2011년 6월

이메일 공격: 이제는 개별 맞춤형

개요

사이버 범죄의 비즈니스 모델이 최근 소규모 표적 공격으로 변화하고 있습니다. 이메일은 여전히 주요 공격 경로이며, 이메일 공격의 빈도 및 공격 대상에 미치는 경제적 피해는 증가하고 있습니다. Cisco SIO(Security Intelligence Operations)의 조사에 따르면, 무차별적인 대량 이메일 공격 기반의 사이버 범죄 비즈니스 활동이 전년 대비 절반 이상 감소했습니다. 그와 더불어 고도의 맞춤형 표적 공격에 따른 비즈니스 활동이 지난해 3배 늘어나는 등 빠르게 증가하는 추세입니다. 경제적 영향은 금전적 손실 및 인증 정보 도용으로 이어지지만, 이러한 공격 피해를 당한 기업은 감염된 호스트를 복구하고 실추된 브랜드 평판을 회복하는 데 적잖은 비용을 부담해야 합니다.

모빌리티 및 통제되지 않는 엔드포인트로 인해 이러한 공격의 영향이 더욱 커짐에 따라 네트워크를 활용하는 새로운 보안 방식의 구현이 더욱 절실해졌습니다. 많은 기업이 위험한 메시지를 식별하고 감염된 웹 사이트 또는 악성코드 다운로드로 이어지는 URL을 클릭하지 않도록 사용자를 교육하고 있으나, 사용자 교육만으로는 이러한 위협으로부터 확실하게 보호할 수 없습니다. 그보다는 방화벽, 웹 프록시, 침입 방지 센서와 같은 정책 적용 요소를 상황 인식형 고급 정책 언어로 관리할 수 있는 고도의 분산된 보안 아키텍처가 필요합니다.

이 백서에서는 공격 트렌드를 조명하고 이러한 공격 캠페인의 영향을 살펴보겠습니다. 이 글의 분석 결과는 Cisco가 전 세계 다양한 산업 분야의 기업들과 함께 실시한 연구 조사를 토대로 합니다.

사이버 범죄 사업: 이메일의 역할

사이버 범죄의 비즈니스 모델이 바뀌면서 지난해 위협 활동에도 큰 변화가 있었습니다. 전체 스팸 볼륨이 80% 감소한 것으로도 알 수 있듯이 대량 공격의 횟수가 감소했습니다. 대신 사이버 범죄자들은 사기 및 악성 공격, 스피어피싱 공격, 표적 공격을 늘리는 등 고부가가치 활동에 주력하고 있습니다.

대량 공격의 감소

표적 공격 전술로 바꾸는 사이버 범죄자가 늘고 있는 가운데 Cisco SIO는 사이버 범죄자가 기존 이메일 기반 공격으로 얻는 이익이 2010년 6월의 11억 달러에서 2011년 6월에는 5억 달러로 전년 대비 50% 이상 감소했다고 추정합니다. 이러한 변화는 일일 스팸량이 2010년 6월의 3천억 통에서 2011년 6월에 400억 통으로 감소한 것에서도 확인됩니다. 이러한 감소는 사용자 전환율이 계속 낮은 수준에 머무는 것과도 상통하며, 전환 시 사용자의 평균 비용 증가를 부분적으로 상쇄하고 있습니다

이러한 감소는 대량 공격의 하위 집합인 스캠 및 악성 공격에 의해 보완되고 있습니다. 전체 대량 공격의 약 0.2%를 차지하는 이 공격 유형은 사이버 범죄자에게 훨씬 큰 이익을 제공하고 있습니다. 지난해 개별 맞춤형 툴이 활용되면서 더 정교하게 짜인 스캠 및 악성 공격의 사용자 전환율은 크게 증가했습니다. 또한 악성코드 및 스캠으로 인한 평균 사용자 손실은 정보 공유의 영향으로 증가했습니다.

Cisco SIO는 예상 총 손실을 추정하면서(표 1 참조) 사용자당 피해액을 250달러로 줄잡아 적용했습니다. 이 금액은 최근 공개된 스캠 및 악성 코드 공격의 최저 추정치와도 일치합니다. 예를 들어, 2011년 6월에 미국 FBI(Federal Bureau of Investigation)에서 적발한 한 이메일 사기는 수신자에게 허가서 발급을 위해 350달러를 내도록 요구하고 그렇지 않으면 법적 조치를 취하겠다는 내용이었습니다. 이 추정치에 기초하면, (대량 공격의 하위 범주인) 스캠 및 악성 공격은 지난 1년간 5백만 달러에서 2억 달러로 성장했습니다.

