Cisco 2014 중기

보안 보고서

개요

크든 작든 모든 사이버 공격은 보안 사슬의 연결 취약점에서 생겨납니다. 연결 취약점은 오래된 소프트웨어, 잘못 작성된 코드, 방치된 웹사이트, 개발자의 실수, 맹목적으로 신뢰하는 사용자 등 다양한 형태로 나타납니다. 공격자들은 집요하게 이러한 약점을 찾아내어 최대한 활용합니다.

공격의 표적이 된 기업과 사용자에게는 불행하게도, 악의적 공격자는 그 표적의 약점을 면밀하게 살피지 않아도 됩니다. IoT(Internet of Things)의 연결 환경을 기반으로 하여 IoE(Internet of Everything) 시대가 빠르게 도래하면서 자동차부터 홈 오토메이션 시스템까지 무엇이든 네트워크에 연결되어 공략 가능한 영역이 확대됨에 따라 과거 어느 때보다도 수월하게 공격할 수 있게 되었습니다.

이러한 사이버 공격은 경제적 비용뿐 아니라 생산성 저하 및 이미지 실추로 인한 손실을 초래하여 심각한 피해를 일으킵니다. 포네몬 인스티튜트(Ponemon Institute)에 따르면, 기업이 데이터 유출로 인해 부담하는 평균 비용은 2013년의 450만 달러에서 2014년에 540만 달러로 늘어났습니다. 미국 국제전략연구소(Center for Strategic and International Studies)의 ***Estimating the Cost of Cybercrime and Cyber Espionage*** 보고서에서도 미국에서 악성 온라인 활동으로 인해 연간 1,000억 달러의 손실이 발생하고 최대 508,000개의 일자리가 사라진다고 지적합니다.[1]

위협 정보

위협 정보로 이동

*Cisco 2014 Midyear Security Report*에서는 2014년 상반기의 위협 정보와 사이버 보안 트렌드를 점검합니다. 인터넷을 비롯하여 우리가 사용하는 시스템에 얼마나 많은 유형의 연결 취약점이 있으며, 그 수와 영향을 줄이기 위한 방법에는 무엇이 있는지 모색하는 데 Cisco의 연구가 도움이 될 것입니다. 그 주요 결과를 간추려 정리하면 다음과 같습니다.

Cisco는 일부 Cisco 고객의 기업 네트워크 내부에서 시작되는 DNS(Domain Name System) 쿼리를 조사하는 "인사이드 아웃(Inside Out)" 프로젝트(또는 도메인 이름과 관련된 IP(Internet Protocol) 주소를 검사하는 프로세스)를 통해 대형 다국적 기업 16곳의 네트워크를 관찰하고 다음과 같은 사실을 확인했습니다.

Cisco에서 조사한 고객 네트워크의 약 70%는 Dynamic DNS (D DNS)에 DNS 쿼리를 요청하는 것으로 나타났습니다.

조사한 고객 네트워크의 90% 이상이 악성코드 배포와 관련 있는 호스트 이름에 대한 DNS 요청을 실행한 것으로 나타났습니다.

조사한 고객 네트워크의 40% 이상이 IPsec(IP Security) VPN, SSL(Secure Sockets Layer) VPN, SSH(Secure Shell) Protocol, SFTP(Simple File Transfer Protocol), FTP, FTPS(FTP Secure)와 같은 서비스를 제공하는 기기와 관련 있는 사이트 및 도메인에 대한 DNS 요청을 실행한 것으로 나타났습니다.

2014년 1월부터 6월까지 게시된 2,528개의 취약점 경고 중에서 28개는 적극적인 공격을 받았습니다. 이는 우선 순위가 높거나 긴급한 조치를 요하는 취약점으로서 신속하게 패치를 적용하여 대응해야 합니다.

전 세계의 스팸량은 2013년에 전반적으로 감소했다가 지난 10월부터 증가하기 시작했지만, 일부 국가에서는 늘어나지 않았습니다.

업계 트랜드

업계 트렌드로 이동

고수익 업종으로 꼽히는 제약 및 화학은 2014년 상반기에도 웹 악성코드 발생 위험이 가장 높은 3대 업종에 포함되었습니다.

언론 및 출판 업계는 웹 악성코드 관측률이 이전의 평균치를 크게 능가했습니다.

2014년에는 NTP(Network Time Protocol) DDoS(distributed denial of service) 공격이 기승을 부렸습니다. 2014년 상반기에 발생한 NTP 증폭 공격 중 매우 심각했던 하나는 글로벌 DNS 제공업체인 CloudFlare의 한 고객을 겨냥한 것이었습니다. 2월에 발생한 공격은 약 400Gbps의 UDP(User Datagram Protocol) 트래픽에 이르러 절정에 달했습니다.

익스플로잇 킷 수는 유명한 블랙홀(Blackhole) 익스플로잇 킷의 개발자로 알려진 폰치(Paunch)가 지난해 체포된 이후 87%가량 줄었다고 Cisco 보안 연구 팀이 밝혔습니다.

2014년 상반기에 확인된 몇몇 익스플로잇 킷이 한때 블랙홀 익스플로잇 킷의 아성을 공략하려 했지만, 아직 확실한 강자가 나타나지 않은 상태입니다.

2014년에는 여러 가지 이유로 POS(Point-of-sale) 취약점이 범죄자들에게 각광받기 시작했습니다.

POS 시스템이 인터넷에 연결되는 경우가 늘면서 기업 네트워크에 침투하려는 범죄자의 진입점이 되고 있습니다.

결제 카드 정보를 중요 데이터로 간주해야 한다는 인식이 자리 잡지 않아 보호가 허술한 편입니다.

기업에서 POS 솔루션의 전체 또는 일부에 서드파티 벤더를 이용하는 경우가 늘면서 범죄자의 액세스 포인트가 늘어났습니다.

전망

전망으로 이동

IoT로 인한 보안 위험 및 기업에서 이러한 위험에 능동적으로 대응해야 하는 이유

탐지하기 어려운 네트워크 위협을 찾아내는 데 있어 예측 분석 및 기계 학습 기술의 효용성

사이버 보안을 전략적 위험이자 비즈니스 프로세스로 바라보기 시작한 기업들의 변화

가시성에 기초하고 위협에 중점을 두는 플랫폼 기반 보안 솔루션의 필요성 - 공격의 전후 및 진행 상태의 전 범위를 다루고 각기 다른 제품으로 인한 복잡성을 해소하면서 보안 허점을 해결하도록 지원하는 솔루션

목차

이 문서에는 검색 및 공유 가능한 내용이 포함되어 있습니다.

Adobe Acrobat에서 찾기(Find) 기능을 열려면 클릭

이메일 및 소셜 미디어로 콘텐츠 공유

권장 소프트웨어:

Adobe Acrobat 버전 7.0 이상

IoT: 새로운 기회이자 위험

IoT(Internet of Things)란 "인터넷을 통해 액세스되는 사물로 이루어진 네트워크라고 기술 분석가와 선구자들은 정의합니다. 이러한 사물에는 내부 상태 또는 외부 환경과의 상호 작용을 가능하게 하는 기능이 내장됩니다. 즉, 사물이 감지 및 통신 능력을 갖게 되면 의사 결정의 방식과 장소, 의사 결정 주체가 바뀌게 됩니다."[2]

2020년이면 약 500억 개의 사물이 IoT에 연결될 것으로 Cisco는 예측하고 있습니다.[3] IoT에 의해 공격 표면이 크게 확대되면서 보안 환경도 이미 변하고 있습니다. IoT 세상에서는 사람, 프로세스, 데이터 간 연결이 증가하므로 지속적이고 광범위한 탐지 및 보호가 더욱 중요해집니다.

급속도로 진화하는 퍼베이시브 컴퓨팅과 고도로 상호 연결된 환경에서는 네트워크에 연결되면 무엇이든 공격자가 악용할 수 있는 공격 표면이 될 수 있습니다. 공격자가 무엇을 할 수 있는가는 *아직도 상당 부분이* 가설이지만, 이들은 이미 계획을 세우고 아이디어를 테스트하면서 소기의 성과를 거두고 있습니다.

최근에는 자동차, 의료 기기, 베이비 모니터까지 해커들의 IoT "연구 개발" 대상에 포함되었습니다.[4-6]

IoT의 궁극적인 목표는 운영 효율성을 높이고 새로운 비즈니스 모델을 활성화하고 삶의 질을 높이는 데 있습니다. 일상의 사물을 연결하고 네트워크화한다면 간단한 데이트를 결합하여 쓸모있는 정보를 얻을 수 있습니다. 그러나 이것은 더 많은 개인 정보와 기업 데이터가 클라우드에 저장되고 각처에 전송될 가능성도 커진다는 것을 의미합니다. 따라서 데이터를 보호하기 위해 적절한 보안을 적용하고 데이터 취급 방식에 관한 개인 정보 보호 정책을 마련하는 것이 더욱 중요한 의미를 갖습니다.

개인 정보 보호는 IoT에서 중대한 문제입니다. 사용자가 정보를 보호하고 지나친 신뢰를 삼가기 위해 주의하고 경계하더라도, 사용자의 통제 범위를 벗어난 보안 사슬의 연결 취약점 때문에 여전히 위험은 사라지지 않습니다(29페이지, 감염된 보안 암호화 연결 참조). 공격자가 자동차, 스마트폰, 홈 오토메이션 시스템 등 각기 다른 출처로부터 입수한 정보의 상관성을 찾아내기 시작하면 하나의 기기, 시스템 또는 애플리케이션에서 얻은 정보에 의존할 때보다 훨씬 거시적인 관점에서 사용자를 파악할 수 있게 됩니다. 쇼핑 습관, 거주지 등 사용자의 세부 정보를 토대로 전례 없이 정교하고 치밀하게 구성된 고도의 표적 공격이 이루어질 수 있습니다.

피트니스 트래킹용 웨어러블 디바이스, DVR(digital video recorder)과 같은 일상적인 기기가 심각한 보안 위험이 될 수 있거나 해커의 관심사가 된다는 주장이 일부에게는 설득력 없게 들릴 수도 있습니다. 그러나 자동차를 비롯하여 전형적인 컴퓨팅 장치가 아니었던 기기가 표준 컴퓨팅 플랫폼에 더 가까워지면서 전형적인 컴퓨팅 기기를 노리던 위협에 취약할 수 있습니다[7].

선두 벤더들은 IoT 기기의 보안 문제에 대해 알고 있으며, 자사 제품에 확실하게 보안을 구성할 수 있는 식견과 경험을 갖추고 있습니다. 후발 주자들은 지난 20년간 사이버 보안 업계가 얻은 교훈을 참고하면서 비슷한 실수가 반복되지 않도록 혁신의 과정에서 노력을 기울일 수 있습니다. 범용 컴퓨터에 적용되었던 모범 사례 중 상당수는 IoT 기기에도 적용되면 이를테면 최신 소프트웨어 설치가 해당됩니다. 그러나 IoT의 뒤를 이을 IoE(Internet of Everything) 세상에서는 대체로 사용자가 아닌 시스템에 의해 보안이 관리될 것이므로, 업계는 이 새로운 환경을 위한 안전한 기술을 설계할 때 이 점을 염두에 두어야 합니다. 여기에는 사용자를 위한 투명성 보장도 포함되며 이러한 투명성을 통해 사용자는 IoT 기기에서 자동으로 보안을 유지하고 있는 것을 확신하거나 수동 조치가 필요한 시점을 알 수 있어야 합니다.

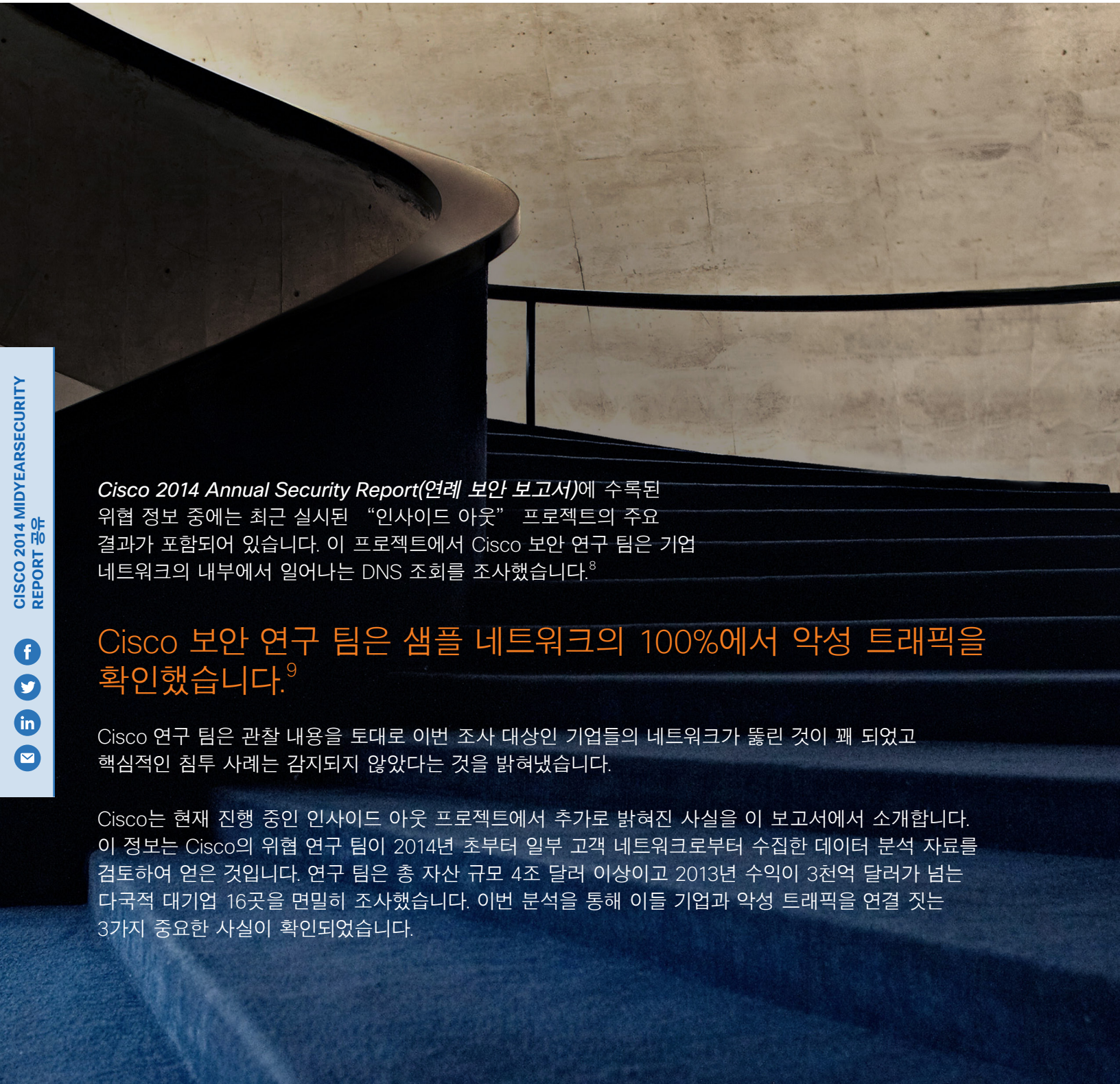
인터넷 에코시스템에는 항상 또 하나의 새로운 것이 추가 될 것입니다. 그와 동시에 버려지고 관리되지 않는 인터넷 연결 기기도 늘어날 것입니다. 오늘날 잊혀졌거나 외면당한 무수히 많은 웹사이트와 마찬가지로(37페이지, WordPress 취약점: 방치되는 매장 참조) 주방 기기, 감시 카메라, 개인용 프린터 등 각종 기기가 보안 사슬의 연결 취약점이 되고 기업화된 해커들이 거의 제약 없이 침투하여 데이터 센터까지 접근할 수 있는 통로를 만들어 줍습니다.

사이버 범죄자의 역량과 동기는 잘 알려져 있습니다. 이들이 IoT에 점차 더 큰 관심을 갖게 되는 것은 자연스러운 일입니다. 전 세계 인류가 인터넷 연결 세상을 처음 접했을 때와 달리 지금은 통찰력을 발휘할 수 있습니다. IoT 환경이 위험을 수반하고 있으며 기업과 사용자가 표적이 될 것임을 우리는 경험을 통해 알고 있습니다. 현재 더 큰 위험은 공격자의 집요함과 IoT(와 IoE)가 본격화되는 속도를 과소평가하는 것입니다.

