White Paper

Cisco Outbreak Filters로 표적 공격과 제로데이 위협 탐지 및 예방

이메일을 통해 확산되는 바이러스 침투는 아주 심각한 결과를 초래할 수 있습니다. 한정된 IT 리소스로는 해결하기 어려울 수 있으며 전체 시스템이 순식간에 중지될 수 있습니다. IT 분야에서 바이러스에 관한 비유가 자주 쓰이는 데에는 이유가 있습니다. 국지적 유행이든 전 세계적 유행이든 상관없이 바이러스가 일단 시스템에 침투되면 급속히 확산되어 시스템을 중단시킬 수 있습니다.

바이러스 침투 현상이란?

매일 발생하는 이메일 기반 공격 중, 다음 기준에 해당하는 경우 바이러스 침투 현상이 발생한 것으로 간주할 수 있습니다.

1. 새로운 악의적인 공격 프로파일(또는 기존에 알려진 공격의 새로운 변종)
2. 중/대규모 피해의 가능성이 있는 경우
3. 확산 규모가 광범위한 경우(다양한 소스에서 여러 개의 인스턴스가 확인됨)

이메일 기반 공격이 위의 조건을 충족할 경우, Cisco TOC(Threat Operations Center)에서는 인시던트를 조사하고 바이러스 침투 규칙을 발표하여 고객을 보호합니다.

IT 바이러스 침투 현상에 의한 비용

IT 부문에서 바이러스 침투 문제가 발생해도 과거의 LoveBug 및 Melissa처럼 더 이상 뉴스 1면을 장식하지는 못하지만, 이러한 바이러스는 여전히 심각한 피해를 초래할 수 있으며 해결 비용도 지속적으로 증가하고 있습니다. 악성코드가 급격히 발전하고 제로데이 공격의 익스플로잇까지 가속화되면서 규모가 작은 일부 격리된 인시던트도 급속히 확산되는 바이러스 침투 현상으로 변모하고 있습니다.

- 10 Worst Computer Viruses of All Time
- 10 Most Destructive Computer Worms and Viruses Ever, 2010년 10월 12일
- 10 of the Most Costly Computer Viruses of All Time, 2012년 5월 29일

바이러스 침투 방어를 위한 모범 사례

IT 보안 상태가 강력하면 감염된 시스템과 확실히 구분되는 안전한 시스템을 구축할 수 있습니다. 바이러스 전문 조직에서는 바이러스 침투를 조사하면서 일반적으로 다음 단계를 포함하는 권장 절차를 개발해왔습니다.

1. 진단을 확인하고 바이러스 침투의 존재 여부를 파악합니다.
2. 침투 현상의 확산을 매핑합니다.
3. 제어 및 예방 시스템을 개발하고 구현합니다.

IT 표준 위원회에서도 이와 비슷한 방법을 권장하고 있습니다. 현재의 복잡하고 역동적인 위협 환경에서 기업 보안을 유지하려면 지속적인 경계를 취해야 하며, 알려진 위험 및 새로운 위험으로부터 네트워크, 데이터, 최종 사용자를 실시간으로 보호할 수 있는 지능형 컨텍스트 인식 보안 솔루션이 포함된 멀티레이어 방어 접근 방식이 필요합니다.

표적 공격은 현재 기업에서 당면하고 있는 주요 보안 문제 중 하나입니다. Cisco SIO(Security Intelligence Operations)에서는 APT(Advanced Persistent Threat), 스피어 피싱(표적 공격이라고도 함) 등 이처럼 탐지하기 어려운 공격이 점점 더 늘어나고 있으며 상호 연관된 영향도 커지고 있다는 점을 파악했습니다. Cisco의 최근 연구에 따르면 표적 공격으로 발생한 연간 전체 감염 비용은 12억 달러를 넘는 것으로 밝혀졌습니다.[1] 그러나 아직 대부분의 조직은 공격이 진행되는 동안에도 공격을 탐지하지 못하며 피해가 발생한 후에야 이를 알게 됩니다.

대다수 사이버 범죄자의 목표는 선호하는 공격 실행 방법에 상관없이 데이터를 탈취하여 본인이 직접 활용하거나 제3자에게 팔아넘겨 이익을 취하는 것입니다. 도난의 표적이 되는 데이터의 범위는 은행 인증서에서 지적 재산, 환자 건강 정보에 이르기까지 다양합니다. 또한, 기업에서 현재 생성, 저장 및 수집하고 있는 "빅 데이터"는 가치가 높은 정보의 보고라고 할 수 있으며 기업 범죄자들은 이러한 정보를 악성코드 및 표적 공격을 통해 장기간에 걸쳐 아무도 모르게 수집할 수 있습니다.

