Cisco AMP Threat Grid - Cloud

악성코드와 지능형 위협에 맞서려면 최상의 보안 툴이 필요합니다. Cisco® AMP(Advanced Malware Protection) Threat Grid는 최고의 악성코드 차단 솔루션인 통합 악성코드 분석과 컨텍스트 기반 인텔리전스를 결합했습니다. 보안 전문가가 능동적으로 사이버 공격을 방어하고 신속하게 복구할 수 있도록 지원합니다.

제품 개요

Cisco AMP Threat Grid는 비공개 커뮤니티로부터 악성코드를 크라우드 소싱하여 고정 및 동적 분석을 포함한 특별한 고급 보안 기술을 적용해 모든 샘플을 분석합니다. 그 결과와 수억 개의 다른 분석된 악성코드 아티팩트의 상관성을 분석하여 악성코드 공격, 캠페인, 그 분포에 대한 종합적인 관점을 제시합니다. 보안팀은 관찰된 활동 및 특성의 샘플 하나를 수백만 개의 다른 샘플과 신속하게 상관 분석하여 이력 및 글로벌 컨텍스트에서 그 동작을 철저하게 파악할 수 있습니다. 이 기능으로 표적 공격뿐 아니라 지능적 악성코드의 광범위한 위협까지 효과적으로 방어할 수 있습니다. Cisco AMP Threat Grid의 상세 보고서에서는 중요 행동 지표를 식별하고 위협 점수를 부여하여 지능적 공격의 우선 순위를 신속하게 결정하고 그로부터 복구할 수 있게 합니다.

기능 및 장점

Cisco AMP Threat Grid의 기능과 이점이 표 1에 나와 있습니다.

표 1. Cisco AMP Threat Grid의 기능 및 이점

기능	혜택
고급 분석	• 악성코드의 동작에 대한 종합적인 보안 통찰력 확보 • Cisco AMP Threat Grid의 광범위한 데이터베이스에 수록된 샘플 소스 및 관련 동작에 직접 연결 • 모든 정보 및 분석 결과에 편리하게 액세스하여 추가 조사 가능
고급 동작 지표	• 뛰어난 정확성으로 오탐 가능성이 낮고 실행 가능한 300여 개의 고급 행동 지표 분석 • 각종 악성코드 그룹 및 악성 동작을 포괄하는 고급 고정 및 동적 분석을 통해 종합적인 지표 생성 • 위협에 대한 가장 폭넓은 컨텍스트를 제공하여 신속하고 자신 있는 의사 결정 지원
위협 점수	• 관찰된 동작의 신뢰도 및 심각도, 이력 데이터, 빈도, 클러스터링 지표 및 샘플을 고려하는 독자적인 분석 및 알고리즘으로 위협 점수 자동 산정 • 각 샘플의 악성 동작 수준을 반영하여 위협에 대한 신뢰할 수 있는 우선 순위 지정 • 더 효과적으로 위협의 우선 순위를 결정하여 Cisco AMP Threat Grid 피드를 사용하는 악성코드 분석가, 사고 대응자, 보안 엔지니어링팀, 제품의 효율성 및 정확도 향상
표준 피드 형식	• 통합하기 용이한 정규화된 피드를 JSON(JavaScript Object Notation), CybOX(Cyber Observable Expression), STIX(Structured Threat Information Express), CSV(comma-separated values)와 같은 각종 표준화된 형식 및 Snort 규칙으로도 제공 • 특정 보안 제품을 위해 맞춤형 피드 형식 제공 • 시간의 경과에 따른 추이를 손쉽게, 일관성 있게 추적하여 실행 가능한 보고서 생성
통합을 위한 API	• 기존 보안 및 네트워크 인프라에서 신속하고 간편하게 위협 인텔리전스 운용 • Cisco AMP Threat Grid의 REST(representational state transfer) API와의 신속하고 편리한 통합 • 게이트웨이, 프록시, SIEM(security information and event management) 플랫폼을 비롯한 각종 서드파티 제품에 대한 통합 지침 제공

종합적이고 최고 품질을 자랑하는 피드 콘텐츠

Cisco AMP Threat Grid는 비공개 파트너 및 고객 커뮤니티로부터 악성코드를 크라우드 소싱하여 악성코드 공격, 캠페인, 그 속성에 대한 종합적인 관점을 제시합니다. 매월 수백만 개의 샘플을 분석하고 테라바이트 단위의 실행 가능한 콘텐츠를 정제하여 명확하게 분류되고 손쉽게 이용할 수 있는 콘텐츠 피드를 작성합니다. 따라서 가장 광범위한 위협을 효과적으로 방어하고 공격의 피해를 줄일 수 있습니다. Cisco AMP Threat Grid는 여러 범주의 사전 패키지 고급 피드를 제공하여 다음과 같은 다양한 위협 유형을 처리합니다.

