표적 피싱

이메일은 대부분의 조직에서 커뮤니케이션에 사용하는 매체가 되었습니다. 안타깝게도 수신 이메일의 대부분은 원치 않은 것이고, 심지어 악성 이메일입니다. 최신 스팸 차단 어플라이언스는 일반적인 스팸 캠페인의 대부분을 걸러내 적법한 이메일만 최종 사용자의 받은 편지함으로 보냅니다. 한편 MAAWG(Messaging Anti-Abuse Working Group)의 조사에 따르면, 스팸 또는 불쾌한 메시지가 수신 메일의 87% 이상을 차지합니다.

온라인 범죄자는 고급 안티 스팸 기술을 피하기 위해 더 위험하고 정교한 수법을 구사하고 있습니다. 스팸 수신자를 의심스러운 제품 구매로 유인할 뿐 아니라 수익 추구형 피싱 공격은 사용자의 개인 정보(이름, 주소 등)와 은행의 로그인 정보까지 수집하려 합니다. 그러한 피싱 이메일의 전송량은 상대적으로 적지만 계속 증가하고 있으며, 표적이 된 피해자는 심각한 위험에 처하게 됩니다. 인터넷 사용자가 서투른 개인 정보 피싱 시도를 정확하게 탐지함에 따라 스팸 발송자들은 더 작은 집단을 대상으로, 특정 그룹에 어필하는 콘텐츠를 내세워 선택적 피싱 공격에 나서고 있습니다. 이와 같이 고도로 표적화된 사회 공학적 이메일 유형을 표적 피싱 또는 "스피어 피싱"이라고 하며, 수준 높은 인터넷 사용자도 여기에 속곤 합니다.

트렌드 및 해결책

1990년대 말부터 피싱 이메일(수신자를 속여 로그인 이름, 비밀번호와 같은 개인 정보를 공개하도록 설계된 메시지)이 받은 편지함에 쏟아져 들어오기 시작했습니다. 유명 온라인 서비스 또는 합법적인 기업에서 보낸 메시지로 위장한 이메일을 만드는 온라인 범죄자, 즉 피셔는 대개 수신자 중 극히 일부에서라도 온라인 뱅킹 또는 기타 로그인 이름/비밀번호를 훔쳐내겠다는 기대 하에 한 번에 수백 통의 이메일을 보냅니다.

현재의 트렌드는 계속되지만 피셔는 더욱 더 교묘해지고 있습니다. 이메일은 올바른 회사 로고를 명시하고 맞춤법과 문법을 따르는 매체이며, 표적 기관을 모방하는 웹 사이트로 연결하는 URL을 사용하는 경우도 있습니다.