표 1: 사이버 범죄자가 대량 공격으로 얻는 이익

이익(백만 달러)	1년 전	현재
스팸 공격	$1,000	$300
스캠 및 악성 공격	$50	$200
합계	$1,050	$500

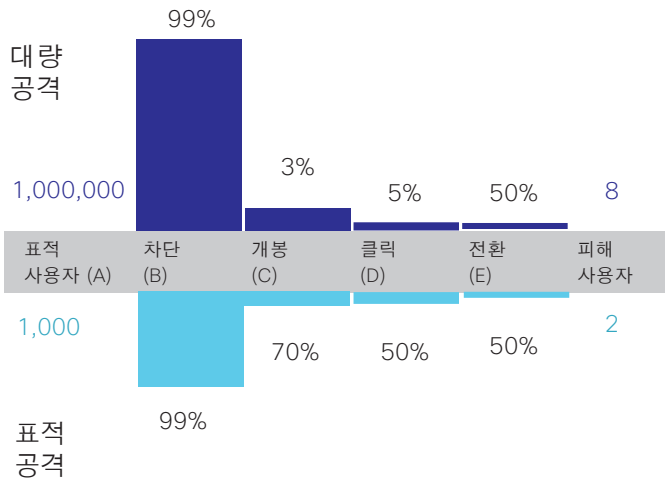
2010년부터 2011년까지 범죄 생태계가 급변했습니다. 전 세계의 경찰 당국, 보안 및 산업 기관이 공조하여 대규모의 스팸 배포 봇넷과 그 협력자들을 일망타진하거나 큰 타격을 입혔습니다. 대형 스팸 배포 제휴 조직인 SpamIt은 2010년 10월, 데이터베이스가 유출되고 러시아 경찰이 그 소유주를 기소하자 영업을 중단했습니다. Rustock, Bredolab, Mega-D 등 주요 봇넷이 큰 타격을 입거나 가동 중단되었습니다. 주요 카르텔의 재정 및 기술 비즈니스 모델이 무너지면서 위협의 규모는 감소하고 더 수익성 있는 활동을 선호하게 되었습니다.

그럼 대량 공격과 표적 공격이 전환 프로세스 및 비즈니스 모델 측면에서 어떻게 다른지 간단하게 살펴보겠습니다.

예전에는 스팸 전환 파이프라인이 연합 봇에서 메시지 전달에 사용한 이메일 주소록에서 시작되었습니다(그림 1의 A 단계 참조). 안티스팸 엔진은 위협 메시지의 대부분을 수신하는 즉시 정확하게 식별하여 차단합니다(B 단계). 스팸 필터를 통과한 메시지는 적법한 메시지로 간주되어 사용자의 편지함에

안착합니다. 식견 있는 사용자는 스팸 메시지를 무시하고 그중 일부만 개봉합니다(C 단계). 그중 소수만이 클릭하고(D 단계), 의심하지 않는 사용자가 제품을 구매하거나 악성코드를 다운로드하면서 "전환 완료"됩니다(E 단계).

그림 1: 위협 전환 파이프라인



이러한 기존 스팸 파이프라인이 아직도 있지만 개별 맞춤화되는 추세이며, 이는 표적 공격에서 가장 확연하게 드러납니다. 일반적으로 표적 공격은 파이프라인 전 범위에서 잔존율이 훨씬 높습니다. 이메일 및 웹 사이트 링크가 유효한 사용자에게 전송되고 보안 엔진과 수신자가 보기에 적법한 것처럼 보일 수 있기 때문입니다. 규모는 적지만 표적 공격의 전환율은 훨씬 높습니다. 전환율이 높은 만큼 더 유용한 입력을 위한 비용이 발생합니다.

- 한정된 속성을 지닌 유효한 이메일 주소의 목록
- 적법한 듯 보이는 메시지 - 주로 알려진 연락처에서 수신자와 관련된 콘텐츠를 보내는 것으로 위장
- 아직 드러나지 않은 고품질의 악성코드
- 단 1번의 표적 공격을 위해 특별히 개발된 (따라서 아직까지 보여진 적이 없는) 새로운 웹 사이트

범죄의 진화가 진행되는 것입니다. 사이버 범죄자들은 유지력을 높이기 위해 캠페인 전술을 새로운 환경에 적응시키고 있습니다.

공격 분류

사이버 범죄 활동이 계속 진화함에 따라 구체적 공격 및 기업에 미치는 영향도 변화합니다.

대량 공격

대량 공격은 분산 네트워크의 초기부터 기본적인 위협 요인으로 자리 잡았습니다. 자동 전파 웜, 분산 서비스 거부(DDoS) 공격, 스팸 등이 경제적 이익을 얻거나 기업에 타격을 주는 데 선호하는 방법입니다. 범죄자는 공통 페이로드를 생성하고 피해자가 대개 본의 아니게 액세스할 만한 곳에 배치합니다. 이를테면 웹 사이트를 감염시키거나 PDF와 같은 파일 형식의 보안 취약점을 악용하거나 구매 이메일을 보내거나 은행 인증서를 대량 피싱합니다.