위협 정보

Cisco 보안 연구 팀은 가장 큰 규모의 텔레메트리 데이터를 토대로 2014년 상반기의 보안 인사이트(insight)를 수집하고 분석했습니다. Cisco의 보안 전문가들은 향후 발생할 수 있는 범죄 행위를 파악하고 위협을 감지할 수 있도록 악성코드 트래픽 및 발견된 기타 위협을 지속적으로 연구하고 분석합니다.

공격의 패러다임 변화:내부 조명



*Cisco 2014 Annual Security Report(연례 보안 보고서)*에 수록된 위협 정보 중에는 최근 실시된 "인사이드 아웃" 프로젝트의 주요 결과가 포함되어 있습니다. 이 프로젝트에서 Cisco 보안 연구 팀은 기업 네트워크의 내부에서 일어나는 DNS 조회를 조사했습니다.[8]

Cisco 보안 연구 팀은 샘플 네트워크의 100%에서 악성 트래픽을 확인했습니다.[9]

Cisco 연구 팀은 관찰 내용을 토대로 이번 조사 대상인 기업들의 네트워크가 뚫린 것이 꽤 되었고 핵심적인 침투 사례는 감지되지 않았다는 것을 밝혀냈습니다.

Cisco는 현재 진행 중인 인사이드 아웃 프로젝트에서 추가로 밝혀진 사실을 이 보고서에서 소개합니다. 이 정보는 Cisco의 위협 연구 팀이 2014년 초부터 일부 고객 네트워크로부터 수집한 데이터 분석 자료를 검토하여 얻은 것입니다. 연구 팀은 총 자산 규모 4조 달러 이상이고 2013년 수익이 3천억 달러가 넘는 다국적 대기업 16곳을 면밀히 조사했습니다. 이번 분석을 통해 이들 기업과 악성 트래픽을 연결 짓는 3가지 중요한 사실이 확인되었습니다.

DDNS 요청

위협 설명

DDNS는 대개 합법적인 용도로 쓰이는 시스템입니다. 즉, 가정 사용자가 예를 들어 homeserver.isp.com과 같은 정적 FQDN(fully qualified domain name)을 인터넷 통신 사업자(ISP)가 동적으로 지정하는 IP 주소 풀 또는 번호에 매핑할 때 사용됩니다.

안타깝게도, DDNS는 다른 합법적인 용도로 개발된 많은 기술 및 기능처럼 공격자들이 애용하는 기술이 되었습니다. 그 이유는 DDNS가 봇넷과 기타 공격 인프라가 탐지 및 후속 조치를 견뎌낼 수 있도록 해주기 때문입니다. name-services.com과 같은 DDNS 서비스 제공자를 통한 도메인 요청량이 비정상적으로 많다면 해당 기업의 네트워크가 감염되었을 가능성이 있습니다. DDNS 제공자에 대한 쿼리 중 상당수 또는 전부가 합법적이지만, 이러한 요청이 정말 합법적인 것인지 항상 주의 깊게 살펴봐야 합니다.

조사 결과

이번 "인사이드 아웃" 프로젝트를 통해 2014년에 관찰한 고객 네트워크 샘플 쿼리의 약 70%(66.67%)가 DDNS에 대해 DNS 쿼리를 실행한 것으로 나타났습니다. (참고: Cisco 보안 연구 팀은 고객 네트워크 분석 샘플 크기가 늘어나면 이 비율이 증가할 것으로 예상합니다.

Cisco에서는 이제 막 이 새로운 범주를 감염지표로 추적하기 시작했습니다. 감염지표란 시스템에서 관찰되는 대개는 미묘한 이벤트 또는 아티팩트로서 시스템의 다른 감염지표와 연계할 경우 공격의 가능성을 나타내는 것입니다. 앞서 언급한 것처럼, 개별 고객이 DDNS 제공자를 이용하는 악성코드에 감염되었다는 의미는 아닙니다. 그러나 Cisco는 이 고객들에게 DDNS 요청을 더 주의 깊게 살펴서 합법적인 비즈니스 목적에 따라 실행되는지 확인하도록 조언했습니다.

MiTB 기능을 갖춘 악성코드 관련 사이트에 대한 요청

위협 설명

Palevo, SpyEye, Zeus는 MiTB(man-in-the-browser) 기능을 갖춘 악성코드군입니다. Palevo, Zeus, SpyEye에 감염된 호스트에 대한 DNS 조회는 매우 심각한 위협으로 간주됩니다. 이 봇넷은 인스턴트 메시지, P2P(peer-to-peer) 네트워크, 이동식 드라이브를 통해 유포됩니다. 이들은 DDoS(distributed denial of service) 공격을 하고, 또한 실시간으로 생성되어 기존 폼에 추가되는 필드에서 정보를 훔쳐내는 데 이용됩니다. Palevo, Zeus, SpyEye가 조명을 받는 이유는 Windows 운영 체제의 브라우저에서 온라인 서식에 입력되는 금융 정보 및 기타 정보를 노리는 악성코드 유형이기 때문입니다.

조사 결과

2014년에 관찰한 고객 네트워크의 90% 이상(93.75%)이 악성코드를 호스팅하는 웹사이트에 트래픽을 보낸 것으로 나타났습니다. 구체적으로 설명하자면, 네트워크에서 Palevo, Zeus, SpyEye 악성코드의 배포와 관련 있거나 이 악성코드에 감염된 것으로 알려진 IP 주소의 호스트 이름에 DNS 요청을 했습니다.

관리 프로토콜과 관련된 FQDN, 사이트, 호스트에 대한 DNS 요청

위협 설명

악의적인 단체는 정보를 훔칠 때 자신의 흔적을 감추기 위해 보안 암호화된 통신 채널 또는 데이터 전송 채널을 이용할 수 있습니다. IPsec(IP Security) VPN, SSL(Secure Sockets Layer) VPN, SSH(Secure Shell) 프로토콜, SFTP(Simple File Transfer Protocol), FTP, FTPS(FTP Secure) 등이 해당됩니다. 기업은 정기적으로 이러한 통신을 모니터링하고 검증해야 합니다. 이러한 유형의 사이트는 암호화된 채널을 통해 들키지 않고 데이터를 추출하는 데 이용될 수 있습니다.

조사 결과

2014년에 관찰한 고객 네트워크의 40% 이상(43.75%)이 IPsec VPN, SSL VPN, SSH, SFTP, FTP, FTPS와 같은 서비스를 제공하는 기기와 관련된 사이트 및 도메인에 대해 DNS 요청을 보낸 것으로 나타났습니다.

Cisco 연구 팀은 기업 네트워크로부터의 DNS 조회를 이용하여 가능한 데이터 유출 및 취약점의 스냅샷을 생성했습니다. Cisco 보안 전문가들이 차단 목록을 토대로 정보를 분석하고 사이버 공격 트렌드, 업종에 따른 특별한 취약점, 공격자 및 표적화된 정보에 영향을 줄 만한 지정학적 요인을 관찰했습니다. 인사이드 아웃 프로젝트에 참여한 Cisco 고객에게는 Cisco에서 작성한 *External Cyber Threat Report(외부 사이버 위협 보고서)*를 교부했습니다.

주목할 지정학적 트렌드

동유럽과 중동의 정세로 인해 사이버 환경에 전 세계 기업, 정부, 기타 기관 및 개인 사용자에게 위험 지형이 확대될 새로운 트렌드가 형성되었다고 Cisco의 사이버 보안 전문가들은 지적합니다.

우크라이나의 정치적 불안은 일련의 DDoS 공격 및 웹사이트 변조 사건을 낳았으며, 이는 오프라인 활동을 보완하기 위한 시도로 보입니다. 크림 반도와 키예프의 혼란 때문에 수 개월 또는 수 년간 드러나지 않고 있었던 우크라이나 네트워크를 표적으로 한 정교한 첩보용 악성코드(일명 Ouroboros 또는 Snake)가 발각되었습니다.

중동에서는 이라크 북부와 서부를 장악한 이라크-레반트 이슬람 국가 세력이 사보타주와 심리전에 소셜 미디어를 이용하고 있습니다.

세계 일부 지역에서 오랫동안 계속되고 있는 종족 및 종교 간 분열이 앞으로 더욱 심화될 것이며, 이미 정부 및 민간 분야 공격자들의 사이버 전술에 주도적으로 영향을 미치기 시작했습니다. 2014년 하반기에 치열한 터키 대선, 미국 중간 선거, 서방의 아프가니스탄 병력 철수가 이루어지면서 글로벌 사이버 환경 전반에 새로운 파장을 일으킬 것으로 예상됩니다.

CISCO 2014 MIDYEARSECURITY REPORT 공유

웹 익스플로잇: 여전히 강세인 Java 공격

Java 프로그래밍 언어 익스플로잇이 Cisco® FireAMP 지능형 악성코드 탐지 플랫폼이 모니터링하는 IOC 중에서 여전히 선두를 차지하고 있습니다. 2014년 상반기에도 난공불락으로 보이는 강세를 이어갔습니다.

그림 1

2014년 중기 애플리케이션 감염 점유율

출처: Cisco® FireAMP[10]

2013년 11월 기준으로 Java 공격이 IOC의 91%를 차지했습니다(***Cisco 2014 연례 보안 보고서).*** 2014년 5월에는 이 수치가 93%로 약간 상승했습니다. Java의 광범위한 공격 표면과 공격 성공률 때문에 공격자들 사이에서 높은 인기를 구가하고 있습니다. (Java 문제 및 그 완화 방법에 대한 자세한 내용은 ***Cisco 2014 연례 보안 보고서[11]을 참조하십시오.)***

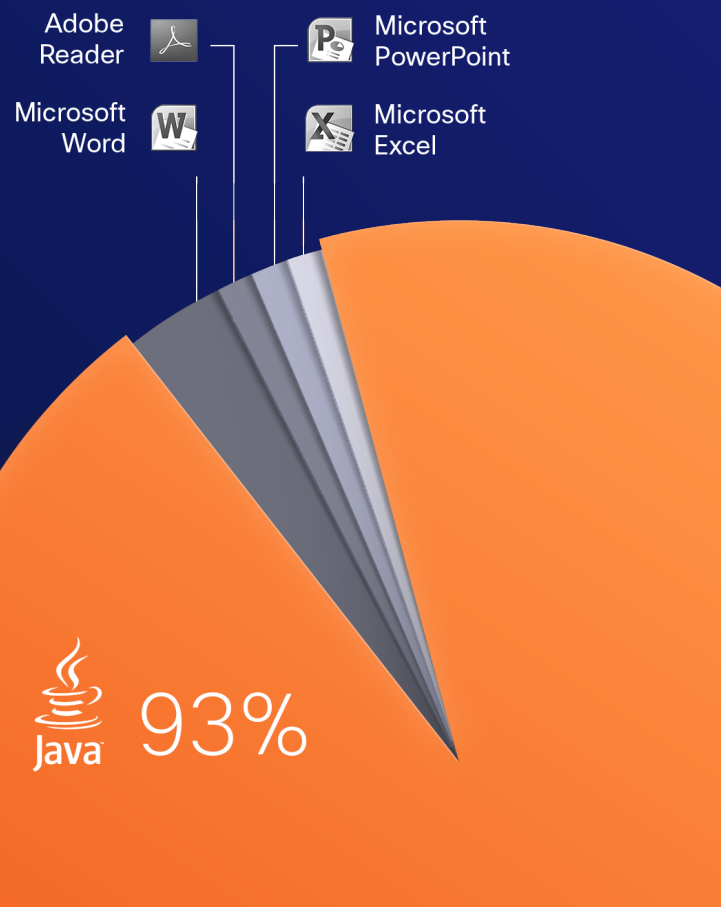


그림 2

Java 웹 악성코드 발생 (2014년 1월 - 5월)

출처: Cisco Cloud Web Security

Java 웹 악성코드 발생은 2014년 3월에 절정에 달해 전체 웹 악성코드의 약 10%를 차지했습니다.

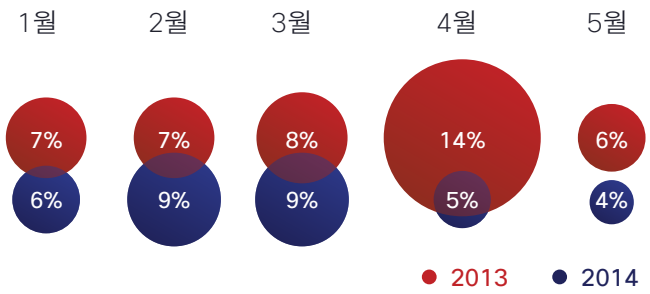


그림 3

Java, PDF, Flash 악성코드 발생 (2014년 1월 - 5월)

출처: Cisco Cloud Web Security

Java, Flash, Adobe PDF 모두 범죄자들에게 인기 높은 공격 벡터입니다.

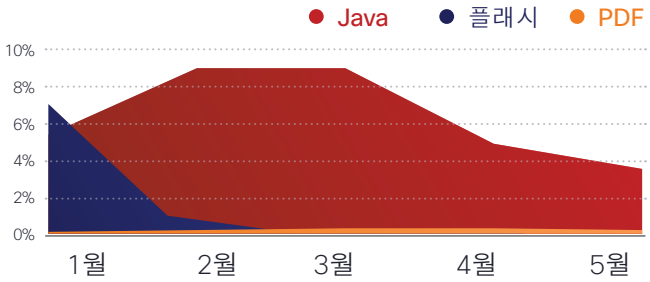
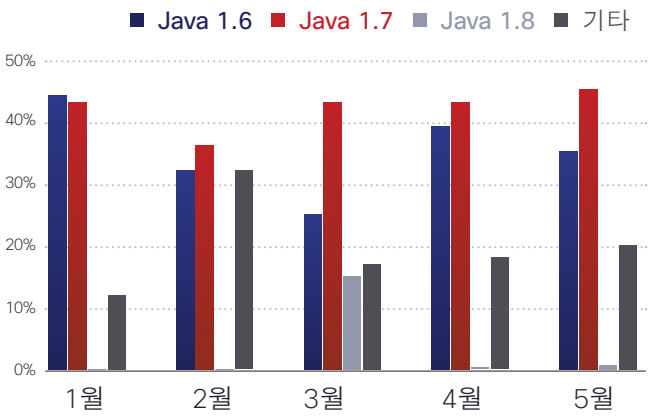


그림 4

버전별 Java 악성코드 발생 (2014년 1월 - 5월)

출처: Cisco Cloud Web Security

이전 버전의 Java, 특히 Java 6와 Java 7에 대한 익스플로잇 공격이 여전히 두드러졌습니다. 3월에 Java 8이 출시되면서 이 최신 버전의 웹 악성코드 발생이 급증했습니다. 그러나 4월 들어서 Java 8 악성코드 발생이 크게 감소했고 이 추세는 5월까지 이어졌습니다. Microsoft Silverlight와 같은 비 Java 계열 벡터를 가장 먼저 집중적으로 노리는 익스플로잇 킷이 늘어남에 따라 (이전보다 강력한 보안 제어 기능을 갖춘) Java 8 대신 공격하기 쉬운 다른 소프트웨어로 초점이 이동할 가능성도 있습니다.



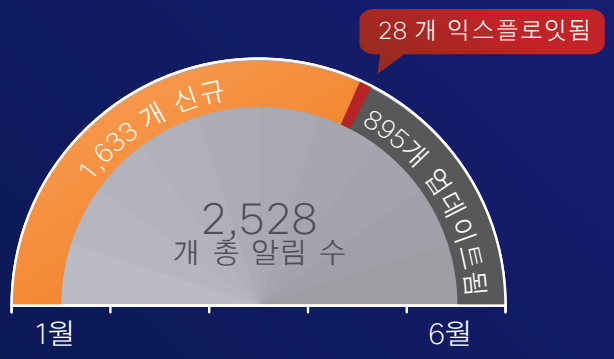
취약점 업데이트: 가장 보편적인 익스플로잇에 집중

그림 5

경고 메트릭(2014년 1월 - 6월)

출처: Cisco Intellishield®

Cisco는 2014년 1월 1일부터 6월 30일까지 알려진 보안 취약점에 대한 멀티벤더 경고 수천 건을 게시했습니다. 다소 불안감을 일으킬 만한 수치이지만, 그중에서 극히 심각한 취약점의 수는 약 1%에 불과했습니다. 이 기간에 2,528개의 신규 취약점 경고가 게시되었지만, 보고서 발표 후에 적극적인 공격 활동이 일어난 것은 28개에 불과했다고 Cisco 연구 팀은 밝혔습니다.



