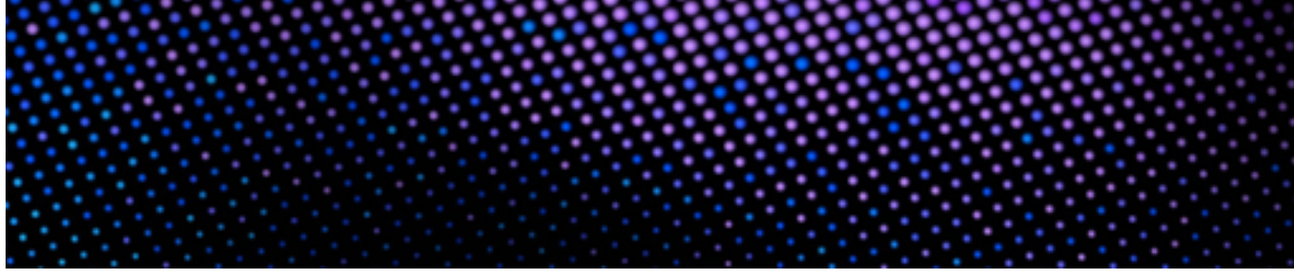
X-Force

랜섬웨어 가이드 완결판: 대비, 대응 및 교정

랜섬웨어 공격 방식 및 효과적인 위험 완화 기술 집중 조명

IBM Security

목차



개요

랜섬웨어란 사이버 범죄자가 데이터를 암호화하거나 훔쳐낸 다음 데이터 복구에 대한 대가를 요구하는 온라인 공격 유형입니다.

지난 10년간 '랜섬웨어' 범주에 해당하는 공격의 양상은 소비자를 대상으로 안티바이러스 제품인 것처럼 속이는 수준에 머무르지 않고 이제는 공공 기관 및 민간 기업을 주요 표적으로 삼으면서 첨단 암호화 기능을 활용하는 고도로 지능화된 악성 코드로 발전했습니다. 위협 인텔리전스가 어느 시점에 어떤 조직이 주요 표적이 될 수 있는지를 밝히는 데 도움이 되기는 하나, 업종, 지역, 규모에 관계없이 누구도 안전하지 않습니다.

랜섬웨어의 침투 범위가 점점 확대되면서 데이터 복구를 위해 지불해야 하는 금액도 증가하고 있습니다. 예전에는 총액이 두 자릿수였다면, 지금은 수백만, 수천만 달러에 달합니다. 기업을 겨냥한 공격자들이 데이터를 풀어주는 대가로 무려 4천만 ~ 8천만 달러를 요구하는 경우도 있습니다.

랜섬웨어의 제3의 축이라 할 수 있는 갈취 수법도 진화했습니다. 공격자들이 비즈니스 모델까지 동원하여 피해자들에게 몸값 지불을 강요합니다. 피해자가 주어진 기한 내에 지불하지 않으면, 범죄자는 공격의 수위를 높이고 기밀 데이터를 공개하겠다고 위협합니다. 심지어 다크 웹에서 경매에 부쳐 최고가에 낙찰하는 경우도 있습니다. 또 다른 한편에서는 랜섬웨어가 파괴형 공격과 융합하는 형태로 발전합니다. 즉, 몸값을 지불하면 데이터를 돌려주겠다고 주장하지만, 진짜 목적은 파괴 및 가동 중단에 있는 것입니다.

랜섬웨어는 뱅킹 트로이 목마, 피싱, DDoS, 크립토재킹 등 오랜 역사를 자랑하는 쟁쟁한 라이벌들을 제치고 오늘날 최강의 사이버 범죄 비즈니스 모델로 자리잡았습니다. 세계 각지의 기업이 랜섬웨어의 공격을 받으면서 총 피해 규모도 수십억 달러에 육박합니다. 설상가상으로, 랜섬웨어는 우리의 삶 자체를 위협하기 시작했습니다.

정보에 근거한 현명한 대응이 절실

랜섬웨어 공격이 발견되면 일분일초가 중요합니다. 아무런 조치도 하지 않으면, 시간은 공격자의 편입니다. 점차 더 많은 데이터와 파일이 암호화되고 더 많은 디바이스가 감염되어 결국 막대한 비용과 피해가 발생하게 됩니다. 즉각적이면서도 정보에 근거한 체계적인 조치가 이루어져야 합니다.

IT 보안 팀에 알려 랜섬웨어에 맞서기 위해 마련한 사고 대응 프로세스를 시작하게 하는 것이 급선무입니다. 외부 업체와 리테이너 계약을 체결했다면 이 업체도 참여시키는 것이 좋습니다.

그 밖에도, 회사가 영업 중인 지역의 요건에 따라, 중앙 정부 내 법 집행 기관 및 감독 기관에 연락하는 것도 고려해야 합니다.

본 가이드 소개

본 자료는 두 가지 목적을 위해 제작되었습니다.

1. **CISO의 관점에서 랜섬웨어의 역사 및 현황을 개괄적으로 살펴보고, 조직의 방어 체계를 강화하는 데 도움이 될 리소스를 소개합니다.**
2. **기술적 관점에서 공격이 일어나기 전에 네트워크를 보호할 방법 및 공격자가 방어선을 뚫었을 경우 효과적으로 복구하기 위한 전략을 검토합니다.**

여러 섹션으로 나누어 공격 전/중/후 단계를 다루겠지만, 그중에서도 초기 대응 섹션에서 가장 중요하고 시급한 조치에 관해 알아볼 것입니다.

현재 랜섬웨어 사고를 겪고 있다면, 당장 사고 대응: 억제 섹션부터 읽어보십시오. 나중에 나머지 섹션도 살펴보면서 랜섬웨어 공격에 관한 종합적인 배경 정보를 얻을 수 있습니다.

본 가이드의 여러 섹션에서 언급되는 IBM Security X-Force 리소스의 출처는 마지막에 요약 정리되어 있으므로 참고하시기 바랍니다.

정의

악성 코드의 변종 및 버전

본 가이드에서 사용하는 용어, 악성 코드 '버전' 및 '변종'은 다음과 같은 의미를 갖습니다.

- **'버전(version)'은 동일한 악성 코드 프로그램을 의미합니다. 이 동일한 프로그램의 새로운 버전과 오래된 버전에는 기능의 차이가 있습니다.**
- **'변종(variant)'은 각기 다른 랜섬웨어 '계열'을 구별하여 설명하는 데 쓰입니다.**

예컨대 사용자의 파일을 암호화한 다음 몸값을 요구하는 랜섬웨어에는 여러 *변종*이 있습니다. 이러한 *변종*은 대개 각기 다른 그룹에 의해 만들어지고, 안티바이러스 회사에 의해 각기 다른 이름으로 명명됩니다. 그리고 고유한 기능을 포함하지만, 그 궁극적인 목표는 동일합니다. 각 *변종*에는 여러 *버전*이 있을 수 있습니다. 시간이 흐르면서 *버전*이 업그레이드되어 새로운 특징과 기능이 추가됩니다.

랜섬웨어 감염 – 일상의 위험

IBM Security X-Force의 조사에 따르면, 랜섬웨어 공격을 받았다는 고객의 수가 빠르게 증가했습니다. 안타깝게도 랜섬웨어 감염은 매우 쉽게 이루어집니다. 직원이 자신도 모르는 사이에 지능적인 이메일의 속임수에 넘어가 회사 네트워크에 연결된 디바이스에서 악성 코드를 실행하면서 감염이 시작되는 경우가 대부분입니다.

일반적으로 랜섬웨어는 본인이 요청하지 않은 (알려졌거나 알려지지 않은 발신자가 보낸) 이메일의 첨부 파일 형태로 피해자에게 배포됩니다. 웹 브라우저 취약점을 통해 사용자 브라우저의 세션에 주입되기도 합니다. 공격자는 이러한 취약점을 노리는 각종 익스플로잇 툴을 활용하여 시스템을 감염시키고 "웹 쉘(web-shells)", "백도어(backdoors)" 심지어 원격 접근 트로이 목마까지 심어 놓습니다. 이를 통해 피해자의 시스템 및 네트워크 인프라를 추가로 감염시킬 수 있습니다. 공격자는 침투한 네트워크에서 초기 거점을 확보한 다음 내부망 이동 및 권한 상승의 수법을 구사하면서 궁극적으로 최대한 많은 디바이스에 랜섬웨어를 배포합니다.

일반적으로 초기 감염이 이런 식으로 발생하므로, 직원 교육이 예방 활동의 핵심 요소가 되어야 합니다.

저마다 다른 랜섬웨어

랜섬웨어 공격에 쓰이는 악성 코드는 2015년부터 빠르게 진화하기 시작했고, 새로운 악성 코드 계열 및 조직화된 사이버 범죄 신디케이트도 랜섬웨어의 무대에 등장했습니다. 최신 랜섬웨어 대부분이 강력하고 대개는 불가역적인 암호화 기술을 사용하지만, 모든 랜섬웨어가 똑같지는 않습니다.

여느 사이버 범죄 활동과 마찬가지로, 기술적 기량은 공격자의 기술과 정교함의 정도에 따라 달라집니다. 해독 키가 없으면 물리칠 수 없는 공격이 있는가 하면, 상대적으로 드물지만 범죄자에게 몸값을 주지 않고도 리버스 엔지니어링을 통해 해결 가능한 경우도 있습니다.

어떤 공격에서 해독 키로 악성 코드를 완화할 수 있는지, 아니면 리버스 엔지니어링으로 해결할 수 있는지 여부를 파악하는 것이 중요합니다. 이러한 정보를 활용하여 감염 대응 방안을 결정할 뿐만 아니라 각 팀에서 운영 정상화를 더 정확히 예측할 수 있습니다. 아울러 공격자와의 협상 또는 협상 거부의 모든 영역에서도 더 현명한 의사결정이 가능해집니다.

관리자 권한 불필요

랜섬웨어 공격은 금방 시스템 전체에 타격을 줄 수 있는데, 여느 악성 코드와 달리 관리자 권한이 필요하지 않는 경우가 대부분이기 때문입니다. 가장 기본적인 단계의 사용자가 지정된 네트워크 디바이스에서 사용하는 권한 수준만 있으면 됩니다. 네트워크를 통해 침투하는 랜섬웨어 공격은 기업의 파일 공유 서버에 악성 코드를 심어 둔 다음, 별 다른 작업 없이 이 저장 폴더를 이용하여 다른 사용자 디바이스로 이동하는 것으로 알려져 있습니다.