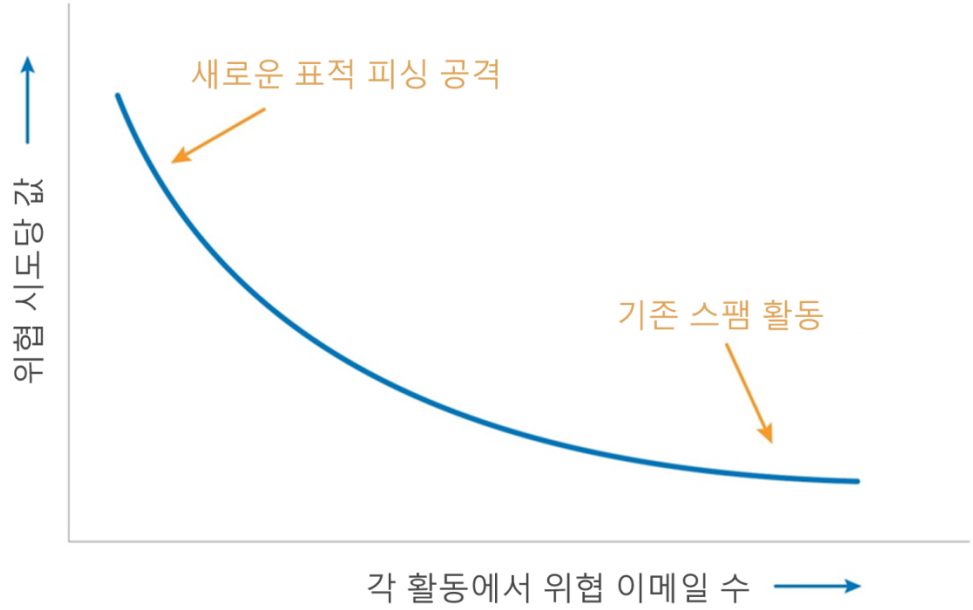
표적 피싱의 증가와 보상

이메일 기반 공격에서 표적 피싱 공격의 비중이 늘고 있습니다. 이는 특정 조직이나 그룹을 표적으로 삼는 것입니다. 표적은 더 수준 높은 개인 데이터, 이를테면 로그인 및 비밀번호 정보를 얻기 위해 정교하게 짜인 피싱 메시지를 받습니다. 그 정보를 통해 기업 네트워크 또는 민감한 정보의 데이터베이스에 액세스할 수 있습니다. 표적 피싱 이메일은 로그인 정보를 입수할 뿐 아니라 악성코드(예: 키스트로크 로깅 프로그램)를 유포하여 피해자가 입력하는 모든 정보를 추적할 수도 있습니다.

온라인 범죄자의 입장에서 표적 피싱은 기존 피싱 캠페인에 비해 많은 시간과 비용을 투자해야 합니다. 이 스캐머는 표적이 된 조직 또는 그룹의 유효한 이메일 주소를 대여하거나 훔쳐내고 수신자를 유도하여 개인 데이터를 얻어낼 만한 설득력 있는 이메일을 작성해야 합니다. 하지만 표적 피싱이 성공하면 더 큰 보상으로 이어질 수 있으므로 투자할 만한 가치가 있습니다.

현재 표적 피싱 메시지는 전체 피싱 캠페인의 약 1%를 차지합니다. 그러나 표적 피싱은 대개 조직 내 소수 정예를 대상으로 하므로 재무, 데이터 보안, 고객 관계 측면에서 막대한 피해로 이어질 수 있습니다. 게다가 개별 맞춤형 표적 피싱은 일반 안티피싱 기술로는 찾아내기가 어려워 해당 기업이 취약한 상태로 방치됩니다.

그림 1. 기존 스팸 캠페인은 대량 발송되며 예상 클릭률과 수익 전환율이 낮습니다. 신종 표적 공격은 근본적으로 더 위험하며 기존 스팸 필터를 통과하기 위해 소규모로 진행됩니다.



표적 피싱이 효과적인 이유

피해자가 웹 사이트를 클릭하여 부지불식간에 민감한 정보를 스캐머에게 전송하거나 자신의 컴퓨터에 악성 코드를 다운로드하도록 유도하는 기술은 더욱 정교해지고 있습니다. 대부분의 스팸이 URL을 포함하여 수신자를 악성 웹 사이트로 연결합니다. 요즘에는 피해자가 연결되는 가짜 웹 사이트가 합법적 사이트와 놀랄 만큼 유사한 디자인인 경우가 많습니다.

University of California Berkeley 조사에 따르면, 오랫동안 자주 인터넷을 사용했더라도 악성 웹 사이트에 속을 때가 있습니다. 사용자가 피싱 웹 사이트에 넘어가지 않으려면 연결되는 모든 웹 사이트에서 콘텐츠의 적법성, 주소 표시줄과 그 보안 설정, 브라우저 프레임의 자물쇠 이미지, 보안 인증서를 지속적으로 점검하는 전략을 세워야 합니다.

