보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

Log4j 취약점 대응에 AhnLab TIP가 필요한 이유

AhnLab 2022-02-07

최근 공격자들은 한 번의 공격에 수십 가지의 기법을 활용해 공격하기도 하고, 보안 취약점을 파고드는 등 공격 대상을 지능적으로 집요하게 노린다. 이와 같은 상황에서 평면적인 위협정보 수집을 통한 대응에 한계를 느낀 사용자들에게 '위협 인텔리전스 플랫폼(Threat Intelligence Platform: TIP)'이 주목받고 있다. 최근 전세계를 떠들썩하게 한 Log4j 취약점은 즉각적인 대응을 요구해 TIP의 필요성을 더욱 부각시키고 있다.

이번 글에서는 안랩의 차세대 위협 인텔리전스 플랫폼 'AhnLab TIP'를 활용한 Log4j 취약점 대응 방안과 AhnLab TIP의 기술적 특장점을 조명한다.

2021년 12월 초 발견된 Log4j 취약점은 역사상 최악의 취약점으로 불리며 아직까지도 전 세계 사용자들을 위협하고 있다. 아파치(Apache) Log4j 2 라이브러리에서 발생하는 원격 코드 실행(Remote Code Execution) 취약점으로, 공격자는 Log4j를 사용하여 로그를 저장할 때 특정 문자열을 활용해 원격 서버의 자바 객체가 실행되도록 유도한다. Log4j 취약점에 관한 자세한 내용은 월간안 1월호 '공포의 Log4j 취약점, 효과적인 대응 방안은?'을 확인하면 된다.

Log4j 취약점 대응의 관건은 '신속성'에 달렸다고 해도 과언이 아니다. 새로운 취약점 발견과 이를 보완한 신규 버전 패치가 짧은 주기로 이어지고, 해커들의 공격 동향이 계속해서 업데이트되는 가운데, 기업들은 최신 정보를 빠르게 입수하여 적절한 조치를 수행해야 한다. 당장 오늘 새로운 취약점이 발견되면, 어제 적용한 조치는 무용지물이 될 수 있기 때문이다.

기업의 보안 담당자들 입장에서는 해야 할 일이 많아졌다. 최신 뉴스를 확인해 동향을 파악하고, 보안기업 혹은 기관의 홈페이지를 통해 공지사항과 지침을 확인해야 한다. 또한, 분석 보고서를 정독해 세부적인 내용을 습득하고 전문 블로그를 탐색해 별도의 인사이트를 얻는 경우도 많다.

문제는 위 문단에서 열거한 정보들이 모두 각기 다른 곳에 산재해 있다는 것이다. 보안 담당자들이 필요한 정보들을 모두 찾으려면 정보가 제공되는 지점을 하나하나 반복적으로 확인해야 한다. 필연적으로 많은 시간과 자원을 투입해야 하고 업무 효율성에 영향을 미칠 수 밖에 없다.

