Cisco Email Security:컨텍스트 적응형 스캐닝 엔진(CASE) 이해

목차

소개

복합적인 위협의 양 증가는 크게 나타났습니다.지난 2년 동안 가장 심각한 바이러스 전파 확산 중 상당수는 스팸 전달과 관련이 있습니다. 즉, 바이러스 페이로드는 스팸, 피싱, 스파이웨어, 그리고 더 많은 바이러스를 보내는 데 사용되는 "좀비" 컴퓨터 군단을 만듭니다.이메일 기반 스파이웨어는 6개월마다 두 배로 증가했으며, URL이 사용자 이름과 비밀번호를 도용하는 "키 로거"를 설치하는 것은 흔한 일입니다.바이러스는 좀비 네트워크를 만들어 대규모 분산형 서비스 거부 공격을 실행하는 데 사용될 수도 있습니다. 예를 들어, Mydoom.B 변종이 SCO의 웹 사이트를 연계 공격으로 오프라인 상태로 만든 경우입니다.

복합적인 위협이 갑자기 증가하는 원인은 무엇입니까?간단히 말해, 그것은 돈이다.1세대 안티스팸 기술(예: 블랙리스트 및 콘텐츠 필터)이 더욱 널리 구축됨에 따라, 기존의 방법(예: 메시지 텍스트에 "제안"이 포함된 고정 서버 은행에서 스팸을 보내는 방법)은 수익성이 낮아졌습니다.안티스팸 기술을 사용하는 네트워크가 증가함에 따라 "단순" 스팸 메시지가 줄어들어 스팸 필터를 지나 수신자의 받은 편지함으로 전달됩니다.이는 스패머의 이익 마진을 손상시키고 이러한 변화에 적응하도록 강요했습니다.

스팸 발송자들은 두 가지 방법으로 이 상황을 처리했습니다.

1. 이들은 더 많은 스팸을 보내면서 배달 속도에서도 손실되는 것을 메워줄 것으로 기대하고 있습니다.
2. 이들은 메시지를 위장하고 메시지당 이익을 늘리기 위해 복합적인 공격에 의존하고 있습니다.

두 번째 기술은 종종 범죄 활동이 된다.공격을 실행하고 바이러스, 피싱 및 기타 위협으로부터 이익을 얻기 위해 조직화된 범죄 네트워크가 구축되었습니다.2004년 존 도버라는 한 개인이 2백만 개 이상의 신용카드 번호를 매매한 후 체포되었는데, 이 번호는 피싱 공격으로 유출되었다.

복합적인 공격에 사용된 기술도 점점 정교해지고 있습니다.Most.N 바이러스는 이메일, 웹 다운로드, 트로이 목마, 좀비 등을 사용했다.기존의 콘텐츠 분석 필터는 이러한 지능형 위협에 대응하지 못합니다.1세대 안티스팸 필터의 많은 사용자는 필터를 "교육"하거나 새 규칙을 작성하는 데 더 많은 시간을 할애해야 한다는 사실을 알게 되었습니다.그러나 이러한 노력에도 불구하고, 탐지율과 처리량은 모두 감소하고 있습니다.그 결과, 각 시스템을 관리하는 데 더 많은 관리 시간을 사용하는 반면, 로드를 처리하는 데 더 많은 시스템이 필요하므로 비용이 증가합니다.

Cisco Email Security는 CASE(Context Adaptive Scanning Engine)라고 하는 고유한 혼합 위협 방어 기술로 이러한 위협을 해결했습니다. Cisco Email Security의 CASE 기술은 기존의 스팸과 정교한 좀비 기반 공격을 모두 차단하는 데 사용됩니다.또한 이 동일한 검사 기술을 사용하여 서명 가용성보다 최대 42시간 앞서 바이러스와 악성코드를 예방하고 단일 통합 스캔을 통해 효율성을 높일 수 있습니다.

