# Advanced Malware Protection:

## 구매자 가이드

# Advanced Malware Protection: 구매자 가이드

## 개요

이 문서는 지능형 악성코드 차단(Advanced Malware Protection, 이하 AMP) 솔루션이 반드시 갖춰야 할 핵심 기능 및 공급자에게 질문해야 할 주요 사항들을 제시합니다. 또한 Cisco가 4가지 기술의 조합을 통해 오늘날의 지능형 악성코드 공격에 맞서고 있는 방법을 소개합니다.

- 고급 분석
- 종합적인 글로벌 보안 위협 인텔리전스
- 다중 폼팩터 지원(네트워크, 엔드포인트, 모바일 디바이스, 보안 게이트웨이, 가상 시스템)
- 지속적 분석과 회귀적 보안

## 서론

오늘날의 공격자들이 충분한 시간만 주어진다면 어떤 조직도 무너뜨릴 만한 리소스와 전문성, 그리고 인내심을 갖고 있다는 것은 이미 잘 알려진 사실입니다. 기존의 방어 체계인 방화벽 및 엔드포인트 안티바이러스는 더 이상 이러한 공격에 효과적이지 않습니다. 악성코드 처리 프로세스는 반드시 발전해야 하며, 더 빠른 시일 내에 이루어져야 합니다. 표적 공격 및 지속적인 악성코드 탐지는 단일한 특정 시점 제어 또는 제품이 효과적으로 대처하기에는 역부족인 큰 문제입니다. AMP는 통합적인 제어 기능과 공격의 전/중/후 전체에 걸쳐 위협을 탐지 및 확인, 추적, 분석 및 치료할 수 있는 지속적인 프로세스를 함께 갖추고 있어야만 합니다.

### 벤더에게 해야 할 질문

- 지속형 악성코드를 찾아내는 데 빅데이터를 어떻게 활용하고 있는가?
- 악성코드의 기능을 정확하게 파악하기 위해 어떻게 악성코드를 분석하는가?
- 악성코드 분석에서 어떻게 자동으로 탐지 기능을 업데이트하는가?
- 새로운 악성코드 위협에 대한 인텔리전스를 어떻게 수집하는가?
- 회귀적 악성코드 탐지를 위해 어떻게 지속적인 분석을 실행하는가?

이런 상황은 호전되지 않고 앞으로 더욱 악화될 것으로 예상됩니다. 다형성 악성코드가 증가하면서 조직은 시간당 수 만 개의 새로운 악성코드 샘플을 처리해야 하는 상황에 처했으며, 공격자는 비교적 단순한 악성코드 도구를 사용하여 디바이스를 감염시킬 수 있게 되었습니다. 확인된 악성코드의 시그니처 및 파일을 비교하는 블랙리스트 방식은 확장성이 떨어지고 샌드박스와 같은 최신 탐지 기술도 100%의 실효성을 장담하지 못합니다.

## 고급 분석 및 종합적인 보안 인텔리전스

기존의 엔드포인트 보호 공급업체들은 확인된 악성코드가 급증하는 상황에서 더 효과적으로 고객을 지원하기 위해 사실상 시그니처 데이터베이스를 클라우드로 옮기는 것을 골자로 한 "클라우드 기반 안티바이러스" 기능을 내놓았습니다. 이를 통해 5분마다 각 엔드포인트에 수 십 억 개의 바이러스 시그니처를 배포해야 하는 부담에서는 해소되었지만, 시그니처 기반 탐지 기술을 회피하도록 설계된 지능형 악성코드 문제는 해결하지 못했습니다.

공격자들은 클라우드 지원 안티바이러스 모델의 또 다른 한계를 악용하여 끈기있게 활동하는 악성코드를 설계했습니다. 바로 악성코드 차단 기술 대부분이 지속성 및 컨텍스트의 부재, 그리고 오로지 파일의 최초 발견 시점에 탐지된 내용(소위 특정 시점 탐지)에 주력한다는 점에 착안한 것입니다. 그러나 지금은 안전한 파일이 나중에 악성 파일로 바뀔 때도 있습니다. 진정한 보호가 이루어지려면 지속적인 분석이 필수적입니다. 보안 팀은 모든 트래픽을 지속적으로 모니터링하면서 파일의 속성이 바뀌더라도 감염의 출처를 밝혀냅니다.

