Cisco 2014
연례 보안 보고서

CISCO

개요

신뢰성 문제

온라인 공격자와 기타 악의적인 사용자가 흔히 사용하는 수법은 신뢰를 악용하는 것입니다. 이들은 사용자들이 정기적으로 상호작용하는 시스템, 애플리케이션, 사람과 기업에 대한 신뢰를 악용합니다. 그리고 이러한 방식은 효과가 있습니다. 공격자들이 감지해내기 어려운 멀웨어를 새로운 방식으로 네트워크에 심어서 데이터를 도용하거나 중요한 시스템을 중단시키는 사례에 대한 증거 자료가 많이 있습니다.

사회 공학적 수법의 암호 및 인증서 탈취에서부터 뻔히 보이는 곳에 감쪽같이 숨어 몇 분 안에 교묘하게 침입하는 등 악의적인 사용자들은 이렇게 대중의 신뢰를 악용하여 지속적으로 해를 입히고 있습니다. 그러나 이러한 신뢰의 문제는 범죄자들이 취약점을 악용하거나 사회 공학적인 수법으로 사용자를 속이는 것을 넘어 공공 및 민간 조직에 대한 신뢰까지 무너트리고 있습니다.

오늘날 네트워크는 두 가지 양상으로 신뢰를 위협받고 있습니다. 하나는 제품의 무결성에 대한 고객의 신뢰 하락입니다. 다른 하나는 악의적인 사용자들이 신뢰 메커니즘을 무너뜨리고 있다는 증거가 쌓이고 있으며 그로 인하여 네트워크 및 애플리케이션의 보장, 인증, 권한 부여 아키텍처가 과연 효율적인지 의문이 제기되고 있습니다.

이 보고서에서 Cisco 는 멀웨어의 변화, 취약성 동향 및 DDos (Distributed Denial-of-Service) 공격의 부활과 같은 주요 보안 문제에 대한 데이터와 정보를 제공합니다. 이 보고서는 또한 특정 조직, 그룹 및 업계를 대상으로 하는 활동과 갈수록 정교해지는 민감한 정보를 노리는 공격자들의 수법도 살펴봅니다. 보고서의 마지막에서는 전체적으로 보안 모델을 점검하고 공격 전, 공격 중, 공격 후와 같이 공격 전반에 대해 파악하기 위해 필요한 권장 사항을 제안합니다.

악의적인 사용자들은 이렇게 대중의 신뢰를 악용하여 지속적으로 해를 입힐 방법을 계속해서 찾아내고 있습니다.

핵심 분석 결과

다음은 *Cisco 2014 연례 보안 보고서* 의 3 가지 핵심 분석 결과입니다.

인터넷 곳곳에 있는 중요한 리소스가 인프라 공격의 표적이 되고 있습니다.

- 악의적인 공격은 웹 호스팅 서버, 네임 서버 및 데이터 센터에 접근 권한을 확보해 나가고 있습니다. 이는 평판이 높고 리소스가 풍부한 자산을 겨냥하는 우버봇 (überbot) 의 생성을 암시합니다.
- 버퍼 오류는 CWE (Common Weakness Enumeration) 위협 범주에서 21% 를 차지하는 대표적인 위협입니다.
- 멀웨어 발생률은 전자 제조업, 농업 및 광업 분야로 전환되는 추세이며 그 발생률이 전체 산업 평균 발생률보다 약 6 배나 높습니다.

악의적인 사용자들은 경계 보안의 틈새를 공격하기 위해 신뢰받고 있는 애플리케이션 사용하고 있습니다.

- 스팸의 하락세는 계속되고 있지만 악의적인 스팸의 비율은 계속해서 비슷한 수준으로 유지되고 있습니다.
- 웹 공격의 91% 가 Java 를 겨냥하고 있으며, Cisco Web Security 서비스를 사용하는 회사 중 76% 는 단종되어 더 이상 지원되지 않는 Java 6 버전을 사용하고 있습니다.
- "워터링 홀 (Watering Hole)" 공격은 멀웨어를 전파하기 위해 특정 산업과 관련된 웹사이트를 표적으로 삼고 있습니다.

다국적 기업들을 조사한 결과 내부 보안침해의 증거가 발견되었습니다. 기업 내부 네트워크에서 의심스러운 트래픽이 발생되고 있으며 의심스러운 사이트로의 접속을 시도하고 있습니다 (조사한 회사 모두 (100%) 가 악성 멜웨어 호스트를 호출).

- 보안침해 흔적지표에 따르면 네트워크가 침입당한 것을 오랫동안 발견하지 못하는 것으로 나타납니다.
- 위협 경보가 전년 대비 14% 증가했으며 (업데이트되지 않은) 새로운 경보도 증가하는 추세입니다.
- 2013 년에 발견된 전체 모바일 멀웨어 중 99% 가 안드로이드 기기를 겨냥한 것이었습니다. 또한 모든 형태의 웹 유포 멀웨어가 가장 많이 발생한 기기도 안드로이드였습니다 (71%).

보고서 내용

Cisco 2014 연례 보안 보고서 는 다음 4 가지 핵심 영역에 대한 보안 정보를 제공합니다.

신뢰성

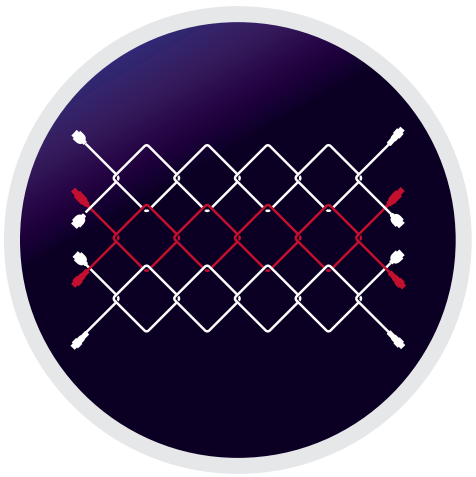
많은 부분이 위험에 처한 상황이므로 모든 조직은 신뢰성, 투명성 및 개인정보보호 사이에서 적절한 균형을 찾아야 합니다. 여기에서, Cisco 는 이러한 균형을 찾고자 하는 보안 실무자의 노력을 방해하는 다음 3 가지 압박 요인에 대해 알아봅니다.

- 더 넓어진 공격 영역
- 공격 모델의 확산과 정교함
- 위협과 솔루션의 복잡성

위협 분석 정보

Cisco 와 Sourcefire 는 최대 규모의 감지 원격 분석 세트를 이용하여 작년 보안 정보를 분석하고 정리하였습니다.

- 인터넷 곳곳에 있는 중요한 리소스가 인프라 공격의 표적이 되고 있습니다.
- 악의적인 사용자들은 경계 보안의 틈새를 공격하기 위해 신뢰받고 있는 애플리케이션을 사용하고 있습니다.
- 보안침해 흔적지표에 따르면 네트워크가 침입당한 것을 오랫동안 발견하지 못하는 것으로 나타납니다.



산업계

이 섹션에서 Cisco SIO (Security Intelligence Operation) 조사관이 Cisco 원격 분석에 속하지 않지만 보안 방식에 영향을 주는 무작위 대입 로그인 시도, 대규모 DDoS 활동 및 랜섬웨어 시도에서부터 높아지는 클라우드 의존성, 보안 전문 인력의 부족 및 기타 문제에 이르는 업계 동향에 대한 논의를 다루었습니다.

권장 사항

조직은 더 넓어진 공격 영역, 공격 모델의 확산과 정교함, 네트워크 상에 늘어가는 복잡성을 경험하고 있습니다. 많은 조직이 새로운 기술의 사용, 아키텍처와 작업 간소화 및 보안 팀의 강화와 같은 효율적인 전략을 활용하여 보안에 대한 비전을 강화하고자 노력하고 있습니다.

이 섹션에서는 위협 중심의 보안 모델을 통해 방어자들이 어떻게 모든 공격 벡터에 걸쳐 전력 공격 전반을 다루고 공격 전, 공격 중, 공격 후와 같이 지속적인 방식으로 항상 공격에 대처할 수 있는지 살펴봅니다

Cisco 의 위협 환경 평가 방법

Cisco 는 널리 보급된 솔루션과 광범위한 보안 분석 정보를 기반으로 위협 평가에서 중요한 역할을 하고 있습니다.

- 매일 160 억 건의 웹 요청을 Cisco Cloud Web Security 를 통해 검사
- 매일 930 억 개의 이메일을 Cisco 에서 호스팅하는 이메일 솔루션으로 검사
- 매일 200,000 개의 IP 주소 평가
- 매일 400,000 개의 멀웨어 샘플 평가
- 매일 3,300 만 개의 엔드포인트 파일을 FireAMP 를 통해 평가
- 매일 2,800 만 건의 네트워크 연결을 FireAMP 를 통해 평가

이러한 활동으로 Cisco 는 다음과 같은 위협을 발견할 수 있습니다.

- 매일 45 억 개의 이메일 차단
- 매일 8,000 만 건의 웹 요청 차단
- FireAMP 에서 매일 6,450 개의 엔드포인트 파일 감지
- FireAMP 에서 매일 3,186 개의 엔드포인트 네트워크 감지
- 매일 50,000 건의 네트워크 침입 감지

목차

이 문서 정보

이 문서에는 검색 및 공유 가능한 내용이 포함되어 있습니다.

Adobe Acrobat 에서 이 아이콘을 이용하여 찾기 기능을 사용할 수 있습니다.

[ ] 이 아이콘을 이용하여 내용을 공유할 수 있습니다.

권장 소프트웨어

Adobe Acrobat 버전 7.0 이상

신뢰성

많은 부분이 위험에 처한 상황이므로 모든 조직은 신뢰성, 투명성 및 개인정보보호 사이에서 적절한 균형을 찾아야 합니다.

새로운 비즈니스 방식, 새로운 보안의 틈새

허술하게 연결된 기술 공급망은 오늘날 복잡한 사이버 위협과 위험 환경의 한 측면입니다.

또한, 네트워크 인스턴트 생성을 통해 어떤 기기가 어느 위치에 있든 상관없이 사용되는 "모두에서 모두로의 인프라 (any-to-any infrastructure)" 의 등장도 마찬가지입니다.[1] 뿐만 아니라 퍼블릭 SaaS (software-as-a-Service) 클라우드, 프라이빗 클라우드 또는 하이브리드 클라우드 등과 같이 어디서나 실행할 수 있는 애플리케이션에 접속을 시도하는 스마트폰, 태블릿 등의 인터넷 지원 장치도 급증하고 있습니다.[2] 심지어 기본적인 인터넷 인프라 서비스도 웹 호스팅 서버, 네임 서버, 데이터 센터의 평판, 대역폭 및 지속적인 업타임과 가용성을 이용하여 더 큰 규모의 활동을 펼치려는 해커들의 목표물이 되었습니다. (43 페이지 "취약한 에코시스템 내의 균열" 참조)

클라우드 컴퓨팅 및 모빌리티와 같은 추세로 인해 가시성이 저하되고 보안상의 복잡성이 증가하고 있지만, 경쟁력 확보와 비즈니스의 성공을 위해 중요한 요소이기 때문에 이러한 추세를 받아들여야만 합니다. 하지만 보안 팀이 기존의 솔루션을 새롭게 급변하는 비즈니스 방식에 맞게 조정하면서 보안의 틈새가 생성되고 더 벌어지고 있습니다. 한편 악의적인 사용자들은 통합되지 않은 포인트 솔루션으로는 처리할 수 없는 틈새를 공격하기 위해 재빠르게 움직이고 있습니다. 이들은 민첩성을 높일 수 있는 리소스를 갖고 있기 때문에 성공을 거두고 있습니다.

기본 인터넷 인프라는 해커의 공격 대상이 되었습니다.

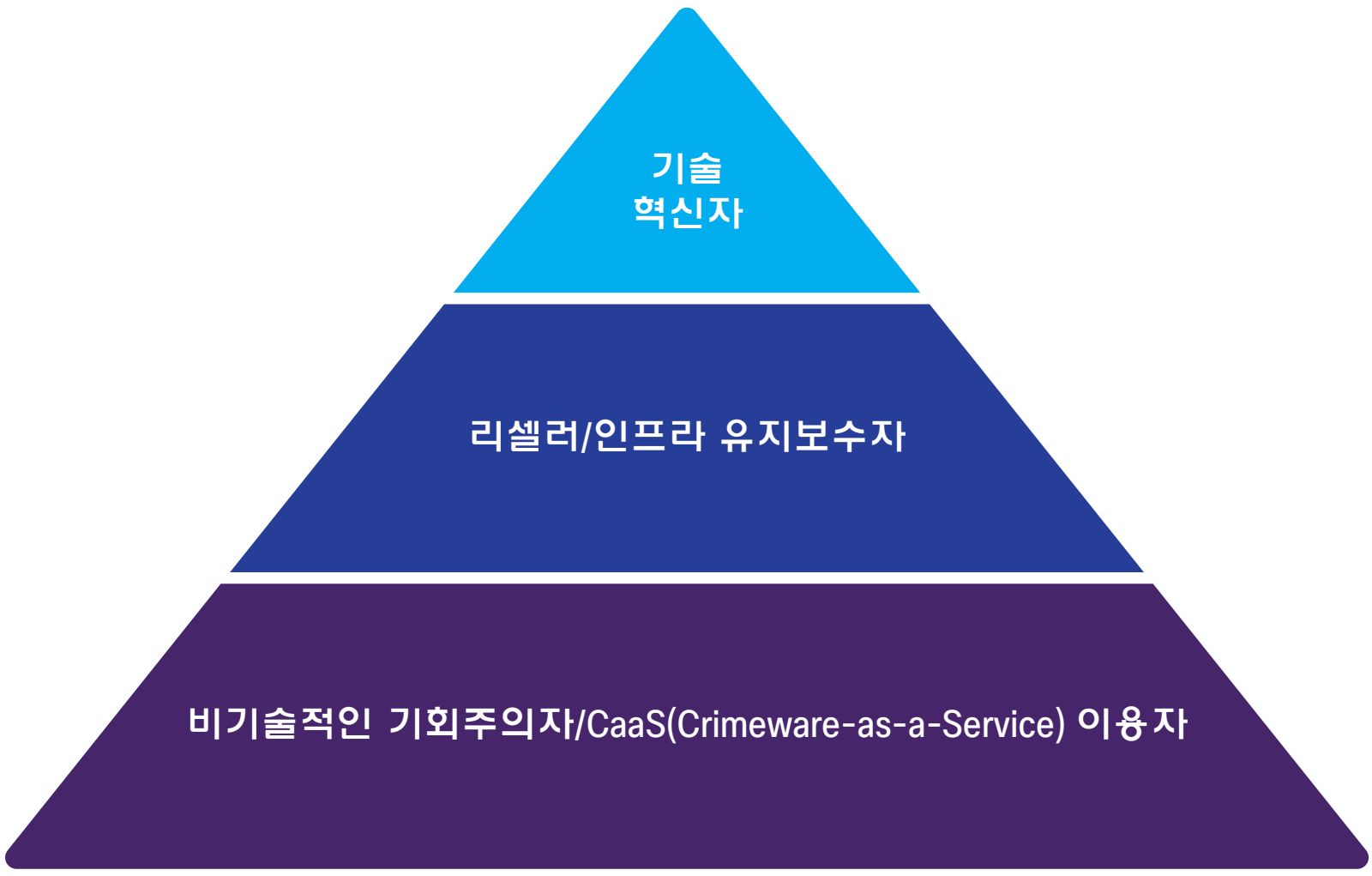
사이버 범죄 네트워크는 확장, 강화되고 있으며 점점 더 많은 숫자가 합법적이고 정교한 비즈니스 네트워크처럼 운영되고 있습니다. 오늘날의 사이버 범죄 계층 구조는 피라미드 형태입니다 (그림 1 참조). 가장 아래에는 공격 활동을 통해 돈을 벌거나 주장을 펼치거나 이 두 가지 모두를 이루고자 하는 "CaaS (Crimeware-as-a-Service)" 사용자와 비기술적 기회주의자가 있습니다. 중앙에는 "중개인" 인 리셀러와 인프라 유지보수자가 있고, 가장 위에는 사법당국의 주요 검거 대상이나 쉽게 찾지 못하는 주요 활동가인 기술 혁신자가 있습니다.

오늘날의 사이버 범죄자들은 뚜렷한 비즈니스 목표를 가지고 공격을 시작합니다. 이들은 원하는 정보가 무엇인지, 어떤 결과를 얻고 싶은지, 이러한 목표를 달성하기 위해 어떤 과정을 거쳐야 하는지 잘 알고 있습니다. 공격자들은 소셜 네트워크상에서 공개된 정보를 통해 많은 시간을 들여 대상에 대해 연구하고 전략적으로 목표를 계획합니다.

또한, 소위 "지하 경제" 에 속하는 많은 관련인들이 어떤 보안 기술이 구축되어 있는지 등 환경에 대한 정보를 수집하는 감시 멀웨어를 유포하여 공격 대상을 정합니다. 일부 멀웨어 제작자들은 이러한 공격 전 정찰을 통해 자신의 멀웨어의 성능을 확인합니다. 그들이 설계한 고급 멀웨어가 일단 네트워크에 심어지면 외부의 C&C (command-and-control) 서버와 통신할 수 있으며, 인프라에서 멀웨어를 측면으로 확산시켜서 중요한 데이터를 탈취하거나 핵심 시스템을 중단시키는 등 임무를 수행합니다.

그림 1

사이버 범죄 계층 구조



신뢰성 저하

시스템, 애플리케이션 그리고 사용자가 알고 지내는 사람들과 기업들에 대해 사용자가 갖고 있는 신뢰를 악용하는 위협은 이제 사이버 세계에 완전하게 정착 되었습니다.

대부분의 방식을 해부해 보면 그 중심에는 신뢰를 악용하는 측면이 있습니다. 주요 웹사이트를 합법적으로 탐색하는 사용자에게 멀웨어를 유포하는 경우, 유명한 회사에서 보낸 것처럼 보이지만 악성 사이트로 연결되는 링크가 포함되어 있는 스팸 이메일, 멀웨어에 감염되어 있는 타사 모바일 애플리케이션을 유명 온라인 마켓플레이스에서 다운로드하는 경우, 내부 직원이 정보 액세스 권한을 이용하여 고용주로부터 지적 재산을 가로채는 것 등이 그 예입니다.

모든 사용자는 기본적으로 사이버 세계에 존재하는 어떤 대상도 신뢰할 수 없고 신뢰해서도 안 된다고 간주해야 할 것입니다. 또한 보안 전문가조차도 모든 네트워크 트래픽을 불신하거나[3] 기업에 기술을 제공하는 공급업체 또는 공급망의 보안 방식을 신뢰하지 않는 것이 조직에 도움이 될 수 있을 것입니다. 하지만 공공 및 민간 부문의 조직, 개인 사용자 및 심지어 국가들까지도 그들이 일상적으로 의존하는 기초 기술을 신뢰할 수 있다는 보장을 연전히 원합니다.

모든 사용자는 기본적으로 사이버 세계에 존재하는 어떤 대상도 신뢰할 수 없고 신뢰해서도 안 된다고 간주해야 합니다.

이런 보안에 대한 확신이 필요해지면서 정부 기관과 기타 그룹이 기술 제품의 신뢰성을 보장하는 데 반드시 갖춰야할 요건을 정의할 수 있게 하는 언어이자 프레임워크인 정보 기술 보안 평가를 위한 국제 공통 기준 (Common Criteria for Information Technology Security Evaluation) 이 더욱 발전하는데 도움이 되었습니다. 현재 미국을 비롯하여 26 개국이 참가 정부의 상호 인증을 평가 제품에 부여하는 다국간 협약인 공통 기준 인정 협정 (Common Criteria Recognition Arrangement) 에 가입되어 있습니다.

하지만 2013 년, 일반적으로 신뢰에 큰 위기가 있었습니다. 그 기폭제는 에드워드 스노든 (Edward Snowden) 이 있었습니다. 미국 정부에서 계약직으로 일했던 에드워드 스노든은 영국의 가디언지 (The Guardian) 에 미 국가안보국 (NSA) 에서 일하면서 얻은 정보를 누설했습니다.[4]

스노든이 지금까지 언론에 누설한 정보에는 NSA 의 전자 감시 및 데이터 수집 프로그램인 PRISM[5] 은 물론 주요 인터넷 회사의 해외 데이터 센터로부터 트래픽을 전송하는 광섬유 네트워크를 도 청한 것으로 추정되는 MUSCULAR 로 알려진 별도의 NSA-GCHQ[6] 프로그램에 대한 자세한 정보가 포함됩니다.[7]

정부의 감시 관행에 대한 스노든의 폭로로 인하여 국가와 국가 사이, 정부와 민간 부문 사이, 국민과 정부 사이, 국민과 공공 및 민간 부문의 조직 사이 등 다양한 단계의 신뢰가 무너졌습니다. 또한 기술 제품에서 의도적이지 않은 취약성과 의도적인 "백도어" 의 존재 및 잠재적인 위험성에 대한 우려와 공급업체들이 최종 사용자를 보호하고 이러한 취약점에 대처하기 위해 충분한 조치를 취하고 있는지에 대한 우려가 자연스럽게 대두 되었습니다.

2014 년 주요 보안 과제

[이렇게 신뢰가 무너지면서 어떤 시스템과 관계가 믿을 만 한것인지 구분하기가 점점 더 어려워지고 있으며 조직은 보안을 약화시키는 다음과 같은 몇 가지 문제와 마주하게 되었습니다.

1 | 더 넓어진 공격 영역
2 | 공격 모델의 확산과 정교함
3 | 위협과 솔루션의 복잡성]

이렇게 복합적인 문제로 인해 악의적인 행위자가 조직이 미처 보안 취약점을 보완하기도 전에 공격을 감행할 수 있는 보안 틈새가 생성되고 악화됩니다.

이러한 위협과 위험성에 대해 앞으로 더욱 자세히 살펴보겠습니다.

1 | 더 넓어진 공격 영역

오늘날의 공격 영역은 악의적인 행위자가 대규모의 취약한 보안 에코시스템을 약화시킬 수 있도록 무한한 가능성을 열어줍니다. 이 영역은 기하급수적으로 늘어났고 여전히 확장 중이며 많은 엔드포인트, 활로, 데이터 등이 여전히 기업의 제어를 받지 않고 있습니다.

데이터는 돈이나 다름없기 때문에, 데이터는 공격자들이 활동을 통해 노리는 주요 대상이 됩니다. 데이터에 "시가" 가 있다면 대기업의 지적 재산이든 개인의 건강 기록이든 데이터는 가치가 있으므로 위험에 처해 있습니다. 대상의 가치가 보안을 침해할 때의 위험보다 크다면 해킹 대상이 될 것입니다. 소규모의 조직도 해킹당할 위험에 처해 있습니다. 그리고 크든 작든 대부분의 조직은 이미 보안침해된 상태이지만 그 사실조차 모르고 있습니다. Cisco 에서 분석한 비즈니스 네트워크 모두 (100%) 에게서 멀웨어를 호스팅하는 웹사이트에 방문한 트래픽이 발견되었습니다.

그림 2

최신 위협 세부 분석

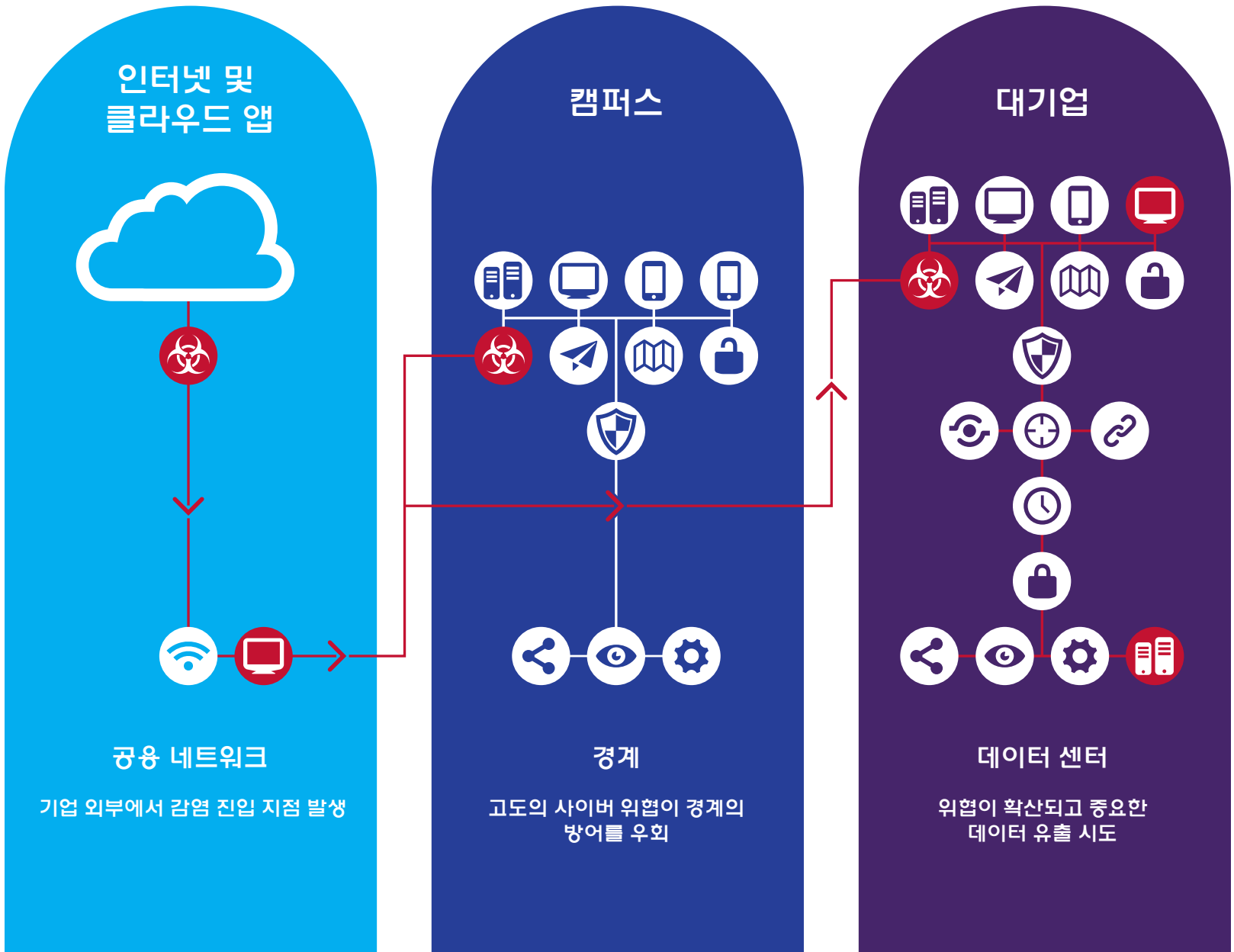


그림 2 에 요약된 최신 위협의 세부 분석에 많은 사이버 범죄 활동의 최종 목적은 데이터 센터에 침투해 중요한 데이터를 탈취하는 것임이 강조되어 있습니다. 이 예시에서, 기업 네트워크 외부의 장치에서 악의적인 활동이 발생합니다. 이렇게 감염시키고 이어서 캠퍼스의 네트워크까지 이동합니다. 이 네트워크는 기업 네트워크로 향하는 발사대 역할을 하게 되며 최종 목표인 데이터 센터가 위협받게 됩니다.

많은 사이버 범죄 공격의 최종 목적은 데이터 센터에 침투해 중요한 데이터를 유출하는 것입니다.

공격 영역이 확대되고 귀중한 데이터가 해킹의 대상이 되는 추세를 감안하여 Cisco 보안 전문가들은 기업에게 "핵심 데이터가 어디에 보관되는가?" 그리고 "클라우드 컴퓨팅 및 모빌리티와 같은 새로운 비즈니스 모델을 제어하기 어려운 상황에서 어떻게 데이터 보호를 위한 안전한 환경을 구축할 수 있을까?" 라는 두 가지 질문에 대해 2014 년에 해답을 찾을 것을 권고하고 있습니다.

2 | 공격 모델의 확산과 정교함

오늘날의 위협 환경은 10 년 전과는 전혀 다릅니다. 기존의 보안 공격이 차단 가능한 정도의 피해를 주는 단순한 공격이었다면 오늘날의 사이버 범죄는 충분한 자금력과 정교한 기술력을 기반으로 심각한 피해를 주고 있습니다.

사이버 범죄의 주요 공격 대상은 기업입니다. 이러한 공격은 감지하기가 매우 어려우며 오랜 시간 동안 네트워크에 머물면서 다른 곳에서 공격을 실행하기 위한 네트워크 리소스를 축적합니다.