따라서 수많은 직원이 매일 네트워크에 접근해야 하는 기업일수록 랜섬웨어 위협에 매우 취약해집니다. 랜섬웨어 공격 예방이 결코 쉬운 일은 아니지만, 위험을 줄이거나 최소화할 수 있으며, 만약 네트워크에 침투했더라도 더 효과적으로 공격을 억제하는 것이 가능합니다.

일반적인 랜섬웨어 활동

어떤 컴퓨터가 랜섬웨어에 감염된 경우, 이 악성 코드가 C&C 서버(C2)에 암호화된 시스템 정보를 보내면서 네트워크 트래픽이 발생할 수 있습니다. 그러나 C2와의 통신이 암호화의 필수 조건은 아닙니다. 최신 랜섬웨어는 대개 암호화에 필요한 공개 키를 가지고 있습니다. 즉, 원격 서버에서 가져오지 않고 이 로컬 키를 사용합니다. 먼저 C2 노드에 연결하여 암호화에 필요한 키를 가져와야 하는 랜섬웨어의 경우, C2에 연결하지 못하면 실패할 가능성이 더 큽니다. 이러한 활동도 소기의 목적을 달성하기 전에 탐지할 수 있습니다.

랜섬웨어 변종 대부분에서 흔히 보여주는 또 다른 활동은 파일 암호화에 방해가 될 만한 각종 하드 코딩 프로세스/서비스, 이를테면 데이터베이스, 보안 애플리케이션, 백업 서비스를 종료하는 것입니다. 알려진 안티바이러스 프로그램 또는 기타 보안 애플리케이션을 찾아낸 다음 제거를 시도하는 변종도 있습니다.

운영 체제가 실행하는 시스템 복원 기능을 차단하고 비활성화하는 것도 대표적인 활동입니다. 많은 변종들이 볼륨 섀도 복사본 삭제, 빈 공간 지우기, 이벤트 로그 지우기, 시스템 복원 기능 비활성화 등의 태스크를 하나 이상 수행하는 명령을 실행합니다.

랜섬웨어 변종 대부분은 주로 개별 사용자 디바이스에 침투하므로, 운영 체제에서 컴퓨터를 정상적으로 작동하기 위해 사용하는 파일이 아니라 사용자가 흔히 생성하고 사용하는 파일을 암호화 대상으로 선택합니다. 피해자가 몸값 지불을 선택하게끔 컴퓨터가 계속 작동하게 하는 데 목적이 있습니다.

암호화 대상이 되는 파일 유형은 같은 랜섬웨어에서도 버전에 따라, 그리고 변종에 따라 달라질 수 있는데, 대개는 다음 범주의 파일을 포함합니다.

1. Microsoft Office 파일(.doc, .docx, .xls, .xlsx, .ppt, .pptx, .rtf)
2. Open Office 파일(.odt, .ods, .odp)
3. Adobe PDF 파일
4. 흔히 볼 수 있는 이미지 파일(.JPG, .PNG, 원본 카메라 파일 등)
5. ext 파일(.txt, .RTF 등)
6. 데이터베이스 파일(.sql, .dba, .mdb, .odb,. db3, .sqlite3 등)
7. 압축 파일(.zip, .rar, .7z 등)
8. 메일 파일(.pst)
9. 키 파일(.pem, .crt 등)

여기에 소개되지 않은 파일도 있습니다. 어떤 랜섬웨어 변종은 150가지 이상의 파일 유형을 타깃으로 삼으며, 공격자의 동기에 따라 차츰 달라질 수 있습니다.

파괴적 랜섬웨어 공격

대부분 랜섬웨어 공격이 경제적 동기에서 비롯된 듯하지만, 다른 의도를 가진 공격자도 있습니다. 처음에는 랜섬웨어 공격처럼 보였으나, 실제로는 디지털 자산 및 데이터를 (온전한 상태로 정당한 소유자에게 돌려주지 않고) 파괴하는 데 목적을 둔 공격일 수도 있습니다.

파괴적 공격에서는 악성 코드를 사용하여 시스템 구성요소를 지우고, 데이터를 손상하며, 기업의 디바이스를 작동 불능 상태로 만듭니다.

그간 파괴적 악성 코드는 국가/정부의 후원을 받는 지능형 공격자가 주로 사용하는 수단으로 헤드라인에 실리곤 했습니다. 그러나 IBM Security X-Force에서 사고 대응 데이터를 새롭게 분석한 바에 따르면, 이 공격은 사이버 범죄자/공격자 사이에서 점점 더 큰 인기를 누리고 있습니다. 몸값을 요구받은 피해자에 대한 압박 강도를 높이고자 와이퍼(wiper) 요소를 포함하는 랜섬웨어 공격도 있습니다.

실제로 IBM Security X-Force 사고 대응 팀은 2019년 상반기에 파괴적 공격의 양이 2018년 하반기보다 무려 200% 늘어난 사실을 확인했습니다.

파괴적 악성 코드 공격의 진화 추이로 미루어 보건대, 랜섬웨어 공격에 대비하려는 기업은 재해 복구 계획도 고려할 필요가 있습니다. 특히 비즈니스 연속성 및 핵심 업무에 미칠 영향을 염두에 두어야 합니다.

랜섬웨어를 통한 데이터 유출

지난 5년간 무서운 상승세를 보여준 또 하나의 새로운 랜섬웨어 공격 모델로 **혼합 공격 모드(blended attack mode)**가 있습니다. 파일을 암호화하고 대가를 요구하는 전형적인 랜섬웨어 공격으로 시작합니다. 하지만 그 배후에서는 공격자가 이미 피해자의 데이터를 빼낸 상태입니다. 상대가 몸값 지불에 응하지 않으면 공격자는 데이터를 공개하거나 온라인 경매에 부치겠다고 위협합니다.

이러한 랜섬웨어 공격은 순식간에 전면적인 데이터 유출 사태로 전개되어 피해 기업이 암호화된 데이터 및 운영 중단으로 고전할 뿐만 아니라 규정 위반 및 이미지 실추까지 감수해야 할 수도 있습니다.

이러한 혼합 공격이 백업 전략을 무용지물로 만들기도 합니다. 백업이 있더라도 피해자가 갈취당하는 것을 막을 수 없기 때문입니다. 혼합 공격을 당하는 기업이 엄청난 압박감을 느껴 몸값을 지불할 가능성도 있으나, 여전히 상당수는 그러한 요구에 굴복하지 않고 스스로 복구하기 위한 대응 계획을 마련하고 이행하는 것을 선호합니다.

최종 사용자: 1차 방어선

랜섬웨어가 실행되면, 정보 시스템이 감염되었음을 알리는 여러 명확한 징후가 나타납니다(사고 대응: 탐지 섹션 참조). 최종 사용자는 연락할 곳, 그리고 이상 징후를 신속하게 신고할 방법을 알고 있어야 합니다.

직원 교육이 매우 중요합니다. 예컨대 어떤 직원이 랜섬웨어에 의해 암호화된 파일, 또는 대부분 공격자가 몸값 지불 방법을 사용자에게 알리기 위해 남겨 놓는 HTML/TXT 파일을 발견할 경우, 이 직원이 잠재적 랜섬웨어 활동을 인식하는 방법은 물론 조직 내에서 당장 도움을 받기 위해 연락할 곳을 알고 있어야 합니다.

최종 사용자가 1차 방어선이 되곤 합니다. 이들이 보안 이벤트를 인식하고 유효한 채널을 통해 문제점을 보고하지 않으면, 아무런 제약 없이 공격이 계속되면서 네트워크 전체로 확산될 수 있습니다.

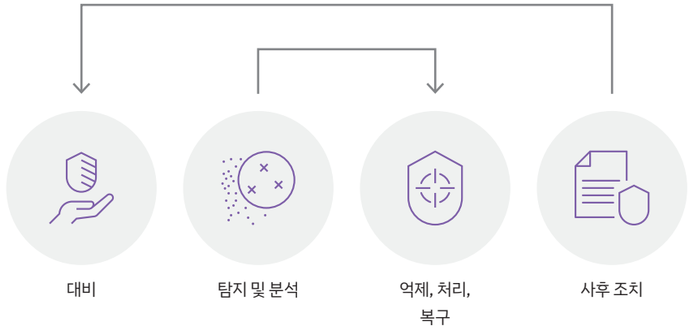
침해 사고 라이프사이클

여기서는 NIST(National Institute of Standards and Technology) 침해 사고 대응 라이프사이클의 랜섬웨어 사고 대응 체계를 따릅니다. 이 프로세스는 NIST 컴퓨터 보안 사고 처리 가이드(NIST Computer Security Incident Handling Guide)에서 자세히 설명합니다. 2020년 가이드에 관해서는 여기를 클릭하여 자세히 알아보십시오.

현재 진행 중인 공격의 범위에 속해 있다면, 다음 단계를 수행해야 합니다.

- 대비
- 탐지 및 분석
- 억제, 처리, 복구
- 사후 조치

그림 1: 사고 대응 라이프사이클(NIST 기준)



다음 섹션부터 각 단계를 자세히 살펴보겠습니다.

대비

공격 라이프사이클에 대한 대비(preparation) 단계에서는 해당 기업이 종사하는 업종, 사용하는 시스템, 장기적 관점에서 적용 가능한 주요 위험 지표(KRI)를 고려할 때 발생 가능성이 높은 사건 및 사고 유형에 대비합니다.

사고 대응 프로세스의 모든 잠재적 요소를 이 글에서 다루지는 않겠지만, 랜섬웨어 사고에 대비하고 가급적 예방하기 위한 조치를 제안합니다.

랜섬웨어 변종 및 공격 전술이 끊임없이 빠르게 진화하고 있는 만큼, IBM Security X-Force는 NIST 침해 사고 대응 라이프사이클의 **대비** 단계가 무엇보다 중요함을 강조합니다.

악성 랜섬웨어 파일을 탐지했다면, 이미 데이터가 암호화되었을 것이기 때문에 대체로 이 공격의 진행을 막기에는 너무 늦은 상태입니다. 그러나 공격을 억제하고, 어쩌면 공격의 일부를 완전히 중단시킬 기회가 아직 남아 있을 수도 있습니다.

