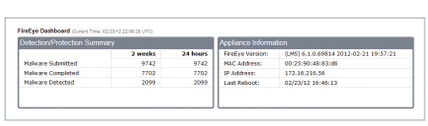
데이터시트

Malware Analysis System

지능형 표적(APT) 공격에 대한 차세대 포렌식 분석

주요 사항

- 의심스러운 파일, 웹 코드 및 실행 파일에 대한 능률적인 배치 처리 분석
- 파일 시스템, 메모리 및 레지스트리의 응용 프로그램 변경 사항 및 시스템 수준의 OS에 대한 심층 보고서
- 샌드박스 또는 라이브 모드 분석을 제공하여 제로 데이 위협 확인
- 테스트 및 분석을 위한환경 구성 및 설정에 필요한 시간 및 노력 절약뿐만 아니라 가상 테스트 이미지의 자동 설정 및 해제
- CMS 통합을 통한 즉각적인 로컬 보호를 위해 악성코드 정보를 동적으로 생성
- 악의적인 URL 세션 및 코드 실행의 분석을 위한패킷 캡쳐 실행
- 사용자 지정 YARA 규칙(버전 1.3 호환) 지원
- AV-Suite를 포함하여 사고 대응 우선 순위 지정 능률화
- 로컬 인증 외에도 원격 타사 AAA(인증, 권한 및 계정) 네트워크 서비스 액세스 지원



완료 및 일시 중지된 가상 실행 엔진 분석 상태를 표시하는 MAS 대시보드

FireEye MAS(Malware Analysis System)는 위협 분석가에게 강력한 자동 구성 테스트 환경에 대한 실무 제어 기능을 제공하여 파일, 이메일, 첨부 파일 및 웹 개체에 숨어 있는 지능적인 악성코드, 제로데이 및 표적 APT 공격을 안전하게 실행하고 분석할 수 있습니다.

사이버 범죄자는 특정 비즈니스, 사용자 계정, 또는 시스템에 침투할 수 있도록 특수화된 공격을 취하기 때문에 분석가들은 목표화된 악의적인 활동을 분석하는 데 도움이 되는 사용하기 쉬운 포렌식 도구를 필요로 합니다.

OS, 브라우저 및 응용프로그램 공격에 대한 액세스

FireEye 가상 실행(Virtual Execution) 엔진을 사용하면 사내 분석가는 초기 공격에서부터 콜백단계 및바이너리다운로드 시도에 이르기까지 모든 공격에 대해 360도 각도로 파악할 수 있습니다. 미리 구성된 Windows 가상 분석 환경을 통해 가상 실행 엔진은 일반 파일 형식, 전자 메일 첨부 파일 및 웹 객체의 상세한 검사를 위해 모든 의심스러운 코드를 실행합니다. FireEye MAS는 악성코드에 대한 단일 파일이나 파일 배치를 검사하고 여러 프로토콜을 이용한 아웃바운드 연결 시도를 추적합니다.

관리가 아닌 분석에 집중

가상 실행 엔진은 Microsoft 운영 체제뿐만 아니라 브라우저, 플러그인 및 기타 여러 응용프로그램의 주요 버전을 실행하는 가상화된 PC 하드웨어를 갖추고 있습니다. MAS 어플라이언스를 사용하면 관리자는 시간이 많이 걸리는 설치, 기준선 설정 및 수동 악성코드 분석에 사용되는 가상 머신 환경의 복원을 할 필요가 없습니다.

샌드박스 또는 허니팟 분석 모드 선택

샌드박스 모드를 통해 분석가는 FireEye의 Web, Email 및 File MPS 어플라이언스에 대해 CMS를 통해 배포될 수 있는 공격의 동적 및 익명 프로파일을 생성할 뿐 아니라 특정 악성코드 샘플의 실행 경로를 확인할 수 있습니다. 악성코드 공격 프로파일에는 악성 코드 식별자, 사용된 URL 및 감염과 공격의 다른 소스가 포함됩니다. 또한 악성코드 통신 프로토콜 특성이 데이터 유출 시도의 동적 차단을 제공하기 위해 공유됩니다.

