보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

비즈니스를 위협하는 랜섬웨어, AhnLab MDS로 대응하기

AhnLab 2023-07-31

랜섬웨어란 '몸값'을 의미하는 랜섬(Ransom)과 소프트웨어(Software)의 합성어로, PC를 악성코드에 감염시켜 저장된 문서나 파일 등을 암호화한 후 복구를 대가로 금전을 요구하는 해킹 기법을 말한다. 랜섬웨어에 의한 침해사고 및 신고 건수는 매년 증가하고 있지만, 랜섬웨어 특성 상 감염 이후 치료 또는 복구가 어렵다. 이번 글에서는 랜섬웨어의 동향과 공격 경로를 살펴보고, 안랩의 샌드박스 기반 랜섬웨어 및 지능형 위협 대응 솔루션, 'AhnLab MDS'를 통한 보안 방안을 자세히 알아보자.

랜섬웨어의 최신 동향은?

2022년 전 세계 랜섬웨어 조직은 활동에 어려움을 겪었다. 주요 랜섬웨어 조직인 레빌(REvil)이 검거되고 콘티(Conti)가 운영을 중단하는 사태가 발생했으며, 우크라이나와 러시아 간 전쟁이 일어났다. 특히 러시아인으로 구성된 다수의 랜섬웨어 조직은 전쟁의 여파로 활동에 제약을 받았다.

하지만 랜섬웨어 피해를 입은 기업의 수는 점진적으로 증가하는 추세를 보인다. 2022년부터 활동한 랜섬웨어 조직은 50개 이상이며, 이 중 신생 랜섬웨어 조직은 23개가 넘는 것으로 알려졌다. 이들은 의료, 통신, 보험, 제조 등 다양한 산업군으로 공격을 확대하고 있다. 일정 수준의 보안 역량을 갖춘 글로벌 기업에서도 랜섬웨어 공격으로 비즈니스가 중단돼 수백억 원에 달하는 손실을 입었다. 국내에서는 최근 '귀신(Gwisin)' 랜섬웨어의 등장으로 골머리를 앓고 있으며, 랜섬웨어 대응 예산과 보안 솔루션 및 운영 인력이 부족한 중소기업이 핵심 표적이 되고 있다.

또한, 랜섬웨어 조직은 다크웹(Dark Web)을 통해 다변화되고 있다. 2020년 이후 RaaS(Ransomware as a Service)가 본격화되면서 랜섬웨어 조직은 정보 탈취형 악성코드(InfoStealer, 인포스틸러)를 이용해 탈취한 개인 및 기업의 주요 정보인 '스틸러(Stealer)' 로그를 다크웹을 통해 거래하기 시작했다. 그 결과, 지난 2년 동안 다크웹에

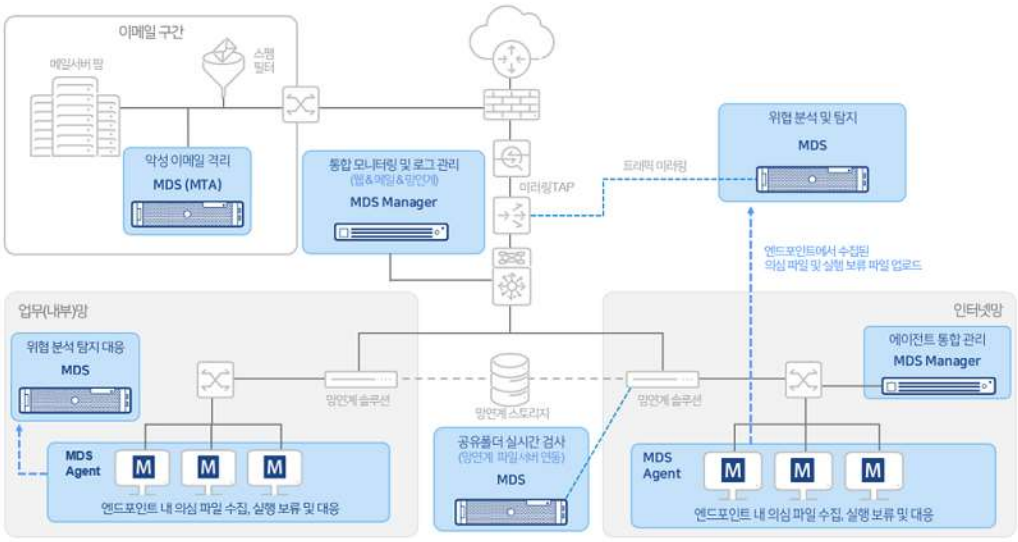
서 활동한 랜섬웨어 조직과 피해 기업의 수는 계속 증가했다. 스틸러 로그는 랜섬웨어 조직의 정보 탈취를 위한 툴 또는 초기 침투(Initial Access)에 활용된다.