공격 전반에 대처하기 위해, 조직은 네트워크, 엔드포인트, 모바일 기기, 가상 환경 등 위협이 발생할 수 있는 모든 위치에서 동작하는 솔루션을 이용하여 폭넓은 공격 벡터에 대응해야 합니다.

> "핵심 데이터가 어디에 보관되는가?", "클라우드 컴퓨팅 및 모빌리티와 같이 기업의 제어가 어려운 새로운 비즈니스 모델에서 어떻게 하면 데이터 보호를 위한 안전한 환경을 구축할 수 있을까?"
>
> Cisco 보안 전문가

3 | 위협과 솔루션의 복잡성

스팸 차단 기능과 안티 바이러스 소프트웨어만으로 네트워크 경계에서 대부분의 위협을 쉽게 감지할 수 있었던 시절은 지나갔습니다. 오늘날의 네트워크는 기존 경계를 넘어 끊임없이 발전하고 있으며 모바일 기기, 웹 지원 및 모바일 애플리케이션, 하이퍼바이저, 소셜 미디어, 웹 브라우저, 가정용 컴퓨터 및 심지어 차량까지 새로운 공격 벡터를 낳고 있습니다. 특정 시점에 적용하는 솔루션으로는 악의적인 행위자가 사용하는 수많은 기술과 전략에 대응하지 못합니다. 이런 점 때문에 보안 팀이 정보 보안을 모니터링하고 관리하기가 더욱 어려워지고 있습니다.

기업이 세분화 된 포인트 솔루션과 여러 관리 플랫폼을 사용하기 때문에 조직의 취약성이 악화되고 있습니다. 그 결과 여러 컨트로 포인트에 걸쳐 서로 연동되지 않는 일련의 서로 다른 기술이 존재하게 되었습니다. 이는 고객 정보, 지적 재산 및 기타 민감한 정보의 보안침해 가능성을 높이며 회사의 명성을 위험에 빠뜨립니다.

특정 시점 솔루션으로는 악의적인 사용자가 사용하는 수많은 기술과 전략에 일일이 대응하지 못합니다.

복잡한 위협 환경 문제를 가장 잘 해결할 수 있는 지속적인 기능이 필요합니다. 무차별적인 공격이 특정 시점에만 발생하는 것이 아니라 지속적으로 발생하기 때문입니다. 또한, 기업의 방어도 지속적이어야 합니다.

위협과 관련 솔루션의 복잡성이 사상 최고치에 달한 시점에서 조직은 보안 전략을 재고할 필요가 있습니다. 포인트 솔루션에 의존하는 대신 네트워크 패브릭 자체에 보안을 통합하여 복잡성을 최소화하면 네트워크에서 다음이 가능하게 됩니다.

- 지속적으로 파일을 모니터링 및 분석하고 악의적인 후속 활동이 실행될 때마다 이를 식별합니다.
- 네트워킹 장치를 배치할 영역을 확장하여 조직이 더 실행을 강화할 수 있도록 지원합니다.
- 보다 많은 트래픽을 감시할 수 있으므로 감지 시간이 빨리집니다.
- 보안용 장치에만 의존해서는 얻을 수 없는 고유한 상황 인식을 종합할 수 있는 기능을 조직에 제공합니다.

모바일과 클라우드 서비스로의 전환으로 인하여 일부는 기업 네트워크와 한번도 연결되지 않을 엔드포인트와 모바일 기기의 보안에 대한 부담이 늘어나고 있습니다. 모바일 기기를 사용하여 회사 리소스에 액세스하는 경우 보안 위험에 노출되는 것이 사실이며 기업의 제어를 받지 않는 잠재적으로 알 수 없는 보안 상태의 타사 클라우드 서비스와 컴퓨터에 쉽게 연결됩니다. 또한 모바일 멀웨어도 증가하고 있어 위험은 한층 더 커집니다. 가장 기본적인 가시성도 부족한 상태에서 대부분의 IT 보안 팀은 이러한 장치에서 잠재적인 위협을 식별할 수 있는 능력이 없습니다.

모바일 기기를 사용하여 회사 리소스에 액세스하는 경우 보안 위험에 노출됩니다.

지속적 기능과 같은 발전된 접근법이 빅 데이터 분석을 통해 정교한 멀웨어를 대처하는 데 더 큰역할을 하게 될 것입니다. 빅데이터 분석은 파일이 네트워크로 이동하거나 엔드포인트 사이를 이동한 후에도 더 높은 가시성을 제공할 수 있도록 확장된 네트워크 전반에서 데이터와 이벤트를 종합합니다. 이는 초기의 특정 시점에 파일을 스캔하여 멀웨어 위치를 파악하는 특정 시점 엔드포인트 보안과 차별화됩니다. 정교한 멀웨어는 이러한 스캔을 피해서 엔드포인트에 빠르게 자리 잡은 후 네트워크 곳곳으로 확산할 수 있습니다.

신뢰할 수 있는 투명한 시스템

더 넓어진 공격 영역, 공격 모델의 확산과 정교함, 위협과 솔루션의 복잡성을 감안할 때, 네트워크 서비스에 어떻게 액세스하는지 와는 상관없이 소비 대상 정보와 해당 정보를 제공하는 시스템을 신뢰할 수 있어야 합니다.

점점 더 많은 정부와 기업이 모빌리티, 협업, 클라우드 컴퓨팅 및 기타 다른 가상화 형태에 투자하고 있기 때문에 정말로 안전한 네트워크를 만드는 것이 더 복잡해졌습니다. 이런 기능이 복원력 개선, 효율성 향상, 비용 절감에는 도움이 되지만 추가적인 위험이 발생합니다. 모조품과 변조된 제품에 대한 문제가 점점 늘어나면서 IT 제품의 제조 과정의 보안도 위험한 상태입니다. 그 결과, 오늘날의 정부와 기업 경영진은 압도적으로 사이버 보안 및 이와 관련된 신뢰 문제를 최대 관심사로 꼽고 있습니다. 보안 실무자들은 "곧 보안침해가 발생할 것을 알게 됐다면 무엇을 다르게 할 것인가?" 라고 자문해야 합니다.

악의적인 행위자들은 기술 공급망에 존재하는 모든 보안 취약점을 찾아 공격합니다. 기술 제품의 취약성과 의도적인 백도어는 결국 공격자들에게 "조직 전체" 에 대한 액세스를 제공할 수도 있습니다. 백도어는 오래전부터 보안 문제가 되어왔으며 은밀한 활동이나 범죄 활동을 용이하게 하는 백도어에 대해 조직은 관심을 가져야 할 것입니다.

신뢰할 수 있는 시스템을 개발한다는 것은 제품 라이프사이클의 처음부터 끝까지 철저하게 보안을 구축하는 것을 의미합니다. CSDL (Cisco Secure Development Life) 라이프사이클[8] 은 제품 구상 단계에서 제품 보안을 구축하고 개발 중에 취약점을 최소화하며 공격을 당했을 때 제품의 복원력을 향상하도록 설계된 반복 가능하고 측정 가능한 방법을 규정하고 있습니다.

악의적인 사용자들은 기술 공급망에 존재하는 모든 보안 취약점을 찾아 공격합니다.

신뢰할 수 있는 시스템은 새로운 위협을 예측하고 미연에 방지할 수 있는 지속적인 보안 개선 방법의 기반이 됩니다. 이러한 인프라는 핵심 정보를 보호할 뿐만 아니라 더욱 중요하게는 핵심 서비스 중단을 피할 수 있습니다. 신뢰받는 공급업체가 지원하는 신뢰할 수 있는 제품을 통해 사용자들은 정보의 남용, 서비스 중단 및 정보 침해에 의한 비용과 평판의 손상을 최소화 할 수 있습니다.

하지만 신뢰할 수 있는 시스템이라고 해서 외부 공격을 완전히 차단할 수 있는 것은 아닙니다. IT 고객과 사용자는 운영을 방해하는 공격을 방어하여 신뢰할 수 있는 시스템의 효율성을 유지하는 데 중요한 역할을 담당하고 있습니다. 여기에는 보안 중심의 업데이트 및 패치 설치, 비정상적인 시스템 동작을 감지하기 위한 끊임없는 경계 및 공격에 대한 효율적인 대책이 포함됩니다.

오늘날 CISO 의 2014 년 주요 과제

오늘날의 위협 환경을 조사하는 CISO (Chief Information Security Officer) 는 테라바이트급의 데이터를 보호하고 엄격한 규정 준수 요건을 충족하며 타사 공급업체와 작업할 때의 위험을 평가하면서 이 모든 작업을 더욱 적은 예산과 제한된 IT 팀을 통해 수행해야 한다는 거대한 과제에 직면해 있습니다. 또한 CISO 는 그 어느 때보다 많은 업무를 수행하고 정교하고 복잡한 위협을 관리해야 합니다. 조직을 위한 보안 접근 방식과 관련해 CISO 에게 조언을 제공하는 Cisco 보안 서비스의 주요 보안 전략 담당자들은 다음과 같이 2014 년의 가장 시급한 문제 및 과제의 목록을 제시합니다.

규정 준수 관리

점점 취약해지는 네트워크 전반에 상주하는 데이터를 보호하고 중요한 리소스를 규정 준수에 포함시키는 것은 CISO 의 가장 일반적인 과제일 것입니다. 보안은 규정 준수만으로는 완벽하게 보장되지 않습니다. 규정 준수는 특수한 규제 환경의 요구 사항에 중점을 둔 최소한의 기준일 뿐입니다. 반면 보안이란 모든 비즈니스 활동을 아우르는 포괄적인 접근 방식입니다.

클라우드 신뢰성

CISO 는 제한된 예산 및 시간 내에서 정보를 안전하게 관리할

다음 페이지에 계속

기술은 계속 발전하고 있으며 공격자들 역시 마찬가지입니다. 시스템의 신뢰성을 보장하려면 네트워크의 초기 설계에서부터 제조, 시스템 통합, 일상적인 운영, 유지보수 및 업데이트 그리고 최종적으로 솔루션의 폐기에 이르는 전체 라이프사이클을 모두 포괄할 수 있어야 합니다.

조직의 고유한 네트워크뿐 아니라 조직이 접속하는 네트워크에까지 신뢰할 수 있는 시스템에 대한 요구가 확대되고 있습니다. Cisco 의 보안 연구 및 운영 팀은 "피봇팅 (pivoting)" 의 사용이 지난 한 해 동안 증가하는 것을 관측했습니다. 사이버 범죄에서 피봇팅이란 주요 에너지 회사의 네트워크나 금융 기관의 데이터 센터와 같은 대형 목표물을 상대로 보다 정교한 전략을 실행하는 기반으로 백도어나 취약점을 이용하거나 공격망의 일부 지점에서 신뢰를 악용하는 것을 의미합니다. 일부 해커들은 조직 사이에 존재하는 신뢰를 피봇팅의 기반으로 이용하여 신뢰받고 있는 비즈니스 파트너를 공격한 다음 수상한 낌새를 차리지 못한 신뢰받고 있는 또 다른 비즈니스 또는 정부 파트너를 공격하고 있습니다.

지금과 같은 위협 환경에는 경계 강화가 필요합니다. 보안은 독립적으로 확인할 수 있는 데이터 및 프로세스를 바탕으로 측정 가능하고 객관적인 방식으로 시스템의 신뢰를 검증함으로써 기업 IT 환경의 일부인 모든 과도적 상태에 도입되어야 합니다. 가장 지속 가능한 접근법은 조직의 고유한 환경에 맞게 구축된 동적 방어로, 여기에는 지속적으로 진화하여 관련성을 유지하는 보안 제어 기능이 포함됩니다.[9]

이런 환경에 신뢰할 수 있는 시스템이 존재할 수 있으며 이러한 시스템을 구축하기 위해서는 투명성이 필수적입니다. "신뢰할 수 있는 시스템은 제품 개발 방식, 신뢰할 수 있는 공급망 및 네트워크 설계, 구현 및 정책으로 구성된 구조적인 접근법과 같은 강력한 기초를 토대로 구축되어야 합니다." 라고 John N. Stewart Cisco 상무 겸 최고 보안 책임자는 말합니다. "하지만 가장 중요한 요소는 공급업체의 투명성입니다."

이전 페이지에서 이어짐

방법을 결정해야 합니다. 예를 들어 클라우드는 점점 증가하는 데이터의 저장소를 경제적이고 민첩하게 관리할 수 있는 방법이지만 클라우드와 관련된 CISO 의 우려는 더욱 커지게 되었습니다. CEO 및 경영진은 많은 비용이 드는 하드웨어를 대체할 완벽한 해결책으로 클라우드를 꼽고 있습니다. 이들은 데이터를 클라우드로 오프로드함으로써 이점을 얻기를 원하며 CISO 가 이러한 작업을 안전하고 신속하게 수행해 줄 것이라고 기대합니다.

공급업체 신뢰성

클라우드의 경우와 마찬가지로 조직은 전문 솔루션 제공을 위해 공급업체를 활용하고자 합니다. 비용 측면에서 볼 때 타사를 활용하는 것은 합리적인 방법입니다. 하지만 타사 공급업체들이 강력한 방어책을 갖추지 못할 수 있다는 점을 알고 있는 범죄자들이 이러한 공급업체를 주요 공격 대상으로 삼게 됩니다.

보안 침해에 대한 대처

모든 조직은 이미 해킹을 당한 적이 있거나 앞으로 공격 대상이 될 가능성이 있으며, 다만 시기의 차이가 있을 뿐임을 인식해야 합니다. 많은 CISO 들이 Operation Night Dragon, RSA 침입 및 2012 년 발생한 대규모 석유 및 가스 기업에 대한 Shamoon 공격과 같은 최근의 해킹 사건을 기억하고 있습니다. (48 페이지 기업 네트워크에서 성행하는 악의적인 활동에 대한 Cisco 의 조사 결과 참조)

투명성이 높아지면 개인정보보호가 그만큼 힘들어지지만 협력을 통해 적절한 균형을 찾을 수 있습니다. 그러면 위협 분석 정보와 보안 관련 모범 사례를 조정할 수 있는 기회가 더 많아질 것입니다. 많은 부분이 위험에 처한 상황이므로 모든 조직은 신뢰, 투명성 및 개인정보보호 사이에서 적절한 균형을 찾아야 합니다.

장기적으로는 모든 사용자에 대해 사이버 보안을 실현할 수 있으며, 새롭게 떠오르는 IoE (Internet of Everything)[10] 경제의 잠재력을 모두 실현할 수 있습니다. 하지만 이런 목표의 달성 여부는 엔드포인트 및 네트워크에서 보안 부담을 지능적으로 분산시키는 효율적인 개인정보 보호정책과 견고한 네트워크 방어에 달려 있습니다. 단기적으로, 그리고 가장 핵심은, 오늘날의 모든 기업이 최고의 방법과 정보를 사용하여 가장 귀중한 자산을 보호하고 광범위한 사이버 보안 문제의 직접적인 원인이 되지 않도록 책임을 지는 것입니다.

오늘날의 조직들은 점점 커지고 복잡해지는 상호 연결된 사이버 보안 에코시스템에 자사의 보안 관행이 어떤 영향을 미칠지 고려해야 합니다. 이렇게 "큰 그림" 을 고려하지 않는 조직은 명성에 타격을 받게 될 수 있으며 이로 인해 해당 조직의 사이트에 대한 액세스를 허용하는 선두 보안업체가 없어진다는 것을 의미합니다. 일단 블랙리스트에 오르면 돌이키기가 쉽지 않으며 일부는 끝내 회복하지 못할 수도 있습니다.

Cisco Trustworthy Systems 에 대한 자세한 내용은 www.cisco.com/go/trustworthy를 참고하십시오.

위협 분석 정보

Cisco 와 Sourcefire 는 최대 규모의 감지 원격 분석 세트를 이용하여 작년 보안 정보를 분석하고 정리하였습니다.

증가하는 위협 경보

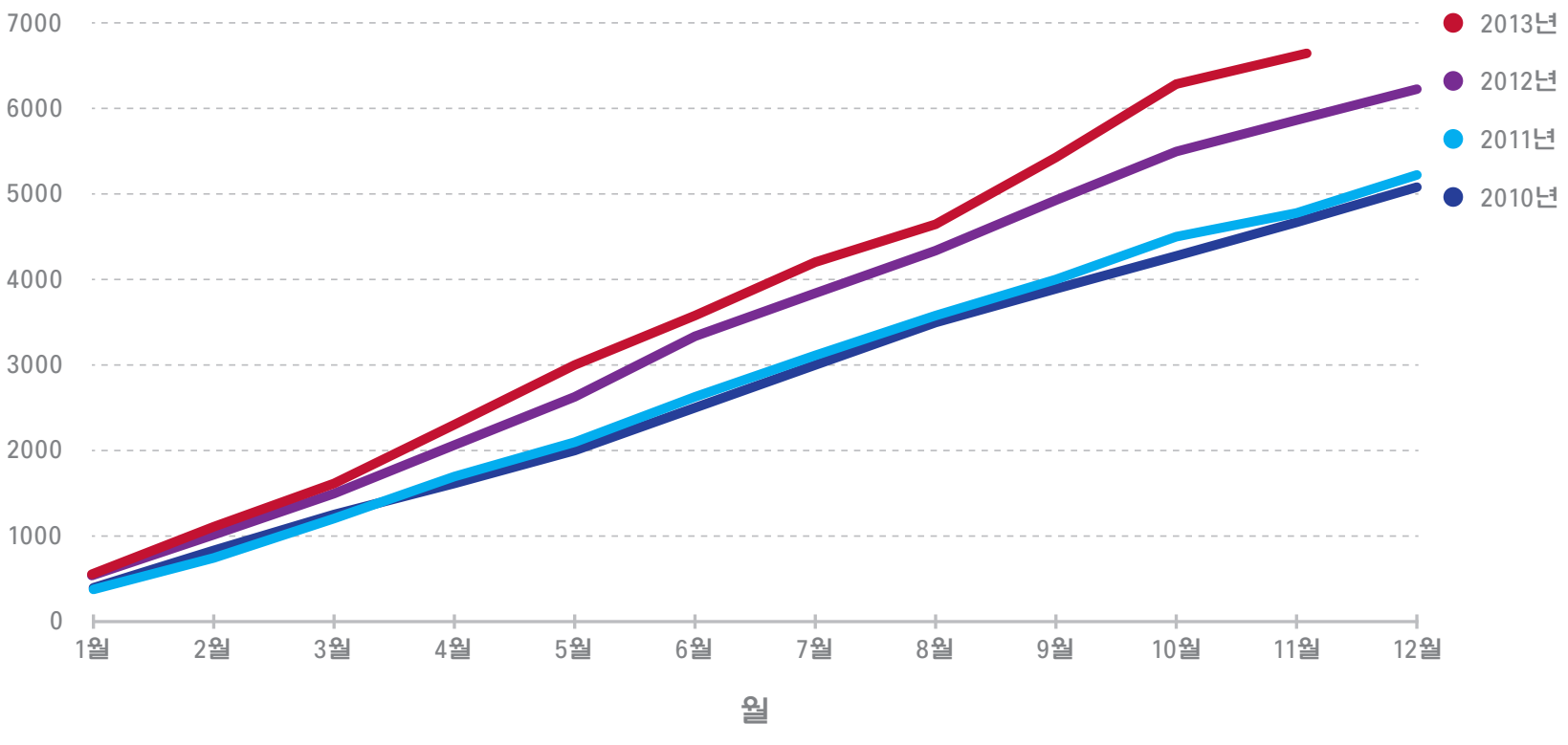
Cisco IntelliShield® 의 보고에 따르면 2013 년에 취약성과 위협이 꾸준한 증가세를 보였습니다. 2013 년 10 월 기준으로 연간 누적 경보가 2012 년에 비해 14% 증가했습니다 (그림 3).

2013 년 10 월에는 IntelliShield 에서 2000 년 5 월에 기록을 시작한 이래 최고 수준에 도달했습니다.

또한 주목해야 할 점은 IntelliShield 의 기록에 의하면 업데이트된 경보와 대조적으로 새로운 경보가 급증했다는 점입니다 (그림 4). 기술 공급업체와 연구원들은 새로운 취약점이 증가하는 것을 관측하였는데 (그림 5), 이런 취약점이 관측되는 것은 매우 안전한 개발 라이프사이클 사용이 더욱 강조되고 있는 것은 물론 자사 제품의 보안이 향상되었기 때문입니다. 새로운 취약점이 급증하는 또 다른 이유로는 제품이 출시되어 취약점이 공격당하기 전에 공급업체에서 자사의 제품 코드를 검사하고 취약점을 보완하고 있다는 신호일 수도 있습니다.

그림 3

2010 년~2013 년 연간 경보 누계



안전한 소프트웨어 개발에 대한 관심이 커지면 공급업체 솔루션의 신뢰성을 쌓을 수 있습니다. 안전한 개발 라이프사이클은 취약성의 위험을 감소시키고 공급업체들이 초기 개발 단계에서 잠재적인 결함을 발견할 수 있게 될 뿐만 아니라 구매자들에게 이 솔루션의 신뢰성에 대한 확신을 줄 수 있습니다.

그림 4

2013 년 새로운 경보 및 업데이트된 경보 수

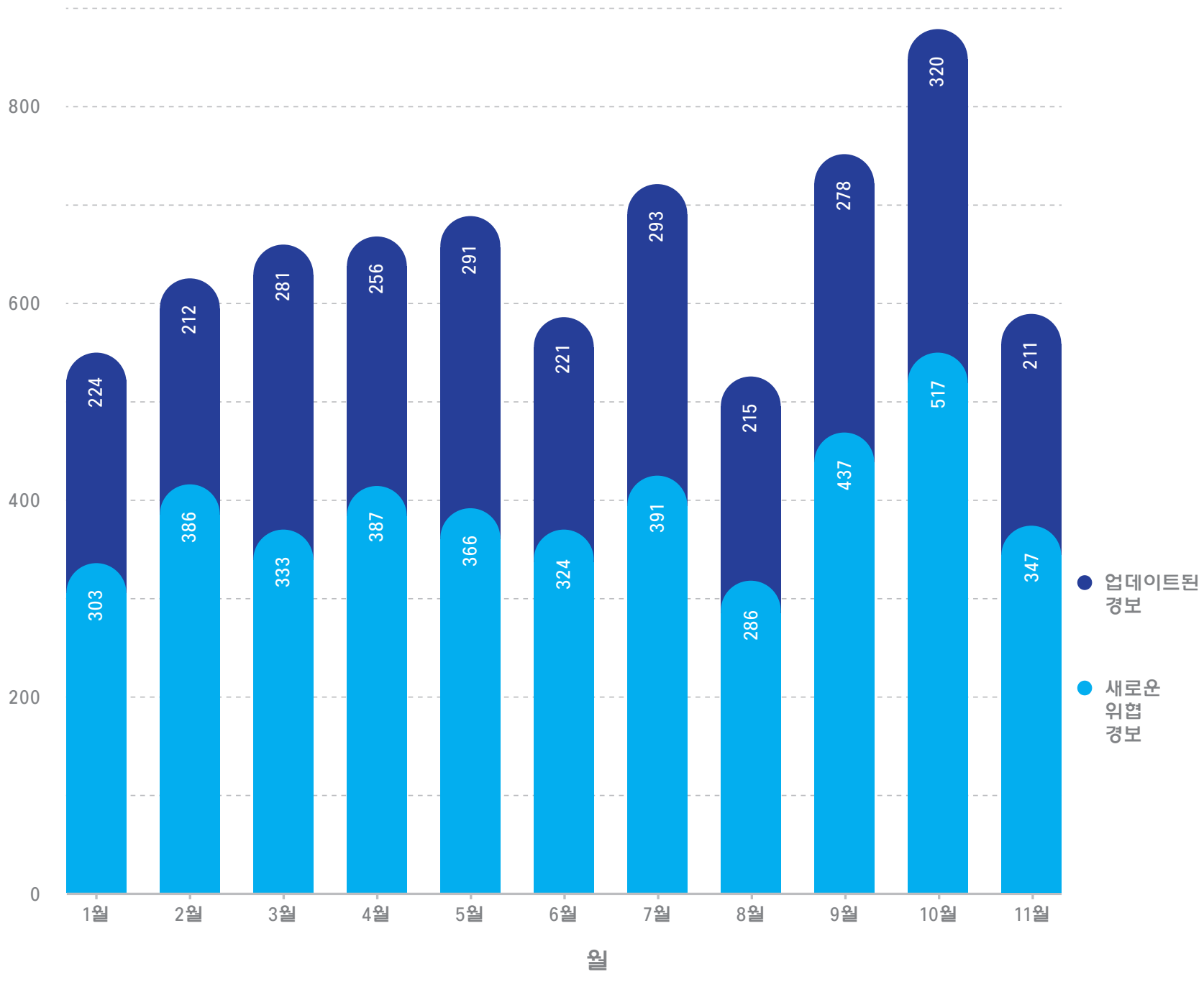


그림 5

Cisco IntelliShield 에서 추적한 일반적인 위협 범주

참조: 이 CWE (Common Weakness Enumeration) 위협 범주는 미국 취약성 데이터베이스 (https://nvd.nist.gov/cwe.cfm)에서 정의한 악의적인 사용자의 네트워크 공격 방법과 일치합니다.

1
CWE-119: 버퍼 오류

2
기타 Intellishield 경고
(활동, 문제, CRR, AMB)

3
CWE-399: 리소스 관리 오류

4
CWE-20: 입력 유효성 검사

5
CWE-264: 승인, 권한
및 액세스 제어

6
CWE-200: 정보 유출/공개

7
CWE-79: XSS(Cross-Site Scripting)

8
CWE-94: 코드 삽입

9
CWE: 설계 오류

CWE-310: 암호화 문제

CWE-287: 인증 문제

CWE-352: CSRF(Cross-Site
Request Forgery)

CWE-22: 경로 탐색

CWE-78: OS 명령 삽입

CWE-89: SQL 인젝션

CWE-362: 경합 상태

CWE-255 인증서 관리

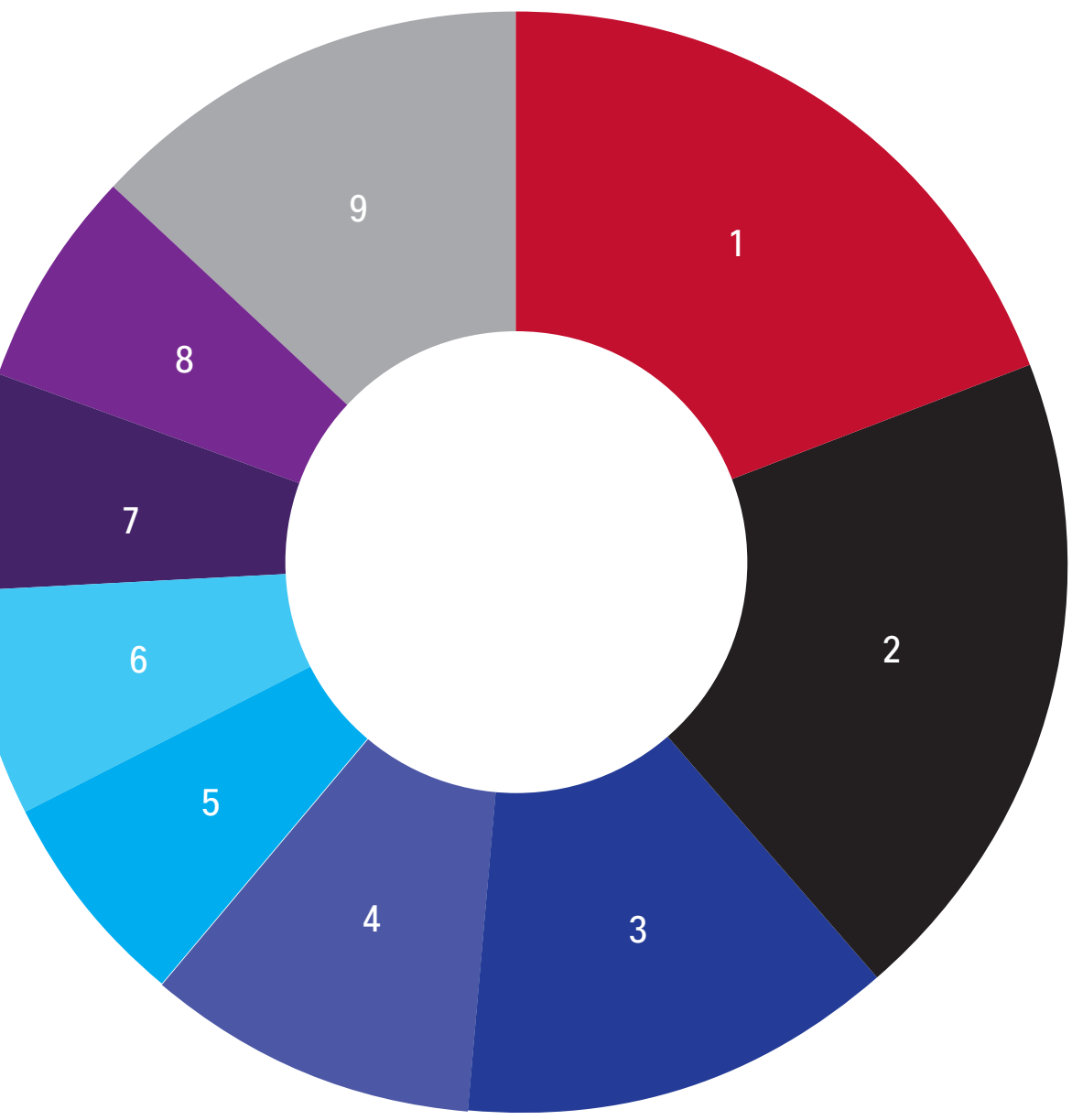
CWE-59: 링크 따라가기

CWE-16: 구성

CWE: 불충분한 정보

CWE: 기타

CWE-189: 숫자 오류



줄어드는 스팸 메일, 여전히 위협적인 악성 스팸

2013 년에는 스팸 메일의 양이 전 세계적으로 하락세를 보였습니다. 그러나 전체적인 양은 줄었어도 악성 스팸의 비율은 비슷한 수준을 유지하고 있습니다.