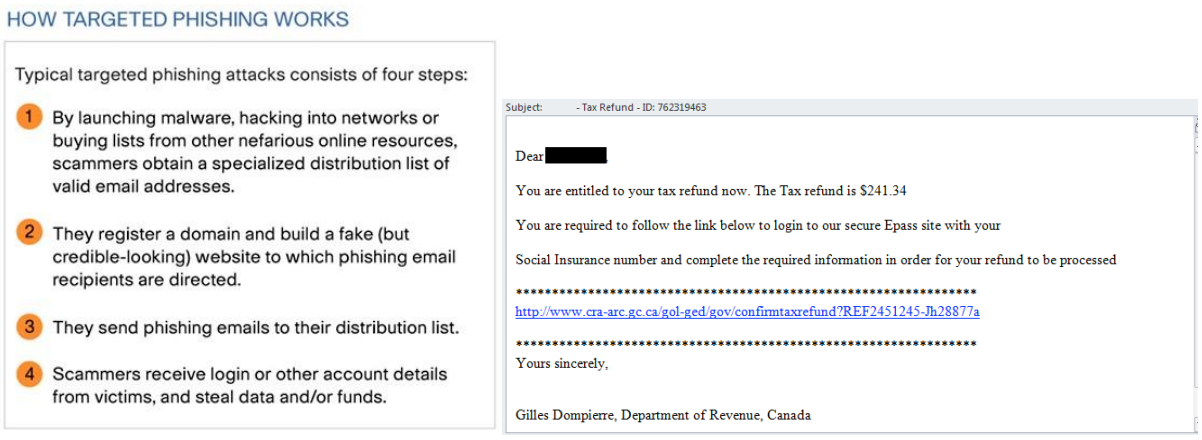
현재 광범위한 배포 목록을 대상으로 하는 피싱 이메일은 사회 공학적 수법에 의존합니다. 이를테면 (가짜 온라인 뱅킹 사이트처럼) 수신자의 조치를 요구하거나 적법한 곳으로 보이는 웹 사이트로 연결하는 콘텐츠를 사용합니다. 하지만 이러한 이메일 유형은 메시지 내에서 개인 데이터를 거의 사용하지 않습니다.

반면에 표적 피싱 이메일 발신자는 표적을 연구하여 새로운 차원의 사회 공학 기술을 구사합니다. 스캐머는 수신자의 이름을 명시하고 그 이메일 주소에 곧바로 메시지를 보내고 관련 콘텐츠를 작성하여 악성 이메일 및 피해자를 연결할 가짜 웹 사이트에 대한 신뢰도를 높입니다.

그림 2에 표시된 다음 예에서 기업의 임원들은 캐나다 세무국을 위장하여 환급 처리를 위해 Epass에 로그인한 후 양식을 작성하도록 요청하는 피싱 이메일을 받았습니다.

이메일의 URL을 클릭하면 Trojan 파일이 실행됩니다. 그리고 수신자의 이메일 브라우저에서 보낸 모든 대화형 데이터를 훔치고, SSL 암호화 이전에 위조 양식 데이터에 액세스할 수 있습니다. 또한 전자 이체된 결제 금액이 수신되지 않았으므로 수신자에게 특정 은행 계좌로 결제 금액을 다시 송신하도록 지시하는 다른 표적 피싱 이메일을 받았습니다.

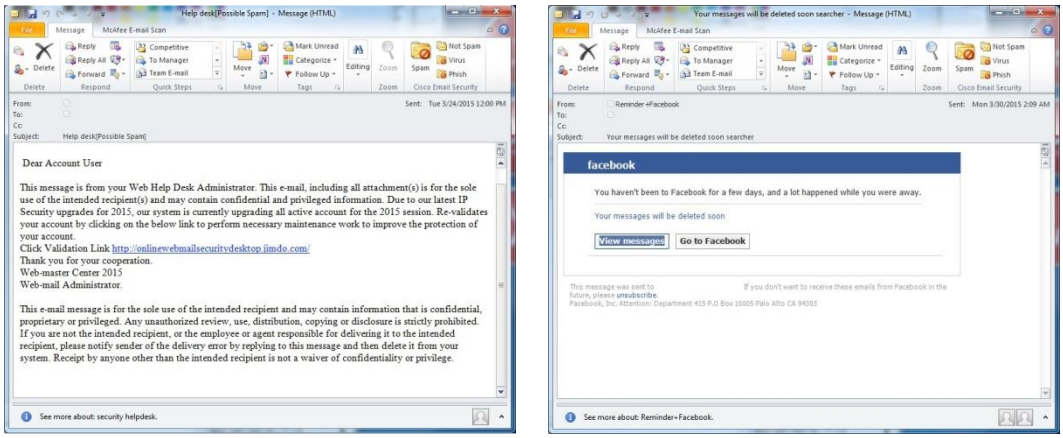
그림 2. 표적 피싱 공격에서는 범죄자가 효율적으로 적정 리소스를 구축하고 피해자가 귀중한 개인 정보를 공개하게끔 유인해야 합니다.



