Cisco
2017 연례 사이버 보안 보고서

cisco

목차

Executive Summary

공격 범위가 증가함에 따라 방어자는 가장 중요한 목표, 즉 공격자가 공격을 수행할 수 있는 영역을 감소하는 데 주력해야 합니다.

공격자들은 그 어느 때보다 많은 툴을 활용하고 있으며 공격의 효과를 최대화하기 위해 각 툴을 사용해야 하는 시기를 잘 알고 있습니다. 모바일 엔드포인트 및 온라인 트래픽의 급증 현상 역시 공격자에게 유리하게 하는 환경입니다. 즉, 공격자들이 공격을 수행할 수 있는 영역과 선택할 수 있는 표적 및 접근 방식이 늘어나고 있습니다.

방어자는 '위협 환경의 확대'라는 당면 과제를 해결하기 위해 폭넓은 전략을 사용해야 합니다. 방어자는 개별적으로 동작하여 정보와 보호 기능을 제공하는 업계 최고의 솔루션을 구매해야 하며, 인재 공급 및 예산이 부족한 시장에서 경쟁을 통해 적절한 인력을 확보해야 합니다.

모든 공격을 중단하기는 어려울 수 있습니다. 그러나 공격자가 공격할 수 있는 영역을 제약하고, 자산 침해 능력을 제한함으로써 위험 및 위협의 영향을 최소화할 수 있습니다. 이를 위해 취할 수 있는 조치 중 하나는 보안 툴 컬렉션을 상호 연결된 통합 보안 아키텍처로 간소화하는 것입니다.

자동화된 아키텍처에서 서로 연동되는 통합 보안 툴을 활용하면 위협 탐지 및 차단 프로세스를 간소화할 수 있습니다. 이는 문제 해결 시간 확보에 도움을 줍니다. 많은 조직이 6개 이상의 벤더가 제공하는 6가지 이상의 솔루션을 사용합니다(**53페이지**). 이러한 조직은 특정일에 수신하는 보안 알림 중 절반만을 확인하는데 그칩니다.

Cisco 2017 연례 사이버 보안 보고서에는 Cisco Security Research의 확인 결과, 인사이트 및 관점이 포함되어 있습니다. 보고서는 공격 준비 시간을 보다 많이 확보하고자 하는 공격자와, 이러한 공격자들의 공격 시도 기회를 차단하려는 방어자 간의 치열한 공방에 대해 중점적으로 설명합니다. 그리고 Cisco 위협 연구진과 기타 전문가들이 수집한 데이터를 살펴봅니다. Cisco 보고서에 포함된 확인 결과 및 인사이트는 빠르게 진화하는 오늘날의 정교한 위협에 조직이 효율적으로 대응하는 데 도움을 주고자 합니다.

이 보고서는 다음과 같은 섹션으로 나뉩니다.

공격자 행동

이 섹션에서는 공격자 측이 취약한 네트워크를 정찰하고 악성코드를 전송하는 방식을 살펴보고 이메일, 서드파티 클라우드 애플리케이션 및 애드웨어와 같은 툴을 공격 수단으로 활용하는 방법을 설명합니다. 이어 사이버 범죄자들이 이러한 공격 수단을 설치하거나 사용하는 방법 역시 설명합니다. 또한, 이 섹션에서는 공격자들이 공격 전술을 최신 상태로 유지하고 탐지를 피하는 방법을 보여주는 Cisco의 "TTE(Time to Evolve, 진화 소요 시간)" 연구에 대해서도 소개합니다. 한편 평균 TTD(Time to Detection, 탐지 소요 시간) 중앙값을 단축하기 위한 Cisco의 노력과 관련된 업데이트 정보, 다양한 업계 및 지역의 악성코드 위험에 대한 Cisco의 최신 연구 결과도 함께 제공합니다.