지능형 악성코드 개발자들은 다양한 기술을 사용해 악성코드의 목적을 숨기는 한편 탐지를 더욱 어렵게 합니다. 이를테면 시그니처 엔진을 속일 수 있을 정도의 다형성 파일, CnC(command-and-control) 네트워크에서 온디맨드 방식으로 악성코드를 확보하는 정교한 다운로더, 자신의 구성 요소를 삭제하여 포렌식 검사기능으로 악성코드를 찾아내 분석하는 것을 어렵게 만드는 삭제 가능 트로이 목마 등이 있습니다. 그 밖에도 많은 예가 있습니다.

더 이상 "생김새"로 악성코드를 식별할 수 없으므로, 효과적인 방어를 위해서는 라이프사이클 내내 악성코드를 수집하고 분석할 새로운 기술이 필요합니다. 이러한 새로운 사전 대응적 보안 인텔리전스 모델은 악성코드의 기능과 경로를 파악합니다. 현재의 위협은 특정 시점 전략을 구사하는 방어 체계를 회피할 수 있고, 최초 탐지 기간이 지난 후에도 시스템을 감염시키고 침입 지표를 남겨놓습니다.

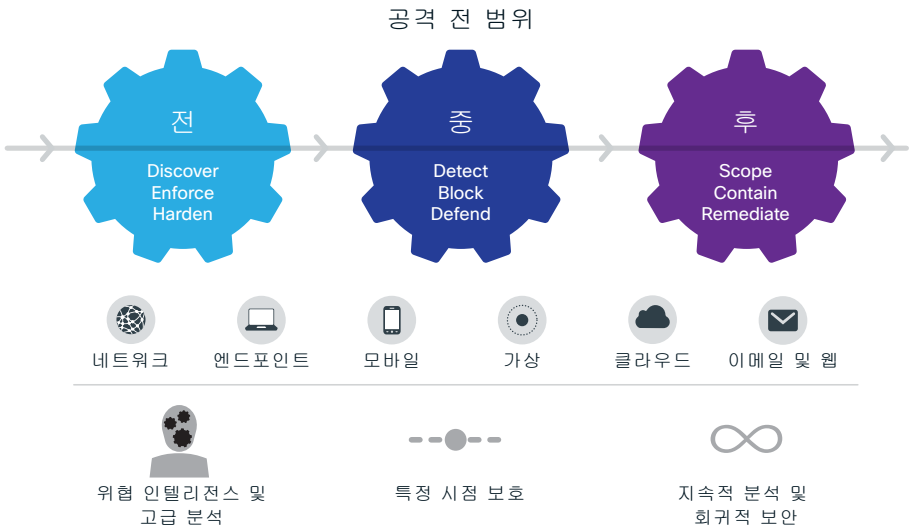
위협만큼 빠른 속도로 대처하는 악성코드 공략 방식이 필요합니다. Cisco는 새롭고 더 포괄적인 방식으로 악성코드 탐지 문제를 해결합니다. 수 천 개의 글로벌 기업과 수 백 만 개의 엔드포인트를 대상으로, Cisco는 매달 수 백 만 개의 악성코드 샘플을 수집합니다. Cisco의 Threat Grid 분석 엔진인 Cisco Talos(Talos Security Intelligence and Research Group) 및 CSI(Collective Security Intelligence) Cloud는 수 만 개의 소프트웨어 속성을 분석하여 악성코드와 안전한 소프트웨어를 구분합니다. 또한 네트워크 트래픽 특성 분석을 통해 CnC 네트워크를 검색하는 악성코드를 식별합니다. 비교를 위해 Cisco 제품 라인에 설치되어 있는 방대한 AMP 자산 데이터를 활용하여[1] 글로벌 차원에서, 그리고 특정 고객의 각 조직에서 정상적인 파일 및 네트워크 활동의 양상을 파악합니다.

1. 현재 AMP 기능은 Cisco Email & Web Security 솔루션에서 추가 라이센스의 형태로 사용할 수 있습니다. 자세한 내용은 http://www.cisco.com/go/amp에서 확인하십시오.

기존의 탐지 전술을 피하도록 설계된 악성코드를 탐지하려면 더욱 정교한 기술이 필요합니다. Cisco는 특별 제작된 모델을 사용하여 형태가 아닌 기능을 기준으로 악성코드를 식별합니다. 따라서 새로운 공격 유형, 심지어 새로운 제로데이 공격도 탐지할 수 있습니다. 이 모델은 악성코드의 변화 속도에 발맞춰 Threat Grid 분석 엔진 및 Talos Security Intelligence and Research Group에서 발견되는 공격 방식을 기반으로 실시간 자동 업데이트됩니다.

