급망 규정 준수 향상
5. 사이버 보험
6. 암호화폐 지갑

DOOSAN

cybereason

기업은 사이버 공격에 어떻게 대비해야 할까요?

공격자들은 생성형 AI와 머신러닝을 활용하여 새로운 공격 방법으로 네트워크에 침투하고 공격 영역을 확장하고 있습니다.

기업은 위협적인 사이버 공격 상황에서 6가지 핵심 과제를 직면하고 있습니다. 비즈니스가 각 과제에 대비하는 데 도움이 되는 방법을 소개합니다.

1/ 사이버 공격은 생성형 AI 등장으로 성공률이 더 높아졌습니다

기업이 AI로 비즈니스 생산성을 높이는 것처럼 공격자도 AI를 활용해 사이버 공격을 진화시키고 있습니다. ChatGPT 4.0과 같은 도구가 등장하면서 개인정보 수집이 쉬워지고 교묘한 피싱 메시지 작성도 가능해졌습니다. 또한 AI의 자연스러운 번역으로 공격은 더욱 정교화되고 있습니다.

AI 사이버 공격을 대비하세요!

모든 임직원이 AI 피싱 공격이 증가하고 있음을 인식하도록 교육해야 합니다. 보안 주의 사항 교육과 함께 정기적인 모의 훈련을 진행하고 모든 팀이 보안 규정을 따르고 있는지 확인해야 합니다.

또한 사이버 보안 파트너와 협력해 중요한 시스템과 데이터를 보호해야 합니다. 사이버리즌은 AI를 기반으로 랜섬웨어를 탐지하고 자동으로 대응하고 있습니다.

생성형 AI의 위험성

2023년 2월, 보안 회사 체크포인트(Checkpoint)는 챗봇의 API를 변경하여 멀웨어 코드를 생성하면 누구든지 손쉽게 바이러스를 생성할 수 있다는 사실을 발견했습니다.

팟캐스트에서 해당 사례를 더 자세히 들어보세요

2/ 기업 간 보안 역량의 격차는 더욱 벌어지고 있습니다

전 세계 사이버 보안 담당자의 역량 수준은 매우 높아졌지만 아직 수많은 기업들은 보안 전문가를 필요로 하고 있습니다.

기업들은 사이버 보안 담당자를 확보하기 위해 가장 많은 투자를 하고 있지만 모든 수요를 충족하기에 보안 전문가는 턱없이 부족합니다.

보안 업무를 효율화하세요!

현재 사이버 보안 담당자의 업무를 효율화는 것이 최우선적인 해결 방법입니다. 통합 관리, 자동화 대응 및 아웃소싱 등으로 보안 담당자의 업무 생산성을 증가시킬 수 있습니다.

사이버리즌은 경고가 아닌 운영 중심의 접근 방식으로 운영을 더욱 효율화하고 있습니다.

3/

레거시 시스템으로 네트워크 취약성이 증가하고 있습니다.

네트워크의 대부분을 클라우드로 마이그레이션하는 추세이지만, 중요한 시스템들은 오프라인으로 유지 중이거나 다크 네트워크에 남아 있습니다. 이 시스템들은 공격에 덜 노출될 것 같지만 사실 보호 수준이 매우 낮습니다. 또한 가장 취약한 링크를 찾기만 하면 한번에 물리적인 액세스 권한을 얻거나 비밀번호 액세스가 가능하기 때문에 소셜엔지니어링 공격의 주요 타겟이 되기도 합니다.

레거시 시스템 보안 수준을 높이세요!

오프라인 또는 폐쇄형 시스템 보호 수준을 높여야 합니다. 액세스를 제어하고, 비밀번호로 보호하고, 직원들에게 소셜 엔지니어링 공격에 대한 보안 교육을 실시해야 합니다. 가볍고 사용자 개입을 최소화하는 non-intosive 보안 솔루션을 제공할 수 있는 보안 파트너와 협력하면 보안 수준을 높일 수 있습니다.

> 세계 최초 원자력 발전소인 영국 셀라필드 해킹 공격도 외부 메모리 스틱 연결 등 레거시 시스템의 취약점에서 시작되었습니다.

4/

보험은 공격 일부를 완화해줍니다.