스팸 유포자들은 빠른 속도를 무기로 이메일 사용자들의 신뢰를 악용하여, 새로운 사건이나 동향으로 인해 수신자의 스팸 사기에 대한 저항이 약화될 때 대량의 스팸을 유포합니다.

2013 년 4 월 15 일에 발생했던 보스턴 마라톤 폭발 사건 후에 대규모 스팸 공격이 발생했습니다. 4 월 16 일과 4 월 17 일에 2 차례에 걸쳐 발생한 이 공격은 폭발 사건으로 인한 영향을 궁금해하는 이메일 사용자들의 관심을 끌도록 설계되었습니다. Cisco 연구원들은 먼저 보스턴 마라톤 폭발이 발생한 후 몇 시간 내에 수백만 건의 폭발 관련 도메인 이름이 등록되었다는 것을 발견했습니다.[11]

두 차례의 스팸 공격 모두 폭발 사건과 관련된 것으로 추정되는 뉴스에 관한 제목이 포함되어 있었으며, 폭발 비디오 또는 유명 언론사의 뉴스로 연결되는 것처럼 보이는 링크가 포함되어 있었습니다. 이 링크를 누르면 실제 뉴스나 비디오로 연결되는 웹 페이지가 열리기는 했지만, 방문객의 컴퓨터를 감염시키는 악성 아이프레임 (iframe) 도 포함되어 있었습니다. 2013 년 4 월 17 일에는, 그 절정에 달하여, 보스턴 마라톤 폭발과 관련된 스팸이 전 세계에 유포된 모든 스팸 메시지 중 40% 를 차지했습니다.

스팸 유포자들은 큰 사건이 발생했을 때 자세한 정보를 알고 싶어하는 사람들의 심리를 이용합니다.

그림 6 은 CNN 뉴스로 위장한 봇넷 (botnet) 의 스팸 공격 중 하나입니다.[12] 그림 7 은 보스턴 마라톤 폭발 스팸 메시지의 소스 HTML 입니다. 마지막 아이프레임 (오퍼스케이티드[obfuscated]) 은 악성 웹사이트용입니다.[13]

뉴스 속보 스팸은 즉각적으로 발생하기 때문에 이메일 사용자들은 스팸 메시지를 합법적인 것으로 더 쉽게 믿어버립니다. 스팸 유포자들은 큰 사건이 발생했을 때 자세한 정보를 알고 싶어하는 사람들의 심리를 이용합니다. 일단 스팸 유포자들이 온라인 사용자가 원하는 내용을 제공하면 감염된 링크를 클릭하는 것과 같이 원하는 행동을 유도하기가 훨씬 쉬워집니다. 또한 사용자들이 메시지에 문제가 있다는 것을 의심하지 않도록 하는 것도 훨씬 쉬워집니다.

그림 6

보스턴 마라톤 스팸

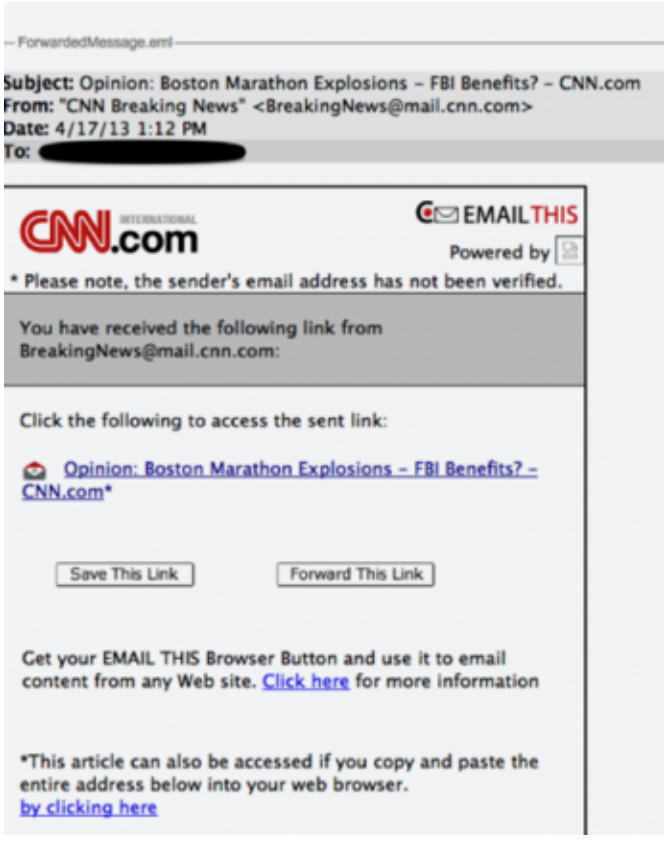
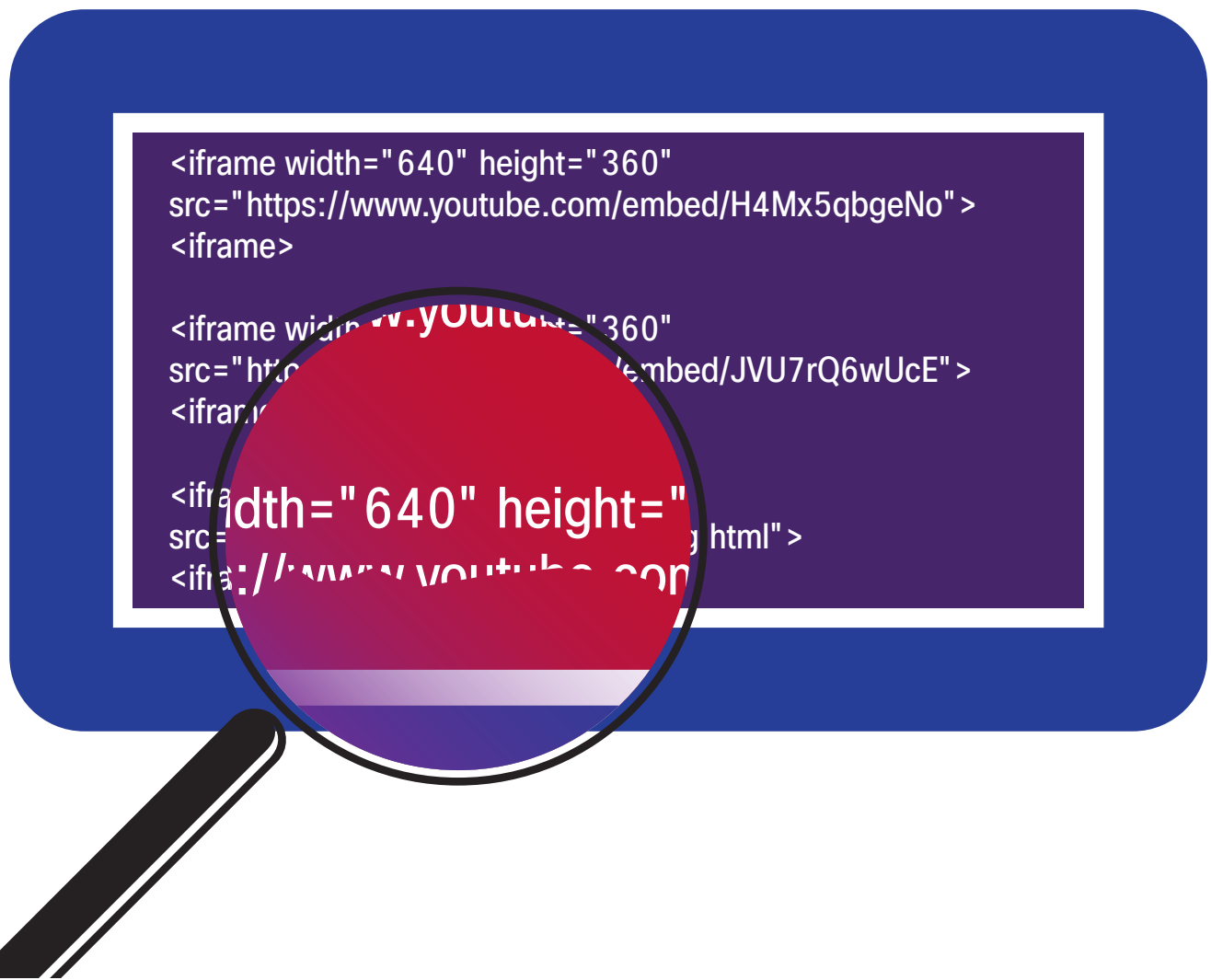


그림 7

보스턴 마라톤 폭발 스팸 메시지의 소스 HTML



스팸의 양

Cisco TRAC (Threat Research Analysis and Communications) /SIO (그림 8) 에 따르면, 그 추세가 국가마다 다르긴 하지만 (그림 9) 전 세계적의 총 스팸의 양은 하락하고 있습니다.

그림 8

2013 년 전 세계 스팸의 양

출처: Cisco TRAC/SIO

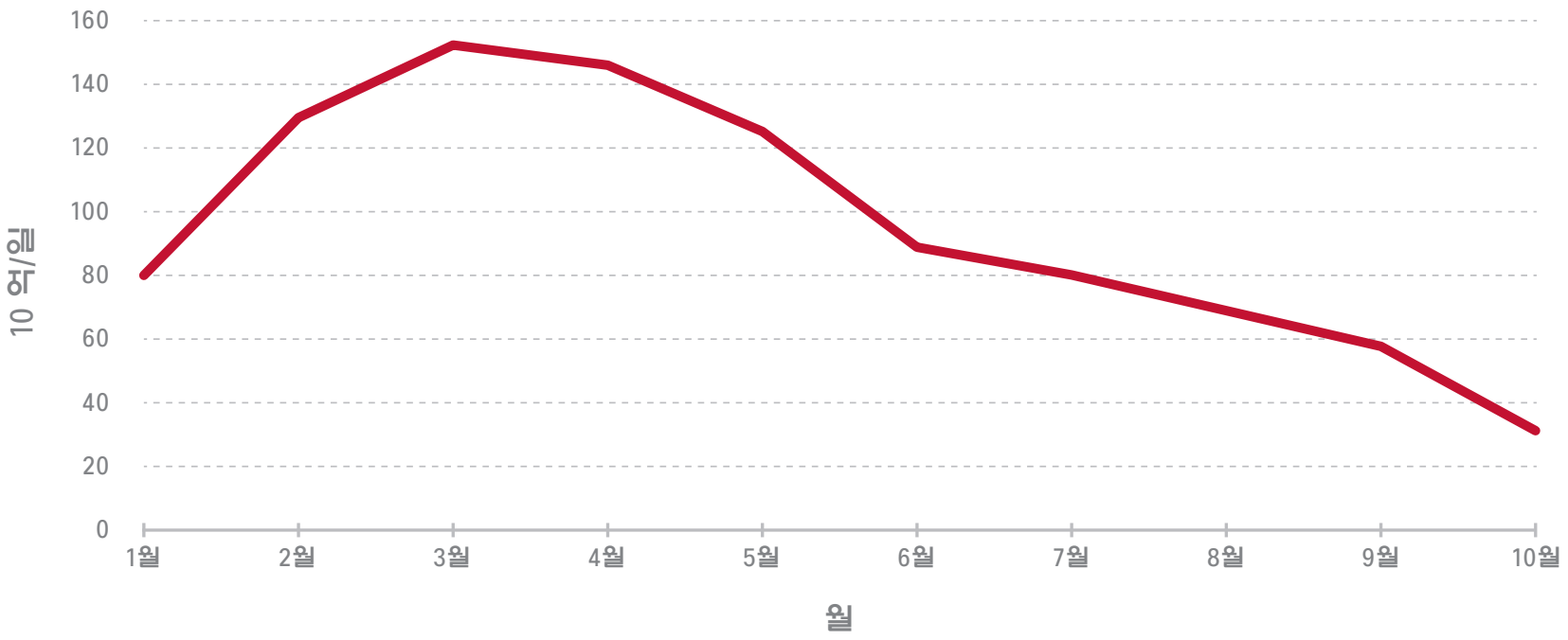


그림 9

2013 년 스팸 양의 추세

출처: Cisco TRAC/SIO

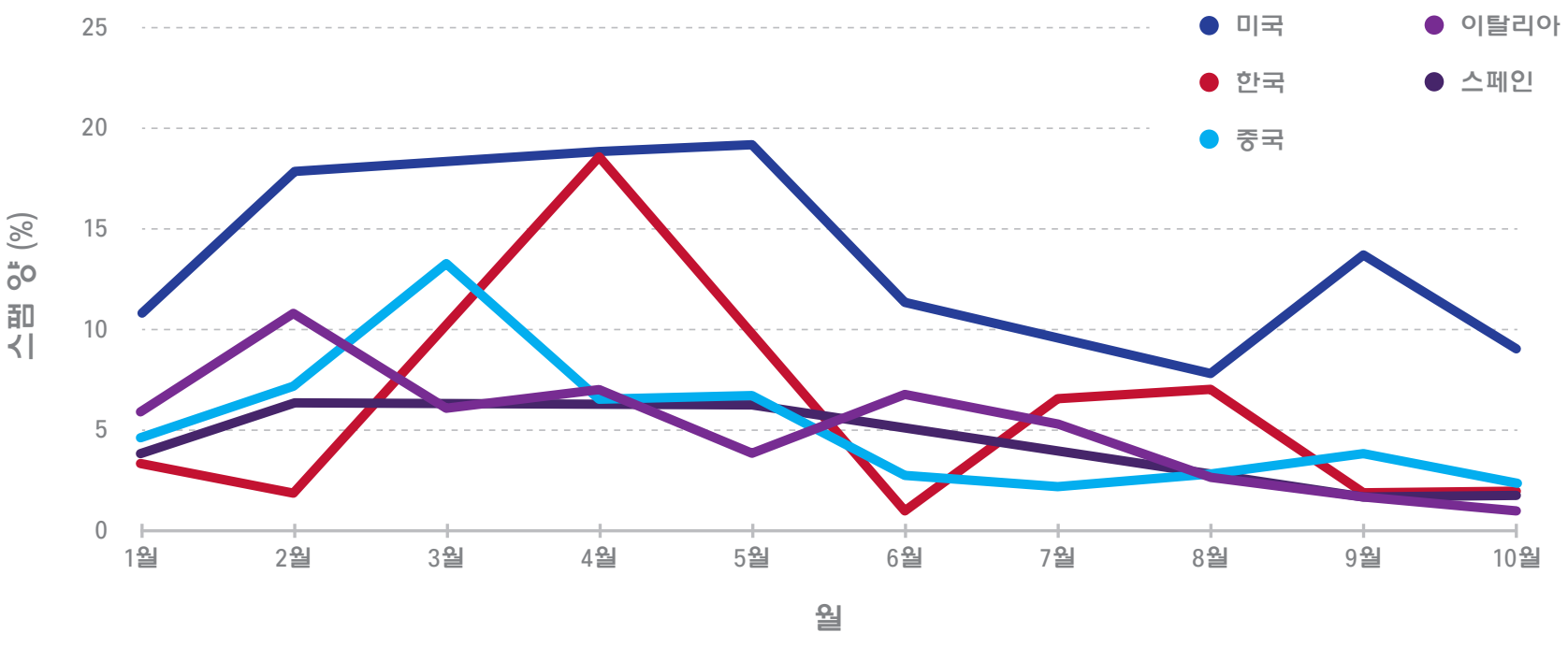


그림 10

전 세계적으로 가장 흔한 스팸 메일 주제

1.
은행 입금/출금 통지
입금, 이체, 결제, 수표 반송, 사기 알림 통지

2.
온라인 상품 구매
제품 주문 확인 및 구매 주문서, 견적, 평가판 요청

3.
첨부 사진
악성 첨부 사진

4.
배송 통지
송장, 배송 또는 픽업, 추적

5.
온라인 데이팅
온라인 데이팅 사이트

6.
세금
세금 서류, 환불, 신고서, 부채 정보, 온라인 세금 납부

7.
페이스북
계정 상태, 업데이트, 통지, 보안 소프트웨어

8.
상품권 또는 바우처
여러 상점으로부터 알림 서비스 (Apple 이 가장 인기)

9.
PayPal
계정 업데이트, 확인, 결제 대금 통지, 결제 대금 분쟁

웹 공격: Java 에서 가장 많이 발생

Cisco 의 데이터에 따르면, 보안을 약화시키는 모든 웹 기반 위협 중에서 사이버 범죄자들이 가장 많이 악용하는 프로그래밍 언어는 여전히 Java 로 나타났습니다.

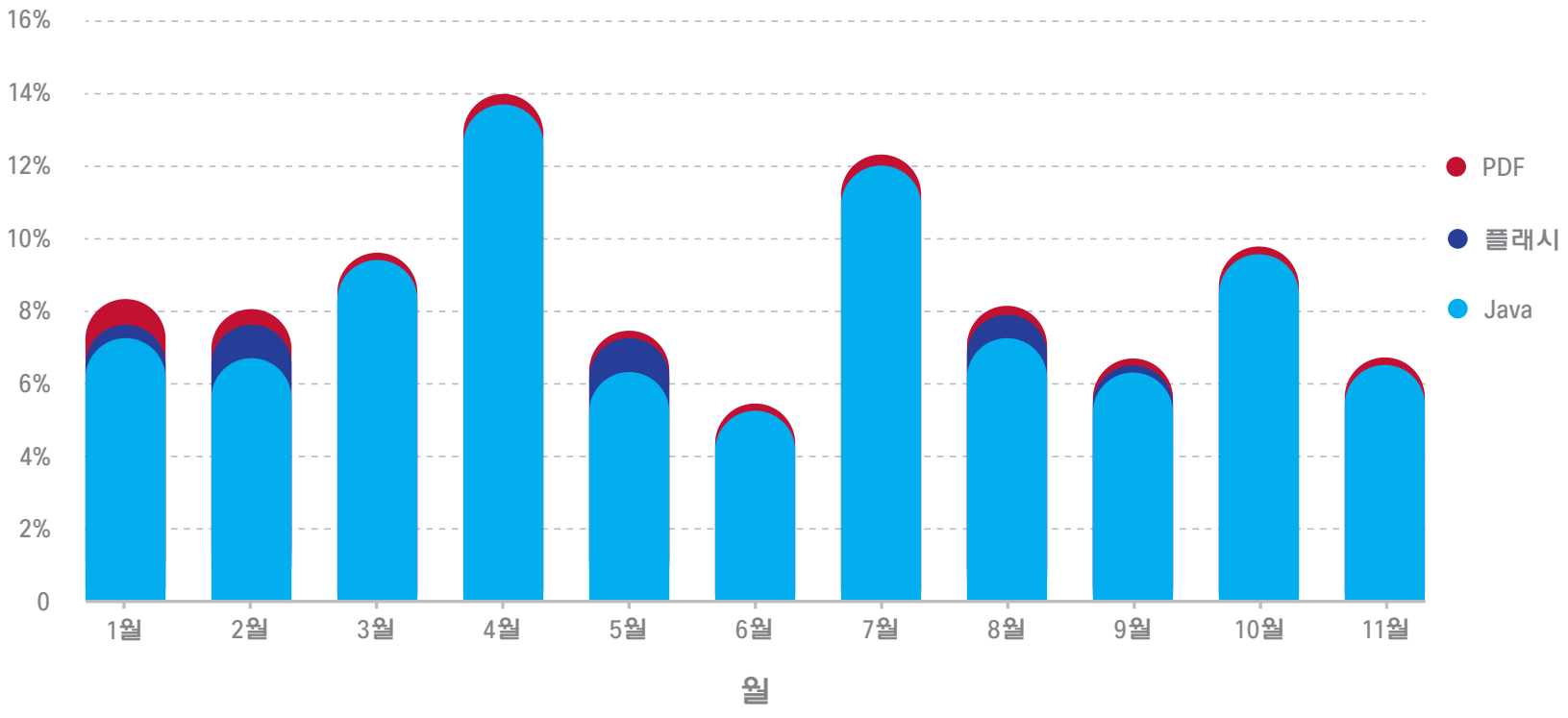
Java 공격은 또 다른 대중적인 사이버 범죄 활동 벡터인 Flash 또는 Adobe PDF 문서 공격보다 훨씬 많습니다 (그림 11).

또한 Cisco 자회사인 Sourcefire 의 데이터에 따르면, Sourcefire 의 고급 멀웨어 분석 및 보호용 FireAMP 솔루션에서 모니터링하는 보안침해 흔적지표 (IoC) 의 대부분 (91%) 을 Java 공격이 차지하고 있는 것으로 나타났습니다 (그림 12). FireAMP 는 엔드포인트에서 실시간으로 보안침해를 감지하고 각 보안침해를 일으킨 소프트웨어의 유형을 기록합니다.

그림 11

2013 년 PDF, Flash 및 Java 를 통해 생성된 악성 공격

출처: Cisco Cloud Web Security 보고서



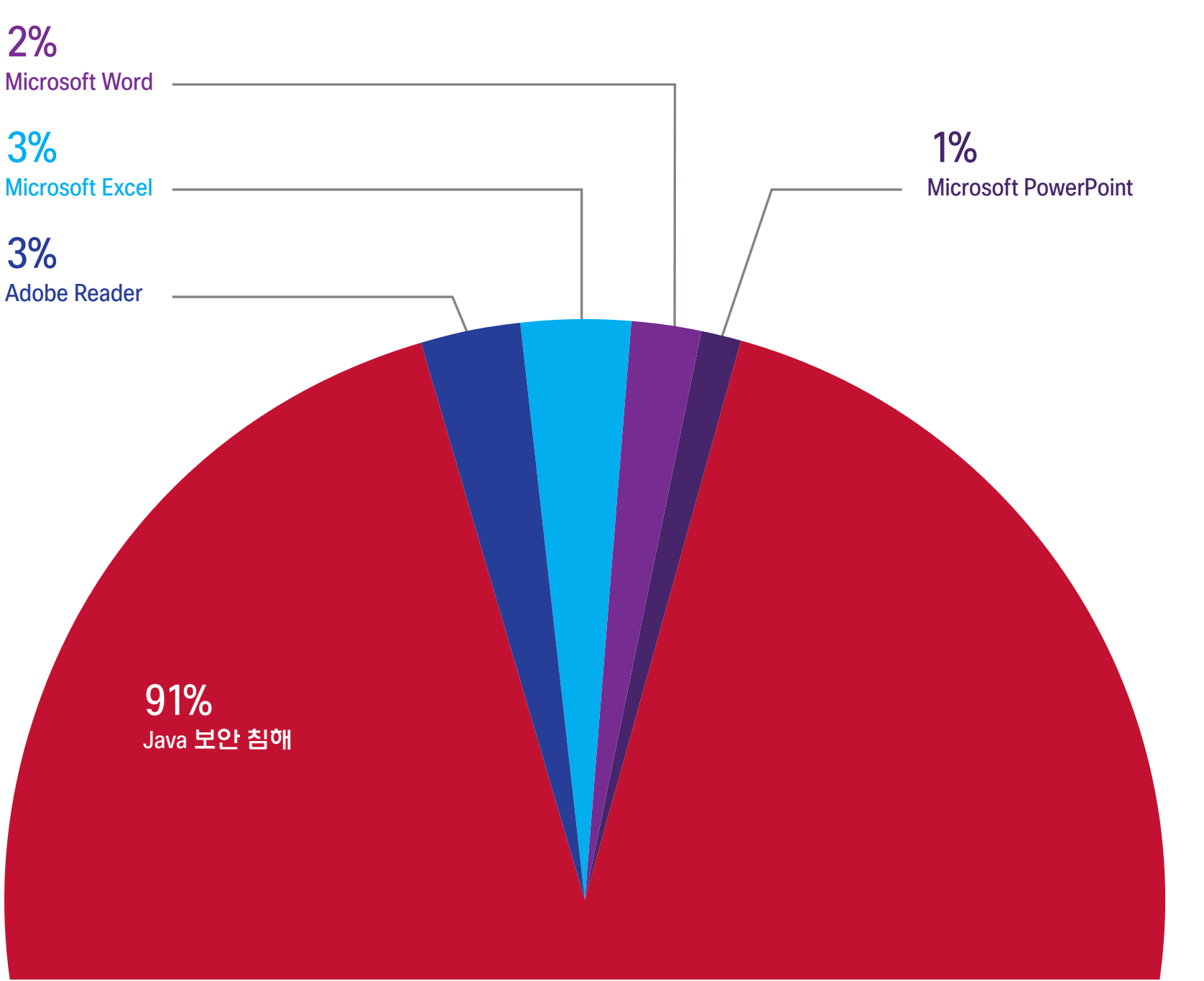
Java 공격과 같은 위협의 경우 보안 실무자들이 직면한 가장 중요한 문제는 멀웨어가 네트워크 환경에 침입하는 방법과 감염을 최소화하기 위해 어디에 노력을 집중시켜야 하는지를 파악하는 것입니다. 개별 동작은 악성이 아닌 것처럼 보일 수 있지만 일련의 사건을 따라가면 멀웨어에 대해 파악할 수 있습니다. 일련의 사건을 따라간다는 것은 악의적인 사용자가 경계 보안을 우회하고 네트워크에 침입하는 데 이용하는 경로를 연결하는 데이터에 대해 사후 분석을 실행할 수 있는 능력을 갖추었다는 것을 의미합니다.

IoC 자체만으로 특정 웹사이트를 방문하는 것이 안전하다는 것을 보여줄 수 있습니다. 따라서 Java 의 실행이 안전한 동작이 되고 실행 파일의 실행 역시 안전하게 됩니다. 하지만 사용자가 아이프레임이 삽입된 웹사이트를 방문하는 경우 조직이 위험에 처하게 되고, Java 가 실행되어 실행 파일을 다운로드하며 해당 파일이 악의적인 동작을 실행합니다.

그림 12

유형별 보안침해 흔적지표

출처: Sourcefire (FireAMP 솔루션)



Java 는 널리 보급되어 사용되기 때문에 사이버 범죄자들이 가장 많이 악용하는 툴이며, 그렇기 때문에 Java 보안침해가 2013 년 "일련의 사건 (chain of events)" 활동 중 가장 악의적인 것이었습니다. Java 의 "소개" 웹 페이지를 보면 알 수 있듯이, 기업 데스크톱 중 97% 가 Java 를 실행 중이며 미국 내 데스크톱 컴퓨터 중 89% 가 Java 를 실행 중입니다.[14]

Java 는 범죄자들이 무시하기에는 너무 큰 공격 영역을 제공합니다. 범죄자들은 순서대로 공격을 실행하는 솔루션을 구축하려는 경향이 있습니다. 예를 들어, 다른 방법을 사용하기 전에 먼저 가장 쉽거나 가장 잘 알려진 취약점을 이용하여 데이터를 도용하거나 네트워크에 침입합니다. 대부분의 경우 Java 의 ROI 가 가장 높기 때문에 범죄자들이 가장 먼저 선택하는 공격 대상이 됩니다.