AMP에 Threat Grid 기술이 통합됨에 따라 위협 인텔리전스 및 고정/동적(샌드박싱) 악성코드 분석 엔진도 추가되었습니다. 이제 AMP에 통합된 Threat Grid(독립형 솔루션으로도 사용 가능)는 전 세계에서 수집된 추가적인 악성코드 기술 자료를 보안 팀에 제공합니다. 조직은 표준 형식으로 제공되는 컨텍스트 기반 인텔리전스 피드를 기존 보안 기술과 원활하게 통합합니다. 350개가 넘는 행동 분석 지표를 바탕으로 매달 수백만 개의 샘플을 분석하여 수 십 억 개의 아티팩트를 생성합니다. 그리고 이해하기 쉬운 위협 점수를 제공하여 보안 팀이 위협의 우선순위를 지정할 수 있게 합니다. Threat Grid 분석 엔진은 악성코드의 활동, 즉 관련 HTTP 및 DNS 트래픽, TCP/IP 스트림, 영향을 주는 프로세스, 레지스트리 활동 등을 파악하여 보안 팀이 네트워크의 잠재적 위협을 더 확실하게 인식할 수 있게 합니다.

그림 1. 공격 전/중/후 및 각종 공격 벡터로 부터 보호하고, 기존의 특정 시점 탐지 기술에 더하여 지속적인 분석 및 회귀적 보안을 제공하는 Cisco의 보안 방식




추가적인 이점으로는 장기간에 걸쳐 파일을 평가하는 클라우드 분석을 포함합니다. Cisco AMP 솔루션은 파일이 처음 분석되고 한참 지난 후에도, 심지어 이미 탐지 지점을 통과했더라도 사용자에게 알림을 전송할 수 있습니다.

최종적으로 이러한 이점은 Cisco AMP 커뮤니티 전체로 확장됩니다. 언제든지 파일 속성이 바뀔 경우 AMP는 알림을 전송합니다. 이러한 경우 Cisco AMP를 사용하는 모든 조직은 악성 파일의 존재에 대해 즉시 알게 되고, 클라우드의 힘을 빌려 "공동 면역" 체제를 마련할 수 있습니다.

## 시간을 되돌려 공격을 막아내는 회귀적 보안

공격자도 가만히 있지는 않습니다. 공격자들은 끊임없이 현재의 보안 제어 기능을 평가하고 전술을 바꿔 방어 체계보다 한발 앞서나가려 합니다. 실제로 대부분의 공격자들은 공격 실행에 앞서 대표적인 악성코드 차단 제품을 대상으로 자신의 악성코드를 테스트합니다. 블랙리스트 방식의 실효성이 감소한 만큼 악성코드를 차단하고 분석하기 위해서는 VM(virtual machine) 기반의 동적 분석 기법을 사용하는 보안 업체들이 늘고 있습니다. 공격자들은 이에 대응하여 전술 변화를 꾀했습니다. VM에서 실행할 때 아무 작업도 하지 않거나 몇 시간 동안 (또는 며칠 간) 공격 실행을 늦추는 것입니다. 그들은 평가 기간에 어떤 악성 활동도 하지 않았으므로 탐지를 피할 것으로 가정합니다. 물론 대기 시간이 지나면 악성코드는 디바이스를 감염시킵니다.

그러나 특정 시점 기술로는 파일을 다시 분석하지 못합니다. 파일이 일단 안전한 것으로 간주되면 탐지 기술이 발전했든 파일에서 악성 동작이 수행됐든 상관없이 계속 "안전한" 것으로 간주됩니다. 설상가상으로 악성코드가 탐지를 피하게 되면, 이런 제어 기능으로는 환경 내에서 전파 상황을 추적하거나, 감염 경로를 분석하거나 잠재적 악성코드 게이트웨이(반복적으로 악성코드에 감염되어 더 광범위한 유포를 위한 거점 역할을 하는 시스템)를 식별할 수 없습니다.

### 회귀적 보안

지속적인 분석을 통해 시간의 추이에 따른 파일 동작, 추적 프로세스, 파일 활동, 커뮤니케이션을 계속 추적하여 감염 사실을 종합적으로 파악하고 근본 원인을 규명한 다음 치료를 수행하는 것입니다. 그러면 과거의 시점으로 돌아가 잠재적 공격을 차단할 수 있습니다. IoC(indication of compromise)가 나타날 때, 이를테면 이벤트 트리거, 파일 속성의 변화, IoC 트리거가 발생할 때 회귀적 보안이 필요하게 됩니다.