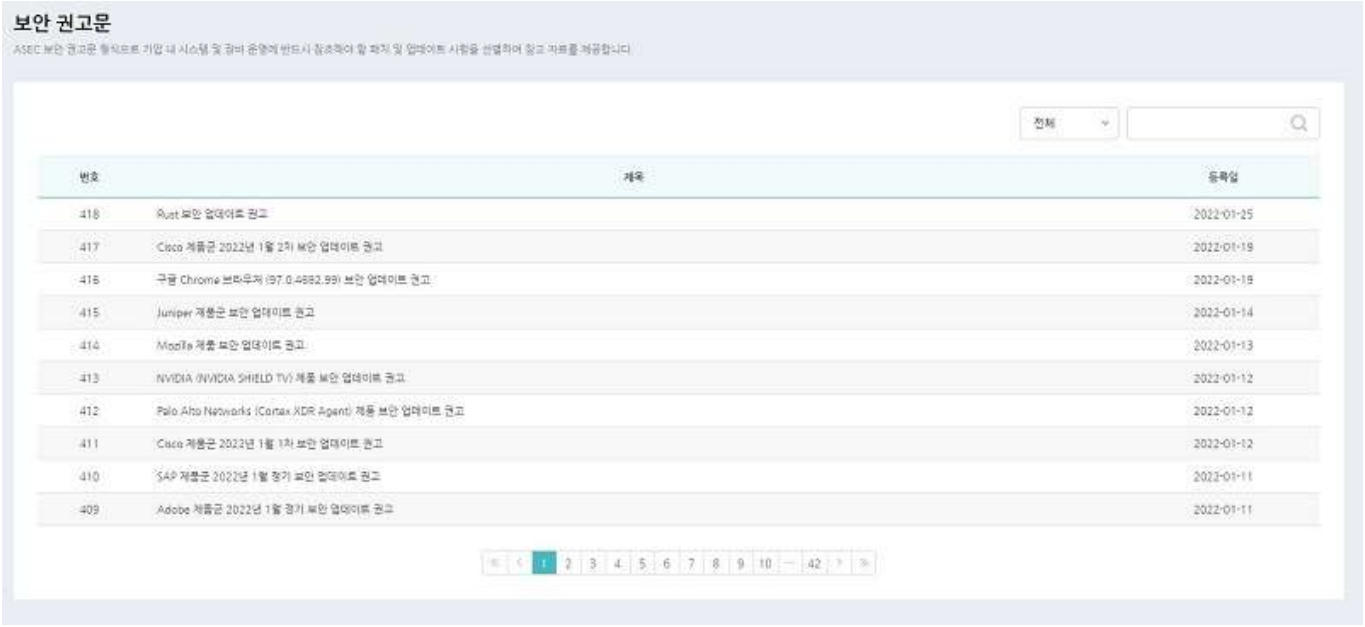
취약점 대응의 핵심은 신속하고 정확한 취약점 인텔리전스 확인

안랩의 데이터 분석 결과, Log4j 취약점이 발견된 2021년 12월 한 달간 자사의 ASEC블로그 월별 방문자수는 연 평균 수치의 약 3배에 달한 것으로 나타났다. Log4j 관련 블로그 게시물은 조회수 8천회 이상을 기록했으며, 취약점 발견 이후 포털사이트의 '안랩' 검색량 역시 급증했다.

이와 같은 긴급한 보안 요구사항에 대응해 안랩은 여러 경로로 Log4j 취약점 대응에 관한 인텔리전스를 제공해왔다. 그리고 그 중심에는 자사의 차세대 위협 인텔리전스 플랫폼 'AhnLab TIP'가 있다.

AhnLab TIP는 안랩의 차별화된 보안 노하우가 담긴 위협정보를 단일 플랫폼에서 제공해, 사용자들의 편의성을 제고하고 위협 대응력을 강화한다. Log4j 취약점에 관해서도 ▲보안권고문 ▲ASEC Notes(전문가 분석내용) ▲취약점 분석 보고서 ▲ASEC블로그 등을 통해 취약점에 관한 세분화된 위협 인텔리전스를 제공해오고 있다.