네트워크에서 처음 보고되거나 확인될 때 신속하게 그 위협을 식별하고 향후 유사한 위협을 차단하는 것이 포함됩니다. 범죄자가 보안 계층에 본격적으로 침투하여 표적에 도달한 경우 상당한 양적 성과를 거둘 수 있으므로 이 비즈니스 모델은 수익성이 좋습니다.

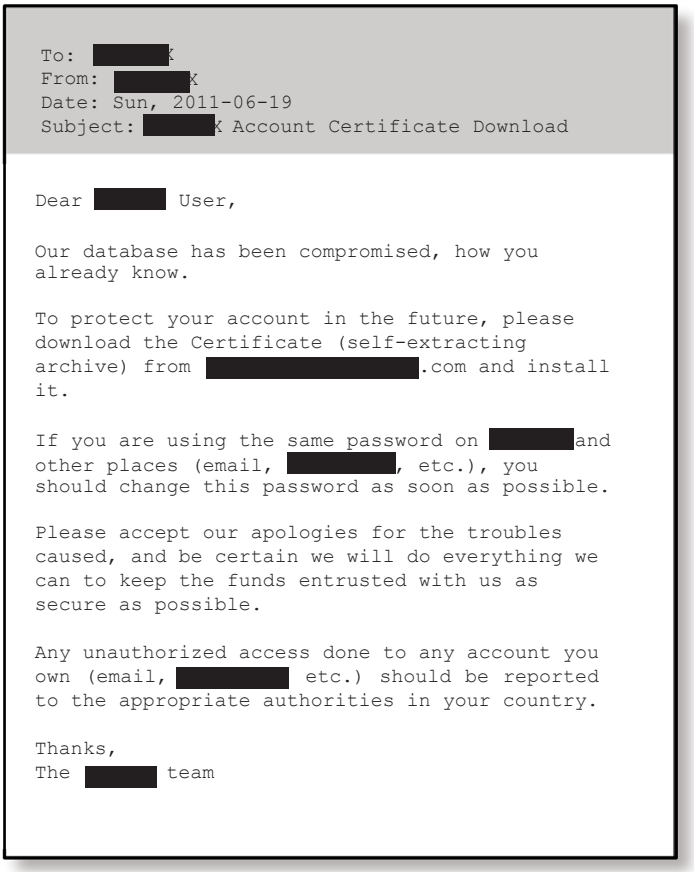
이러한 공격 유형에서 큰 부분을 차지하는 것이 급성장 중인 스캠과 악성 공격입니다. 범죄 생태계 진화의 일환으로 이 공격도 더욱 집중화되고 있습니다. 공격 경로 또는 전달 엔진(SMS, 이메일, 소셜 미디어 등)이 무엇이든 간에 범죄자들은 신중하게 표적을 고르고 사용자의 지리적 위치, 직책 등과 같은 개별 맞춤형 정보를 이용합니다. 이러한 스캠의 예를 들면 다음과 같습니다.

- 특정 지역 주민을 대상으로 한 SMS 금융 사기
- URL 단축 서비스를 이용한 이메일 캠페인
- 범죄자가 어떤 사용자 또는 사용자 그룹의 친구 행세를 하면서 금전적 이익을 얻는 소셜 미디어 스캠

이러한 전략은 소수의 위협을 전파하지만 피해자를 공략하는 데 효과를 거둘 수 있습니다. 하지만 범죄자에게 항상 비용 대비 효과가 입증되는 것은 아닙니다. 그러나 가치가 높은 피해자를 공략하는 이러한 방식이 지능적이고 조직화되고 수익을 추구하는 범죄자들에게 각광받기 시작했습니다. 범죄자가 구체적인 피해자 프로필을 대상으로 할 경우 이를 스피어피싱 공격이라고 합니다.

스피어피싱 공격은 특정 사용자 프로필을 노리는데, 주로 기업의 거래 은행 계좌에 액세스할 수 있는 고위직 사용자가 선정됩니다. 스피어피싱 공격은 치밀하게 계획되고 상황 정보를 활용하여 사용자가 적법한 콘텐츠를 다룬다고 느끼게 합니다. 스피어피싱 이메일은 개인적으로 중요한 특정 품목 또는 회사와 관련된 문제를 다루는 것처럼 보일 수 있습니다. 이를테면 급여 착오 또는 법적 문제에 대해 논의하는 것처럼 위장합니다. Cisco SIO의 연구에 따르면, 스피어피싱 공격의 80% 이상이 악성 콘텐츠 웹 사이트에 연결되는 링크를 포함합니다. 그러나 연결된 웹 사이트는 정교하게 만들어지고 지금까지 드러난 적이 없기 때문에 탐지하기가 까다롭습니다.