- RAT(remote-access Trojan)를 비롯한 각종 트로이 목마 및 다른 악성코드를 유포하고 실행 파일 다운로드와 같은 특정 행동을 수행하는 것으로 알려진 악성코드 그룹
- 아웃바운드 네트워크 통신을 설정하고 비정상적인 네트워크 활동을 보여주는 악성코드 예를 들면 악성 네트워크 활동을 시작하는 PDF 파일과 Microsoft Office 문서, 각종 프로토콜과 채널을 통해 통신하는 악성코드, 비표준 또는 불일치한 네트워크 프로토콜의 사용, 알려진 싱크홀을 통한 통신 등이 포함됩니다. Cisco AMP Threat Grid는 구체적인 행동 지표를 통해 피드를 생성합니다. 여기에는 아웃바운드 통신을 확인하는 데 쓰이는 네트워크 지표도 포함됩니다.
- Windows 호스트 파일 및 DLL(동적 링크 라이브러리)을 수정하는 등의 호스트의 악성 활동, 레지스트리 수정 없이 악성 파일을 설치하고 호스트에 지속성을 유지하는 하이재킹 기법
- Cisco AMP Threat Grid에서 평가한 위협 점수가 높은 악성코드

표 2에서는 Cisco AMP Threat Grid에서 지원하는 플랫폼과 Cisco IOS® Software 릴리스를 보여줍니다.

표 2. Cisco AMP Threat Grid: 지원되는 플랫폼과 OS

제품군	지원되는 플랫폼	지원되는 Cisco IOS 이미지(기능 세트)
Cisco AMP Threat Grid 포털	• Windows XP • Windows 7	**지원되지 않음**
Cisco AMP Threat Grid 동적 분석	분석에 지원되는 파일 형식: • PE32(Portable Executable 32-bit) 파일: 실행 파일(exe), 동적 링크 라이브러리(dll) • Java 아카이브(jar) • Adobe PDF(Portable Document Format) • Microsoft Office 문서: rtf, doc(s), xls(x), ppt(x) • 컨테이너인 ZIP(zip) • URL: 인터넷 바로 가기 파일(URL) • HTML 문서	**해당 없음**

라이센스

Cisco AMP Threat Grid 기능에서는 프로세스 매핑 및 레지스트리 분석, 네트워크 연결, 해당 환경의 악성코드 실행 동영상(가능한 경우) 등을 포함한 심층 분석 및 결과를 제공합니다. 분석한 인텔리전스 데이터에 대한 배치 피드도 이용 가능하며 더 광범위한 Cisco AMP Threat Grid 데이터에서 맞춤형 피드를 생성하는 기능도 있습니다.

또한 Cisco AMP Threat Grid 고객은 직접 클라우드 포털에 또는 Cisco AMP Threat Grid API에서 자동화된 방식으로 샘플을 제출할 수 있습니다. 모든 클라우드 서비스 요소의 라이센스가 1년 또는 3년 콘텐츠 서브스크립션으로 제공됩니다. 서브스크립션 레벨에는 레벨당 사용자 계정 수, 1일 기준 Cisco AMP Threat Grid 클라우드에 분석을 위해 파일을 제출하는 횟수가 포함됩니다.

표 3에서는 조사 및 분석을 위해 Cisco AMP Threat Grid 포털에 로그인할 수 있는 분석가 계정 수, 그에 따라 수동으로 또는 API를 통해 Cisco Threat Grid 클라우드에 제출하여 고정 및 동적 분석을 수행할 수 있는 파일 수를 보여줍니다.

표 3. 분석가 계정 라이센스 및 분석을 위해 제출 가능한 파일

라이센스 레벨: 계정 수	1일 최대 제출 횟수
5	500
10	1,500
25	2,500
100	10,000

Cisco 및 파트너 서비스

Cisco 및 Cisco 공인 파트너의 서비스를 이용하여 Cisco AMP Threat Grid의 고급 위협 피드 및 REST API와의 통합을 계획하고 구현할 수 있습니다. 계획 및 설계 서비스는 기존 인프라, Cisco AMP Threat Grid 고급 피드 형식, 운영 프로세스에 따라 조정되므로 고급 위협 피드를 가장 효과적으로 활용할 수 있습니다.

자세한 정보

Cisco AMP Threat Grid 통합 악성코드 분석 및 위협 분석에 대한 자세한 내용은 http://www.cisco.com/c/en/us/solutions/enterprise-networks/advanced-malware-protection/index.html을 참조하십시오.

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Printed in USA C78-733495-00 12/14