충분한 예행연습을 거친 심층 방어 전략, 그리고 랜섬웨어 공격을 막기 위해 특별히 마련된 철저한 대비 계획이 있느냐에 따라 성패가 결정됩니다. 대비 단계에서 결코 소홀히 해서는 안 될 몇 가지 요소를 다음 섹션부터 살펴보겠습니다.

역할 기반 최종 사용자 교육

선제적 최종 사용자 교육 및 훈련은 여전히 모든 유형의 감염을 예방하기 위해 꼭 필요합니다. 피싱, BEC(Business Email Compromise) 사기, 악성 스팸, 그리고 더 폭넓게는 랜섬웨어 및 악성 코드 사고 전반이 여기에 해당됩니다. 최종 사용자가 보안 사고를 가장 먼저 경험하는 경우가 다반사이기 때문입니다. 철저히 보호받는 환경에서도 사용자가 1차 방어선이 되므로, 최종 사용자를 대상으로 하는 정기 교육을 통해 일어날 법한 위협의 유형, 해야 할 또는 해서는 안 될 행동, 문제를 보고할 곳과 그 방법을 알려야 합니다.

결국 보안 의식이 투철한 인적 자원을 귀중한 문화적 자산으로 확보함으로써 큰 비용을 들이지 않고도 조직 전체의 보안 수준을 몇 배로 끌어올릴 수 있습니다.

대표적인 감염 경로, 이메일

연구 조사에 따르면, 지금도 이메일은 랜섬웨어 공격의 대표적인 감염 경로입니다. 어떤 유형의 기업에서든 이메일이 필수 비즈니스 수단으로 자리잡았기 때문에 공격자에게는 잠재적 피해자에 도달하여 공격을 실행할, 더없이 친숙할 뿐만 아니라 효과도 뛰어난 방법입니다.

베스트 프랙티스

이메일은 해커가 랜섬웨어 배포에 자주 사용하는 공격 경로입니다. 직원의 보안 의식을 강화하는 교육을 통해 의심스러운 이메일의 특징 및 그런 이메일을 받을 때의 대처 방법을 알려야 합니다.

사용자에게 이메일 보안 교육을 자주 실시하십시오. 악성 코드의 행동을 시뮬레이션하는 이메일 또는 첨부 파일을 직원들에게 보내는 식으로, 예고 없는 모의 피싱 훈련을 정기적으로 하는 캠페인도 고려해 보십시오. 그러한 캠페인을 통해 의심스러운 첨부 파일이나 링크를 클릭하는 사용자 수에 관한 지표를 생성하여 현재의 의식 수준을 점검할 뿐만 아니라 장기적인 개선 방안을 문서화할 수 있습니다.

캠페인이 성공하려면, 의심스러운 첨부 파일/링크를 클릭하는 사용자 수의 기준선을 정한 다음 직원 교육을 진행해야 합니다. 그리고 후속 캠페인을 통해 조직 내의 인식 제고 효과를 정량화합니다. 자체적으로 테스트 캠페인을 기획하거나, 이러한 유형의 사이버 보안 의식 캠페인을 전문으로 하는 외주 업체를 이용할 수도 있습니다.

또 다른 감염 경로, 매크로

랜섬웨어를 비롯하여 일반적인 악성 코드는 주로 생산성 파일 안에 포함된 상태로 유포되기 때문에 이메일 필터 및 보안 시스템에 의해 차단될 가능성이 낮습니다. 매크로를 통해 악성 코드를 유포하는 것은 오래되었지만 여전히 유효한 수법입니다. 적어도 1990년대 중반부터 사이버 범죄에 쓰이기 시작한 이 전통적인 공격 방식은 한층 더 진화하여 지금도 사용자 및 기업 네트워크를 위협하고 있습니다.

Office 제품군 문서, 스프레드시트 등 일반 업무용 툴에 악성 코드가 숨어 있는 경우가 많습니다. 사용자를 속여 코드를 실행하기 위해 매크로의 형태로 있다가 스크립트를 시작합니다. 사용자는 배후에서 일어나는 상황을 미처 알지 못합니다. 사용자가 문서를 열면 "추가 정보를 확인하기 위해 매크로를 활성화"하라는 메시지가 나타납니다. 이 매크로는 PowerShell 스크립트를 사용하여 추가 페이로드를 가져옵니다. 전송 과정에서 보안 제어를 우회하기 위한 툴도 사용합니다.

신뢰할 만한 워크플로우를 통해 매크로를 활성화할 수도 있으나, 모든 활동을 위해 매크로 활성화가 반드시 필요한 것은 아닙니다. 불필요한 매크로는 비활성화함으로써 방어 체계를 한층 더 강화하고 잠재적 위험성이 있는 매크로 실행을 막을 수 있습니다.

이메일 첨부에 포함된 매크로의 위험성을 사용자에게 알리는 교육을 정례화하고, 사용자가 위험한 행동을 스스로 식별할 수 있도록 더 철저하게 매크로 관련 알림을 보내며, 그룹 정책을 최신 상태로 유지하는 한편 인터넷에서 다운로드한 Word, Excel, PowerPoint 문서에서는 매크로 실행을 차단하는 등의 베스트 프랙티스를 실천할 수 있습니다.

잘못된 구성이 진입 지점

기업에서 ID, 권한, Active Directory를 관리하는 방식에 따라 보안 침해 수법이 달라지기도 합니다. 잘못된 구성(misconfiguration)은 대개 사전 예방이 가능하므로, 공격자가 찾아내기 전에 해결하는 것이 가장 바람직합니다. X-Force 사고 대응 팀에서 경험한 사례 중 하나는 Active Directory Manager에 대해 웹 기반 접근을 설정해 두었는데 이를 비공개로 유지하는 컨트롤이 사라진 경우입니다. 그러면 해당 인터페이스가 인터넷에 노출되고, 결국 공격자가 해당 기업에 대한 진입 지점으로 활용할 수도 있습니다.

반드시 변경해야 하는 기본 비밀번호

기본 비밀번호를 바꾸는 것이 극히 초보적인 방법으로 보일 수 있으나, 중요 자산, 시스템, 인터페이스에서도 지켜지지 않을 때가 많습니다. 이 허점을 간과해서는 안 됩니다. 공격자가 손쉽게 침투하여 거점을 확보할 수 있기 때문입니다.

기본 비밀번호는 반드시 변경하고, 인프라 전 범위를 대상으로 정기 점검을 통해 누락되거나 방치된 것이 없음을 확인하십시오.

가급적 다단계 인증 사용

비밀번호는 가장 쉽게 훔칠 수 있는 기밀 정보 중 하나입니다. 온라인에 유출된 데이터에서도 흔히 볼 수 있습니다. 비밀번호만 사용하는 보안은 안전하지 않습니다. 가급적 모든 로그인 시스템에 다단계 인증(multi-factor authentication, MFA)을 구축하여 유출된 비밀번호 또는 도용된 기본 로그인 자격증명 정보가 공격에 쓰이지 않게 하십시오.

이메일 첨부에서 실행 파일 제거/차단

대부분 기업에서는 실행 파일이 첨부된 이메일을 보내거나 받을 수 없게 이메일 서버를 구성합니다. 이런 까닭에 공격자는 ZIP 아카이브 첨부 파일에 실행형 악성 코드를 숨겨 놓고 이메일을 보내는 방법을 구사합니다.

ZIP 아카이브 첨부 파일의 내부를 조사하도록 이메일 게이트웨이를 구성하는 곳도 많지만, 실행 파일을 제거하지 않을 때도 있습니다. 안티바이러스 검사에서 문제의 실행 파일을 위협으로 탐지하지 않으면, 결국 사용자의 편지함 및 엔드포인트에 도달합니다. 지능형 악성 코드가 방어 체계를 뚫고 들어와 공격자에게 교두보를 마련해 주는 셈입니다.

첨부 파일이 이메일 방어 장치를 통과할 위험을 최소화할 수 있습니다. 가능하다면 아카이브에 포함된 파일(비밀번호가 설정되지 않은 파일)을 비롯하여 EXE, COM, SCR 확장자를 사용하는 모든 실행 파일을 제거하도록 이메일 서버를 구성합니다. .JS 확장자 파일도 사용자 편지함에 전달하기 전에 제거하는 것이 좋습니다.

어떤 기업은 매크로를 포함한 모든 Office 첨부 문서를 자동으로 격리합니다. 더 나아가 유형에 상관없이 모든 첨부 파일을 일단 격리한 다음 승인을 받으면 최종 수신자에게 배포하는 곳도 있습니다.

Office 문서 취급 방법 중 하나로, 신뢰할 만한 (서명된) 매크로는 화이트리스트에 넣고 나머지는 모두 차단할 수 있습니다. 새로운 비즈니스 문서 매크로를 화이트리스트에 추가해야 하는 경우, 반드시 변경 관리를 통해 완전한 감사 추적 기록을 생성함으로써 악의적 의도를 가진 내부자에 의한 오용의 위험을 최소화할 수 있습니다.

최신 버전의 안티바이러스 및 엔드포인트 보호 수단 사용

엔드포인트 안티바이러스 솔루션이 위협을 탐지하는 유일한 보호 메커니즘은 아니지만, 전사적 차원에서 사용자에게 배포하는, 초기 단계의 위협 탐지 수단으로 많이 사용됩니다.

안티바이러스 솔루션을 최신 바이러스 정의로 업데이트하여 효과를 극대화해야 합니다. 랜섬웨어는 탐지 기술을 피하기 위해 끊임없이 진화하고 발전합니다. 매일같이 새로운 버전이 등장하며, 일반적인 기업용 안티바이러스 제품에서 며칠이 지나도 탐지하지 못하는 경우도 많습니다. 그 사이에 공격자는 침투에 성공하여 거점을 확보할 수 있습니다.

용도별로 지정된 안티바이러스 제품을 사용하는 방법도 고려할 만합니다. 이를테면 데스크탑용, 서버용, 이메일 게이트웨이용으로 각각 다른 안티바이러스 제품을 사용하는 것입니다. 이러한 전략으로 새로운 위협의 차단 범위를 극대화할 수 있습니다. 이 안티바이러스 솔루션 중 하나에서 놓치더라도 다른 솔루션에서 탐지할 수 있기 때문입니다.