Cisco Email Security 기능 중 하나인 Cisco Outbreak Filters에서는 인바운드 및 아웃바운드 메시지의 위협을 평가합니다. 이러한 필터는 정교한 규칙 세트 및 동적 격리 기능을 활용하여 표적 이메일 공격을 확실하게 차단하는 업계 최초의 맞춤형 엔진입니다. 이 백서에서는 이러한 솔루션을 사용하여 이메일 기반 바이러스 침투를 방어하는 모범 사례를 알아봅니다.

실시간으로 위협 식별 및 차단

Cisco에서는 게이트웨이에서의 위협 방어 기능을 확장합니다. Cisco Outbreak Filters는 클라우드에서 Cisco SIO와 연동되어 Cisco Email Security를 통해 이메일 기반 위협을 식별하고 차단합니다.

이 시스템에서는 다양한 시그니처 기반 악성코드 차단 스캔 엔진 및 휴리스틱 탐지 엔진을 사용하여 모든 인바운드 및 아웃바운드 웹 트래픽에 신종 및 알려진 웹 악성코드가 있는지 실시간으로 스캔합니다. 기존의 시그니처 기반 안티바이러스와는 확연히 다른 이러한 인텔리전스는 AI(인공 지능)를 기반으로 하며, 하루에 확인하는 수십억 개의 웹 요청을 활용하여 어떤 트래픽이 "정상"이고 "악성"인지 파악합니다. 이러한 인텔리전스 기능을 사용하면 시그니처 업데이트를 기다릴 필요없이 악성코드를 차단할 수 있으며, 제로데이 위협이 발생할 가능성을 효과적으로 차단할 수 있습니다.

[1] "Email Attacks: This Time It's Personal", Cisco, 2011: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf

그림 1. 제로데이 악성코드 아키텍처

그림 1에 나와 있듯이, 최종 사용자가 웹 페이지를 방문하면 이 페이지의 구조는 Cisco SIO의 인텔리전스 시스템에 의해 HTML, 스크립트, Flash, PDF와 같은 페이지의 구성 요소로 분리됩니다. 모든 웹 콘텐츠가 여러 안티바이러스 엔진을 통과하여 알려진 위협이 제거되면 제로데이 위협을 식별하고 차단하기 위해 이 "안전한" 트래픽을 다시 한 번 실시간으로 분석합니다. 이 시스템에서는 제로데이 악성코드를 정확하게 탐지하기 위해 개발된 세 가지 기술인 심층 콘텐츠 분석, 체계적인 콘텐츠 조사, 가상 스크립트 에뮬레이션과 "scanlet"을 함께 사용하여 각 콘텐츠의 세부 요소를 스캔합니다.

- **심층 콘텐츠 분석에서는** 콘텐츠를 검사하여 악의성 유무를 식별합니다. 이러한 프로세스에서는 AI 학습을 통해 정확성이 유지하고 있는 알려진 "정상" 통계 모델과 콘텐츠를 비교하는 작업을 수행합니다. 예를 들어, 애니메이션 GIF에 프레임이 1개밖에 없는지, 이미지 파일에 실행 코드 또는 기타 비정상적인 콘텐츠가 포함되어 있는지 등을 비교합니다.
- **체계적인 콘텐츠 조사에서는** 콘텐츠의 구조를 검사하여 잠재 위험의 징후를 다시 확인합니다. 예를 들어, Cisco SIO에서 분석한 콘텐츠를 토대로 새로운 난독 실행 파일이 악성 파일일 가능성이 95%인 것으로 확인될 수 있습니다. 이러한 확인 결과는 다양한 종류의 scanlet(예: 평판 scanlet 및 Flash, Java, PDF, 아카이브, 실행 파일, 파일 이상 현상 등에 사용되는 Scanlet)을 사용하여 페이지 콘텐츠를 스캔하는 과정을 통해 얻게 됩니다. 이러한 scanlet은 높은 성능을 유지하면서 실행됩니다.
- **가상 스크립트 에뮬레이션은** 스크립트와 같은 동적 웹 콘텐츠를 검사하는 작업에 특히 중요합니다. Cisco Outbreak Filters의 클라우드 인프라에서 스크립트를 실행하면 숨겨진 리디렉션 또는 컴퓨터에서 사용자 설정을 편집하려고 시도하는 "드라이브바이" 다운로드와 같은 악의적인 움직임을 모니터링할 수 있습니다. 악의적인 움직임이 탐지되면 해당 스크립트는 차단되고 최종 사용자에게 전달되지 않습니다.