이처럼 랜섬웨어 조직은 아직까지 매우 활발하게 활동 중이며, 여전히 기업 비즈니스에 있어 심각한 위협으로 간주된다. 공격자는 전형적인 공격 방식인 암호화 외에도 표적으로 삼은 기관의 중요한 데이터를 부가적인 협박 수단으로 삼아 유출하는 수법도 꾸준히 사용하고 있어 비즈니스 연속성을 유지하기 위한 대비가 필요하다. 또한, 보안이 비교적 취약한 본사의 협력사나 계열사를 공격하는 방식은 여러 제조업체에 막대한 피해를 주고 있어 랜섬웨어를 공급망 공격의 일부로 고려하고 대책을 강구해야 하는 상황이다.

랜섬웨어 대응에 최적화된 AhnLab MDS

랜섬웨어는 이메일, 네트워크, 엔드포인트, 망연계 등 사용자가 이용하는 모든 구간을 통해 유입될 수 있다. 특히 이메일은 불특정 다수에게 랜섬웨어를 유포할 수 있는 최고의 공격 수단으로, 공격자는 업무용 첨부 파일 형태로 악성코드를 퍼뜨리거나 사회공학기법을 활용한 랜섬웨어 공격을 수행한다. 이 외에, 업무에 필요한 불법 프로그램, 크랙(Crack), 보안 업데이트 파일로 위장한 랜섬웨어도 있으며, USB 외장하드 또한 랜섬웨어로부터 자유로울 수 없다.

안랩은 랜섬웨어 공격에 대응하는 최적의 보안 방안으로 안랩의 AhnLab MDS와 AhnLab MDS Agent, AhnLab MDS Agent 관제 서비스를 제시한다. 이들은 각각 다양한 경로로 유입되는 파일을 수집 및 실행을 보류하고, 시그니처 기반의 정적(Static) 및 평판 탐지와 비시그니처(Signature less) 방식인 샌드박스 기반 동적(Dynamic) 분석을 통해 악성 여부를 판별한 후 조치한다.



[그림 1] AhnLab MDS 구축 구성도

AhnLab MDS의 역할

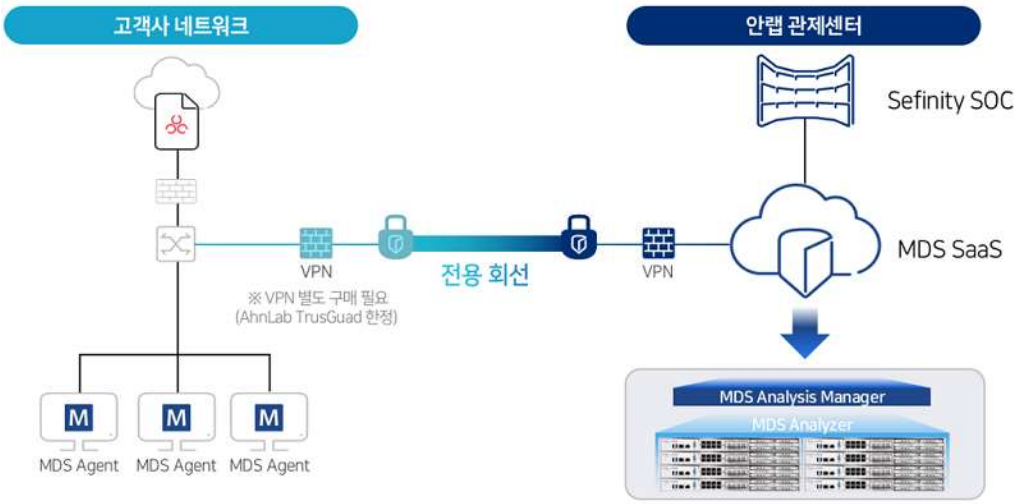
AhnLab MDS는 Mirror 트래픽 탐지/차단 구성뿐만 아니라 MTA(Mail Transfer Agent) 라이선스를 활성화해 메일 서버 탐지/차단 전용 장비로 구성할 수 있다. MTA는 MDS의 정적 분석, 동적 분석 기능을 포함하며, 메일 전송 및 필터링/격리, 피싱/스캠 메일 대응이 가능하다. 고객사 메일 서버 앞 단에 AhnLab MDS(MTA)를 구축하면 메일이 유입됐을 때 첨부 파일과 메일 본문을 파싱해 악성 URL 탐지, AI 기반 주요 키워드 확보 및 피싱 메일 DB와의 유사도 비교 등의 행위 분석을 수행한다. 그런 다음, 정상 메일만 서버로 수신할 수 있도록 악성으로 의심되는 메일을 장비 내부에 격리하고, 메일 수신자와 보안 담당자에게 알림을 전송한다.