서명에 의존하지 않고 의심스러운 행동 및 인증되지 않은 애플리케이션을 탐지하는 새로운 엔드포인트 보호 솔루션도 검토해 보십시오.

'temp' 폴더에서 프로그램 실행 제한

악성 코드는 흔히 'Temp' 폴더를 최초 실행 지점으로 사용하는데, 랜섬웨어도 예외는 아닙니다. 가급적 그룹 정책 오브젝트(GPO) 또는 소프트웨어 제한 정책(SRP)을 사용하여 범용 'Temp' 폴더에서, 또는 사용자 프로필의 'Temp' 폴더(예: "**c:\users\<user>\ appdata\temp**")에서 모든 프로그램의 실행을 제한하십시오.

예컨대 랜섬웨어 대부분은 처음 실행될 때 악성 페이로드를 사용자의 'Temp' 폴더에 복사한 다음 실행 사슬을 이어가려 합니다. 이 폴더를 차단함으로써 악성 코드 초기 감염을 막을 수 있습니다.

큰 도움이 될 또 다른 해결책으로 Windows AppLocker가 있습니다. 이 기능으로 임시 폴더뿐만 아니라 **%AppData%, %LocalAppData%** 등과 같이 여러 악성 코드/랜섬웨어 계열에 쓰이는 비표준 폴더에서도 실행 파일이 시작되는 것을 막을 수 있습니다. 한편 합법적인 상용 전문 소프트웨어는 프로그램을 시작할 때 이러한 폴더를 사용하지 않습니다.

계속 공세적으로 최신 패치 관리 정책 시행

IT 네트워크에 랜섬웨어를 심어 두려는 공격자는 주로 제로데이 취약점을 이용하여 네트워크 내부에 거점을 확보하려 합니다. 제로데이 취약점은 모니터링하기에 까다로운 공격 경로일 수 있습니다. 공격 가능한 새로운 취약점이 수시로, 때로는 매일같이 등장하기 때문입니다.

위협 인텔리전스에 따르면, 랜섬웨어를 비롯하여 다양한 악성 코드 유형을 사용하는 공격자는 종합적인 공격 전략의 일환으로 제로데이 취약점을 발 빠르게 찾아내 이용합니다.

베스트 프랙티스

엄격한 패치 관리 정책을 통해 귀사를 랜섬웨어 위협으로부터 안전하게 지킬 수 있습니다. 최고 위험도 애플리케이션, 패치 자체의 중요도, CVSS 점수를 고려하는 위험 기반 접근 방식으로 패치 적용의 우선순위를 정하는 것도 좋습니다.

제로데이 취약점이 빈번하게 출현하는 것처럼 보이지만, 패치도 빠르게 제공되는 편입니다. 각 기업은 공세적인 패치 관리 정책을 채택해야 합니다. Adobe Flash, Java 등 많은 직원이 사용하는 기능과 관련된 브라우저 취약점에서는 특히 더 시급합니다. 가급적 자동으로 패치를 배포하고 적시에 적용해야 합니다. 위험도가 높은 문제에 패치를 적용할 수 없는 경우에 대비하여 분리 조치(segregation), 완화 통제, 보완 통제와 같은 수단도 마련해야 합니다.

DNS 가시성 향상, 싱크홀 및 웹 필터링 기능 강화

랜섬웨어의 경우, 초기 단계에 악성 코드가 DNS 변환(resolution)을 시도할 때 통신 사업자의 도메인 생성 알고리즘(DGA)을 이용하기도 합니다. 그러면 알려진 악성 도메인을 식별하여 차단하기가 더 어렵습니다. 악성 코드에서 C&C 서버와 연결할 목적으로 무수히 많은 도메인 이름을 생성하고 사용할 수 있기 때문입니다.

그럼에도 불구하고, 기업의 도메인 이름 서버(DNS)를 제대로 파악하고 있으면 침해 사고를 처리하고 조기 경고 시스템을 구축할 때 큰 도움이 됩니다. DNS 요청을 검색하고 모니터링하다가 자주 생성되는 DGA 스타일의 DNS 요청과 같은 패턴을 발견하게 됩니다. 이그레스(egress) 게이트웨이에서 지정된 IP나 도메인을 곧바로 차단하기보다는 DNS 싱크홀 기능을 구현하는 것도 좋은 방법입니다. 싱크홀을 사용하면, 도메인(및 IP)을 특정 내부 서버로 리디렉션한 다음 차단된 사이트에 대한 접근을 시도하는 사용자에게 경고할 수 있습니다. 이 싱크홀은 위험한 도메인에 접속하려는 컴퓨터에 대해서도 실시간 알림을 제공할 수 있습니다.

평판 기반 웹 필터링 기능의 구현도 고려할 만합니다. 차단 목록에 포함된 IP, 도메인, 사이트 전반을 계속 추적하는 것은 끝없는 작업입니다. 차세대 방화벽 및 프록시에서는 실시간 평판 피드(reputation feeds)를 사용합니다. 즉, 크라우드 소싱한 인텔리전스 정보를 활용하여 위험한 것으로 알려진 목적지를 신속하게 알리고, 악성 콘텐츠가 있는 것으로 확인된 사이트에 대해서는 빠른 차단 기능을 제공하는 방식으로 보호합니다.

IBM은 Quad9 파트너입니다. Quad9은 무료로 이용 가능한 애니캐스트 기반의 재귀적 DNS 플랫폼입니다. 알려진 악성 도메인을 차단하여 컴퓨터 및 IoT 디바이스가 악성 코드 또는 피싱 사이트에 연결하는 것을 막습니다.

최소 권한의 원칙 적용

랜섬웨어는 로컬 시스템 및 네트워크 공유에 있는 일반 사용자 파일을 노립니다. 따라서 IBM Security X-Force는 기업 네트워크의 파일 접근에 대해 최소 권한(Least Privilege) 방법론을 따르라고 조언합니다. 최소 권한의 원칙에서는 관리자가 각 사용자의 일상 업무 요구사항에 필요한 최소한의 권한을 부여합니다.

베스트 프랙티스

IBM Security X-Force는 기업 네트워크의 파일 접근에 대해 최소 권한의 원칙을 제안합니다.

감염된 컴퓨터는 현재 로그인한 사용자의 권한으로 작동하고 있으므로, 읽기/쓰기 접근이 가능한 파일만 골라내 암호화할 수 있습니다. 사용자가 온갖 네트워크 공유에 대해 읽기/쓰기 접근 권한을 가질 필요가 없다면, 적어도 정기적인 접근이 필요하지 않은 위치에서는 쓰기 권한을 없애는 것도 좋습니다.

X-Force 사고 대응 팀에서 자주 목격한 실수 중 하나는 보안 팀이 로컬 사용자가 각자의 디바이스에서 관리자 권한을 갖도록 허용하는 것입니다. 이러한 특별 권한이 부여되면, 랜섬웨어가 해당 디바이스 및 그 연결 대상에 대해 더 유해한 활동을 할 수 있어 공격의 피해도 커지기 마련입니다. 로컬 관리자 권한을 없애 사용자에 의한 실수 및 공격자의 활동을 모두 제한하십시오.

플래시 비활성화

Adobe Flash는 잘 알려진 랜섬웨어 감염 경로 중 하나입니다. 널리 쓰이는 인터넷 브라우저 중 일부는 심각한 보안 결점을 이유로 Flash를 기본적으로 차단하는 조치에 착수했습니다. IBM Security X-Force는 Flash의 위험성을 고려하여 각 기업에서 기본적으로 Flash를 비활성화할 것을 권장합니다.

일부 사용자가 업무상 Flash를 사용해야 하는 경우, 고위험도 전용 네트워크를 따로 만들어 격리 상태로 운영하는 것과 같은 추가적인 안전 장치를 두면 됩니다. Flash 비활성화가 인터넷 활동의 모든 위험을 해소할 방법은 아니더라도, 공격자가 자주 이용하는 감염 경로를 줄일 수 있다는 이점이 있습니다.

Flash 단종일(End of Life, EOL)은 2020년 12월 31일입니다. 그 이후에는 Adobe에서 배포하거나 업데이트하지 않습니다. 관련 위험을 최소화하기 위해 더는 사용하지 않아야 합니다.

WSH 비활성화 고려

지난 몇 년 새 랜섬웨어 및 기타 악성 코드에서 JavaScript/VBScript를 사용하는 경우가 늘었습니다. 악성 코드 개발자가 스크립팅을 애용하는 이유는 모든 Windows 시스템에서 기본적으로 Windows 스크립팅 호스트(WSH)가 활성화되어 있기 때문입니다. 악성 코드 개발자가 좋아하는 기능이지만, 정작 일반 기업의 일상 업무에는 거의 또는 전혀 쓰이지 않습니다.

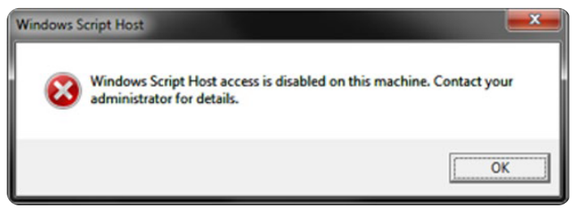
스크립팅은 랜섬웨어 개발자의 공격 표면을 넓힐 수 있는 위험한 기능입니다. 그러면 악성 코드 스크립트가 성공적으로 실행되어 랜섬웨어 공격으로 이어질 가능성이 높아집니다.

일부 악성 스크립팅은 중앙에서 그룹 정책을 통해 차단할 수 있습니다. 다음과 같이 레지스트리 키와 값을 생성하면 됩니다.

> **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings\ Enabled에서 'Value data' 필드를 '0'으로 설정합니다(따옴표 없이 숫자 0 입력).**

그러면 JavaScript/VBScript를 사용하여 감염 루틴을 실행하려는 랜섬웨어 및 기타 악성 코드를 제한할 수 있습니다. 스크립트가 실행되지 않고 사용자의 화면에 WSH 경고 메시지가 나타나 스크립팅이 비활성화되었음을 알립니다.

그림 2: Windows Script Host 비활성화 메시지



WSH를 비활성화하면, 사용자는 WSH를 사용하는 모든 스크립트(VBScript 및 JScript 스크립트 등)를 실행할 수 없게 됩니다. 일상 업무에 필요하다면 다른 대책을 강구해야 합니다.

