보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

효과적인 랜섬웨어 대응, 무엇이 필요한가?

AhnLab 2021-08-02

이제 랜섬웨어는 지근거리에서 우리에게 지속적인 위협을 가하는 존재가 되었다. 계속해서 피해 발생하고 있지만 어느 누구도 완벽한 랜섬웨어 방어를 장담하지 못한다. 그리고 그것이 현실이다. 하지만, 단계 별로 충실하게 랜섬웨어 대응 체계를 구축하면 사전 예방 역량을 강화하고 감염 시에도 피해를 최소화할 수 있다.

이번 글에서는 효과적인 랜섬웨어 대응을 위해 갖춰야할 사항들을 알아본다.

2021년 8월 현재, 랜섬웨어 공격을 한 번도 겪어보지 않은 기업을 찾는 것이 힘든 상황이 되었다. 그만큼, 기업, 금융, 의료 및 공공 기관, 생산 시설 등 다양한 조직부터 일반 개인의 PC까지 랜섬웨어 공격은 수년간 멈추지 않고 발생하고 있다.

랜섬웨어 대응 방안이라는 주제를 다루면서 필자는 적지 않은 고민을 하게 되었다.

"랜섬웨어는 총 10가지 종류가 있고 최적화된 대응 방안은 7가지가 있다. 이것만 알고 있으면 93.19%의 랜섬웨어에 대해 대응이 가능하다"

위처럼 깔끔하게 내용을 정리해 전달할 수 있다면 모두가 만족할 수 있을 것이다. 하지만, 랜섬웨어 대응은 이처럼 간단하고 명쾌한 해답을 제시하기 어려운 것이 현실이다.

당장 이 글을 읽고 있는 독자들도 처한 환경이 다르고 각각의 업무마다 상이한 특성을 갖고 있다. 또, 업종 별 비즈니스 카테고리와 사업의 규모도 모두 다르다. 보안 조직 구성과 인력, 사전 구비된 솔루션까지 어느 조직도 모두 같지 않다.

이처럼 복잡다단한 랜섬웨어 대응, 현실적으로 어디서부터 어떻게 시작해야 대응 체계를 구축하고 피해를 최소화 할 수 있을지 다양한 시각으로 범용적인 대응 방안을 정리해 보았다.

랜섬웨어 공격 방식

구체적인 대응 방안을 살펴보기에 앞서 현재까지 대표적으로 알려진 랜섬웨어 공격 방식에 대해 살펴보자.

[그림 1] 랜섬웨어 공격 방식 정리

첫 번째로, 상당수의 랜섬웨어 공격이 다양한 파일을 통해 발생하고 있다. 랜섬웨어를 정상 파일로 위장해 사용자가 메일이나 SNS, 웹사이트를 통해 다운로드 받도록 유도하는 형태이다. 감염 성공 시, 디스크 내 문서파일을 암호화하는 경우가 가장 많았지만, 정상적인 부팅을 차단하고 디스크에 잠금(Lock)을 거는 사례도 증가하고 있다.

두 번째는 파일리스 공격이다. 별도의 악성코드 파일을 이용하지 않고, 웹 브라우저 취약점을 통해 PC 내 실행중인 정상 프로세스를 활용하여 랜섬웨어 공격을 시도한다. 취약한 광고 배너를 통해 감염되는 경우도 있지만, 공격자는 일반 사용자보다 원자재, 자동차, 건설, 정유, 원자력 에너지와 같이 전문적 업무에 필요한 정보를 다루는 사이트를 주요 공격 타깃으로 삼는다. PC 내 중요한 고급자료가 저장되는 경우 복호화 비용을 지불할 확률도 높아지기 때문이다.

세 번째는 비트락커를 통한 공격이다. 비트락커는 윈도에서 기본으로 지원하고 있는 디스크 암호화 방법으로, 패스워드를 입력해야 디스크 내 파일에 접근할 수 있도록 하는 보안 지원 기능이다.

공격자는 주요 서버를 타깃으로 내부에 침투한 뒤, 원격 데스크톱으로 접속하여 별다른 랜섬웨어 악성코드 없이, 비트락커로 디스크를 암호화하고 패스워드 제공 비용을 요구한다.

이러한 다양한 랜섬웨어 공격을 방어하기 위해서는 여러가지 대응 방안을 복합적으로 준비해야 한다.