방어자 행동

이 섹션에서는 취약점과 관련된 업데이트 정보를 제공합니다. 미들웨어 라이브러리의 취약점, 즉 공격자들이 다양한 애플리케이션에 동일한 툴을 사용할 수 있는 점이 새롭게 부각되는 현실입니다. 공격자는 이러한 취약점을 악용함으로써 사용자의 자산을 침해하는 데 필요한 시간과 비용을 줄일 수 있습니다. 또한, 패치 트렌드에 대한 Cisco의 연구 결과도 공유합니다. Cisco는 일반적인 웹 브라우저 및 솔루션의 안전한 버전 도입을 장려하기 위해 사용자에게 정기적으로 업데이트를 제공함으로써 얻을 수 있는 이점에 주목합니다.

Cisco 2017 보안 기능 벤치마크 조사

이 섹션에서는 보안 전문가들이 자신의 조직 내 보안 상태를 어떻게 인식하는가에 초점을 맞춘, Cisco의 3차 보안 기능 벤치마크 조사의 결과를 다룹니다. 올해 보안 전문가들은 현재 보유하고 있는 툴에는 확신을 보였지만, 이러한 리소스가 공격자들의 공격 가능 영역을 줄이는 데 도움이 되는지는 확신하지 못하고 있습니다. 이 조사에서는 공개적 보안 침해가 기회, 매출 및 고객에 대해 상당한 영향을 주고 있다는 점도 설명합니다. **조직의 보안 상태와 관련된 보다 상세한 분석 정보를 확인하려면 49페이지로 이동하십시오**.

업계 동향

이 섹션에서는 가치 사슬(value chain) 보안 유지의 중요성에 대해 설명합니다. 이와 관련하여 정부가 벤더 제품의 취약점 및 제로 데이 익스플로잇에 대한 정보를 수집할 때 적용되는 피해 정도를 살펴봅니다. 또한, 고속 환경에서 데이터를 보호하기 위한 솔루션으로 신속한 암호화 기능을 사용하는 방법에 대해서도 설명합니다. 마지막으로, 글로벌 인터넷 트래픽 및 잠재적 공격 범위가 증가함에 따라 조직에서 해결해야 하는 보안 관련 당면 과제에 관해 간략하게 설명합니다.

결론

결론에서는 방어자들이 공격 체인 전반에 걸쳐 일반적으로 발생하는 보안 관련 과제를 보다 효율적으로 해결하고 공격자들의 공격 가능 영역을 줄일 수 있도록 보안 방식을 조정하도록 제안합니다. 또한, 이 섹션에서는 간소화된 통합형 보안 구축 방식과 관련된 구체적인 지침을 제공합니다. 이러한 방식을 도입하면 경영진의 리더십, 정책, 프로토콜 및 툴을 서로 연결하여 위협을 방지하거나 탐지 및 차단할 수 있습니다.