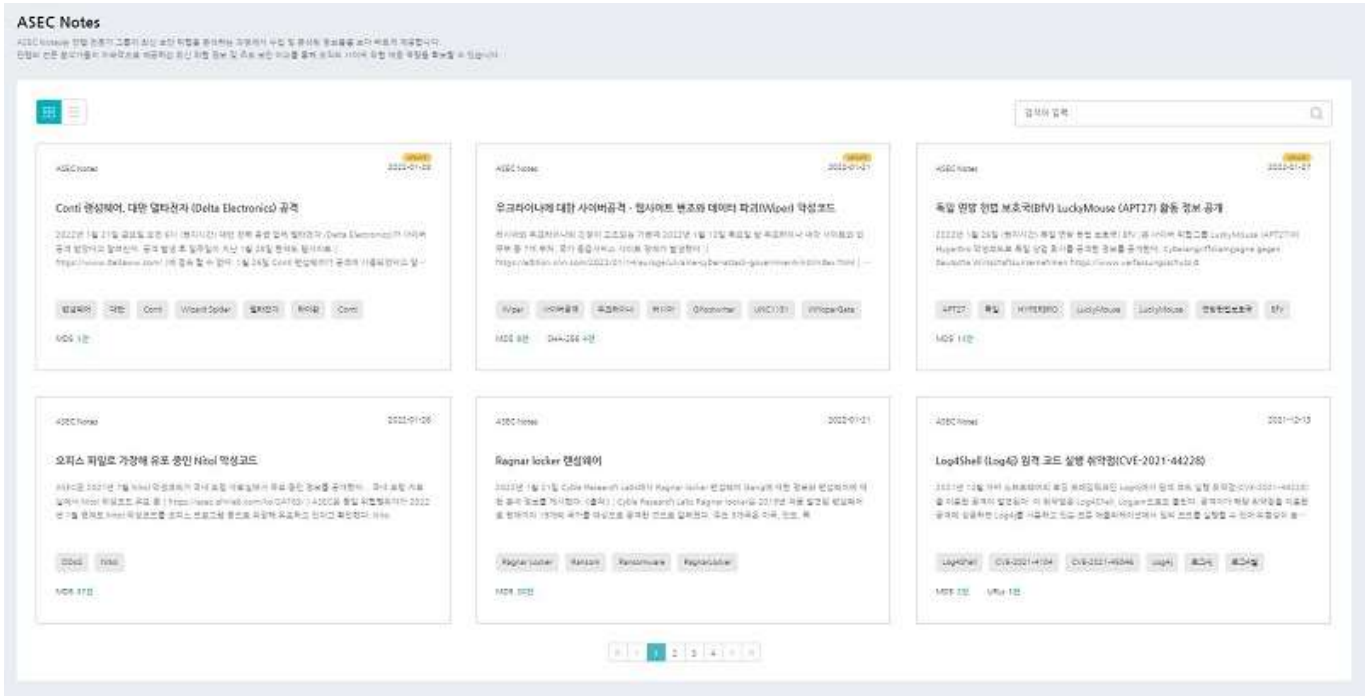
먼저, 보안권고문은 위협이나 취약점에 관해 사용자들이 조치해야 할 내용을 간결하게 정리한 문서이다. AhnLab TIP에 게시된 Log4j 취약점 관련 보안권고문을 보면, 취약점에 대한 간략한 정보부터 영향 받는 버전과 취약점 패치 안내까지 사용자 입장에서 보안 강화를 위해 당장 수행해야 하는 항목들에 관한 정보가 업데이트 되어 있다.



[그림 1] AhnLab TIP 보안권고문

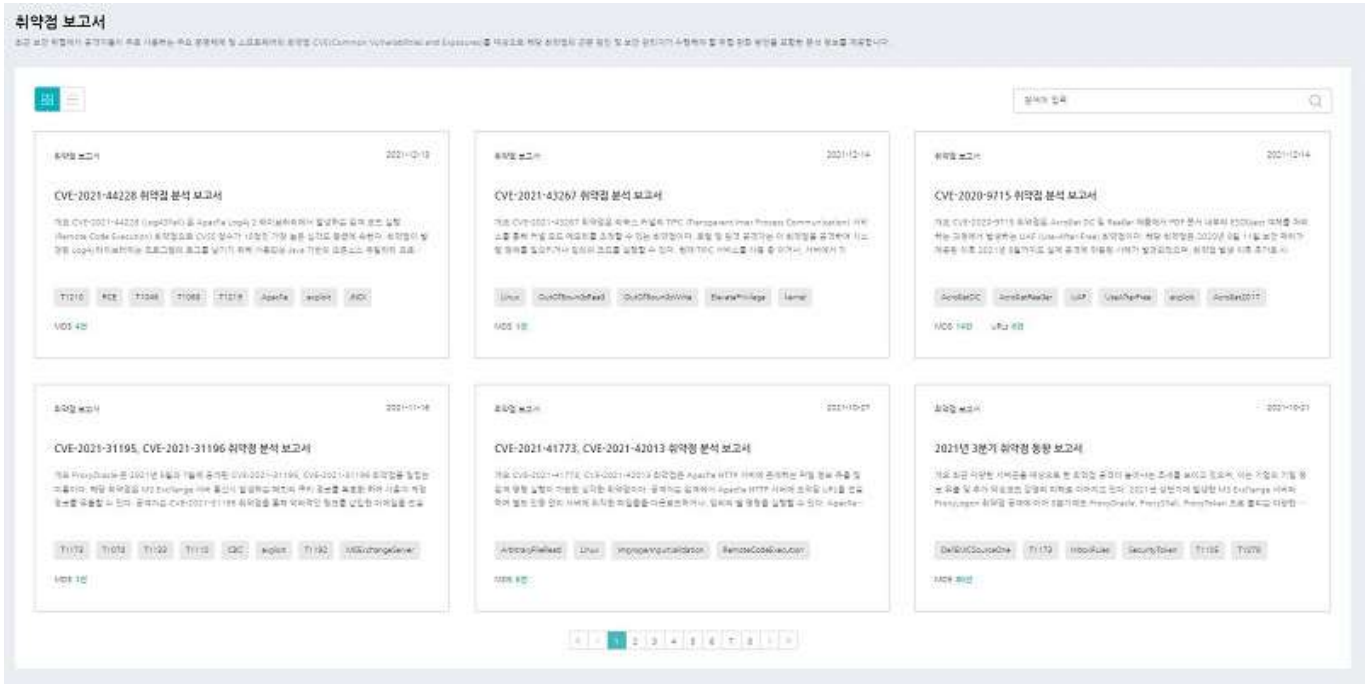
ASEC Notes는 안랩 전문가 그룹이 최신 보안 위협을 분석하는 과정에서 수집 및 분석된 정보들을 보다 빠르게 제공한다. 신속한 사이버 위협에 대응하기 위해 각종 뉴스와 연관된 자체 위협 분석 정보와 알려지지 않은 출처인 딥웹 및 다크웹 등 음성화 사이트에서 유통되고 있는 위협 정보들을 제공하여 사용자가 위협에 효과적으로 대응할 수 있도록 한다.

