McAfee Advanced Threat Defense

지능형 악성 프로그램 탐지

McAfee® Advanced Threat Defense는 조직에서 오늘날 진화한 우회 악성 프로그램을 탐지하고 위협 정보에 대한 조치를 즉시 취해 조직을 보호할 수 있도록 도와 드립니다. 기존 샌드박스와 달리 이 솔루션에는 탐지 기능을 확대하고 우회 위협을 노출하는 조사 기능이 추가되어 있습니다. 환경 전반에서 위협 정보를 즉각적으로 공유할 수 있도록 네트워크와 엔드포인트부터 조사까지 보안 솔루션 간의 통합을 강화하여 보호 및 조사 성능이 향상되었습니다. 유연한 배포 옵션은 모든 네트워크를 지원합니다.

McAfee 기술은 네트워크 주변부에서 엔드포인트까지 전체 영역의 진화한 악성 프로그램 분석 기능을 기존 기능과 연계하고 위협 인텔리전스를 전체 IT 환경과 공유하여 탐지 방법을 혁신했습니다. McAfee 솔루션은 에코시스템 간에 위협 인텔리전스를 공유하여 통합된 보안 솔루션으로 명령 및 컨트롤 통신을 즉시 종료하고, 손상된 시스템을 격리하고, 동일하거나 유사한 위협의 추가 인스턴스를 차단하고, 영향을 평가하고, 적절한 조치를 취합니다.

McAfee Advanced Threat Defense: 진화한 위협 탐지

McAfee Advanced Threat Defense는 혁신적인 계층화된 접근 방법을 사용하여 오늘날의 은폐형 제로 데이 악성 프로그램을 탐지합니다. 안티바이러스 시그니처, 평판 및 실시간 에뮬레이션같은 로우터치 분석 엔진을 동적 분석(샌드박싱)과 결합하여 실제 동작을 분석합니다. 심층적인 정적 코드 분석을 통해 조사가 계속되며 파일 특성 및 명령 세트를 검사하여 예상 동작 또는 우회 동작을 파악하고 알려진 악성 프로그램 패밀리와의 유사성을 평가합니다. 분석의 마지막 단계인 McAfee Advanced Threat Defense에서는 특히 심층 신경망을 이용한 기계 학습을 통해 식별된 악성 지표를 찾습니다. 이와 같이 결합된 솔루션은 시장에서 가장 강력하고 진화한 악성 프로그램 보안 보호를 제공하며, 심층적인 검사와 성능 모두의 요구 사항을 효율적으로 균형 있게 조정합니다. 식별된 악성 프로그램을 더욱 쉽게 탐지하여 시그니처, 실시간 에뮬레이션 성능 이점 등과 같은 분석 방법의 강도는 낮추면서 샌드박싱에 심층적인 정적 코드 분석 및 기계 학습을 통해 확보한 통찰력을 추가하여 위장한 우회 위협에 대한 탐지 수준을 강화합니다. 동적 환경에서는 실행되지 않을 수 있는 악성 지표는 심층적인 언패킹이나 정적 코드 분석 및 기계 학습 통찰력을 통해 식별될 수 있습니다.

McAfee Advanced Threat Defense의 핵심 차별화 요소

광범위한 솔루션 통합

- 기존 McAfee 솔루션, 제3자 이메일 게이트웨이 및 개방형 표준을 지원하는 기타 제품과의 통합
- 조직 전반에서 발생부터 억제 및 보호까지의 격차를 없앰
- 워크플로 간소화로 응답 및 수정 시간 단축
- 자동화 이용 가능

강력한 분석 기능

- 탁월한 분석 데이터를 사용한 정확한 탐지를 위해 심층적인 정적 코드 분석, 동적 분석 및 기계 학습 결합
- SOC를 지원하고 조사를 활성화하는 고급 기능

McAfee에 문의

악성 프로그램 작성자는 패킹을 사용하여 코드의 구성을 바꾸거나 숨겨 탐지를 피합니다. 대부분의 제품은 분석을 위해 전체 원본(소스) 실행 코드를 제대로 언패킹할 수 없습니다. McAfee Advanced Threat Defense에는 불명확성을 해소하여 원래의 실행 코드를 드러내는 확장된 언패킹 기능을 포함합니다. 따라서 심층적인 정적 코드 분석은 높은 수준의 파일 특성에 이상이 있는지 확인하고 특성 및 명령 세트를 분석하여 예상 동작을 파악할 수 있습니다.

