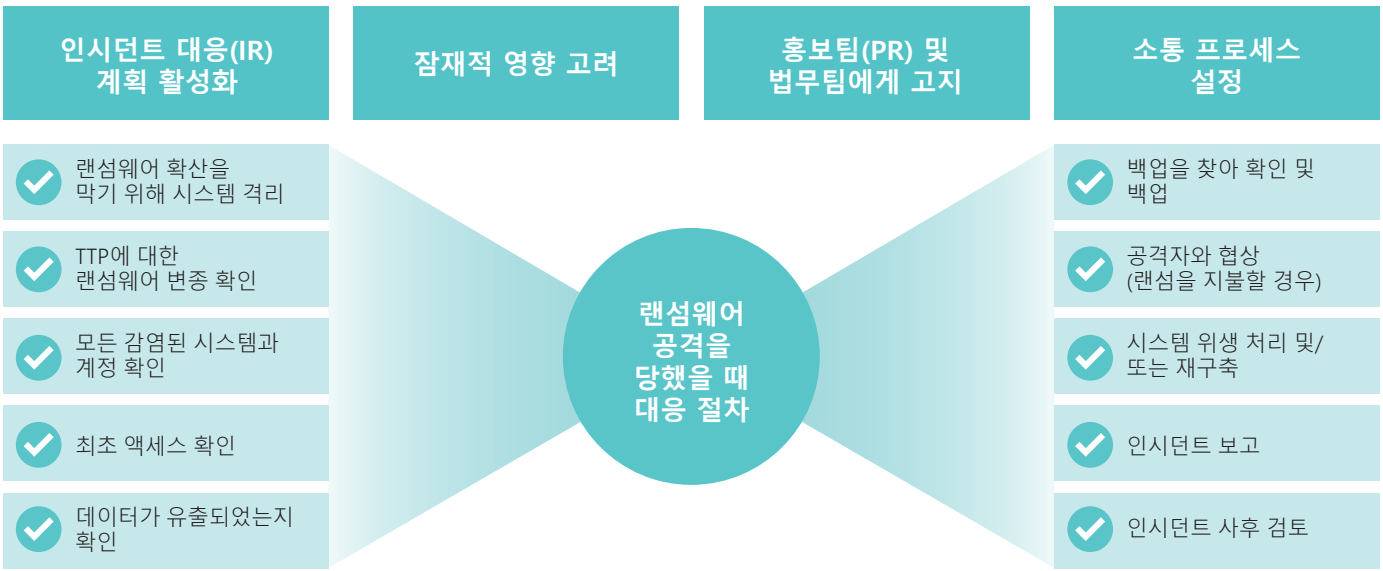
체크리스트

랜섬웨어 공격을 당했을 경우의 대처법



2019년에 1억 8,700만 건이 넘는 랜섬웨어 공격이 있었습니다. 이는 매일 기업에 50만 회가 넘는 공격이 발생하는 것과 같습니다. 아직 랜섬웨어 공격의 피해를 보지 않았다면 언젠가는 당하게 됩니다. 이미 랜섬웨어 공격을 당했다면 언젠가 또 당할 수도 있습니다. 그날이 오면 여러분, 팀, 회사에 미치는 영향을 최소화할 대책이 마련되어 있어야 합니다.

기업에서 랜섬웨어 공격을 당했을 때 취해야 할 조치를 간단히 설명하면 아래와 같습니다.

랜섬웨어 공격을 당했을 때 대응 절차

첫째: 당황하지 마세요!

- 빠르지만, 체계적인 행동이 필요합니다. 계획된 인시던트 대응(IR) 절차가 있다면 차분하게 실행하세요. 아직 절차를 마련하지 못했다면, 다음과 같은 가이드라인이 도움이 될 수 있습니다. 아니면, 보안 공급업체에 도움을 청하세요. 인시던트를 보험사에 알리는 것도 좋습니다. 보험사는 이런 상황에 도움을 제공하는 훈련을 받은 전문가들이 있어서 이들 중에서 선택할 수도 있습니다.