Cisco Outbreak Filters: 표적 공격에 한발 앞서 대비

스팸이 감소하는 추세를 보인 후 표적 이메일 공격이 점점 더 확산되고 있습니다. Cisco SIO에 따르면 2010년 8월부터 2011년 11월 사이에 하루 3,790억 개 이상이었던 스팸 메시지가 약 1,240억 개로 줄어든 것으로 나타났으며, 이러한 감소세는 2007년 이래로 유례가 없었습니다.[2] 이러한 감소 현상의 한 가지 중요한 원인은 Bredolab 및 Rustock과 같은 주요 봇넷이 와해되었기 때문입니다.

그러나 이러한 최대 규모의 봇넷 일부가 폐쇄되기 전부터 많은 사이버 범죄자들은 대량 스팸을 발송하는 대신 표적 공격을 개발하고 실행하는 데 더 많은 리소스를 할애하기 시작했습니다. 그 이유는 표적 사기의 경우 수법이 통하리라 예상되는 수신자로부터 한 번의 응답만 받으면 되지만 대량 스팸을 발송할 경우에는 더 많은 응답률이 요구되기 때문입니다. 표적 공격은 기본적으로 이메일을 통해 실행되며 그 비율이 전 세계 조직에 발송되는 인바운드 스팸 메시지 중 1%도 되지 않지만, 스팸에 대한 인지도가 높은 사용자조차도 이러한 사기성 공격의 피해자가 될 수 있을 정도로 매우 효과적입니다.

표적 공격은 다음과 같이 분류됩니다.

- **APT(Advanced Persistent Threat):** 이러한 메시지는 장기간에 걸쳐 조직의 네트워크로 침투하려고 시도하는 광범위한 공격에 포함되어 전송됩니다.
- **스피어 피싱 및 웨일링(whaling):** 이러한 메시지는 금전 또는 정보를 빼내려는 목적으로 특정 개인을 표적 대상으로 합니다. 일례로 조직의 은행 정보를 빼내는 소프트웨어를 설치하기 위해 기업의 재무 부서를 대상으로 한 표적 공격을 들 수 있습니다.

표적 공격의 경우 기업 웹 사이트 및 Facebook, LinkedIn 등의 소셜 네트워킹 사이트에서 쉽게 확보할 수 있는 데이터를 사용합니다. 공격자는 도시 이름 또는 대상자의 이름을 포함하거나 친구 또는 회사 동료가 보낸 이메일인 것처럼 조작하여 공격이 성공할 가능성을 높입니다. 이들은 보안 사슬의 연결 취약점이 일반적인 최종 사용자라는 점을 알고 있으며, 소셜 엔지니어링을 통해 가장 많은 결과를 얻을 수 있다는 점도 알고 있습니다.

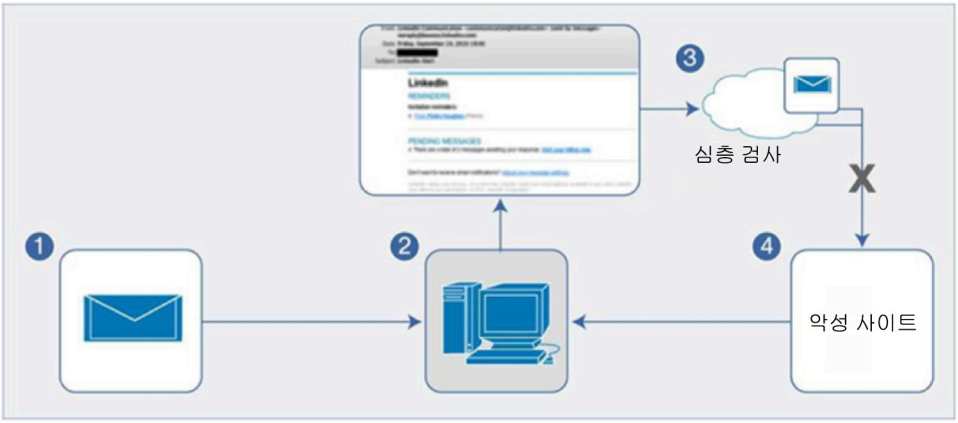
Cisco Outbreak Filters는 다음을 통해 기업이 표적 공격을 탐지하고 예방할 수 있도록 지원합니다.