> "**FireEye** 솔루션의 가장 큰 매력 중 하나는 가상 실행 환경에서 분석이 수행되어 플래그 지정된 코드 부분이 실제로 위협 요소인지 확인할 수 있다는 것입니다. 생성된 세부 정보를 통해 문제를 해결하기 위한 최적의 옵션을 식별해 낼 수 있습니다. 이렇게 하면 어떻게 대응할 지를 정확히 파악할 수 있게 됩니다."
>
> *— 사이버 보안 이사, 에너지 분야 회사*

샌드박스 분석 외에도 FireEye는 실시간으로 작동하는 네트워크 '허니팟' 모드를 제공하여 악성코드 라이프사이클에 대한 전체적인 분석을 가능하게 합니다. 오늘날의 지능적인악성코드는 여러 단계를 걸쳐 전통적인 보안 시스템을 우회합니다. 첫 번째 취약점 공격 단계는 단순히 이후 범죄를 위해 교두보를 구축하는 것입니다.

FireEye는 여러 벡터에 걸쳐 공격하는 응용 프로그램, 이메일, 웹 및 OS의 전체적인 위협 분석에 대해 여러 프로토콜을 통해 인바운드 및 아웃바운드 검사를 통합합니다.

YARA 기반 룰로 커스터마이제이션을 가능하게 합니다

MAS는 바이트 수준의 룰을 지정하고 조직에 대한 고유한 위협을 신속하게 분석하는 사용자 지정 YARA 룰설정을 지원합니다. 사용자 지정 룰은 이전에 악성으로 분류된 악의적인 개체뿐만 아니라 악성 가능성이 높은 개체를 식별하기 위해 가상 실행 엔진 분석의 한 부분으로 사용됩니다.

글로벌 악성코드 방지 네트워크

악성코드 분석 시스템인 MAS는은 아웃바운드 데이터 유출 시도를 방지하고 알려진 인바운드 공격을 중단시키기 위해 FireEye CMS를 통해 다른 MPS 어플라이언스에 악성코드 포렌식 데이터를 자동으로 공유할 수 있습니다. 또한 FireEye MPC(Malware Protection Cloud)를 통해 MAS 위협 데이터를 공유하여 잠재적인 위협에 대처할 수 있습니다.

휴리스틱 기반의 복잡한 튜닝이 필요없는 가상 실행 엔진(VX engine)을 통해 FireEye MAS 관리자는 실행/분석을 위한 환경 설치 및 구성에 필요한 시간을 절약할 수 있습니다. 이는 위협 분석가가 네트워크 및 보안 관리 오버헤드를 추가하지 않고 지능형 표적공격(APT)을 분석할 수 있는 간편하고 비용 효율적인 솔루션입니다.

기술 사양

	MAS 4310	MAS 7300	MAS 8300
폼 팩터	1U 랙 마운트	1U 랙 마운트	2U 랙 마운트
무게	13.6Kg	13.6Kg	22.7Kg
크기(WxDxH)	43.7 x 65.0 x 4.3 cm	43.7 x 65.0 x 4.3 cm	43.7 x 70.9 x 8.9 cm
엔클로저	19인치 랙에 맞음	19인치 랙에 맞음	19인치 랙에 맞음
관리 포트	(2) 10/100/1000 BASE-T 포트	(2) 10/100/1000 BASE-T 포트	(2) 10/100/1000 BASE-T 포트
모니터링 포트	해당 없음	해당 없음	(2) 10/100/1000 BASE-T 포트
성능	하루 당 최대 25,000개의 개체	하루 당 최대 50,000개의 개체	하루 당 최대 100,000개의 개체
AC 입력 전압	자동 전환 100 ~ 240 VAC 모든 범위	자동 전환 100 ~ 240 VAC 모든 범위	자동 전환 100 ~ 240 VAC 모든 범위
AC 입력 전류	8.5-6.0 A	8.5-6.0 A	9.5-7.2 A
전원 공급 장치/RAID	이중화 700W/ 2 SAS HDD (HW RAID1 내)	이중화 700W/ 2 SAS HDD (HW RAID1 내)	이중화 1400W/ 2 SAS HDD (HW RAID1 내)
주파수	50-60Hz	50-60Hz	50-60Hz
작동 온도	10°C에서 35°C	10°C에서 35°C	10°C에서 35°C

주: 모든 성능값은 시스템 구성과 처리 중인 트래픽 프로파일에 따라 달라집니다.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408.321.6300 | APAC@FireEye.com | www.FireEye.com