- 보안 인시던트의 잠재적 영향을 생각하세요. 이미 피해를 본 영역(예: 데이터 암호화, 애플리케이션 사용 중단)뿐만 아니라, 잠재적으로 피해를 볼 수 있는 추가 영역을 고려합니다.

- 사내 홍보팀과 법무팀이 대비를 시작할 수 있도록 알리세요. 이들에게 알리면 여러분이 추가 정보를 수집하는 동안 더욱 공식적인 소통 및 보고 구조를 세울 것입니다.

- 소통 방법을 결정하고, 각 사업부의 담당자 연락처로 프로토콜을 업데이트합니다. 예를 들어 3시간마다 모든 관련 팀 책임자에게 상황에 대해 알립니다. 사람들이 끊임없이 업데이트를 요구해서 팀이 인시던트 해결에 집중하지 못하게 되는 상황을 막는 데 중요한 절차입니다.

시스템 격리 및 확산 중단

- 위협이 확산되지 못하도록 격리하는 방법은 여러 옵션이 있습니다. 인시던트가 이미 광범위하게 확산되었다면 네트워크 수준에서 차단을 적용하거나(예: 스위치나 방화벽 엣지에서 트래픽 격리) 임시로 인터넷 연결을 중단합니다. 인스턴트 범위가 좁고 몇 개의 시스템만 감염된 것이 확인되었다면, 이더넷이나 Wi-Fi 연결을 끊어서 기기 수준에서 격리할 수도 있습니다. 엔드포인트 탐지 및 대응(EDR) 등의 기술을 사용할 수 있다면 더욱 정밀하게 프로세스 수준에서 공격을 차단할 수 있습니다. 비즈니스에 미치는 영향을 최소화하는 가장 좋은 즉각적 옵션입니다. 포렌식 증거가 손실되지 않도록 모든 시스템이 계속 작동하도록 하는 것을 잊지 마세요. 공격자의 활동을 차단하면, 공격자가 눈치채고 움직이지 않아서 전체 공격 범위를 찾아내기 어려울 수 있습니다.

- 상황에 따라, 감염된 시스템의 데이터 드라이브와 메모리의 포렌식 이미지를 캡처합니다. 그러나 한 번도 해본 적이 없다면 시도하지 마세요. 팀원들이 아무리 자신감이 넘쳐도, 이럴 때 첫 시도를 해서는 안 됩니다.

온라인 또는 클라우드 도구를 사용하고 있다면 업로드하는 문서를 공공 단체에 검토받을 수도 있습니다.

랜섬웨어 변종 식별

- 공격 전략, 기술, 절차(TTP) 대부분은 각 랜섬웨어 변종에 대해 공개적으로 기록되어 있습니다. 어떤 공격에 맞서고 있는지 알면 어디서 위협을 찾고, 위협이 어떻게 확산되는지 실마리를 얻고 잔존공격에 대한 자세한 정보를 파악할 수 있습니다.

- 변종에 따라서 랜섬웨어에 감염된 파일을 해독할 수 있는 암호 해독 도구가 존재할 수도 있습니다. No More Ransom 웹사이트에 암호 해독 도구를 찾을 수 있는 좋은 참고 자료가 나와 있습니다. 랜섬웨어 노트 자체로도 랜섬웨어 그룹 및/또는 변종에 대해 알려주는 지표가 됩니다. 또한, 랜섬웨어를 ID Ransomware에 업로드하면 변종을 찾는 데 도움이 될 수도 있습니다.

- 온라인 또는 클라우드 도구를 사용하고 있다면 업로드하는 문서를 공공 단체에 검토 받을 수도 있습니다.