Log4j 취약점의 경우, 지금까지 공개된 취약점 별로 게시물이 업데이트되어 있으며, 취약한 제품 버전부터 해당 취약점을 활용한 공격 방법에 관한 분석, 취약점으로 인한 영향과 패치에 관한 내용까지 포함한다.



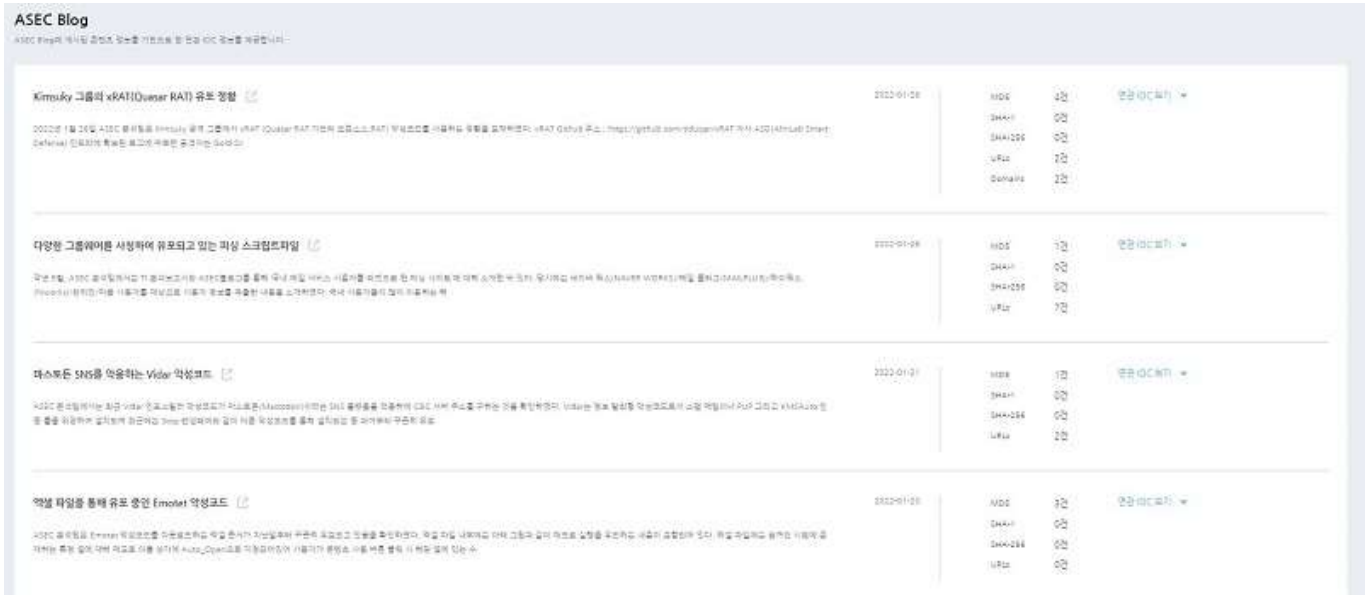
[그림 2] AhnLab TIP ASEC Notes

다음은 취약점 분석 보고서로 Log4j 취약점에 관한 모든 분석 내용이 담겨 있는 문서다. 취약점의 최근 동향부터 발생 원인과 이를 활용한 공격 과정의 세부 분석 내용, 대응을 위한 상세한 가이드, 안랩의 대응 현황까지 사용자가 취약점으로 인한 피해를 최소화기 위해 알아야할 전체적인 내용을 깊이 있게 다루는 것이 특징이다.