대응 방안 1: 컨설팅, '객관적인 현황 분석'

랜섬웨어 대응의 첫 단계는 보안 컨설팅을 통한 '객관적인 현황 분석'이다. 실제 사례를 살펴보면 안타깝게도 랜섬웨어 사고를 당하고 난 뒤 후속 조치를 위해 보안 컨설팅을 의뢰해 진행하는 경우가 많다.

보안 컨설팅은 전반적인 보안 수준을 끌어 올리는데 큰 효과가 있기 때문에, 체계적인 보안 대응 프로세스가 갖춰지지 않은 조직이나 환경에서, 랜섬웨어 공격을 사전 예방할 수 있는 가장 좋은 방안이다.

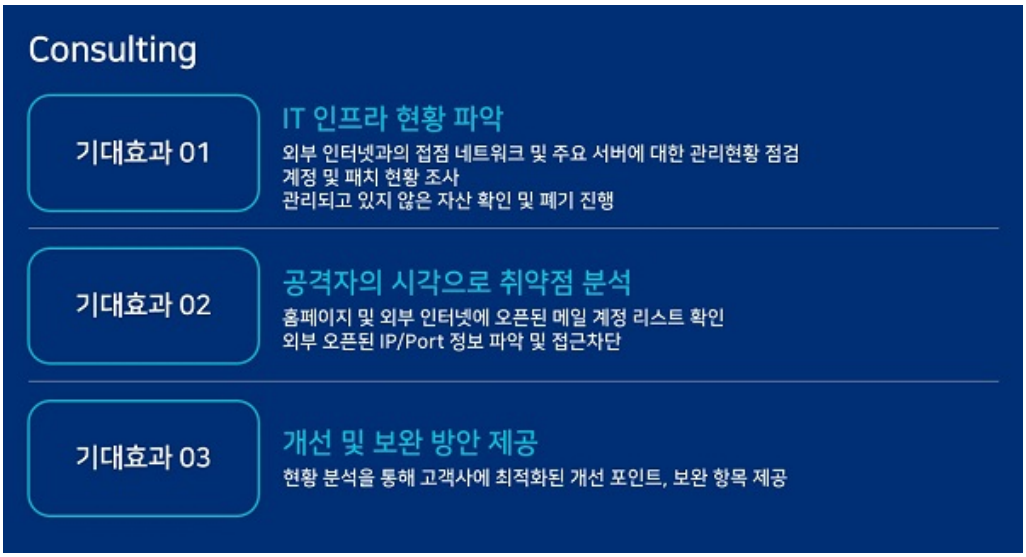
보안 컨설팅을 구체적으로 살펴보면, 먼저 조직 내부로 접근할 수 있는 다양한 취약점 루트를 찾아내기 위해 공격자의 시각으로 내부 인프라를 점검한다. 과거 발생한 사례 분석 자료가 풍부하게 준비되어 있기 때문에 어느 부분이 취약한지, 어떤 대응이 필요한지에 대해 신속하고 최적화된 대응을 우선 순위에 두고 가이드 할 수 있다.

보안 컨설팅을 통해 제공되는 리포트는 전반적인 침해 상황 분석과 함께 취약점 진단 정보를 제공한다. 여기에는 백신 관리, 패치, 계정과 공유폴더까지 공격자가 공격루트로 활용할만한 다양한 영역에 대한 점검 결과도 포함되어 있다.

특히, 주요 자산에 대해서는 상세 분석을 진행하므로, 최신 패치 적용 현황부터 시스템 운영 현황까지 세부 통계 데이터도 제공 가능하다. 또, 업계 평균과 비교해 어느 정도 보안 수준을 유지하고 있는지에 대해 수치화 된 평가 지수도 확인할 수 있다. 이를 통해 가장 준비가 부족한 부분을 인지하고 긴급 대응해야 할 우선 순위를 선정할 수 있도록 지원한다.