사회 공학적 성공 전술

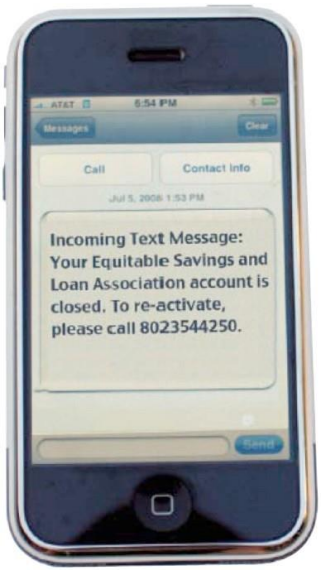
표적 피싱 공격은 기업의 임원만을 대상으로 하지 않습니다. 최근에는 Apple 또는 Facebook에서 고객에게 보낸 이메일로 위장하면서 계정을 검토하거나 특별 메시지 수신을 위해 본인의 계정으로 로그인하도록 요구합니다(그림 3 참조). 대학의 IT 부서에서 보낸 것처럼 보이는 또 다른 표적 공격에서는 이메일 사용자에게 웹 메일 자격 증명을 사용하여 회신해야 대학 이메일 계정을 유지하거나 보안 업그레이드를 받을 수 있다고 속였습니다. 이렇게 공격당한 계정은 대개 대규모 스팸 활동에 사용되곤 합니다.

그림 3. 계정 및 이메일 자격 증명 수집을 위해 Facebook 및 대학 IT 부서에서 보낸 것처럼 위장한 표적 피싱 메시지의 예



표적 피싱을 보내는 스캐머는 가짜 또는 감염된 웹 사이트로 피해자를 유인하기 위해 전술을 더욱 발전시킵니다. 온라인 범죄자가 휴대폰에 문자 메시지를 보낸 경우도 있습니다(그림 4). 한 지역 은행과 동일한 지역의 휴대 전화를 표적으로 한 공격에서는 고객의 계좌가 의심스러운 활동 때문에 폐쇄되었다고 알리면서 계좌를 다시 활성화하려면 어떤 전화 번호로 전화를 걸도록 지시했습니다. 이 번호는 스캐머가 계좌 번호와 로그인 자격 증명을 수집하기 위해 개설한 것이었습니다.

그림 4. 범죄자들은 자동화된 시스템을 구축하고 의심하지 않는 고객으로부터 은행 로그인 정보를 수집하기도 했습니다.



표적 피싱 공격이 어떤 식으로 침투하든 그 목적은 개인 데이터를 확보하여 돈 또는 정보를 노린 온라인 범죄에 이용하는 것입니다. 2015년에 표적 피싱 활동을 성공적으로 보낸 발신인들이 세계에서 가장 강력한 행정부 중 하나인 미국 백악관 사이트 중 하나를 스캠하여 기밀 정보를 누설했습니다.

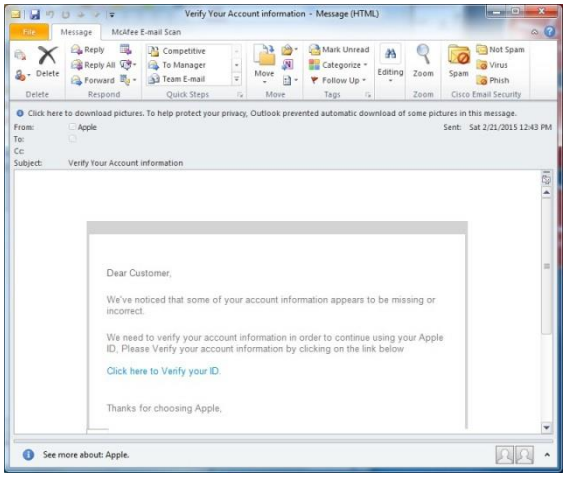
백악관의 경우 온라인 스캐머들은 아메리카 지역의 외무부에 해당하는 미국의 국무부에서 부정한 방식으로 이메일 계정 정보를 획득했습니다. 범죄자들은 DOS의 직원으로 가장하여 개별 백악관 직원에게 링크를 클릭하도록 요청하는 이메일을 보냈습니다. 하지만 링크를 클릭하면 시스템이 손상됩니다.