Java 문제 완화

Java 기반 공격이 가장 흔하며 취약성을 제거하기도 어렵지만 그 영향을 줄일 방법은 있습니다.

- 필요한 경우 네트워크에서 브라우저의 Java 사용을 해제하여 이런 공격이 시작되는 것을 차단할 수 있습니다.
- 여러 보안 솔루션에 구축된 Cisco NetFlow와 같은 원격 분석 툴을 사용하면 Java 관련 트래픽을 모니터링할 수 있으므로 보안 전문가가 위협의 원인을 더욱 효과적으로 파악할 수 있게 됩니다.
- 포괄적인 패치 관리를 통해서도 여러 가지 보안 허점을 해결할 수 있습니다.
- 네트워크에 들어온 파일을 지속적으로 추적 및 분석하는 엔드포인트 모니터링 및 분석 툴을 통해 안전한 것처럼 통과했지만 이후 악의적인 동작을 보이는 위협을 사후에 감지하고 저지할 수 있습니다.
- IoC 를 사용해 보안침해 가능성이 있는 장치의 우선 순위 목록을 생성하여 (정상으로 보이는 사건이라도) 악성 코드 분석 정보와의 상관 관계를 분석하고 기존의 안티 바이러스 시그니처 없이 제로 데이 (zero-day) 감염 여부를 확인할 수 있습니다.

또한 Java 를 최신 버전으로 업그레이드하는 것도 취약점을 최소화하는 데 도움이 됩니다. Cisco TRAC/SIO 의 조사에 따르면 Cisco 고객 중 90% 가 Java 프로그램의 가장 최신 버전인 Java 7 Runtime Environment 버전을 사용하고 있는 것으로 나타났습니다. 이 버전에서 더 강력한 보호 기능을 제공할 수 있으므로 보안 측면에서 볼 때 이것은 바람직한 모습입니다.

하지만 Cisco TRAC/SIO 조사에 따르면 Cisco 솔루션을 사용하는 기업 중 76% 가 Java 7 과 함께 Java 6 Runtime Environment 도 사용하는 것으로 나타났습니다. Java 6 는 단종되어 더이상 지원되지 않는 구 버전입니다. 애플리케이션에 따라 Java 코드를 실행하는 데 필요한 버전이 다르므로 두 가지 Java Runtime Environment 버전을 모두 사용하는 기업이 많습니다. 하지만 Cisco 가 설문 조사 한 기업 중 3/4 이상이 단종되어 패치가 공개적으로 제공되지 않는 취약점을 가진 솔루션을 사용하고 있어 범죄자들이 이러한 약점을 공격할 가능성이 많습니다.

2013 년 한 해 동안, Java 웹 멀웨어 발생률은 4 월에 가장 많았으며 모든 웹 멀웨어 중 14% 를 차지했습니다. 이 수치는 2013 년 5 월과 6 월에 모든 웹 멀웨어 중 각각 6% 와 5% 가량으로 최저 수준으로 감소했소했습니다 (그림 13).

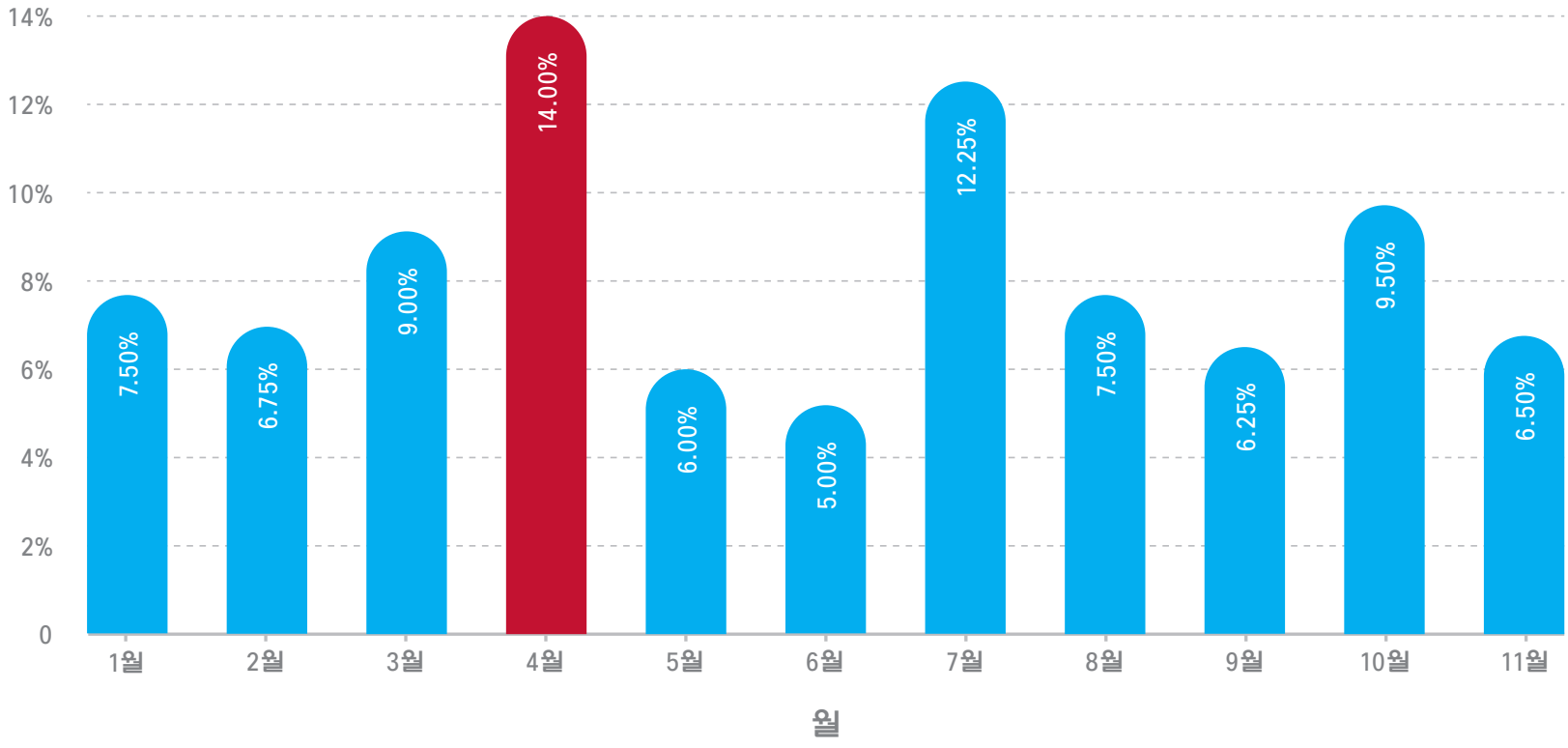
(올해 초 Oracle 은 Oracle Technology Network 의 Java Archive 에서 기존의 Java SE 6 업데이트를 이용할 수 있으나, 그들의 공개 다운로드 사이트에는 더 이상 Java SE 6 업데이트를 게시하지 않는다고 발표했습니다.)

제한된 시간 내에 웹 공격에 대처해야 하는 보안 전문가가 Java 에 가장 많은 관심을 집중하기로 결정한다면, 그것은 리소스를 적재적소에 활용하는 결정을 내린 것입니다.

그림 13

2013 년 Java 웹 멀웨어 발생률

출처: Cisco TRAC/SIO



BYOD 및 모빌리티: 사이버 범죄에 취약한 고도의 장치

사이버 범죄자들과 이러한 범죄의 대상이 되는 사용자들 모두 같은 문제를 공유하고 있습니다. 모두 사업적 이익을 얻기 위해 BYOD (Bring-Your-Own-Device) 및 모빌리티 트렌드를 어떻게 활용하는 것이 가장 좋은 것인지 고심하고 있습니다.

두 가지 점이 범죄자에게 유리하게 작용하고 있는 것으로 보입니다. 첫째는 모바일 플랫폼의 확산입니다. Cisco 보안 전문가들은 점점 더 많은 스마트폰, 태블릿 및 기타 장치들이 기존의 데스크톱 및 노트북 컴퓨터와 같은 기능을 수행할 수록 이 장치에 대한 멀웨어를 설계하기가 더욱 쉬워진다고 지적합니다.

두 번째는 모바일 앱 사용의 증가입니다. 사용자가 모바일 앱을 다운로드할 때, 기본적으로 경량 클라이언트가 엔드포인트에 구축되며 코드가 다운로드됩니다. 또 다른 문제는 많은 사용자들이 보안을 전혀 고려하지 않은 채 모바일 앱을 주기적으로 다운로드한다는 것입니다.

많은 사용자들이 보안에 대해 전혀 생각하지 않고 모바일 앱을 주기적으로 다운로드합니다.

한편, 오늘날 보안팀은 기기와 장소에 상관없이 모든 애플리케이션 또는 리소스에 접속하려는 모든 사용자를 보호하기 위해 "모두에서 모두로의 문제 (any-to-any problem)"를 해결하려고 노력하고 있습니다.[15] BYOD 경향으로 인해 이러한 문제가 더 복잡해지고 있습니다. 이러한 유형의 장비를 모두 관리하는 것은, 특히 특히 제한된 IT 예산으로는 어려운 일입니다. BYOD 환경에서 CISO 는 특히 데이터 공간을 철저하게 관리해야 합니다.

모빌리티로 인해 사용자와 데이터의 보안이 침해될 수 있는 새로운 방식이 나타나고 있습니다. Cisco 연구원들은 무선 채널을 이용하여 해당 채널에서 교환되는 데이터를 엿보고 해당 데이터에 액세스한다는 사실을 발견했습니다. 또한 모빌리티로 인해 조직에도 다양한 보안 문제가 야기됩니다. 직원 소유 장치를 분실 또는 도난 했을 때 보안 장치가 없는 경우 지적 재산 및 기타 민감한 데이터의 손실과 같은 여러 보안 문제에 직면하게 됩니다.

기업 보안 개선을 위한 솔루션 중 하나로, Cisco 의 전문가들은, 모든 장치가 네트워크에 액세스하기 전에 안전을 확인 받을 수 있는 모바일 기기 관리 프로그램을 공식적으로 마련할 수 있다고 말합니다. 최소한 사용자 인증에 PIN (개인 식별 번호) 잠금 설정이 의무사항으로 적용되어야 하며 장치가 분실 또는 도난된 경우 보안 팀에서 해당 장치를 원격으로 장치를 종료하거나 데이터를 삭제할 수 있어야 합니다.

2013 모바일 멀웨어 추세

Cisco TRAC/SIO 와 Cisco 의 자회사인 Sourcefire 는 2013 년 모바일 멀웨어 추세에 대해 다음과 같은 조사를 실시했습니다.

2013 년 발생한 모든 웹 멀웨어 중 특정 기기를 겨냥한 모바일 멀웨어는 1.2% 에 불과합니다. 모바일 멀웨어의 비중은 크지 않지만 멀웨어 개발자가 공격할 수 있는 논리적이며 새로운 영역이라는 점에 주목할 필요가 있습니다.

2013 년 발생한 모든 웹 멀웨어 중 특정 기기를 겨냥한 모바일 멀웨어는 1.2% 에 불과합니다.

Cisco TRAC/SIO 연구에 따르면 기기를 보안침해하려는 목적을 가진 모바일 멀웨어 중 99% 는 안드로이드 기기를 겨냥합니다. J2ME (Java Micro Edition) 지원 기기를 공격하는 트로이 목마가 모든 모바일 멀웨어 발생률 중 0.84% 를 차지하여 2013 년 두 번째로 많이 발생한 멀웨어로 드러났습니다.

하지만 모든 모바일 멀웨어가 특정 기기를 대상으로 설계되는 것은 아닙니다. 많은 멀웨어에는 피싱 (Phishing), 라이크재킹 (Likejacking), 기타 사회 공학적 기법 또는 예상하지 못한 웹사이트로의 강제적인 리디렉션 등이 포함됩니다. Cisco TRAC/SIO 의 사용자 에이전트 분석에 따르면 웹을 통해 감염되는 모든 멀웨어 유형의 발생율이 안드로이드 사용자가 71% 로 가장 높았으며 Apple iPhone 사용자가 14% 로 두 번째로 높은 비율을 나타냈습니다 (그림 14).

Cisco TRAC/SIO 연구원들은 또한 2013 년 애드웨어 및 중소기업 관련 스파이웨어 실행과 같이 안드로이드 기기를 보안침해로 금전적인 이득을 취하려는 시도 또한 보고했습니다.

Cisco TRAC/SIO 의 조사에 따르면 가장 많이 발견되는 모바일 멀웨어는 Andr/Qdplugin-A 로 43.8% 를 차지했습니다. 보통 비공식 마켓플레이스를 통해 유통되는 리패지지 버전의 합법적인 애플리케이션에서 일반적으로 발견됩니다 (그림 15).

그림 14

모바일 기기별 웹 멀웨어 발생률

출처: Cisco Cloud Web Security 보고서

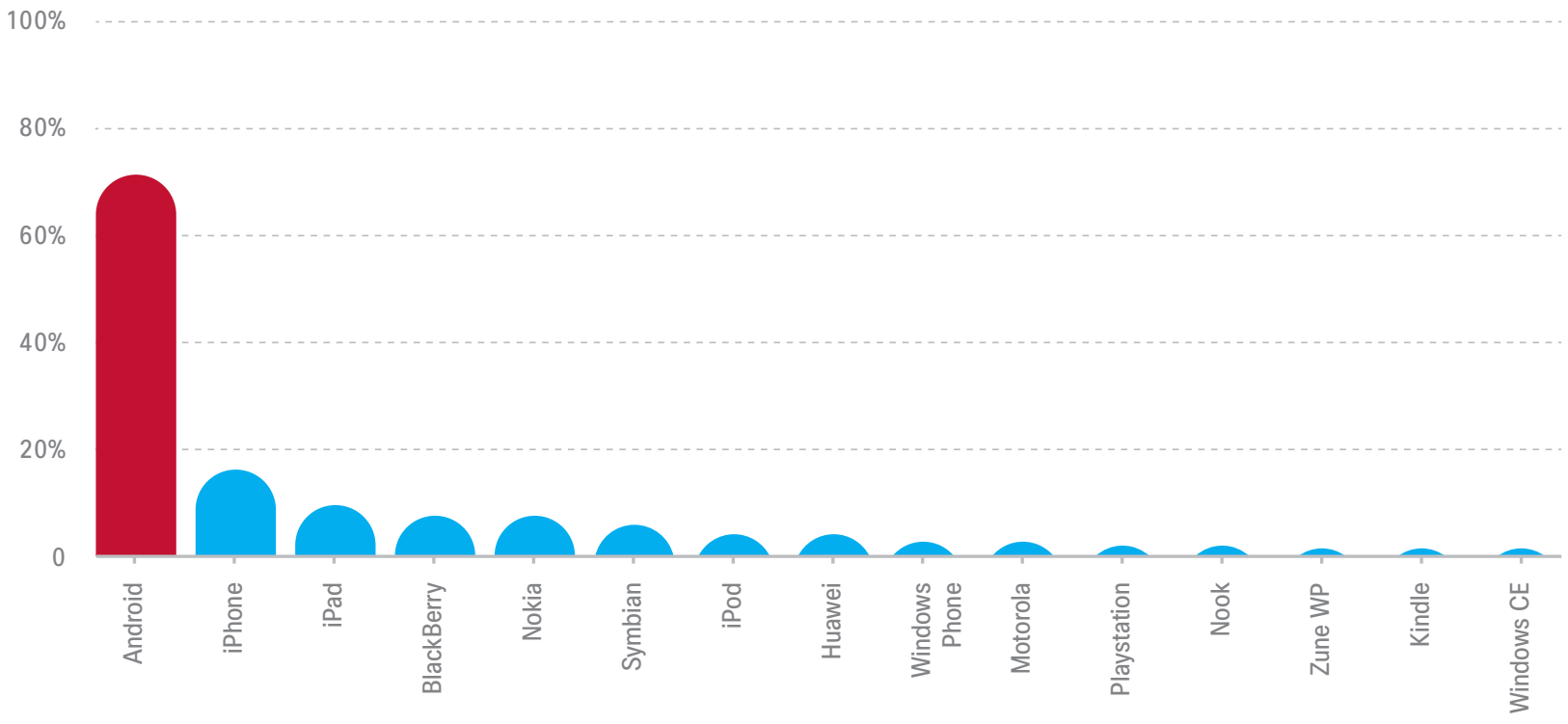


그림 15

2013 년 발생한 10 가지 주요 모바일 멀웨어

출처: Cisco Cloud Web Security 보고서

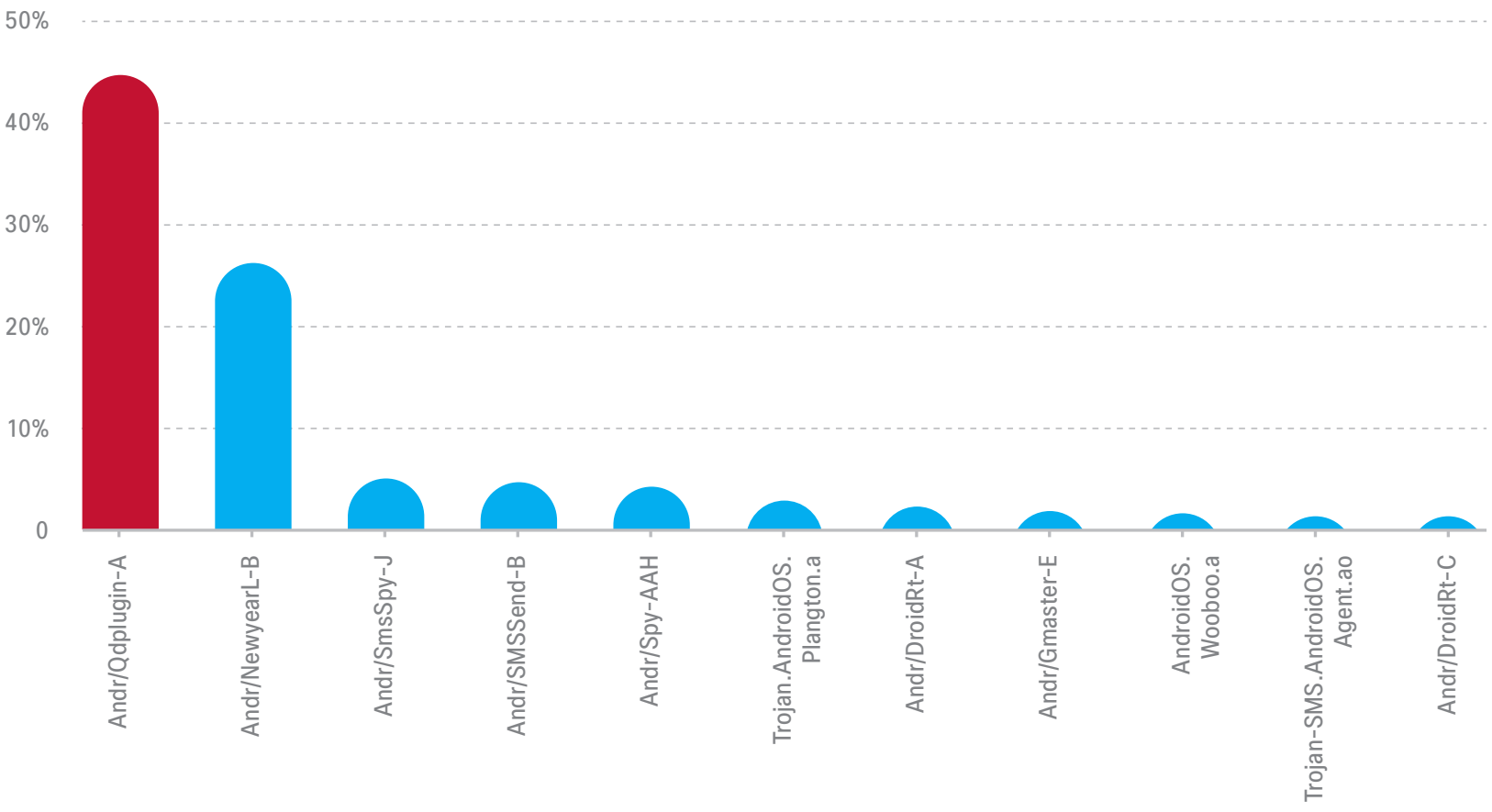
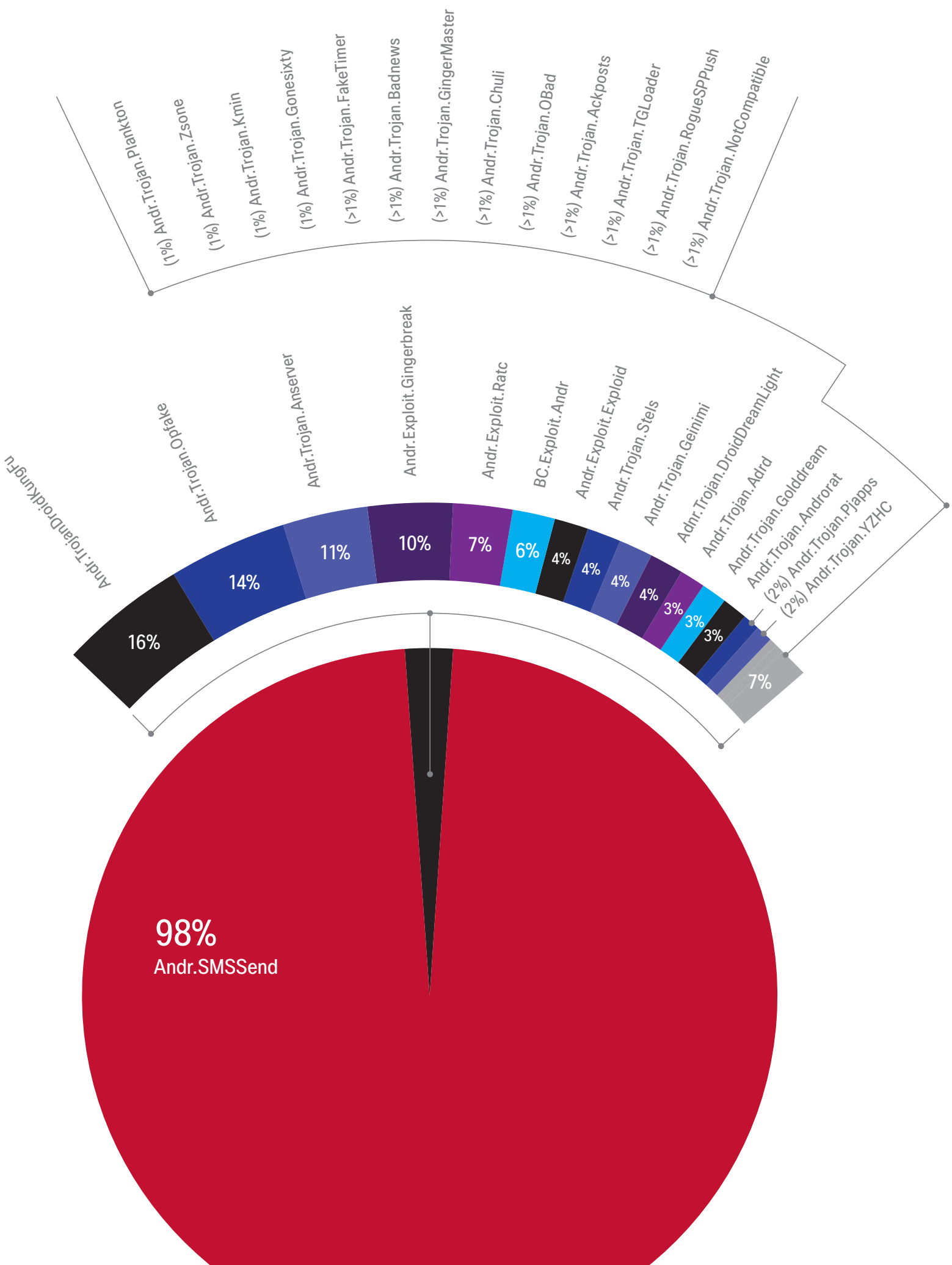


그림 16

2013 년 발견된 주요 안드로이드 멀웨어군

참고: 모든 안드로이드 멀웨어 중 SMSSend 가 98% 를 차지하였고 나머지 2% 는 비율별로 표시되었습니다. 출처: Sourcefire



표적 공격: 집요하게 파고들어 오는 "방문객" 을 막아야 하는 어려움

여러분의 네트워크은 이미 표적 공격에 의해 침입 당했을 가능성이 높습니다.

네트워크 안에 침입하게 되면, 계속 머물면서 데이터를 은밀하게 도용하거나 네트워크 리소스를 이용해 "피봇팅" 한 후 다른 개체를 공격하는 경향이 있습니다 (피봇팅에 대한 자세한 내용은 18 페이지 참조). 이로 인해 피해는 데이터 도난이나 비즈니스 중단을 넘어 네트워크 공격이 적시에 해결되지 않았을 때, 파트너 및 고객의 신뢰를 잃을 수 있습니다.

표적 공격은 지적 재산, 고객 데이터 및 정부의 기밀 정보를 위협합니다. 공격자는 조직의 보안 인프라를 교묘하게 피해가는 툴을 사용합니다. 공격 범죄자는 이러한 행위를 아무도 모르게 하기 위해 IoC 즉 "보안침해 흔적지표" 가 거의 드러나지 않는 용의주도한 방법을 이용합니다. 네트워크에 침투하고 목적을 이루기 위해 공격자가 사용하는 방법에는 공격의 단계별로 이어지는 사건과 공격의 단계에서 일어나는 일련의 사건인 "공격 사슬 (Attack Chain)" 이 포함됩니다.

네트워크에서 표적 공격이 숨을 공간을 찾아내면 아무도 모르게 효율적으로 원하는 작업을 수행합니다.

범죄자들은 아무도 모르게 보안을 침해하기 위해 용의주도한 방법을 사용합니다.

그림 17

공격 사슬 (The Attack Chain)

오늘날의 모든 위협을 파악하고 네트워크를 효과적으로 방어하기 위해 IT 보안 전문가들은 공격자의 관점에서 생각해야 합니다. 악의적인 행위자가 목적을 이루기 위해 사용하는 방식을 충분히 이해하면 조직의 방어 체계를 강화할 수 있는 방법을 찾을 수 있습니다. "사이버 킬 체인" 의 단순화된 버전인 공격 사슬은 공격의 단계별로 이어지는 사건과 공격의 단계에서 일어나는 사건을 보여줍니다.

1. 설문 조사

보안을 위해 구축된 기술을 비롯해 네트워크, 엔드포인트, 모바일, 가상화를 비롯한 전체 환경을 파악

2. 생성

공격을 위한 상황 인식(context-aware) 악성코드 생성

3. 테스트

악성코드가 의도한 대로 작동하는지, 특히 구축된 보안 툴의 감지를 피할 수 있는지 확인

4. 실행

확장된 네트워크를 탐색해 환경을 인식하고 감지를 회피하며 대상에 도달할 때까지 은밀하게 이동

5. 목적 달성

데이터 수집, 시스템 중단 또는 파괴

멀웨어 스냅샷: 2013 년에 관찰된 동향

Cisco 보안 전문가들은 향후 발생할 수 있는 범죄 행위를 파악하고 위협을 감지할 수 있도록 멀웨어 트래픽 및 발견된 기타 위협에 대해 연구와 분석을 지속하고 있습니다.