그림 2: 스피어피싱 메시지



To: [redacted]
From: [redacted]
Date: Sun, 2011-06-19
Subject: [redacted] Account Certificate Download

Dear [redacted] User,

Our database has been compromised, how you already know.

To protect your account in the future, please download the Certificate (self-extracting archive) from [redacted].com and install it.

If you are using the same password on [redacted] and other places (email, [redacted], etc.), you should change this password as soon as possible.

Please accept our apologies for the troubles caused, and be certain we will do everything we can to keep the funds entrusted with us as secure as possible.

Any unauthorized access done to any account you own (email, [redacted] etc.) should be reported to the appropriate authorities in your country.

Thanks,
The [redacted] team

표적 공격

표적 공격은 고도의 맞춤형 위협으로서 특정 사용자 또는 사용자 그룹을 대상으로 대개는 지적 재산의 도용을 목적으로 합니다. 이 공격은 그 규모가 매우 작으므로 자신도 모르게 감염된 계정을 통해 알려진 엔터티로 위장하거나 전문 봇넷 배포 채널을 통해 익명성을 띱니다. 표적 공격은 어떤 형태로든 악성코드를 사용하며, 제로데이 익스플로잇을 통해 조기에 시스템에 진입하여 장기적으로 원하는 데이터를 수집할 때도 많습니다. 범죄자는 이 공격에서 여러 방식으로 피해자에게 접근합니다. 표적 공격은 방어하기가 쉽지 않으며, 피해자에게 가장 심각한 타격을 줄 수도 있습니다.

표적 공격과 스피어피싱은 그 구조적으로는 유사할 수 있으나 피해자에 대한 초점에서 큰 차이가 있습니다. 표적 공격은 특정 사용자 또는 사용자 그룹을 겨냥하는 반면 스피어피싱 공격은 공통점을 갖는 집단, 이를테면 동일 은행의 고객을 대상으로 합니다. 표적 공격자는 주로 공격 대상에 대한 각종 정보를 확보하고 있습니다. 소셜 네트워크, 보도 자료, 공개된 기업의 공문서로부터 정보를 수집합니다. 스피어피싱 공격도 개별 맞춤형 정보를 포함할 수 있으나, 표적 공격은 고도로 맞춤화되고 표적의 특별한 관심사에 부합하는 방대한 정보를 포함할 수 있습니다.

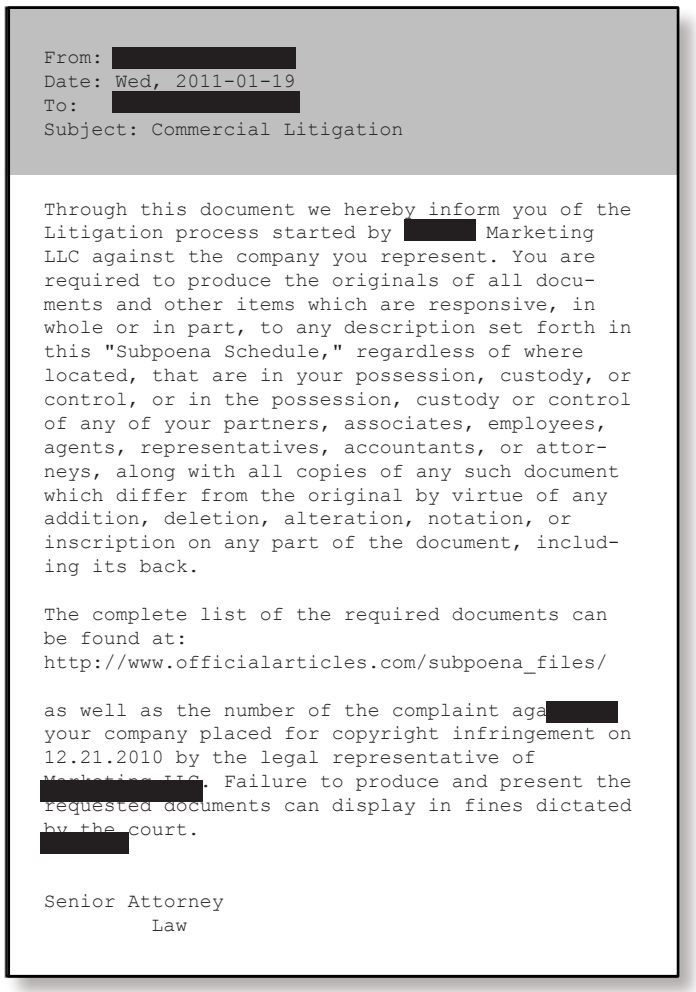
표 2: 표적 공격과 스피어피싱 공격 비교

특징	표적 공격	스피어피싱 공격
의도	지적 재산 도용	금전적 이익
악성코드	예, 종종 제로데이 익스플로잇 사용	가능성 있음
표적 정찰	예	아니요
개별 맞춤화 정도	매우 높음	일부

