컨텐츠 위협 방어

파일 공유와 컨텐츠 저장소에 상주하는 악성코드를 탐지하고 제거

개요

FireEye® FX 위협 방어 플랫폼은 광범위한 파일 유형에서 발생하는 공격으로부터 데이터 자산을 보호합니다. 웹 메일, 온라인 파일 전송 툴, 클라우드, 이동식 파일 저장 장치는 파일 공유 및 컨텐츠 리포지터리로 확산되는 악성코드를 불러올 수 있습니다. FireEye FX는 네트워크 파일 공유와 기업 컨텐츠 관리 저장소를 분석하여 차세대 방화벽, IPS, AV, 게이트웨이를 우회하는 악성코드를 탐지하고 격리시킵니다.

파일 공유 서버에 상주하는 악성코드에 대한 문제

오늘날의 지능형 사이버 공격은 정교한 악성코드와 APT(지능형 지속 위협) 기법을 사용하여 방어 시스템에 침투하고 파일 공유 및 컨텐츠 리포지터리를 통해 내부로 확산됩니다. 따라서 악성코드는 네트워크에 장기적인 거점을 구축하고 오프라인 시스템을 포함한 다수의 시스템을 감염시킬 수 있습니다. 많은 기업 데이터 센터의 전형적인 방어 체계는 합법적인 방법으로 네트워크에 침입하는 공격을 방어하는 데 비효율적이기 때문에, 이러한 지능형, 컨텐츠 기반의 악성코드에 특히 취약합니다. 그리고 사이버 범죄자들은 이러한 취약점을 악용하여 악성코드를 네트워크 파일 공유로 확산시키고 데이터 저장소에 내장하기 때문에, 시스템 복구 후에도 위협은 지속됩니다.

지능형 공격 라이프사이클에 대항하기 위한 컨텐츠 보호

컨텐츠에 잠복해 있는 악성코드를 탐지할 방법이 없다면, APT는 네트워크 자산을 악용하여 독점 정보를 추출하고 막대한 피해를 입힐 수 있습니다. FireEye FX 시리즈는 특허를 받은 FireEye 다중 경로 가상 실행 ™(MVX) 엔진을 사용하여 파일 공유와 기업 컨텐츠 리포지터리를 분석합니다. 이 MVX 엔진은 일반적인 파일 형식(PDF, MS Office, vCards, ZIP/RAR/TNEF 등)과 멀티미디어 컨텐츠(QuickTime, MP3, Real Player, JPG, PNG 등)에 내장된 제로데이 악성코드를 탐지합니다. FireEye FX 시리즈는 접근 가능한 네트워크 파일 공유 및 컨텐츠 저장소를 주기적으로, 온디맨드 방식으로 스캔하여, 발견되지 못한 악성코드를 식별하고 격리시킵니다. 이 플랫폼은 지능형 공격 라이프사이클의 주요 단계를 파괴시킵니다.

알려지지 않은 제로데이 위협을 탐지하는 FireEye MVX

FireEye FX는 특별한 목적으로 설계된 FireEye MVX 엔진을 사용하여 각 파일을 검사하고, 제로데이 익스플로잇이나 악성코드 존재의 여부를 확인합니다. FireEye MVX 엔진은 안전한 가상 환경에서 동적 시그니처리스 분석을 통해 제로데이, 다중 흐름 및 기타 우회 공격을 탐지합니다. 또한 전에 관찰된 적이 없는 익스플로잇과 악성코드를 식별하여 사이버 공격 킬 체인의 감염 및 침해 단계를 저지합니다.

주요 기능

- 기존 AV 엔진이 탐지하지 못하는 잠복 악성코드 발견
- 격리(보호 모드) 또는 분석 전용(모니터 모드)으로 설치
- CIFS 및 NFS와 호환되는 파일 공유에 대해 온디맨드 스캔을 주기적으로 제공
- WebDAV 프로토콜을 활용하여 선제적인 Sharepoint 보호를 제공
- PDF, Microsoft Office 문서, 멀티미디어 파일과 같은 광범위한 파일 형태에 대한 분석을 포함
- FireEye AV 제품군과 통합하여 사고 대응의 우선 순위 결정 및 명명 규칙을 간소화
- FireEye CM과 FireEye DTI를 통해서 FireEye 플랫폼과 위협 데이터를 공유

FireEye®

FireEye MVX 스마트 그리드의 강점 활용

MVX 스마트 그리드는 세계 최고의 네트워크 보안 솔루션을 하이브리드 또는 프라이빗 클라우드 기반의 유연하고 확장 가능한 설치 아키텍처로 제공합니다. MVX 스마트 그리드는 FireEye의 선구적인 MVX 엔진을 분리하고 하드웨어 및 가상 Smart Nodes™를 개발하는 혁신적인 접근 방식을 바탕으로 캠퍼스, 지사 및 원격 사용자를 더 효과적으로 보호합니다. Smart Nodes는 MVX 엔진이 핵심 동적 분석을 수행하는 동안 정적 분석, 분석, IPS, 어플라이드 인텔리전스 같은 다양한 기술을 사용하여 인터넷 트래픽을 분석하고 위협 요소를 탐지 및 차단합니다.