최상의 방법은 어떤 탐지 기술도 100% 완벽할 수 없다고 가정하는 것입니다. 오로지 탐지 기술만으로 확실하게 보호할 수 있다고 생각하는 것은 주요 자산을 보호하는 능력을 과신할 뿐 아니라 적들의 공격 능력을 과소평가하는 일입니다. 조직은 자신의 방어 체계가 뚫릴 수 있음을 인정해야 합니다. 감염의 범위와 상황을 인식하고 신속하게 피해를 억제하는 한편 위협 요소, 근본 원인, 악성코드 게이트웨이를 제거할 수 있어야 합니다. 그러기 위해서는 회귀적 보안이 필요합니다.

AMP의 회귀적 보안 기술을 통해 사실상 시간을 되돌려 감염된 파일이 식별된 시점과 상관없이 어떤 디바이스가 악성코드에 노출되었는지 확인할 수 있습니다. 파일 경로 및 IoC(indications of compromise)의 2가지 요소가 이러한 기능을 지원합니다. 파일 경로에서는 보호 네트워크를 지나는 모든 파일을 추적하고 노출된 보호 대상 디바이스 각각의 전체 활동 기록에 대한 액세스를 가능하게 합니다. IoC에서는 파일 경로에서 제공하는 정보를 활용하여 행동 패턴을 만들고 이를 통해 시스템에 존재하지만 탐지되지 않는 악성코드가 있는지 찾습니다.

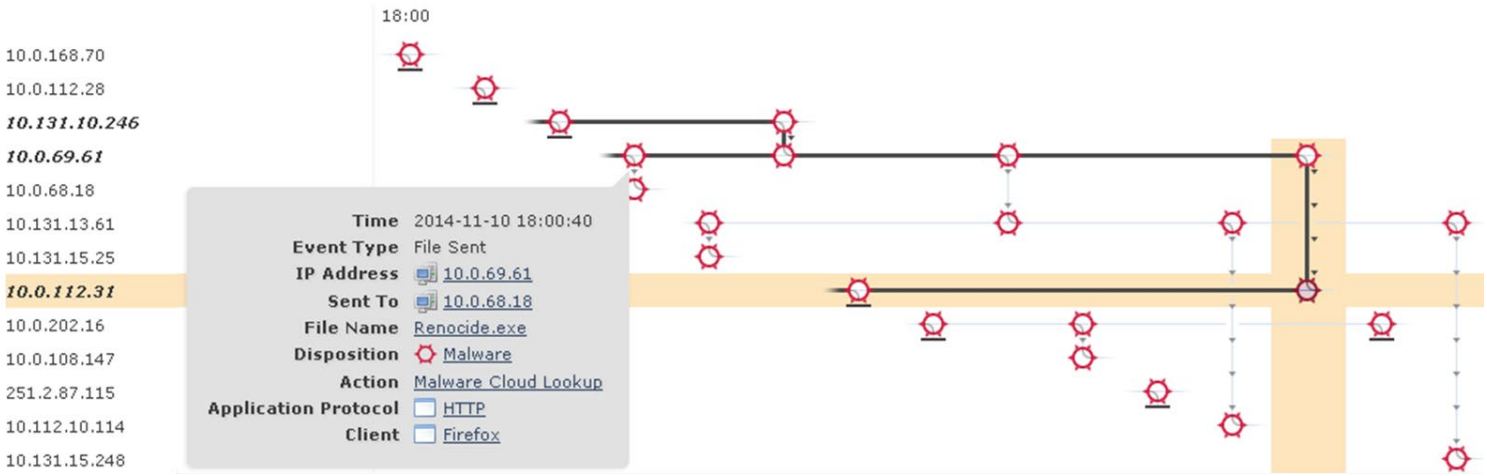
## 경로 분석을 통한 악성코드 추적

어떤 파일이 나중에 악성코드로 판명될 경우 기존의 악성코드 차단 방어 기술로는 해결 방법이 제한적일 수 밖에 없습니다. 타임머신을 타고 과거로 돌아가 파일의 진입을 차단하는 것 역시 불가능합니다. 악성코드는 이미 침투한 상태이고, 그 악성코드가 얼마나 확산되었는지 또는 어떤 해를 입혔는지 알 수가 없습니다. 대부분의 악성코드 차단 제어 기능은 여기서 한계에 부딪히며, 사용자는 문제의 범위를 온전히 파악하지 못하고 해결 방법도 모색할 수 없습니다.