심층적인 정적 코드, 기계 학습 및 동적 분석이 함께 진행되어 의심스런 악성 프로그램을 완벽하고 세부적으로 평가합니다. 뛰어난 분석 결과에서는 상황을 전반적으로 파악하고 조치 우선순위를 정하는 데 도움이 되는 요약 보고서뿐 아니라, 악성 프로그램에 대한 분석가 등급 데이터가 포함된 상세한 보고서를 생성합니다.

향상된 보호

네트워크 주변부에서 엔드포인트까지 전체 영역에서 McAfee Advanced Threat Defense와 보안 장치 간에 견고한 통합이 이루어지면 McAfee Advanced Threat Defense가 파일을 악성 파일로 결정하는 즉시 통합 보안 장치에서 즉각적인 조치가 수행될 수 있습니다. 탐지 및 보호 동작이 서로 견고하게 자동으로 통합되는 것도 중요합니다.

McAfee Advanced Threat Defense는 McAfee Threat Intelligence Exchange 또는 McAfee Advanced Threat Defense Email Connector를 통해 다양한 방법으로 일부 보안 솔루션과 직접 통합할 수 있습니다.

직접 통합하면 McAfee Advanced Threat Defense가 파일을 악성 파일로 결정하는 보안 솔루션에서 조치를 취할 수 있습니다. 위협 인텔리전스를 기존 정책 시행 프로세스에 즉시 통합하고 동일하거나 유사한 파일의 추가 인스턴스를 네트워크에 침입하지 못하도록 차단합니다.

McAfee Advanced Threat Defense에서 악성 파일로 결정한 파일은 전체 분석을 내장된 기능으로 수행한 경우처럼 통합 제품의 로고와 대시보드에 표시되므로, 워크플로가 간소화되고 관리자가 단일 인터페이스를 통해 경로를 효율적으로 관리할 수 있습니다.

McAfee Threat Intelligence Exchange를 통합하여 McAfee Advanced Threat Defense의 방어 기능이 강화되고 (McAfee Endpoint Protection 포함) 을 비롯한 방어 기능이 강화되고 광범위한 통합 보안 솔루션에서 분석 결과와 손상 표시기에 액세스할 수 있습니다. McAfee Advanced Threat Defense에서 파일을 악성 파일로 결정하면 McAfee Threat Intelligence Exchange는 평판 업데이트를 통해 위협 정보를 조직 내에 통합된 모든 대응 조치에 즉시 게시합니다.

유연한 중앙 집중식 배포

- 여러 프로토콜을 지원하는 중앙 집중식 배포로 비용 절감
- 모든 네트워크를 지원하는 유연한 배포 옵션

통합 솔루션

- McAfee® Active Response
- McAfee® Advanced Threat Defense Email Connector
- McAfee® Enterprise Security Manager
- McAfee® ePolicy Orchestrator® 소프트웨어
- McAfee® Network Security Platform
- McAfee® Threat Intelligence Exchange
  - McAfee® Application Control
  - McAfee® Endpoint Protection
  - McAfee® Security for Email Servers
  - McAfee® Server Security
- McAfee® Web Gateway
- Bro Network Security Monitor
- TAXII(Trusted Automated eXchange of Indicator Information)

McAfee Threat Intelligence Exchange 지원 엔드포인트에서는 최초 감염 악성 프로그램의 설치를 차단하고 파일이 이후에 나타날 경우에 대비하여 사전 예방적으로 보호할 수 있습니다. McAfee Threat Intelligence Exchange 지원 게이트웨이는 파일이 조직에 침입하는 것을 차단할 수 있습니다. 또한 McAfee Threat Intelligence Exchange 지원 엔드포인트는 네트워크에 연결되어 있지 않은 상태에서도 악성 파일 업데이트를 계속 수신하므로 대역 외 페이로드 제공의 사각지대를 제거할 수 있습니다.

McAfee Advanced Threat Defense Email Connector를 사용하면 McAfee Advanced Threat Defense가 이메일 게이트웨이에서 분석할 이메일 첨부 파일을 받을 수 있습니다. McAfee Advanced Threat Defense는 첨부 파일을 분석하고 메시지 헤더 내 모든 활성 이메일 게이트웨이로 판정을 반환합니다. 이메일 게이트웨이는 첨부 파일 삭제 또는 격리를 포함하여 악성 프로그램이 내부 네트워크를 감염시키거나 네트워크에 확산되지 않도록 차단하는 등의 정책 기반 작업을 수행할 수 있습니다. 오프라인 모드를 사용하면 McAfee Advanced Threat Defense로 스캔하는 동안 최종 사용자에게 전달할 첨부 파일이 있는 이메일을 보낼 수 있습니다. 이메일 게이트웨이는 첨부 파일에 대한 판정을 기다리지 않습니다. 관리자는 McAfee Advanced Threat Defense 또는 McAfee Threat Intelligence Exchange를 통해 첨부 파일 스캔 결과를 확인합니다. 이메일 서버에서의 향상된 탐지를 위해 McAfee Advanced Threat Defense는 McAfee Threat Intelligence Exchange를 통해 McAfee Security for Email Servers와 통합됩니다.