그림 18

주요 멀웨어 종류

이 그림은 주요 멀웨어 종류를 보여줍니다. 트로이 목마가 가장 일반적인 멀웨어이며 그 뒤를 애드웨어가 잇고 있습니다.
출처: Sourcefire (ClamAV 및 FireAMP 솔루션)

그림 19

주요 Windows 멀웨어군

이 그림은 주요 Windows 멀웨어군을 보여줍니다. 가장 큰 비중을 차지하는 Trojan.Onlinegames 는 주로 패스워드 스틸러 (password stealer) 로 구성되어 있습니다. 이 멀웨어는 Sourcefire 의 ClamAV 안티 바이러스 솔루션으로 감지할 수 있습니다. 출처: Sourcefire (ClamAV 솔루션)

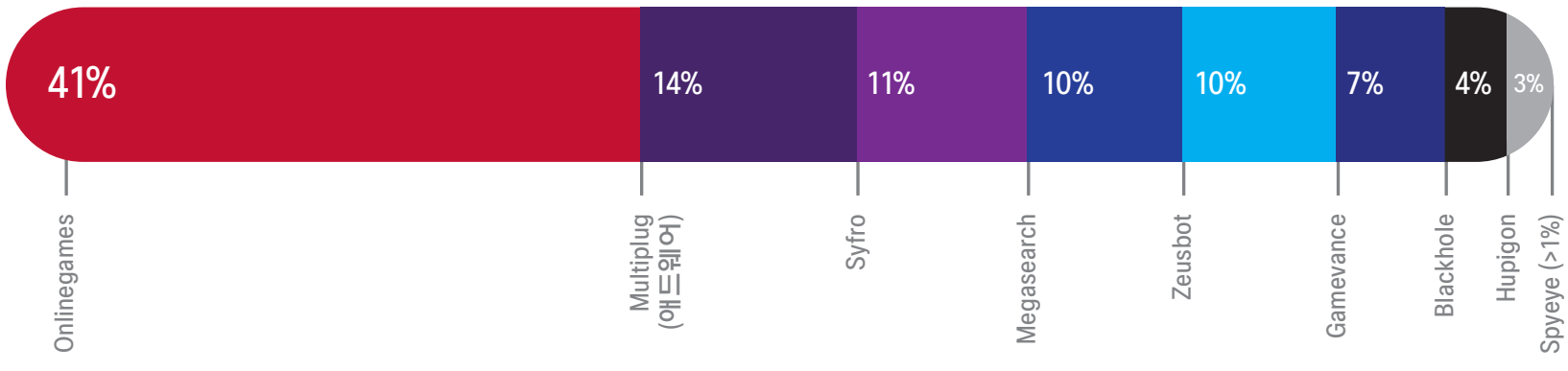


그림 20

2013 년, 10 가지 주요 웹 멀웨어 종류

이 그림은 Cisco TRAC/SIO 의 조사에서 발견된 가장 많이 발생한 멀웨어 호스트를 보여줍니다.
출처: Cisco Cloud Web Security 보고서

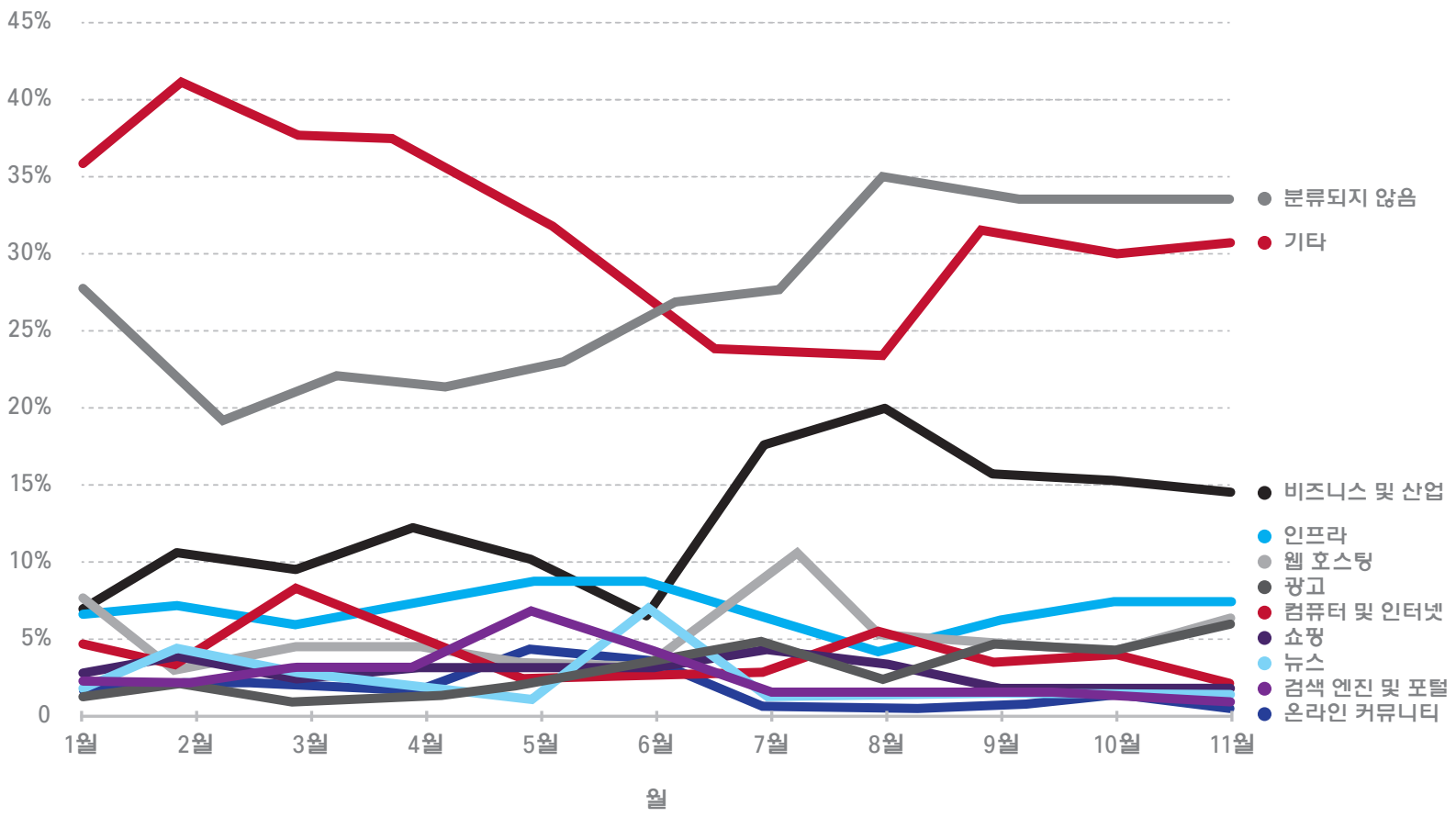
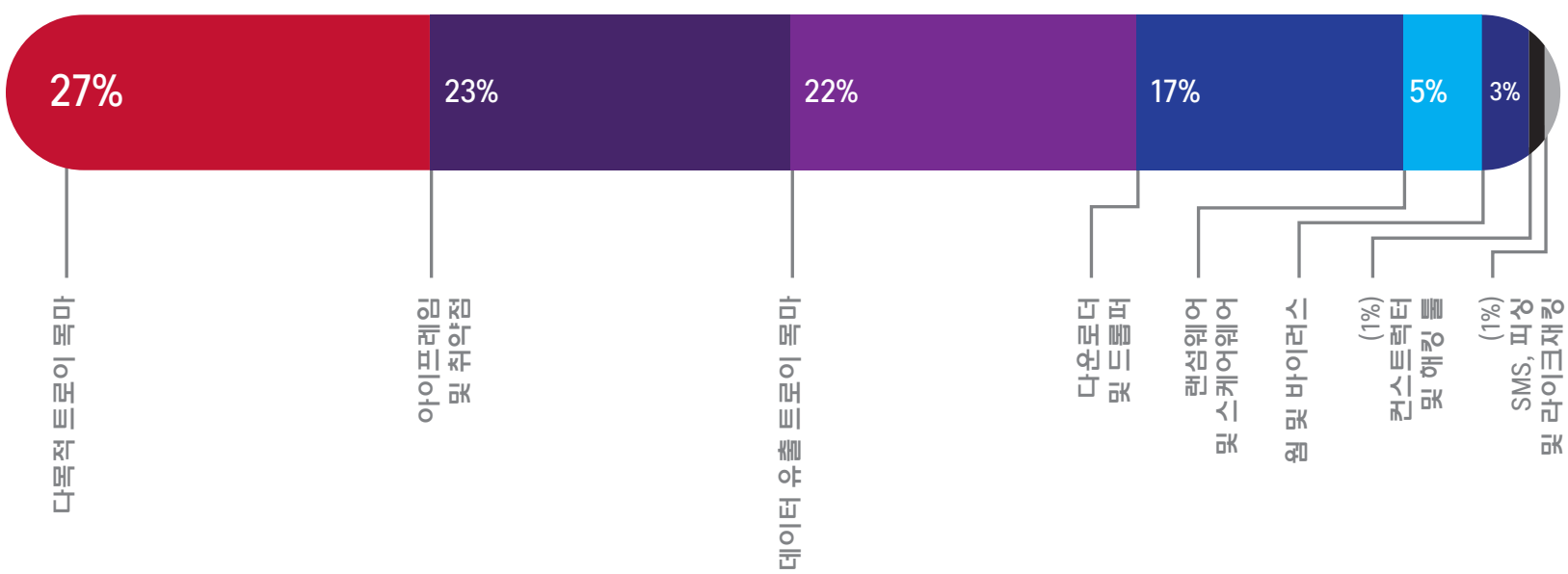


그림 21

2013 년, 총 발생률별 멀웨어 종류

출처: Cisco TRAC/SIO



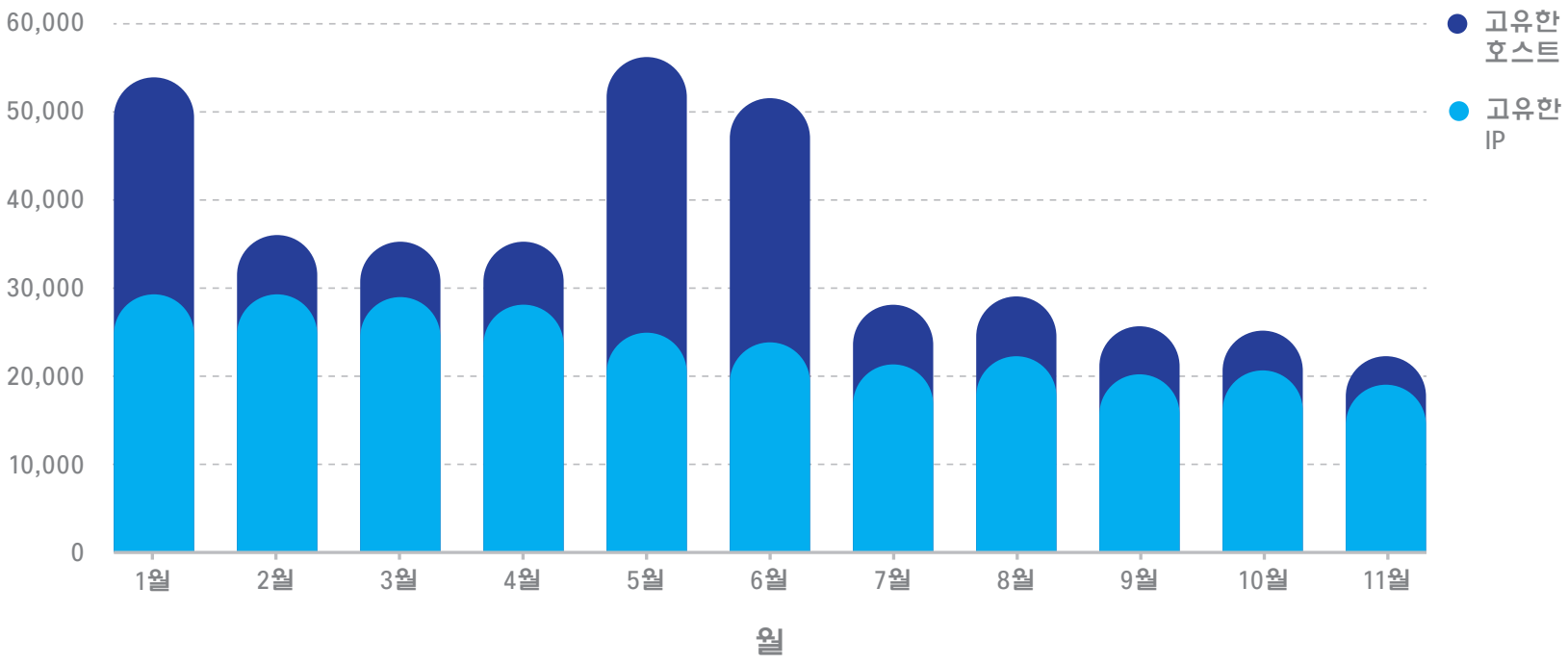
Cisco TRAC/SIO 가 2013 년에 실시한 조사에 따르면 웹을 통해 감염되는 멀웨어 중에서 다목적 트로이 목마가 27% 로 가장 많이 발견됐습니다. 두 번째로 많이 발생한 종류는 취약점과 아이프레임 (iframes) 같은 악성 스크립트로 23% 를 차지했습니다. 패스워드 스틸러 (password stealer) 나 백도어와 같은 데이터 유출 트로이 목마는 전체 웹 멀웨어 중 22% 였으며, 다운로더 및 드롭퍼 트로이 목마의 발생률은 17% 로 4 위를 차지했습니다 (그림 21 참조).

그리고 고유 멀웨어 호스트와 IP 주소가 꾸준하게 2013 년 1 월과 9 월 사이에 30% 감소한 것으로 보아 멀웨어가 밀집되어 있는 호스트와 IP 주소의 수가 줄어들고 있는 것으로 보입니다 (그림 22). (참고: IP 주소는 여러 도메인의 웹사이트를 지원 가능합니다.) 호스트의 수가 감소하고 멀웨어의 수도 안정된 추세를 보이는 상황에서, 좋은 호스트가 범죄자의 목적을 이루는 데 도움이 되기 때문에 이러한 호스트의 가치와 평판이 더욱 중요시되고 있습니다.

그림 22

2013 년, 고유한 멀웨어 호스트 및 IP 주소

출처: Cisco Cloud Web Security 보고서



특정 기업을 대상으로 하는 워터링 홀 공격

악의적인 행위자가 특정 산업의 조직에 멀웨어를 유포하는 방법 중 하나로 "워터링 홀 (Watering Hole)" 공격이 있습니다. 마치 먹잇감을 노리는 것처럼 특정 그룹 (예를 들어 항공업 종사자) 을 노리는 사이버 범죄자들은 이 그룹에서 자주 방문하는 웹사이트를 모니터링하고, 이 중 하나 이상의 웹사이트에 멀웨어를 감염시킨 후, 대상 그룹의 사용자 중 누군가 웹사이트를 방문해 보안침해될 때까지 기다립니다.

워터링 홀 공격은 합법적인 웹사이트가 이용하므로 기본적으로 신뢰의 악용에 속합니다. 또한 스피어 피싱의 유형 중 하나입니다. 다만 스피어 피싱은 선정한 개인을 공격하는 반면 워터링 홀은 공통의 관심사를 가진 사용자 그룹을 보안침해하도록 고안되었습니다. 워터링 홀 공격은 대상을 가리지 않으며 감염된 웹사이트를 방문하는 모든 사용자를 위협합니다.

4 월 말 핵 관련 컨텐츠를 호스팅하는 미국 노동부 웹사이트의 특정 페이지에서 워터링 홀 공격이 발생했습니다.[16] 그 후 Cisco TRAC/SIO 연구원들은 2013 년 5 월 초에 다른 여러 사이트에서 에너지 및 석유 부문을 대상으로 하는 워터링 홀 공격을 관찰하였습니다. 이 두 가지 공격에 이용된 특정 공격 기술 등의 유사성으로 볼 때 이 두

다음 페이지에 계속

주요 대상: 업종

Cisco TRAC/SIO 에 따르면 제약, 화학, 전자제품 제조업과 같은 고수익 산업 부문의 웹 멀웨어 발생률이 높은 것으로 나타났습니다.

이 발생률은 특정 업종의 제품 및 서비스의 가치 변동에 따라 달라집니다.

Cisco TRAC/SIO 연구에 의해 이전에는 상대적으로 안전한 분야였던 농업 및 광업 부문에서 멀웨어 발생률이 크게 증가한 것이 발견되었습니다. 사이버 범죄자들이 귀한 금속 자원의 감소 및 기후 변화로 인한 식품 공급의 지장 등과 같은 추세에 관심을 두게 된 것이 이러한 업종에서 멀웨어 발생이 증가하는 이유입니다.

전자 제품 업계에서도 멀웨어 발생률은 계속 증가하고 있습니다. Cisco 보안 전문가들은 이 업종을 공격하는 멀웨어는 일반적으로 악의적인 행위자가 지적 재산에 접근하는 것을 지원하도록 설계되었으며, 탈취 후, 경쟁 우위로 사용하거나 최고 입찰가를 지불하는 사람에게 판매한다고 보고했습니다.

업종별 멀웨어 발생률을 파악하기 위해 Cisco TRAC/SIO 연구원들은 Cisco Cloud Web Security를 통해 프록시하는 모든 조직의 멀웨어 발생률의 중앙치 (median) 과 이 서비스를 통해 프록시하는 특정 업종 내 모든 기업의 멀웨어 발생률 중앙치를 비교했습니다. 업종의 발생률이 100% 보다 높으면 웹 멀웨어 발생 위험도가 정상치보다 높은 것이며 100% 보다 낮으면 위험도가 낮은 것입니다. 예를 들어 발생률이 170% 인 기업의 위험도는 중앙치보다 위험이 70% 더 높습니다. 반면 발생률이 70% 인 기업의 위험도는 중앙치보다 위험이 30% 낮습니다 (그림 23).

이전 페이지에서 이어짐

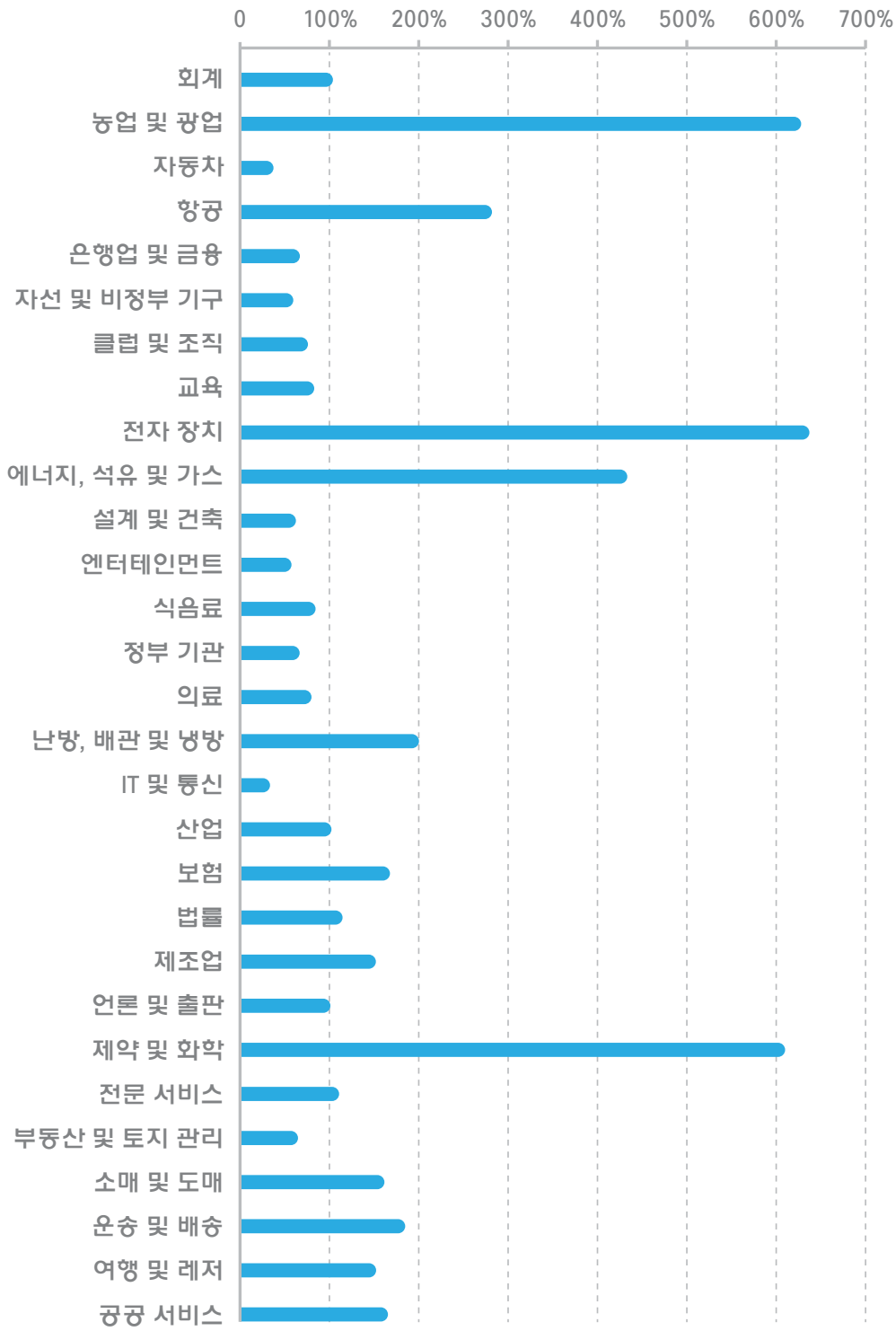
공격이 서로 관련되었을 가능성이 큽니다. 또한 Cisco TRAC/SIO 의 조사를 통해 이러한 웹사이트 중 다수가 같은 웹 디자이너 및 호스팅 공급업체를 이용했다는 점이 밝혀졌습니다. 이는 최초의 보안침해가 해당 공급업체에서 피싱 또는 탈취한 인증서로 인해 발생했을 것을 암시합니다.[17]

이러한 공격으로부터 사용자를 보호하려면 시스템과 웹 브라우저에 패치를 철저하게 적용해 공격당할 수 있는 취약점의 수를 최소화해야 합니다. 또한 사용자의 브라우저에 웹 트래픽을 제공하기 전에 멀웨어를 필터링하고 검사하는 것도 중요합니다.

그림 23

2013 년 업종별 위험도 및 웹 멀웨어 발생률

출처: Cisco Cloud Web Security 보고서



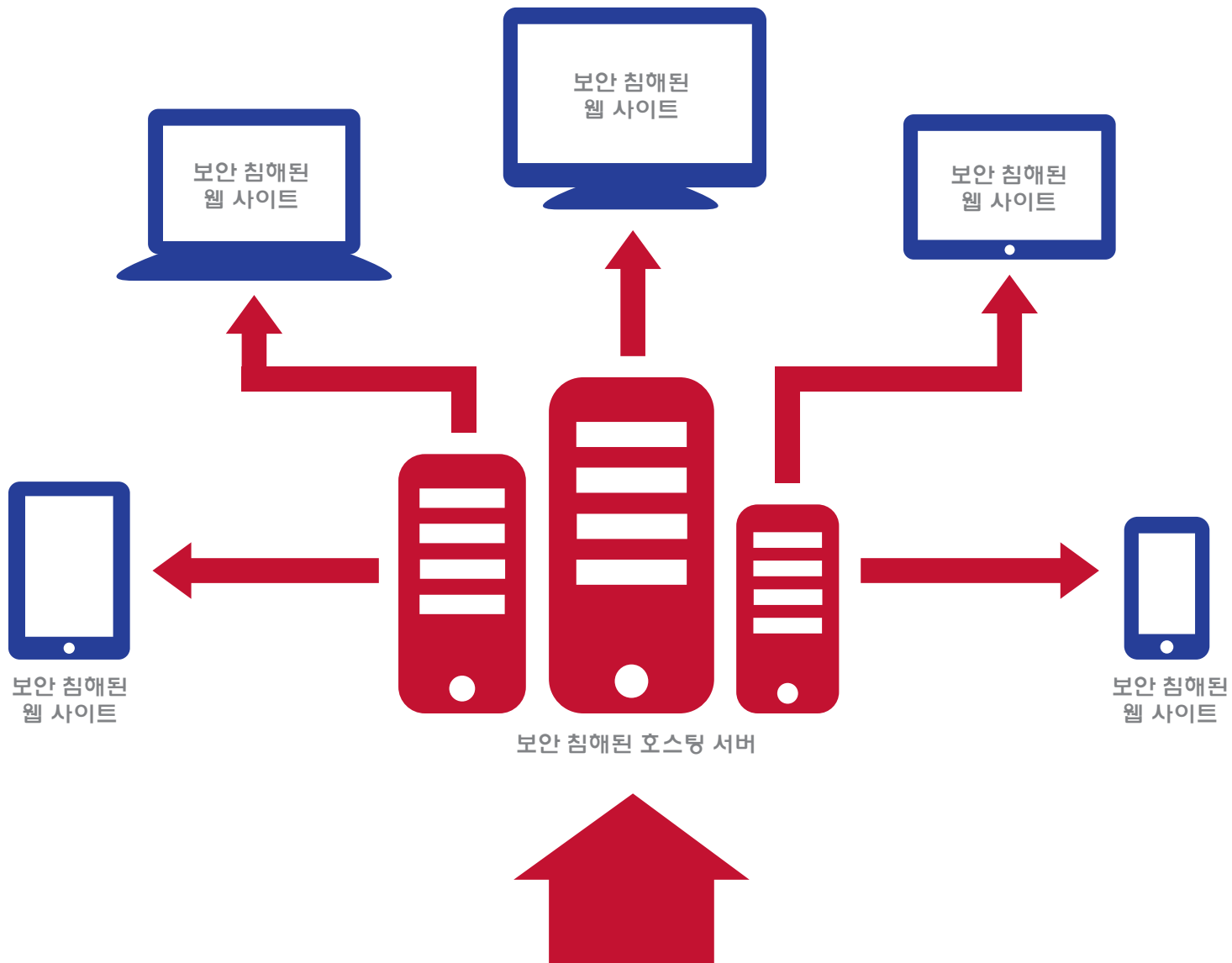
취약한 에코시스템 내의 균열

사이버 범죄자들은 인터넷 인프라 성능을 활용하면 단순히 개별 컴퓨터에 액세스할 때보다 훨씬 큰 이득을 얻을 수 있다는 점을 알게 되었습니다.

최근의 공격은 서버가 제공하는 강력한 처리 성능 및 대역폭을 이용하려는 목적으로 웹 호스팅 서버, 네임 서버 및 데이터 센터에 액세스 권한을 확보하는 새로운 양상을 보입니다. 정치적인 주장, 경쟁업체 공격 또는 수익 창출 등 목적이 무엇이든, 이 방식으로 위험을 눈치채지 못한 많은 컴퓨터 사용자를 공격하고 목표 조직에 더 큰 영향을 미칠 수 있습니다.

그림 24

효율적인 감염 전략



인터넷 인프라를 대상으로 하는 이러한 추세를 볼 때 기본적으로 웹 기반 자체를 신뢰할 수 없다는 사실을 알 수 있습니다. 호스팅 서버의 루트 액세스를 확보하기 위해 사용되는 방법은 다양하여 관리 워크스테이션에서 서버 로그인 인증서를 도용하는 트로이 목마, 서버에서 사용되는 타사 관리 툴의 취약점, 무작위 대입 로그인 시도와 같은 전략 등이 있습니다 (53 페이지 참조). 또한 서버 소프트웨어 자체에 존재하는 알려지지 않은 취약점도 침입의 원인이 될 수 있습니다.

호스팅 서버가 보안침해 되면 전 세계 수천 개의 웹사이트와 사이트 소유자가 감염될 수 있습니다 (그림 24).

보안침해된 서버에서 호스팅되는 웹사이트는 리디렉터 (감염 사슬에서의 매개체) 이자 멀웨어 저장소 역할을 합니다. 다수의 보안침대 된 사이트가 소수의 악성 도메인으로부터 멀웨어를 로딩하는 것이 (다수 대 소수 관계) 아니라 다수 대 다수 관계로 변화하여 이에 대한 해결책을 찾기가 어려워지고 있습니다.

도메인 네임 서버가 이 새로운 공격 유형의 주요 대상이며, 정확한 공격 방법은 아직 파악되지 않은 상태입니다. 개별 웹사이트 및 호스팅 서버뿐만 아니라 특정 호스팅 공급업체의 네임 서버도 보안침해되고 있습니다. Cisco 보안 연구원들은 이렇게 인터넷 인프라를 공격하는 추세로 인해 사이버 범죄자들이 웹 기반의 주요 부분을 통제할 수 있게 되어 위협 환경이 변화하고 있다고 말합니다.

"사이버 범죄는 큰 이득을 취하는 수단이 된 동시에 고도로 상업화되었으므로 이에 대응할 수 있는 강력한 인프라가 필요합니다." 라고 Cisco 위협 분석 정보 책임자인 Gavin Reid 이사가 말합니다. "공격자들은 호스팅 서버와 데이터 센터를 보안침해하여 대규모의 대역폭에 액세스할 수 있을 뿐만 아니라 이 리소스의 지속적인 업타임을 통해 이득을 얻을 수 있습니다."

"사이버 범죄는 큰 이득을 취하는 수단이 된 동시에 고도로 상업화되었으므로 이에 대응하기 위한 강력한 인프라가 필요합니다."