선제적인 SharePoint 컨텐츠 스캔과 격리 기능

FireEye FX는 컨텐츠를 지속적으로 스캔하여 Sharepoint 리포지터리에서 발견된 악성코드에 대해 경보를 발하고 영구적으로 격리시킵니다. 이 플랫폼은 WebDAV 프로토콜을 통해 Sharepoint 서비스와 안전하게 통합함으로써, Sharepoint 리포지터리를 사용하는 기업의 비즈니스 워크플로우를 보호합니다.

맞춤화할 수 있는 YARA 기반의 룰

FireEye FX는 맞춤화된 YARA 룰을 지원하여 대량 파일에 대한 조직 특유의 위협을 분석합니다.

사고에 대한 우선 순위 결정을 능률화

안티바이러스 벤더들이 FireEye FX가 저지한 악성코드를 탐지할 수 있는지 확인하기 위해 FireEye AV 제품군을 사용하여 각 악성 객체를 분석합니다. 따라서 기업들은 사고 대응 후속 조치의 우선 순위를 효과적으로 결정하고, 알려진 악성코드에 대해 일반적으로 사용하는 명명 규칙을 활용할 수 있습니다.

악성코드 인텔리전스 공유

동적으로 생성되는 실시간 위협 인텔리전스는 모든 FireEye 제품이 FireEye CM 플랫폼과의 통합을 통해서 로컬 네트워크를 보호하는 데 도움이 될 수 있습니다. 이 인텔리전스는 FireEye DTI(Dynamic Threat Intelligence™) 클라우드를 통해 전세계의 모든 구독자에게 신규 위협 인텔리전스를 제공합니다.

룰에 대한 튜닝없이 0에 가까운 오탐률

FireEye FX는 튜닝의 필요 없이 관리가 용이한 클라이언트리스 플랫폼입니다. 유연한 설치 모드에는 분석 전용 모니터링과 능동적인 격리 기능이 포함됩니다. 이러한 기능을 통해, 기업들이 얼마나 많은 악성코드가 파일 공유에 상주하는지 확인하고, 악성코드의 내부 확산을 적극적으로 중단시킬 수 있습니다.

Content Smart Node는 필요에 따른 적절한 방어 체계를 제공합니다.

콘텐츠와 보안 관리자는 FireEye Content Smart Node를 통해 유연한 가상 솔루션을 적용하여 기업 전반에 걸쳐 미션크리티컬 콘텐츠를 보호할 수 있습니다. 또한, FireEye MVX Smart Grid 플랫폼을 함께 사용하면 컨텐츠 보호 기능의 확장과 배포를 필요에 따라 원활하게 수행할 수 있습니다.

표 1. FireEye Content Smart Node

	FX 2500V
OS 지원	Microsoft Windows, Mac OS X
성능	70,000 파일/일
네트워크 인터페이스 포트	Ether 1, Ether 2
CPU 코어	2개
메모리	8GB
드라이브 용량	512GB
하이퍼바이저 지원	VMWare ESXi 6.0 이상

FireEye에 대한 더 자세한 정보를 원하시면 다음의 웹사이트를 방문하십시오.

www.FireEye.kr

FireEye Korea
서울 특별시 강남구 테헤란로 534. 글라스타워 20층 전화: 02.2092.6580 / korea.info@fireeye.com

www.FireEye.kr

FireEye®는 인텔리전스 기반 SaaS(Security-as-a-Service)의 선두주자입니다. FireEye는 고객 보안 운영의 완벽한 확장을 위해 혁신적인 보안 기술, 국가 수준의 위협 인텔리전스 및 세계적으로 유명한 Mandiant® 컨설팅을 결합한 단일 플랫폼을 제공합니다. 이러한 접근방식으로 FireEye는 사이버 공격 대비, 예방, 대응에 어려움을 겪는 조직들을 위해 사이버 보안의 복잡성과 부담을 덜어주고 있습니다. FireEye는 포브스 글로벌 2000 기업 중 940개 이상의 기업을 포함, 전세계 67개국에 걸쳐 5,000여개의 고객사를 보유하고 있습니다.

FireEye