AhnLab MDS Agent

AhnLab MDS Agent는 선택적으로 적용 가능한 옵션으로, 사용자 PC에 설치돼 네트워크를 통과하지 않거나 AhnLab MDS의 탐지를 우회한 신규 파일을 수집하고 실행을 보류한다. 실행을 보류하는 이 기능은 'Execution Holding(EH)'이라고도 불리며, 분석 결과가 없는 파일은 해당 PC에서 실행되지 못하도록 하여 랜섬웨어 감염을 예방한다. 해당 파일은 MDS 서버에 수집돼 분석 과정을 거치게 되며, 악성으로 판단되거나 분석 결과가 불분명한 파일은 해당 PC에서의 실행을 제한하거나 삭제할 수 있다.

AhnLab MDS Agent 관제 서비스

안랩은 최근 AhnLab MDS Agent 관제 서비스를 출시했다. 해당 서비스는 MDS 장비를 구매하기 어렵거나 보안 전문가가 없는 소규모 기관 및 기업에 특화됐다. 사용자가 PC에서 실행형 및 스크립트 기반 파일을 실행하면 AhnLab MDS Agent가 파일 실행을 잠시 보류하는 동시에 파일을 안랩의 내부 인프라에 구축된 AhnLab MDS로 자동 전송한다. 악성으로 확인된 파일은 즉시 삭제하고, 실시간 요약 및 상세 정보, TI 평판 정보가 포함된 대응 보고서를 보안 담당자에게 메일로 발송한다. 분석이 완료되기 전까지 파일 실행을 중지하기 때문에 랜섬웨어와 같은 악성코드의 최초 감염을 차단할 수 있다.



[그림 2] AhnLab MDS Agent 관제 서비스 구성도

AhnLab MDS Agent 관제 서비스를 백신과 함께 사용할 경우, 알려진 악성코드는 백신으로 대응하고, 알려지지 않은 위협은 AhnLab MDS Agent 관제 서비스로 예방하는 식으로 상호 보완할 수 있다. 또한, 별도의 장비를 구축하지 않고 AhnLab MDS Agent를 설치하기만 하면 서비스를 즉시 이용할 수 있어 중소기업도 구축 비용 및 운영 인력 부족으로 인한 부담 없이 엔드포인트 위협 대응 역량을 확보할 수 있다.

AhnLab MDS 신규 모델, 무엇이 달라졌나?

올해 5월 AhnLab MDS 제품은 기존 A모델에서 B모델로 업그레이드됐다. 고성능 패킷 처리 라이브러리를 탑재한 B모델은 트래픽을 A모델 대비 2배 이상 처리하도록 성능이 향상돼 일시적으로 트래픽 양을 증가시키는 형태의 랜섬웨어 공격도 완벽하게 방어한다.

[그림 3] AhnLab MDS B모델 개선사항

B모델의 최상위 장비는 10Gbps 트래픽을 처리할 수 있다. 성능 향상은 CPU 업그레이드를 통해 구현했는데, CPU 코어 수를 60% 늘려 CPU 성능을 43% 높였다. 또한, 기존 SD카드와 SATA3 SSD, HDD 저장소를 NVMe GEN4 M.2 SSD와 SATA3 SSD로 변경해 분석 성능도 개선했다.

이를 통해 B모델이 최고 사양 장비를 기준으로 작동할 수 있는 가상머신(Virtual Machine, VM)의 수가 128개에서 160개로 증가했으며, 단독으로 관리할 수 있는 에이전트의 수도 기존에는 5,000개였던 것에 비해 현재는 6,000개로 늘었다.

추가로, AhnLab MDS를 도입한 고객사는 악성코드 전문가 분석 서비스를 제공받을 수 있다. 이 서비스는 유료로 제공되지만, 올해 5월에 출시된 MDS 최신 펌웨어 버전부터는 3회 무료로 제공한다. AhnLab MDS를 통해 수집된 파일을 악성코드 분석 전문가 서비스를 통해 업로드하면, 안랩의 악성코드 분석 전문가가 해당 파일을 확인한 후 악성코드 유입 경로, 공격 기법, 대응 방안 등에 대한 보고서를 제공한다.

결론

랜섬웨어는 감염 이후 치료 또는 복구가 어렵기 때문에 사전 예방이 매우 중요하다. 랜섬웨어 공격을 예방하려면 먼저 중요한 자료를 정기적으로 백업하고, 인터넷과 분리된 곳에 보관한다. 모든 소프트웨어는 최신 버전으로 업데이트해야 하며, 백신과 같은 보안 소프트웨어를 설치하고 주기적으로 검사해야 한다. 또, 출처가 불명확한 URL은 실행해서는 안 되며, 기업 시스템에 대한 보안 취약점 점검을 수행하고 패치를 적용해야 안전하다. 이 같은 보안 수칙을 실천하면서, AhnLab MDS 및 AhnLab MDS Agent, AhnLab MDS Agent 관제 서비스를 도입한다면 안랩의 전문적인 악성코드 분석 및 대응 역량을 바탕으로 랜섬웨어로부터 기업을 보다 더 안전하게 보호할 수 있을 것이다.

AhnLab 콘텐츠기획팀 서보경 사원