[그림 3] AhnLab TIP 취약점 분석 보고서

국내 뿐 아니라 세계적인 위협정보 채널로 자리매김한 ASEC블로그에서도 수 차례에 걸친 포스팅을 통해 Log4j 취약점에 관한 내용을 다뤄왔다. AhnLab TIP 사용자들은 대중에 공개되는 ASEC블로그 게시물 뿐만 아니라 연관 침해지표(Indicators of Compromise: IOC)까지 매칭하여 보다 깊이 있는 위협 분석정보를 한 눈에 파악할 수 있다.



[그림 4] AhnLab TIP ASEC블로그 게시물과 연관 IOC

이 밖에, AhnLab TIP 사용자들은 플랫폼 내 검색창에 Log4j 검색어를 입력하면 앞서 설명한 콘텐츠 뿐만 아니라, 뉴스 클리핑 서비스의 Log4j 관련 국내외 언론 기사와 소셜미디어 게시물까지 Log4j와 연관된 모든 위협 정보를 편리하게 확인할 수 있다.

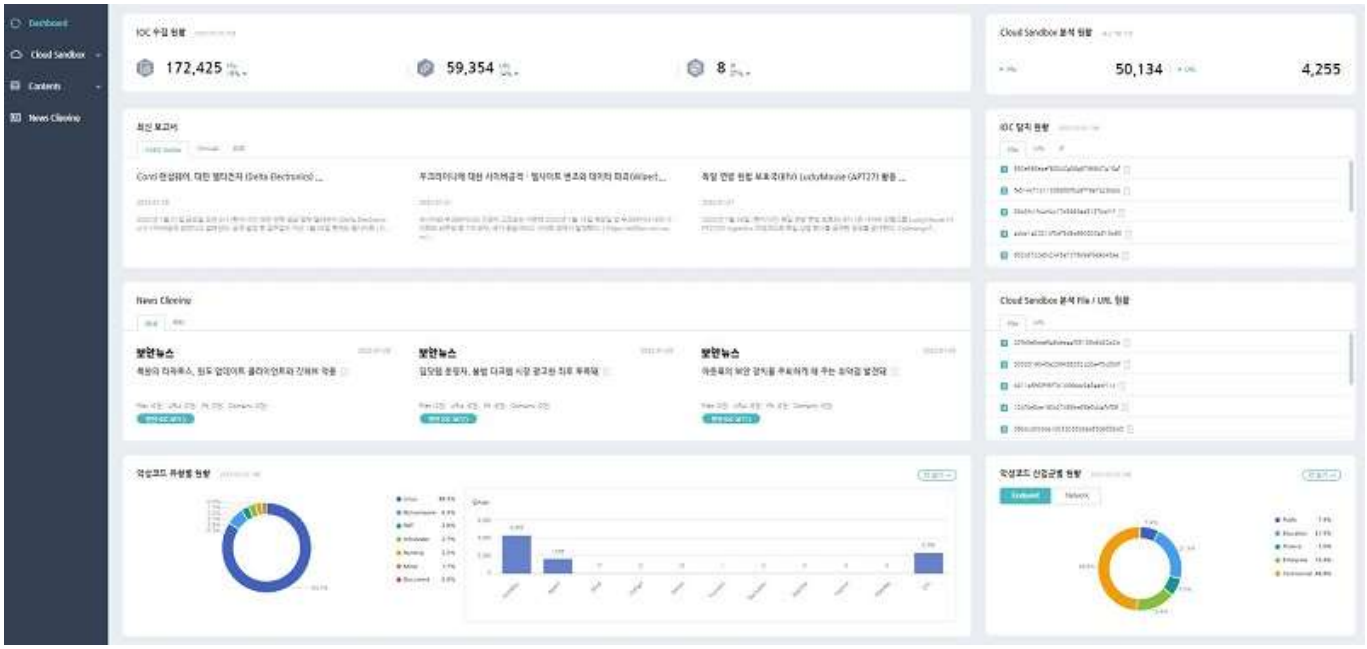
AhnLab TIP의 위협 인텔리전스, 배경에는 탁월한 기술력이 있다

AhnLab TIP가 제공하는 다양한 위협 인텔리전스의 배경에는 방대한 위협 정보를 수집하고 분석할 수 있는 안랩의 탁월한 기술력이 자리하고 있다. 안랩의 다양한 보안 솔루션들과 연동하고 있는 AhnLab TIP는 솔루션들이 탐지한 위협 정보들을 집약하고 분석해 사용자들에게 독보적인 위협 인텔리전스를 제공하고 있다.

다음은 기술적인 관점에서 AhnLab TIP가 보유한 특장점을 정리한 것이다.

1. 다양한 정보 수집처를 활용한 위협 인텔리전스 제공

AhnLab TIP는 엔드포인트, 네트워크, 모바일 등 방대한 보안 영역에 걸쳐 안랩이 보유한 자체 센서, 안랩 시큐리티대응센터(ASEC), 컴퓨터침해사고대응센터(CERT), 시큐리티 파트너, 해커/범죄자/연구 관련 각종 포럼에서 정보를 수집하는 웹 크롤러(Web Crawlers), 오픈소스 및 각종 SNS 소스 등을 통해 수집한 위협 데이터와 수십억 개의 침해 지표를 연관시키고, 데이터를 실제 적용가능한 인사이트로 전환한다.



