Cisco Threat Grid Premium - 클라우드

Cisco® Threat Grid는 최고의 악성코드 차단 솔루션인 통합 악성코드 분석과 상황 기반 인텔리전스를 결합한 솔루션입니다. 보안 전문가가 능동적으로 사이버 공격을 방어하고 신속하게 복구할 수 있도록 지원합니다.

제품 개요

Cisco Threat Grid는 비공개 커뮤니티로부터 악성코드를 크라우드 소싱한 다음 정적 및 동적(샌드박싱) 분석과 같은 고도로 안전한 독자적인 기술을 사용하여 모든 샘플을 분석합니다. 그 결과와 수억 개의 다른 분석된 악성코드 아티팩트의 상관성을 연구하여 악성코드 공격, 캠페인, 그 분포에 대한 종합적인 관점을 제시합니다. 따라서 보안 팀은 관찰된 활동 및 특성의 단일 샘플에 대한 상관 관계를 빠르게 파악하고 이를 수백만 개의 다른 샘플과 비교하여 기록 내역과 전체적인 맥락을 바탕으로 행동을 파악할 수 있습니다. 이 기능으로 애널리스트는 표적 공격뿐 아니라 지능형 악성코드의 광범위한 위협까지 효과적으로 방어할 수 있습니다. 또한 중요 행동 지표 식별 및 위협 점수 할당 등 Threat Grid의 상세 보고서를 활용하면 지능형 공격의 우선 순위를 신속하게 결정하고 복구할 수 있습니다.

기능 및 이점

Threat Grid Premium의 기능과 이점이 표 1에 나와 있습니다.

표 1. 기능 및 이점

기능	이점
고급 분석	• 악성코드의 동작에 대한 종합적인 보안 통찰력 확보 • Threat Grid의 광범위한 데이터베이스에 수록된 샘플 소스 및 관련 동작에 직접 연결 • 모든 정보 및 분석 결과에 편리하게 액세스하여 추가 조사 수행
고급 행동 지표	• 뛰어난 정확성으로 오탐 가능성이 거의 없는 실행 가능한 800여 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 상황을 제공하여 신속하고 자신 있는 의사 결정을 할 수 있도록 지원
GloveBox	• 네트워크가 감염될 위험 없이 악성코드를 분석하도록 안전한 환경 제공 • 분석가가 애플리케이션을 열고 워크플로 프로세스를 복제하고 악성코드 동작을 확인하며 가상 머신을 리부팅할 수 있도록 지원
위협 점수	• 더 효과적으로 위협의 우선순위를 결정하여 Threat Grid 피드를 사용하는 악성코드 분석가, 사고 대응자, 보안 엔지니어링 팀, 제품의 효율성 및 정확도를 향상 • 관찰된 동작의 신뢰도 및 심각도, 이력 데이터, 빈도, 클러스터링 지표 및 샘플을 고려하는 독자적인 분석 및 알고리즘으로 위협 점수 자동 산정 • 각 샘플의 악성 행동 수준을 반영하여 위협에 대한 신뢰할 수 있는 우선순위 지정
통합을 위한 API	• 기존 보안 및 네트워크 인프라에서 신속하고 간편하게 위협 인텔리전스 운용 • Cisco Threat Grid의 REST(representational state transfer) API와 신속하고 편리하게 통합 • 게이트웨이, 프록시, SIEM(security information and event management) 플랫폼을 비롯한 각종 서드파티 제품에 대한 통합 지침 제공
표준 피드 형식	• 통합하기 용이한 정규화된 피드를 JSON(JavaScript Object Notation), STIX(Structured Threat Information Expression), 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 손쉽고, 일관성 있게 추적하여 실행 가능한 보고서 생성

지능형 인텔리전스, 분석, 보고

Threat Grid의 클라우드 기반 서비스는 가장 강력한 상황 기반의 위협 인텔리전스를 제공합니다. Threat Grid는 수백만 개의 파일을 안전하게 분석하고 그 결과를 이미 분석된 수억 개의 다른 악성코드 아티팩트와 비교하여 연관성을 찾아냅니다. 이를 통해 이전 내역을 포함하여 악성코드를 종합적으로 파악할 수 있습니다. 분석가는 각 데이터 요소를 전환하고 드릴다운할 수 있는 기능을 사용하여 분석 과정에서 더욱 심층적인 확인이 가능하므로, 무해한 것으로 위장한 악성 파일을 식별할 수 있습니다. 강력한 검색, 상관관계 분석, 보고 기능은 악성코드 아티팩트, 지표, 샘플에 대한 자세한 정보를 제공합니다. 자세한 분석 보고서에는 이러한 관련 네트워크 트래픽 및 악성코드 아티팩트를 비롯하여 모든 악성코드 샘플 활동이 포함됩니다.

광범위한 최상의 피드 콘텐츠

Cisco 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 위협 인텔리전스 피드를 작성합니다. 따라서 가장 광범위한 위협을 효과적으로 방어하고 공격의 피해를 줄일 수 있습니다. Threat Grid는 여러 범주의 사전 패키지 프리미엄 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. 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 그 예입니다. 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
- Threat Grid에서 평가한 위협 점수가 높은 악성코드

표 2에는 Cisco Threat Grid에서 지원하는 플랫폼이 나와 있습니다.