주요 조사 결과

- 주로 사용되던 세 가지 익스플로잇 킷, 즉 Angler, Nuclear 및 Neutrino가 2016년 들어 더 이상 공격에 사용되지 않으면서 소규모 및 신규 공격자들이 등장했습니다.
- Cisco 2017 보안 기능 벤치마크 조사에 따르면 대부분의 기업 환경은 6개의 보안 벤더에서 제공하는 6가지 이상의 보안 제품을 사용하고 있습니다. 보안 전문가 중 55%는 6개 이상의 벤더를, 45%는 1~5개 벤더를, 그리고 65%는 6개 이상의 제품을 사용하고 있습니다.
- 해당 조사에 따르면 고급 보안 제품 및 솔루션 도입에 가장 큰 제약이 되는 요소는 예산(응답자의 35%가 언급함), 제품 호환성(28%), 인증(25%) 및 인재(25%)인 것으로 나타났습니다.
- 이와 더불어 조직은 다양한 제약으로 인해 특정일에 수신하는 보안 알림 중 56%만을 확인할 수 있습니다. 확인한 알림 중 절반(28%)은 정상 알림으로 확인되며 정상 알림 중 치료되는 알림은 절반에도 미치지 못하는 46%에 불과합니다. 한편, 보안 운영 관리자 중 44%는 매일 5,000건이 넘는 보안 알림을 확인합니다.
- 2016년에 엔터프라이즈 환경에 도입한 서드파티 클라우드 애플리케이션 중 27%는 보안 위험성이 높은 것으로 나타났습니다. 개방형 인증(OAuth) 연결에서는 사용자가 액세스 권한을 부여하고 나면 기업 클라우드 및 SaaS(Software-as-a-service) 플랫폼과 자유롭게 통신할 수 있습니다.
- Cisco가 다양한 업종에 걸쳐 130개 조직을 대상으로 확인한 결과에 따르면, 이러한 회사 중 75%가 애드웨어에 감염된 적이 있는 것으로 나타났습니다. 공격자들은 이와 같이 감염된 애플리케이션을 통해 다른 악성코드 공격을 더욱 쉽게 수행할 수 있습니다.
- 멀버타이징 공격을 감행하는 공격자들이 브로커("게이트"라고도 함)를 이용하는 빈도가 증가하고 있습니다. 즉, 브로커를 통해 이동 속도를 높이고 공격할 수 있는 영역을 유지하고 탐지를 피할 수 있습니다. 공격자들은 이러한 중간 링크를 활용하여 초기 리디렉션을 변경하지 않고도 악성 서버 사이를 빠르게 전환할 수 있습니다.
- 스팸은 총 이메일량의 과반수(65%)를 차지하며, Cisco의 확인 결과에 따르면 갈수록 성장하는 대규모 스팸 전송 봇넷으로 인해 전 세계의 스팸량은 계속해서 증가하고 있는 것으로 나타났습니다. Cisco 위협 연구 결과에 따르면 2016년에 확인된 전 세계 스팸 중 약 8~10%는 악성으로 분류되는 것이었습니다. 또한, 악성 첨부 파일이 포함된 스팸의 비율도 증가하고 있으며 공격자들은 매우 다양한 파일 형식을 실험하고 있는 것으로 확인되었습니다.
- 보안 기능 벤치마크 조사에 따르면, 아직 보안 침해가 발생하지 않은 조직은 자사 네트워크가 안전하다고 확신하고 있습니다. 하지만 설문조사 대상 보안 전문가 중 49%가 조직에서 보안 침해가 발생한 후 공개 조사를 관리해야 했다고 응답한 점을 고려하면 이러한 확신은 잘못되었을 가능성이 높습니다.

- 또한, Cisco 2017 보안 기능 벤치마크 조사에서는 공격을 당했던 조직의 약 25%가 비즈니스 기회를 상실한 것으로 확인되었습니다. 조직 10곳 중 4곳이 심각한 손실을 입었다고 답변했습니다. 조직 5곳 중 1곳은 공격으로 인해 고객을 잃었으며 거의 30%에 달하는 조직에서는 매출까지 감소했습니다.
- 위와 관련해, 보안 침해 발생 시 가장 크게 영향 받는 부분은 운영 및 재무이며(각각 36%와 30%) 그 다음으로는 브랜드 평판과 고객 유지(26%)인 것으로 나타났습니다.
- 보안 침해로 인한 네트워크 중단은 장기적인 영향을 주는 경우가 많습니다. 벤치마크 조사에 따르면 중단의 45%는 1~8시간 동안, 15%는 9~16시간, 그리고 11%는 17~24시간 동안 계속되었습니다. 이러한 중단 가운데 중 41%(55페이지 참조)는 시스템의 11~30%에 영향을 주었습니다.
- 플랫폼이나 애플리케이션 간의 브리지 또는 커넥터 역할인 미들웨어어의 취약점이 더욱 명확하게 나타나고 있으며, 이로 인해 미들웨어가 위협 벡터로 활용되는 문제가 발생하고 있습니다. 대부분의 기업이 미들웨어를 사용하므로 모든 산업에 위협을 줄 수 있습니다. Cisco® 프로젝트를 진행하는 과정에서 수행된 위협 연구에서는 조사 대상이었던 신규 취약점의 대다수가 미들웨어 사용으로 인한 것으로 확인되었습니다.
- 패치 및 업그레이드를 설치하는 정기 소프트웨어 업데이트는 사용자 행위에 영향을 줄 수 있습니다. 연구 결과에 따르면, 예측 가능한 정기 업데이트 일정이 제공되면 사용자가 소프트웨어를 더 빠르게 업그레이드할 수 있으므로 공격자들이 취약점을 이용할 수 있는 시간을 줄일 수 있습니다.
- 2017 보안 기능 벤치마크 조사에서는 대부분의 조직이 보안 기능 중 20% 이상을 서드파티 벤더에 의존하고 있으며, 이러한 리소스를 많이 사용할수록 향후 해당 리소스 활용 가능성이 높은 것으로 나타났습니다.