CASE 이해, 컨텍스트에서 혼합된 위협 탐지

1세대 필터는 메시지의 내용을 확인하고 결정을 내리도록 설계되었습니다.예를 들어, "자유"라는 단어가 "허브"라는 단어와 함께 두 번 이상 메시지에 나타나면 스팸일 가능성이 있습니다.이러한 접근 방식은 스팸 발송자가 "사용자를 위한" 대신 "f0r y0u"와 같은 문자 대신 숨겨진 문자 또는 숫자를 사용하여 쉽게 패할 수 있습니다. Bayesian 필터와 같은 2세대 기술은 스팸과 합법적인 이메일의 특성을 자동으로 구별하는 방법을 익혀 이러한 제한을 해결하려고 했습니다.하지만 이러한 기술들은 훈련하기에 너무 어렵고, 반응하기에는 너무 늦었고, 스캔하는 데 너무 느렸다는 것을 증명했습니다.

오늘날의 스팸과 함께 사용되는 고급 난독화 기술을 고려할 때 최신 필터의 상태에서는 수신 메일을 전체 컨텍스트에서 검사해야 합니다.CASE는 메시지의 합법성을 평가하는 사람이 사용하는 논리를 에뮬레이트하는 고급 기계 학습 기술을 사용합니다.Cisco Email Security의 CASE 기술과 함께 인간 리더는 다음과 같은 네 가지 기본적인 질문을 합니다.

1. 누가 메시지를 보냈죠?
2. 메시지의 링크는 어디로 가야 합니까?
3. 메시지가 어떻게 생성되었습니까?
4. 메시지에 포함된 내용

다음은 평가된 각 논리적 영역을 검사하는 것입니다.

누구?

앞서 설명한 것처럼 1세대 스팸 필터는 주로 스팸 식별을 위해 키워드 검색을 사용합니다 .Cisco(IronPort)는 평판 필터링 개념을 도입하여 이메일 보안 업계에 혁신을 가져왔습니다.콘텐츠 필터링이 "메시지에 무엇이 있습니까?"라는 질문을 하는 동안, 평판 필터링은 "메시지를 보낸 사람?"을 질문합니다.이 간단하지만 강력한 개념은 위협을 평가하는 상황을 확대했습니다.2005년에는 거의 모든 주요 상용 보안 벤더가 어떤 유형의 평판 시스템을 채택했습니다.

평판 결정에는 지정된 발신자의 동작에 대한 광범위한 데이터 집합을 검토하는 것이 포함됩니다(발신자는 IP 주소 전송 메일로 정의됨). Cisco는 시간이 지남에 따라 이메일 볼륨, 이 IP에 의해 적중되는 "스팸 트랩" 수, 발신지, 호스트 감염 여부 등 120개 이상의 다양한 매개변수를 고려합니다 .Cisco에는 알고리즘을 개발하고 유지 관리하는 통계 전문가 팀이 있으며, 이 데이터를 처리하여 평판 점수를 생성합니다.그런 다음 이 평판 점수는 수신 Cisco ESA(Email Security Appliance)에서 사용할 수 있습니다. 그러면 신뢰성에 따라 발신자를 조절할 수 있습니다.간단히 말해, 발신자가 더 많이 나타나면 더 느려집니다.평판 필터링은 또한 메시지가 수락되기 전에 연결을 거부하거나 제한하여 급증하는 이메일 볼륨과 관련된 문제를 해결하므로 메일 시스템의 성능과 가용성이 크게 향상됩니다.Cisco ESA 평판 필터는 수신 스팸의 80% 이상을 차단하며, 이는 경쟁사 시스템보다 약 2배 빠른 것입니다.

어디?

2003년에는 이메일 콘텐츠 분석과 평판이 함께 사용되었지만, 스패머와 바이러스 작성자의 전술의 정교함은 계속 증가하고 있습니다.이에 대응하여 Cisco(IronPort)는 웹 평판 개념을 도입했습니다.