사고 대응 계획 수립 및 예행연습

조직 운영의 모든 단계에 영향을 미칠 뿐만 아니라, 특히 디지털 자산 및 데이터 접근에 큰 타격을 주는 각종 위협, 가동 중단, 재해 등으로 힘든 상황에 처했을 때 기업이 빠르고 효과적으로 대처할 수 있도록 사고 대응 계획을 마련합니다.

체계적이고 세심한 대응을 위한 정책과 계획을 미리 마련함으로써 문제 발생 시 혼란 및 공황으로 인한 부적절한 의사결정을 최소화합니다.

사고 대응 계획의 방법론에서 명확한 탐지/억제/처리/운영 재개 단계를 포함해야 하지만, 거기서 끝나서는 안 됩니다. 사후 근본 원인 분석을 진행하여 이번 경험을 통해 얻은 교훈을 정리함으로써 기존 계획의 완성도를 더 높이고 향후 사고 발생 시 취할 조치를 세밀하게 조정할 수 있습니다.

대부분 프레임워크, 특히 NIST 사고 대응 프로세스는 크게 4단계로 구성됩니다.

1. 대비(Preparation)
2. 탐지 및 분석(Detection and Analysis)
3. 억제, 처리, 복구(Containment, Eradication and Recovery)
4. 사후 조치(Post-Incident Activity)

여기서는 NIST 프레임워크에 기초한 랜섬웨어 공격 대응 단계를 좀 더 자세히 살펴보겠습니다. 귀사의 첫 계획을 수립하는 방법에 관해서는 NIST 가이드를 참조하십시오. 또는 SANS 프레임워크 및 핸드북을 활용할 수도 있습니다.

어떤 계획을 얼마나 상세히 문서화하든 간에, 그 계획에 대한 예행연습을 반드시 진행하여 실무 팀이 시작 및 실행 방법을 숙지하게 해야 합니다.

베스트 프랙티스

잘 짜여진 사고 대응 계획을 보유하고 있으면서 평상시에 예행연습까지 잘 되어 있으면 실제 상황 발생 시 시간과 비용을 절약할 수 있습니다. IBM 2020 데이터 유출 사고 비용 보고서에 따르면, 테스트를 통해 검증된 계획이 없는 기업에서 발생한 비용은 529만 달러에 달했지만, 검증된 계획이 있는 곳에서는 329만 달러로 훨씬 더 적었습니다.

경영진의 뛰어난 커뮤니케이션 능력도 필요합니다. 여기에는 미디어 및 이해 관계자의 질문에 답하고, 규정에 따른 정보 공개 요건 및 일정을 준수하며, 회사 전체에 영향을 미칠 사고를 수습하면서 리더십을 발휘하는 것도 포함됩니다.

TTX(tabletop exercises)라고도 부르는 모의 훈련은 좋은 출발점이 됩니다. 그러나 위기 상황에서 대응 계획의 실효성을 검증하려면, 일상 업무 활동의 물리적 영역을 훈련 범위에 최대한 포함시켜야 합니다. 예행연습을 실시한 팀이 실제 상황에서 더 유능한 모습을 보여줄 것입니다. 이러한 예행연습을 통해 각 팀의 역량이 더욱더 향상됩니다.

계획 개발, TTX, 계획 연습의 어떤 단계에서든 도움이 필요할 경우, IBM 전문가 팀이 도와드리겠습니다. 자세한 내용은 IBM Security Command Center에 문의하십시오.

사고 대응: 탐지

기업에서 랜섬웨어 감염 사실을 처음 발견하는 경로는 실제 상황에 따라 달라질 수 있으나, 대개는 어떤 직원이 파일에 접근할 수 없음을 깨달은 후 몸값 요구 메시지를 받거나, 특정 서비스 이용이 불가하다는 알림을 받으면서 시작합니다. 공격 초기 단계에는 이미 감염된 시스템, 그리고 감염될 위험성이 큰 시스템을 모두 찾아내는 데 가장 많은 시간이 걸립니다.

일차적 목표는 감염 확산을 최대한 빨리 억제하고, 감염된 시스템을 격리하여 전사적 차원의 위험 부담을 최소화하는 것입니다. 이러한 노력을 통해 어쩌면 공격자가 진행 중인 암호화 프로세스를 중단시켜 해당 기업이 입을 피해를 최소화하고 데이터, 시스템, 비즈니스 운영 복원에 드는 수고도 줄일 수 있습니다.

고객의 랜섬웨어 공격 대응에 참여하고 지원한 IBM Security의 경험에 따르면, 공격 발견 시나리오를 몇 가지 유형으로 정리할 수 있습니다. 이 대표적인 시나리오를 다음 섹션에서 차례로 살펴보겠습니다.

각 시나리오를 검토하면서 유의할 점이 있습니다. 파일을 암호화하는 감염된 호스트를 하나 찾아내더라도, 나머지 호스트가 무사하다고 생각해서는 안 됩니다. 어떤 기업의 호스트 하나가 감염된 것이 확인되면, 다른 호스트도 감염되었을 가능성이 높습니다. 해당 취약점이 사내에 구축된 모든 호스트에 존재할 수도 있기 때문입니다.

파일 암호화의 주범인 감염된 호스트를 발견한 경우, 특히 네트워크 공유에서 찾아냈다면, 그 호스트를 오프라인 상태로 만든 다음 네트워크 공유를 철저히 모니터링하십시오. 다른 감염된 호스트가 암호화 프로세스를 이어갈 수도 있습니다.

시나리오 1 — 네트워크 사용자가 네트워크 공유에 있는 파일에 대한 접근을 시도하다가 그 파일이 암호화되었음을 확인

공유 폴더에 접근하려던 사용자가 그 위치에서 암호화된 파일을 발견하는 경우입니다. 해당 기업에게는 잠재적 위험 부담이 가장 큽니다. 네트워크 어딘가에 감염된 컴퓨터가 있고, 그곳의 사용자는 계속 그 컴퓨터로 네트워크 공유에 접근하고 있습니다. 현재 이 사용자의 권한으로 활동 중인 랜섬웨어는 네트워크 공유 및 폴더를 돌아다니면서 이 사용자가 접근할 수 있는 모든 파일을 암호화하는 중입니다.

규모가 큰 조직에서는 사용자가 접근할 수 있는 파일도 많습니다. 수십만 개의 파일이 암호화되거나 도용되었을지도 모릅니다. 대용량 네트워크 공유는 랜섬웨어가 암호화하는 데 며칠이 걸리기도 하지만, 그렇다 하더라도 발견되기 전에 이미 암호화 프로세스가 시작된 상태일 것입니다. 매우 큰 피해를 일으키는 이 단계는 탐지하기가 쉽지 않습니다. 피해자 컴퓨터에 아직 몸값에 관한 메시지가 나타나지 않기 때문입니다.

초기 감염을 억제하려면, 랜섬웨어 암호화 활동이 진행 중인 감염된 컴퓨터를 찾아내는 게 급선무입니다. 감염된 사용자의 범위를 좁히기 위해 대개는 암호화된 파일의 소유자 권한을 확인합니다. 각 폴더에 새로 생긴 파일, 즉 사용자에게 파일이 암호화되었음을 알리는 기능을 하는 파일의 소유자 권한을 살펴보는 방법도 있습니다. 대체로 이 새 파일은 랜섬웨어가 실행 중인 사용자 권한을 상속합니다. 초기에 랜섬웨어에 감염된 사용자 계정이 파일 소유자 이름으로 표시됩니다.

사용자를 찾아냈으면 그 디바이스 및 접근 권한을 비활성화하여 공유 위치에서 진행 중인 암호화 프로세스를 중단시켜야 합니다.

시나리오 2 – 로컬 파일에 대한 접근을 시도한 사용자가 해당 파일이 암호화되었음을 발견

두 번째로 가능한 시나리오는 어떤 컴퓨터가 감염된 상태에서 사용자가 이 로컬 시스템의 파일이 암호화되어 접근할 수 없음을 알게 된 경우입니다. 아직 사용자의 화면에 몸값 요구 메시지가 나타나지 않았습니다. 대부분 랜섬웨어 변종은 암호화한 폴더 각각에 텍스트 파일이나 HTML 파일을 남겨 놓습니다. 이 파일을 통해 사용자에게 암호화 사실을 알리고 몸값을 요구합니다. 하지만 이 시나리오에서는 암호화 프로세스가 진행 중인데, 사용자가 우연히 (암호화된) 파일에 대한 접근을 시도한 것 같습니다. 아직 랜섬웨어의 악성 활동이 완료되지 않은 상태입니다.

이러한 상황에서는 문제의 컴퓨터를 즉시 종료해야 합니다. 진행 중인 악성 프로세스가 로컬 드라이브, 어쩌면 네트워크 드라이브의 여러 폴더를 돌아다니면서 접근 불가능한 상태로 만들 우려가 있기 때문입니다.

감염된 시스템을 리부팅하거나 재시작하지 마십시오.

감염된 시스템에서 즉시 최대 절전 모드로 전환하고 네트워크 연결을 끊은 다음 IT 보안 팀에 알려야 합니다.

시스템을 끄는 방법도 있지만, 최대 절전 모드로 전환하면 일부 랜섬웨어 변종이 메모리에 보관하는 해독 키를 찾아낼 수도 있습니다. 아울러 직원들에게 시스템을 리부팅하지 말라고 안내하십시오. 랜섬웨어 암호화 프로세스가 다시 초기화되어 재실행될 수도 있습니다.