서론

서론

공격자들은 리소스에 액세스할 권한을 얻고 제약 없이 공격 시간을 벌기 위해 방대하고 다양한 기술적 포트폴리오를 보유 중입니다. 공격자들의 전략은 공격을 위한 모든 기본 사항을 포괄적으로 다루며, 다음과 같은 내용을 포함합니다.

- **패치 및 업데이트 지연 상황 이용**
- **사회 공학적으로 고안된 함정으로 사용자 유인**
- **광고 등의 적법해 보이는 온라인 콘텐츠에 악성코드 주입**

공격자들은 미들웨어 취약점 공격, 악성 스팸 전송 등의 여러 가지 기타 기능을 사용하며 목표를 달성하고 나면 신속하게 공격을 자동 종료할 수 있습니다.

공격자들은 위협 방식을 향상시키기 위해 끊임없이 노력하며, 공격 속도를 높이고 있습니다. 또한 공격할 수 있는 영역을 확장하기 위한 방식도 모색하고 있습니다. 갈수록 빨라지는 모바일 속도 및 온라인 디바이스의 확산으로 발생하는 인터넷 트래픽의 폭증으로 인해 공격자들은 공격 범위를 수월하게 확장할 수 있습니다. 이는 기업이 직면하는 위험성을 높이는 요인입니다. Cisco 2017 보안 기능 벤치마크 조사에서는 공격을 당했던 조직의 1/3 이상이 20% 이상의 매출 감소를 경험한 것으로 확인되었습니다. 응답자의 49%는 보안 침해로 인해 기업에서 공개 조사를 받았다고 답했습니다.

큰 피해를 입고도 안정적인 상태를 유지할 수 있는 기업은 많지 않을 것입니다. 방어자들은 공격자의 공격 가능 영역을 줄이는 데 리소스를 집중 투입해야 합니다. 그러면 공격자가 중요한 기업 리소스에 액세스하여 탐지할 수 없고 공격 활동을 수행하기 매우 어려워집니다.

이 목표를 달성하려면 자동화가 필수적입니다. 자동화를 진행하면 네트워크 환경의 전반적인 활동을 파악할 수 있으므로 한정된 리소스를 위협 조사 및 해결 과정에 집중 투입할 수 있습니다. 또한, 보안 운영을 간소화하면 공격자가 아무런 제약없이 공격할 수 있는 영역을 더욱 효율적으로 없앨 수 있습니다.(53페이지).

이처럼 여러 기술이 복잡하게 활용되면 보안 성능이 떨어지는 게 당연합니다. 물론 보안 관련 인재를 추가로 채용하면 됩니다. 전문가가 많을수록 조직의 기술 관리 능력이 높아지기 때문입니다. 그러나 보안 관련 인재가 부족하고 보안 예산도 제한되어 있으므로 인재를 충분히 고용하기는 어렵습니다. 이에 대부분의 조직은 기존의 인재를 적절하게 활용해야 합니다. 조직에서는 아웃소싱을 통해 인재를 확보하여 예산을 절약하는 동시에 보안 팀을 강화해야 합니다.