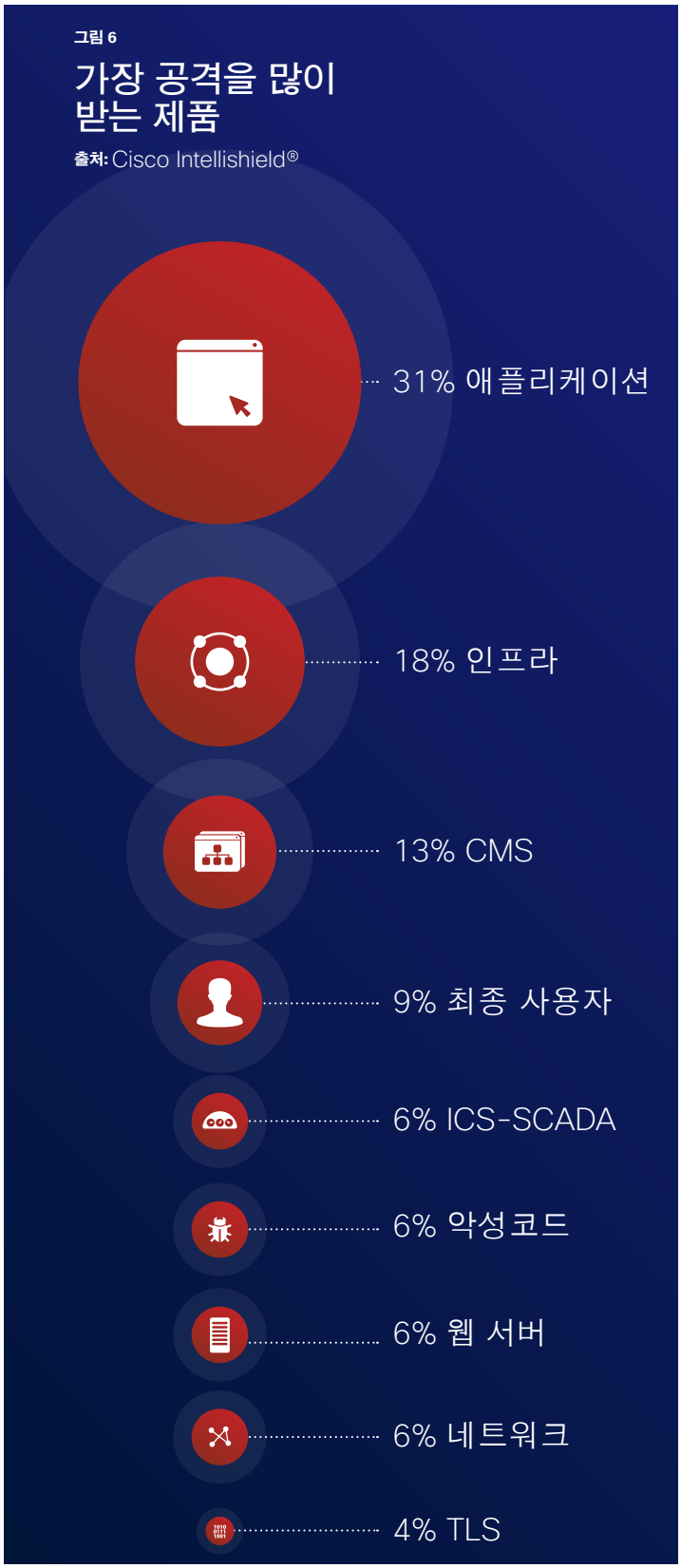
공격자들은 보편적인 취약점을 집중적으로 공략합니다. 즉 "연구 개발"을 통해 공격하기 쉬운 "약한 고리"를 찾아냅니다. 그런 다음 성공적인 익스플로잇은 익스플로잇 킷에 통합하여 지하 경제에서 판매합니다. Java와 Silverlight 프로그래밍 언어는 무수히 많은 대중적인 익스플로잇 킷을 양산하는 대표적인 취약점입니다. (15페이지, 웹 익스플로잇: 여전히 강세인 Java 공격 및 33페이지, 익스플로잇 킷: 본격적으로 시작된 경쟁을 참조하십시오.)

취약점 보고서가 게시되면 보안 전문가와 언론 매체는 제로데이 취약점에 주목하게 됩니다. 관심이 집중되는 그러한 소식에 대처하는 것이 시급하다고 생각하기 때문입니다. 그러나 기업은 범죄자들이 가장 적극적으로 이용하는 소수의 취약점을 해결하는 데 우선적으로 시간과 예산을 투자해야 합니다. 다른 취약점은 좀 더 통상적인 프로세스를 통해 관리할 수 있습니다.

그림 6

가장 공격을 많이 받는 제품

출처: Cisco Intellishield®



기업에서는 "긴급 패치 프로세스"를 마련하고 표준 패치 프로세스와 함께 실시하는 것이 바람직합니다. 표적이 된 우선적 취약점을 신속하게 해결하고, 덜 시급한 다른 취약점은 정기적인 유지 보수 및 패치 프로세스에 포함시켜 해결할 수 있습니다. 그러면 더 정확한 위험 관리가 가능해집니다. 이것이 모든 패치를 설치하려 하거나 정기 유지 보수 시점까지 아예 설치하지 않는 것보다 나은 방법입니다. 긴급 패치 프로세스를 효과적으로 운영하려면 긴급한 취약점을 식별할 수 있는 강력한 보안 인텔리전스가 필요합니다.

그림 6은 2014년 상반기에 가장 많은 익스플로잇 공격이 있었던 제품들입니다. 그림 7은 CVSS(Common Vulnerability Scoring System)를 통해 확인한, 가장 보편적으로 공격당한 취약점들입니다.

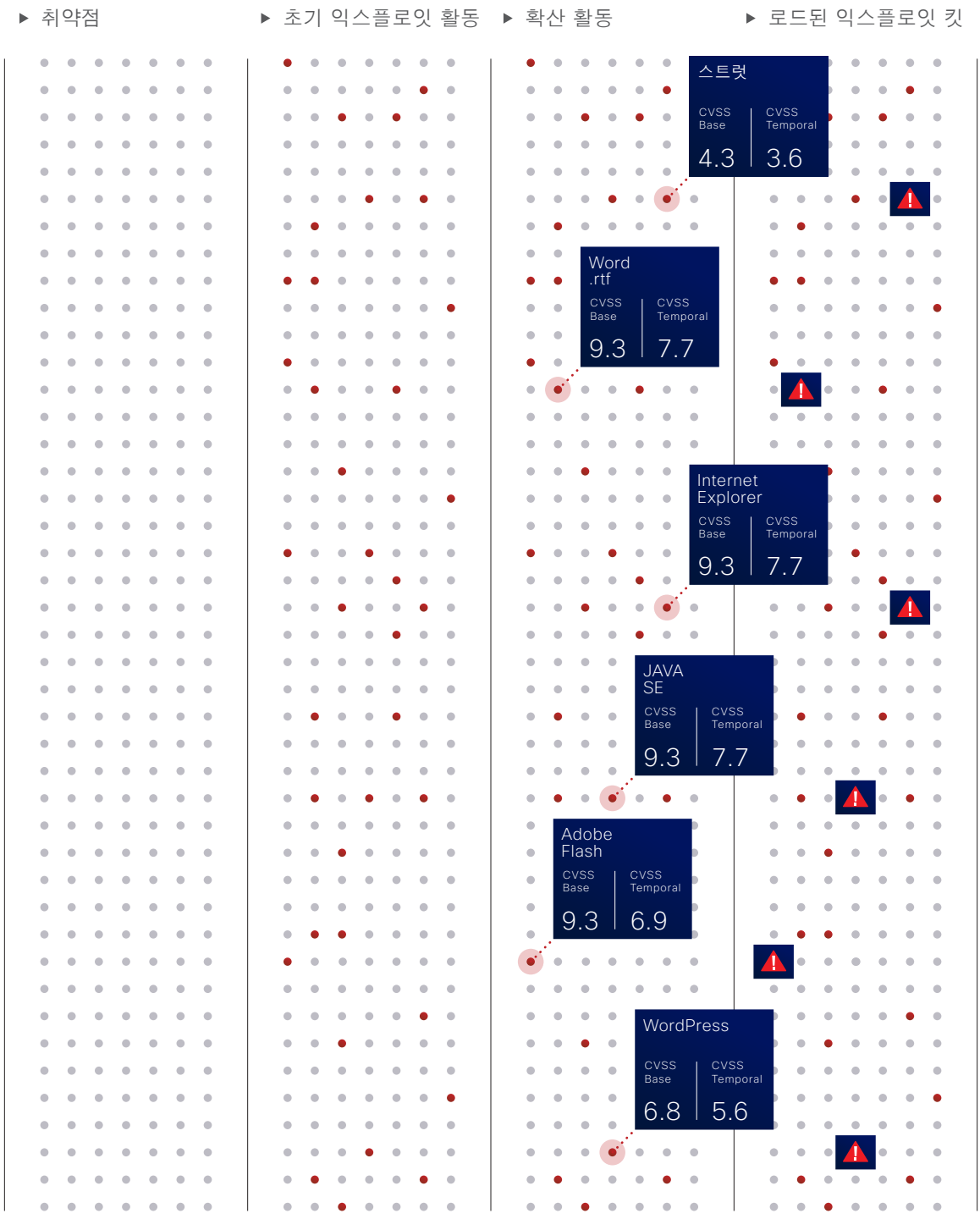
CVSS 차트의 "Urgency" 점수는 해당 취약점이 적극적인 공격을 받고 있다는 것을 나타내므로 유용합니다. 이는 적극적인 익스플로잇 공격을 나타내는 "Temporal" 점수와 상통합니다. 또한 기업은 공격 대상이 된 제품의 목록을 통해 어떤 제품을 현재 사용 중이며 그중에서 모니터링 및 패치 적용이 필요한 제품을 파악할 수 있습니다.

한편 그림 7의 취약점은 해당 관찰 기간에 초기 익스플로잇 활동 징후를 나타낸 것입니다. 이러한 취약점 중 상당수는 아직 주류는 아니라는 의미이며, 이것은 해당 공격 코드가 아직은 대중적이라는 의미는 아닙니다.

그림 7

공격 빈도가 가장 높은 취약점

출처: Cisco Intellishield®



Heartbleed: 걱정할 문제는 아님

일부 기업은 (OpenSSL 암호화 라이브러리의 보안 취약점의) "하트블리드 버그(Heartbleed bug)"에 노출되지 않았습니다. 이 취약점이 없는 오래된 버전의 OpenSSL을 사용했기 때문입니다.[12] 이 취약점은 TLS 하트비트 확장기능(RFC6520)을 구현하여 TLS 암호화 통신에서 보안 키 또는 개인 정보의 유출을 가능하게 합니다.[13]

그러나 이 기업들은 2014년 1월부터 4월까지 하트블리드와 *무관한* TLS 및 인증서 검증 취약점이 16개 발견되었다는 사실에 주목해야 합니다.

이 취약점 때문에 위험에 처할 수 있습니다. 또한 Cisco 보안 전문가들은 모든 사용자가 하트블리드로 인한 위험에 노출되었을 가능성이 있다고 생각하고 암호 변경, 웹 계정 폐쇄와 같은 적절한 조치를 취할 것을 권장합니다.[14]

하트블리드가 발견된 후 OpenSSL 프로젝트(OpenSSL.org)는 OpenSSL 소프트웨어의 몇 가지 결함을 추가로 보고했습니다. 그중에는 "공격자가 DoS 상태를 만들거나 경우에 따라서는 원격 코드 실행을 허용하는 것도 있었습니다."[15] 이러한 결함 중 일부는 오랫동안 간과되었던 약점입니다. 예를 들어, 일본의 보안 연구자가 발견한 CCS 인젝션 취약점은 16년 된 OpenSSL 소프트웨어 보안 결함으로서 공격자가 인터넷을 통해 전송되는 암호화된 데이터를 가로채 해독하는 것을 가능하게 합니다.[16]

산업별 위험 보고서: 일부 업종의 이례적인 증가

고수익 업종으로 꼽히는 제약 및 화학이 2014년 상반기에도 웹 악성코드 발생 위험이 가장 높은 3대 업종에 포함되었습니다. 2013년에는 1위를 기록한 바 있습니다.[17] 항공 산업도 Top 5에 다시 올랐는데, 이번에는 3위에 올랐습니다.[18] 항공 회사들이 보유한 지적 재산의 가치를 고려하면 놀라운 일이 아닙니다.

한편 현재 1위에 오른 언론 및 출판은 Cisco 보안 연구팀이 2008년부터 이 데이터를 취합하면서 관찰했던 평균적인 웹 악성코드 발생률보다 훨씬 높은 수치를 기록했습니다.

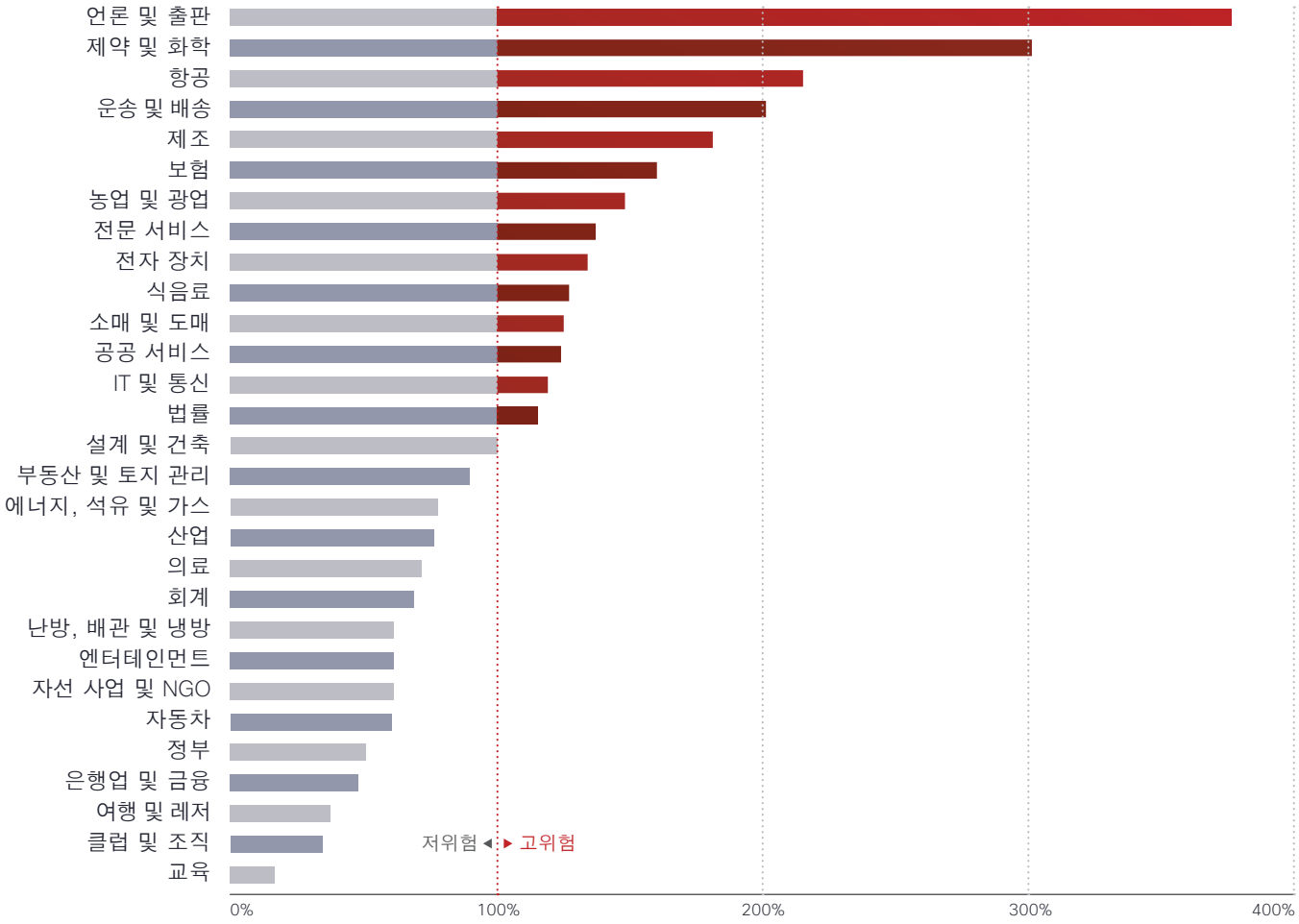
2014년 동계 올림픽, 아카데미 시상식 등 이목이 집중되는 행사 또는 말레이시아 항공 370편의 미스테리, 한국의 여객선 침몰 사고와 같은 대형 뉴스를 악용한 익스플로잇 및 기타 스캠이 단행된 것이 언론 및 출판 업계에서 악성코드 발생이 증가한 원인일 것입니다. 이러한 스캠은 사람의 "취약한 부분"을 노립니다. 즉 사용자는 주의를 끄는 헤드라인에 속아 악성코드를 호스팅하는 사이트를 클릭하곤 합니다.