[그림 5] AhnLab TIP 메인화면

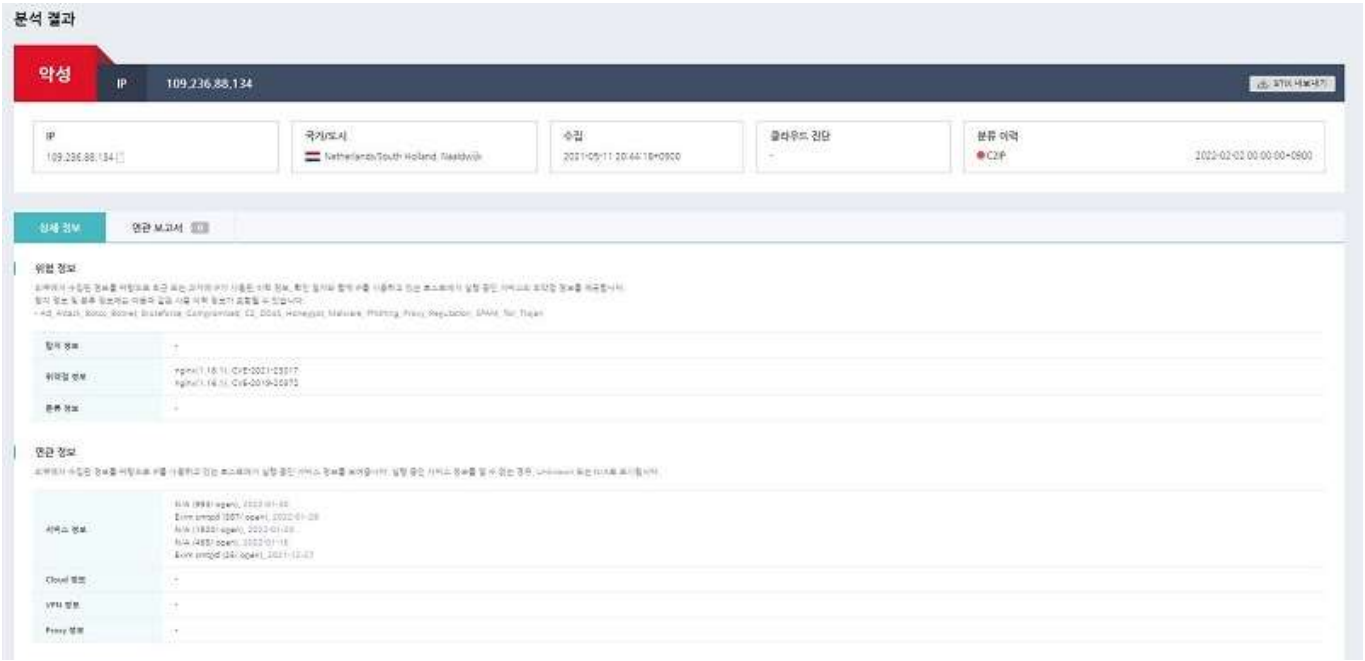
2. 여러 자체 센서를 통해 수집한 샘플 분석 및 연관 IOC 제공

AhnLab TIP는 안랩이 다양한 산업군의 사용자에게 제공하고 있는 안티 멀웨어, 침입탐지시스템(IDS) 또는 침입방지시스템(IPS) 등에서 자체적으로 수집하거나 외부의 신뢰도 있는 출처로부터 수집된 데이터를 정제한다. 이후, 파일 정보, 공격 패턴, URL 및 IP 주소와 같은 IOC를 생성하여 위협에 즉시 대응할 수 있는 정보를 신속하게 제공한다.

사용자는 보안 위협 탐지와 대응 사이의 간격을 좁히고, 차별화된 인사이트를 바탕으로 보안 의사결정을 내릴 수 있다. 