AMP의 근간이 되는 빅데이터 및 고급 분석 기능을 만나보십시오. AMP의 경로 분석 기능으로 악성코드의 이동 경로를 정확하게 파악할 수 있습니다. 경우에 따라 감염된 디바이스를 즉시 자동으로 치료할 수도 있습니다. 경로 분석은 파일의 이동 경로 및 시스템에 대해 수행한 작업을 시각적 맵핑으로 제공합니다. 하지만 네트워크 전 범위에서 파일의 활동을 파악하는 데 머무르지 않습니다. AMP는 파일의 속성과 관계없이 각 실행 파일이 단일 엔드포인트에서 벌인 세부적인 활동도 보여줍니다. 그런 다음 어떤 엔드포인트에서의 활동 내역에서 더 나아가 악성 파일이 확장 네트워크의 어디에서 다른 엔드포인트로 이동했는가를 보여주면서 보안 팀에 높은 수준의 가시성을 선사합니다. 더 중요한 점은 AMP가 모든 파일의 모든 사용처를 추적하므로 (최초의 악성코드 피해자인) "Patient Zero" 와 감염된 다른 디바이스를 모두 찾아내 근본적으로 감염을 해결할 수 있습니다. 클린업 이후 단 하나의 악성코드라도 남아 있으면 재감염의 가능성이 높다는 것은 이미 잘 알려진 사실입니다.

또한 경로 분석은 파일 활동과 관련된 정보만을 분석하는 것이 아닙니다. 파일의 계보, 사용, 종속성, 커뮤니케이션, 프로토콜에 대한 정보도 추적할 수 있습니다. AMP는 어떤 파일이 악성코드를 설치하는지 추적하여 감염된 악성코드 또는 의심스러운 활동의 근본 원인을 신속하게 규명할 수 있습니다. 보안 팀은 공격이 진행되는 동안 탐지에서 제어 모드로 전환하고 바이러스 보안 침해와 감염 경로을 신속하게 파악하여 효과적으로 추가 감염을 방지할 수 있습니다.

그림 2. 파일 경로 분석 화면은 악성코드의 진입 지점, 활동, 관련된 엔드포인트 정보와 함께 악성코드의 유포 현황을 보여줍니다.



탐지 건수가 많으면, 특히 악성코드와 관련된 이벤트가 많을 경우에는 어디에 우선 순위를 두고 즉시 대응할지 결정하기가 매우 어렵습니다. 엔드포인트에서 악성 파일 차단과 같은 단 한번의 이벤트로 인해 감염되었다고 단정할 수는 없습니다. 하지만 정상으로 보이더라도 여러 건의 이벤트가 동시다발적으로 일어난다면 시스템이 감염되었고 보안 사고가 임박했거나 진행 중일 가능성이 높습니다.