보안 컨설팅은 계정 관리에 대한 분석 결과도 제공한다. 실제로 여전히 많은 조직에서 기본 디폴트 관리자 계정을 사용하고, 동일한 패스워드를 여러 서버에 적용해서 운영하고 있으며, 패스워드 만료 기간과 같은 정책도 운영하고 있지 않다. 이 경우 공격자 입장에서는 서버에 대한 관리자 권한을 손에 넣는 것이 훨씬 수월해진다. 컨설팅에서는 계정 관리를 통해 주요 서버의 계정이 어떻게 관리되고 있는지 현황을 파악하고 효율적인 계정 관리 체계에 대한 가이드를 제공한다.

컨설팅을 통해 기대할 수 있는 랜섬웨어 대응 효과는 다음과 같다..



[그림 2] 컨설팅을 통한 랜섬웨어 대응 기대효과

우선, IT 인프라 최신 현황을 확인할 수 있다. 이 과정에서 사용하지 않는 낙후된 서버에 대한 점검 및 폐기도 진행한다. 이처럼 관리되지 않는 서버가 내부에 있다면, 공격자는 오래된 취약점 코드를 활용해 공격을 시작할 수 있다.

두 번째는 내부 취약점 분석이다. 공격자의 시각에서부터 다양한 부분에 대한 점검을 진행하고, 공개된 홈페이지에 노출된 대외 메일 계정 정보부터 외부에서 접속 가능하도록 오픈되어 있는 IP/Port에 대한 점검도 진행한다.

마지막 세 번째는 분석을 통한 개선방향 도출 및 맞춤형 보완 방안 제공이다. 이는 일반적인 대응 방안이 아닌 컨설팅 과정을 통해 파악한 조직의 특성을 반영, 최적화된 맞춤 대응 방안을 제공하는 것이 특징이다.

대응 방안 2: 트레이닝, '쉽고 친근한 접근'

다음 랜섬웨어 대응 방안은 바로 트레이닝(Training)이다. 여기서 트레이닝은 보안 담당자 그리고 일반 사용자에 대한 교육 등 다양한 종류의 트레이닝을 포함한다.

랜섬웨어 공격은 사용자의 호기심이나 실수를 유도하도록 설계되어 있으며, 이는 과거부터 계속 되어온 공격 기술 중 하나이다. 기능에 맞게 세분화된 보안 조직과 다양한 솔루션이 준비되어 있어도, 사용자의 보안 교육이 제대로 되어 있지 않다면 랜섬웨어 공격은 언제든 발생할 가능성이 존재한다.

보안 담당자는 최적화된 내부 사용자 보안 교육을 위해서, 기본적으로 최신 보안 이슈와 트렌드를 지속적으로 접하고 업데이트 해야 한다.

이에 대해 안랩은 자사가 보유한 플랫폼을 적극 활용해 다양한 최신 보안정보를 제공하고 있다.

먼저, 자사 홈페이지 '안랩닷컴'에서는 정기 간행물을 통해 최신 보안 이슈에 대한 다양한 정보를 확인할 수 있다. 주간 '시큐리티 레터'는 매주 최신 보안뉴스와 이슈, 그리고 사용자에게 도움이 될 만한 IT 관련 정보를 정리해 발간되고 있다. 매달 초 발행되는 '월간 安'은 '시큐리티 레터'보다 더 다양한 보안 주제에 대해 전문가의 심층적이고 상세한 분석 내용을 다룬다.

안랩의 보안 전문가들이 다양한 위협을 다각도로 분석해 인사이트를 제공하는 ASEC 블로그는 최신 위협 인텔리전스를 습득할 수 있는 최적의 플랫폼이다. 매주 약 2회 혹은 그 이상의 빈도로 게재되는 콘텐츠를 통해 국내 사용자들과 밀접한 연관이 있는 위협 정보를 지속적으로 공급한다. 한편, ASEC 블로그는 지난해부터 영문과 일문 서비스도 제공하고 있으며 70개 이상 국가 사용자들이 접속하고 해외 언론에도 인용되는 등 글로벌 시장에서의 입지를 넓혀가고 있다.

이 밖에, 언론에서 발행하는 보안뉴스도 일일이 검색해서 찾을 필요 없이, 안랩닷컴 '최신 보안 뉴스' 영역에서 날짜 별로 정리되어 있는 스크랩된 보안 기사를 확인할 수 있다. 또, '보안 용어사전'을 통해 신문기사나 보안 블로그에서 접한 새로운 보안 용어에 대해 서도 이해하기 쉽고 정확한 정보를 확인할 수 있다.