최초 액세스 식별

- 최초 액세스 지점, 또는 최초 감염자를 찾으면 보안의 구멍을 메우는 데 도움이 됩니다. 일반적인 최초 액세스 벡터는 피싱, 엣지 서비스 익스플로잇(예: Remote Desktop services), 무단 자격 검증 사용입니다. 그 외에 다른 최초 액세스 벡터로는 드라이브 바이 해킹, 공개 웹사이트 및 애플리케이션 익스플로잇, 이동식 미디어, 추가된 하드웨어, 공급망 해킹이 있습니다.

- 이런 조치가 어려울 때도 있지만, 디지털 포렌식이나 IR 전문가, 컨설턴트의 전문성을 빌려 최초 액세스 지점을 찾아야 할 수도 있습니다.

모든 감염된 시스템과 계정 확인(범위)

- 공격이 끝난 이후에도 공격자가 여전히 네트워크에 발을 담그고 있을 수 있습니다. C2 서버와 아직 통신 중인 활성 멀웨어나 잔류물을 찾아내는 것이 중요합니다. 일반적인 기술은 다음과 같습니다.
  - 악성 페이로드를 실행하는 새 프로세스 생성
  - 레지스트리 키 사용
  - 새로 예약된 작업 생성

- 게다가 공격자는 권한이 있든 없든 여러 계정(예: Active Directory (AD) 계정)을 해킹했을 가능성이 크므로 해당 계정을 비활성화합니다. 그 과정에서 새로운 악성 계정이 생성되지 않도록 합니다. 다른 AD 구성 요소(예: Group Policy Object(GPO))는 새로 생성되었거나 수정된 개체가 있는지 검토하여 확인해야 합니다. 이는 공격자가 랜섬웨어 페이로드를 모든 시스템에 내보낼 때 사용하는 일반적 전략입니다.

- 조치를 취하기 전에 조사 결과를 기록합니다. 실제 조치를 취하면 공격자가 경계하게 되고, 훨씬 심각한 공격을 가하게 될 수 있습니다. 데이터를 복구하거나 데이터 침해의 완전한 영향을 파악하기 어려울 수 있습니다.

대부분의 경우, 공격자는 온라인 백업을 손상하려 할 것입니다. 백업이 존재하는지 확인하고, 데이터가 정확하고 복구 가능한지 확인하세요.

데이터가 유출되었는지 확인

- 랜섬웨어 공격은 파일을 암호화하고 데이터를 유출하기까지 하는 경우가 많습니다. 독점 정보 또는 수치스러운 데이터를 온라인에 공개하겠다고 위협하여 랜섬을 얻어낼 가능성을 높이기 위해서입니다. 데이터 유출의 징후(예: 대규모 데이터 전송)를 방화벽 엣지 기기에서 찾습니다. 또한, 서버에서 클라우드 스토리지 애플리케이션(예: Dropbox, AWS)으로 나가는 수상한 통신을 찾습니다. 클라우드 액세스 보안 브로커(CASB) 솔루션이 있다면 방화벽 로그와 함께 여기에서 주로 정보를 확인하면 됩니다.

- 이 절차도 어려울 수 있는데, 디지털 포렌식 팀이나 IR 전문 컨설턴트를 데려와 더욱 철저한 조사가 필요한 상황이 생길 수도 있습니다.

백업을 찾아서 사용 가능한지 확인

- 랜섬웨어 공격은 온라인 백업과 볼륨 섀도 사본을 삭제하여 여러분이 데이터를 복구하고, 나아가서는 랜섬을 지불하지 않게 되는 가능성을 낮추려고 합니다. 따라서 백업 기술이 인시던트에 영향을 받지 않았고, 아직 사용 가능한지 확인해야 합니다. 그리고 복구에 사용할 수 있는 온라인/오프라인 백업이 있는지 확인합니다.

- 대부분의 경우, 공격자는 온라인 백업을 손상하려 할 것입니다. 백업이 존재하는지 확인하고, 데이터가 정확하고 복구 가능한지 확인하세요.