이 보고서의 뒷부분에서 설명하는 것처럼, 이러한 당면 과제를 근본적으로 해결하려면 인력, 프로세스 및 기술을 통합된 방식으로 조직화해야 합니다. 그리고 보안을 조직적으로 관리하려면 기업에서 보호해야 하는 대상과 보호하기 위해 사용해야 하는 수단을 명확하게 파악해야 합니다.

Cisco 2017 연례 사이버 보안 보고서는 조직과 사용자가 공격을 방어하는 데 사용할 수 있는 보안 업계의 최신 기술 관련 정보를 제공하며, 공격자들이 이러한 방어 기능을 무력화하는 데 사용하는 기술과 전략에 대해서도 설명합니다. 또한 기업의 보안 상태와 공격 방어 준비 상태에 대한 인식을 조사한 Cisco 2017 보안 기능 벤치마크 조사의 주요 분석 결과를 중점적으로 소개합니다.

공격 범위의 확장

공격 범위의 확장

모바일 디바이스. 퍼블릭 클라우드. 클라우드 인프라. 사용자 행위. Cisco의 3차 연례 보안 기능 벤치마크 조사에 참여한 보안 전문가들은 조직의 사이버 공격 노출 위험을 고려할 때 이러한 요소를 모두 주요 문제 발생 원인으로 언급했습니다(**그림 1**). 우선, 모바일 디바이스가 확산됨에 따라 보호해야 하는 엔드포인트의 수가 증가합니다. 클라우드로 인해 보안 경계 역시 확대되고 있습니다. 또한, 사용자는 보안 사슬에서 항상 약점으로 간주되며 앞으로도 이러한 추세는 지속될 전망입니다.

기업에서 디지털화를 도입하고 만물 인터넷(IoE)[1]이 구체화됨에 따라 방어자들이 고려해야 할 요소도 증가하고 있습니다. 공격 범위는 계속 확장될 것이므로 공격자들이 공격할 수 있는 영역도 늘어날 것입니다.

Cisco® VNI(Visual Networking Index)는 10년 이상 글로벌 IP 트래픽의 예측 정보를 제공해 왔으며 네트워크 확장을 용이하게 하는 동적 요인을 분석했습니다. 최근 공개된 보고서 *제타바이트의 시대 - 트렌드 및 분석*[2]에서는 다음과 같은 통계를 확인할 수 있습니다.

- **2016년 말에는 연간 글로벌 IP 트래픽이 제타바이트(ZB)의 경계를 넘어서고 2020년에는 연간 2.3ZB에 이를 것으로 전망됩니다. 1제타바이트는 1,000엑사바이트(EB) 또는 10억 테라바이트(TB)에 해당합니다. 즉, 향후 5년간 글로벌 IP 트래픽은 3배 증가할 것으로 예상됩니다.**
- **2020년에는 무선 및 모바일 디바이스의 트래픽이 전체 IP 트래픽의 2/3(66%)를 차지할 것으로 전망됩니다. 유선 디바이스는 34%에 불과할 것으로 보입니다.**
- **2015~2020년의 평균 광대역 속도는 2배 가까이 빨라질 것으로 보입니다.**
- **2020년에는 전 세계의 모든 소비자 인터넷 트래픽 중 82%(2015년의 경우 70%)가 IP 비디오 트래픽이 될 것으로 예상됩니다.**

그림 1 보안 전문가가 생각하는 사이버 공격 관련 주요 문제 발생 원인

모바일 디바이스	퍼블릭 클라우드의 데이터	클라우드 인프라	사용자 행위(예: 이메일이나 웹사이트의 악성 링크 클릭)
58%	57%	57%	57%

해당 범주의 보안 유지가 매우 또는 가장 어렵다고 답변한 보안 전문가의 비율

출처: Cisco 2017 보안 기능 벤치마크 조사

2017년 그래픽 다운로드: www.cisco.com/go/acr2017graphics

[1] "Internet of Everything FAQ," Cisco: **http://ioeassessment.cisco.com/learn/ioe-faq**.
[2] *The Zettabyte Era—Trends and Analysis*, Cisco VNI, 2016: **http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html**.