거의 모든 응답자가 사이버 보험에 가입했다고 응답했음에도 불구하고 이 중 40%만이 랜섬웨어 피해가 보장된다고 답했습니다. 실제로 보험금을 청구한 기업들 중 절반 정보만이 비용을 전액 보상받을 수 있었습니다.

사이버 보험 범위를 확인하세요!

사이버 보험은 사이버공격으로 인한 손실 및 손해로부터 기업을 보호합니다. 기업은 실제 침해 보상에 대해 사이버 보험 정책을 완전히 이해하고 있어야 합니다.

5/ 보안 담당자는 다음 공격 대비를 위해 플랜을 세워야 합니다.

기업은 랜섬웨어 침해 이후 또 다른 공격의 타깃이 될 가능성이 높음에도 불구하고 41%만이 다음 공격을 대비하고 있습니다. 이때 보안 격차는 사고 대응 프로세스에서 가장 큰 차이를 보입니다.

모의 훈련으로 보안을 테스트하세요!

현재 사용 가능한 리소스로 실행 가능한 범위에 집중해 보안을 강화해야 합니다. 가장 좋은 방법은 사고 대응 프로세스를 테스트하는 것입니다. 이때 사이버 보안 파트너와 협력해서 랜섬웨어 위험 평가를 수행하는 것도 도움이 됩니다. 평가는 랜섬웨어 공격을 시뮬레이션하고 정해진 보안 플랜대로 사람, 프로세스 및 기술적 측면을 테스트하는 '모의 훈련'으로 구성되어야 합니다. 테스트 결과를 활용해 기업은 리소스를 어떻게 활용할지 방향을 정할 수 있습니다.

6/ 몸값을 지불하는 것은 해결책이 아닙니다.

설문 응답자의 84%는 자신의 조직이 몸값을 지불했다고 답했습니다. 그러나 몸값을 지불한 대부분의 기업은 시스템과 데이터를 손상된 채로 돌려 받았습니다. 그리고 그 중 78%는 다시 랜섬웨어 공격을 받았고, 63%는 두번째 공격에서 더 많은 돈을 요구 받았습니다.

몸값 지불이 아니라 공격 예방에 노력하세요!

지난 2년간의 결과가 말해주듯 몸값을 지불하는 것은 보안 사고의 해결책이 아닙니다.
기업은 공격 후 해결하기 보다 공격 예방에 더 힘써야 합니다. 랜섬웨어 보안 기술을 보유한 사이버 보안 파트너와 협력하여 랜섬웨어 침해를 막아야합니다. 랜섬웨어 침해 시 잠재적 손실이 수백만 달러에 이를 것이라 예상되시나요? 그렇다면 하루 빨리 비즈니스 보호를 시작하세요.

결론: 몸값 지불은 해결책이 아닙니다.

이번 설문을 통해 랜섬웨어 공격자에게 수백만 달러를 지불하는 것은 해결책이 될 수 없음을 다시 한 번 확인했습니다. 몸값을 지불한다고 해서 시스템과 데이터가 손상되지 않았고, 암시장에서 거래되지 않았으며 더 이상 공격받지 않는다는 보장은 없습니다. 또한 설문 결과는 일단 약점이 한 번 드러나면 다시 공격받을 가능성이 높다는 사실도 보여줍니다. 기업은 랜섬웨어를 사전 예방해 비즈니스를 보호해야 하며 그러기 위해서는 우선 공격의 위험성과 영향을 이해하고 있어야 합니다.

이 설문 조사의 결과는 랜섬웨어 침해의 실제 위험과 피해를 이해하는데 도움을 줍니다. 이를 통해 랜섬웨어 대응 문제를 우선순위화하고 조직 보안을 강화하기 위해서 충분한 투자가 이루어져야 한다는 사실을 확인했습니다.

랜섬웨어 역량, 대응 플랜 및 기술에 투자하세요.

앞서 권장했던 모의 훈련으로 보호 및 대응 플랜의 약점을 식별할 수 있습니다. 전반적인 보안 기초를 보강하기 위해 사이버 보안 파트너사와 협력하는 것도 좋지만 시작 단계라면 아래 권장 사항을 먼저 참고하시기 바랍니다.