다행히 공격자들은 미국 대통령 일정 등이 들어 있는 기밀이 아닌 시스템에만 액세스했습니다. 백악관에서는 정보를 기밀 시스템과 기밀이 아닌 시스템으로 구분하여 보관하는 보안 전략을 수립하고 있습니다. 이 전략에서는 사용자가 정보에 액세스할 경우 결국에는 정보가 훼손된다고 가정하는 실용적인 데이터 보안 방식을 제안하고 있습니다.

최근에 발생한 또 다른 피싱 활동 역시 이러한 메시지와 연관된 위협이었으며, 범죄자들이 은행 거래 정보 이상의 것을 원한다는 사실을 입증합니다. 활동이 포함된 이메일이 주요 의료 사업자인 Anthem Blue Cross and Blue Shield의 8,000만 현재 고객과 이전 고객에게 전송되었습니다. 이러한 이메일에서는 Anthem을 대표하는 것처럼 위장하고 고객의 정보가 해킹되었다고 언급했습니다. 그런 다음 신용 상태를 무료로 모니터링하기 위한 링크를 제공했습니다. Anthem에서는 8,000만 고객 모두에게 이메일을 보내 이 피싱에 대해 경고해야 했습니다. Apple iTunes 고객에게 계정 확인을 요청한 활동(그림 5)도 있었습니다.

그 요구대로 하면 iTunes 계정 정보가 스캐머에게 유출될 뿐 아니라 피해자의 계정에 허위로 청구되었습니다.

그림 5. iTunes 계정과 관련된 것처럼 보이는 메시지가 피해자로 하여금 로그인 정보를 제공하게 유도합니다.



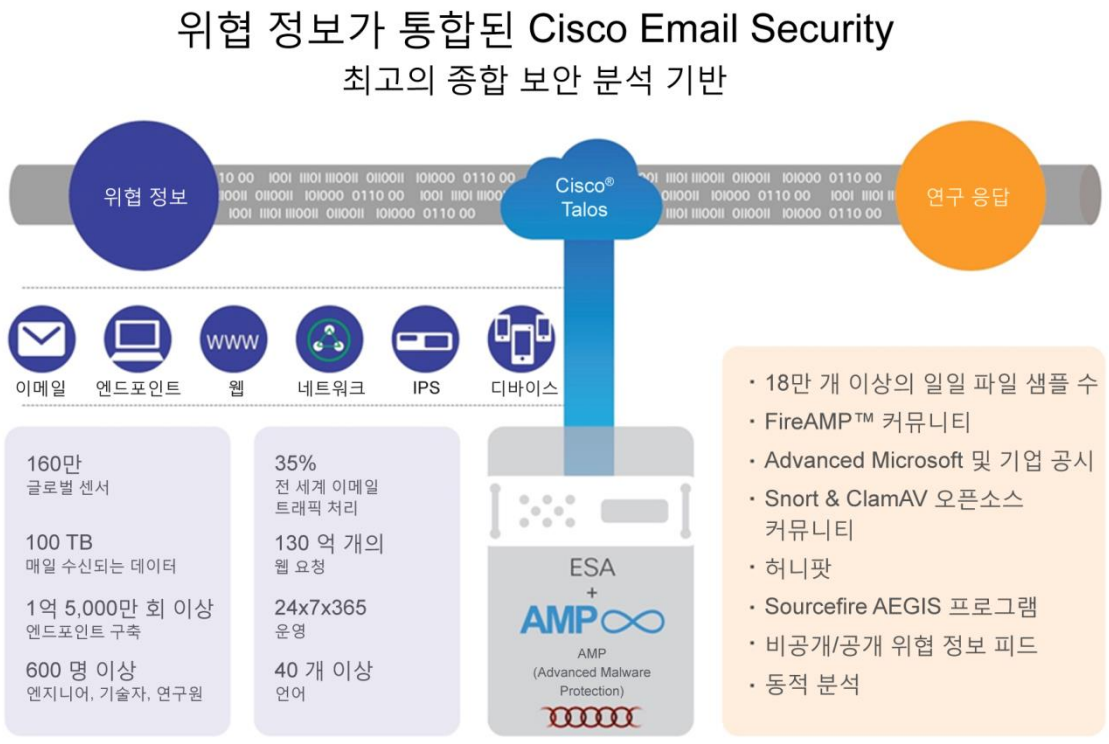
수신자가 피싱 이메일에 속지 않더라도 표적 피싱 공격은 기업 및 고객 관계에 악영향을 미칩니다. Forrester Research에 따르면, 표적 피싱 메시지를 받은 임원들은 이메일을 신뢰하지 않게 됩니다. Phishing Concerns Impact Consumer Online Financial Behavior 보고서에서 Forrester는 미국 소비자의 26%는 온라인 금융 상품을 이용하지 않으며, 20%는 거래하는 금융 기관의 이메일을 열어보거나 온라인 뱅킹 또는 결제 서비스에 가입하지 않는다고 밝혔습니다.