잘 알려진 표적 공격의 예로 Stuxnet이 있습니다. 2010년 7월에 발견된 이 컴퓨터 웜은 산업용 소프트웨어와 장비를 표적으로 삼았습니다. Stuxnet은 Widows에서 바로가기 파일을 다루는 방식의 취약점을 이용했기 때문에 이 웜이 신규 시스템에 확산될 수 있었습니다. 이 웜은 SCADA(Supervisory Control and Data Acquisition) 시스템 또는 복잡한 산업용 네트워크(예: 발전소, 화학 제조 시설 등)를 관리하는 시스템을 공격할 목적으로 특별히 만들어진 것으로 보입니다. Stuxnet은 네트워크에 연결되지 않은 시스템을 돌아다닐 수 있다는 점에서 뛰어납니다. 즉 네트워크나 인터넷에 연결되지 않은 시스템도 위험합니다. 운영자들은 고객에게 큰 불편을 주지 않고서는 벤더들이 기본 Siemens 비밀번호(몇 년 전에 웹에 공개되었음)를 수정할 수 없다고 생각했습니다. SCADA 시스템 운영자가 잘못된 보안 인식 하에 작업했을 가능성도 있습니다. 시스템이 공용 인터넷에 연결되지 않았으므로 감염되지 않을 것이라 생각했을 수도 있습니다. Federal News Radio 웹 사이트에서는 Stuxnet을 "역사상 가장 지능적인 악성코드"라고 불렀습니다.

2011년 1월, Cisco SIO는 한 대기업의 고위 임원에게 발송된 표적 공격 메시지를 탐지했습니다. 이 캠페인은 지금까지 본 적이 없는 리소스를 사용했다는 점에서 정교한 공격이었습니다. 알 수 없는 발신자가 합법적이지만 감염된 호주의 서버를 통해 메시지를 보냈습니다. 이 이메일 메시지는 언뜻 보면 적법한 것 같습니다(그림 3). 내장된 작업 URL은 합법적이지만 감염된 법률 관련 블로그에서 호스팅되었습니다. 클릭하면 사용자의 브라우저는 알려지지 않았던 Phoenix 익스플로잇 킷의 사본으로 연결되었습니다. 익스플로잇이 성공하면 피해자의 컴퓨터에 Zeus 트로이 목마를 설치했습니다.

그림 3: 표적 공격 메시지



From: [redacted]
Date: Wed, 2011-01-19
To: [redacted]
Subject: Commercial Litigation

Through this document we hereby inform you of the Litigation process started by [redacted] Marketing LLC against the company you represent. You are required to produce the originals of all documents and other items which are responsive, in whole or in part, to any description set forth in this "Subpoena Schedule," regardless of where located, that are in your possession, custody, or control, or in the possession, custody or control of any of your partners, associates, employees, agents, representatives, accountants, or attorneys, along with all copies of any such document which differ from the original by virtue of any addition, deletion, alteration, notation, or inscription on any part of the document, including its back.

The complete list of the required documents can be found at:
http://www.officialarticles.com/subpoena_files/

as well as the number of the complaint aga[redacted] your company placed for copyright infringement on 12.21.2010 by the legal representative of [redacted]. Failure to produce and present the requested documents can display in fines dictated by the court.

Senior Attorney
Law

공격의 경제성

일반적인 캠페인의 경제성은 대량 공격 비즈니스 모델과 표적 공격 비즈니스 모델의 차이점을 확실하게 드러냅니다. 이와 관련하여 표 3에서는 대량 공격 표본과 스피어피싱 공격 표본을 대상으로 사이버 범죄자의 입장에서 전환 파이프라인의 수율과 상대적 경제성을 비교합니다.