표 2. 지원되는 플랫폼 및 운영 체제

제품군	지원되는 플랫폼
Threat Grid 포털	• Windows XP • Windows 7 32비트 • Windows 7 64비트 • Windows 7 64비트(한국어) • Windows 7 64비트(일본어)
Threat Grid 동적 분석	분석에 지원되는 파일 형식: • .BAT - 배치 파일 • .CHM - Compiled HTML Help – Microsoft Compiled HTML Help • .DLL - 참조: PE32 및 PE32+ • .HTA - HTML 애플리케이션 • .HWP, .HWT, .HWPX - win7-x64-kr VM에서만 제공(Hancom Office 전용) • .JAR - Java Archives • .JS – JavaScript

제품군	지원되는 플랫폼
	• .JSE - Encoded JavaScript • .JTD, .JTT, .JTDC, .JTTC: win7-x64-jp VM에서만 제공(Ichitaro 전용) • .LNK - Windows 바로가기 파일 • .MSI - Microsoft 설치 프로그램 파일 • MHTML - Mime HTML 파일 • Microsoft Office 문서(DOC, .DOCX, .RTF, .XLS, .XLSX, .PPT, .PPTX 포함) • PDF - Portable Document Format(JavaScript 리소스를 포함한 자세한 정적 포렌식) • PE32 파일 및 실행 파일(.EXE) • 라이브러리(.DLL) • .PE32+ 파일 – win7-x64 VM에서만 제공 • 실행 파일(.EXE) • 라이브러리(.DLL) • .PS1 - Powershell • .SWF - Flash 파일 • URL(인터넷 바로가기 파일 또는 URL 직접 제출. 자세한 정적 포렌식 또는 JavaScript 리소스.) • .VBE - Encoded Visual Basic • .VBN - Virus Bin – .ZIP 참조 • .VBS - Visual Basic Script • .WSF - Windows Script 파일 • Office 문서 유형 기반의 .XML 및 XML(.DOCX, .XLSX, .PPTX) • XML - .XML(Extensible Markup Language), Office의 XML은 해당 프로그램에서 열림(Office 2003). 모든 기타 XML은 IE에서 열림 • ZIP – 아카이브 및 격리 형식(.BZ2, .GZip, .XZ도 포함) • ZIP(.ZIP) - 아카이브 중첩이 없고, 비밀번호 또는 '감염' 사실이 없는 일종의 컨테이너. Cisco에서는 AV 서비스를 대상으로 하는 유명한 공격인 42.zip을 비롯하여 zip bomb 및 quine 같은 알려진 압축 해제 공격 문제로 인해 중첩된 ZIP 아카이브를 지원하지 않음 • 격리 파일 유형에는 .SEP, .VBN이 포함됨

라이선싱

Threat Grid 기능에서는 프로세스 매핑 및 레지스트리 변경, 네트워크 연결, 해당 환경의 악성코드 실행 동영상(가능한 경우) 등을 포함한 심층 분석 및 결과를 제공합니다. 분석한 인텔리전스 데이터에 대한 배치 피드에 액세스할 수 있으며 광범위한 Threat Grid 데이터에서 맞춤형 피드를 생성할 수 있습니다. Threat Grid는 Cisco AMP(Advanced Malware Protection) 라이선스와 통합되어 매일 제한된 수의 분석용 샘플을 제공합니다. 고객은 샘플 팩을 통해 더 많은 일일 샘플 제출 수를 쉽게 추가할 수 있습니다.

Threat Grid Premium 가입자는 직접 클라우드 포털을 통해 또는 Threat Grid API를 통해 자동화하여 샘플을 제출할 수 있습니다. 모든 클라우드 서비스 요소의 라이선스가 1년, 3년 또는 5년 콘텐츠 서브스크립션으로 제공됩니다. 서브스크립션 레벨에는 레벨당 사용자 계정 수, 1일 기준 Cisco AMP Threat Grid 클라우드에 분석을 위해 파일을 제출하는 횟수가 포함됩니다.

표 3에는 조사 및 분석을 위해 Threat Grid 포털에 로그인할 수 있는 분석가 계정 수, 그에 따라 수동으로 또는 API를 통해 Threat Grid 클라우드에 제출하여 고정 및 동적 분석을 수행할 수 있는 파일 수가 나와 있습니다.

표 3. 분석가 계정 라이선스 및 분석을 위해 제출 가능한 파일

라이선스 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 인증 파트너의 서비스를 이용하여 Threat Grid의 프리미엄 위협 피드 및 REST(Representational State Transfer) API와의 통합을 계획하고 구현할 수 있습니다. 계획 및 설계 서비스는 기존 인프라, Cisco AMP Threat Grid 프리미엄 피드 형식, 운영 프로세스에 따라 조정되므로 프리미엄 위협 피드를 가장 효과적으로 활용할 수 있습니다.

Cisco Capital

여러분의 목표 달성을 돕는 금융 지원 솔루션

Cisco Capital이 목표 달성과 경쟁력 유지에 필요한 기술 도입을 도와드리겠습니다. 고객의 설비 투자 부담을 줄여드립니다. 성장을 가속화하십시오. 투자 및 ROI를 최적화하십시오. Cisco Capital 파이낸싱은 하드웨어, 소프트웨어, 서비스, 보완적인 서드파티 장비 도입에 유연성을 제공합니다. 또한, 예측 가능한 비용 결제를 한 번만 하면 됩니다. Cisco Capital은 100여 개 국가에서 이용 가능합니다. 자세히 보기.

추가 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 C78-733495-02 03/17