크고 작은 언론 및 출판 사이트는 세계 각처의 개인 소비자, 기업, 기관으로부터 다양한 트래픽이 유입될 수 있습니다. 게다가 수익 때문에 광고에 대한 의존도가 높습니다. 특히 이 점 때문에 악성 광고의 성장이 2014년 상반기 언론 및 출판 업계의 웹 악성코드 발생률 증가에 다소 영향을 미쳤다고 볼 수 있습니다. (35페이지, 악성 광고: 인터넷 경제의 교란자를 참조하십시오.)

그림 8

업종별 웹 악성코드 발생 위험, 1H14

출처: Cisco Cloud Web Security



Cisco의 보안 연구 팀은 업종별 악성코드 발생 현황을 알아보고자 Cisco Cloud Web Security를 통해 프록시하는 모든 기업의 악성코드 발생률 중앙치(median)와 이 서비스를 통해 프록시하는 특정 업종에 속한 모든 기업의 악성코드 발생률 중앙치를 비교했습니다. 업종의 발생률이 100%보다 높으면 평균적인 웹 악성코드 발생 위험보다 높고, 100% 미만이면 위험도가 낮은 것입니다. 예를 들어 발생률이 170%인 기업은 중앙치에 해당하는 곳에 비해 위험도가 70% 더 높습니다. 반면 발생률이 70%인 기업은 중앙치의 기업보다 위험도가 30% 낮습니다.

지역별 악성코드 발생률

Cisco 보안 연구 팀은 최초로 각 지역의 업종별 웹 악성코드 발생 위험 데이터를 제시합니다. 지역은 AMER(북미, 중미, 남미), APJC(아시아 태평양, 중국, 일본, 인도). EMEAR(아프리카, 유럽, 중동)로 구분했습니다.

AMER 지역(그림 9)에서는 항공 분야가 다른 업종을 큰 차이로 누르며 선두에 올랐습니다.

특정 지역의 업종별 위험은 해당 지역의 GDP에 좌우됩니다. 일반적으로 해당 업종의 상품 및 서비스 또는 지적 재산의 가치가 높을수록 악성코드 발생 위험이 높습니다.

어떤 업종은 그 분야의 생산량이 없는 지역에서 낮게 나타날 수도 있습니다. 이는 농업, 식음료, 운송 업계에 흔히 나타나는 "팜투테이블(farm-to-table)" 리스크의 원인입니다. 또한 EMEAR에서 소매 식음료 업종의 웹 악성코드 발생 건수가 가장 높은 이유일 수도 있습니다. 이 지역은 최근 가뭄, 홍수, 사회 불안정의 요인이 주민들의 기본 생필품 및 인프라 이용에 영향을 미쳤습니다.

발생과 감염

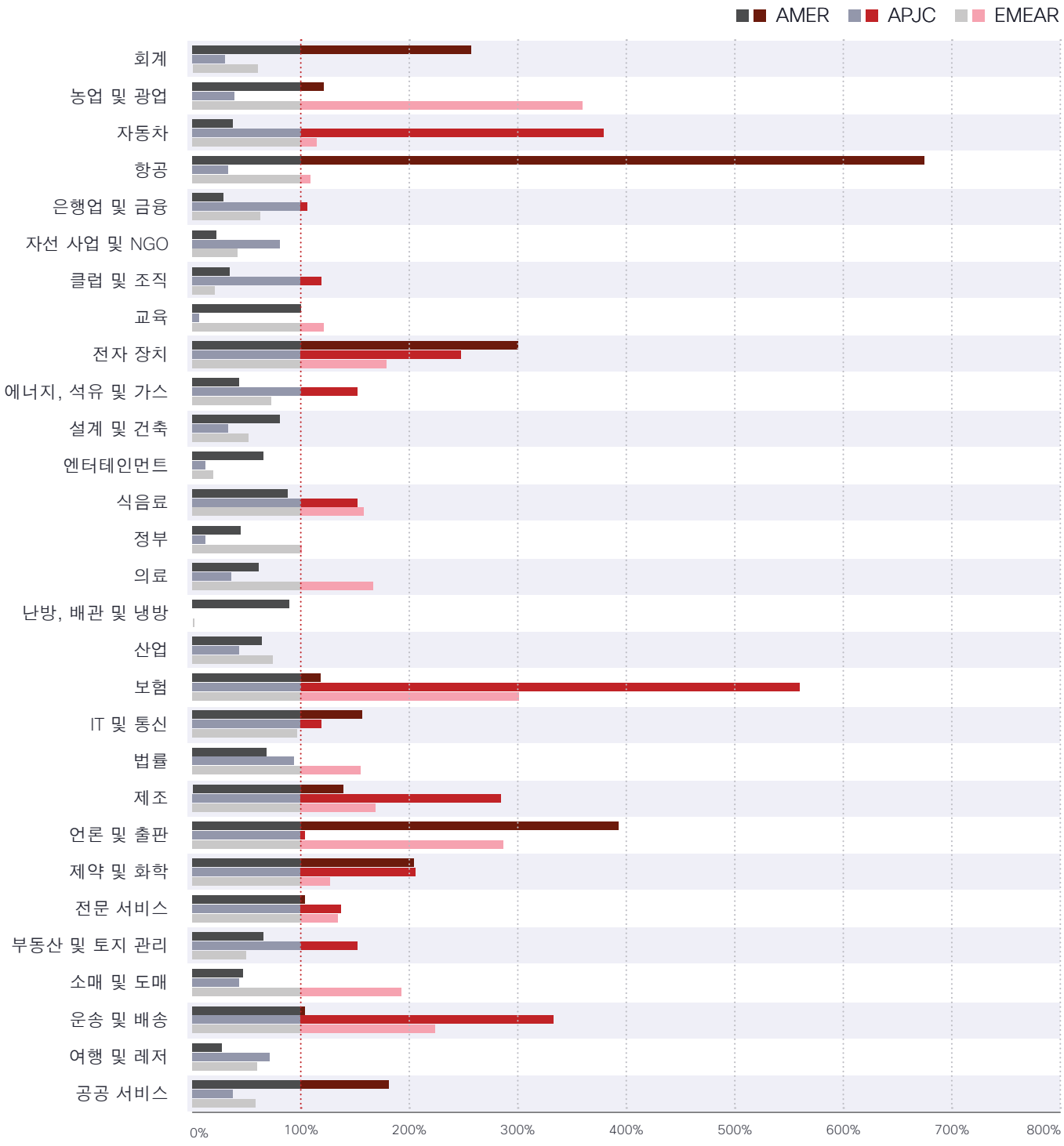
"발생(encounter)"이란 악성코드가 차단된 경우를 의미합니다. "감염(compromise)"과 달리 사용자는 바이너리 파일이 다운로드되지 않았기 때문에 발생 단계에서 감염되지 않습니다.

APJC에서는 최고 위험 업종이 보험이었고 제약 및 화학, 전자 업종이 그 뒤를 이었습니다. APJC 지역에서 최근 발생한 지진, 쓰나미와 같은 대형 재해, 2011년 일본의 원자력 발전소 사고 및 그에 따라 보험 시장이 겪은 압박이 보험 업계가 공격자의 주요 표적이 된 이유로 볼 수 있습니다. 또한 보험 업종이 주요 기업 및 기관의 서비스 제공자라는 사실을 고려하면, 공격자들이 보험사 고객의 기밀 정보를 빼내거나 고객사의 네트워크 및 데이터 센터에 침투할 경로를 찾기 위해 보험사를 공격한다는 추정도 가능합니다.

그림 9

각 지역의 업종별 웹 악성코드 발생 위험

출처: Cisco Cloud Web Security



5대 고위험 업종 지역별

그림 10에 AMER, APJC, EMEAR, 각 지역의 5대 고위험 업종의 실태가 자세히 나타나 있습니다. 모든 업종에서 iFrame과 악성 스크립트가 주를 이루지만, 세 지역 모두 특정 업종을 겨냥한 공격에 대한 의존도가 높은 것으로 보입니다. APJC의 운송 및 배송 업계에서는 사용자의 신뢰 관계를 노리는 스캠, 피싱, 클릭 사기가 빈번합니다.

세 지역 모두 랜섬웨어(Ransomware), 스캐어웨어(Scareware), 바이러스, 웜과 같은 기술을 구사하면서 5대 고위험 업종을 공격하는 시도도 드물게 나타납니다. 모바일 웹 악성코드 발생도 세 지역 모두 낮은 수준입니다.

이 차트의 내용은 웹 기반 위협의 유형보다는 Cisco Cloud Web Security 데이터에 기초하여 웹 악성코드 차단(즉, 발생)이 일어난 위치를 중심으로 작성된 것입니다.

그림 10

업종별 웹 악성코드 위험

출처: Cisco Cloud Web Security

스팸 업데이트: “라이프 이벤트” 스팸의 확산

스팸 개발자들은 지금까지 수신자가 (대개 악성코드 또는 감염된 웹사이트로 연결되는) 메시지를 열고 링크를 클릭하도록 속이기 위해 사회공학적 수법을 구사해 왔습니다. 택배 배송 또는 긴급한 세금 문제로 위장하는 것이 대표적인 수법이지만, 이제 보안 전문가들은 감정을 이용하는 “라이프 이벤트” 또는 “불행”과 관련한 스팸이 증가하는 추세라고 지적합니다.

예를 들어, “라이프 이벤트” 스팸은 생명을 위협하는 질병의 치료나 회복을, “불행”과 관련한 스팸은 주택 압류, 파산 등을 언급하기도 합니다. 둘 다 긴급 택배 배송 메시지보다 훨씬 더 강력한 영향력을 수신자에게 발휘하여 메시지 클릭을 유도할 수 있습니다.

“라이프 이벤트”와 “불행”과 관련한 스팸은 보안 보호의 보편적인 약점을 노린 것입니다. 사회공학적 기법에 대비하도록 교육받은 사용자도 개인의 불행을 덜어준다는 내용에 반응을 나타내기 마련입니다.

여느 스팸과 마찬가지로 라이프 이벤트 스팸을 줄이기 위해서는 동적으로 업데이트되는 스팸 차단 기술을 사용해야 합니다.

더욱 민첩해진 스패머들, 성공률을 높이기 위한 접근 방식의 변화

스패머는 자신의 메시지를 차단하는 첨단 기술에 신속하게 대응합니다. 문구, 이미지, 도메인 이름을 바꿔 스팸 필터를 피합니다. 그리고 어떤 메시지의 실효성이 떨어지면 완전히 바꾸기도 합니다.

Cisco 보안 연구 팀은 네트워크 침투 또는 정보 도용의 기회를 노리는 스패머들의 새로운 전술을 고객에게 알리고자 스팸의 유형 및 그 진화 형태를 모니터링합니다. 스패머들의 전술 변화에 따라 Cisco 연구 팀이 특정 스팸 유형(예: 전자 결제에 대한 허위 공지)의 공격 범위에 대한 안내를 수십 차례 업데이트할 수도 있습니다.

평균 속도의 2배로 증가한 글로벌 스팸량, 일부 국가의 스팸량 급감

그림 11

글로벌 스팸량(2014년 1월 - 2014년 5월)

출처: Cisco Threat Intelligence Platform

글로벌 스팸량은 2013년에 전반적으로 감소했다가 지난 10월부터 다시 늘어나기 시작했습니다. Cisco 연구 팀에 따르면, 현재의 스팸량은 2010년 말 이후 최고 수준에 이르렀습니다. 2013년 6월부터 2014년 1월까지 평균 스팸량은 월 500억 건에서 1천억 건이었습니다. 그러나 2014년 3월 기준으로 월 2천억 건을 초과했고 이것은 평균 속도의 2배로 증가한 것입니다.[19]

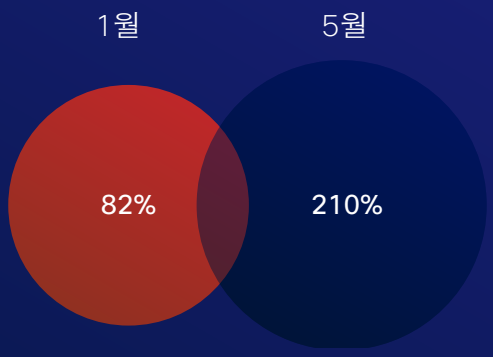
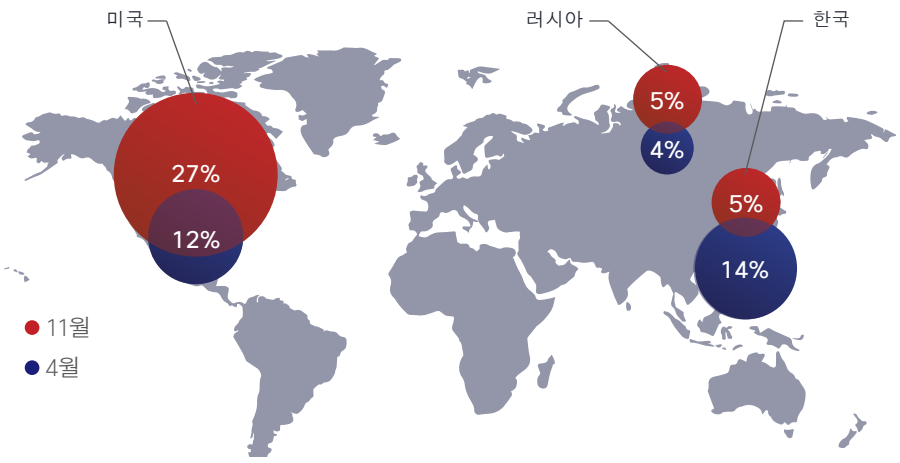


그림 12

국가별 스팸량 트렌드(2013년 11월 - 2014년 4월)

출처: Cisco Threat Intelligence Platform

또한 글로벌 스팸량이 증가했지만 모든 국가에서 늘어난 것은 아닙니다. 러시아와 미국은 2013년 11월 이후 스팸량이 급감했습니다. 한편 한국은 Cisco 보안 연구 팀이 모니터링한 다른 10개국에 비해 스팸량이 크게 증가했습니다.