표 3. 대량 피싱과 스피어피싱 공격의 경제성 비교

일반적인 캠페인의 예	대량 피싱 공격 (단일 캠페인)	스피어피싱 공격 (단일 캠페인)
(A) 캠페인의 총 메시지 발송량	1,000,000	1,000
(B) 차단율	99%	99%
(C) 개봉률	3%	70%
(D) 클릭률	5%	50%
(E) 전환율	50%	50%
피해자	**8**	**2**
피해자별 가치	$2,000	$80,000
캠페인 총 가치	**$16,000**	**$160,000**
캠페인 총 비용	$2,000	$10,000
캠페인 총 이익	**$14,000**	**$150,000**

개별 캠페인으로 보면 스피어피싱공격의 경제적 가치가 대량 공격보다 훨씬 우수합니다. 비용도 훨씬 높지만, 그 수율과 이익도 높습니다. Cisco SIO의 추정에 따르면 목록 수집의 품질, 배포된 봇넷, 이메일 생성 툴, 구매한 악성 코드, 제작한 웹 사이트, 캠페인 관리 툴, 주문 처리 백엔드 인프라, 주문 처리 업체, 사용자 배경 조사 활동을 고려할 때 스피어피싱 공격의 비용은 대량 공격의 5배입니다.이와 같이 높은 기본 비용과 많은 공수가 투입되는 만큼 고도의 전문 기술력이 요구됩니다. 또한 수율이 높아야 효과가 있습니다.

사이버 범죄자들은 상충하는 우선 순위를 균형적으로 조정하고 있습니다. 더 많은 사용자를 감염시킬 것입니까, 아니면 보안 벤더의 감시를 피할 만큼 소규모의 공격을 유지할 것입니까? 스피어피싱 공격 캠페인은 그 규모가 제한적이지만 사용자의 개봉률과 클릭률이 훨씬 높습니다. 사이버 범죄자들은 이러한 제약 하에 회사의 거래 은행 계좌에 액세스할 수 있는 비즈니스 사용자를 주로 공략하면서 감염당 투자 수익을 충분히 확보하려 합니다. 따라서 피해자당 평균 가치가 대량 공격의 40배에 이를 수도 있습니다. 궁극적으로 이 모델은 타당성이 입증됩니다. 단일 스피어피싱 공격 캠페인으로 얻는 이익이 대량 공격의 10배 이상이 될 수 있습니다.

이러한 잠재적 투자 가치 때문에 사이버 범죄의 비즈니스 모델이 바뀌고 있는 것입니다. 현재 스패밍의 기회 비용은 안티스팸의 효율성 및 사용자 인식의 증가로 인해 투자 수익보다 높을 수 있습니다. 그 대신 사이버 범죄자들은 다양한 유형의 표적 공격에 시간과 공수를 집중하는데, 대개는 더 많은 이익을 낼 수 있는 기업 및 개인 소유 은행 계좌와 고가의 지적 재산에 접근하는 데 목적이 있습니다.

일부 사이버 범죄자는 더 개별 맞춤형 공격이 되도록 이메일 마케팅 벤더를 감염시키는 데 주력합니다. 이들은 유효한 이름, 이메일 주소, 기타 속성 데이터를 보유하고 있기 때문입니다. 이러한 개인 정보가 스캠 및 악성 공격(대량 공격 또는 스피어피싱)에 사용되면 사용자가 첨부 이메일을 열어볼 가능성이 높아집니다.

대량 스팸의 감소와 최근 데이터 유출 사고의 상관성은 흥미롭습니다. 그러나 기억할 점은 공격이 더욱 개별 맞춤화되고 있다는 사실입니다.

개별 맞춤형 공격의 영향

스피어피싱 공격의 영향

스피어피싱 공격은 다른 위협 유형에 비해 그 규모는 작지만 현재 기업들에게 심각한 타격을 주고 있습니다. 스피어피싱 공격의 대부분은 재정적 손실로 이어져 피해자에게는 매우 위험하고 사이버 범죄자에게는 더없이 유익합니다.

스피어피싱은 대량 스캠 및 악성 공격보다 더 우수한 맞춤형 기법을 구사하므로 사용자의 개봉률과 전환율이 훨씬 높습니다. 이러한 성공 요인 덕분에 스피어피싱 공격의 감염은 더욱 효과적이며 따라서 더욱 보편화되고 있습니다. 이를 입증하듯 Federal Trade Commission의 조사에서도 매년 9백만 명의 미국인들이 신원 정보를 도용당하는 것으로 확인되었습니다.

스피어피싱 공격의 피해자당 가치는 천차만별이지만, 그 중앙값과 평균값은 매우 높습니다. 예를 들어, Javelin Strategy & Research의 1차 소비자 조사에서 피해자당 신원 사기 평균 피해액은 $4,607였습니다(2010년). 사용자 손실을 $400로 줄잡아 볼 경우 스피어피싱 공격으로 사이버 범죄자가 누릴 총이익은 2010년 6월 기준으로 연간 1억 5천만 달러입니다(표 4 참조). 이 그림을 보면 1년 전의 5천만 달러에서 3배가량 증가한 것입니다. 앞으로 몇 개월간 사이버 범죄자들이 예전의 비즈니스 활동 수준을 회복하면서 이 증가세는 계속될 것으로 보입니다.