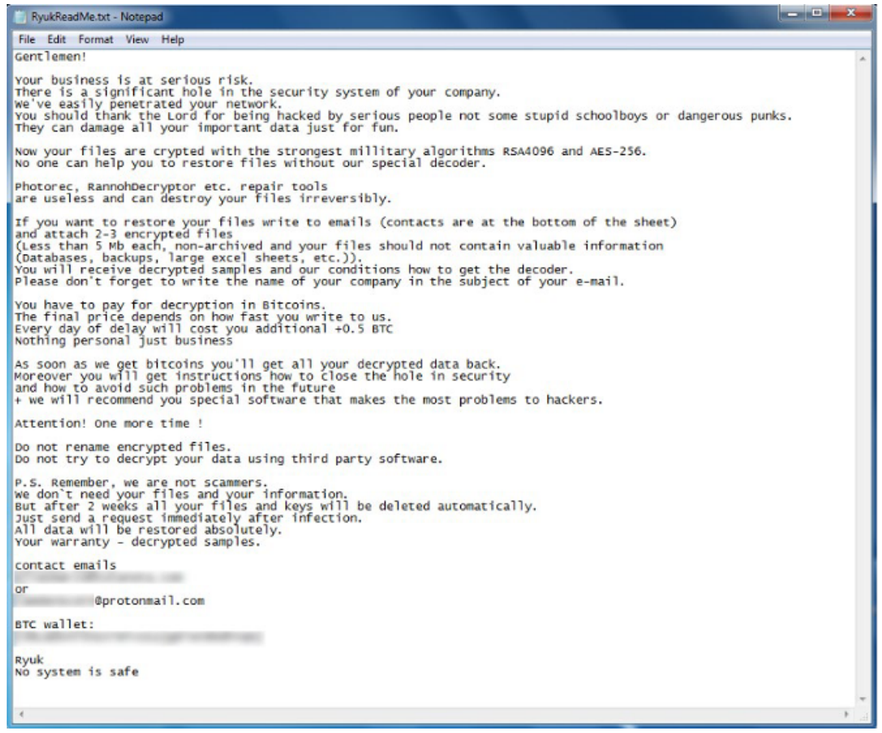
시나리오 3 – 사용자가 자신의 컴퓨터에서 몸값 요구 메시지 수신

회사 직원의 디바이스가 아무도 모르는 새 감염되어 이 사용자의 모든 로컬 파일은 물론 사용자가 네트워크 공유에서 접근할 수 있는 파일까지 모두 암호화하기 시작했습니다.

암호화 프로세스가 끝나면, 감염된 컴퓨터의 화면에 메시지가 나타나 사용자에게 파일이 암호화된 사실과 몸값을 지불할 방법을 알려줍니다.

사용자에게 표시되는 메시지의 내용은 랜섬웨어 계열에 따라 다르지만, 대개 아래의 예와 비슷합니다. 이 메시지는 Ryuk 랜섬웨어 범죄조직이 사용한 것입니다. 이 조직은 2019년 ~ 2020년에 전 세계의 기업을 상대로 수차례 공격을 벌인 바 있습니다.

그림 3: 랜섬웨어 공격자가 보낸 메시지의 예 – Ryuk



감염된 컴퓨터에 표시되는 메시지는 사용자에게 감염 사실을, 보안 팀에게는 침해 사고가 진행 중임을 알릴 뿐만 아니라 해당 공격에 쓰인 랜섬웨어 변종에 관한 단서도 제공합니다.

스크린샷 기능이나 모바일 디바이스의 사진 앱을 사용하여 화면의 메시지를 캡처하고, 해당 침해 사고와 관련하여 수집하는 포렌식 정보에 포함시켜 보관해야 합니다.

시나리오 4 – 대량 파일 조작 알림

보안 팀이 랜섬웨어 공격이 진행 중임을 알게 되는 또 다른 경로는 파일 조작 임계치가 정상적인 일일 기록 수치를 크게 넘어설 때입니다. 해당 규칙이 설정되어 있는 SIEM 솔루션에서 이와 관련된 알림을 보내곤 합니다.

다음은 분석 단계입니다.

사고 대응: 분 석

분석(Analysis) 단계에서는 크게 2가지 영역에 집중합니다.

1. 해당 랜섬웨어의 변종 특정
2. 악성 코드가 침투한 방법 확인(근본 원인 분석)

악성 코드 식별

분석 단계를 시작할 때, 침투한 랜섬웨어의 변종을 확실히 파악하는 게 중요합니다. 랜섬웨어 변종이 다양하고, 우후죽순으로 생겨나는 새로운 변종의 기능이 저마다 다르기 때문에, 억제 단계로 진행하기에 앞서 어떤 랜섬웨어 변종인지를 알아야 합니다.

어떤 랜섬웨어 버전은 내부망 이동(lateral movement) 기능을 활용할 수 있습니다. 반면에 이런 기능이 없는 버전도 있습니다. 각 랜섬웨어 코드의 기능은 향후 진행할 억제 및 처리 활동에 지대한 영향을 줍니다.

변종을 알아내기가 쉽지 않을 수 있습니다. X-Force는 사내의 분야별 전문가(SME) 또는 외부 전문가(예: 보안 서비스 제공업체)의 도움을 받아 변종 및 그 배후 조직을 알아내는 것을 권장합니다.

초기 근본 원인 분석

약식 근본 원인 분석(Root Cause Analysis, RCA)을 수행하여 보안 팀이 해당 랜섬웨어가 디지털 환경에 유입된 과정을 파악하도록 돕습니다.

정식 RCA는 사후 조치 단계까지 미룰 수 있으나, 약식 RCA는 억제 단계를 계획하고 시행하는 데 큰 도움이 됩니다. 기초적인 RCA가 이루어지지 않으면 감염 사이클이 반복되기 쉽습니다. 복구 단계 이전에 RCA를 수행하는 것도 중요합니다. 상당한 시간과 노력을 들여 복구한 파일이 곧 다시 암호화되는 사태가 생길 수도 있기 때문입니다.

대표적인 진입 지점은 다음과 같습니다.

- 이메일
- 브라우저 취약점
- 기타 취약점

이메일 진입 지점

랜섬웨어가 기업에 침투할 때 가장 많이 이용하는 진입 지점은 수신자가 요청하지 않은 이메일(첨부 파일), 또는 드라이브 바이 다운로드(drive-by download) 감염을 유발하는 웹 브라우저 취약점입니다.

직원이 요청하지 않은, 랜섬웨어가 포함된 이메일을 받았다면, 회사의 이메일 저장소 전체를 신속히 조사하여 다른 직원의 편지함에도 그런 이메일이 (어쩌면 미개봉 상태로) 있는지를 확인해야 합니다. 즉시 해당 이메일을 골라내 제거하여 직원이 열어볼 수 없게 합니다.

드라이브 바이 다운로드 침투

웹 브라우저 취약점은 좀 더 복잡하고 확인하기가 어려운 편이지만, 여기서는 해당 기업의 패치 관리 인프라를 RCA에 활용할 수 있습니다. 올바른 분석을 통해 최초로 감염을 일으킨 웹사이트를 찾아내 네트워크에서 그 사이트에 대한 접근을 차단할 수 있습니다.

확인된 악성 사이트 차단이 가장 먼저 할 일이지만, 그렇다고 해서 모바일로 연결된 직원, 즉 LAN(Local Area Network) 바깥에서 일하기 때문에 회사의 방화벽 규칙에 의해 차단되지 않는 직원까지 자동으로 보호하는 것은 아니므로 유의해야 합니다. 게다가 그 사이트와 동시에, 또는 조금 후에 활성화되어 악성 코드를 유포하기 시작한 다른 사이트도 있을 수 있습니다.

익스플로잇과 수동 감염

랜섬웨어를 사용하는 공격자가 기업에 침투하는 또 다른 방법으로, 특정 소프트웨어/서버 취약점에 대한 익스플로잇 공격을 한 다음 네트워크의 주요 영역에 직접 랜섬웨어를 심어 두어 최대한 많은 디바이스를 감염시키는 방식도 있습니다. 이러한 경우, 악성 활동 프로세스가 특정 시간에 시작하도록 설정하는 게 가능합니다. 범죄자들은 직원이나 보안 팀이 실시간으로 발견할 가능성을 줄이기 위해 시작 시간을 주말이나 휴일로 설정하기도 합니다.

X-Force는 사내 사고 대응 SME 또는 외부 서드파티 SME의 도움을 받아 제대로 RCA를 진행할 것을 권장합니다.

사고 대응: 억제

억제(Containment) 단계는 대응 계획의 핵심 영역 중 하나입니다. 랜섬웨어 감염이 의심되는 시스템을 찾아내면, 즉시 네트워크(WiFi 연결 포함)에서 분리한 다음, 종료하거나 가급적 최대 절전 모드로 전환합니다. 그러면 랜섬웨어에 의해 암호화 프로세스가 계속될 위험을 최소화하면서 포렌식 및 샘플 분석을 지원할 수 있습니다.

대규모 보안 팀도 종종 사고 대응(Incident Response, IR) 사이클의 초기에, 그리고 억제 단계에서 “집중” 지원이 필요합니다. 보안 위반이 발생하기 전에 IR 전문 업체와 계약을 체결하지 않은 기업은 발견 단계 이후에 필요한 지원을 확보하는 데 두세 배의 시간이 걸리곤 합니다.

감염된 시스템을 신속히 네트워크에서 격리하지 않으면, 악성 코드가 계속 로컬 시스템이나 네트워크 공유에 있는 더 많은 파일을 암호화하면서 사고의 범위가 확대되고 결국 복구 작업도 늘어납니다.

엔드포인트 탐지 및 대응(EDR, MDR) 실행

보안 자동화는 어떤 공격에서든, 특히 랜섬웨어 감염에서 정말 중요합니다.

기초적인 안티바이러스 보호에 머무르지 말고 진정한 **엔드포인트 탐지 및 대응(Endpoint Detection and Response, EDR)** 솔루션을 도입해야 합니다. EDR 솔루션은 악성 코드 공격 대응에 여러모로 유용합니다.