또한, 국내 시장을 노리는 보안 위협에 가장 빠르게 대응할 수 있으며, 향후 유사 산업군에서 발생할 수 있는 미래 위협에 대한 예측도 가능하다.

[그림 6] 연관 IOC 정보

안랩은 2021년 11월, AhnLab TIP 서비스 기능 고도화를 진행하여 네트워크 보안 장비로부터 수집된 정보와 AhnLab CERT 및 검증된 외부 인텔리전스를 바탕으로 보다 정확한 IP IOC도 제공하고 있다.



[그림 7] IP IOC 정보

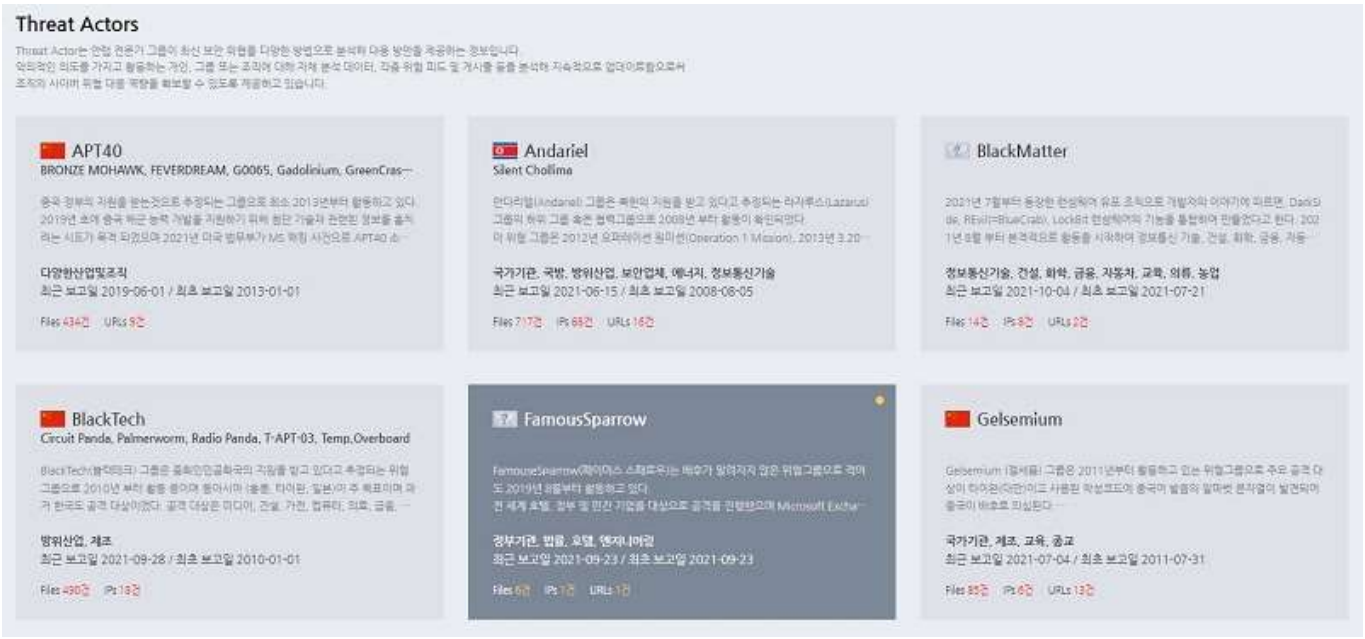
사용자는 별도로 제공되는 API를 통해 탐지된 정보에 대한 세부 연관 정보를 확인할 수 있으며, 분석 결과로 생성된 IOC를 실시간으로 연동해 조직에서 운영하는 솔루션에 적용할 수도 있다.