Gavin Reid, Cisco 위협 분석 정보 책임자

연관성: DarkLeech 및 Linux/CDorked

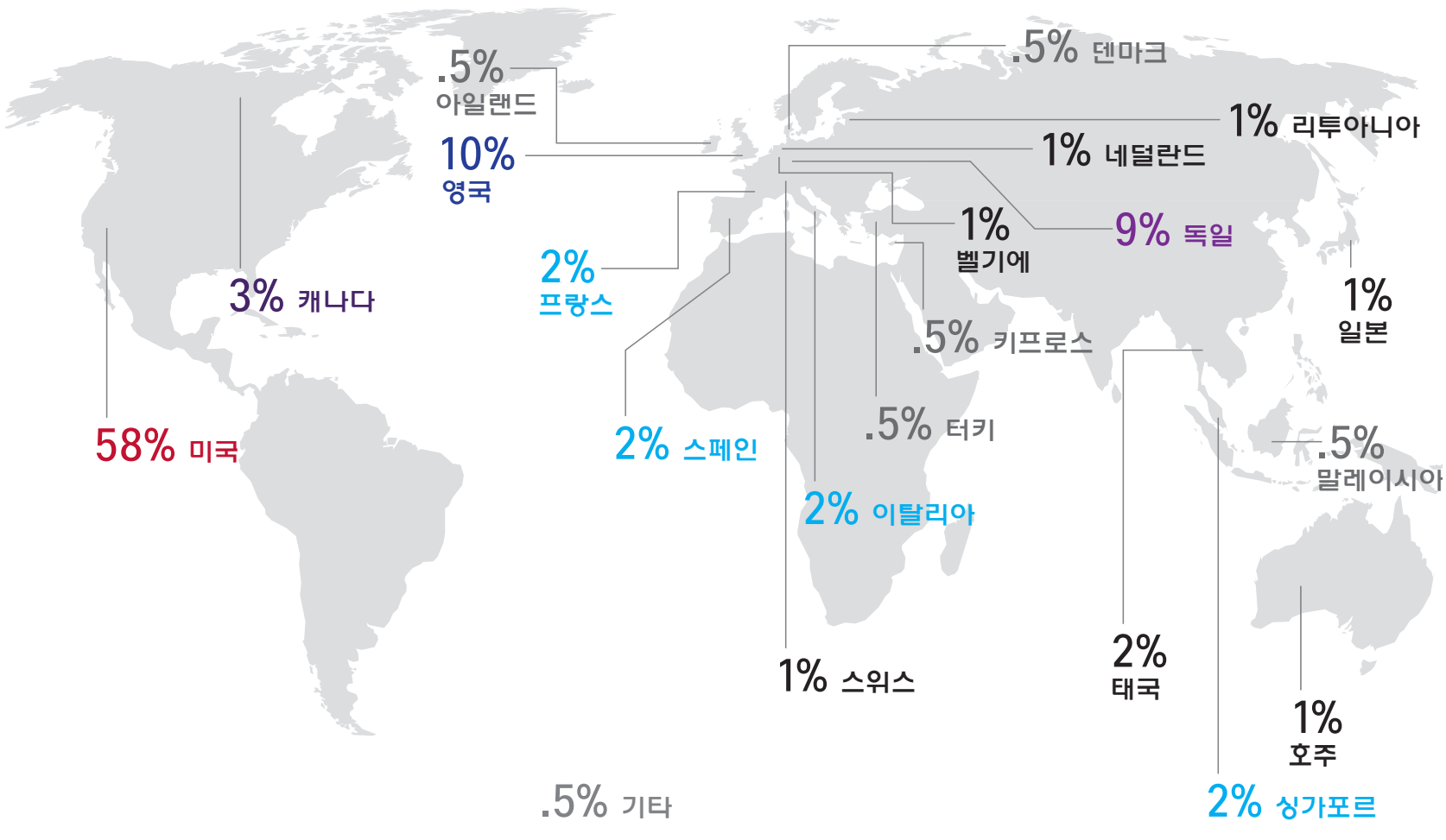
Cisco 가 2013 년 보고한 다크리치 (DarkLeech) 공격 활동[18] 은 호스팅 서버가 보안침해되어 대규모 공격을 위한 기반으로 어떻게 사용될 수 있는지 잘 보여줍니다. 다크리치 공격은 Apache HTTP 서버 소프트웨어를 사용하는 전 세계의 최소 20,000 개의[19] 합법적인 웹사이트를 단시간에 보안침해한 것으로 추정됩니다. 사이트는 원격 공격자가 악성 Apache 모듈을 업로드 및 구성하도록 허용하는 SSHD (Secure Shell daemon) 백도어에 감염되었습니다. 보안을 침해한 공격자는 호스팅되는 웹사이트에 실시간으로 아이프레임 (HTML 요소) 을 동적으로 삽입하여 블랙홀 익스플로잇 키트 (Blackhole exploit kit) 를 통해 공격 코드 및 기타 악성 컨텐츠를 유포했습니다.

다크리치 아이프레임 (DarkLeech iframe) 은 사이트를 방문하는 순간에만 삽입되므로 감염 여부를 쉽게 확인하지 못할 수 있습니다. 또한 범죄자들은 보안침해를 감지하지 못하도록 방문자가 검색 엔진 결과 페이지를 통해 방문한 경우에만 아이프레임을 삽입하고 방문자의 IP

그림 25

2013 년 다크리치 (DarkLeech) 로 인한 국가별 서버 보안침해

출처: Cisco TRAC/SIO



주소가 사이트 소유자 또는 호스팅 공급업체의 IP 주소와 일치하는 경우에는 아이프레임을 삽입하지 않으며 아이프레임을 24 시간 동안 한 번만 개별 방문자에게 삽입하는 등 정교한 조건 기준을 사용합니다.

Cisco TRAC/SIO 조사에 따르면 전 세계에 걸쳐 DarkLeech 로 인한 보안침해가 발생했으며 호스팅 공급업체의 수가 많은 국가들의 감염률이 높은 것으로 나타났습니다.

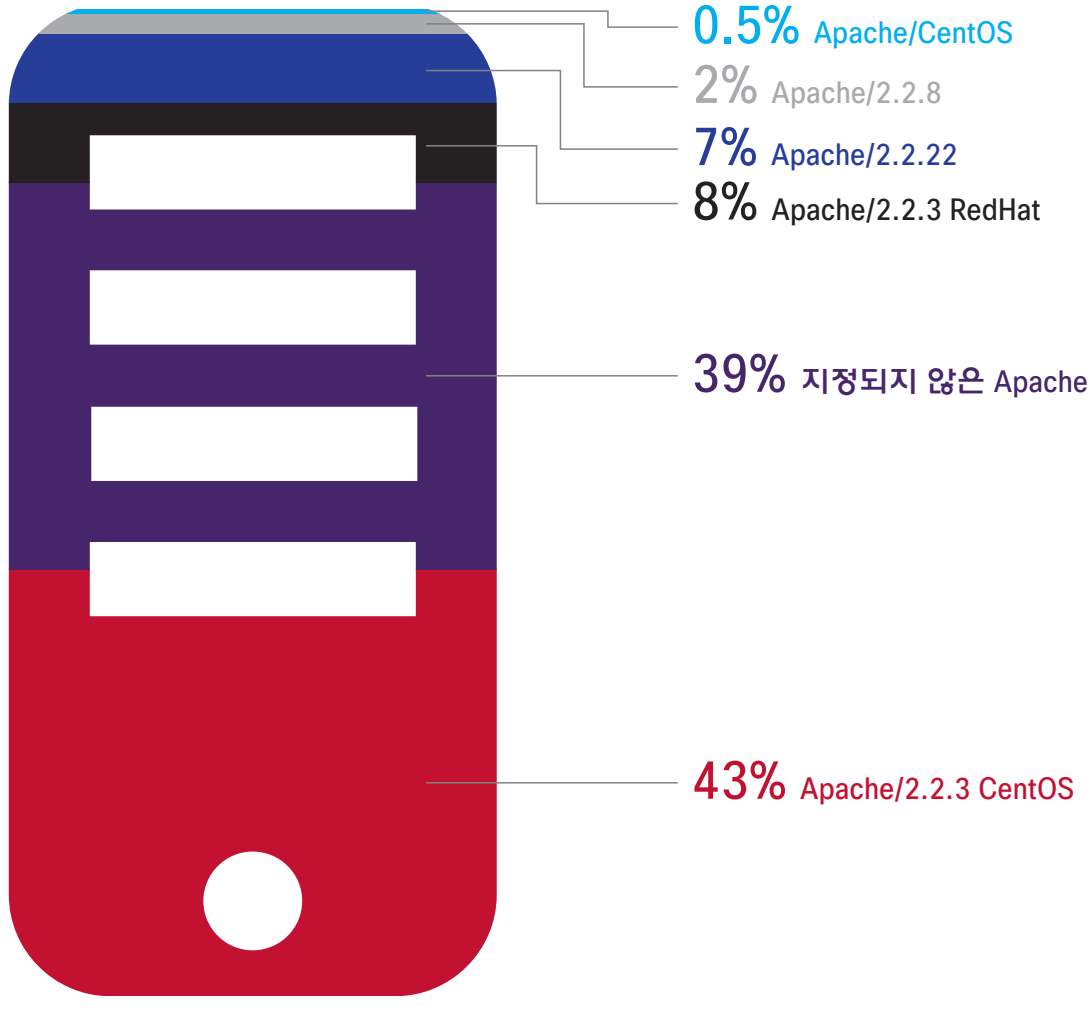
Cisco SIO/TRAC 연구원들은 감염된 서버 소프트웨어 버전가 배포된 것을 확인하기 위해 보안침해된 서버 수천 개를 조회했습니다.

2013 년 4 월에 서버 수천 개를 감염시킨 Apache HTTP 서버 소프트웨어를 실행하는 또 다른 악성 백도어가 발견되었습니다. Linux/CDorked[20] 는 cPanel 이 설치된 Apache 버전에서 HTTPD 바이너리를 대체합니다. Nginx와 Lighttpd 를 공격 대상으로 하는 유사한 백도어도 발견되었습니다. CDorked 도 다크리치 (DarkLeech) 공격 방법과 마찬가지로, 조건 기준을

그림 26

DarkLeech 로 인해 보안침해된 서버 응답

출처: Cisco TRAC/SIO



사용하여 감염된 서버에 호스팅되는 웹사이트에 아이프레임을 동적으로 삽입합니다. 감염된 웹사이트를 탐색하는 모든 방문자는 다른 악성 웹사이트의 악성 컨텐츠가 유포되며, 이 웹사이트에서 크라임웨어 툴킷이 사용자의 PC 를 추가적으로 보안침해하려고 시도합니다.[21]

Linux/CDorked 가 웹사이트 도메인을 평균 24 시간 이내에 순환하는 것이 Linux/CDorked 의 독특한 특징입니다. 보안침해 사이트 중에서 이보다 오래 사용되는 경우는 많지 않습니다. 따라서 멀웨어 도메인이 보고되었어도 공격자는 이미 사라진 상태입니다. 또한 Linux/CDorked 의 경우에도 감지를 피하기 위해 보안침해된 호스트를 순환하면서 호스팅 공급업체가 자주 (약 2 주마다) 변경됩니다. 악의적인 사용자는 이러한 동일 호스팅 공급업체의 보안침해된 네임 서버를 통해 전환 과정에서 도메인에 대한 제어를 잃지 않고 호스트 사이에서 이동할 수 있습니다. 새로운 호스트로 이동한 공격자는 일반적인 사용자에게 합법적으로 보이기 위해 주로 타이포스쿼팅 (typosquatting) 방식[22] 의 도메인 이름을 사용해 새로운 도메인 순환을 시작합니다.

CDorked 와 DarkLeech 는 모두 훨씬 규모가 크고 복잡한 전략의 일부로 볼 수 있습니다.

Cisco TRAC/SIO 가 분석한 CDorked 의 트래픽 패턴에서 다크리치 (DarkLeech) 와의 연관성을 발견할 수 있습니다. 특히 CDorked 에서 사용하는 특수하게 암호화된 참조 URL 은 다크리치의 트래픽을 명확하게 나타냅니다. 하지만 이것이 이 멀웨어의 전부가 아닙니다. CDorked 와 다크리치는 모두 훨씬 규모가 크고 복잡한 전략의 일부인 것으로 보입니다.

"이렇게 정교한 보안침해를 통해 사이버 범죄자들이 수천 개 이상의 웹사이트와 여러 호스팅 서버 및 이러한 호스트가 사용하는 네임 서버에 대해 상당한 통제력을 확보했음을 알 수 있습니다." 라고 Cisco 위협 분석 정보 책임자인 Gavin Reid 이사는 말합니다. "최근에 많이 발생하는 개별 웹사이트에 대한 무작위 대입 로그인 공격과 더불어 대규모의 강력한 봇넷 (botnet) 이라고 밖에 설명할 수 없는 공격에 웹 인프라가 이용되는 새로운 추세가 나타나고 있습니다. 이러한 우버봇 (überbot) 은 전례 없는 규모의 스팸 발송, 멀웨어 유포, 디도스 (DDoS) 공격 실행 등에 이용될 수 있습니다."

표적 공격의 신호인 악성 트래픽, 모든 기업의 네트워크에서 감지

Cisco 가 실시한 위협 분석 정보 추세 조사에 따르면 모든 기업 네트워크 (100%) 에서 악성 트래픽이 발견되었습니다. 이는 교묘한 범죄자 또는 다른 사용자들이 이러한 네트워크에 침투해 오랜 시간 동안 아무도 모르게 활동해 왔다는 증거입니다.

모든 조직은 이미 해킹을 당했을 것이라고 추정해야 할 것이며 앞으로 공격 대상이 될 가능성의 문제가 아니라 언제 그리고 얼마나 오랫동안 공격받을지의 문제라는 것에 최소한 동의해야 합니다.

기업 내부 네트워크에서 시작된 DNS (Domain Name Service) 검색을 검토하는 최근 프로젝트에서 Cisco 위협 분석 정보 전문가들은 모든 사례에서 악용 또는 보안침해된 증거가 있음을 발견했습니다 (그림 27). 예를 들어 Cisco 에서 분석한 모든 기업 네트워크 (100%) 에서 멀웨어를 호스팅하는 웹사이트에 방문한 트래픽이 발견되었으며, 이 중 92% 는 보통 악성코드를 호스팅하는 웹 페이지로 컨텐츠 없는 트래픽을 전송했습니다. 또한 대상 네트워크의 96% 에서 가로채기 한 서버로 트래픽을 전송했습니다.

Cisco 는 또한 일반적으로 군대나 정부와 거래하지 않는 기업 내에서 군대 또는 정부 웹사이트로 이동하는 트래픽을 감지했을 뿐만 아니라 미국과의 무역이 금지된 국가와 같이 위험한 지역의 웹사이트로 이동하는 트래픽을 감지했습니다. Cisco 는 이러한 사이트가 이용되는 이유는 공공 또는 정부 조직의 유명세 때문인 것으로 보고 있습니다. 이러한 사이트로 연결되는 트래픽이 반드시 보안침해를 의미하지는 않지만, 정부 또는 군대와 자주 거래하지 않는 조직에서 이러한 트래픽이 발생한 경우에는 범죄자가 조직의 네트워크를 보안침해하여 정부 또는 군대의 웹사이트 및 네트워크에 침투하는 데 사용했다는 것을 의미할 수도 있습니다.

네트워크를 악의적인 위협으로부터 보호하려는 조직의 노력에도 불구하고 Cisco 가 2013 년에 분석한 모든 조직에서 의심스러운 트래픽이 발견되었습니다. DNS 검색을 통해 확인된 트래픽은 확실한 IoC 를 제공할 수 있으며 네트워크 내의 감지하기 어려운 위협을 저지하려는 조직은 이 트래픽을 더 자세히 조사할 필요가 있습니다. 이런 방법을 통해 일반적으로 찾아내기 매우 어려운 범죄 활동에 대한 가시성을 높일 수 있습니다.

그림 27

악의적인 트래픽의 확산

SPECIAL CISCO :

비트스쿼팅의 새로운 양상과 공격 방어하는 새로운 대응책

독특한 도메인 이름과 같거나 혼동을 일으키는 도메인 이름을 등록하는 방법인 사이버스쿼팅 (Cybersquatting) 은 오랫동안 사이버 범죄에 이용되어 왔습니다. 최근에는 고유한 도메인과 2 진 숫자 하나만 다른 도메인 이름을 등록하는 방법인 "비트스쿼팅 (bitsquatting)" 이 멀웨어 또는 신용사기를 호스팅하는 사이트로 인터넷 트래픽을 리디렉션하는 또 다른 방법으로 이용되고 있습니다.

비트스쿼팅은 컴퓨터 메모리의 비트 오류를 공격하는 일종의 사이버스쿼팅입니다. 메모리에서 읽는 비트 상태가 이전에 읽은 상태와 1 개 이상 다른 경우 메모리 오류가 발생합니다. 이러한 메모리 내의 오류는 우주 방사선 (초당 10,000 제곱미터씩 지구로 날아오는 고에너지 입자), 권장되는 환경 매개변수 범위 밖에서 사용되는 장치, 제조 결함, 저위력 핵폭발 등 여러 요인에 의해 발생할 수 있습니다.

하나의 비트가 변경되면 "twitter.com" 과 같은 도메인이 "twitte2.com" 과 같은 비트스쿼트 도메인으로 바뀔 수 있습니다. 공격자는 비트스쿼트 도메인을 등록해 메모리 오류가 발생하기를 기다리기만 하면 인터넷 트래픽을 가로챌 수 있습니다.

보안 연구원들은 가장 많이 이용된 도메인 이름을 대상으로 비트스쿼팅 공격이 발생할 가능성이 가장 높다고 보는데, 이는 비트 오류가 발생할 때 메모리 내에 이러한 도메인이 나타날 가능성이 가장 높기 때문입니다. 하지만 최근 Cisco 가 실시한 조사에 따르면 이전에는 공격 대상이 될 만큼 "많이 이용" 되지 않는 것으로 간주되던 도메인이 실제로는 상당한 양의 비트스쿼트 트래픽을 생성할 것으로 예상됩니다. 이는 장치당 메모리의 양과 인터넷에 연결된 장치의 수가 모두 증가하고 있기 때문입니다. Cisco 는 2020 년경에는 인터넷에 연결된 "지능형 사물" 의 수가 370 억 개에 달할 것으로 예상하고 있습니다.[23]

비트스쿼팅 공격 벡터

Cisco TRAC/SIO 는 다음을 포함하는 새로운 비트스쿼팅 공격 벡터를 발견했습니다.

- **하위 도메인 구분 기호 비트스쿼팅:** 도메인 이름 표시에 대해 허용되는 구문에 따르면 도메인 이름 내 유효한 문자는 A-Z, a-z, 0-9 및 하이픈 (-) 뿐입니다. 하지만 비트스쿼트 도메인을 확인할 때, 이러한 문자로 검색을 제한하면 도메인 이름에서 또 다른 유효한 중요한 문자인 점 (.) 을 간과하게 됩니다. 새로운 비트스쿼팅 기술에는 문자 "n" (이진 01101110) 과 "." (이진 00101110) 간 변환이 발생하는 비트 오류를 이용하는 기술이 포함됩니다.
- **"n" 이 "." 으로 변환되는 하위 도메인 구분 기호:** 위의 기술은 변형되어 이용될 수 있는데 2 단계 도메인 이름이 문자 "n" 을 포함하고 문자 "n" 다음에 두 개 이상의 문자가 있는 경우 이는 잠재적인 비트스쿼트가 됩니다. 예를 들어 "windowsupdate.com" 은 "dowsupdate.com" 으로 변환될 수 있습니다.
- **URL 구분 기호 비트스쿼트:** 도메인 이름에서 자주 사용되는 문맥은 URL 내에 포함됩니다. 일반적인 URL 내에서 "/" 와 같은 슬래시 문자는 호스트 이름 체계를 URL 경로로부터 구분하는 구분 기호 역할을 합니다. 슬래시 문자 (이진 00101111) 와 문자 "o" (이진 01101111) 는 비트 하나 차이로 서로 변환될 수 있습니다.

다음 페이지에 계속

이전 페이지에서 이어짐

비트스쿼팅 공격 방지: 비트스쿼트 RPZ 생성

비트스쿼팅을 방지하기 위해 일반적으로 사용되는 방법에는 다음과 같이 두 가지가 있지만 이 중 어떤 것도 최적의 예방책으로 볼 수 없습니다.

- ECC (오류 정정) 메모리 사용: 이 솔루션을 효과적으로 적용하려면 설치된 장치의 전체 기반을 전 세계에서 동시에 업그레이드해야 합니다.
- 비트스쿼트 도메인을 등록하여 타사의 등록 방지: 많이 이용되는 비트스쿼트 도메인이 이미 대부분 등록되었기 때문에 이 방법이 불가능한 경우도 있습니다. 또한 도메인 이름의 길이에 따라 많은 비용이 소요됩니다.

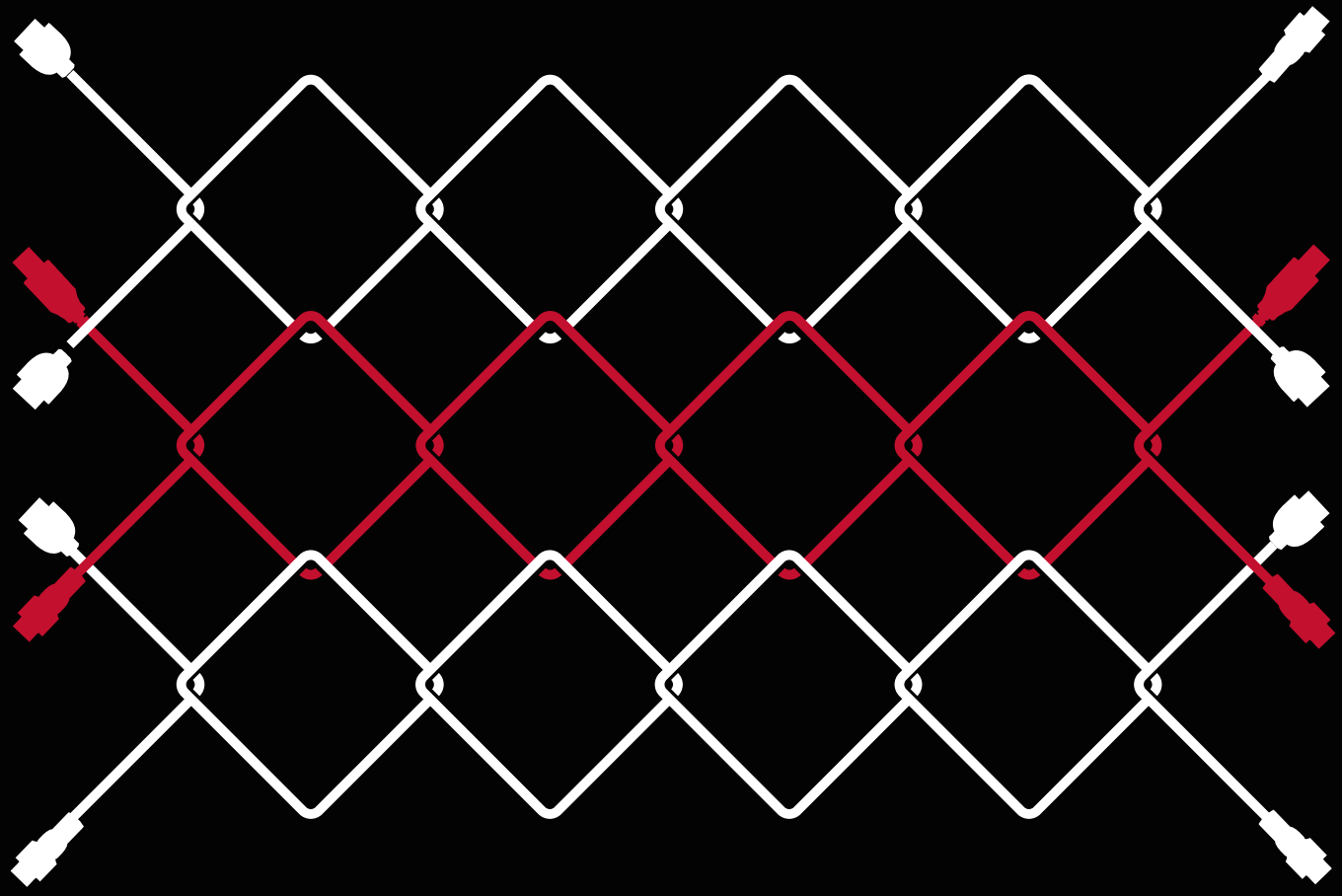
한 가지 좋은 소식은 이러한 예방책 외에도 인터넷 트래픽이 뜻하지 않게 잘못 연결되지 않도록 사용자를 보호하기 위해 보안 전문가가 이용할 수 있는 방법이 있다는 것입니다. 새로운 예방책을 충분히 도입하면 비트스쿼팅 문제를 거의 완벽하게 해결할 수 있습니다.

예를 들어 RPZ (Response Policy Zone) 는 BIND 버전 9.8.1 이래 구성 옵션으로 사용되어 왔으며 BIND 의 이전 버전에 대한 패치도 존재합니다. (BIND 는 널리 사용되는 인터넷 DNS 소프트웨어입니다.) RPZ 는 DNS 확인자가 특정 DNS 요청에 해당 도메인 이름이 존재하지 않는다고 (NXDOMAIN) 응답하도록 허용하는 로컬 영역 파일로서, 사용자를 "폐쇄된 플랫폼 (Walled Garden)" 또는 다른 가능한 영역으로 리디렉션합니다.

DNS 확인자 사용자에 대한 단일 비트 오류 영향을 최소화하기 위해 DNS 확인자 관리자는 자주 사용되거나 내부 전용인 도메인 이름의 비트스쿼팅을 방지하는 RPZ 를 생성할 수 있습니다. 예를 들어 이러한 도메인에 대한 비트스쿼팅 변수와 관련해 DNS 확인자에게 전달된 모든 요청에 NXDOMAIN 이라고 응답하도록 RPZ 를 설정하여 클라이언트 쪽의 어떠한 작업에도 비트 오류가 발생하지 않도록 함으로써 비트 오류를 자동으로 "해결" 할 수 있습니다.[24]

산업계

Cisco SIO 연구원들이 Cisco 의 원격 분석에 속하지 않는 산업계 동향에 대해 상세히 살펴봅니다.



무작위 대입 로그인 시도 웹사이트를 보안침해하기 위해 많이 이용되는 방법

사이버 범죄자들의 기존 공격 방법 중 하나인 무작위 대입 로그인 시도는 2013 년 상반기에 그 발생률이 3 배 증가했습니다.

Cisco TRAC/SIO 연구원들은 조사 과정에서 이러한 활동에 사용된 데이터의 중심지를 발견했습니다. 여기에는 "password123" 과 같이 알기 쉬운 조합을 비롯해 강력한 암호까지 망라한 890 만 개의 사용자 이름과 암호의 가능한 조합이 포함되어 있었습니다. 도난된 사용자 인증서가 이러한 목록 유지에 유용하게 사용되고 있습니다.

그림 28

무작위 대입 로그인 시도 방식

최근 무작위 대입 로그인 시도는 WordPress 및 Joomla 와 같은 널리 사용되는 CMS (Content-management System) 플랫폼을 주요 대상으로 하고 있습니다. CMS 를 통해 무단 액세스를 확보하려는 시도가 성공한 경우 공격자는 PHP (Hypertext Preprocessor) 백도어 및 기타 악성 스크립트를 보안침해된 웹사이트에 업로드할 수 있게 됩니다. 때로는 이러한 보안침해를 통해 공격자가 호스팅 서버 경로를 찾은 다음 이러한 서버를 무단 확보할 수도 있습니다 (그림 28).

전 세계에서 WordPress 사이트는 약 670 만 개 이상에 달하고 많은 퍼블리셔가 블로그, 뉴스 사이트, 기업 사이트, 잡지, 소셜 네트워크, 스포츠 사이트 등을 생성하기 위해 이 플랫폼을 사용하고 있으므로 많은 사이버 범죄자들이 CMS 를 통한 액세스 확보에 관심을 갖게 된 것은 당연합니다.[25] 급속하게 성장하고 있는 CMS 플랫폼인 Drupal 도 공격 대상이 되었습니다. 예를 들면 5 월에는 "Drupal.org 서버 인프라에 설치된 타사 소프트웨어를 통해 Drupal 에 무단 액세스 시도가 발생" 하여 사용자들에게 암호를 변경하라는 지침이 전달되었습니다.[26]

많은 사이버 범죄자들이 CMS 를 통한 액세스 확보에 관심을 갖게 되었습니다.