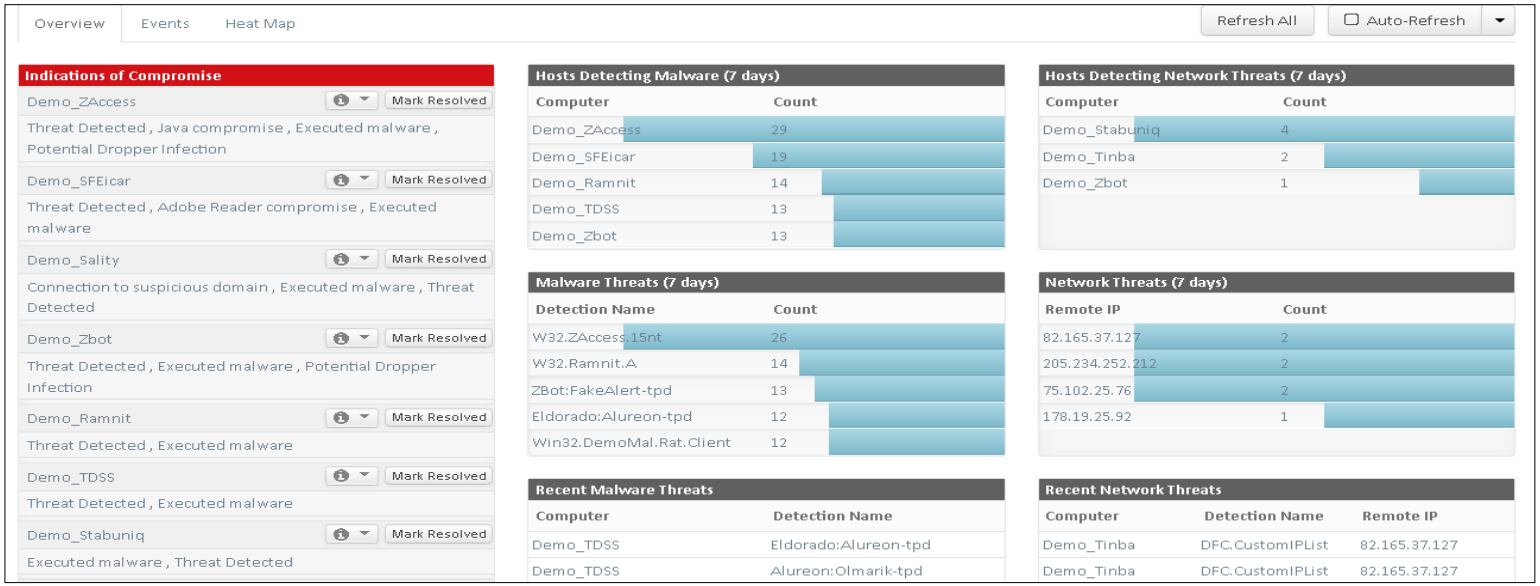
## IoC는 지문이 아닌 패턴 식별

AMP의 IoC 기능을 통해 더 심층적인 분석을 수행하여 진행 중인 공격의 징후를 보이는 시스템을 찾아낼 수 있습니다. 이 기능은 특정 시점 탐지 기술의 차원을 넘어 최초 분석 이후에도 지속적으로 악성코드 관련 활동을 수집, 분석, 연계하면서 자동화된 분석 및 위험 우선순위 결정을 가능하게 합니다.

마지막으로 악성코드가 사내에 침투하여 자리 잡은 경우 대개는 CnC 서버와 통신을 시도합니다. 또는 공격자가 직접 제어하는 경우라면 정찰 활동에 나서서 원래의 목표에 점점 접근합니다.

Cisco AMP는 보호받는 엔드포인트의 통신 활동을 모니터링하는 하고 이를 종합 보안 인텔리전스 분석 내용과 비교하여 감염 여부를 확인하며, 필요한 경우 엔드포인트에서 악성코드의 배포와 통신을 차단합니다. 보안 전문가는 이 기능을 활용하여 기업 네트워크의 보호 구역에 속하지 않는 엔드포인트, 이를테면 원격 근무자 또는 모바일 직원이 사용하는 시스템에서 악성코드의 확산을 효과적으로 억제할 수 있습니다. 또한 경로 분석 및 IoC는 수집된 네트워크 활동 정보를 토대로 더 신속하게 조사하고 위협의 우선 순위를 결정합니다.

그림 3. 시스템의 IoC를 보여주는 Cisco AMP 대시보드 화면



## 통합의 효과: 네트워크, 보안 게이트웨이, 물리적 및 가상 엔드포인트, 모바일 기기에 정책 적용

어떤 보안 제어 기능도 진공 상태에서는 실행될 수 없습니다. 지능형 악성코드를 막기 위해서는 네트워크, 게이트웨이, 엔드포인트 방어 기술 간의 긴밀한 공조가 필요합니다. 더 신속하게 탐지하고 대응하며 악성코드 침입 시 심각한 보안 사고로 확대되기 전에 처리하려면 보안 도구는 서로 연동하고 정보를 공유하며 이벤트의 상관성을 분석해야 합니다. 또한 모든 레벨에서 위협 및 치료 활동을 추적하는 중앙 관리 콘솔도 필요합니다. Cisco는 클라우드 기반 보안 인텔리전스, 지능형 네트워크 분석, 다중 정책 시행 지점을 활용하는 통합 시스템을 제공하여 지능형 악성코드가 암암리에 활동할 수 없게 합니다.

Cisco의 광범위한 AMP 기능은 접근하는 악성코드를 탐지하고 차단하도록 네트워크에서 보호를 시작합니다. 모든 파일이 네트워크를 드나들 때 AMP는 파일 핑거프린트(file fingerprint)를 생성하고 Cisco FireSIGHT™ Management Center(관리 센터)를 통해 파일의 악성 여부를 판단합니다.

Management Center에서 그 파일을 본 적이 없다면 종합 보안 인텔리전스에 확인하고 Cisco의 보안 인텔리전스 네트워크에서 그 파일이 발견된 적이 있는지 조사합니다. 이와 같은 간단한 조회 기능은 (네트워크의 모든 파일을 대상으로 하는 샌드박스 기능보다) 확장성이 뛰어나고 시스템 레이턴시에 영향을 미치지 않습니다. 악성으로 판별된 파일에 대해서는 Management Center에서 파일 경로 기능을 통해 위험의 컨텍스트와 범위를 확인합니다.