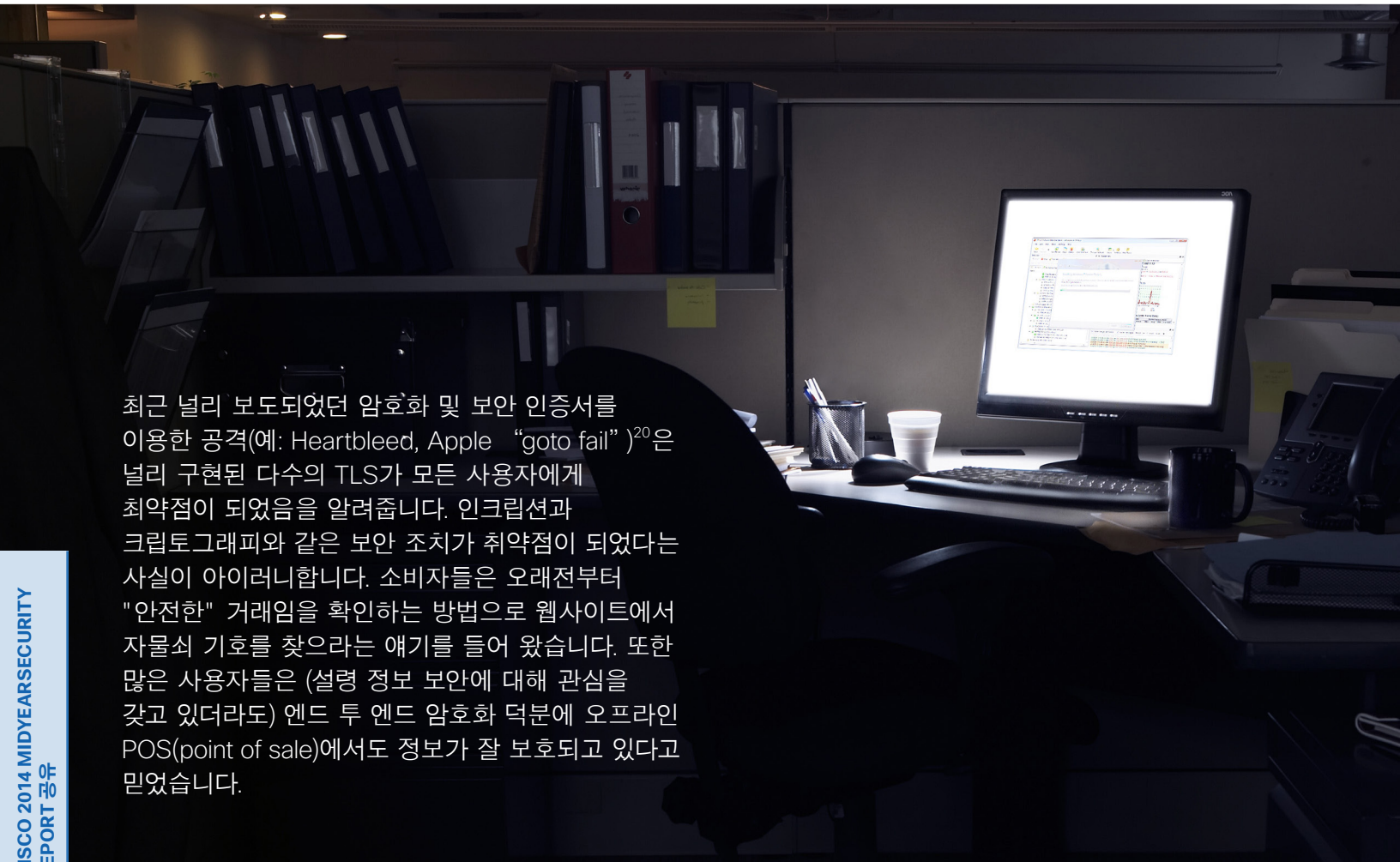


아르헨티나	2% | 7%	독일	2% | 6%
중국	11% | 5%	이란	1% | 4%
일본	2% | 7%	스페인	3% | 7%
영국	2% | 4%		

업계 트랜드

Cisco 보안 전문가들은 2014년 상반기에 관찰한 위협 및 보안 트렌드를 소개하고 분석할 뿐 아니라 향후 몇 개월에 대한 예측도 내놓습니다.

감염된 보안암호화 연결



최근 널리 보도되었던 암호화 및 보안 인증서를 이용한 공격(예: Heartbleed, Apple "goto fail")[20]은 널리 구현된 다수의 TLS가 모든 사용자에게 최약점이 되었음을 알려줍니다. 인크립션과 크립토그래피와 같은 보안 조치가 취약점이 되었다는 사실이 아이러니합니다. 소비자들은 오래전부터 "안전한" 거래임을 확인하는 방법으로 웹사이트에서 자물쇠 기호를 찾으라는 얘기를 들어 왔습니다. 또한 많은 사용자들은 (설령 정보 보안에 대해 관심을 갖고 있더라도) 엔드 투 엔드 암호화 덕분에 오프라인 POS(point of sale)에서도 정보가 잘 보호되고 있다고 믿었습니다.

그러나 지난 6개월간의 경험으로 볼 때, 사용자가 아무리 주의와 경계를 기울이고 얼마나 많은 보안 장치를 갖추더라도 통제 불가한 연결 취약점 때문에 여전히 심각한 위험에 처할 가능성이 있습니다.

결제 기능을 이용하는 기업이라면 감염된 보안 암호화 연결의 문제를 시급히 해결해야 합니다. 그러기 위해서는 암호화 및 기타 보안 제품을 상용화하는 업계 프로세스에 대한 더 면밀한 점검이 요구됩니다.

CISCO 2014 MIDYEARSECURITY REPORT 공유

하트블리드 및 이와 유사한 사건들을 보면, 보안 암호화 연결 및 관련 기술을 이용하는 많은 기업은 다음과 같이 생각하고 있습니다.

- 표준 및 인기 오픈 소스 코드 기반의 암호화 프로토콜은 강력한 보안을 제공한다.
- 서드파티에서 제공한 코드를 비롯하여 보안 제품 및 서비스에 포함된 모든 소스 코드는 보안 전문가가 철저히 검증한 것이다.

둘 다 사실이 아니지만, 하트블리드와 같이 취약점 및 기타 보안 틈새을 이용하고 사용자의 신뢰를 악용하는 공격이 성공할 수 있는 빌미를 제공합니다.

업계 프로세스를 개선하는 것은 쉽지 않은 일입니다. Cisco 보안 전문가들에 따르면, 현재의 OpenSSL은 올바르게 구현하고 취약점을 테스트하기에 너무 복잡하고 까다롭습니다. 현재의 오픈 소스 및 전용 코드 검증 프로세스는 더 충실한 모델이 필요하지만, 누가 그러한 모델을 개발하고 관리할 것인가는 해결되지 않은 문제입니다. 한편 보안 커뮤니티는 무너진 CA(certificate authority) 시스템을 바로잡을 수 있느냐를 놓고 논쟁이 벌어지고 있습니다.

보안 업계에서는 간소화가 관건입니다. 인증할 코드의 양을 최소화하는 것이 안전한 구현을 위한 중요한 단계입니다. Cisco 보안 전문가들은 오픈 소스 SSL/TLS 보안 라이브러리 개선은 적어도 다음 사항을 포함해야 한다고 생각합니다.

- 프로토콜 및 그 구현의 복잡성 완화
- 코드가 올바르게 구현되었고 어떠한 취약점도 없으며 숨겨진 결함이 없음을 검증
- 자격을 갖춘 전문가가 코드를 테스트하고 검증했음을 보장

하트블리드와 같은 최근 사건에서 비롯된 긍정적 변화: 개발자 커뮤니티의 많은 이들이 이제 능동적인 대응적 관점에서 코드를 조사하면서 결함을 찾아 해결하고 있습니다. Linux Foundation도 최근 Core Infrastructure Initiative를 조직했다고 밝혔습니다. 이는 "기술 기업들이 공조하여 지원이 필요한 오픈 소스 프로젝트를 찾아내 재정적으로 지원하고 개발자들이 오픈 소스의 성공을 안겨다 준 커뮤니티의 원칙을 준수하면서 지속적으로 개발할 수 있도록 지원하는 데 목적이 있습니다."[21] OpenSSL은 Core Infrastructure Initiative의 재정 지원 대상으로 검토 중인 첫 프로젝트 중 하나입니다. Cisco는 이 이니셔티브의 설립 후원사 중 하나입니다.

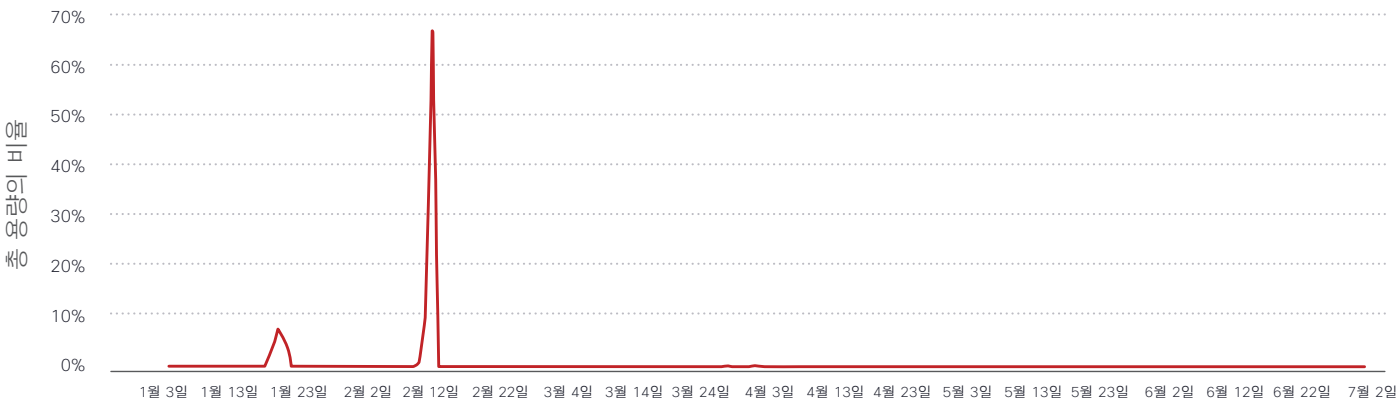
증폭 공격: NTP를 이용한 공격 수법의 등장

Cisco의 보안 전문가들은 *Cisco 2014 연례 보안 보고서*에서 DDoS 공격, 즉 DNS 증폭 수법의 공격이 2014년에도 기업에게 가장 심각한 보안 문제가 될 것이라고 경고했습니다.[22] 그러나 그전에도 Cisco 연구팀은 네트워크에 연결된 컴퓨터의 시간을 동기화하는 NTP가 보안 약점이며 증폭 DDoS 공격의 벡터가 될 수 있음을 주장한 바 있습니다. 이러한 예측의 근거는 갈수록 늘어나는 취약한 NTP 서버를 이용하도록 설계된 공격 툴이 해커들 사이에서 확산되기 시작했다는 사실입니다.[23]

그림 13

CloudFlare NTP DDoS 공격, 2014

출처: Cisco Threat Intelligence Platform

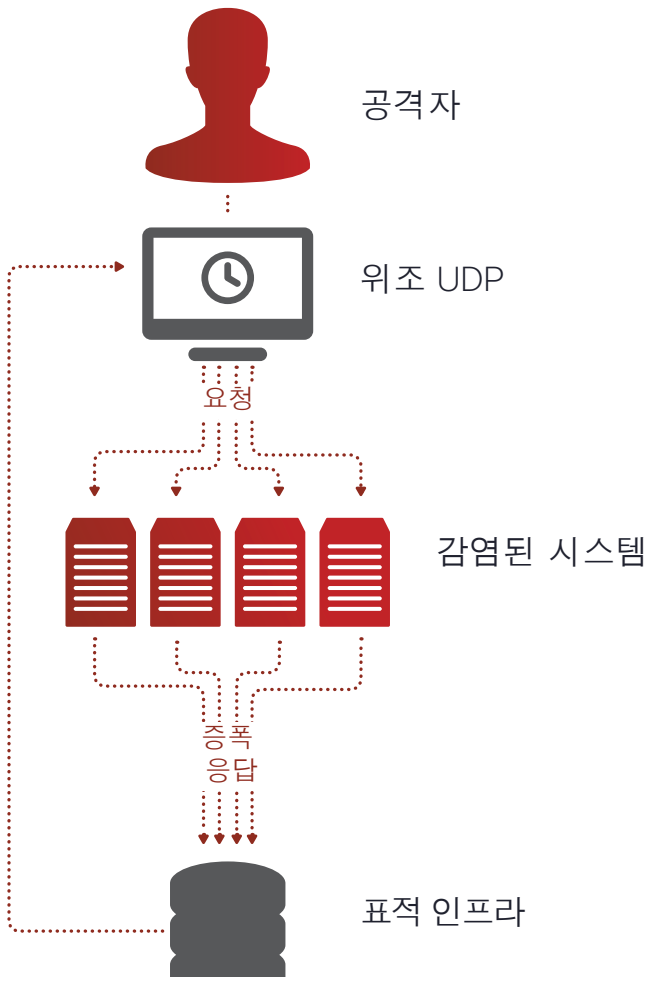


2014년 상반기에 발생한 NTP 증폭 공격 중 매우 심각했던 하나는 글로벌 DNS 제공업체인 CloudFlare의 한 고객을 겨냥한 것이었습니다(그림 13 참조). 2월에 일어났던 이 공격은 약 400Gbps의 UDP 트래픽을 생성하면서 절정에 달했습니다. 이는 2013년 3월, 공개된 DNS 리졸버 3만 개, 300Gbps를 대상으로 했던 Spamhaus DDoS를 능가하는 수준이었습니다.[24]

일부 공격자들이 실험적으로 NTP를 DDoS 공격 수단으로 이용하는 이유는 쉽게 이해할 수 있습니다. NTP 문제를 널리 알리기 위해 마련된 NTP 스캐닝 프로젝트인 OpenNTPProject.org는 취약한 NTP 서버를 1백만 대 이상 찾아냈습니다.[25] 이 서버들의 대역폭을 합하면 지금까지 확인된 어떤 DDoS 공격보다도 큰 규모입니다.

그림 14

NTP 공격의 실행



NTP 증폭 공격을 실행하려면 취약한 NTP 시스템에 작은 크기의 요청을 보냅니다. 이때 UDP 패킷의 주소를 위조하여 공격자가 멈추게 하려는 표적 시스템에서 그 요청을 보낸 것처럼 위장합니다. 이 UDP는 무상태(stateless)입니다. DNS 및 NTP 증폭 공격 모두 UDP 주소를 스푸핑하는 기능이 필수적입니다. 공격에 이용된 NTP 서버는 작은 크기의 요청에 대해 모든 정보가 포함된 매우 큰 용량의 응답을 보냅니다. 표적 시스템은 이를 감당하지 못하고 멈춥니다. (UDP 스푸핑을 방지하기 위한 업계 차원의 노력이 진행 중이며, 이는 더 지켜볼 필요가 있습니다.)

NTP 증폭 공격의 가능성을 방지하려면 공용 NTP 서버를 최신 버전의 NTP로 업그레이드해야 합니다. 이 보고서를 쓰는 시점에서 최신 버전은 4.2.7입니다. 이와 같이 업데이트하면 MON_GETLIST 또는 “monlist” 명령이 더 이상 지원되지 않습니다. 이는 NTP 서버가 최근에 상호 작용했던 시스템 600대의 주소를 반환하는 원격 명령입니다. 업그레이드하기 어려울 경우 NTP 구성의 *noquery* 옵션을 사용하여 monlist 쿼리를 막을 수 있습니다.

NTP 증폭 공격이 새로운 유형의 DDoS 공격일 수도 있지만, DNS 증폭은 앞으로도 많은 공격자가 애용하는 수단이 될 것입니다. Open Resolver Project는 2013년 10월 기준으로 심각한 위협인 개방형 리졸버가 2,800만 개에 달한다고 밝혔습니다.[26]

익스플로잇 킷: 본격적으로 시작된 경쟁

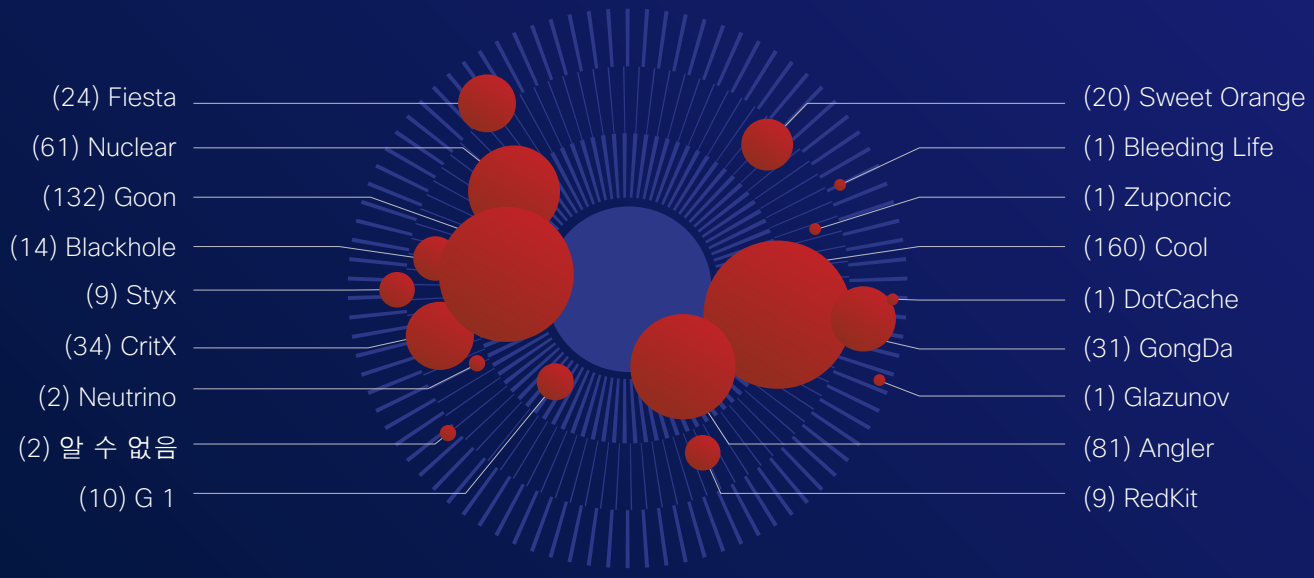
"블랙홀(Blackhole) 익스플로잇 킷을 개발하고 유포한 당사자로 알려진 '폰치(Paunch)' 라는 별명의 악성코드 거물"이 2013년 10월, 러시아에서 체포되고[27] 얼마 되지 않아 익스플로잇 킷 개발자들이 한때 그의 아성이었던 곳에서 쟁탈전을 벌이기 시작했습니다.