하지만 이러한 시스템이 주요 공격 대상이 된 이유는 높은 이용률뿐만이 아닙니다. 이러한 사이트 중 대부분이 높은 이용률에도 불구하고 사이트 소유자에 의해 방치되고 있습니다. 방치된 블로그 및 구매 후 사용하지 않는 상태로 남겨진 도메인이 수백 만개에 달하며 이 중 대다수는 현재 사이버 범죄자의 소유가 된 것으로 예상됩니다. Cisco 보안 전문가들은 전 세계 신흥 인터넷 시장에서 점점 많은 사용자들이 블로그 또는 웹사이트 구축 후 이를 방치하게 되면서 이 문제의 심각성이 커질 것으로 예상하고 있습니다.

또한 CMS 의 기능을 확대하고 비디오, 동영상 및 게임을 지원하도록 설계된 플러그인의 사용이 확산됨에 따라 악의적인 사용자들이 WordPress 및 Joomla 와 같은 플랫폼에 무단 액세스를 시도하기에 유리한 환경이 조성되고 있습니다. Cisco 연구원들이 2013 년에 발견한 많은 CMS 보안침해의 원인은 보안을 고려하지 않은 채 허술하게 설계되고 PHP 웹 스크립트 언어로 작성된 플러그인으로 볼 수 있습니다.

DNS :
완화 방법

Cisco 보안 전문가에 따르면 DNS 증폭을 통해 시작된 공격 문제가 2014 년에도 계속될 것으로 예상됩니다. Open Resolver Project (openresolverproject.org) 는 2013 년 10 월부터 인터넷에 존재하는 2,800 만 개의 개방 확인자가 "심각한 위협" 이 되고 있다고 보고했습니다 (300Gbps 의 속도로 이루어진 Spamhaus DDoS 공격에 사용된 개방 확인자는 30,000 개에 불과).

개방 확인자는 응답을 보낼 때 필터링을 수행하지 않습니다. DNS 는 상태 비저장 UDP 프로토콜을 사용하며, 이에 따라 다른 대상을 대신해 요청을 생성할 수 있게 됩니다. 그 결과 이러한 대상에게 수신되는 트래픽이 증폭됩니다. 따라서 머지않아 업계에서는 개방 확인자를 파악하고 이를 폐쇄하는 수순의 작업을 수행해야 할 것입니다.

기업은 공격을 방지하기 위한 Internet Engineering Task Force 의 BCP (Best Current Practice) 38 구축과 같은 다양한 방법을 통해 DNS 증폭을 통한 공격 가능성을 줄일 수 있습니다. BCP 에서는 IP 연결 공급업체에게 고객을 통해 네트워크에 진입하는 패킷을 필터링하고 고객에게 할당되지 않은 소스 주소를 가진 모든 패킷을 삭제할 것을 권장합니다.[30] BCP 는 Cisco 와 공동 제작되었으며

다음 페이지에 계속

디도스 (DDoS) 공격: 오래된 수법의 새로운 등장

표적으로 삼은 웹사이트의 유/출입 트래픽을 방해하고 서비스를 마비시킬 수 있는 디도스 (DDoS[Distributed Denial-of-Service]) 공격의 횟수와 강도가 증가했습니다.

디도스 공격은 "오래된" 사이버 범죄 방법으로 간주되어 왔기 때문에 많은 기업들은 기존의 보안 조치로 이런 공격에 적절히 대비할 수 있다고 믿어 왔습니다. 하지만 정치적인 의도를 가지고 여러 금융 기관을 대상으로 이루어졌던 Operation Ababil 을 포함해 2012 년과 2013 년에 대규모 디도스 공격이 발생하면서 이러한 믿음은 흔들리게 되었습니다.[27]

"디도스 공격은 2014 년 공공 및 민간 부문 조직에 있어 주요 보안 문제가 될 것입니다." 라고 John N. Stewart 수석 부사장겸 최고 보안 책임자는 말합니다. "앞으로의 공격은 더욱 장기간, 폭넓게 발생할 것으로 예상됩니다. 모든 조직, 특히 금융 서비스 및 에너지와 같이 이미 주요 공격 대상인 업종을 운영하거나 이와 관련된 조직은 '디도스 공격에 민첩하게 대응할 수 있을까?'라고 자문해 보아야 합니다."

57 페이지 "DarkSeoul" 참조). 이러한 공격이 발생하면 당황한 은행 직원이 고객에게 이체 통지서를 보내지 못하여 고객이 사기를 신고하지 못하게 될 수도 있습니다. 또한 이러한 공격으로부터 기관이 복구되는 시점에는 이미 금융 손실을 만회하기가 불가능합니다. 2012 년 12 월 24 일에 캘리포니아 지역 금융 기관에서 "은행 직원 모르게 고객의 온라인 계좌가 탈취되어 900,000 달러 이상의 자금이 도난 된 사건은 이러한 공격의 한 예입니다."[28]

이전 페이지에서 이어짐

uRPF 구축 및 실행에 대한 지침을 제공합니다.[31]

또 다른 방지책으로는 모든 신뢰할 수 있는 DNS 서버에서 속도 제한을 사용하도록 구성하는 방법이 있습니다. 기업의 도메인을 지원하는 신뢰할 수 있는 네임 서버는 일반적으로 모든 요청에 개방됩니다. DNS RRL (DNS Response Rate Limiting) **은 기업이 DDoS 공격의 매개체로 이용되지 못하도록 DNS 서버가 같은 개체로부터의 같은 질문에 지나치게 많이 응답하지 못하도록 설정하는 기능입니다.** DNS RRL **은 DNS 서버에서 활성화되며, 서버 관리자가 공격자의 증폭 공격에 서버가 사용되는 것을 막을 수 있는 방법 중 하나입니다.** DNS **응답 속도 제한은 새로운 기능으로 모든 DNS 서버에서 지원되지는 않지만 많이 사용되는** DNS **서버인** ISC BIND **에서는 지원됩니다.**

또한 모든 반복 DNS **서버는** ACL (Access Control List) **을 통해 고유한 네트워크 호스트의 쿼리에만 응답하도록 구성되어야 합니다.** ACL **이 올바르게 관리되지 않으면 특히 대규모의 가용 대역폭이 지원되는 대규모 서버의 경우** DNS **공격의 주요 원인이 될 수 있습니다. 이 방법은 또한** DDoS **공격의 매개체가 될 가능성을 줄이는 데 도움이 됩니다.**

다음 페이지에 계속

43 페이지의 "취약한 에코시스템의 균열" 참조). 악의적인 사용자들은 인터넷 인프라의 일부를 무단으로 확보하여 대규모의 대역폭을 이용함으로써 강력한 공격을 무제한으로 실행할 준비를 마칠 수 있습니다. 이러한 상황은 이미 발생하고 있습니다. 2013 년 8 월에 중국 정부는 사상 최대 규모의 디도스 공격으로 인해 중국 인터넷이 4 시간 동안 마비되었다고 보고했습니다.[29]

스팸 유포자들도 수익 창출에 방해가 되는 것으로 간주되는 조직을 반격하기 위해 디도스 공격을 이용합니다. 2013 년 3 월에는 스팸 유포자들을 추적하여 Spamhaus Block List, 즉 의심스러운 IP 주소의 디렉토리를 생성하는 비영리 조직인 Spamhaus 에 DDoS 공격이 발생해 웹사이트가 일시적으로 마비되고 전 세계의 인터넷 트래픽이 저하되었습니다. 공격자들은 사용 약관이 느슨한 네덜란드 호스팅 공급업체인 CyberBunker 및 Spamhaus 의 활동에 공개적으로 불만을 나타낸 적이 있는 STOPhaus 와 관련이 있는 것으로 알려졌습니다. 이 디도스 공격은 폭넓게 사용되던 Spamhaus 서비스에서 CyberBunker 를 블랙리스트에 추가한 후에 발생했습니다. 이에 따른 보복으로 스팸 유포자들은 디도스 공격을 통해 Spamhaus 웹사이트를 마비시키고자 한 것입니다.

이 디도스 사건에는 고유한 IP 범위 외의 쿼리에도 응답하는 개방 DNS 확인자를 공격하는 DNS 증폭 공격이 이용되었습니다. 공격자는 개방 확인자에 대상처럼 위장된 소스 주소와 함께 교묘하게 만들어진 매우 작은 크기의 쿼리를 보냄으로써 의도한 대상에서 훨씬 대규모의 응답을 유도할 수 있습니다. Spamhaus 웹사이트를 마비시키려는 첫 번째 시도가 실패한 뒤 공격자들은 Spamhaus 에 대한 주요 공급업체들을 대상으로 증폭 공격을 실행했습니다.

이전 페이지에서 이어짐

"신뢰할 수 있는 네임 서버가 DDoS 공격의 매개체가 되는 개체에 대한 지원을 중단하도록 허용하는 것과 관련한 논의가 보안 업계에서 이루어지고 있으므로 기업은 위에 설명된 간단한 방지책을 시행해야 합니다." 라고 Cisco 위협 분석 정보 책임자인 Gavin Reid 씨는 말합니다.

DNS 모범 사례에 대한 자세한 내용은 "DNS 모범 사례, 네트워크 보호, 공격 파악" (http://www.cisco.com/web/about/security/intelligence/dns-bcp.html) 을 참조하십시오.

다크서울 (DarkSeoul)

"디도스 공격: 오래된 수법의 새로운 등장" 에서 살펴본 것처럼 사이버 범죄자들의 새로운 관심 부문 및 호스팅 서버를 보안침해하는 전문 기술의 급속한 발전으로 인해 더욱 쉽게 디도스 공격을 실행하고 조직의 자산을 도용할 수 있게 되었습니다.

Cisco 보안 연구원들은 향후 디도스 공격은 도난으로 인한 경제적 손실 등 심각한 운영 중단 및 손실을 야기할 수 있다고 경고합니다.

2013 년 3 월 발생한 다크서울 (DarkSeoul) 은 수만 개의 PC 와 서버의 하드 드라이브에 있는 데이터를 파괴하도록 설계된 멀웨어인 "와이퍼 (Wiper)" 가 사용되었습니다. 이 공격은 한국의 금융 기관 및 언론사를 대상으로 한 공격으로, 페이로드를 동시에 활성화하도록 설정되었습니다. 그러나 와이퍼 멀웨어는 공격의 특징 중 하나일 뿐입니다. 이 멀웨어가 작동됨과 동시에 한국 네트워크 공급업체 LG U+의 웹사이트가 손상되었으며 공격 대상이 된 다른 조직의 네트워크가 마비되었습니다. 이는 와이퍼 멀웨어에서는 재현되지 않는 기능입니다.[32]

일부에서는 이 공격이 북한에서 남한 경제를 교란시키기 위해 시작한 사이버 전쟁이거나 다른 국가로부터의 방해 공작이라고 생각했습니다. 하지만 다크서울 (DarkSeoul) 공격은 금전적 이득을 은폐하기 위한 것이었을 수도 있습니다.[33]

이 공격의 특징과 배후에 대해 보안 연구원들이 아직 파악 중이지만, 다크서울 공격 계획이 2011 부터 시작되었을 수 있다는 증거가 발견되었습니다. 바로 그해 미국 FBI (연방 수사국) 는 피해자의 계좌로부터 불법적으로 자금을 이체하는 행위를 은폐하기 위해 설계된 금융 트로이 목마에 대해 최초로 경고했습니다.[34] 그리고 2012 년에 RSA 보안 기업은 예정된 날짜에 공격을 시작해 "보안 팀이 이러한 공격을 저지하기 전에 가능한 최대한 많은 보안침해 계좌로부터 자산을 유출시키는" 정교한 트로이 목마 공격을 계획하는 새로운 유형의 사이버 범죄에 대해 보고했습니다.[35] 2012 년 12 월 24 일에는 온라인 절도범이 캘리포니아 지역 금융 기관의 자산을 훔치는 동안 이를 감추기 위해 DDoS 공격을 이용했습니다.[36]

Cisco TRAC/SIO 연구원에 따르면 언론 및 금융 기관에 대한 다크서울 공격에서 발견된 멀웨어 바이너리 중 하나는 동일 한국 은행들의 고객을 노린 금융 트로이 목마인 것으로 나타났습니다. 다크서울 공격이 발생하기 전까지 발생한 사이버 범죄의 움직임과 더불어 이 사실을 고려해 볼 때, 이 공격은 다른 것으로 가장한 절도 행위였을 수도 있습니다.

랜섬웨어 (Ransomware)

2013 년 공격자들은 기존의 봇넷 방식의 PC 감염과는 확연히 다른 방법을 사용했습니다. 이러한 새로운 추세 중 하나는 랜섬웨어가 보안침해된 웹사이트, 악성 이메일 및 다운로더 트로이 목마의 최종 멀웨어 페이로드로서 이용되는 사례가 늘고 있다는 점입니다. 랜섬웨어는 요구된 금액이 지불될 때까지 감염된 시스템의 정상적인 작동을 방해하는 멀웨어의 일종입니다.

2013 년 공격자들은 기존의 봇넷 방식의 PC 감염과는 확연히 다른 방법을 사용했습니다.

랜섬웨어를 사용하면 추적이 어려울 뿐만 아니라 공격자는 기존의 봇넷을 통한 중개 임대 서비스를 사용하지 않고도 직접적인 수익원을 확보할 수 있습니다. 공격자는 실업 또는 경기 침체로 인해 개인 기업이 크게 증가한 합법적인 지역 경제를 모방하기도 하지만, 이 사이버 범죄는 예방책으로 인해 봇넷 가용성과 액세스 가능한 익스플로잇 키트가 감소로 인해 발생했습니다.

2013 년 가을 랜섬웨어의 새로운 유형인 CryptoLocker 가 해독할 수 없는 것으로 간주되는 RSA 2048 비트 키 쌍과 AES-256 의 조합으로 피해자의 파일을 암호화하기 시작했습니다. CryptoLocker 는 파일을 로컬 시스템 밖으로 이동시켜 임의의 쓰기 가능한 매핑된 드라이브에 일치하는 파일 유형을 포함시킵니다. 암호화가 끝나면 요구된 금액을 지불하라는 자세한 지시사항이 포함된 일련의 대화 상자가 피해자에게 표시됩니다 (그림 29). 또한 특정한 시간 내에 지불하라는 타이머도 함께 표시됩니다 (30~100 시간). 또한 이러한 대화 상자에는 요구된 금액을 시한 내에 지불하지 않으면 C&C (command-and-control) 서버에서 개인 키가 삭제되며 그 이후에는 파일을 해독할 수 없다는 경고도 표시됩니다.

CryptoLocker 는 블랙홀 및 쿨 익스플로잇 키트 프레임워크 제작자가 체포되어 해당 키트가 사라진 시점인 10 월 중순에 발생했습니다.

그림 29

특정 금액의 지불을 지시하는 CryptoLocker

보안 전문 인력의 부족 및 솔루션의 격차

[사이버 범죄자들이 사용하는 기술과 전술의 정교함과, 네트워크를 침해하고 데이터를 도용하는 연속적인 공격 시도가 이러한 위협에 대처하는 IT 및 보안 전문가들의 능력을 앞지르고 있습니다. 하지만 대다수 기업들은 네트워크를 지속적으로 감시하거나 사이버 범죄자의 침입을 탐지할 수 있는 인력이나 시스템을 보유하고 있지 못한 상태입니다.]

이 문제는 보안 전문 인력의 부족으로 인해 더욱 심각해지고 있습니다. 예산이 충분한 경우에도 CISO 는 최신 보안 기술을 갖춘 인력을 고용하는 데 어려움을 겪고 있습니다. 2014 년경에는 전 세계적으로 업계의 보안 전문가가 100 만 명 이상 부족할 것으로 예상됩니다. 또한 비즈니스 목표에 맞춰 보안 데이터를 이해하고 분석할 수 있는 데이터 과학 기술을 갖춘 보안 전문가도 부족한 상황입니다. (68 페이지의 부록, "보안 조직을 위한 데이터 과학자의 필요성: 보안 실무자를 위한 기초 데이터 분석 툴" 참조)

CISO 는 최신 보안 기술을 보유한 인력을 고용하고자 노력합니다.

새로운 환경으로서의 클라우드

CISO 가 Cisco 보안 전문가에게 설명한 바와 같이 (18 페이지 참조), 중요 비즈니스 데이터를 클라우드로 점점 더 많이 이동시킴에 따라 관련된 보안 우려가 커지고 있습니다.

Cisco 의 Michael Fuhrman 엔지니어링 부사장에 따르면 클라우드 혁신은 1990 년대 후반에 이루어진 웹 기반 솔루션의 부상에 비교할 수 있습니다.

"이러한 혁신에 따라 최신 기술의 비즈니스 활용 방식이 크게 변화했으며 이와 함께 사이버 범죄도 증가했습니다." 라고 Fuhrman 부사장은 말합니다. "오늘날에는 클라우드가 이러한 변화의 원인이 되고 있습니다. 기업들은 많은 중요 애플리케이션을 클라우드에 호스팅할 뿐만 아니라 클라우드를 통해 중요 비즈니스 정보를 이용 및 분석하고 있습니다."

클라우드 컴퓨팅의 부상은 부인할 수 없는 추세이며 앞으로도 지속될 것입니다.

클라우드 컴퓨팅의 부상은 부인할 수 없는 추세이며 앞으로도 지속될 것입니다. Cisco 는 2017 년까지 클라우드 네트워크 트래픽이 3 배 이상 증가할 것으로 전망합니다.[37]

보안 전문가들은 2014 년 이후 기업의 전체 네트워크 환경이 클라우드로 전환될 것으로 예상하고 있습니다. 최근 수년 간 이러한 네트워크 경계는 점점 모호해지고 있습니다. 하지만 클라우드에 존재하는 수많은 애플리케이션 및 데이터로 인해, 조직이 기업 네트워크 경계 안팎으로 무엇이 이동하고 있는지, 사용자들이 무엇을 하는지 파악하기가 점점 어려워지고 있습니다.

이러한 클라우드로의 전환에 따라 데이터 저장, 이동 및 액세스 위치가 변화하고 있으며 이는 공격자에게 점점 큰 기회를 제공하고 있습니다.

클라우드로 데이터에 대한 제어를 넘기면서 발생하는 우려와 함께, 클라우드 공급업체가 보안 침해로부터 제품을 보호하는 방식에 대한 정보가 부족하다는 점도 문제가 됩니다. 대부분의 조직은 공급업체의 서비스 레벨 계약 내용이나 공급업체에서 보안 소프트웨어 또는 취약점 패치를 얼마나 자주 업그레이드하는지에 대해 제대로 문의하지 않습니다.

조직은 클라우드 공급업체에서 공격 방지 또는 진행 중인 공격을 감지 및 저지하기 위해 가장 정교한 툴 및 전략을 사용하고 있는지 확인해야 합니다. 정보 보안 팀은 이를 위해 "우리의 데이터를 신뢰할 수 있는 방식으로 관리 및 보호하기 위해 공급업체에서 어떠한 제어를 수행하는지" 알아봐야 합니다.

한편 클라우드 공급업체는 악화되는 위협 환경에 대응하기 위해 요구되는 더 많은 국제 규정을 준수하기 위한 일련의 관리 가능한 제어 세트를 파악하고 구축하는 데 어려움을 겪고 있습니다.

"보안 및 중요 인프라를 위해 공급업체를 선택할 때 우리는 종종 검증된 기술과 평판을 기준으로 선택합니다." 라고 수석 부사장겸 최고 보안 책임자는 말합니다. "최근에는 공급업체의 프로세스 및 발전하는 보안 접근 방식도 중요한 요인이 되고 있습니다."

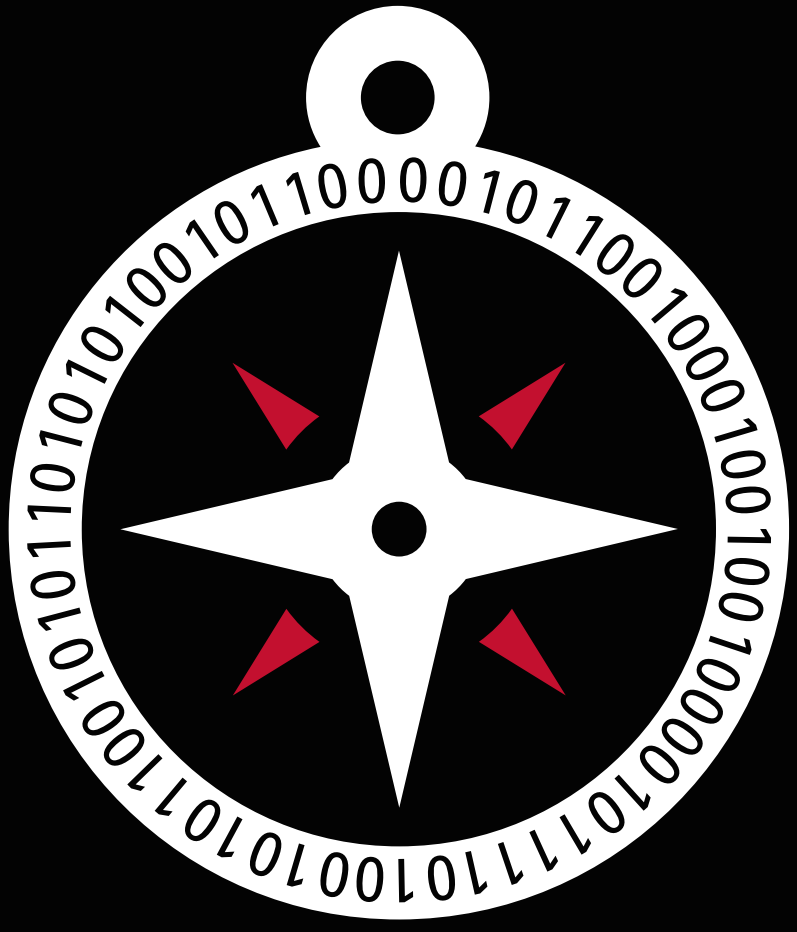
한편, 조직은 네트워크 경계 밖의 위치 및 중요 비즈니스 데이터에 대한 클라우드 사용의 증가와 같은 클라우드의 위협 요소를 이용해 정확하고 신속한 보안 결정을 내릴 수도 있습니다. 클라우드를 통해 이동하는 트래픽이 증가함에 따라, 역시 클라우드를 이용하는 보안 솔루션을 통해 이러한 트래픽을 신속하고 간단하게 분석하여 이러한 보완적인 정보의 이점을 얻을 수 있습니다. 또한 소규모 조직이나 예산이 제한된 조직의 경우 올바르게 보호 및 관리되는 클라우드 서비스를 통해 기업의 자체 서버 및 방화벽보다 강력한 보안 기능을 제공할 수 있습니다.

"보안 및 핵심 인프라를 위해 공급업체를 선택할 때 우리는 종종 검증된 기술과 평판을 기준으로 선택합니다. 최근에는 공급업체의 프로세스 및 발전하는 보안 접근 방식도 점점 중요한 요인이 되고 있습니다."

John N. Stewart, Cisco 수석 부사장 및 CSO (Chief Security Officer)

권장 사항

점점 많은 조직들이 최신 기술을 활용하고 조직의 아키텍처 및 운영을 간소화하며 보안 팀의 역량을 강화하는 효과적인 전략을 바탕으로 보안 비전을 강화하고자 노력하고 있습니다.



2014 년 목표: 신뢰성 검증 및 파악 능력 향상

오늘날 네트워크 또는 장치와 관련한 신뢰 수준을 동적으로 평가해야 하는 환경에서 조직은 일관성 없는 시행, 고립된 위협 분석 정보, 관리할 수많은 공급업체 및 제품으로 이어지는 분산된 보안 모델로 인해 고심하고 있습니다.

조직, 데이터 및 악의적인 사용자의 교묘한 공격 간의 관계는 하나의 어플라이언스로 대응하기에는 너무 복잡합니다. 또한 대부분의 조직에는 클라우드 컴퓨팅, 모빌리티 그리고 기술 발전에 기반한 기타 새로운 비즈니스 방식이 제시하는 과제 및 기회에 맞게 조직의 보안 모델을 조율할 수 있는 전문 지식과 경험을 갖춘 보안 인력이 부족한 상황입니다.

지난 10 년간 모든 유형의 조직들이 보안의 틈새를 새로 발생시키지 않고 기존의 틈새도 더 벌어지지 않도록 하면서 혁신을 수용하는 방법을 파악하기 위해 노력해 왔습니다. 2013 년에는 신뢰성 문제가 주요 화두로 부각되었습니다. 오늘날 모든 사용자들은 직장 또는 개인 생활에서 매일 사용하는 기술의 신뢰성에 대해 의문을 갖고 있습니다. 따라서 기술 공급업체가 고객에게 제조 프로세스에서 보안이 최우선으로 고려되는 사항임을 보장하고 이러한 주장을 뒷받침해야 할 필요성이 그 어느 때보다도 커졌습니다.

"오늘날 시장에서는 신뢰성이 더욱 중요시되고 있으며 공급업체의 제품 설계 프로세스 및 기술은 위협과 관련된 오늘날의 요구 사항을 충족해야 합니다." 라고 Cisco 의 최고 보안 책임자인 John N. Stewart 씨는 말합니다. "신뢰성에 대한 약속만으로는 충분하지 않습니다. 기업은 인증된 제품, 통합된 개발 프로세스, 혁신적인 기술 및 업계에서 인정받는 입지를 통한 검증을 필요로 합니다. 또한 조직에서 사용하는 기술 제품 및 이러한 제품을 제공하는 공급업체의 신뢰성을 검증하는 것이 조직의 지속적인 우선 사항이 되어야 합니다."

기업의 보안을 강화하기 위해서는 보안 운영과 비즈니스 목표를 더욱 효과적으로 조율하는 것도 중요합니다. 이러한 조율은 자원이 제한되고 예산이 부족한 환경에서 CISO 및 조직의 기타 보안 책임자들이 주요 위험과 적절한 방지책을 파악하는 데 도움이 됩니다. 여기에는 기업의 모든 자원을 동시에 완벽하게 보호할 수는 없다는 사실을 인정하는 과정이 포함됩니다. "사이버 보안의 관점에서 가장 중요한 사항이 무엇인지에 대해 합의해야 합니다." 라고 Cisco 위협 분석 정보 책임자인 Gavin Reid 씨는 말합니다. "이는 모든 문제에 대한 만능 해결책을 찾기를 바라는 것보다 생산적인 방식입니다."

보안과 관련된 오늘날의 당면 과제를 해결하려면 조직은 보안 모델을 포괄적으로 검토하고 다음과 같은 전체 공격 전반에 대해 파악해야 합니다.

- 공격 전: 네트워크를 방어하기 위해 조직은 장치, 운영 체제, 서비스, 애플리케이션, 사용자와 같은 네트워크의 요소를 파악해야 합니다. 또한 액세스 제어를 구현하고 보안 정책을 시행하며 중요 자산에 대한 애플리케이션 및 전반적인 액세스를 차단해야 합니다. 하지만 정책 및 제어는 이 과정의 일부에 지나지 않습니다. 이러한 조치를 통해 공격 영역을 줄일 수는 있지만 공격자가 목적을 이루기 위해 찾아내고 공격할 수 있는 틈새는 항상 존재합니다.
- 공격 중: 조직은 네트워크, 엔드포인트, 모바일 기기 및 가상 환경과 같이 위협이 나타날 수 있는 모든 지점에서 작동하는 솔루션을 통해 폭넓은 공격 벡터에 대응해야 합니다. 효과적인 솔루션이 구축되면 보안 전문가들이 더욱 효과적으로 위협을 차단하고 운영 환경을 방어할 수 있습니다.
- 공격 후: 대체로 공격은 성공하는 경우가 많습니다. 따라서 조직은 손실 정도 파악, 이벤트 저장, 문제 해결 및 정상적인 운영 재개와 같은 조치를 최대한 신속하게 수행하기 위한 공식적인 계획을 마련해야 합니다.

"공격자와 이들이 사용하는 툴은 기존의 방어책을 피하도록 발전되어 왔습니다. 실제로 이제는 공격이 과연 발생할 것인지가 아니라 언제 발생할 것인지에 관심을 두어야 합니다." 라고 Cisco 보안 그룹의 수석 보안 설계자인 Marty Roesch 씨는 말합니다. "공격 전, 공격 중, 공격 후와 같이 공격 전반에 대한 파악 능력에 기반하고 위협에 중점을 둔 보안 접근 방식이 필요합니다."