- **고급 규칙 세트:** Cisco SIO 위협 연구원들은 광범위한 표적 공격 휴리스틱을 관리하는 업무를 담당하고 있습니다. 이들은 세계 최대의 실시간 표적 공격 집단을 찾아내고, 이를 연구하여 중요한 패턴 및 공통적인 특징을 파악했습니다. Cisco에서는 이를 토대로 신종 위협을 한 번에 더욱 잘 식별하도록 지원하는 규칙을 만들고 개선합니다. 표적 공격 휴리스틱의 경우 Cisco SenderBase에서 제공된 인텔리전스를 보안 어플라이언스 및 알려진 공격에서 파생된 콘텐츠와 결합합니다. 이 인텔리전스는 URL, 헤더, 메시지 본문과 같은 각 메시지의 다양한 요소를 평가하여 메시지 내의 위협을 식별하는 데 사용됩니다. 이러한 휴리스틱은 다른 Cisco Outbreak Filters 규칙과 연동하여 제공된 메시지가 표적 공격인지를 확인합니다.
- **Dynamic Quarantine:** Cisco에서는 Dynamic Quarantine을 활용하여 의심스러운 메시지를 즉시 격리합니다. 격리된 메시지는 Cisco Outbreak Filters에서 지속적으로 다시 평가됩니다.

[2] Cisco 2011 Annual Security Report, Cisco, 2011: http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf.

- **SIO 활용:** 클라우드를 통해 Cisco SIO를 활용하여 이메일의 의심스러운 링크를 재작성하면 해당 링크가 클라우드 기반 시스템에 연결되어 심층적인 검사와 분석을 수행할 수 있습니다. (예: http://www.threatlink.com이 http://secure-web.cisco.com/auth=X& URL=www.threatlink.com) 사용자가 링크를 클릭하면 Cisco의 가상 환경을 통해 동적 웹 콘텐츠가 실행되며 악성 데이터의 존재 여부를 확인하는 스캔이 이루어집니다. 이 서비스는 웹 페이지에 포함된 콘텐츠의 모든 세부 요소(이미지, 파일, 스크립트, 난독 코드 등)를 분석하는 수많은 콘텐츠 분석 scanlet으로 구성되어 있습니다. 모든 콘텐츠는 악성코드 존재 여부를 확인하기 위해 구조 및 동작 분석을 거칩니다. 악성코드가 확인되면 감염된 콘텐츠의 특정 요소는 차단되지만 안전한 콘텐츠는 최종 사용자에게 전달됩니다. Cisco Outbreak Filter 스캔에 연결되도록 URL을 재작성하면 사용자가 링크로 이동하는 데 사용하는 디바이스가 랩톱, 스마트폰, 태블릿 중 무엇이든지 간에 상관없이 사용자를 보호할 수 있습니다.

그림 2. Cisco Outbreak Intelligence를 사용하는 Cisco Outbreak Filters의 간단한 흐름



Cisco Outbreak Filters의 기본적인 프로세스는 그림 2에 나와 있습니다.

1. Cisco Outbreak Filters에서 수신 이메일을 스캔합니다. 정교한 규칙 세트에서는 이를 잠재적인 피싱 또는 표적 공격 이메일로 식별하며 어플라이언스에서 구성된 것으로 처리합니다. 기본적으로 해당 이메일이 피싱임을 나타내는 고지 문구가 이메일 텍스트 앞에 추가되며 이메일에 포함된 URL이 다시 작성됩니다.
2. 다시 작성된 URL이 포함된 이메일이 사용자의 받은 편지함에 전달됩니다.
3. 이메일을 열면 다시 작성된 이 이메일 링크에서 사용자를 공용 프록시로 보냅니다. 해당 프록시에서는 웹 페이지 콘텐츠가 인터셉트되고 클라우드에서 실시간으로 스캔이 이루어집니다.
4. 페이지에서 악성코드가 탐지된 경우, 차단된 페이지 메시지가 사용자에게 표시되며 URL에 대한 정보는 Cisco Outbreak Filters 시스템에서 Cisco SIO로 다시 전달됩니다. 또는 사용자가 (1) 프록시를 통해 페이지를 둘러보거나 (2) 사이트로 바로 이동하도록 선택할 수 있습니다.

Outbreak Filters에서 탐지하는 항목

Cisco Outbreak Filters는 악성코드, 피싱, 사기, 바이러스 감염 이메일이라는 네 가지 카테고리로 구성되며 일반적으로 사용되는 20개 이상의 다양한 사기 유형을 탐지합니다. 다음 목록에는 Cisco Outbreak Filters에서 탐지할 수 있는 몇 가지 공격 유형이 나와 있습니다.