블랙홀은 명실공히 가장 광범위하게 사용되고 성공적으로 관리되었던 익스플로잇 킷입니다. 폰치와 블랙홀이 정부 당국의 단속을 받아 사라지자 공격자들은 새로운 익스플로잇 킷으로 관심을 돌렸습니다. 2014년 상반기에 많은 제품들이 최고의 자리를 차지하기 위해 각축을 벌였지만, 아직 일인자가 확실히 가려지지 않은 상황입니다.

그림 15

2014년 1월 이후 관찰된 익스플로잇 킷

출처: Cisco Threat Intelligence Platform



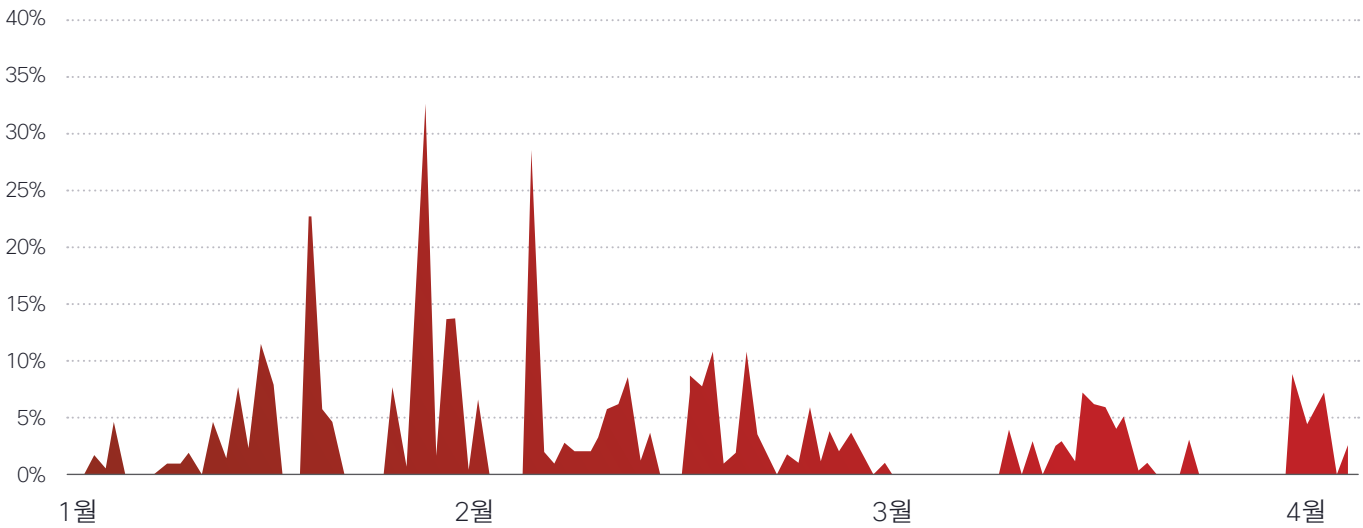
(공격 건수)익스플로잇 킷 이름

더욱 치열해진 경쟁에도 불구하고 익스플로잇 킷 수는 지난해 폰치가 체포된 이후 87%가량 감소했다고 Cisco 보안 연구 팀은 밝히고 있습니다(그림 16 참조).

그림 16

익스플로잇 킷 수 감소(2014년 1월 - 4월)

출처: Cisco Threat Intelligence Platform



또한 더 표적화되고 지능화된 공격에 익스플로잇 킷이 사용되고 있습니다. 즉 공격자들이 직접적인 인프라 침투 경로가 될 애플리케이션, 프로그램, 시스템의 취약점을 찾아내고자 특정 사용자를 공략하기 시작했습니다. 예를 들어, “LightsOut” 또는 “Hello” 익스플로잇 킷은 에너지 업계를 겨냥한 것입니다.

악성 광고: 인터넷 경제의 교란자

인터넷 광고 지출이 다른 모든 미디어 유형의 지출을 능가하고 있습니다.[28] 1994년 Hotwired의 간단한 배너 광고로 시작했던 인터넷 광고의 소박한 시작을 생각하면 20년 만에 엄청난 성장을 이룬 것입니다. 인터넷 광고는 사용자들이 불편하게 여기기도 하지만, 웹의 대부분을 무료로 이용할 수 있게 해준다는 점에서 중요합니다. 그러한 모델이 바뀌거나 사람들이 더 이상 인터넷 광고를 신뢰하지 않게 되면 인터넷 환경에서 그 파장은 엄청날 것입니다.

"악성 광고(malvertising)", 즉 악성코드 유포에 이용되는 온라인 광고는 그러한 모델과 사용자의 신뢰를 위협합니다. 모든 인터넷 사용자에게 피해를 주고 인터넷 경제를 교란시킵니다. Cisco 보안 전문가들에 따르면, 악성 광고는 공격 사슬의 전 범위에서 분업, 협업, 전문화가 이루어지면서 고도로 발전한 현대 사이버 범죄 경제의 진면목을 보여줍니다.

악성 광고가 더욱 보편화되고 있으며, 공격자들은 고도화된 방법으로 목표 대상을 대상으로 공격을 수행할 수 있습니다. 특정 시점에 특정 계층(예: 월드컵 경기를 시청하는 독일의 축구 팬들)을 표적으로 하려는 악성 광고주는 합법적인 광고 거래를 이용하여 목적을 달성할 수 있습니다. 합법적인 광고주와 마찬가지로 광고 거래의 게이트키퍼 역할을 하는 기업에 발생합니다. 광고비(1회당 2천 달러 이상)을 선불하고 최대한 서둘러 광고를 내보내도록 요구하여 광고 콘텐츠를 점검할 시간을 거의 또는 전혀 주지 않습니다.

악성 광고 피해자는 평소처럼 웹 서핑을 하다가 악성코드에 감염되므로 어디서 어떻게 감염되었는지 알 방법이 없습니다. 그 출처를 밝히는 것도 거의 불가능합니다. 악성코드를 배포한 광고는 오래전에 자취를 감추었기 때문입니다.

엄청난 폐해: 랜섬웨어에서 악성 광고의 역할

Cisco ***2014 연례 보안 보고서***에서 지적한 것처럼, 악성 광고는 랜섬웨어인 CryptoLocker가 유포되는 데 핵심적인 역할을 했습니다. 랜섬웨어는 몸값이라는 이름에서 느껴지는 것처럼 그 폐해가 큽니다. 피해자의 컴퓨터에 있는 파일을 암호화한 다음 몸값을 요구하는 악성코드 유형입니다.[29]

CryptoLocker는 최근 무력화되었습니다. 미국 법무부는 지난 6월, 다른 국가의 치안 기관 및 기술 전문 기업들과의 공조를 통해 2년간 활동해 온, CryptoLocker의 주요 유통 경로였던 "Gameover Zeus"라는 거물급 봇넷을 일망타진했다고 밝혔습니다.[30] 그러나 얼마 되지 않아 새로운 브랜드의 랜섬웨어, "CryptoWall"이 나타나 그 자리를 차지했습니다.

Cisco 연구 팀은 2014년 상반기에 웹을 이용하는 공격 캠페인, 특히 악성 광고를 통해 (공격자가 대여하거나 구입한) 익스플로잇 킷 호스팅 사이트로 사용자를 리디렉션하는 공격을 집중 해부했습니다. 이러한 공격은 사용자의 시스템에 "드로퍼"를 보내고 취약한 시스템을 감염시킵니다. Cisco 보안 전문가들은 이번 조사 과정에서 "RIG"라는 새로운 익스플로잇 킷의 특성에 부합하는 많은 트래픽을 발견했습니다. 이 킷은 2014년 4월, 범죄자들의 포럼에서 처음 확인되었습니다.[31] RIG는 악성 광고를 이용하여 합법적인 유명 웹사이트 방문자에게 드라이브 바이 공격을 가합니다. 이 공격 툴킷이 CryptoWall 랜섬웨어 유포에 사용되고 있습니다.

Cisco는 6월 초, 악성 광고에 의해 리디렉션되는 다수의 감염된 WordPress 사이트에 대한 요청을 차단했습니다.

(37페이지, WordPress 취약점: 방치되는 매장을 참조하십시오.)

이 사이트의 랜딩 페이지는 Java, Flash 그리고 멀티미디어 프로토콜인 Microsoft Silverlight에 대한 익스플로잇을 호스팅합니다. Cisco 연구 팀에 따르면, 익스플로잇 실행을 지원하는 Microsoft Silverlight용 플러그인이 사이버 범죄자들에게 어필하고 있는 것으로 보입니다. Fiesta는 2013년에 Silverlight 익스플로잇을 수록한 익스플로잇 킷 중 가장 먼저 알려진 것입니다. RIG와 또 다른 익스플로잇 킷인 Angler가 치열한 익스플로잇 킷 시장의 경쟁에 발 빠르게 합류했습니다. (33페이지, 익스플로잇 킷: 본격적으로 시작된 경쟁을 참조하십시오.)

WordPress 취약점: 방치되는 매장

크고 작은 기업 모두 WordPress를 활용합니다. 이 웹 소프트웨어는 스크립트와 추가 기능을 모아둔것으로, 사용자가 자신의 웹사이트에서 블로그, 포럼, 전자상거래 등 원하는 기능을 손쉽게 구현할 수 있게 해줍니다.

WordPress는 보안이 아닌 기능성을 염두에 두고 설계되었습니다.

대부분의 WordPress 사용자는 이를 제대로 보호할 만한 지식이나 기술력이 없습니다. 그리고 사용자들이 WordPress CMS(콘텐츠 관리 시스템) 및 이와 유사한 시스템을 사용하여 웹사이트를 구축했다가 더 이상 관리하지 않고 방치하는 경우도 많습니다.

이러한 사이트가 도처에 무수히 많으며, 이는 보안 사슬의 심각한 약점으로 작용합니다. 공격자는 오랫동안 방치된 사이트를 확보하여 악성 이진 파일을 업로드하고 익스플로잇 유포 사이트로 활용합니다. 사용자는 현재 서비스 중이고 합법적이지만 역시 감염되었을 다른 웹사이트를 둘러보다가 이러한 사이트를 만납니다. iFrame이 방치된 사이트의 콘텐츠를 가져와 합법적 사이트의 사용자에게 서비스하는 것입니다.

WordPress가 이러한 문제를 가진 유일한 CMS는 아닙니다. 그러나 Joomla, e107 등의 다른 CMS와 비교할 수 없을 만큼 높은 인기를 누리고 있습니다. 방치된 웹사이트는 인터넷 전체의 보안에 심각한 위험이 되며, 어느 누구도 이러한 사이트를 신경 쓰지 않으므로 이를 정리하거나 종료시키기가 쉽지 않습니다. 사이트 소유자가 어떤 조치를 취하더라도 진입 지점에 패치를 적용하는 데 그칠 뿐, 이미 감염되었는지 여부는 확인하지 않습니다. 백도어를 찾아 완전히 제거하지 않습니다.

여러 대표적인 호스팅 제공업체들은 호스팅 패키지의 일환으로 상업용 웹사이트용 WordPress 설치 매니지드 서비스를 저렴한 가격으로 제공하고 있습니다. 이들은 모든 패치를 적용하고 알맞은 보안 설정이 갖춰져 있는지 확인합니다. 앞으로 더 많은 사용자들이 이러한 유형의 서비스를 이용하면 WordPress 취약점이 있는 사이트 수가 줄어들 것입니다.

POS 공격: 결제카드 데이터를 노리는 범죄자들이 애용하는 공격 벡터

여러 가지 트렌드가 맞물리면서 POS 시스템은 대량의 신용카드 데이터를 훔쳐내 신속하게 이익을 취하려는 범죄자에게 매력적인 공격 대상이 되었습니다. 최근 대형 소매업체에서 발생한 보안 사고들은 이러한 공격 유형이 매우 신속하게, 성공적으로 진행될 수 있음을 보여줍니다. 결제카드 데이터 공격에 대비하여 감지 기능을 점검하는 것이 바람직하며, 공격 과정 및 그 이후의 위협 요소 제거 절차를 단축하는 노력도 필요합니다.

이 공격은 결제카드의 마그네틱 선에 저장된 데이터를 훔쳐냅니다. 유출된 데이터를 사용하여 가짜 신용카드를 만들고 매장에서 사기 구매에 이용할 수 있습니다. POS 악성코드는 메모리에서 데이터를 추출하므로, 디스크 또는 네트워크의 데이터 암호화 기능을 피할 수 있습니다. 다음과 같은 트렌드에 힘입어 이 익스플로잇이 더 큰 규모로 실행되고 있습니다.

POS 인터넷 연결

POS 시스템이 인터넷에 연결되는 경우가 늘면서 기업 네트워크에 침투하려는 범죄자의 진입점이 되고 있습니다.

인식 부족

많은 기업에서 결제카드 정보를 중요 데이터로 간주해야 한다는 인식이 부족하여 보호가 소홀한 편입니다.

서드파티 벤더

기업에서 POS 솔루션의 전체 또는 일부에 외부 벤더를 이용하는 경우가 늘면서 범죄자의 액세스 포인트가 많아졌습니다.

결제카드 데이터는 온라인 범죄 시장에서 각광받는 상품이므로 투자 수익이 높습니다. 범죄자들은 POS 시스템에서 데이터를 훔쳐내는 것이 전자상거래 가맹점에서 유출하는 것보다 효과적이라고 생각합니다. 은행에서 이러한 데이터 도용을 감지하고 차단하는 기술력이 발전하고 있기 때문입니다.

또한 미국은 선진 경제권 중에서는 드물게 더 안전한 "칩과 PIN" 시스템 대신 결제카드 마그네틱 선을 주로 사용하므로 마그네틱 선에 수록된 데이터를 쉽게 현금화할 수 있습니다. (그러나 칩/PIN 시스템에서도 카드 데이터의 엔드 투 엔드 암호화가 이루어지지 않으면 카드 번호와 유효 기한을 알아내 온라인 거래에 사용할 수 있습니다.)

결제카드 데이터 모니터링 강화

POS에서 결제카드 데이터 및 기타 중요 정보가 유출되는 것을 방지하려면 범죄자의 진입을 차단하는 기술적 장벽의 구현에 더 투자해야 합니다. 또한 기업의 보안 전문가가 결제카드 데이터에 더 큰 관심을 기울이도록 인식의 변화가 있어야 합니다.

POS에 하드웨어 암호화 기기를 추가하는 곳도 있습니다. 그러면 네트워크를 이동하는 결제카드 데이터의 가로채기를 방지하는 데 도움이 됩니다. 그 비용 부담이 너무 크다면 적어도 이 데이터를 "중요" 데이터로 분류하고 모니터링하면서 무단 액세스 및 비정상적인 이동을 감지해야 합니다. 초기에 네트워크를 감염시킬 수 있는 방법은 무궁무진합니다. 그리고 기업은 공격자가 이미 네트워크에 침투했을 가능성도 고려해야 합니다.

결제카드 데이터 도용의 가능성을 나타내는 가장 타당성 높은 IOC는 툴셋이 유입되었거나 새로운 프로세스가 POS 터미널에서 실행되거나 압축된 데이터가 동일한 크기 및 빈도로 추출되는 것입니다. 확장된 네트워크의 전 범위에서 이러한 동작을 분석할 수 있는 시스템의 도입을 고려해야 합니다.