이는 메시지가 평가되는 상황을 넓히기 위한 새로운 핵심 벡터입니다.이메일의 평판 계산에 사용되는 접근 방식과 마찬가지로 Cisco Web Reputation은 지정된 URL의 평판 평가를 위해 45개 이상의 서버 관련 매개변수를 살펴봅니다.이 매개변수에는 시간에 따른 URL에 대한 HTTP 요청 볼륨, 평판 점수가 낮은 IP 주소에서 URL이 호스팅되는지 여부, 이 URL이 알려진 "좀비" 또는 감염된 PC 호스트와 연결되었는지 여부, URL에서 사용하는 도메인의 기간이 포함됩니다.이메일 평판과 마찬가지로, 이 웹 평판은 세분화된 점수를 사용하여 측정되며, 이를 통해 정교한 위협의 모호성을 처리할 수 있습니다.

어떻게?

Cisco Email Security의 상황 분석에 대한 또 다른 새로운 접근 방식은 메시지 구성을 검토하는 것입니다.Microsoft Outlook과 같은 합법적인 메일 클라이언트는 MIME 인코딩, HTML 또는 기타 유사한 방법을 사용하여 고유한 방법으로 메시지를 작성합니다.메시지의 제작 원리를 보여주고 있다.가장 대표적인 예는 스팸 서버가 합법적인 메일 클라이언트의 구축을 에뮬레이트하려고 할 때 발생합니다.이것은 하기 어렵고, 불완전한 에뮬레이션은 잘못된 메시지의 믿을 만한 표시입니다.

뭐?

전체 상황 분석에서는 메시지의 내용을 고려해야 하지만 앞서 언급한 것처럼, 콘텐츠 분석만으로는 부적법한 메일을 식별하는 데 충분하지 않습니다.Cisco Email Security의 CASE 기술은 최첨단 기계 학습 기술을 사용하여 완전한 콘텐츠 분석을 수행합니다.이러한 기법은 메시지의 내용을 검사하고 다양한 범주에서 점수를 매기도록 합니다. 즉, 재무, 포르노입니까, 아니면 다른 스팸과 상관관계가 있는 것으로 알려진 콘텐츠를 포함하고 있습니까?이 콘텐츠 분석은 메시지의 전체 컨텍스트를 평가하기 위해 Who, Where, How, What 등의 다른 특성과 함께 CASE에 포함됩니다.

사례 적용 사례

CASE에서 분석한 데이터의 범위 때문에 이 기술은 IPAS(IronPort Anti-Spam), 그레이메일 및 VOF(Virus Outbreak Filter)를 비롯한 다양한 보안 애플리케이션에서 사용됩니다. 아래 예에서는 CASE를 사용하여 스팸을 중지하는 방법을 설명합니다.메시지의 콘텐츠는 피싱되는 조직과 거의 동일하므로 메시지의 콘텐츠 분석으로 어떤 위협도 식별할 수 없습니다.콘텐츠 기반 필터에는 이 메시지가 합법적인 통신인 것 같습니다.이 메시지가 스팸인지 여부를 확인하기 위해 "What(무엇을)"에 주로 의존하는 필터는 메시지를 합법적인 것으로 인식하도록 쉽게 속일 수 있습니다.그러나 메시지의 전체 컨텍스트를 분석하면 다른 그림이 그려집니다.

- 보내는 메일 서버의 IP 주소가 의심스럽습니다. 볼륨이 갑자기 급증했고 그 대가로 도메인이 메일을 수락하지 않습니다.
- 이메일의 URL은 소비자 광대역 네트워크에 있는 것으로 보이는 서버를 가리킵니다.
- 메시지에 광고된 URL은 링크를 클릭할 때 사용자가 탐색하는 "실제" URL과 다릅니다.

이러한 세 가지 요소를 모두 컨텍스트에서 고려한다면 이는 합법적인 메시지가 아니라 사실상 스팸 공격이라는 것이 분명해집니다.

기존 "콘텐츠 필터"
찾을 콘텐츠 필터

무엇을? 메시지 콘텐츠가 정상입니다.

