HIS Visual

알면 보이는 싸움의 기술
랜섬웨어 완벽 방어·차단하기

올 초 IT 전문 매거진의 설문조사에 따르면 '랜섬웨어[1] 공격을 당한 경험이 있는가' 라는 질문에 응답자의 75%가 공격을 당했고, 50% 이상이 피해를 봤다고 답변했으며, 피해자의 54%는 데이터를 포기했다고 한다. 랜섬웨어에 감염이 되면 서비스 중단에 그치지 않고 기업의 중요한 데이터 손실을 피할 수 없다. 지난 6월 1일 토크IT에서 방영된 '랜섬웨어 대응방안에 대한 오해와 진실' 방송을 통해 랜섬웨어와 대응 방법을 알아보자.

랜섬웨어를 둘러싼 오해와 진실

랜섬웨어에 감염됐어도 기업의 신뢰도에 영향을 미칠 것을 우려해 답변을 안 한 경우를 고려하면 더 많은 감염과 피해 사례가 있을 수 있다. 컴퓨터 사용자의 문서를 '인질' 로 삼아 돈을 요구하는 랜섬웨어에 대한 오해 '다섯 가지' 를 먼저 살펴보자.

오해 1

백신 · 방화벽 · APT 방어 솔루션을 도입하면 안전하다?

PC에 설치되는 백신, 방화벽, IDS(Intrusion Detection System)[2]/IPS(Intrusion Prevention System)[3], APT 방어 솔루션 등에 랜섬웨어 패턴을 등록해 예방한다고 해도 절대 안심할 수 없다. 랜섬웨어는 지금도 진화하고 있다. 모든 패턴을 등록하는 것도, 지속해서 업데이트하기도 쉽지 않다. 랜섬웨어 감염 파일을 복호화해 복구하기 위해 백신 프로그램으로 랜섬웨어 감염 파일을 치료하려 해도 복호키를 확보하지 못하면 무용지물이다.

1) 랜섬웨어 : 미국에서 발견된 스파이웨어 등의 신종 악성 프로그램으로 컴퓨터 사용자의 문서를 볼모로 잡고 돈을 요구해, '랜섬(Ransom)' 이라 함. 인터넷 사용자의 컴퓨터에 잠입해 내부 문서나 스프레이시트, 이미지 등을 암호화해 열지 못하도록 만든 후 해독용 열쇠 프로그램을 전송해 준다며 금품을 요구한다.

2) IDS(Intrusion Detection System) : 침입 탐지 시스템. 컴퓨터 또는 네트워크에서 발생하는 이벤트들을 모니터링하고, 침입 발생여부를 탐지하고 대응하는 자동화된 시스템

3) IPS(Intrusion Prevention System) : 침입 방지 시스템. 비 인가된 사용자가 자원의 무결성, 기밀성, 가용성을 저해하는 행위를 실시간으로 탐지해 차단한다.

오해 2

랜섬웨어 방어 전용 제품이어야만 한다?

랜섬웨어 전용 제품의 경우 1 '미끼' 를 투척해 랜섬웨어 악성코드가 파일을 암호화하는 것을 찾아내 차단하거나 2 감염 프로세스 전체를 보고 블랙리스트, 화이트리스트, 임계치 기반 정책의 3단계에 걸쳐 차단을 하거나 3 랜섬웨어 프로세스 차단과 백업을 동시에 수행하는 등 세 가지 방법을 사용한다. 하지만 이 경우에도 완벽한 대응은 어렵다. 전 세계적으로 발생하는 랜섬웨어는 지금도 계속 진화하기 때문에, '동작 프로세스' 와 '공격 대상 파일' 을 변경하며 금전적 이득을 취하고자 한다.

오해 3

이메일 및 광고를 모니터링해 차단하면 된다?

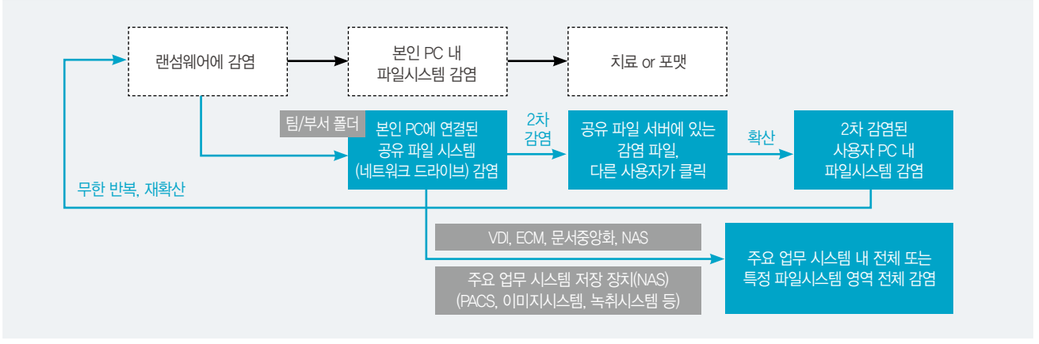
국내 소프트웨어 회사의 '2016년 3분기 스팸 메일 동향 분석 리포트' 에 따르면 바이러스 메일은 전 분기 대비 92% 증가했으며, 첨부파일을 통한 랜섬웨어가 다수를 차지했다고 한다. 랜섬웨어는 발신자와 제목을 수시로 변형하고 있어 완벽한 차단이 불가능하다. 영어로 오는 메일을 차단하면 80% 정도 막을 수 있다고 하지만 최근에는 한국어 스팸 메일도 늘고 있어 효용성이 낮다.