또한, Cisco *VNI™ Forecast and Methodology(2015~2020년)* 백서[3]의 예측에 따르면 2020년의 글로벌 인터넷 트래픽량은 2005년의 95배에 달할 것으로 전망됩니다.

사이버 범죄자들은 당연히 이러한 사실에 주목하고 있습니다. 트렌드에 민첩하게 대응하려는 이른바 지하 경제의 공격자도 이미 확인되고 있습니다. 이러한 공격자들은 확장된 공격 범위 전반에 막대한 피해를 입힐 수 있는 고도의 특화 공격 방식을 고안 중입니다. 한편 보안 팀은 항상 많은 알림을 확인하고 해결하기에도 바쁜 상태입니다. 따라서 네트워크 환경에서 여러 일련의 보안 제품을 사용해야 하는데, 이로 인해 환경은 갈수록 복잡해지며 조직의 위협에 대한 민감성도 높아질 수 있습니다.

조직은 다음과 같은 조치를 취해야 합니다.

- **보안 기술 통합**
- **네트워크 운영 간소화**
- **자동화 활용도 제고**

이러한 방식을 통해 운영 비용과 보안 인력의 부담을 줄이고, 더욱 만족스러운 결과를 얻을 수 있습니다. 그러나 무엇보다도 중요한 것은, 이러한 방식 덕분에 공격자들의 공격 영역을 없애는 데에 더 많은 시간을 투자할 수 있다는 점입니다.

[3] *Cisco VNI Forecast and Methodology, 2015–2020*, Cisco VNI, 2016: **http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html**.

공격자 행동

공격자 행동

정찰 | 공격 수단 구축 | 전송 | 설치

공격자가 표적을 연구, 식별 및 선택

웹 공격 방법: 공격자의 캠페인 준비 작업을 지원하는 "단발성" 위협

정찰은 사이버 공격 실행을 위한 기본 단계입니다. 이 단계에서 공격자는 사용자의 컴퓨터에 액세스하고 궁극적으로는 조직 침투에 활용할 수 있는 취약한 인터넷 인프라 또는 네트워크를 찾아냅니다.

2016년의 웹 공격 방법으로는 의심스러운 Windows 바이너리 및 PUA(Potentially Unwanted Application, 사용자 동의 없이 설치된 애플리케이션)가 타 항목과 큰 차이로 1, 2위를 차지했습니다(**그림 2 참조**). 의심스러운 Windows 바이너리는 스파이웨어 및 애드웨어와 같은 위협을 유발합니다. PUA의 예로는 악성 브라우저 확장 등이 있습니다.

설문조사 스캠을 동반한 가짜 서비스 및 미디어 콘텐츠를 포함하는 Facebook 스캠이 3위를 차지했습니다. Cisco가 가장 흔히 관찰되는 악성코드를 대상으로 진행하는 연간/중기 위협 목록에서 Facebook 스캠이 지속적으로 상위에 오르는 현상은 사이버 공격에서 소셜 엔지니어링의 근본적인 역할을 극명하게 보여 줍니다. 현재 Facebook의 월별 실제 사용자 수는 전 세계적으로 18억 명에 달합니다.[4] 따라서 사이버 범죄자들과 기타 공격자들이 공격 대상을 찾을 수 있는 최적의 수단이라 할 수 있습니다. 이러한 상황을 감안하여 최근 가짜 뉴스와 정보를 삭제하는 단계를 진행하고 있다고 Facebook이 발표한 것은 긍정적인 발전입니다. 평론가들에 따르면, 이러한 콘텐츠는 2016년의 미국 대선에서도 투표자들에게 영향을 주었을 가능성이 있다고 합니다.[5]

그림 2 가장 흔히 볼 수 있는 악성코드

출처: Cisco Security Research

[4] Facebook stats, September 2016: http://newsroom.fb.com/company-info/.

[5] "Zuckerberg Vows to Weed Out Facebook 'Fake News,'" by Jessica Guynn and Kevin McCoy, *USA Today*, November 14, 2016: http://www.usatoday.com/story/tech/2016/11/13/zuckerberg-vows-weed-out-facebook-fake-news/93770512/.