또한 모든 결제카드 처리 시스템에서 애플리케이션 및 프로세스 변경 감지를 수행하는 것도 바람직합니다. 엔드포인트가 변경될 때마다 즉각적인 분석이 이루어져야 합니다. 또한 대부분의 프로토콜은 효율성과 속도를 위해 압축을 이용하지만, 압축 툴 자체는 기업의 "애플리케이션 화이트리스트"에 포함되어야 합니다.

마지막으로, 네트워크를 세그먼트화하여 범죄자가 귀중한 데이터에 쉽게 접근할 수 없게 해야 합니다. POS 시스템은 엔터프라이즈 네트워크와 다른 네트워크 세그먼트에 배치함으로써 POS 시스템에 대한 접근 및 피벗 공격을 제한해야 합니다.

모바일 단말기가 급증하고 엔터프라이즈 네트워크에서도 확산됨에 따라 세그먼트화에 강력한 ID 기능을 포함시켜야 합니다. 즉 사용자가 누구인지, 어떤 유형의 단말기를 사용하여 어떤 방법으로 네트워크에 액세스하는지 알 수 있어야 합니다. 예를 들어, 회사캠퍼스 무선 LAN에서 회사 소유의 랩톱을 통해 액세스하는 것은 허용하지만, 원격 액세스 VPN을 통해 태블릿으로 액세스하는 것은 POS 데이터의 중요도 때문에 거부할 수 있습니다.

Cisco는 결제카드 데이터를 노리는 공격자들이 앞으로도 POS 시스템에 계속 주력할 것으로 예상합니다. 그러나 면밀한 감지 및 알림 시스템을 갖추고 하드웨어 암호화를 구현한다면 그러한 시도를 무산시킬 수 있습니다.

사회공학:
인간 관계의 약한 고리 찾기

어떤 기업에서 최신 보안 소프트웨어에 수십만 달러 이상을 투자하고 이제 네트워크를 통한 표적 공격으로부터 안전하다고 자신할 수 있습니다. 그러나 사무실 또는 서버 팜의 정문으로 들어오는 사람이 바로 위협이라면 네트워크 에지 소프트웨어가 무슨 소용이 있을까요?

지능적인 범죄자들은 감염된 웹사이트 링크가 포함된 피싱 이메일을 만들기보다는 직접 현장에 나타나 물리적으로 네트워크에 연결하는 수법으로 더 큰 이익을 챙깁니다. (스팸과 기타 온라인 사회공학적 공격이 사라졌다는 의미는 아닙니다. 자세한 내용은 26페이지를 참조하십시오.) 이더넷에 연결하고 IP 전화기의 연결을 끊고 그 케이블을 사용하여 네트워크 정보에 접근하는 것이 가능하다면 엄청난 피해로 이어질 수 있습니다. 사회공학은 사람을 해킹하는 기술입니다. 즉 사람, 즉 직원이 디지털 및 물리적 보안의 가장 약한 고리가 됩니다.

범죄자는 직접적인 방문에서도 이메일 및 감염된 웹사이트 공격과 유사한 사회공학적 전술을 구사합니다. 구내에 접근할 권한을 부여하는 누군가로부터 (잘못된) 신뢰를 얻는 것이 핵심입니다.

범죄자는 표적으로 삼은 직원에 대해 LinkedIn을 통해 분석합니다. 이를테면 현재 하는 일, 출신 대학, 좋아하는 스포츠 팀까지 알아낸 다음 그 사람이 알 만한 사람 또는 신뢰할 만한 누군가로 위장합니다.

특히 전문가들 사이에서 소셜 네트워크가 각광받으면서 누구라도 방대한 정보와 사진을 입수한 상태에서 말 그대로 문 안으로 걸어 들어올 수 있습니다.

온라인 검색으로 수집한 배경 정보를 토대로 기자인 척하고 인터뷰를 요청하거나, 잠재적 파트너 또는 고객의 행세를 하면서 면담을 요청합니다. 가짜 신분증까지 착용하여 권한 있는 사람처럼 보일 수도 있습니다.

범죄자는 표적으로 삼은 기업의 정문에서 그러한 사기를 벌일 필요가 없다고 생각할 수도 있습니다. 그 대신 더 약한 고리를 노립니다. 즉 진짜 표적인 네트워크에 대한 액세스 권한 또는 연결 기능을 가진. 보안이 더 허술한 비즈니스 파트너 또는 공급자입니다. 이는 표적의 보안 수준이 높지만 신뢰받는 비즈니스 파트너의 보안은 그렇지 않은 경우 매우 효과적입니다. 해커는 항상 가장 쉬운 길을 찾으려 합니다.

사회공학을 기반으로 하고 물리적 네트워크 접근을 수반하는 보안 사고를 막기 위해서는 네트워크 액세스를 허가하기에 앞서 네트워크 액세스 포트에서 인증 및 권한 부여 기능을 적용해야 합니다. 또한 사용자별로, 기기별로, 사용자와 기기별로 또는 기타 구성에 따라 "동적 보안 도메인"을 구축할 수도 있습니다. 이러한 동적 보안 도메인에는 802.1x, 포트 ACL(access-control list), VPN, 호스트 포스처 평가와 같은 기술도 사용됩니다.

솔루션

공격자가 유선, 무선, VPN 등 어떤 액세스 방식을 사용하더라도 IT 전문가가 상황에 따라 맞춤형 보안 도메인, 즉 "버블"을 생성할 수 있습니다. 범죄자가 현장에서 포트에 랩톱을 연결할 경우 네트워크에서 그 사람을 일단 멈추게 하고 인증, 프로파일링, 포스처 평가를 실시하고 그 행동을 지켜본 다음 상황별 정책에 따라 네트워크 액세스를 제한하는 매우 구체적이고 동적인 사용 권한을 부여합니다.

전망

Cisco 보안 전문가들이 기업에서 보안을 하나의 비즈니스 프로세스로 간주하고 사내의 기술 책임자와 비즈니스 책임자 간의 대화를 활성화하고 날로 감지하기 어려워지는 위협에 대한 가시성을 높여줄 첨단 기술 솔루션을 활용함으로써 보안을 향상시킬 수 있는 방법을 소개합니다.

실생활에 적합한 지능적인 사이버보안

보안 사슬의 약점을 바로잡고 보강하기 위해서는 각 기업과 업계가 경영진 차원에서 사이버 위험에 대한 인식을 제고하고 사이버 보안을 비즈니스 과제로 받아들이는 것이 중요합니다. 비즈니스 전략, 보안 업무, 사이버 레질리언스를 위한 제어 기능을 연계하는 것도 필수적입니다. 예측 분석과 같은 새로운 지능형 솔루션을 도입하여 "떠들썩한" 네트워크의 전 범위에서 네트워크 가시성을 강화하려는 노력도 필요합니다.

오늘날 기업에서 공격의 전후 및 진행 상태의 전 범위에서 방어하기 위해서는 보안 위협이 나타날 만한 모든 영역에서 제 기능을 할 보안 솔루션으로 다양한 공격 벡터를 해결해야 합니다. 여기에는 네트워크, 모바일 기기, 가상 시스템, 클라우드 또는 데이터 센터가 모두 포함됩니다.

이미 확인되었고 공격의 대상이 된 Java, Flash, Adobe PDF 취약점, WordPress로 만들었다가 방치된 웹사이트, 오랫동안 간과했던 OpenSSL 소프트웨어의 보안 틈새, 보호되지 않은 물리적 네트워크 액세스 지점, 취약한 NTP 서버 등 각종 보안 틈새을 줄이고 각기 다르고 상호 단절된 제품과 솔루션으로 인한 복잡성을 해소하는 것이 모든 사용자에게 더 우수한 보안을 제공하는 지름길입니다. 비즈니스 요구 사항을 뒷받침할 네트워크 탄력성을 확보하고 발견된 네트워크 기기의 라이프사이클 상태를 평가하고 잠재적 보안 취약점을 밝혀내고 운영 체제 버전을 관리하는 것도 중요합니다.[32]

기업이 이와 같이 알려졌거나 새롭게 대두한 보안 문제를 해결하도록 지원하는 Cisco의 전략은 3대 전략적 과제를 기반으로 합니다.

가시성에 기초

더 많이 볼 수 있으면 더 많이 정보를 서로 연결하면서 인텔리전스를 적용할 수 있습니다. 그에 따라 상황을 이해하고 더 현명한 결정을 내리고 수동으로 또는 자동으로 조치를 취할 수 있습니다.

위협 중심

지속적인 분석을 통해 그리고 클라우드에서 제공하고 실효성을 위해 모든 보안 솔루션끼리 공유하는 실시간 보안 인텔리전스를 통해 위협을 감지, 파악, 차단하는 데 주력해야 합니다.

플랫폼 기반

보안은 이제 네트워크 문제에 머무르지 않습니다. 네트워크 기기와 클라우드까지 포괄하는 민첩하고 개방적인 플랫폼으로 구성된 통합 시스템이 필요합니다.

실생활에 적합한 지능적인 사이버보안이라면, 안전한 IoT를 지원하고 컴퓨팅과 마찬가지로 보안도 강력하고 효율적이며 보편적인 형태로 엔드 유저에게 제공될 수 있는 IoE 환경의 기초를 마련하는 데 기여해야 합니다.

체계적 보안: 보안의 비즈니스 프로세스화

보안 평가를 실시하면 어떤 보안 문제의 근본적인 원인이 비즈니스 부서의 운영 오류 및 기술적 오류에 있는 경우가 많습니다. 운영 성숙도 및/또는 역량이 부족하면 보안 제어가 부실하거나 아예 없습니다.

현재 기업들이 사이버 보안을 전략적 위험으로 인식함에 따라 "보안 운영 성숙도"를 달성하는 데 관심이 집중되고 있습니다. 즉 기업이 가시적 관점에서 사이버 보안 위험을 조명하고 지속적으로 사이버 보안 실무를 개선하는 것입니다.

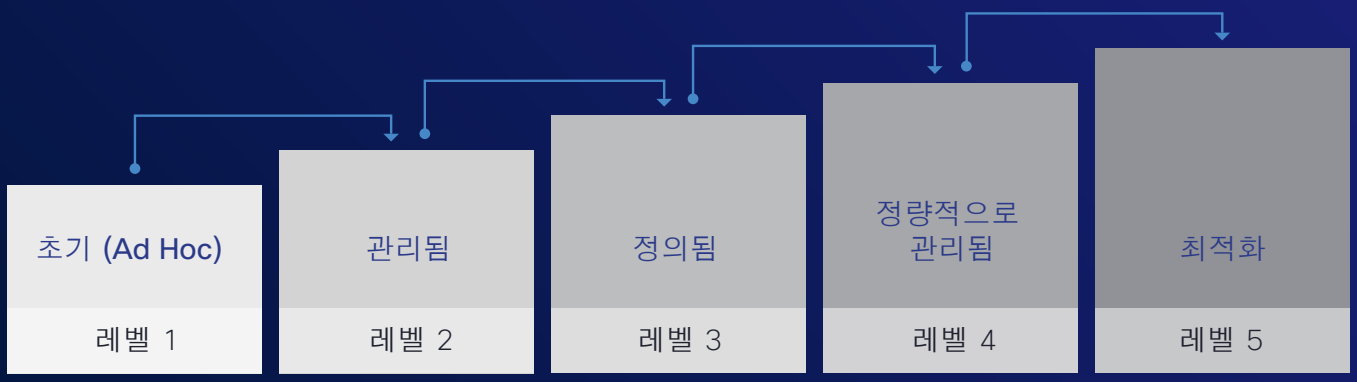
많은 기업은 이와 관련하여 서비스 제공업체의 도움을 받아 보안을 고도로 표준화되고 계량화된 비즈니스 프로세스 또는 프로세스 모음으로 정립하는 중입니다. 이를 정기적으로 검토하면서 전략적 목표를 달성합니다. 보안을 비즈니스 프로세스로 간주하는 결정은 대개 전사적 범위에서 GRC(governance, risk, compliance)를 개선하기 위해 마련된 더 광범위한 비즈니스 이니셔티브에서 비롯됩니다. IT 보안과 관련하여 규정을 준수하는 것만으로는 충분하지 않다는 것을 너무 늦게 깨닫는 기업이 많습니다.

보안을 체계화하고 제도화하는 기업은 다음 질문에 더 정확하게 답할 수 있습니다.

1. 무엇을 보호해야 하는가?
2. 기존의 보안 기능은 얼마나 효과적인가?
3. 사이버 보안과 관련하여 어떤 노력이 필요한가?

그림 17

CMMI 모델



체계적 보안이 구현되면 전사적 범위에서 IT 보안의 현재에 대한 가시성을 높일 수 있습니다. 어떤 직원이 책임자인지, 그 책임을 맡기에 적합한 사람인지, 그 일을 제대로 해내고 있는지 알 수 있습니다. 체계적 보안을 구현한 기업은 IT 리소스가 효과적으로 구축되고 사용되고 있는가도 확인할 수 있습니다.

체계적 보안의 핵심 구성 요소 중 하나는 보안 책임자, 즉 CIO(chief information officer) 또는 CISO(chief information security officer)와 비즈니스 책임자 간의 생산적인 대화입니다. 사이버 보안을 공식적인 비즈니스 프로세스로 삼기 위해서는 이 두 리더들이 더 긴밀하게, 자주 공조하면서 수용 가능한 위험 수준을 정의하고 조직의 보안을 위한 전략적 목표를 세워야 합니다. CISO는 이러한 대화를 활성화하기 위해 비즈니스 책임자가 명확하게 이해할 수 있는 언어로 사이버 보안 정보를 전달할 방법을 찾아야 합니다. 예를 들어, 특정 사이버 보안 위험의 예방 조치를 취함으로써 누릴 가치를 메트릭을 통해 설명할 수 있습니다.

또한 체계적 보안은 "성숙도 모델"의 도입을 의미합니다. Carnegie Mellon의 CMMI(Capability Maturity Model Integration)도 그러한 예입니다. 널리 사용되는 이 모델은 1980년대에 이 대학의 소프트웨어 공학 연구소 프로젝트로 시작했습니다. 그림 17에서 보여주는 것처럼, 성숙도 모델의 출발점은 "ad hoc" 단계입니다. 사실상 "문제 해결(firefighting)" 모드입니다. 최종 단계에 도달하면 표준화되고 반복 및 측정 가능한 프로세스를 갖게 됩니다.

비즈니스의 관점에서 본 사이버 위험

많은 기업에서 IoT가 제시하는 포괄적 연결 환경의 비전에 비즈니스 모델의 성패를 걸고 있습니다. 그러나 빠른 속도로 자리 잡고 있는 이 환경에 대비하고 궁극적으로 성공을 거두기 위해서는 기업의 경영진이 네트워크에 대한 의존도가 높아짐에 따라 수반되는 사이버 위험을 비즈니스의 관점에서 이해해야 합니다.

사이버 보안 문제를 공개적으로 언급하지 않는 것이 오랜 관행으로 자리 잡은 곳도 많지만, 상황이 바뀌고 있습니다. 더 많은 비즈니스 리더들이 사이버 보안 위험이 모든 기업의 공통 과제임을 깨닫고 있습니다. 특히 기업이 더욱 디지털화되고 정보 자산이 전략적 자산으로 자리 잡음에 따라 이러한 인식은 확고해집니다.

또한 이들은 IoT 환경에서는 보안 위협과 이를 완화할 모범 사례에 대한 허심탄회한 대화가 사내에서, (경쟁사를 포함하여) 기업 간에, 공공 부문과 민간 부문 간에 이루어져야 한다는 것도 받아들이기 시작했습니다. 사이버 보안 위험이 비즈니스에 미칠 영향에 관심을 갖게 된 이사회가 압박의 강도를 높임에 따라 최고 경영진 차원에서 이러한 인식이 확산되고 있습니다.