- 피싱
- 자선단체 빙자 스팸
- 해외 도난 사기
- 세미나 빙자 스팸
- 유산 상속 스팸
- 금융 URL
- 은행 이체
- 위조 자기앞수표
- 자금 운반책
- 대출
- 금융 관련 전화
- 위조 거래

이러한 공격 유형 목록은 유동적으로 변경되어 사이버 범죄자가 사용자로 하여금 URL 및/또는 첨부 파일을 열어보도록 유도하기 위해 사용하는 최신 수법 동향에 관한 정보를 지속적으로 제공합니다.

사전 대응 멀티레이어 보안 접근 방법

새로운 위협은 빠른 속도로 꾸준히 나타나고 있으며, 매달 수천 가지의 새로운 악성코드 유형이 탐지되고 있습니다. 공격은 더욱 표적화되고 있으며 다양한 악성코드 변종을 활용하므로, 악성코드 차단 공급업체가 모든 신종 악성코드 샘플을 확보하여 시그니처를 개발할 가능성은 점점 희박해지고 있습니다. 이메일 기반 위협은 소량으로 발송되는 데다가 확인 또는 분류되지 않은 맞춤형 URL이 포함되어 있으므로 탐지하기가 더욱 어렵습니다. 이러한 추세로 인해 기업은 네트워크, 데이터 및 최종 사용자의 보안을 유지하는 데 더욱 사전 대응적인 멀티레이어 접근법을 취하는 것이 중요해졌습니다.

Cisco Outbreak Filters는 기업에서 이메일 또는 웹을 통해 전달되는 위협을 차단할 수 있도록 지원하기 위해 설계되었습니다. Cisco에서는 상호 연계된 다양한 탐지 기술, 자동 시스템 학습 휴리스틱, 업계 최대의 웹 데이터 세트를 함께 사용하여 신종 및 알려진 웹 악성코드에 대처할 수 있는 가장 효과적인 솔루션을 제공합니다. 이 시스템에서는 테라바이트 단위의 웹 코드를 매일 분석하며, 2004년부터 독점적인 웹 데이터 세트를 컴파일하는 작업을 수행해오고 있습니다. Cisco Outbreak Filters에서는 의심스러운 이메일 메시지를 동적으로 격리하며, Cisco Outbreak Intelligence를 사용하여 URL의 안전성을 확인함으로써 표적 공격을 차단합니다.

Cisco Outbreak Filters는 세계 최대의 클라우드 기반 보안 에코시스템인 Cisco SIO에 연결되어 있으며, Cisco SIO에서는 조기 경고 인텔리전스, 위협 및 취약점 분석, 검증된 Cisco 위협 완화 솔루션을 제공하여 오늘날의 가장 정교한 위협으로부터 네트워크를 보호할 수 있도록 지원합니다.

왜 Cisco인가?

네트워크에 있어서 보안은 그 어느 때보다도 중요합니다. 위협과 위험이 상존하고 기밀 유지와 제어의 문제가 우려되는 상황에서 사업의 연속성을 제공하고 가치있는 정보를 보호하며 브랜드 명성을 유지하고 새로운 기술을 채택하려면 보안이 필수입니다. 안전한 네트워크에서는 직원들이 이동 중에도 적절한 정보에 안전하게 연결할 수 있습니다. 또한 고객과 파트너가 회사와 더 편리하게 사업을 수행할 수 있습니다.

Cisco만큼 네트워크 보안을 잘 아는 조직은 어디에도 없습니다. 시장을 이끄는 리더십, 위협으로부터의 최상의 보호 및 예방, 혁신적인 제품 및 긴 수명으로 인정받는 Cisco는 귀사의 보안 요구에 꼭 필요한 공급업체입니다.

추가 정보

Cisco Outbreak Intelligence 또는 Cisco Outbreak Filters를 전사 보안 전략의 구성 요소로 사용했을 때 얻을 수 있는 혜택이 무엇인지 알아보려면 Cisco Email Security의 Try Before You Buy 프로그램에 참여하는 것이 가장 좋습니다. 회사 네트워크에서 무료로 30일간 시험해볼 수 있도록 완전한 기능을 갖춘 평가 어플라이언스를 받으려면 http://www.cisco.com/go/emailsecurity를 방문하십시오.

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Printed in USA C11-727467-02 11/13