안랩은 지난해부터 가속화된 언택트 트렌드에 대응해 웨비나를 포함한 동영상 플랫폼을 적극적으로 활성화하고 있다. 지난 7월, 리뉴얼을 완료해 오픈한 웨비나 & 동영상 플랫폼 '안랩TV'는 사용자 친화적인 디자인과 편리한 검색 기능을 통해 사용성을 극대화했다. 무엇보다, 랜섬웨어 대응, 원격 근무 보안 등 최신 보안 트렌드에 관한 풍부한 영상을 단일 플랫폼에서 제공해 사용자들에게 보다 유익한 보안 정보를 제공할 수 있을 것으로 기대된다.

[그림 3] 안랩TV 리뉴얼 오픈

안랩이 운영하는 유튜브 채널 '삼평동연구소'는 IT, 보안, 개발 지식 공유를 목적으로 다양한 카테고리의 콘텐츠를 지속적으로 업데이트 하고 있다. 삼평동연구소의 영상은 보안을 전문적으로 다루지 않는 일반 사용자도 쉽게 이해할 수 있도록 구성되어 있다. 트렌드에 맞게 짧은 시간에 재미

와 함께 유익한 정보가 기억에 남도록 제작되었기 때문에 사내 보안 교육에 활용할만한 다양한 콘텐츠를 제공한다.

교육과 트레이닝을 통한 보안 인식 제고는 일반적으로 여겨질 수 있지만 랜섬웨어 대응에 있어 핵심적인 역할을 한다. 빈번하고 지속적인 랜섬웨어 사고, 이제 보안 대응을 전문가의 역할로만 한정 짓기에 위협은 너무도 가까이 와 있다. 따라서, 보안 담당자와 일반 사용자가 함께 대응해 나가는 노력이 필요하다.

일반 사용자를 대상으로 막연하게 최신 보안뉴스에 나온 랜섬웨어 공격을 안내하기 보다는, 직접 조직을 타깃으로 발생한 공격 사례나, 동종 업계에서 발생한 공격에 대해 일반 사용자의 눈높이로 내용을 정리하여 콘텐츠를 제작 & 공유하는 것도 권장할만한 방법 중 하나이다. 이를 통해 내부 구성원들이 보다 관심을 갖고 예방 활동에 참여하도록 유도할 수 있다.

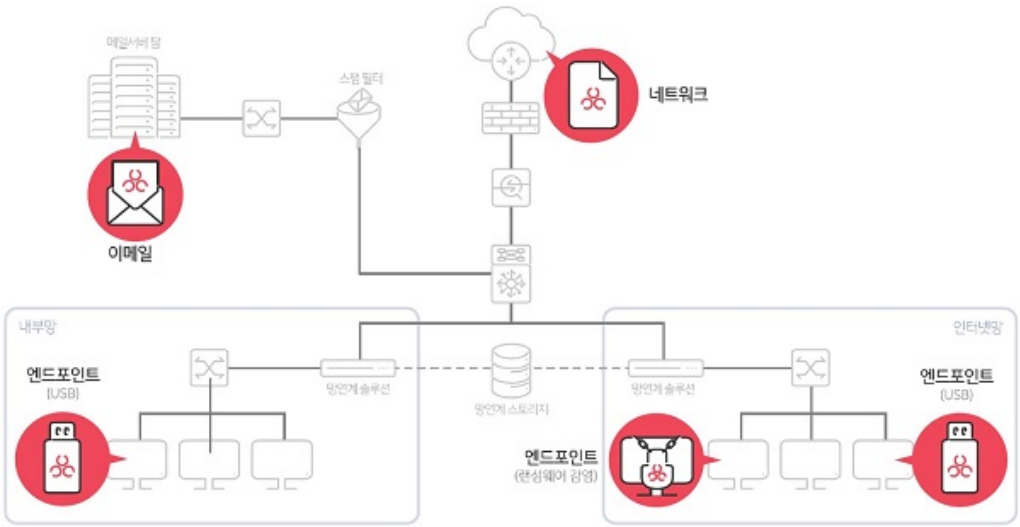
대응 방안 3: 솔루션, 자동화된 대응 체계

다음 세 번째 단계는 솔루션을 통한 자동화된 대응 체계 수립이다.