Cisco의 가벼운 엔드포인트 악성코드 차단 에이전트(Cisco AMP™ 커넥터)를 각 보호받는 디바이스에 구현하여, 모든 파일 활동을 종합 보안 인텔리전스 및 알려진 악성코드와 비교하여 점검할 수도 있습니다. AMP for Endpoint는 악성 파일을 찾아낼 뿐 아니라 보호받는 디바이스에서 악성코드의 동작을 탐지하고 차단합니다. 지금까지 본 적이 없는 파일이더라도 제로데이 공격에 대비하여 엔드포인트를 보호합니다. AMP for Endpoints는 앞서 소개한 회고적 보안 및 경로 기능을 활용하여 보안 침해의 범위를 파악하고 즉각적인 치료가 필요한 디바이스를 알아냅니다.

파일이 의심스러운 것으로 표시될 경우 AMP는 심층 파일 분석을 수행합니다. 앞서 설명한 대로 Cisco의 클라우드 기반 분석은 악성코드로 확인된 파일의 동작을 정확히 파악하고 그 공격을 프로파일링합니다. AMP for Endpoint와의 통합으로 추가적인 인텔리전스 피드, 고정 분석, 동적 분석 엔진을 접목시켜 더 심층적으로 악성코드를 조사할 수 있게 되었습니다. 이러한 프로세스에서 IoC가 생성되고, 이를 통해 이미 네트워크에 침투했을 악성코드를 찾아낼 수 있습니다.

AMP는 이러한 악성코드 프로필을 참조하여 악성코드 공격에 미리 대응할 수 있도록 지원합니다. 나중에(회귀적 보안을 통해) 악성 파일로 판명될 경우 또는 Cisco AMP 커뮤니티의 다른 환경에서 식별될 경우 CSI Cloud가 해당 조직의 Management Center에 업데이트된 정보를 전송하여 네트워크 또는 엔드포인트에서 악성코드를 차단할 수 있게 합니다. 따라서 Cisco AMP 커뮤니티의 다른 구성원들과 공동 면역 체계를 구축할 수 있습니다. 또한 로컬 관리자가 지역화된 공격을 발견하여 즉각적인 조치를 취해야 하는 경우 특정 파일 및 IP 주소를 차단에 필요한 맞춤 규칙을 설정할 수도 있습니다.

Cisco AMP for Endpoints는 모바일 디바이스도 보호합니다. AMP 모바일 커넥터는 같은 보안 인텔리전스 클라우드를 활용하여 Android 애플리케이션에 위협 요소가 있는지 신속하게 실시간으로 분석합니다. 가시성의 범위가 모바일 디바이스까지 확대되므로 어떤 디바이스가 감염되었는지, 어떤 애플리케이션 때문에 악성코드가 유입되었는지 빠르게 확인할 수 있습니다. 강력한 제어 기능으로 특정 애플리케이션을 블랙리스트에 추가함으로써 공격에 맞설 수 있습니다. 즉, 기업 리소스에 액세스하는 모바일 디바이스에서 사용 가능한 애플리케이션을 제한합니다.

AMP 기능은 현재 Cisco Email & Web Security 게이트웨이, Cisco Cloud Web Security, Cisco ASA with FirePOWER Services에서 사용 가능합니다. 이러한 어플라이언스에 AMP 기능을 추가함으로써 잠재적 진입 지점에서 더 효과적으로 지능형 악성코드를 탐지하고 차단할 수 있습니다. AMP의 주요 기능으로는 앞서 소개한 파일 평판 및 파일 샌드박싱 기능이 있습니다. 또한 회귀적 경고 기능으로 게이트웨이를 지나간 파일을 지속적으로 분석하고 CSI Cloud의 실시간 업데이트를 통해 끊임없이 변화하는 보안 위협에 미리 대응할 수 있습니다. 악성 파일이 위협으로 식별되면 AMP는 관리자에게 경고하고, 네트워크의 어떤 영역 및 애플리케이션이 언제 감염되었을 가능성이 있는지 알려줍니다. 따라서 고객은 공격이 확산되기 전에 빠르게 파악하여 해결할 수 있습니다.