조사를 개선하고 자동화하기 위한 위협 공유

조직에서 공격을 조사하고 교정하기 위해서는 더 나은 결정을 내리고 적절히 대응할 수 있도록 실행 가능한 포괄적인 정보를 갖추어야 합니다. McAfee Advanced Threat Defense는 조사를 개선하고 자동화하기 위해 전체 환경에서 쉽게 공유되는 상세한 위협 정보를 생산합니다. McAfee DXL(Data Exchange Layer) 및 REST 응용프로그램 프로그래밍 인터페이스(APIs) 지원은 다른 제품과의 통합을 가능하게 하며 STIX(Structured Threat Information eXpression/TAXII(Trusted Automated eXchange of Indicator Information) 등 널리 사용되는 위협 공유 표준을 통해 조직은 협업 보안 에코시스템을 생성하고, 지원하고, 확장할 수 있습니다.

McAfee 에코시스템 내에서 McAfee Enterprise Security Manager는 McAfee Advanced Threat Defense 및 기타 보안 시스템에서 제공하는 세부 파일 평판 및 실행 이벤트를 사용하고 연계하여 진화한 보안 정보, 위험 우선 순위 지정 및 실시간 상황 인식을 위한 고급 경보 및 기록 보기를 제공합니다. McAfee Advanced Threat Defense의 데이터 손상 표시기를 통해 McAfee Enterprise Security Manager는 최대 6개월 전부터 유지하고 있는 네트워크 또는 시스템 데이터에서 아티팩트의 징후를 발견하게 됩니다. 새로 식별된 악성 프로그램 소스와 이전에 통신했던 시스템을 밝혀낼 수 있습니다. McAfee Endpoint Protection, McAfee Threat Intelligence Exchange 및 McAfee Active Response와의 긴밀한 통합 덕분에 새로운 구성 실행, 새로운 정책 구현, 파일 제거, 위험을 사전 예방적으로 완화할 수 있는 소프트웨어 업데이트 배포 등과 같은 작업 및 가시성을 통해 보안 작업의 응답성과 효율성을 최적화할 수 있습니다. 네트워크를 통해

감염된 엔드포인트가 McAfee Active Response에서 자동으로 식별되고 McAfee Advanced Threat Defense 보고서에 나열되면 정보에 기반한 조치를 쉽게 수행할 수 있습니다. 이러한 세부 보고서를 McAfee Active Response 내의 단일 작업 공간에서 확인할 수 있으면 분석가의 효율이 높아집니다.

고급 기능으로 조사 지원

McAfee Advanced Threat Defense는 다음을 비롯하여 다양한 고급 기능을 제공합니다.

- **구성할 수 있는 운영 체제 및 응용프로그램 지원:** 엄선된 환경 변수로 맞춤형 분석 이미지를 구성하여 위협을 확인하고 조사를 지원합니다.
- **사용자 대화식 모드:** 분석가가 악성 프로그램 샘플과 직접 상호 작용할 수 있습니다.
- **포괄적인 언패킹 기능:** 조사 시간을 며칠에서 몇 분으로 단축할 수 있습니다.
- **전체 로직 경로:** 일반적인 샌드박스 환경에서 유휴 상태로 남아 있는 추가적인 로직 경로를 강제 실행하여 보다 심층적인 샘플 분석을 수행할 수 있습니다.
- **여러 가상 환경에 샘플 제출:** 파일 실행을 위해 필요한 환경 변수를 결정하여 조사 시간을 단축합니다.
- **상세 보고서:** MITRE ATT&CK™ 매핑, 디스어셈블리 출력, 메모리 덤프, 그래픽 기능 호출 다이어그램, 임베디드 또는 삭제된 파일 정보, 사용자 API 로그 및 PCAP 정보를 포함한 검사를 위한 중요한 정보를 제공합니다. 위협 일정은 공격 실행 단계를 가시화하는 데 도움이 됩니다.
- **Bro Network Security Monitor 통합:** 트래픽을 모니터링 및 캡처하고 조사를 위해 파일을 McAfee Advanced Threat Defense에 전달하도록 의심스러운 네트워크 세그먼트에 Bro 센서를 배포합니다.