1. **초기 단계에, 더 일찍 공격을 발견할 수 있습니다. 나흘 걸리던 탐지가 이틀 만에 끝나기도 하므로, 공격 범위가 인프라 전반으로 확산되는 것을 막을 수 있습니다.**
2. **감염된 시스템을 완전히 격리할 수 있습니다. 격리된 상태라 함은 전원은 켜져 있으나, 네트워크의 다른 어떤 요소와도 차단된 상태를 말합니다. 그러면 감염된 디바이스에서 중요한 포렌식 데이터를 얻을 수 있습니다. 로컬 시스템 바깥에는 어떤 피해도 주지 않습니다.**
3. **취약점 교정(remediation) 과정에서 이 디바이스를 포렌식에 활용할 수 있습니다.**

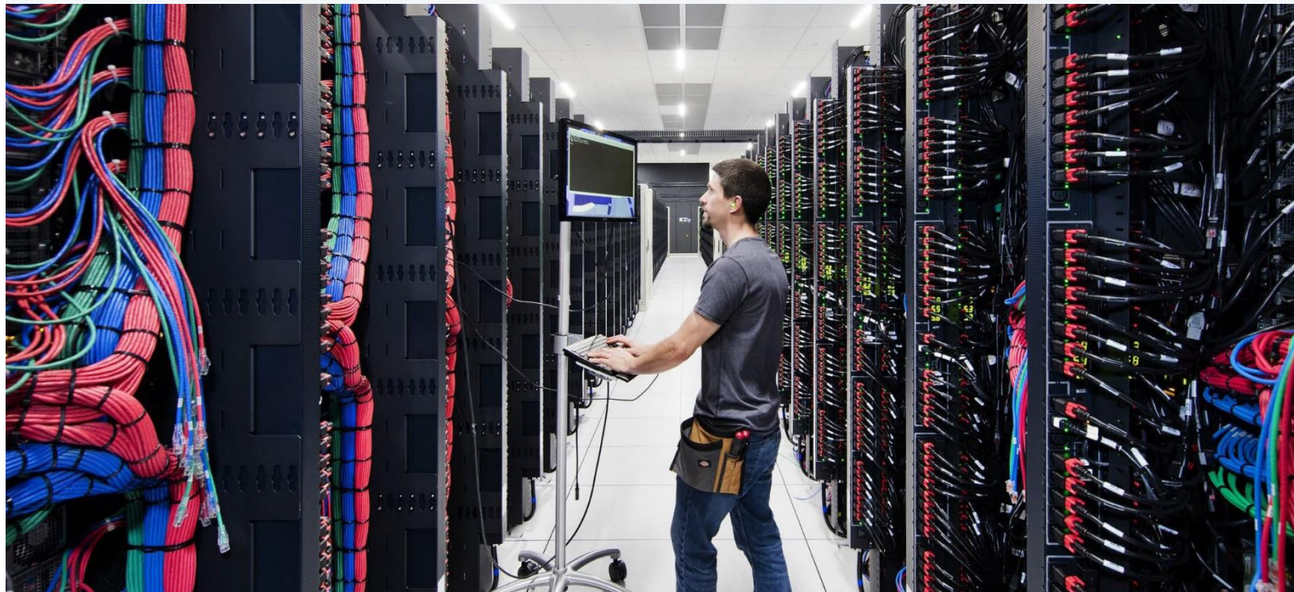
아직 EDR 솔루션이 없거나 정기적으로 사용하지 않았다면, 랜섬웨어 공격에 대한 조사를 시작할 때 서둘러 도입해야 합니다. 외부 서비스 제공업체에 맡길 수도 있는데, 단, 사고 대응 전문가가 참여해야 합니다.

후의 억제 수단 – 접근 강제 종료

랜섬웨어 감염의 출처 및 암호화 프로세스의 시작점이 금방 확인되지 않는다면, 최후의 방법으로 **파일 공유를 오프라인 상태**로 만들어 비즈니스에 대한 위험 및 영향을 최소화하는 것을 고려해야 합니다.

파일 서버를 종료할 필요는 없지만, 파일 공유에 대한 접근은 모두 강제 종료해야 합니다. 공유를 삭제하거나, 네트워크 또는 호스트 기반 방화벽 ACL을 통해 제한하는 등의 방법이 있습니다. 접근을 제한할 때 공유 위치에 있는 파일에 대한 권한을 바꾸는 것은 권장하지 않습니다. 파일 수가 많으면 변경된 권한 정보가 전달되는 데 몇 시간이 걸릴 수 있고, 그 사이에 암호화 프로세스가 계속될 우려가 있습니다.

Microsoft CIFS(Common Internet File System) 프로토콜/SMB(Server Message Block) 프로토콜을 UNIX, Linux 등 다른 운영 체제에서 사용하고 있다면, 이들 시스템에 대해서도 보호 조치를 해야 합니다. 이러한 노력을 통해 네트워크 공유가 암호화될 가능성을 크게 줄일 수 있습니다. 랜섬웨어가 이 프로토콜을 사용하여 네트워크를 돌아다니면서 암호화할 데이터가 있는 곳을 찾아낼 가능성이 있기 때문입니다.



사고 대응: 처리

처리(Eradication) 단계에서는 사내의 감염된 시스템에서 랜섬웨어를 제거합니다. 공격의 범위에 따라, 이 작업에 많은 시간이 걸리고 사용자 디바이스뿐만 아니라 더 많은 핵심 시스템 및 서비스가 영향을 받을 수도 있습니다.

X-Force는 랜섬웨어에 감염된 것으로 확인된 시스템의 경우 반드시 신뢰할 수 있는 소스와 템플릿, 안전하게 보관된 설정을 사용하여 다시 빌드할 것을 권장합니다.

아울러 근본 원인 분석(RCA)에서 랜섬웨어가 이메일 또는 기타 메커니즘을 통해 침투했음을 확인했다면, 여기에 접근하는 다른 사용자도 조사해야 합니다.

- **RCA를 통해 초기에 악성 코드가 이메일 메시지를 통해 유입된 것으로 확인되면, 아직 메일 저장소에 대기 중인 모든 메시지를 조사하고 위협을 제거해야 합니다. 이메일을 수신했거나 개봉한 시스템도, 여기서 랜섬웨어가 실행되지 않았음을 확인할 때까지는 격리할 필요가 있습니다.**
- **RCA 결과, 랜섬웨어가 웹 브라우저 익스플로잇을 통해 유입된 것으로 나타나면 해당 사이트를 차단하고 모니터링해야 합니다. 그런 다음 취약한 브라우저 구성요소를 업데이트하거나 제거할 필요성도 따져봐야 합니다.**
- **공격의 영향을 받은 모든 사용자는 예방 조치 차원에서 비밀번호를 바꿔야 합니다. 이 조치는 공격자에게 경각심을 불러일으키지 않도록 신중하게, 전략적으로 진행해야 합니다. 공격자가 수많은 자격증명 정보 세트를 보유한 경우, 초기 접근이 갑자기 거부되면 이러한 자격증명 정보를 이용하여 피봇팅(pivoting) 공격을 시도할 수도 있습니다.**

사고 대응: 복구

랜섬웨어를 억제하고 감염의 근본 원인을 규명했다면, 복구(Recovery) 단계를 시작할 때 몇 가지 고려할 사항이 있습니다.

복구를 시작하기에 앞서 억제 단계를 완료하고 감염의 근본 원인을 확실히 밝히는 것이 중요합니다.

취약점 패치

근본 원인 분석 결과, 취약한 시스템이 공격의 빌미를 제공했다면, 그 취약점에 패치를 적용하여 공격의 재발을 방지해야 합니다. 패치 적용이 어렵다면, 해당 시스템을 격리하고 보완 통제 장치를 마련하여 위험에 대한 노출을 최소화합니다.

백업에서 데이터 복원

X-Force는 (다른 옵션을 고려하기에 앞서) 일차적으로, 내부 백업 인프라를 사용하여 문제의 파일을 복원할 것을 권장합니다. 그러기 위해서는 해당 데이터에 대한 백업 프로세스가 이미 있는 상태에서 백업 빈도 및 완전성에 관한 분석을 통해 데이터의 완전한 복원이 가능함을 확인해야 합니다.

필요한 복구 시점에 백업의 상태를 검증하는 것이 중요합니다. 공격자가 수개월 전부터 네트워크에서 활동했고 백업 파일도 암호화되었다면, 백업을 사용하여 시스템을 복원하는 것이 현실적으로 불가능할 수 있습니다.

베스트 프랙티스

시스템 백업은 중요한 베스트 프랙티스 중 하나입니다. 중요 시스템에 대해 정기적으로 유효한 백업을 생성하고 그 백업의 상태를 테스트해야 합니다. 백업은 기본 네트워크와 다른 곳에 저장하고, 쓰기가 아닌 읽기 접근 권한만 부여하십시오. 오프라인 백업이 바람직하지만, 비용 및 물류 부담이 따를 수 있습니다.

오랫동안 네트워크에서 은밀하게 활동한 공격자는 백업에도 영구적인 메커니즘을 심어 두었다가 몸값이 지불된 후에도 다시 해당 기업을 위협할 수 있습니다. 백업을 이중화하고, 수시로 점검하며, 격리하거나 오프라인 상태로 보관하여 조작의 가능성을 최소화하는 것이 바람직합니다.

네트워크 공유가 악성 암호화의 피해를 입은 경우, 최신 백업에 부분적으로 암호화된 파일이 포함되었을 수도 있습니다. 예컨대 어떤 기업의 파일 공유를 매일 백업하는데, 감염된 직원의 디바이스가 무려 5일간 탐지되지 않고 파일 공유의 모든 것을 암호화했다면, 지난 5일간 생성된 백업 중에 암호화된 파일이 포함되었을 수도 있습니다.

업계 표준 베스트 프랙티스를 따르는 신뢰할 만한 백업 프로세스를 마련하는 것이 좋습니다. 이를테면 로컬에 백업을 보관할 뿐만 아니라 이동식 미디어(테이프, 광디스크, 이동식 하드 디스크 등) 및 클라우드 기반 리소스에도 아카이빙합니다.

로컬 디스크 이미지, 복제, 기타 로컬 네트워크 백업에만 의존했다가 낭패를 볼 수도 있습니다. 이들 역시 랜섬웨어에 의해 암호화될 가능성이 있고, 랜섬웨어가 파일을 암호화한 후에 백업이 실행되었다면 내부 복구용으로 사용할 수 없기 때문입니다.

암호화 되돌리기?

백업에서 파일을 온전히 복원하지 못할 수도 있습니다. 그럴 때는 몸값을 내지 않고 암호화를 해결할 방법을 모색해야 할 것입니다. 어쩌면 감염된 시스템에서 해독 키를 찾아낼 수 있습니다. 둘 다 가능한 방법이지만, 성공 가능성은 매우 낮습니다.

랜섬웨어 감염의 변종 및 버전을 알아내면, 해결책을 찾는 데 도움이 될 수도 있습니다. 이 정보가 복구 단계에서도 유용하게 쓰입니다. 복구 방식 및 각 방법의 결과를 판단하는 데 참조할 수 있습니다.