랜섬웨어 전용 솔루션이 시장에 많이 나와있지만, 다양한 공격 중, 솔루션에서 모니터링하는 일부 영역에 대해서만 최적화된 방어 기능이 동작하기 때문에, 치밀하게 설계된 타깃형 랜섬웨어 공격을 방어하기에는 분명한 한계가 있다.

사실 랜섬웨어는 일정 수준 이상의 솔루션을 도입하고 체계를 갖춰 운영한다면 공격으로 인한 피해를 최소화 하는데 효과적으로 활용할 수 있다. 랜섬웨어 대응에 있어 다양한 구간 별로 운영되는 솔루션의 역할에 대해 알아보자.

[그림 4]는 랜섬웨어 공격이 시작되는 구간이다.

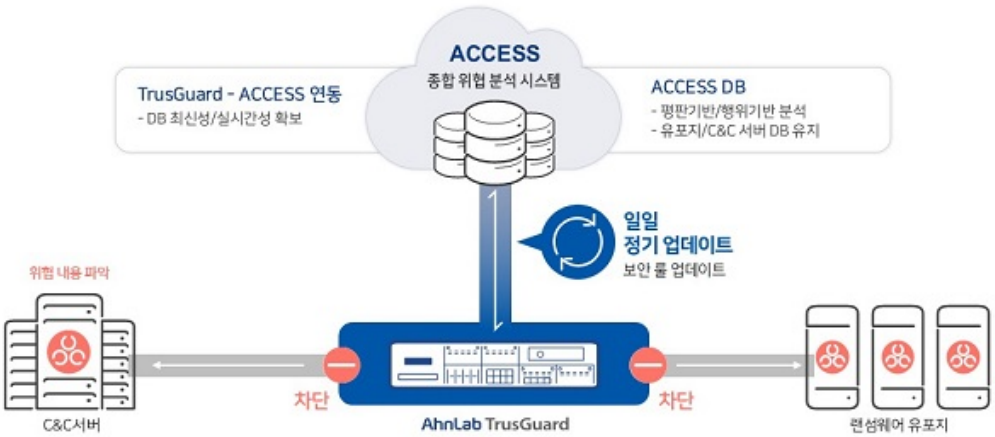


[그림 4] 랜섬웨어 공격 시작 구간

보다시피 네트워크, 이메일, 엔드포인트 구간을 통한 랜섬웨어 공격이 발생하고 있기 때문에 해당 영역의 보안 솔루션을 통해 대응이 가능하다.

네트워크: 방화벽, IPS/IDS, APT 대응 솔루션의 조화

기본적으로 네트워크 구간에는 방화벽이 존재한다. 방화벽은 랜섬웨어 다운로드 가능성이 높은 IP나 웹사이트에 대해서 실시간으로 차단하는 기능을 제공하며, 외부에서 내부의 중요 자산에 대한 IP, 포트(Port) 접근을 차단하는 역할도 담당한다.



[그림 5] AhnLab TrusGuard 방화벽을 통한 랜섬웨어 대응

관리자는 실시간으로 차단 가능한 Blacklist C&C IP 최신 업데이트를 진행해야 하며 IP, 포트에 대한 차단, 허용 규칙을 철저하게 관리해야 한다. 그리고 반드시 주기적인 방화벽 정책 체크를 진행해, 관리되지 않은 외부 접근 허용 정책이 존재하는지 점검해야 한다.

다음으로 IPS(Intrusion Prevention System)과 IDS(Intrusion Detection System) 솔루션은 외부에서 시도하는 스캔 공격을 탐지하고, 감염 PC에서 네트워크 취약점 공격을 통해 주요 서버로 확산을 시도하는 공격을 방어한다. 이를 통해서 감염이 의심되는 PC 정보도 탐지해 낼 수 있다.

마지막으로 APT솔루션은 네트워크 구간에서 웹, 파일서버, FTP를 통해 이동되는 전체 파일 중에 랜섬웨어를 식별하고 분석한다. 시그니처, 평판 엔진 외에도 샌드박스 엔진으로 알려지지 않은 신·변종 랜섬웨어도 탐지한다. 인터넷망 백본 외에 주요 서버가 위치한 네트워크 구간도 함께 모니터링 한다면 다양한 프로토콜을 통한 위협을 실시간으로 탐지하고 차단할 수 있다.