배포

유연성이 높은 진화한 위협 분석 배포 옵션은 모든 네트워크를 지원합니다. McAfee Advanced Threat Defense는 Azure Marketplace에서의 가용성과 함께 개인 및 공용 클라우드 모두에 대한 지원을 포함하여 사내 어플라이언스 또는 가상 폼팩터로 사용할 수 있습니다.

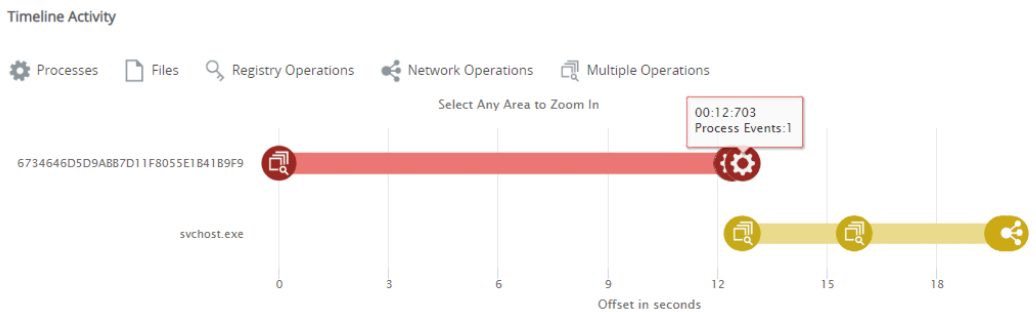

그림 1. 일정 활동은 분석된 위협의 실행 단계를 가시화합니다.

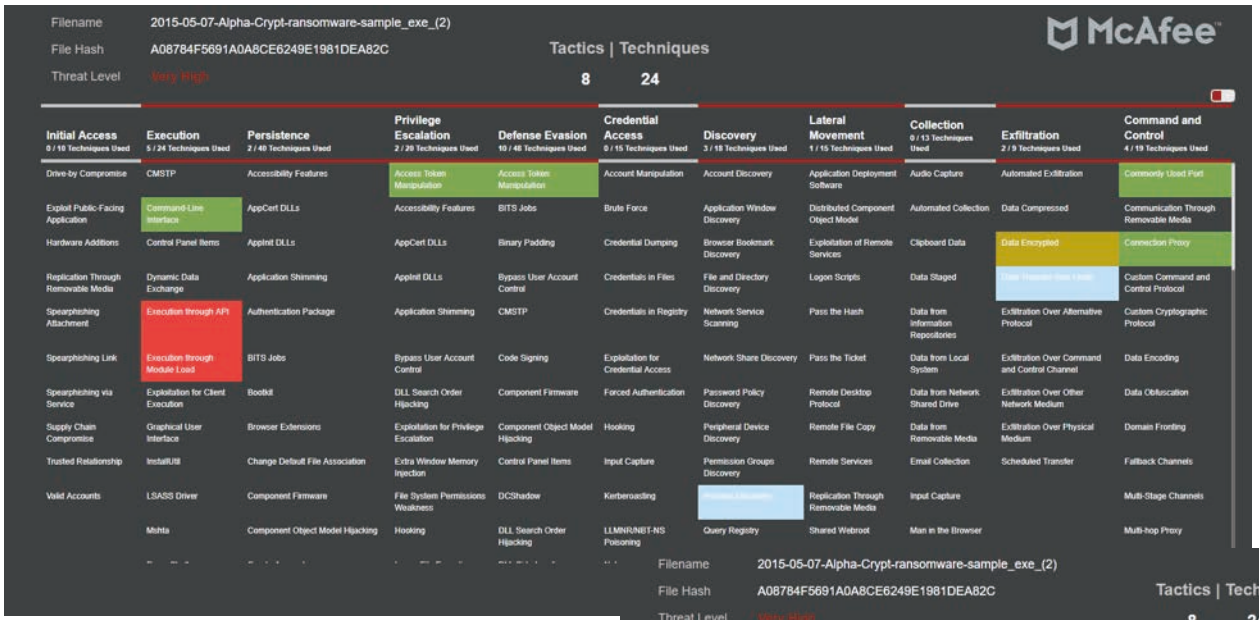

그림 2. 맵을 MITRE ATT&CK™ 프레임워크에 제공합니다.