Cisco에서 표적 피싱을 막아내는 방법

Cisco에서는 더욱 확장되는 고급 기술의 모음을 통해 최종 사용자가 현재 보고 있는 이메일이 계정 정보를 얻기 위한 불법적인 이메일인지 판단하는 부담에서 벗어나게 합니다. Cisco® 솔루션 고객은 안전하게 이메일과 웹을 사용할 수 있으며, 표적 피싱과 같은 새로운 공격 유형으로부터 보호받습니다. Cisco에서는 멀티레이어 방식을 통해 전 세계의 이메일 및 웹 트래픽을 모니터링하고 고급 웹 평판 필터 및 이메일 인증 기술을 활용합니다.

SenderBase: Cisco SenderBase® 네트워크는 전 세계 이메일 및 웹 트래픽의 35%를 지속적으로 모니터링합니다. SenderBase는 200여 종의 매개변수, 이를테면 이메일 발신 및 웹 사이트 트래픽 볼륨, 불만 수준, spam-trap 계정, DNS(Domain Name System) 확인, 출처 국가, 블랙리스트 유무 등을 추적합니다. 그런 다음 수집된 데이터를 토대로 평판 점수를 산정하여 각 수신 이메일 메시지 및 여기에 포함된 URL의 위협 수준을 나타냅니다. 악성 이메일의 90%가 URL을 포함하고 있으므로, 웹 및 이메일 트래픽을 모두 모니터링하는 SenderBase의 특별한 기능은 Cisco에서 효과적으로 표적 피싱 공격을 식별하고 차단하는 데 핵심적인 역할을 합니다.

그림 6. 이메일 이상의 것을 포함하는 Cisco 제품 포트폴리오 및 보안 인텔리전스. 이메일 및 웹 보안, 방화벽, IPS(Intrusion Prevention System), 엔드포인트를 비롯하여 보안을 효과적으로 제공하는 데 필요한 위협 관련 정보와 통찰력을 얻습니다.



Cisco Web Reputation Filter: Cisco Web Reputation Filter는 각 URL이 악성 콘텐츠를 호스팅할 가능성에 따라 모든 이메일의 URL에 웹 평판 점수를 부여합니다. 그러면 Cisco 이메일 및 웹 보안 어플라이언스가 이 평판 점수를 토대로 특정 발신자의 이메일과 특정 웹 사이트의 트래픽을 허용하거나 플래그를 지정하거나 차단합니다.

평판 점수는 SenderBase 데이터와 스푸핑하기 어려운 IP 주소 데이터에 대한 추가 분석 결과를 토대로 합니다. 이를테면 도메인 이름이 등록된 지 얼마나 되었는지, 사이트가 어떤 국가에서 호스팅되었고, 어떤 도메인이 실제로 Fortune 500대 기업에서 호스팅되고, 얼마나 자주 변경되는지 확인합니다.

Cisco Anti-Spam: Cisco Anti-Spam 엔진에서는 URL의 평판 구성 요소를 활용하여 메시지 처리에 관한 결정을 내립니다. 평판이 나쁜 URL은 스팸 판정 임계값에 대한 메시지 점수가 높아서, 스팸 또는 스팸 의심 태그가 지정됩니다.