표적 공격의 영향

표적 공격은 그 악의적 특성 때문에 사회 전반과 특히 개별 기업에게 막대한 비용을 치르게 합니다. 사이버 범죄자가 표적 공격으로 얻는 이익은 상당한 규모이지만 추정하기가 쉽지 않습니다. 피해자 및 관련된 지적 재산에 따라 크게 달라지기 때문입니다. 그러나 사이버 범죄자가 얻는 이익은 피해 기업이 감당한 전체 비용의 일부입니다. 기업의 평판과 이미지에도 큰 영향을 미치기 때문입니다.

기업이 표적 공격으로 치르는 비용은 크게 달라질 수 있습니다. FBI에 따르면, 수천 달러부터 수억 달러에 이르기도 합니다. 역시 Ponemon Institute도 기업의 데이터 유출 사고당 잠재적 비용을 1백만 달러 ~ 5800만 달러로 추정했습니다. 예를 들어, 한 대형 게임랫폼 공급업체는 2011년 2분기에 발생한 네트워크 무단 액세스 때문에 발생한 관련 비용이 지금까지 알려진 것만 1억 7,200만 달러에 달한다고 밝혔습니다. 비용에는 개인 정보 도용 방지 프로그램, 신원 도용 손실을 보상하기 위한 보험, "복구" 프로그램 비용, 고객 지원 비용, 네트워크 보안 강화 비용, 법률 및 전문가 비용, 향후 잠재적 매출 감소가 이익에 미칠 영향 등이 포함됩니다.

또 다른 예로 한 결제대행사는 데이터 보안 사고로 인해 수백만 개의 사용자 계정 인증서가 유출되었습니다. 1년 후 이 회사는 총 1억 5백만 달러의 비용을 지출했다고 밝혔습니다. 이 회사의 10-Q SEC 제출 자료에 따르면, "이 비용의 대부분, 즉 약 9,080만 달러는 (i) MasterCard 및 VISA에서 당사와 스폰서 은행에 대해 실시한 평가, (ii) 스폰서 은행(계약에 따라 당사에 면책 권리를 주장할 수 있음)에 대해 제기된 소송 중 일부를 해결하기 위해 몇몇 카드 브랜드에게 제안한 합의, (iii) 합의가 진행 중인 몇몇 배상 청구인과의 합의 예상 비용"이었습니다. 보안 사고 시점부터 10-Q 결과 보고까지의 같은 기간에 이 회사는 Standard and Poor's 500 Index 기준 가치의 30%, 즉 3억 달러 상당의 주주 가치 손실이 발생했다고 밝혔습니다.

결국 금전적 손실과 복구 비용보다 기업의 이미지 실추가 훨씬 큰 비용 부담이 됩니다.

공격의 전반적인 영향

표 4는 이러한 추정치를 종합한 것으로 사이버 범죄자가 각 공격 유형에서 얻을 수 있는 연간 총 금전적 이익을 보여줍니다.

표 4: 사이버 범죄자가 얻을 연간 총 금전적 이익

이익(백만 달러)	1년 전	현재
대량 공격	$1,050	$500
스피어피싱 공격	$50	$150
표적 공격	가변적, 위 참조	가변적, 위 참조
합계	$1,100	$650

사이버 범죄의 비즈니스 모델 변화가 저조한 위협 활동을 어느 정도 보상하는 이익을 제공하고 있음이 분명합니다. 기업들은 사이버 범죄 활동의 감소로 인한 반사 효과를 부분적으로만 누릴 수 있습니다. 재정적 손실보다 훨씬 큰 비용이 발생할 수 있기 때문입니다. Cisco SIO는 이 총 손실을 추정하기 위해 세계 각처의 361개 기업/기관을 대상으로 1차 조사를 실시하여 그들의 관점을 조명했습니다.

공격이 기업에 미치는 영향은 다음과 같이 분류할 수 있습니다.

1. 재정적
2. 복구
3. 평판

재정적: 사이버 범죄로 인한 직접적인 재정적 손실은 구체적 공격에 따라 크게 달라질 수 있습니다. 따라서 기업에서 그 손실을 추정할 수는 없습니다.

복구: 스피어피싱 및 표적 공격의 복구 비용은 피해를 당한 기업에서 발생합니다. 관리 팀이 감염된 호스트를 찾아내 복구해야 합니다. 은밀하게 사용되는 애플리케이션이 늘어나는 만큼 이는 만만치 않은 일이 될 수 있습니다. 현재 표적 공격 및 그 기본 악성코드의 복잡성 때문에 막대한 복구 비용이 발생할 수 있습니다.

여기에는 감염된 호스트를 해결하는 데 드는 시간과 그에 따른 기회 비용도 포함됩니다. Cisco는 설문에 참여한 기업에서 감염된 호스트가 복구하려면 평균 2시간을 전적으로 매달려야 한다는 사실을 확인했습니다. 복구당 2시간의 공수에 해당하는 비용은 기업에 따라 달라집니다. 그 기간의 기회 비용도 마찬가지입니다.