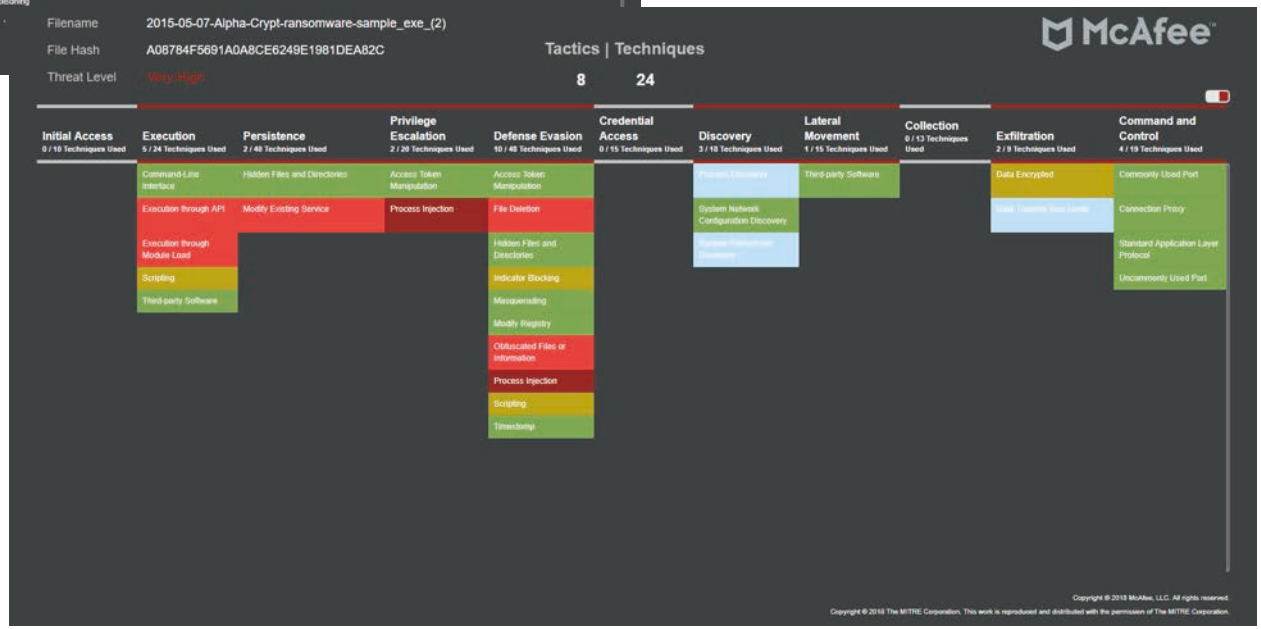

그림 3. 그림 2에 표시된 결과의 필터링된 보기는 확인된 기술 보고에 중점을 둡니다.

McAfee Advanced Threat Defense 사양		
물리적 폼 팩터	ATD-3100 1U 랙 마운트	ATD-6100 1U 랙 마운트
가상 폼 팩터	v1008 ESXi 5.5, 6.0, 6.5, 6.7 Hyper-V Windows Server 2012 R2, Windows Server 2016 Azure Marketplace	
탐지		
지원되는 파일 샘플 유형	PE 파일, Adobe 파일, Microsoft Office 제품군 파일, 이미지 파일, 아카이브, Java, Android 응용프로그램 패키지, URL	
분석 방법	McAfee Anti-Malware Engine, GTI 평판(파일/URL/IP), Gateway Anti-Malware(에뮬레이션 및 동작 분석), 동적 분석(샌드박싱), 심층적인 코드 분석, 사용자 지정 YARA 규칙, 기계 학습: 심층 신경망	
지원되는 OS	Windows 10(64비트), Windows 8.1(64비트), Windows 8(32비트/64비트), Windows 7(32비트/64비트), Windows XP (32비트/64비트), Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, Windows Server 2003, Android Windows 운영 체제 지원은 모든 언어로 제공됩니다.	
출력 형식	STIX, OpenIOC, XML, JSON, HTML, PDF, 텍스트	
제출 방법	포인트 제품 통합, RESTful API, 수동 제출 및 McAfee Advanced Threat Defense Email Connector(SMTP)	

자세한 내용

자세한 내용 또는 McAfee Advanced Threat Defense 평가를 시작하려면 담당자에게 문의하거나 다음을 확인하십시오.

www.mcafee.com/atd.

McAfee (Singapore) Pte Ltd
10 Kallang Avenue #08-10
Aperia Tower 2
Singapore 339510
www.mcafee.com/kr