컨텍스트 적응형 스캐닝
CASE에서 발견한 내용

뭐?메시지 내용이 합법적입니다.
어떻게? 메시지 생성은 Microsoft를 에뮬레이트함 Outlook 클라이언트.
누구?
1) 발송되는 이메일의 양이 갑자기 급증함
2) 그 답례로 메일 서버는 메일을 받지 않습니다.
3) 우크라이나에 있는 메일 서버

어디?
1) 하루 전에 등록된 표시 및 대상 URL 웹 사이트
인이 일치하지 않습니다.
2) 소비자 광대역 네트워크에서 호스팅되는 웹 사
입니다.
3) "Whois" 데이터는 도메인 소유자를 알려진 스파
표시합니다.

판정:알 수 없음

판정:차단

CASE가 신종 바이러스 필터에서 사용되는 경우 별도로 조정된 데이터 집합에도 동일한 점수 및 기계 학습 기능이 적용됩니다.Virus Outbreak Filters는 Cisco가 제공하고 CASE 기술을 기반으로 하는 예방적 안티바이러스 솔루션입니다.Outbreak Filters 솔루션은 "실시간" Outbreak 규칙(Cisco Talos 특정 전파 확산에 의해 발급됨) 및 "상시 작동" 적응형 규칙(항상 CASE에 상주함)을 기준으로 메시지를 검사하여 사용자가 완전히 형성될 기회를 갖기 전에 보안 침해를 방지합니다.CASE를 사용하면 Virus Outbreak Filter에서 몇 가지 방법으로 바이러스 침입을 정확하게 탐지하고 차단할 수 있습니다.첫째, CASE는 첨부 파일의 파일 확장명, 파일 크기, 파일 이름, 파일 이름 키워드, 파일 매직(파일의 실제 확장명) 및 포함된 URL과 같은 매개변수를 기반으로 메시지를 신속하게 스캔할 수 있습니다.CASE 기술은 메시지를 이러한 수준의 세부 정보로 분석하므로 Cisco Talos는 오탐을 최소화하면서 보안 침해를 정확하게 차단하는 매우 세분화된 Outbreak Rules를 실행할 수 있습니다.CASE는 업데이트된 Outbreak Rules를 동적으로 수신하여 최신 전파 확산을 방지할 수 있습니다.

CASE 기술은 Outbreak Rules를 기반으로 메시지를 분석하는 것 외에도 적응형 규칙을 기반으로 메시지를 검사합니다.적응형 규칙은 감염되는 메시지에서 바이러스를 나타내는 악성 및 스푸핑 특성을 검사하는 정교한 휴리스틱 및 알고리즘입니다.Adaptive Rules는 이러한 매개 변수 외에도 SBVS(SenderBase Virus Score)를 기준으로 메시지에 점수를 부여합니다.SBVS는 SBRS(SenderBase Reputation Score)와 비슷하지만, 전송 당사자가 스팸이 아닌 바이러스 이메일을 보낼 가능성을 기준으로 순위를 매겼습니다.바이러스 이메일의 대부분은 이전에 감염된 "좀비" 머신에 의해 전송되므로, 이러한 전송 대상을 확인하고 점수를 매기는 것은 바이러스를 잡는 데 있어 필수적인 요소입니다.

Cisco Email Security의 CASE 기술을 사용하면 CASE는 여러 가지 방법으로 메시지를 검사하므로 Virus Outbreak Filter를 통해 기존 안티바이러스 솔루션보다 앞서 바이러스 침투를 방지할 수 있습니다.또한 메시지 첨부 파일, 메시지 내용, 메시지 생성의 다양한 특성을 분석할 수 있을 뿐만 아니라 발신자 평판을 기준으로 메시지를 분석할 수 있습니다.또한 CASE는 IronPort Anti-Spam 및 Reputation Filters 엔진으로도 작동하므로 이러한 모든 애플리케이션에 대해 메시지를 한 번만 검사하면 됩니다.