최근 미국 증권거래위원회(SEC)의 조치는 기업의 이사회가 사이버 보안을 최우선 관심사로 다루는 데 일조했습니다. SEC는 2011년에 상장 기업의 사이버 보안 보고 요건을 공표하면서[33] 상장 기업은 "중대한 사이버 보안 사고 또는 공격이 있을 때 또는 그러한 사고가 발생할 실질적인 위험이 있을 때" 그 사실을 주주에게 알리도록 규정했습니다.[34] 또한 SEC는 올해 초, 사이버 보안 라운드 테이블을 열어 "사이버 보안에 대해, 시장의 구성원과 상장 기업이 사이버 보안과 관련하여 직면할 문제점과 과제에 대해 그리고 이러한 문제를 해결하는 방법에 대해 논의"하는 자리를 가졌습니다.[35]

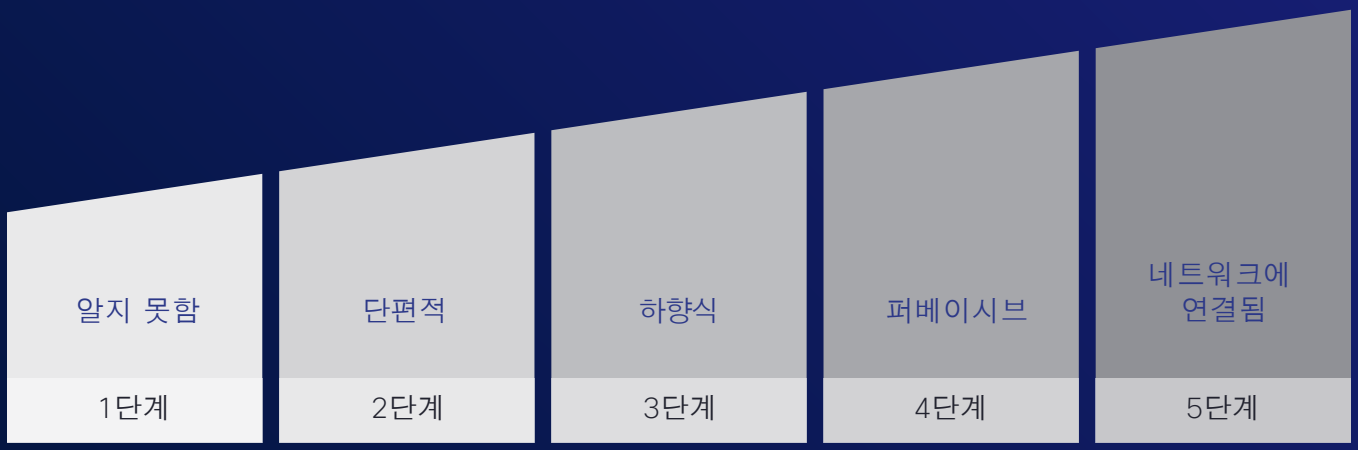
글로벌 차원에서는 공공-민간 공조를 통해 더 발전된 세상을 실현하기 위해 조직된 세계 기구인 WEF(World Economic Forum)는 2011년에 사이버 보안 및 기타 인터넷 관련 사안을 이사회에 상정하기 위해 "사이버 레질리언스(cyber resilience)" 개념을 도입했습니다. WEF는 각 기업의 보안 수준이 오로지 보안 사슬의 가장 약한 고리에 의해 결정되는 상호 종속적인 에코시스템으로 사이버 레질리언스를 규정하고 이를 지원합니다. 이는 WEF의 "Partnering for Cyber Resilience"[36] 이니셔티브의 4대 기본 원칙 중 하나에 잘 나타나 있습니다.

즉, 우리 모두가 의존하고 있는 보안 사슬의 가장 약한 고리에 의해 보안 수준이 결정된다. 우리 각자는 긴밀하게 연결된 이 세상의 안전에 기여한다. 개방적이고 안전하며 탄력적인 온라인 공간은 공공재이다. 모든 구성원은 이 자원을 개발하고 지원할 책임을 공유한다.

WEF의 사이버 레질리언스 이니셔티브는 CEO와 다른 최고 경영진(CIO, CISO 등)이 사내에서 사이버 보안에 대한 논의를 활성화하고 사이버 위험 및 기회에 대해 비즈니스 관점에서 대화할 수 있도록 지원합니다. 이를테면, "사이버 위험에 대한 우려 때문에 어떤 가치 창출형 기술에 대해 투자하지 않을 경우 어떤 비용이 발생할까?"에 대해 논의합니다.

그림 18

기업의 사이버 레질리언스 성숙도 모델

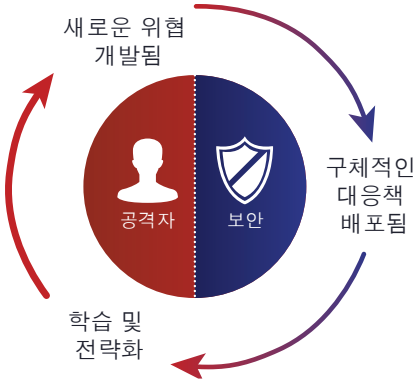


WEF에 따르면, 사이버 레질리언스를 달성하기 위해서는 리스크에 기초하여 사이버 보안에 접근해야 합니다. 이는 사이버 보안을 강화하려는 모든 기업에게 유효한 방식입니다. WEF는 사이버 레질리언스 실현 경로를 제시하는 이 성숙도 모델을 제공합니다.

WEF는 사이버 레질리언스 이니셔티브를 통해 사이버 보안이 사내의 단일 부서, 즉 IT 팀에 의해 실현될 수 있는 것이 아님을 강조합니다. 사이버 기능이 기술적일 뿐 아니라 제도적인 기능이기 때문입니다. 또한 WE는 사내에서 사이버 보안에 대한 인식을 제고하는 것이 CEO의 책임임을 명시합니다. CEO는 해당 기업의 사이버 레질리언스를 실현할 최종적인 책임도 갖고 있습니다.

예측 분석: 더 강력한 보안 실현

악순환입니다. 보안 업계가 어떤 사이버 보안 위협에 대한 대책을 마련하면 공격자는 이를 피할 새로운 방법을 찾아냅니다. 공격자는 어떤 유형의 보안 솔루션이 구축되는지 미리 파악하여 더 드러나지 않고 감지되지 않을 행동 패턴을 개발하여 그 위협 요소를 은닉합니다. 보안 솔루션과 전문가가 쉽게 찾아낼 수 있는 "낮게 열린 열매"는 줄어들고 있습니다. 공격자들이 명령 제어 동작을 실제 트래픽과 구별할 수 없도록 만들어낸 더 많은 암호 트래픽, 더 많은 스크램블링, 무작위적인 트래픽과 싸워야 합니다.



오늘날의 "복잡다단한" 네트워크에 대한 가시성 부재는 보편적 보안 위협이 숨을 곳이 많다는 뜻입니다. 그러한 복잡성을 극복하고 네트워크에서 뭔가 비정상적인 일이 벌어지고 있음을 파악하기 위해서는 "정상적인" 것이 무엇인지 알아야 합니다. 예측 분석은 통찰력을 제공하고 보안 솔루션의 탄력성을 높여주는 새로운 감지 기술입니다. 행동 분석 및 이상 감지를 통해 네트워크에서 이상적 동작(감염의 징후)을 파악합니다.

예측 분석을 통해 기업 네트워크를 구성하는 호스트 서버와 사용자의 동작을 평가할 수 있습니다. 다수의 소형 모델 및 축약된 과거 동작으로부터 모델을 도출하여 어떤 구성 요소가 장차 어떻게 행동할지 예측합니다. 클라우드에서 데이터의 상관성을 파악하여 위협 탐지의 속도, 민첩성, 수준을 높이는 것이 바람직합니다. 예상되는 동작의 불일치가 크거나 계속될 경우 조사 대상으로 표시됩니다.

예측 분석은 기존 보안 기술의 정확도를 높이고 알려지지 않았거나 이례적인 네트워크 동작을 더 정확하게 감지하는 데 도움이 됩니다. 고급 의사 결정 알고리즘을 적용하여 여러 매개 변수를 분석하고 실제 트래픽 데이터에 적용합니다. 기계 학습 기능을 활용하여 시스템에서 학습하고 관찰한 내용을 토대로 적응할 수 있게 합니다.

기계 학습 시스템은 탐정과 비슷합니다. 어디에 위험이 있을지 알아보고 이미 발생했거나 진행 중이거나 임박한 사건의 증거를 찾아냅니다. 그리고 보안 또는 치안 문제를 직접 다루지는 않지만, 다른 시스템에서 예기치 않은 위협을 찾아내 조치를 취할 수 있도록 지원합니다. 예측 분석이 가치를 발휘하고 보안 실효성을 높이는 데 기여하기 위해서는 콘텐츠 기반 보안 솔루션, 경계 관리 솔루션, 정책 관리 솔루션과 함께 구축해야 합니다.

회사 소개

Cisco는 실생활에 적합한 지능적인 사이버보안을 제공합니다. 이러한 비전은 복잡성을 완화하면서 공격의 전 범위에 뛰어난 가시성, 지속적인 제어, 지능형 위협 방어를 할 수 있는 위협 중심의 접근 방식에 기초합니다. 이러한 위협 중심의 보안 모델을 통해 공격의 전후 및 진행 상태에 신속하게 대처할 수 있습니다.

Cisco Collective Security Intelligence 에코시스템의 위협 분석가들은 뛰어난 식견과 정교한 빅데이터 시스템을 접목시켜 알려졌거나 새로운 위협을 찾아내 분석하고 차단합니다. Cisco의 명성 높은 보안 전문가들은 수십억 건의 웹 요청과 이메일, 수백만 건의 악성코드 샘플, 오픈 소스 데이터 세트, 수천 건의 네트워크 침입 사례를 종합적으로 원격 분석하여 최고 수준의 가시성을 제공하는 첨단 인프라 및 시스템을 활용합니다.

그 결과물인 "빅 인텔리전스(big intelligence)"는 전 세계의 확장된 네트워크를 즉시, 포괄적으로 보호하면서 더 우수한 보안 실효성을 실현합니다.

Cisco의 위협 중심 보안 접근법에 대한 자세한 내용은 www.cisco.com/go/security에서 확인하십시오.

미주

1 *Estimating the Cost of Cyber Crime and Cyber Espionage*, Center for Strategic and International Studies (CSIS), 2013년 7월: https://csis.org/event/estimating-cost-cyber-crime-and-cyber-espionage.

2 "Internet of Things," Cisco.com: http://www.cisco.com/web/solutions/trends/iot/overview.html.

3 "Internet of Things" infographic, Cisco Internet Business Solutions Group: http://share.cisco.com/internet-of-things.html.

4 "Hackers Reveal Nasty New Car Attacks–With Me Behind The Wheel", Andy Greenberg, *Forbes*, 2013년 8월 12일: http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/.

5 "Hackers Reportedly Targeted Three Large Medical Device Makers," iHealthBeat.com, 2014년 2월 11일: www.ihealthbeat.org/articles/2014/2/11/hackers-reportedly-targeted-three-large-medical-device-makers.

6 "How secure is your baby monitor? What can happen when the 'Internet of Things' gets hacked," by Matt Hartley, *Financial Post,* 2014년 5월 3일: http://business.financialpost.com/2014/05/03/how-secure-is-your-baby-monitor-what-can-happen-when-the-internet-of-things-gets-hacked/?__lsa=bc1b-f93e.

7 "The Internet of Everything, Including Malware," Craig Williams, Cisco Security blog, 2014년 12월 4일: http://blogs.cisco.com/security/the-internet-of-everything-including-malware/.

8 이 보고서는 고객으로부터 발생할 수 있는 잠재적 악성 FQDN, 도메인, 사이트 등에 대한 요청 수를 파악하는 데 중점을 둡니다.

9 *Cisco 2014 Annual Security Report:* https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

10 Vulnerability Research Team의 AEGIS 프로그램과의 직접적인 인텔리전스 공유에 참여하려는 고객은 threatintel@cisco.com으로 문의할 수 있습니다.

11 상동

12 Heartbleed에 대한 자세한 내용은 www.cisco.com/web/about/security/intelligence/ERP-Heartbleed.html을 참조하십시오.

13 "OpenSSL Heartbleed vulnerability CVE-2014-0160 – Cisco products and mitigations", Pano Kampanakis, Cisco Security blog, 2014년 4월 9일: http://blogs.cisco.com/security/openssl-heartbleed-vulnerability-cve-2014-0160-cisco-products-and-mitigations.

14 OpenSSL Heartbleed 취약점 완화에 대한 자세한 내용은 "Cisco Event Response: OpenSSL Heartbleed Vulnerability CVE-2014-0160," 2014년 4월 22일 , Cisco.com: www.cisco.com/web/about/security/intelligence/ERP-Heartbleed.html을 참조하십시오.

15 "New OpenSSL Defects – Another Heartbleed? Tor Stripped?" by James Lyne, *Forbes*, 2013년 6월 5일: www.forbes.com/sites/jameslyne/2014/06/05/new-openssl-defects-another-heartbleed.

16 "Severe OpenSSL Security Bug Uncovered by Japanese Researcher Months After Heartbleed," Luke Villapaz, *International Business Times*, 2014년 6월 5일: www.ibtimes.com/severe-openssl-security-bug-uncovered-japanese-researcher-months-after-heartbleed-1594989.

17 *Cisco 2014 Annual Security Report:* https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

18 상동

19 "Spam Hits Three Year High-Water Mark," Cisco Security blog, 2014-05-02: http://blogs.cisco.com/security/spam-hits-three-year-high-water-mark.

20 "Major Apple security flaw: Patch issued, users open to MITM attacks," Violet Blue, "Zero Day" blog, *ZDNet*, 2014년 2월 22일: http://www.zdnet.com/major-apple-security-flaw-patch-issued-users-open-to-mitm-attacks-7000026624/.

[21] "Amazon Web Services, Cisco, Dell, Facebook, Fujitsu, Google, IBM, Intel, Microsoft, NetApp, Rackspace, VMware and The Linux Foundation Form New Initiative to Support Critical Open Source Projects," media release, Linux Foundation, 2014년 4월 24일. 이 이니셔티브에 대한 자세한 내용: http://www.linuxfoundation.org/news-media/announcements/2014/04/amazon-web-services-cisco-dell-facebook-fujitsu-google-ibm-intel

[22] *Cisco 2014 Annual Security Report:* https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

[23] "When Network Clocks Attack," Jaeson Schultz, Cisco Security blog, 2014년 1월 10일: http://blogs.cisco.com/security/when-network-clocks-attack/.

[24] "Chronology of a DDoS: Spamhaus," Seth Hanford, Cisco Security blog, 2013년 3월 28일: http://blogs.cisco.com/security/chronology-of-a-ddos-spamhaus/.

[25] NTP 서버의 취약성 여부를 확인하려면 openntpproject.org를 방문하십시오. DNS 모범 사례에 대한 자세한 내용은 "DNS Best Practices, Network Protections, and Attack Identification": http://www.cisco.com/web/about/security/intelligence/를 참조하십시오.

[26] Open Resolver project: www.openresolverproject.org.

[27] "Meet Paunch: The Accused Author of the Blackhole Exploit Kit," Brian Krebs, KrebsOnSecurity blog, 2013년 12월 6일: http://krebsonsecurity.com/2013/12/meet-Paunch-the-accused-author-of-the-blackhole-exploit-kit/.

[28] "Global Internet Ad Spend Sees Double-Digit Growth, Outpaces Other Media," *Nielsen,* 2012년 7월 10일: http://www.nielsen.com/us/en/newswire/2012/global-internet-ad-spend-sees-double-digit-growth-outpaces-other-media.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+NielsenWire+(Nielsen+Wire).

[29] *Cisco 2014 Annual Security Report:* https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

[30] "Malicious Advertisements on Major Websites Lead to Ransomware," by Jeremy Kirk, IDG News Service, 2014년 6월 6일: http://www.pcworld.com/article/2360820/malicious-advertisements-on-major-websites-lead-to-ransomware.html.

[31] "RIG Exploit Kit Strikes Oil," Andrew Tsonchev, Cisco Security blog, 2014년 6월 5일: http://blogs.cisco.com/security/rig-exploit-kit-strikes-oil/.

[32] Network Barometer Report: A gauge of global networks' readiness to support business, *Dimension Data,* 2013: http://www.dimensiondata.com/Global/Documents/Network%20Barometer%20Report%202013.pdf.

[33] "CF Disclosure Guidance: Topic No. 2: Cybersecurity," Division of Corporation Finance, SEC, 2011년 10월 13일: http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[34] "Cybersecurity: SEC outlines requirement that companies report data breaches," Ellen Nakashima and David S. Hilzenrath, *The Washington Post,* 2011년 10월 14일: http://www.washingtonpost.com/world/national-security/cybersecurity-sec-outlines-requirement-that-companies-report-data-breaches/2011/10/14/gIQArGjskL_story.html.

[35] "Cybersecurity Roundtable," SEC: http://www.sec.gov/spotlight/cybersecurity-roundtable.shtml.

[36] WEF의 Partnering for Cyber Resilience 이니셔티브에 대한 자세한 내용은 http://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience를 참조하십시오.