백업의 무결성을 확인하고 마지막으로 알려진 정상 상태로 복구

- 공격자는 여러 번 랜섬웨어 공격을 감행하면서 네트워크에 며칠, 길면 몇 주씩 머무르다가 파일을 암호화하기로 결정합니다. 즉, 악성 페이로드가 있는 백업이 남아 있을 수 있으며 이 백업을 사용하여 깨끗한 시스템으로 복구해서는 안 됩니다. 인시던트를 조사하는 동안 최초 액세스 날짜와 시간이 언제인지 알아내야 합니다. 그런 다음, 그 이전의 날짜에서 복구해야 합니다. 어느 쪽이든 백업을 스캔해서 문제가 없는지 확인해야 합니다.

시스템 위생 처리 또는 새로운 빌드 생성

- 시스템에 잔류한 모든 활동 중인 멀웨어나 인시던트를 찾아내는 능력에 자신감이 있다면 시스템을 다시 빌드하는 시간을 절약할 수 있습니다. 그러나 새로운 깨끗한 시스템을 만드는 것이 더 쉽고 안전할 수 있습니다. 완전히 별도의 깨끗한 환경을 빌드하여 마이그레이션하는 방법도 생각해볼 수 있습니다. 가상 환경을 설정한다면 그리 오래 걸리지 않을 것입니다. 네트워크나 네트워크 망분리를 다시 설계하거나 처리할 때 보안 컨트롤을 설치하고, 모범 사례를 준수하여 기기가 다시 감염되지 않도록 하세요.

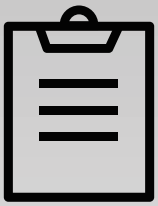
인시던트 보고

- 이제 법무팀을 다시 방문할 시간입니다. 모든 팀(예: 법무팀, 보험사)에게 보고하는 것이 중요합니다. 또한, 법 집행 기관에 대한 신고가 필수이자 의무라는 것을 알아야 합니다.

- 공격을 공개할지 결정합니다. 때에 따라서 네트워크에 대한 일부 또는 모든 정보를 공개해야 할 법적 의무가 있을 수도 있습니다. 필요할 경우, 공격을 공개해야 하는 시점을 확인하세요. 침해된 데이터를 확인하고 난 후, 법무팀에서 이와 같은 조사에 도움을 줄 수 있습니다. 법 집행 기관에 공격에 대해 알리면 공개 기록이 남고, 일반에 공개하더라도 마찬가지일 수 있습니다.

- 심각한 공격이고 여러 지역에서 비즈니스를 운영하고 있으면, 지역/지방 법 집행 기관이 아니라 국가적 법 집행 기관에 연락할 필요가 있습니다.

- 상황에 따라서, 법 집행 기관에 연락하는 것이 유리할 수 있습니다. 특히, 이들이 보안 인시던트를 해결하는 데 추가적 리소스를 제공해줄 수도 있습니다. 데이터가 유출되었다면 이를 찾는 데 도움을 받을 수도 있습니다. 게다가 경찰 조서를 제출하면 사이버 보험에 필요한 증빙 자료가 될 수 있습니다. (법무팀에서 필요성을 결정해야 합니다.)



대부분의 경우, 공격자는 온라인 백업을 손상하려 할 것입니다. 백업이 존재하는지 확인하고, 데이터가 정확하고 복구 가능한지 확인하세요.

랜섬을 지불하려고 하시나요? 먼저 협상하세요.

- 법 집행 기관은 랜섬을 지불하는 곳을 좋게 보지 않습니다. 하지만 랜섬을 지불할 생각이라면 랜섬을 낮추는 전문 협상 기술이 있는 보안 회사를 고용해야 합니다. 악의적 행위자는 대개 협상 의지가 있습니다. 법무팀이나 외부 자문이 추천 협상자 명단을 보유하고 있는 경우가 많으니 그 중에서 선택하면 됩니다.