Cisco Outbreak Filters: 이러한 필터에서는 표적 규칙, URL 평판 및 분석을 사용하여 피싱, 해외 도난, 자금 운반책, 419 등과 같은 약 20가지의 위협을 식별합니다. 관리자는 Outbreak Filters를 사용하여 메시지에 대한 경고를 미리 작성하고 클라우드에서 클릭 시간에 분석하기 위해 의심스러운 URL을 전달되기 이전에 다시 작성함으로써 피싱 사이트, 새로운 위협, 알려지지 않은 위협(예: 감염된 파일 다운로드 또는 드라이브 바이 악성코드 사이트)을 차단할 수 있습니다.

Cisco AMP(Advanced Malware Protection): Cisco AMP에서는 파일 평판, 샌드박싱 및 회귀 분석을 함께 사용하여 악성코드를 차단하고 악의적인 이메일 첨부 파일로부터 사용자를 보호합니다. Cisco AMP는 파일이 ESA를 통과할 때 조직을 보호하는 것 이상의 작업을 수행합니다. 파일 회귀 분석에서는 파일이 조직에 도착한 이후에 파일의 속성이 변경될 경우 업데이트된 정보를 제공합니다. 이 고유한 기능은 샌드박싱을 통해 실제 의도를 숨기려고 시도하는 악의적인 파일로부터 보호합니다.

SPF, DKIM 및 DMARC 이메일 확인: 고급 이메일 인증 기술을 통해 발신자 신원에 대한 주장이 정확한지 판단합니다. SPF(Sender Policy Framework)와 DKIM(DomainKeys Identified Mail)은 널리 사용되는 보완적 이메일 인증 방식으로서 사기 이메일을 탐지할 수 있습니다. DMARC(Domain- Based Message Authentication, Reporting, and Conformance)에서는 이러한 방식을 상호 연계하는 추가적인 로직을 제공합니다. 이 인증 기술은 현재 산업 그룹, 이메일 서비스 업체, 대기업을 중심으로 보급되고 있으며, 그 사용자 기반이 확대되면서 더욱 효과적으로 피싱 이메일을 차단하고 있습니다.

<table>
<tr><td>SPF는 발신자 경로 인증 형태 중 하나로서 수신자가 인증된 메일 서버가 특정 도메인에 해당되는지 확인하고 수신된 이메일이 실제로 그 인증된 출처에서 보낸 것인지 검증하도록 지원합니다. 메일 발신자(ISP, 기업 등)는 이 기술을 사용하여 SPF 레코드를 게시합니다. 이 레코드는 어떤 호스트에서 그 이름을 사용할 수 있는지 지정합니다. SPF 호환 메일 수신자는 이메일 트랜잭션 과정에서 게시된 SPF 레코드를 사용하여 발신 MTA(Mail Transfer Agent)의 신원 인증을 테스트합니다.</td><td>DKIM은 암호화 기술 기반의 인증 방식으로서 어떤 도메인에서 보낸 이메일을 확인하고 인증할 수 있습니다. DKIM은 여러 이메일 헤더 필드로 구성된 암호 서명(즉, 키)과 메시지 본문을 제공합니다. DKIM의 보호를 받은 웹 도메인은 DNS 레코드에 공개 키(도메인 키)를 게시하는데, 이는 자체 생성된 개인 서명 키에 대응합니다. 이메일 수신자는 그 키를 사용하여 메시지 헤더와 본문이 발신 도메인의 신원과 일치하는지 확인할 수 있습니다. 즉 이메일이 피싱 또는 기타 악성 메시지일 가능성을 판단할 수 있습니다.</td></tr>
<tr><td colspan="2">DMARC는 이메일 발신자가 메시지 확인, 속성, 보고에 대한 정책 및 환경 설정을 지정할 수 있도록 해주는 정책 배포 메커니즘입니다. DMARC 사용 발신자의 메시지를 받는 수신자는 이 정보를 사용하여 메일 처리를 개선할 수 있습니다. DMARC를 사용하는 수신자는 이 정보를 사용하여 이메일에 대해 조치 안 함, 격리, 전달되기 전에 메시지를 변경하여 이메일 거절 등 수신 이메일에 대한 다양한 결정을 내릴 수 있습니다.</td></tr>
</table>