이메일: APT 대응 솔루션 활용

이메일을 통해 들어오는 랜섬웨어를 방어하기 위해서는 첨부파일과 메일 본문의 링크까지 검사해야 한다.

최근에는 빈번한 랜섬웨어 공격 때문에 메일의 첨부파일에 대해 점점 제약을 두는 경우가 많다. 메일에 첨부된 실행파일이나 공격에 활용되는 다양한 스크립트 확장자를 사전에 필터링하는 정

책을 적용하는 것이다. 이에 공격자들은 랜섬웨어를 직접 첨부하지 않고 메일 본문 또는 문서파일 내에 랜섬웨어 다운로드 링크를 삽입해 발송하는 수법을 활용하고 있다.

이와 같은 랜섬웨어 공격을 효과적으로 방어하기 위해서는 APT 솔루션을 통해, 메일 본문, 첨부문서의 본문 링크를 이용해 배포되는 파일을 수집해 샌드박스 분석을 진행해야 한다.

엔드포인트: 보안 플랫폼 연동을 통한 대응

그간 안랩은 위협 고도화에 대응해 유기적인 연동과 보안 플랫폼의 중요성을 지속적으로 강조해 왔다. 특히 엔드포인트 구간에서 위협에 효과적으로 대응하기 위해서는 백신, 패치 관리, EDR 등이 각자의 역할을 하면서 유기적으로 통합되어야 한다.

[그림 6] AhnLab EPP 구조도

세부적으로 하나씩 살펴보면, 먼저 백신 솔루션은 윈도우를 비롯해 유닉스, 리눅스, 맥OS, VDI 환경에서 알려진 랜섬웨어를 유입 시점에 시그니처와 행위 분석을 바탕으로 엔드포인트 구간에서 차단한다. 중요 폴더를 랜섬웨어 보호대상으로 등록해 놓을 경우 랜섬웨어 감염 시 폴더 내 파일이 암호화 되는 것을 사전에 방지할 수 있다.

다만, 백신을 엔드포인트의 가장 기본 솔루션으로 운영하면서도 일부 기능만 제한적으로 사용하는 경우가 많다. 이에, 최신 엔진 업데이트와 함께 랜섬웨어 대응을 위해 만들어진 다양한 기능을 활성화하여 운영하는 방안을 권고한다.

다음은 패치 관리(Patch Management) 솔루션이다. 혹자는 '패치 관리가 랜섬웨어와 무슨 관련이 있을까?'라는 의문을 가질 수도 있다.

하지만, 많은 랜섬웨어가 운영체제(OS)와 응용프로그램 취약점을 이용해 PC 관리자 권한을 탈취하려는 시도를 한다. 일부 랜섬웨어는 PC 1대를 감염시키고 나서, 네트워크의 다른 PC로 감염 확산을 시도하는 행위를 한다. 이때 OS 취약점을 이용하면 최신 패치가 되어있지 않은 수백, 수천 대

의 PC로 감염을 확산시킬 수 있다. 실제로, 잘 알려진 워너크라이(WannaCry) 랜섬웨어가 이런 방식으로 엄청나게 많은 PC를 감염시킨 바 있다.

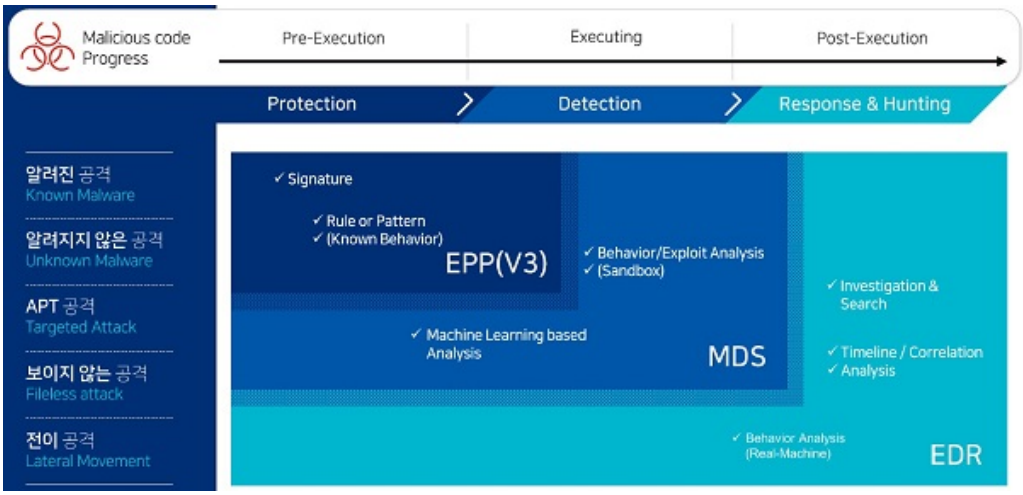
취약점 관리 측면에서 최신 보안 패치는 굉장히 중요하며, 이를 통해 랜섬웨어 감염 가능성을 낮추고 확산을 최소화하는 방향으로 활용 가능하다.