- 랜섬 협상에는 시간이 걸린다는 것을 기억하세요. 협상은 데이터를 되돌려받는 것이 목적입니다. 또한, 공격자와 협상하더라도 데이터가 삭제되지 않거나 데이터가 공개되지 않는다는 보장은 없습니다.

- 협상을 할 때 공격자가 데이터를 훔쳤다고 주장할 경우, 훔친 데이터의 검증 가능한 샘플(예: 디렉터리 구조)을 제공해달라고 요청하세요. 일반적으로 증거를 제공해줄 겁니다.

- 랜섬을 지불하더라도 공격자가 익스플로잇한 취약성이 해결되지는 않으므로, 최초 액세스를 찾아 취약성을 패치해야 합니다.

인시던트 사후 검토

- 군에는 이런 격언이 있습니다. "적과의 대면에서 계획은 아무 소용이 없다." 완벽한 계획은 없습니다. 특히, 실제 환경에서 검증을 거치지 않았다면 더욱 그렇습니다. 그래서 인시던트 대응을 검토하여 어떻게 적절한 조치를 했는지 파악하고, 개선할 부분을 기록해야 합니다. 이런 "교훈"을 기록하는 단계는 대응과 복구 역량을 지속적으로 개선하는 데 도움이 됩니다. 이 검토는 복구 단계가 끝난 후 모든 사람의 기억이 생생할 때 최대한 빨리 실행하는 것이 좋습니다.

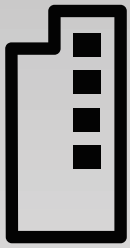
- 전체 공격 표면을 평가하고 누락된 보안 컨트롤이 있는지 확인하는 것이 좋습니다. 이런 외부 컨설턴트는 공통적인 프레임워크(예: National Institute of Standards and Technology(NIST))를 활용하므로 진행 상황을 측정할 기준이 생기게 됩니다.

누구나 공격을 받습니다. 누구나 계획이 필요합니다. 오늘 바로 시작하세요.

- 랜섬웨어 공격을 받아서 이 체크리스트를 읽고 계신다면, 이 절차를 신중하게 따르세요. 특히, 첫 번째 절차가 중요합니다. 당황하면 실수를 하게 되고, 문제를 악화시킬 수 있습니다. 도움을 줄 전문가가 있다는 것을 기억하세요.

- 이와 같은 절차는 기본에 불과합니다. 계획하고 기록할 것이 많습니다. 예를 들어, 중요 대응팀을 찾아내고, 누가 무엇을 하는지 파악하고, 보고 계통을 수립하고, 대변인을 지정하고, 중요한 복구 리소스를 만들어 분리하고, 네트워크 외부에 효과적인 백업 구축이 필요합니다.

- 도움을 줄 수 있는 기관이 많이 있습니다. 먼저 가장 신뢰하는 보안 공급업체와 상의하세요. 대부분 네트워크 테스트, IR 계획 수립, 포렌식 및 복구 서비스를 제공할 전문팀이 준비되어 있습니다. 하지만 어떤 조치를 하든, 기다리지 마세요. 여러분의 기업을 노리는 사이버 범죄자들은 바로 그것을 원합니다.



도움을 줄 수 있는 기관이 많이 있습니다. 먼저 가장 신뢰하는 보안 공급업체와 상의하세요.

면책: 이 문서에 언급된 외부 웹사이트와 이들이 제공하는 정보는 FortiGuard Labs에서 신뢰도를 보장하지 않습니다. 그러나 이들은 당사에 독립적인 검증을 받지 않았으며, 이러한 인용이 어떤 종류의 승인을 의미하는 것은 아닙니다.

FORTINET

www.fortinet.com/kr

서울특별시 강남구 영동대로 325 에스타워 14 /15층 **전화:** 080-559-8989 **Email:** kr-callcenter@fortinet.com

863720-A-0-KR