DMARC, SPF 및 DKIM은 표적 피싱 메시지를 탐지하는 데 매우 효율적이지만, 제한이 있습니다. AOTA(According to the Authentication and Online Trust Alliance)에 따르면, 전 세계의 합법적인 이메일 중 약 절반이 현재 인증된 상태입니다. 이와 같은 보급률로 미루어보건대, 스팸 및 피싱 이메일을 받을 가능성이 높은 기업 임원은 이메일 인증 실패에 주목하는 추가적인 이메일 필터링 및 차단 툴을 활용하여 효과를 거둘 수 있습니다.

HTML 무결성 유지: HTML-Convert라고도 하는 HTML 무결성 유지는 미리 결정된 기준에 따라 추가적인 이메일 보호를 수행합니다. 이를테면 SPF와 DKIM으로 메시지를 인증할 수 없는 경우에 유용합니다. HTML 무결성 유지를 사용할 경우 URL은 클릭할 수 없게 되고 일반 텍스트로 변환되어 숨겨진 잠재적 악성 콘텐츠가 수신자에게 드러나게 됩니다. 수신자 입장에서는 메시지에 포함된 적법한 URL을 방문할 때 부담으로 작용할 수 있습니다. 일반 텍스트 링크를 복사하여 브라우저에 붙여넣어야 그 웹 사이트로 이동할 수 있기 때문입니다. 그러나 스캐머의 표적이 되는 사용자라면 효과적인 추가적인 보호 계층이 됩니다. 어떤 웹 사이트에 방문하려 하는지 알 수 있기 때문입니다.

Cisco S-Series Web Security Appliance: 표적 피싱 및 기타 악성코드 공격에 대한 심층적인 방어 체계를 원하는 기업에 Cisco S-Series Web Security Appliance는 통합적이고 관리하기 편리한 계층적 웹 보안 플랫폼이 됩니다. 강력한 평판 필터와 악성코드 차단 방어 기술을 사용하면서 웹 트래픽의 전 범위를 다루고 알려졌거나 알려지지 않은 사이트로부터 보호합니다.

Cisco Cloud Web Security: Cloud Web Security는 표적 피싱 및 기타 악성코드 공격에 대해 S-Series Web Security Appliance 수준의 심층 방어를 제공하지만, 조직에서 클라우드를 효율적으로 활용하고 조직 내부와 외부의 모든 위치에서 모바일 지식 근로자를 웹 위협으로부터 보호할 수 있습니다.

요약

새로운 피싱 위협이 심각한 위험으로 자리 잡고 있습니다. 바로 표적 피싱입니다. 이러한 메시지에서는 이를테면 수신자의 이름과 소속 회사까지 언급하는 고도의 사회 공학적 수법을 구사하여 엄선된 피해자의 신뢰를 얻어 기밀 데이터 또는 재산을 온라인 범죄자에게 내주게 만듭니다.

표적 피싱 이메일은 더 많은 리소스를 필요로 하므로 현재는 전 세계 피싱 이메일 공격의 일부에 불과합니다. 그러나 큰 보상으로 이어질 수 있어, 그 수가 증가할 것이 분명합니다.

기업에서 표적 피싱 활동과 기타 악성코드 공격의 피해를 당하지 않도록 Cisco는 인터넷 트래픽 모니터링, 평판 필터, URL 지원 안티스팸 서비스, Cisco 보안 침해 필터 및 지능형 악성코드 차단, URL 필터링, 인증 기술을 결합한 통합적인 멀티레이어 이메일 및 웹 보안 방식을 제공합니다.

담당자

Cisco 콘텐츠 보안 제품이 어떻게 고객의 이메일 인프라를 보호하고 그 안정성과 관리 편의성을 높이는 데 도움이 될 것인지 평가할 수 있도록 Cisco Sales Representative, 채널 파트너, 지원 엔지니어가 언제라도 도와드리겠습니다. 업계 최고로 꼽히는 Cisco 제품의 혜택을 누리고 싶다면 800-428-9596으로 전화하거나 http://www.cisco.com/go/emailsecurity에서 문의하십시오.

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

C11-701843-01 05/15