다음은 최근 몇 년 간 '핫한' 솔루션으로 주목받고 있는 EDR이다. EDR 솔루션은 PC의 모든 행위를 감시 및 추적하며 랜섬웨어의 주요 행위를 탐지한다. 구체적으로는 암호화 및 백업 삭제 행위를 탐지하고, 감염에 이르기까지의 모든 공격 흐름과 연관 정보를 수집한다. 즉, EDR에서 제공하는 정보를 통해 공격 루트를 비롯해 정책적으로 차단해야 할 C&C IP/URL 정보도 확인할 수 있다.

이어서, APT 솔루션의 에이전트도 랜섬웨어 대응 기능을 제공한다. 네트워크, 메일, USB를 통해 실행되는 파일을 실행 보류 후, 분석 장비의 샌드박스에서 검사한다. 랜섬웨어는 PC 내 문서를 대상으로 암호화 동작을 수행하므로, 샌드박스 행위 분석을 통해 이를 빠르게 탐지해 낼 수 있다. 이렇게 탐지된 랜섬웨어는 실행 보류 상태에서 차단 및 삭제되므로, 감염 전에 자동으로 모든 대응을 완료할 수 있어 가장 효과적인 대응 방식이라 할 수 있다.

아울러, 파일리스 공격도 APT 솔루션 에이전트를 통해 대응이 가능하다. 웹브라우저 취약점 공격을 모니터링하고, 발견 시점에 취약점 코드가 삽입된 프로세스를 강제 종료해서, 악성 행위가 발현되는 것을 사전 차단한다.

[그림 7]은 엔드포인트 영역에서 랜섬웨어 공격 발생 시, 솔루션 별 대응 순서를 정리한 것이다.



[그림 7] 엔드포인트 솔루션 별 랜섬웨어 대응 순서

먼저, 백신에서 시그니처 엔진을 이용해 알려진 랜섬웨어를 파일 생성 시점에 실시간으로 삭제한다. 백신에서 탐지되지 않는 신·변종 랜섬웨어는 APT 솔루션이 샌드박스와 머신러닝 엔진으로 분석해 감염 전에 차단한다. EDR은 랜섬웨어 공격 시 공격자가 활용한 전체적인 감염 루트와 잔여 악성코드 여부를 확인하여 최종 대응할 수 있도록 정보를 제공한다. 또, 확인된 공격 루트와 악성코드 정보는 다양한 솔루션의 Blacklist 기능을 활용하여 실시간 차단되도록 등록하여 관리한다.

TIP: 최신 위협 정보 습득

TIP(Threat Intelligence Platform)를 활용할 경우 랜섬웨어 공격에 대한 다양한 최신 정보를 얻을 수 있다.

TIP는 악성코드 관련 해시(Hash)나 IP의 정상·악성 여부를 제공하는데 그치지 않고, 실제 기업·기관에서 발생한 침해 사고와 관련된 위협 상관 관계 분석 등 풍부한 위협 정보를 제공한다. TIP의 'IOC Feeds' 기능은 악성코드 관련 정보, 네트워크 정보와 최신 취약점 정보를 공유한다. 뿐만 아니라, 다양한 상세 분석 정보와 산업군별 공격 발생 추이 및 통계 정보도 제공한다.