서비스를 통해 보안 과제를 해결하는 방식

더 넓어진 공격 영역, 공격 모델의 빠른 확산과 정교함, 네트워크 복잡성 증가에 따라 점점 많은 조직이 최신 기술을 활용하고 조직의 아키텍처 및 운영을 간소화하며 보안 팀의 역량을 강화하는 보안 비전을 강화하고자 노력하고 있습니다.

60 페이지에서 다룬 대로, 보안 전문 인력의 부족으로 인해 이러한 문제는 더욱 복잡해지고 있습니다. 또한 보안 업계의 혁신은 이러한 새로운 툴을 도입 및 운영할 수 있는 조직의 능력보다 빠른 속도로 이루어지고 있습니다.

변화하는 보안 환경에 효과적으로 대응할 수 있는 적절한 인재를 찾기는 쉽지 않습니다. 이를 보완하기 위한 외부 리소스를 활용하면 비용을 줄일 수 있을 뿐만 아니라 보다 우선 순위가 높은 과제에 주력할 수 있는 리소스를 확보할 수 있습니다.

시스템 취약점 극복

사이버 보안을 유지하기 위해서는 위험을 예방하는 것이 무엇보다 중요합니다. 따라서 점점 많은 사이버 범죄자들이 개별 컴퓨터가 아닌 인터넷 인프라를 보안침해하는 데 관심을 돌리고 있는 상황에서 Cisco 보안 전문가들은 ISP 및 호스팅 기업들이 인터넷 무결성을 보호하기 위해 보다 적극적인 역할을 수행할 것을 권장하고 있습니다.

DarkLeech 및 Linux/CDorked (45 페이지 참조) 와 같은 감지하기 어려운 위험을 파악하려면 호스팅 공급업체의 "인적 대응" 이 확대되어야 합니다. 이러한 대응에는 사용자의 보고를 진지하게 받아들이고 철저하게 조사하는 것이 포함됩니다. 공급업체는 또한 서버 운영 체제 설치의 무결성을 검증할 수 있도록 보다 효과적인 제어 기능을 구축해야 합니다. Cisco 연구원들은 CDorked 와 같은 교묘한 멀웨어 때문에, 설치의 무결성을 검증하기 위한 제어 기능이 이미 구축되어 있지 않으면 보안 팀에서 바이너리 교체 여부를 확인할 방법이 없다고 말합니다.

물론 개별 사용자의 시스템도 보안침해될 수 있지만 위협이 시작되기 훨씬 전부터 망이 약화되는 경우가 많습니다. 오늘날 망 내부에서의 공격 발생 빈도가 증가함에 따라 공급업체는 인터넷 인프라를 대상으로 하는 잠재적인 위협에 대한 인식을 개선할 필요가 있습니다.

부록

데이터 과학자를 필요로 하는 보안 조직

보안 실무자를 위한 기초 데이터 분석 툴

CSO (Chief Security Officer) 팀은 과거와는 비교할 수 없을 정도로 많은 데이터를 수집하며 이러한 데이터가 가진 분석 정보에는 커다란 활용 가치가 있습니다. 보안 관련 데이터를 분석해 공격자의 활동에 대해 파악하고 공격을 방지하는 방법에 대한 실용적인 정보를 얻을 수 있습니다.

보안 실무자들은는 이미 데이터 분석을 수행하고 있으며 기록이 생성되고 표시될 것으로 기대하고 있습니다. 침입 테스트 담당자는 진단을 마친 후 조사 기록을 작성합니다. 운영 체제 설계자는 감사 서브시스템을 구축합니다. 애플리케이션 개발자는 로그를 생성하는 애플리케이션을 설계합니다.

어떠한 기록을 사용하든 한 가지 분명한 사실은 보안 실무자가 수많은 데이터를 보유하고 있으며 이러한 데이터를 분석해 중요한 정보를 발견할 수 있다는 것입니다.

보안 실무자는 수많은 데이터를 보유하고 있으며 이러한 데이터를 분석함으로써 중요한 사실을 발견할 수 있습니다.

데이터 분석 자체는 새로운 개념이 아니지만 보안 환경의 변화로 인해 데이터 분석 프로세스에 다음과 같은 변화가 발생했습니다.

- 엄청난 양의 데이터가 생성되고 있습니다.
- 애드 혹 데이터 분석이 더욱 자주 필요하게 되었습니다.
- 표준화된 보고서는 유용하지만 그것만으로는 충분하지 않습니다.

다행히 이렇게 더욱 복잡해진 환경에도 불구하고 보안 실무자가 데이터 분석을 수행하는 데 따르는 장애 요인은 적으며 데이터 분석 툴 에코시스템은 풍부합니다. 다음은 보안 실무자들이 데이터 분석을 시작하는 데 사용할 수 있는 몇몇 무료 툴에 대한 개요입니다.

Wireshark 및 Scapy 를 통한 트래픽 분석

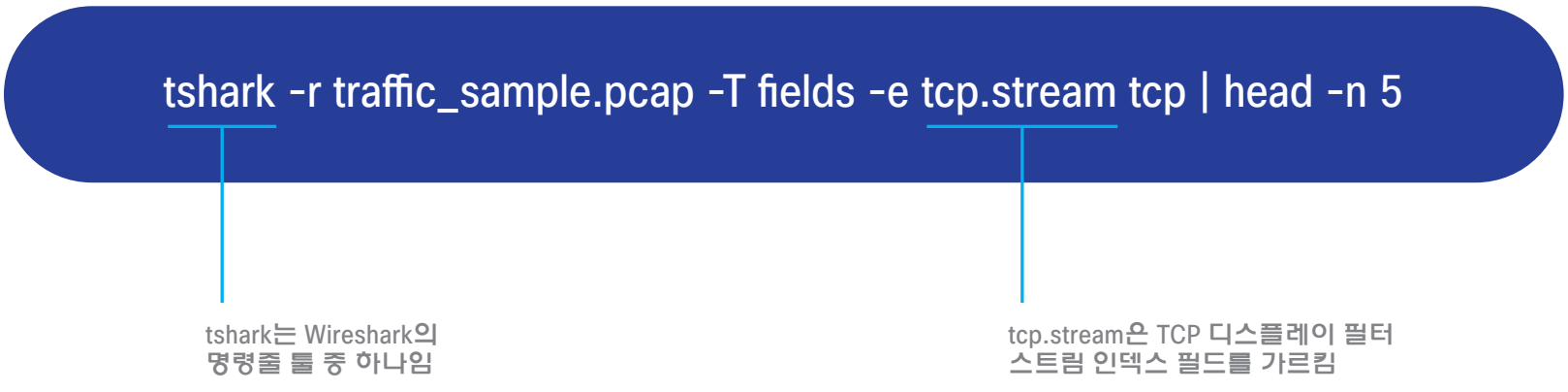
트래픽 분석에 매우 유용한 두 가지 툴로는 Wireshark 와 Scapy를 들 수 있습니다. Wireshark 는 소개할 필요도 없을 만큼 유명합니다. Scapy는 트래픽을 생성하거나 검사하기 위해 Python 모듈로써 또는 대화식으로 사용할 수 있는 Python 기반 툴입니다.

Wireshark 는 다양한 필수 명령줄 툴 및 프로토콜 분석기를 제공합니다. 예를 들어 Wireshark 의 tcp.stream 디스플레이 필터 필드를 사용하면 여러 TCP 스트림을 포함하는 pcap 파일을 단일 TCP 스트림에 속하는 모든 패킷을 포함하는 각각의 작은 파일로 나눌 수 있습니다.

그림 A1 은 traffic_sample.pcap 의 최초의 TCP 패킷 5 개의 TCP 스트림 인덱스를 인쇄하는 이러한 명령을 나타냅니다.

그림 A1

tcp.stream 인덱스를 추출하기 위한 tshark 명령



이러한 정보를 바탕으로 traffic_sample.pcap 를 다음과 같은 개별 pcap 파일로 나누는 스크립트를 작성할 수 있습니다.

```
$ cat ~/bin/uniq_stream.sh
#!/bin/bash

function getfile_name () {

                orig_name=$1
                stream=$2
                file_name= ”$ (echo $orig_name | cut -d ’.’ -f1)"
                file_name+= ”-${stream}.pcap ”

                echo “${file_name}”

                return 0
}

streams=$ (tshark -r ${1} -T fields -e tcp.stream | sort -un | tr ‘\n ’ ‘ ‘)

for x in ${streams}
do
                file_name=$ (getfile_name ${1} ${x})
                echo “Creating ${file_name}...”
                tshark -r ${1} -w $file_name tcp.stream eq ${x}
done
$
```

이 스크립트는 traffic_sample.pcap 의 각 TCP 스트림 147 개에 대한 단일 pcap 파일을 생성합니다. 이제 각 TCP 스트림에 대한 추가 분석을 더욱 쉽게 수행할 수 있습니다. traffic_sample.pcap 의 비 TCP 패킷은 다음과 같은 새로운 pcap 파일에 포함되지 않습니다.

```
$ /bin/uniq_stream.sh traffic_sample.pcap
Creating traffic_sample-1.pcap...
Creating traffic_sample-2.pcap...
...
...
Creating traffic_sample-146.pcap...
Creating traffic_sample-147.pcap...
```

Scapy 에는 고유한 이점이 있습니다. Scapy 는 Python 에서 개발되었으므로 Python 언어 및 기타 Python 툴의 모든 기능을 사용할 수 있습니다. 다음 정보는 Scapy 가 연산자 오버로드를 이용하여 트래픽 작업을 신속하고 간단하게 수행할 수 있도록 하는 방식을 나타냅니다.

```
# scapy
>>> dns_query = IP () /UDP () /DNS ()
>>> from socket import gethostbyname,gethostname
>>> dns_query[IP].src = gethostbyname (gethostname () )
>>> dns_query[IP].dst = “8.8.8.8 ”
>>> import random
>>> random.seed ()
>>> dns_query[UDP].sport = random.randint (0, 2**16)
>>> dns_query[DNS].id = random.randint (0, 2**16)
>>> dns_query[DNS].qdcount = 1
>>> dns_query[DNS].qd = DNSQR (qname= “www.cisco.com ”)
>>> scapy.sendrecv.sr1 (dns_query)
>>> response = scapy.sendrecv.sr1 (dns_query)
Begin emission:
.....Finished to send 1 packets.
.*
Received 14 packets, got 1 answers, remaining 0 packets
>>> response[DNS].ar[DNSRR].rdata
‘64.102.255.44 ’
>>>
```

이 예는 패킷을 구성하는 방법과 라이브 트래픽을 분석하는 방법을 나타냅니다. Scapy 를 사용해 pcap 파일도 간단하게 분석할 수 있습니다.

CSV 데이터 분석

CSV (Comma-separated Value) 는 데이터 교환에 많이 사용되는 형식입니다. tshark 를 포함한 많은 툴 사용시 데이터를 CSV 형식으로 내보낼 수 있습니다. 일반적으로 보안 실무자들은 Excel 과 같은 스프레드시트 프로그램을 사용해 CSV 데이터를 분석합니다. 또한 grep, cut, sed, awk, uniq, and sort 와 같은 명령줄 툴을 사용할 수도 있습니다.

Csvkit 를 대체 툴로 사용해 보십시오. Csvkit 는 명령줄에서 CSV 데이터를 보다 쉽게 처리하는 데 사용할 수 있는 여러 유틸리티를 제공합니다. 다음의 CSV 파일을 살펴보고 src 열에 tty.example.org 호스트가 포함된 모든 행을 쉽게 찾는 방법을 확인해 보십시오.

```
$ head -n 3 tcp_data.csv
src,srcport,dst,dstport
“tty.example.org ”,“51816 ”,”vex.example.org ”,”443 ”
“vex.example.org ”,”443 ”,”tty.example.org ”,”51816 ”

$ csvgrep -n tcp_data.csv
                1: src
                2: srcport
                3: dst
                4: dstport

$ csvgrep -c 1 -r ‘tty\.example\.org ’ tcp_data.csv | head -n 5
src,srcport,dst,dstport
tty.example.org,51816,vex.example.org,443
tty.example.org,51816,vex.example.org,443
tty.example.org,51427,paz.example.org,5222
tty.example.org,51767,bid.example.org,80
```

Csvkit 는 여러 유틸리티의 호스트를 포함합니다. Csvstat 는 여러 통계를 자동으로 계산하므로 특히 유용합니다. 예를 들어 주요 src 호스트 5 개의 빈도를 다음과 같이 쉽게 계산할 수 있습니다.

```
$ csvstat -c 1 tcp_data.csv
  1. src
  <type 'unicode '>
  Nulls: False
  Unique values: 55
  5 most frequent values:
                tty.example.org:        2866
                lad.example.org:        1242
                bin.example.org:        531
                trw.example.org:        443
                met.example.org:        363
Max length: 15

Row count: 6896
```

Matplotlib, Pandas, IPython 및 기타

(http://www.scipy.org) 는 이러한 툴을 찾을 수 있는 유용한 사이트입니다. Matplotlib, Pandas 및 Ipython 은 특수한 용도로 사용할 수 있는 툴입니다.

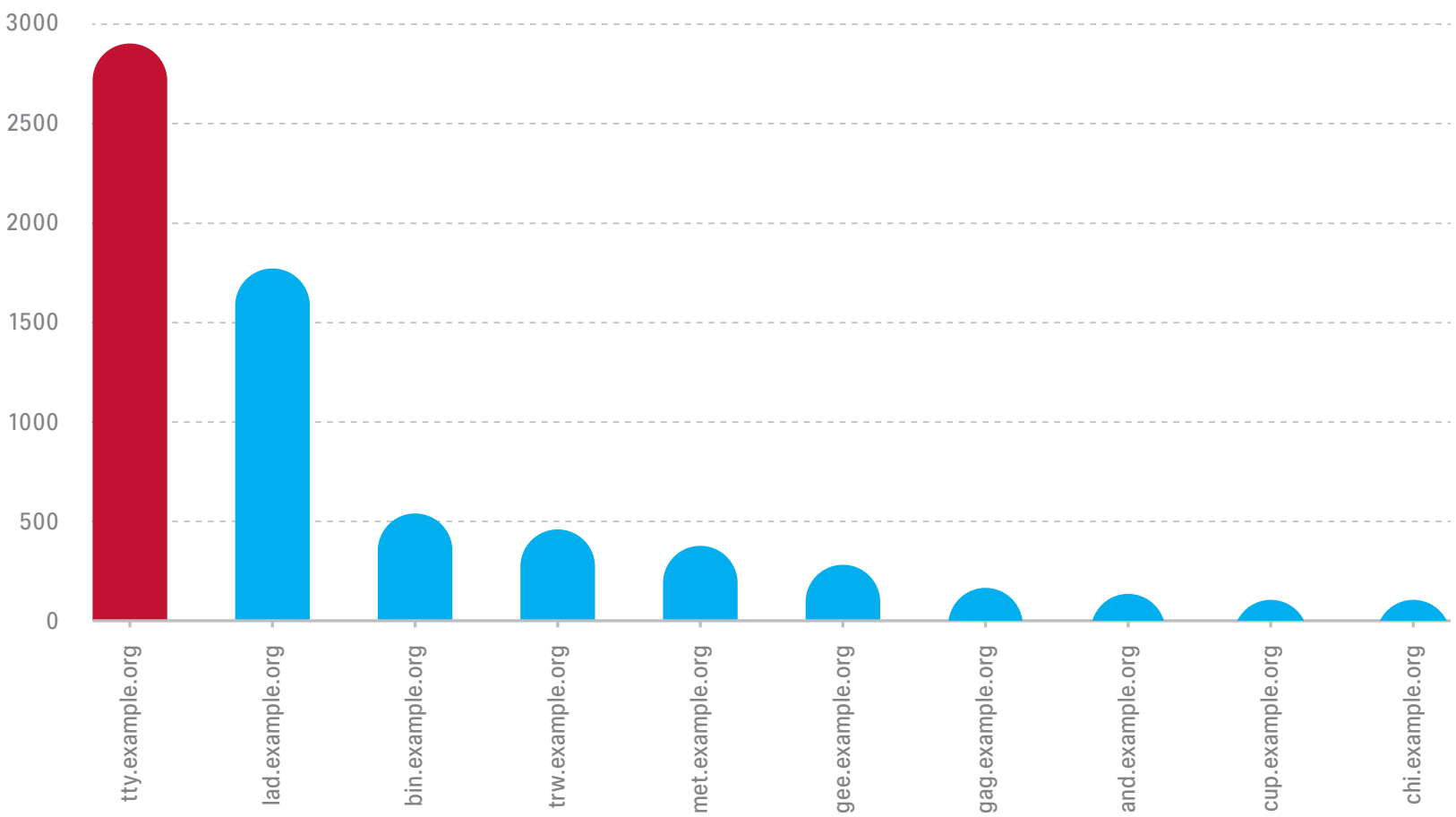
- Matplotlib 는 쉽고 유연한 방식으로 사용할 수 있으며 시각화 기능을 제공합니다.
- Pandas 는 원시 데이터를 조작 및 검사하는 툴을 제공합니다.
- Ipython 은 Python 인터프리터에 대화식 데이터 분석에 유용한 기능을 제공합니다.

다음은 보안 실무자가 이러한 세 가지 툴을 사용해 tcp_data.csv 의 주요 src 호스트를 그래프로 나타내는 방법을 보여줍니다.

```
In [3]: df = read_csv (“/Users/shiva/tmp/data_analysis/tcp_data.csv”)
In [4]: df
Out[4]:
<class ‘pandas.core.frame.DataFrame ’>
Int64Index: 6896 entries, 0 to 6895
Data columns (total 4 columns) :
src 6896 non-null values
srcport 6896 non-null values
dst 6896 non-null values
dstport 6896 non-null values
dtypes: int64 (2), object (2)
In [5]: df[ ‘src ’].value_counts () [0:10]
Out[5]:
tty.example.org 2866
lad.example.org 1242
bin.example.org 531
trw.example.org 443
met.example.org 363
gee.example.org 240
gag.example.org 126
and.example.org 107
cup.example.org 95
chi.example.org 93
dtype: int64
In [6]: df[ ‘src ’].value_counts () [0:10].plot (kind= “bar ”)
Out[6]: <matplotlib.axes.AxesSubplot at 0x8479c30>
```

그림 A2

플롯 () 을 사용해 생성된 차트



Pandas 의 이점은 데이터 탐색 기능에 있습니다. 예를 들어 tty.example.org 가 통신하는 각각의 고유한 dst 와 dstport 의 조합을 위해 연결하는 고유한 srcport 의 수를 다음과 같이 간단하게 찾을 수 있습니다.

```
In [229]: tty_df = df[df.src == “tty.example.org ”]
In [230]: num_ports = lambda x: len (set (x) )
In [231]: pivot_table (tty_df, rows=[ ‘dst ’,‘dstport ’], values= ‘srcport ’, aggfunc=num_ports)
Out[231]:
dst dstport
add.example.org 80 2
ala.example.org 80 3
and.example.org 80 1
auk.example.org 80 2
bid.example.org 80 1
…
```

데이터 분석 시작

위의 페이지에 있는 예들은 지금까지 언급된 툴의 활용 방법 중 극히 일부에 지나지 않습니다. 하지만 보안 실무자들이 의미 있는 데이터 분석을 시작하기 위해 참고하기에는 충분합니다.

CSO 는 보안 실무자들이 데이터 과학자 역할을 수행하도록 해야 합니다. 사용 가능한 데이터를 상세히 분석하면 유용한 정보를 얻을 수 있습니다. 그러면 시간이 지남에 따라 데이터의 어느 부분을 탐색해야 하는지 알 수 있게 됩니다. 일부 조직의 경우 팀에 전담 데이터 과학자를 배치하면 도움이 될 수도 있습니다.

Cisco SIO 정보

Cisco SIO

오늘날 민첩한 분산형 네트워크를 관리 및 보호해야 하는 과제가 점점 커지고 있습니다.

사이버 범죄자들은 소비자 애플리케이션과 장치에 대한 사용자의 신뢰를 지속적으로 악용하여 조직과 직원에 대한 위험을 증가시키고 있습니다. 제품 계층화 및 복수 필터 사용에 의존하는 기존 보안은 요즈음처럼 빠르게 번식하고 전 세계의 목표물을 대상으로 하며 복수 벡터를 사용하여 전파되고 있는 최신 멀웨어를 방어하기에 충분하지 않습니다.

Cisco 는 Cisco SIO (Security Intelligence Operations) 의 실시간 위협 분석 정보를 사용하여 최신 위협보다 한발 앞서 나갑니다. Cisco SIO 는 배포된 Cisco 이메일, 웹, 방화벽 및 IPS (Intrusion Prevention System) 솔루션의 라이브 데이터 피드 75 테라바이트 이상이 매일 분석되고 있는 세계 최대 규모의 클라우드 기반 보안 에코시스템입니다.

Cisco SIO 는 데이터를 분석하고 처리하여 위험을 자동으로 분류하고 200 개 이상의 매개 변수를 사용해 규칙을 생성합니다. 보안 연구원은 또한 네트워크, 애플리케이션 및 장치에 폭넓은 영향을 미칠 가능성이 있는 보안 사건의 정보도 수집 및 제공합니다. 규칙이 배포된 Cisco 보안 장치에 3~5 분마다 동적으로 전송됩니다.

기존의 보안 방식으로는 최근 발생하는 멀웨어에 충분히 대비할 수 없습니다.

Cisco SIO 팀은 또한 위협 저지를 위한 보안 모범 사례 권장 사항과 전술 안내에 대한 자료도 출간합니다. Cisco 는 통합성, 적시성, 포괄성 및 효과성을 갖춘 완전한 보안 솔루션을 제공하여 전 세계 조직에 종합적 보안을 구현하기 위해 최선을 다하고 있습니다. 조직은 Cisco 의 지원으로 위협 및 취약성 연구 시간을 줄이는 대신 보안에 대한 사전 대응적 접근 방식을 취하는 데 더 주력할 수 있습니다.

조기 경보 분석 정보, 위협 및 취약성 분석과 Cisco 의 입증된 완화 솔루션에 대한 자세히 알아보려면 www.cisco.com/go/sio 를 방문하십시오.

미주

1 모두에서 모두로의 진화에 대한 자세한 내용은 *Cisco 2013 연례 보안 보고서* 의 "The Nexus of Devices, Clouds, and Applications" 참조: https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf.

2 Ibid.

3 *No More Chewy Centers: Introducing The Zero Trust Model Of Information Security,* John Kindervag, Forrester, 2012 년 11 월 12 일

4 "Timeline of Edward Snowden ' s Revelations", *Al Jazeera America*: http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html.

5 "NSA collecting phone records of millions of Verizon customers daily", Glenn Greenwald, *The Guardian*, 2013 년 6 월 5 일: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

6 GCHQ: 영국 정보 기관인 Government Communications Headquarters

7 "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say", Barton Gellman 및 Ashkan Soltani, 2013 년 10 월 30 일, *The Washington Post*: http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

8 자세한 내용은 "CSDL (Cisco Secure Development Life cycle)" 참조: http://www.cisco.com/web/about/security/cspo/csdl/index.html.

9 Ibid.

10 Cisco 는 IoE (Internet of Everything) 를 "사람, 프로세스, 데이터 및 사물의 융합을 통해 향후 이루어질 급격한 인터넷 성장의 물결" 이라고 정의함

11 "Massive Spam and Malware Campaign Following the Boston Tragedy", *Cisco 보안 블로그*, 2013 년 4 월 17 일: http://blogs.cisco.com/security/massive-spam-and-malware-campaign-following-the-boston-tragedy/.

12 Ibid.

13 Ibid.

14 Java 웹사이트의 "소개" 페이지: http://www.java.com/en/about/.

15 "모두에서 모두로의 혁신" 에 대한 자세한 내용은 *Cisco 2013 연례 보안 보고서* 참조: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf.

16 "Department of Labor Watering Hole Attack Confirmed to be 0-Day with Possible Advanced Reconnaissance Capabilities," by Craig Williams, *Cisco Security Blog*, May 4, 2013: http://blogs.cisco.com/security/department-of-labor-watering-hole-attack-confirmed-to-be-0-day-with-possible-advanced-reconnaissance-capabilities/.

17 "Watering-Hole Attacks Target Energy Sector",by Emmanuel Tacheau, *Cisco Security Blog*, Sept. 18, 2013 : http://blogs.cisco.com/security/watering-hole-attacks-target-energy-sector/.

18 "Apache DarkLeech Compromises", by Mary Landesman, *Cisco Security Blog*, Apr. 2, 2013: http://blogs.cisco.com/security/apache-DarkLeech-compromises/.

19 "Ongoing malware attack targeting Apache hijacks 20,000 sites", by Dan Goodin, *Ars Technica*, Apr. 2, 2013: http://arstechnica.com/security/2013/04/exclusive-ongoing-malware-attack-targeting-apache-hijacks-20000-sites/.

20 "Linux/CDorked FAQ", Mary Landesman 의 *Cisco Security Blog*, May 1, 2013: http://blogs.cisco.com/security/linuxcdorked-faqs/.

21 "DarkLeech Apache Attacks Intensify", by Matthew J. Schwartz, *InformationWeek,* Apr. 30, 2013: http://www.informationweek.com/security/attacks/DarkLeech-apache-attacks-intensify/240153922.

22 타이포스쿼팅은 많이 이용되는 도메일 이름과 문자 하나만 다른 도메인 이름을 등록하는 방법입니다.

23 "Thanks to IoE, the next decade looks positively ‘nutty", by Dave Evans, *Cisco Platform Blog*, Feb. 12, 2013: http://blogs.cisco.com/news/thanks-to-ioe-the-next-decade-looks-positively-nutty/.

[24] 비트스쿼팅 방지 전략에 대한 자세한 내용은 2013 년 Cisco 백서 *Examining the Bitsquatting Attack Surface* 참조: http://blogs.cisco.com/wp-content/uploads/Schultz-Examining_the_Bitsquatting_Attack_Surface-whitepaper.pdf.

[25] "WordPress Sites in the World" and "A Look at Activity Across WordPress.com", WordPress.com: http://en.wordpress.com/stats/.

[26] "Important Security Update: Reset Your Drupal.org Password" Drupal.org, May 29, 2013: https://drupal.org/news/130529SecurityUpdate.

[27] Operation Ababil 공격의 패턴 및 심각성에 대한 상세한 보고서는 "Cisco Event Response: Distributed Denial of Service Attacks on Financial Institutions" 에서 참조: http://www.cisco.com/web/about/security/intelligence/ERP-financial-DDoS.html.

[28] "DDoS Attack on Bank Hid $900,000 Cyberheist", by Brian Kreb, *KrebsonSecurity blog*, Feb. 19, 2013: http://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/.

[29] "Chinese Internet Hit by Attack Over Weekend", by Paul Mozer, *China Real Time Report*, WSJ.com, Aug. 26, 2013: http://blogs.wsj.com/chinarealtime/2013/08/26/chinese-internet-hit-by-attack-over-weekend/.

[30] 출처: Wikipedia: "Ingress Filtering": http://en.wikipedia.org/wiki/Ingress_filtering.

[31] "Understanding Unicast Reverse Path Forwarding", Cisco Website: http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html.

[32] "Your Hard Drive Will Self-Destruct at 2 p.m.: Inside the South Korean Cyberattack", by Sean Gallagher, *Ars Technica*, Mar. 20, 2013: http://arstechnica.com/security/2013/03/your-hard-drive-will-self-destruct-at-2pm-inside-the-south-korean-cyber-attack/.

[33] "Thoughts on DarkSeoul: Data Sharing and Targeted Attackers", by Seth Hanford, *Cisco Security Blog*, Mar. 27, 2013: http://blogs.cisco.com/tag/darkseoul/.

[34] Ibid.

[35] "Cyber Gang Seeks Botmasters to Wage Massive Wave of Trojan Attacks Against U.S. Banks," by Mor Ahuvia, RSA, Oct. 4, 2012: https://blogs.rsa.com/cyber-gang-seeks-botmasters-to-wage-massive-wave-of-trojan-attacks-against-u-s-banks/.

[36] "DDoS Attack on Bank Hid $900,000 Cyberheist", by Brian Krebs, *KrebsonSecurity Blog*, Feb. 19, 2013: http://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/.

[37] "Cisco projects data center-cloud traffic to triple by 2017", ZDNet, Oct. 15, 2013: http://www.zdnet.com/cisco-projects-data-center-cloud-traffic-to-triple-by-2017-7000021985/.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International
BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.