3. APT 인텔리전스 정보 제공 – 해킹 그룹(Threat Actor)의 프로파일링 정보제공

최근 사이버 위협은 다양한 경로를 이용한 단계적인 공격을 통해 네트워크 침입 후 확산을 수행하여 조직 내부의 중요 데이터를 유출시키는 형태로 진행되고 있다. 또, 공격 목적도 경제적 이익을 추구하는 경향을 보이며, 가상화폐 채굴형 악성코드와 랜섬웨어 공

격이 증가하는 추세가 나타나고 있다.

AhnLab TIP의 해킹 그룹 분석정보는 공격자들이 어떤 의도로 공격을 수행하는지 파악하고, 유사한 공격 수법과 패턴을 분석한다. 이를 바탕으로, 공격자의 신원, 의심되는 동기, 의도한 효과, 공격 기법과 같은 다양한 정보를 제공해 사용자로 하여금 공격을 사전에 대비할 수 있도록 한다.



[그림 8] Threat Actor 메뉴

해당 정보는 기본적인 데이터 피드에 그치지 않고, 전 세계적으로 활동하는 공격자들의 침해 기술 정보를 수집하고, 공격의 맥락(context)을 파악하는데 도움이 되는 연관관계 정보 및 사용자가 속한 산업군과 현재 이슈를 고려해 최적화된 위협 인텔리전스를 제공한다.

4. 클라우드 샌드박스 분석

AhnLab TIP는 알려지지 않은 위협 대응을 위해 다양한 운영체제(OS)를 지원하는 샌드박스 환경에서 악성코드를 실행시켜 실제 악성코드 감염 시 발생되는 행위를 분석한다. 이를 통해 공격이 시스템에 미치는 영향을 확인하며, 위협 현황 정보를 시각화하고 행위별 위협 수준 정보를 제공한다.

순항하는 AhnLab TIP, 위협 인텔리전스 필요성의 방증

2020년 말 출시된 AhnLab TIP는 2021년에 정부부처와 공공기관을 비롯해 금융 및 IT 대기업 등 다양한 산업군에서 고객사를 확보했다. 특히 지난 6월에는 대형 금융사 및 유통사를 대상으로 사업을 수주하며 레퍼런스를 확대했다.

이처럼 AhnLab TIP가 순항하는 이유는 전문적이고 체계적인 위협 인텔리전스를 편리하게 제공받고자 하는 기업들의 요구사항을 충족했기 때문으로 풀이된다. 서두에 언급한 바와 같이 변화와 고도화를 거듭하는 위협 환경에서 분산된 위협 정보를 수집하는 것은 이제 물리적으로 한계가 있다.

AhnLab TIP는 더욱 정교한 위협정보 제공을 위해 국내외 다양한 기관과 협력하며 정보 수집 경로를 확대하고 있다. 콘텐츠 범위를 확대하는 한편, AhnLab TIP에서 생성된 위협 인텔리전스를 안랩의 솔루션 및 서비스와 연동하여 악성코드 탐지 및 제거를 자동화하는 기능을 점진적으로 제공할 예정이다.

안랩은 기업/기관 고객을 대상으로 AhnLab TIP를 30일간 무료로 이용해 볼 수 있는 AhnLab TIP 체험 서비스를 상시 제공하고 있다. 해당 서비스를 이용을 원하는 기업/기관은 안랩 TIP 전용 페이지에 접속 후 'Request a Trial'을 통해 신청하면 된다. 이 밖에, AhnLab TIP에 대한 소개와 주요기능은 제품소개 동영상을 통해 확인할 수 있다.

►AhnLab TIP 30일 무료체험 바로가기

►AhnLab TIP 제품소개 동영상 바로가기