오해 4

랜섬웨어 방지는 개인의 몫이다?

랜섬웨어의 1차 피해는 개인이 입지만 업무 환경이 네트워크 기반에서 이루어지고 있어 사내의 누군가가 랜섬웨어 피해자가 되면 네트워크에 연결된 공유 폴더가 통째로 감염될 수 있다. 피해가 전사적으로 확산되는 것은 시간문제다. 감염 확산 경로 및 영향 정도를 살펴볼 때 랜섬웨어는 개인의 문제가 아닌 기업 전체의 문제라고 봐야 한다.

랜섬웨어 감염 확산 경로 및 영향도



오해 5

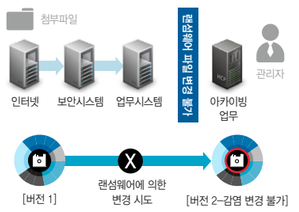
랜섬웨어 감염 대응의 유일한 방안은 **백업뿐이다?**

모든 종류의 랜섬웨어에 대한 대비책으로 기존의 백신이나 방화벽 등의 알려진 방식으로 대응하는 것은 현실적으로 불가능하다. 백업만이 유일한 대비책이라는 주장도 있지만, 그렇지도 않다. 백업은 문제 발생 시 데이터 복구를 위한 '보험'의 성격이 강하다. 하지만 현실적으로는 이슈가 발생한 바로 그 시점으로 복구하기 어렵다. 이를 대비해 실시간 백업을 한다면 감염 역시 실시간으로 확산될 수 있다. 중요도가 높은 시점의 데이터를 잃어버릴 수밖에 없는 상황이다.

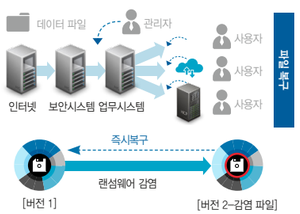
랜섬웨어 대응! 발상의 전환을 하자

기존의 랜섬웨어 대응 방안은 크게 두 가지로 나눌 수 있다. 먼저 보안 시스템에서 이메일, 광고에 대한 바이러스 검사 및 첨부 파일을 검사하는 방식이다. 다양한 형태의 랜섬웨어가 탄생하면서 이 방식으로는 100% 감시할 수 없다. 두 번째는 백업 시스템으로 데이터 백업을 수행한 후 백업 데이터로 복구하는 방식이다. 이 경우 복구 시간이 길고 데이터 손실이 발생한다. 개별 PC 사용자에 대한 대응 역시 미비하다.

제안 01 **파일 변경 원천 차단**



제안 02 **파일 버저닝 통한 업무 시스템 복구**



효성인포메이션시스템(HIS)이 제안하는 방법은 두 가지다. 감지, 차단, 예방을 위한 보안 솔루션으로는 100% 예방과 차단을 할 수 없으므로 파일 변경 자체를 차단하는 것이 첫 번째다. 백업 및 복구 솔루션을 도입해도 완벽하지 못하다면 감염 직전의 최신 버전으로 되돌리자는 것이 두 번째다.

HIS의 제안 01 파일 변경 원천 차단

파일 변경 원천 차단(WORM, Write Once Read Many)은 주로 장기 보관 원본인 아카이빙성 파일이나 원본성 파일의 감염 리스크를 줄일 방법으로, 컴플라이언스 상의 데이터 보관과 관리 의미가 강한 파일 감염의 위험 부담을 크게 줄일 수 있다. HCP(Hitachi Content Platform)는 내 · 외부에서의 어떠한 시도에도 파일 감염이나 변경할 수 없도록 한다.

HIS의 제안 02 파일 버저닝 통한 업무 시스템 복구

중요 업무 시스템 단위로 랜섬웨어에 대응하는 방법이다. 감염 직전의 버전으로 빠르게 복구하는 것으로, 별도의 백업 시스템이 없어도 된다. 시스템 아카이빙 복구 방식은 관리자 단위에 의해서만 데이터 복원이 가능하고, 개별 사용자별 복원이 불가능했다. 따라서 복원 시점의 최신 데이터 복원에 어려움이 있다. HCP는 랜섬웨어의 패턴에 관계없이 이전 버전으로 바로 복원이 가능하다.