앞서 살펴본 것처럼, 악성코드는 여러 공격 벡터를 통해 유입될 수 있습니다. 조직의 전 범위에서 각종 활동을 빠짐없이 모니터링하는 것이 중요합니다. 글로벌 보안 인텔리전스 네트워크를 활용하고 게이트웨이, 네트워크, 엔드포인트, 모바일 디바이스, 가상 시스템에서 보안 침해를 탐지, 차단, 추적, 조사하고 제거함으로써 지원 범위가 한정된 다른 보안 제어 기능에서 놓치기 쉬운 사각지대를 없앨 수 있습니다.

모든 AMP 구축 및 그 기능에 대한 자세한 내용은 http://www.cisco.com/go/amp를 참조하십시오.

## AMP 적용 사례

실제 사례는 통합 AMP 솔루션의 진가를 확인하는 가장 좋은 방법이기도 합니다. AMP는 Java 제로데이 공격이 공표되기 48시간 전에 이를 탐지해냈습니다. 이 사례에서는 AMP for Endpoints가 여러 디바이스에서 특이한 활동을 탐지했습니다. 고객은 CSI Cloud로 파일을 분석했고 이 파일을 악성코드로 판단했습니다.

그 다음 단계는 공격의 범위를 파악하고 최대한 신속하게 감염을 치료하는 것이었습니다. 이어서 경로 분석 기능을 사용하여 어떤 디바이스가 문제의 파일에 노출되었는지 또는 어디서 공격의 행동 패턴이 나타났는지 파악했습니다. 감염된 디바이스를 치료한 다음에는 파일과 IoC를 모두 차단하는 맞춤형 규칙을 설정했습니다.

하지만 이 규칙이 필요했던 것은 잠깐이었습니다. 그 사건 이후 모든 AMP 고객이 그 악성코드의 프로필을 받아 공격을 예방할 수 있었습니다. 파일 및 지표가 빅데이터 분석 엔진에 추가되었기 때문에 그 공격의 모든 인스턴스가 디바이스 또는 네트워크에 침투하기 전에 차단되었습니다. 이 과정에서 고객은 공격에 대한 알림을 받아 각자의 환경에 해당 위협이 있는지 조사할 수 있었습니다. 결국 한 번의 조치로 이 제로데이 공격이 공개적으로 알려지기 전에 전 세계의 모든 Cisco AMP 고객이 보호받을 수 있었습니다.

## 결론

지능형 악성코드 공격을 탐지하고 제거하려면 혁신적인 솔루션이 필요하다는 데 업계 관계자 모두 동의하지만, 기존의 엔드포인트 탐지 솔루션이든 최첨단 방어 체계든 오로지 탐지 기술에만 의존하는 곳이 너무 많습니다. 연이어 헤드라인을 장식하는 정보 유출 및 보안 사고 뉴스에서 입증된 것처럼 그러한 방식은 실패할 수밖에 없습니다.

지능형 공격을 효과적으로 막아낼 가능성을 높이려면 지속적인 분석과 빅데이터 분석 기능으로 네트워크 전반에서 물리적 환경과 가상 환경에서 보호 대상 엔드포인트 및 모바일 디바이스에서 발생하는 파일의 상호 작용 및 활동을 추적해야 합니다. 상당수의 공격이 기존 솔루션의 탐지 기간에는 잠복해 있기 때문에 악성코드 판정을 회귀적으로 변경하고 해당 파일과 그 지표의 사내 이동 경로를 추적함으로써 이러한 지능적인 공격의 피해를 효과적으로 줄이고 해결할 수 있습니다.

또한 AMP는 보호 대상 엔드포인트 디바이스뿐만 아니라 네트워크, 모바일 디바이스, 가상 시스템까지 포괄하면서 일관성 있는 보호 수준을 보장해야 합니다. 다음 공격의 표적이 누구일지 예측할 수 없기 때문입니다.

AMP는 다음과 같은 이점을 제공합니다.

- 엔드포인트, 네트워크, 모바일 디바이스, 보안 게이트웨이, 가상 시스템에서 일관된 정책을 적용하면서 유연하게 구축
- 업계보다 한발 앞서 새로운 공격을 대한 식별하고 분석하는 데 유용한 CSI Cloud
- 회귀적으로 악성코드 파악, 사내 악성코드의 확산에 앞서 경로 분석을 통해 악성코드의 모든 인스턴스 발견
- 글로벌 Cisco AMP 커뮤니티가 제공하는 공동 면역 체계 - Talos의 조사 결과 그리고 수 백 만 개의 AMP 보호 에이전트에서 확인한 파일 샘플

보안 평가에 Cisco AMP 솔루션을 포함하려면 http://www.cisco.com/go/amp를 참조하십시오.