TIP가 제공하는 '뉴스 클리핑'을 활용하면 국내, 해외 뉴스를 통해 다양한 보안 이슈를 접할 수 있다. 그리고, 실제 조직 내로 동일한 공격 시도 있었는지 확인하고자 할 경우 TIP의 최신 뉴스 정보와 함께, 해당 공격에 사용한 파일과 IP/URL 목록을 확인하면 된다. 목록에서 해당 파일 및 IP를 클릭할 경우 상세 분석 정보와 연관 공격 히스토리도 직접 확인할 수 있다.

마지막으로, '클라우드 샌드박스' 역시 TIP에서 제공된다. 파일 또는 URL을 TIP에서 제공하는 클라우드 샌드박스 환경에서 분석할 수 있다. 윈도우와 리눅스 환경을 지원하며, 분석 결과에 대한 다양한 이벤트 분석 정보도 확인 가능하다.

이처럼 다양한 구간에 걸쳐 여러 솔루션을 통해 랜섬웨어에 대응하는 방법을 알아봤다. 랜섬웨어를 효율적으로 예방하고 대응하기 위해서는 특정 솔루션에만 기대는 것이 아니라, 현재 운영하고 있는 다양한 보안 솔루션들을 적재적소에 최적화하여 활용해야 한다.

대응 방안 4: 전문 서비스, '보안 전문가의 지원'

마지막으로 제안하는 랜섬웨어 대응 방법은 바로 보안 전문 서비스 활용이다.

앞서 소개한 컨설팅, 트레이닝, 솔루션이 랜섬웨어 감염을 사전 예방하는 목적이라면, 보안 전문 서비스는 보안 사고 발생 이후 어떻게 피해를 최소화하고 대응해 나갈지에 관한 가이드를 제공하는 것이 핵심이다.

두 가지 대표적인 서비스를 설명하면, 먼저 '악성코드 전문가 분석 서비스'는 랜섬웨어 등 공격에 사용된 파일을 분석가가 직접 정밀하게 분석하여 파일의 주요 행위, 특징 및 대응 방안을 종합적으로 검토해 고객에게 보고서를 제공한다.

다음으로, 침해사고 분석 서비스인 'A-FIRST(AhnLab Forensic & Incident Response Service Team)'은 랜섬웨어로 인한 보안 사고 발생 시, 감염된 자산에 대한 디지털포렌식 작업을 통해 감염이 어떤 경로로 발생했는지, 어떤 범위까지 피해가 있었는지를 분석하는 서비스다. A-FIRST의 보고서는 보안 사고의 시작부터 끝까지 전체 과정을 면밀하게 분석해 결과를 제공한다. 이를 통해 대응 및 사고 수습 방안에 대한 자세한 정보를 가이드한다.

결론: 랜섬웨어 대응, 기술과 사람의 협력 필요

지금까지 4가지 랜섬웨어 대응 방안에 대해 살펴봤다. 짧은 기간에 랜섬웨어 대응 방안을 마련하기 위해서는 솔루션을 검토하는 것이 가장 빠르지만, 보안 관점에서 내부 IT 인프라 환경에 대해 상세 분석을 진행한 적이 없는 환경이라면, 컨설팅을 통해 외부에 노출된 위협부터 제거해 나가는 것이 더 합리적인 방안이라 생각한다.

지금까지 필자가 많은 기업과 기관에 방문해 다양한 환경을 직접 접하면서, 가장 랜섬웨어 대응을 잘하고 있다고 생각된 곳은 최적화된 솔루션을 갖추고 있으면서 함께 일반 구성원의 보안 인식도 높은 조직이었다.

해당 조직은 일반 구성원들도 내부를 타깃으로 발생했던 랜섬웨어 공격 사례를 메일이나 공지를 통해 전달받고 있으며, 랜섬웨어 의심 메일이나 파일을 확인할 경우 어떻게 신고해야 하는지 숙지하고 있었다. 또, 실제 감염이 발생할 경우에는 보안 조직에서 수립한 대응 프로세스를 가이드 받고 빠르게 확산 방지 조치를 수행한다.

결국 랜섬웨어는 기술과 사람이 협력할 때 가장 효과적으로 대응할 수 있다. 랜섬웨어에 대한 막연한 두려움을 갖기보다는, 대응을 위해 현재 준비된 것이 무엇이며 어떤 것을 더 보완해야 할지 지속적으로 검토하여 더욱 견고한 방어 체계를 만들어 나가야 한다.

AhnLab 솔루션컨설팅팀 이종현 차장