랜섬웨어, 그것이 알고 싶다
Q&A

01

랜섬웨어의 감염 경로는 어떻게 되는가. 또 감염된 후 복구 방법이 암호 코드를 받아서 푸는 방법도 잘 안되는 경우가 많다고 하는데 이유가 무엇인가.

랜섬웨어는 웹 사이트, 스팸 메일이나 피싱, 파일공유 사이트, 사회 관계망 서비스 등 네트워크가 연결된 환경에서 다양한 경로로 감염된다. 일부 해독이 된 코드에 대해서는 복호화가 가능하나 지속해서 새로운 코드가 개발되므로 복호화만으로는 랜섬웨어에 완벽하게 대응할 수 없다.

02

정품인증이 안된 OS에서 거의 랜섬웨어가 발생하고 있다고 들었고, 내 경우도 그렇다. 그렇다면 윈도우 업데이트 만으로도 충분하지 않을까. Virus Defender와 같이 사용하면 방어가 되지 않나.

코드가 분석된 랜섬웨어는 보안 솔루션으로 충분히 대응할 수 있지만 랜섬웨어가 지속적인 코드 개발로 업데이트되고 있으므로 보안 솔루션만으로는 완벽한 대응이 어렵다.

03

회사의 업무 PC가 랜섬웨어에 걸린 적이 있다. 아무리 노력해도 걸리는 건 어쩔 수 없구나 하는 생각이 들었다. 결국, 개인의 백업 능력에 따라 피해가 커지거나 줄일 수 있다는 생각이 든다.

'외부로부터의 공격을 막아야만 한다' 그리고 '잃어버린 데이터는 복구해야 한다'라는 프레임에 갇혀있다 보니 다른 좋은 방안을 놓치고 있는 것 같다.

04

리눅스, 애플 등 윈도우 외의 시스템도 마찬가지로 랜섬웨어에 감염이 되는가.

최근 리눅스 시스템에 감염된 랜섬웨어 피해 사례도 발견되었다. 랜섬웨어는 계속 IT의 취약점을 찾아서 공격할 것이다.

05

랜섬웨어에 감염되고, 폴더들이 암호화된 후에 복호화를 하지 않은 상태에서 그대로 내버려 두면 어떻게 되나. CERBER Ver 6 같은 경우 숙주가 되는 실행 파일을 스스로 삭제하고 사라져서 추가 감염은 안 된다고 들었다.

랜섬웨어 종류마다 다르다. 최근 랜섬웨어가 더욱 진화되면서 숙주 파일은 사라지지 않고 남아있는 경우가 대부분이다. 그로 인해 다시 랜섬웨어에 감염되면 결국 중요한 데이터를 잃어버리게 된다. 적극적으로 해결해야 한다.

06

랜섬웨어 방어 전용 제품 사용은 백신처럼 로컬 PC에 설치해야 하는가. 로컬 PC에 설치해 사용할 경우 기존의 DRM이나 백신 소프트웨어와 충돌이 나지 않나.

HCP의 경우 개인 PC에 에이전트 형식으로 설치하는 프로그램이 아닌 기업시스템 내에서 랜섬웨어에 대응하는 솔루션이다. 그러므로 에이전트 설치로 인한 DRM과의 충돌은 염려하지 않아도 된다.

07

'랜섬웨어를 막는다' 라기 보다는 랜섬웨어에 감염되었을 때 빨리 복구하기 위한 솔루션이라고 보면 되나.

장기 보관이 필요한 기업의 중요한 데이터에 대해서는 위변조 방지를 통해 데이터 자체에 읽기/쓰기(Read/Write)가 불가능하게 만드는 방식으로 랜섬웨어에 대해 원천적으로 방어한다. 변경 사항이 많고 사용자 간 공유가 많은 파일에 대해서는 버저닝 기능을 통해 복구 기능을 제공한다.

08

랜섬웨어에 대한 100% 방어는 불가능하다고 본다. 기업에서는 가상화를 통한 백업과 문서중앙화를 철저히 적용하면 랜섬웨어는 점차 소멸되지 않겠는가.

기업이 다양한 대응 방안을 도입하고 있기 때문에 랜섬웨어 피해를 점차 감소할 것이지만, 새로운 랜섬웨어 코드가 지속해서 개발되고 있으므로 복구 방안을 항시 준비하고 있어야 한다.

09

랜섬웨어에 대비해 백업하는 경우 백업 속도와 복원 속도가 관건이다. 이 부분에 효성인포메이션시스템 솔루션은 어떤 강점이 있는가.

우리가 제안하는 방법은 풀백업과 증분백업 등 일반적인 백업 방안이 아니다. 파일 변경이 있을 때마다 새로운 버전을 생성하는 버저닝 기능으로 백업을 수행한다. 백업 속도를 굳이 안 따져도 된다. 복원에 대해서는 원하는 시점으로 모든 파일의 버전을 변경할 수 있다.