Cisco SIO의 조사에 따르면, 감염된 사용자당 예상 직접 복구 비용이 640달러로 직접적인 금전적 손실의 2.1배에 달합니다.

평판: 장기적으로 피해 기업과 사용자가 공격의 부정적 영향을 입을 수 있습니다. 예를 들어, 어떤 브랜드를 키우는 데 몇 년의 시간이 걸립니다. 하지만 부정적인 사건이나 뉴스 보도, 특히 널리 알려진 경우에는 회사의 이미지를 순식간에 무너뜨릴 수 있습니다. 직접적인 영향 중에는 거래 급감도 있는데, 그로 인해 기업이 문을 닫을 수도 있습니다.

평판 저하의 실제 비용을 산정하는 건 쉽지 않습니다. 기업의 브랜드 가치를 평가하는 일이기 때문입니다. 그렇지만 각 기업은 부정적 사건이 평판에 악영향을 미치고 이는 심각한 매출 감소 및 주주 가치 상실로 이어질 수 있음을 분명히 해야 합니다.

Cisco SIO의 조사에 따르면, 감염된 사용자당 예상 평판 비용이 1,900달러로 직접적인 금전적 손실의 6.4배에 달합니다

종합적인 영향: 스피어피싱 공격과 표적 공격의 총비용은 사이버 범죄자가 직접적으로 얻는 금전적 이익보다 훨씬 큽니다. 표 5는 Cisco SIO 설문 조사에 참여한 361개 기업의 결과를 정리한 것입니다. ..

표 5: 기업이 부담할 공격당 종합 비용

기업 규모	금전적 손실*	복구 비용*	평판 비용*
최대 1,000명의 사용자	$327	$558	$2,346
1,000명 ~ 5,000명	$233	$484	$1,436
5,000명 이상	$290	$833	$1,553

*감염된 사용자당

해당 기업 및 공격에 따라 비용이 달라질 수 있으나 한 가지 사실을 분명합니다. 종합적으로 막대한 비용이 발생할 수 있다는 것입니다. 또한 평판 관리 및 복구 노력은 기업에게 큰 부담으로 작용할 수 있습니다.

결론

소규모 표적 공격의 증가는 산업, 지리적 위치, 규모와 상관없이 많은 기업의 사용자에게 영향을 미쳤습니다. 이 공격이 확산됨에 따라 범죄자의 경제적 이익과 피해 기업이 입는 타격이 모두 증가했습니다. 기업은 금전적 손실 외에도 감염된 호스트를 복구하는 비용과 브랜드 이미지 실추로 인한 비용까지 부담해야 합니다. 표적 공격 횟수가 증가할 것으로 예상되는 만큼 사이버 범죄 활동은 더욱 진화하고 더 큰 영향을 미칠 것입니다.

솔루션: Cisco Security Intelligence Operations

계층화된 제품과 여러 필터의 사용에 의존하는 기존의 보안 방식은 빠르게 확산되고 전 세계를 대상으로 하며 여러 경로를 통해 전파되는 차세대 악성코드와 맞서기에 역부족입니다.

Cisco는 세계 최대 규모의 클라우드 기반 보안 에코시스템인 Cisco SIO를 통해 실시간 위협 정보를 활용하면서 최신 위협에 한발 앞서 대비하고 있습니다. Cisco SIO는 이미 구축된 Cisco 이메일, 웹, 방화벽, 침입 방지 솔루션에서 가져오는 1백만여 개의 라이브 데이터 피드로부터 SensorBase 데이터를 수집하여 활용합니다.

Cisco SIO는 데이터를 분석하고 처리하여 위험을 자동으로 분류하고 200개 이상의 매개 변수를 사용해 규칙을 생성합니다. 보안 연구진 역시 네트워크, 애플리케이션, 장치에 광범위한 영향을 미칠 수 있는 보안 이벤트에 대한 정보를 수집하고 제공합니다. 이러한 규칙은 구축된 Cisco 보안 장치에 3~5분마다 동적으로 전송됩니다. Cisco SIO 팀은 또한 위협을 효과적으로 막아내기 위한 보안 모범 사례와 전술적 지침도 발행합니다.

Cisco는 통합성, 적시성, 포괄성 및 효과성을 갖춘 완전한 보안 솔루션을 제공하여 세계 각처의 기업과 기관에 종합적 보안을 구현하기 위해 최선을 다하고 있습니다. Cisco와 함께 위협 및 취약성 조사 시간을 줄이고 보안에 대한 사전 대응적 접근 방식을 마련하는 데 더 주력할 수 있습니다.

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.