보안 전문가

랜섬웨어 보호 경험이 있는 사이버 보안 전문가를 고용하고 데이터 및 시스템 보호를 자동화하여 업무를 효율화하세요. 보안 운영은 아웃소싱을 통해 업무 시간 외 모니터링을 진행하고 공격 발견 시 초기 단계에서 자동으로 격리 조치를 하는 위협 탐지 및 대응 솔루션 도입으로 보안 격차를 해소해야 합니다.

프로세스

비즈니스 전략 및 방향성과 합의된 플랜으로 적절한 리소스를 투입하세요. 사이버 보안 플랜에는 이사회(의사 결정 책임), PR 및 마케팅(위기 관리 및 고객 커뮤니케이션 담당) 등 비즈니스의 모든 부서가 함께 참여해야 합니다. 그리고 정기적으로 보안 대응 프로세스를 테스트하는 것도 좋은 방법입니다.

기술

최신 기술에 투자하세요. 보안 기술 적용 범위가 온/오프라인 네트워크를 모두 포함하는지 확인해야 합니다. 또한 공격의 모든 단계에서 보호가 가능하고 최후의 대책으로 침해 받은 파일 롤백(되돌리기)이 가능한 랜섬웨어 보안 솔루션을 적용해야 합니다. 보안 파트너와 협력해 24x7x365 모니터링이 포함된 관리형 탐지 및 대응 서비스를 배포하여 공격이 언제 발생하든 즉시 공격을 탐지, 차단 및 해결할 수 있어야 합니다.

DOOSAN

cybereason

AI 기반 보안으로 비즈니스 보안을 강화하세요

사이버리즌은 다계층 보호, AI 기반 엔드포인트, 커널(운영체제 핵심 프로그램)부터 클라우드까지 포괄적인 가시성, 랜섬웨어 예측 보호 기능으로 사이버 보안 공격을 대비합니다. 연중무휴로 모니터링하며 보안 운영을 최적화할 뿐만 아니라 가장 빠르게 공격을 탐지, 분류 및 대응합니다.

사이버리즌의 APAC 대표 파트너 두산디지털이노베이션에 문의하세요

Contact. ddi.marketing@doosan.com

두산디지털이노베이션

두산디지털이노베이션은 사이버리즌의 APAC 대표 파트너로 사이버리즌 XDR을 제공해 클라우드 및 전체 엔터프라이즈 에코시스템을 공격으로부터 보호합니다.

AI 기반 사이버리즌 방어 플랫폼은 최신 랜섬웨어 및 고급 공격 기술에 대해 예측하고 예방, 탐지 및 대응합니다. 사이버리즌 MalOp™는 공격 영향을 받은 모든 장치, 사용자 및 시스템에 대해 빠른 속도와 정확성으로 공격 전체 맥락을 담은 인텔리전스를 즉시 제공합니다.

사이버리즌의 랜섬웨어 보호 역량

사이버리즌은 9개 계층으로 엔드포인트를 보호(EPP)하고 엔드포인트 탐지(EDR) 통합 기술 및 관리형 탐지 및 대응(MDR) 서비스를 결합해 가장 지능적인 랜섬웨어 공격까지 차단합니다.
평균적으로 위협 탐지에 1분, 공격 분류에 5분, 공격 차단에 30분 소요되며 이 결과는 휴일 및 근무시간 외 모든 시간에 발생한 공격을 포함한 평균 대응 시간입니다.

설문조사에 대해

이 설문조사는 2023년 9월 25일부터 10월 6일까지 직원이 500명 이상인 조직의 사이버 보안 전문가 총 1,008명을 대상으로 진행되었습니다. 설문 응답자 87%는 임직원 수 500-999명인 조직에 근무중이며 13% 는 임직원 1000명 이상 규모의 기업에서 근무하고 있습니다. 참가 국가는 미국, 영국, 프랑스, 독일이며 다양한 업종으로부터 답변을 받았습니다. IT 및 통신이 31%로 가장 높았고, 제조 및 유틸리티(13%)와 소매, 케이터링 및 레저(10%)가 그 뒤를 이었습니다. 기타 산업에는 건축, 엔지니어링 및 건축, 예술 및 문화, 교육, 의료, 법률, 운송 등이 포함되었습니다