고성능, 저렴한 비용

CASE 기술의 이면에 있는 논리는 매우 정교할 수 있으므로 CPU가 매우 많이 사용됩니다.효율성을 극대화하기 위해 CASE는 고유한 "조기 종료" 기술을 사용합니다.조기 종료(Early exit)는 CASE에

서 처리하는 무수한 규칙의 효율성을 우선합니다.CASE 기술은 가장 큰 영향과 가장 낮은 비용으로 규칙을 실행합니다.통계 판정에 도달하면(양수 또는 음수) 추가 규칙이 실행되지 않으므로 시스템 리소스가 절약됩니다.이 접근 방식의 우아함은 각 규칙의 효율성을 잘 이해하고 있습니다.CASE는 효율성 변화에 따라 규칙 실행 순서를 자동으로 모니터링하고 조정합니다.

조기 종료의 결과는 CASE 기술이 기존 규칙 기반 필터보다 약 100% 더 빠르게 메시지를 처리한다는 것입니다.이는 대규모 ISP와 기업에 확실한 이점을 제공합니다.하지만 중소기업에도 혜택이 있습니다.CASE의 효율성과 Cisco Email Security의 AsyncOS 운영 체제의 효율성은 AsyncOS 및 CASE 기술을 갖춘 ESA를 매우 저렴한 하드웨어에서 구현하여 자본 비용을 절감할 수 있음을 의미합니다.

CASE 기술을 통해 관리 오버헤드를 없앰으로써 비용이 절감됩니다.CASE는 매일 수천 번씩 자동 조정되고 업데이트됩니다.Cisco Talos는 숙련된 다국어 기술자 및 통계학자를 제공합니다.Cisco Talos 분석가는 Cisco Email Security 고객의 네트워크 또는 글로벌 이메일 트래픽 패턴에서 탐지된 메일 흐름의 이상 징후를 강조하는 특수 툴을 갖추고 있습니다.Cisco Talos는 시스템에 자동으로 푸시되는 새 규칙을 실시간으로 생성합니다.Cisco Talos는 또한 CASE에서 사용하는 다양한 규칙을 학습하는 데 사용되는 "스팸 및 햄"의 방대한 양의 코퍼스를 유지 관리합니다.자동으로 업데이트되는 CASE 규칙은 관리자가 필터를 조정하고 조정하거나 스팸 격리를 통과하는 데 시간을 허비하지 않아도 된다는 것을 의미합니다.

요약

스팸, 바이러스, 악성코드, 스파이웨어, 서비스 거부 공격, 디렉토리 수집 공격은 모두 동일한 근본적인 동기(이익)에 의해 추진됩니다.이러한 이익은 상품 판매 또는 광고 또는 정보 도용을 통해 얻을 수 있습니다.이러한 판매 수익으로 인해 전문 엔지니어가 개발한 정교한 공격이 증가하고 있습니다.고급 이메일 보안 시스템은 이러한 위협에 대처하기 위해 가장 광범위한 상황에서 메시지를 분석해야 합니다.Cisco Email Security의 Context Adaptive Scanning Engine 기술은 다음과 같은 4가지 기본적인 질문을 합니다.누가, 어디서, 무엇을, 어떻게 - 혼합된 위협으로부터 합법적인 메시지를 차단합니다.

- "누가"는 메시지를 보낸 발신자의 이메일 평판입니다.
- "Where"는 웹 사이트를 호스팅하는 소스의 평판입니다. 링크가 어디로 이동할지 분석합니다.
- "무엇을"란 메시지 내용, 즉 메시지에 포함된 내용을 분석하는 것입니다(1세대 시스템은 "무엇을" 분석 유형에만 의존하는 경우가 많음).
- 마지막으로, "How"는 메시지가 구성되는 방식을 분석합니다.

누가, 어디서, 무엇을, 무엇을, 어떻게 분석하는가를 분석하는 기본 프레임워크는 바이러스 전파, 피싱 공격, 이메일 기반 스파이웨어 또는 기타 이메일 위협을 차단하는 것과 마찬가지로 스팸을 차단하는 데 효과적입니다.데이터 세트 및 분석 규칙 집합은 각 위협에 대해 특별히 조정됩니다.CASE 기술을 통해 Cisco ESA는 단일 고성능 엔진에서 이러한 위협을 처리함으로써 가능한 한 높은 효율성으로 가장 광범위한 위협을 차단할 수 있습니다.