암호화 리버스 엔지니어링의 가능성을 타진하려면, 먼저 악성 코드 변종에 대해 정통하고 여러 가지 옵션을 탐색 및 제시할 수 있는 SME를 참여시켜야 합니다.

당국 신고 요건

대부분 기업은 각자에 적용되는 규정 준수 및 규제 요건을 잘 알고 있습니다. 일반적으로 이러한 요건은 모든 데이터 침해 및 고객/개인 정보 유출 사건에 적용됩니다. 정부 기관, 군, 공공 기관은 더욱 특화된 보고 의무가 부여되기도 합니다.

민간 영역에서는 업종에 따라, 침해 행위에 대한 신고 요건이 현지 법에 의거하여 달라질 수 있습니다. 규제 요건, 국가 간 고객 데이터 유출, 특별 데이터(예: 의료 데이터) 유출 관련 사항이 여기에 포함될 수 있습니다. PCI-DSS, HIPAA, GDPR, CCPA(California Consumer Privacy Act) 등과 같은 특정 요건이 적용되기도 합니다. 하지만 거의 모든 경우에 침해 행위에 대한 신고는 즉시 이루어져야 합니다.

미국에서는 침해 행위가 확인되는 즉시 FBI IC3(Internet Crime Complaint Center) 절차에 착수해야 합니다. 또한, 현지 법 집행 기관에도 알리는 것이 좋습니다.

IBM Security Resilient에서는 기업이 신고 절차 및 시기를 신속히 확인할 수 있도록 지원합니다.

몸값 지불: 고려할 점

결국 몸값 지불 여부를 결정해야 하는 순간이 올 수도 있습니다. 예컨대 최대한 일찍 운영을 정상화해야 하거나, 다른 방법으로는 복구 불가능한 중요 파일에 접근해야 하는 경우에는 서둘러 결정하라는 압박을 받기도 합니다. 인명 피해가 예상되거나, 즉시 운영이 정상화되지 않으면 회사의 존립이 위태로워지는 등의 이유로 몸값 지불을 고려하게 됩니다.

몸값을 지불하거나, 지불하지 않겠다는 결정 모두 중대한 영향을 미칠 것입니다. 해당 기업의 위험 관리, 비즈니스 연속성 목표/다운타임 비용, 규제 관련 사항, 법적 영향, 공격자가 모든 파일을 해독할 방법을 제공하지 않거나 몸값을 받은 후 더 큰 금액을 요구할 가능성을 고려하면서 결정해야 합니다.

일반적으로, 몸값 지불 결정에는 회사 내부의 이해 관계자들이 참여해야 합니다. 그와 더불어 사고 대응 SME의 자문을 구하고, 회사와 계약한 사이버 보험사의 약관 및 서비스도 확인하는 것이 바람직합니다. 몸값 협상 전문가가 참여할 경우, 해당 사이버 범죄 단체의 이전 사례에 관한 정보를 얻을 수도 있습니다.

여기서는 몸값 지불 결정에 관한 논의에서 중요하게 다뤄야 할 점을 정리합니다.

몸값 지불이 복구를 보장하지 않음

말 그대로 범죄자, 신뢰할 수 없는 상대에게 돈을 주는 것입니다. 몸값을 챙긴 범죄자가 약속을 지킬 수도, 지키지 않을 수도 있습니다. (회수 불가한) 지불이 완료되는 순간 사라질 위험성도 있습니다. 대부분 사이버 범죄자가 몸값이 지불되면 파일을 해독할 수단을 제공하지만, 그렇지 않을 가능성도 배제할 수 없습니다.

몸값 지불이 즉각적인 복구를 의미하지 않음

몸값을 내고 해독 키를 받더라도, 이 키를 사용하여 당장 복구할 수 있는 경우는 드뭅니다. 파일 해독은 수작업으로 이루어집니다. 게다가 개별적으로 해독해야 하므로, 시간이 오래 걸리는 수고스러운 과정입니다.

범죄자가 돈을 받고 해독 키를 제공하더라도, 복구 절차가 시스템 이미지를 다시 생성하는 것만큼 복잡하고 까다로울 수 있습니다. 몸값을 내지 않았을 때 못지않게 험난하고 비용이 많이 드는 복구 과정이 기다리는 셈입니다.

몸값 지불이 불법일 수도 있음

랜섬웨어 공격자에게 돈을 주어야 하는 상황이 늘면서 새로운 형태의 비즈니스가 등장했습니다. 바로 랜섬웨어 협상가들입니다. 이 새로운 분야에 뛰어든 민간 업체들이 기업의 몸값 협상 및 지불 과정을 돕는 유료 서비스를 제공합니다. 하지만 몸값 지불 여부를 결정할 때는 협상 기술 말고도 고려할 사항이 있습니다.

만약 미국 정부의 제재 대상 국가에 있는 사이버 범죄자에게 몸값을 지불했다가 연방법을 위반할 수 있습니다. 2020년 10월 1일 자 미 재무부 산하 해외자산 관리국(Office of Foreign Assets Control, OFAC) 권고안에 따르면, 러시아, 북한, 이란 등 제재 대상 국가의 공격자에게 몸값을 지불하는 데 동조할 경우 벌금이 부과될 수 있습니다. 랜섬웨어 협상 서비스를 제공하는 기업과 그 고객도 이 권고안의 적용을 받습니다.

> “OFAC는 랜섬웨어 공격의 피해자 및 대응 관계자가 랜섬웨어 지불 요구에서 제재와의 연관성이 의심될 경우 즉시 OFAC에 문의할 것을 권장합니다. 피해자는 해당 공격에 미국 금융 기관이 관련된 경우, 또는 주요 금융 서비스 제공에 심각한 타격을 줄 가능성이 있는 경우, 미 재무부 산하 사이버 보안/중요 인프라 보호국(Office of Cybersecurity and Critical Infrastructure protection)에도 알려야 합니다.”
>
> 출처: OFAC

귀사가 특정 단체나 지역과 관련된 공격임을 쉽게 알아내지 못하는 상황에도, 몸값 지불 결정으로 인해 OFAC로부터 벌금이 부과될 수 있습니다.

몸값 지불로 인해 더 공고해지는 사이버 범죄자의 비즈니스 모델

사이버 범죄자에게 돈을 건네면, 그들의 비즈니스 모델은 한층 더 강화됩니다. 더 많은 범죄자들이 몰려들게 만들고, 사이버 범죄 및 이 생태계에서 일어나는 각종 범죄까지 경제적으로 지원하는 셈입니다. 몸값을 지불하면, 여기에 고무된 공격자들이 결국 공격 빈도 및 몸값 액수를 점점 더 늘릴 것입니다.

몸값을 내면, 결국 공격자들에게 공격 횟수 및 몸값을 늘릴 동기를 부여하는 셈입니다.

사고 대응: 사후 조치

사후 조치(Post-incident activity)는 대응 계획의 중요한 부분이므로 생략해서는 안 됩니다. 사고의 규모에 상관없이, 상황 종료 후 이해 관계자들과 만나 잘된 점 및 잘되지 않은 점에 관해 논의하는 것이 좋습니다. 이러한 “학습 효과” 분석을 통해 차츰 프로세스를 개선하고, 향후 사고가 발생하더라도 더 효율적으로 처리하여 잠재적 영향을 최소화할 수 있습니다.

인프라 탐지 및 보호에 쓰이는 기술적 통제 장치에 대한 분석도 포함해야 합니다. 기술의 실효성을 분석함으로써 보안 성숙도 모델을 한층 더 발전시키기 위해 보안 기술의 아키텍처 수정, 투자 철회 또는 신규 투자가 필요한지를 확인할 수 있습니다.

각 기업의 상황은 저마다 다릅니다. 따라서 여기서 살펴본 권장 사항은 일반적인 차원으로 이해해야 합니다. 귀사가 겪을 수 있는 어떤 사고 유형에서든 도움이 필요하다면, 해당 IR 팀 또는 서비스 제공업체에 문의하십시오.

IBM Security X-Force 리소스

IBM Security X-Force IR(Incident Response) 핫라인

북미
24x7 핫라인: 1-888-241-9812

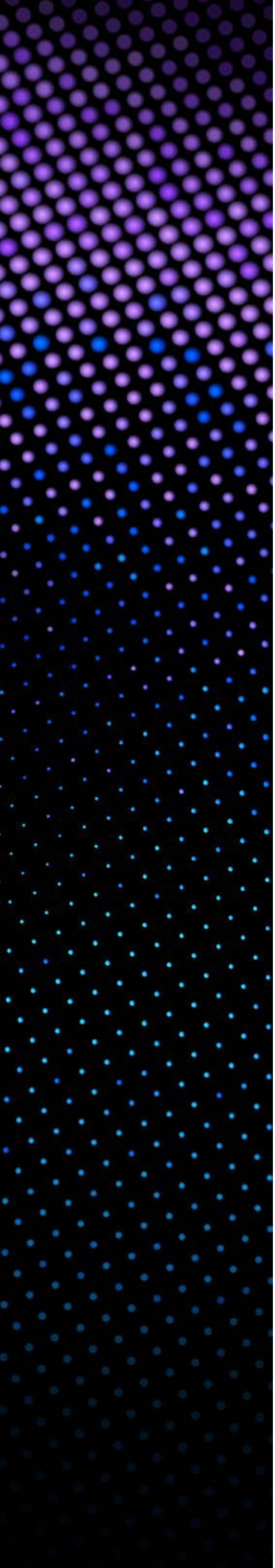
글로벌 핫라인:
+00 1 (312) 212-8034

IBM Security X-Force Threat Intelligence

위협 인텔리전스 서비스 - 글로벌 인텔리전스 전문가 팀이 통합 플랫폼에서 차원 높은 분석을 통해 보안 워크플로우 애플리케이션을 위한 위협 정보를 제공합니다.

IBM Security X-Force IR(Incident Response)

사고 대응 서비스 - 리테이너 서브스크립션 및 선제적 서비스를 통해 사고 대응 시간을 단축하고 보안 침해의 영향을 최소화하면서 더 빠른 복구를 지원합니다.



IBM Security

저자

Limor Kessem
Mitch Mayne

IBM Security
New Orchard Rd
Armonk, NY 10504

Produced in the United States of America
2020년 11월

IBM