브라우저 리디렉션 악성코드도 2016년 가장 많이 발견된 상위 5개 악성코드 유형 중 하나입니다. *Cisco 2016 중기 사이버 보안 보고서*[6]에서 설명하는 것처럼, 브라우저가 감염되면 사용자는 악성 광고(멀버타이징)에 노출될 수 있습니다. 공격자들은 이러한 광고를 이용해 랜섬웨어 및 기타 악성코드 공격을 시작합니다. Cisco 위협 연구진은 애드 인젝터(ad injector), 브라우저 설정 하이재커, 유틸리티, 다운로더 등의 악성 애드웨어와 관련된 문제가 갈수록 심각하다고 경고하고 있습니다. 실제로 애드웨어 문제와 관련해 최근 조사한 회사 중 75%에서 애드웨어 감염이 확인되었습니다. (이 항목에 대한 자세한 내용은 "조사 결과: 전체 조직 중 75%가 애드웨어 감염 경험", **23페이지** 참조)

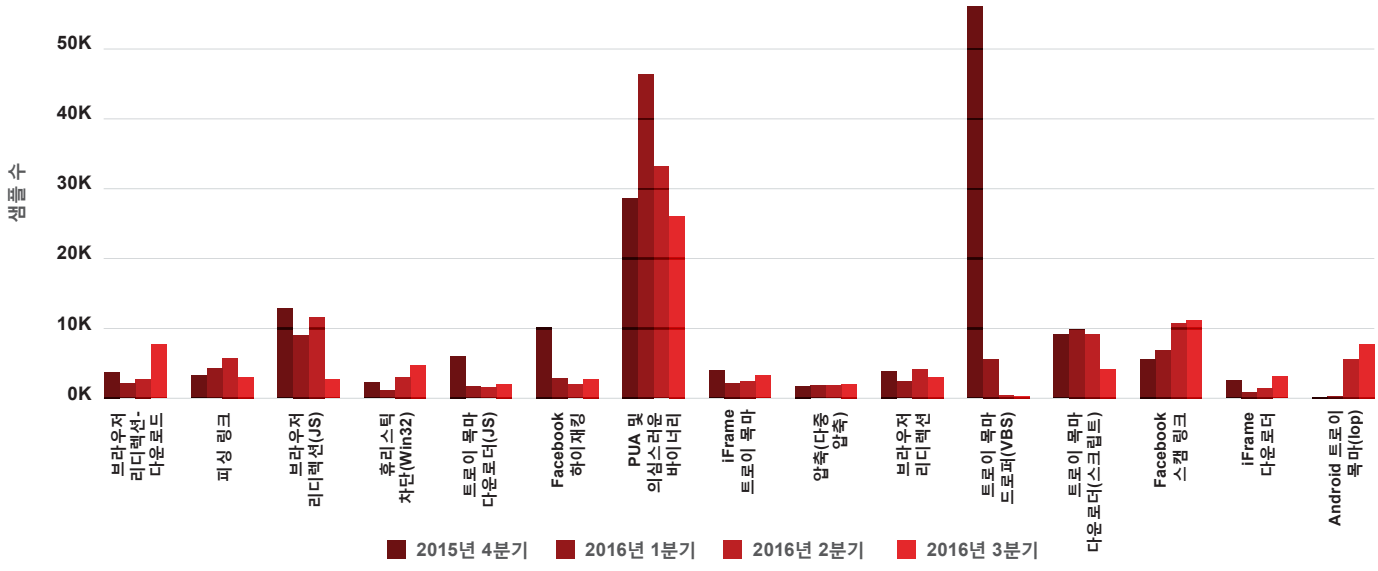
브라우저 JavaScript 악용 악성코드 및 브라우저 iFrame 악용 악성코드와 같이 **그림 3**의 기타 악성코드 유형 역시 브라우저를 쉽게 감염시킬 수 있도록 설계되어 있습니다. 트로이 목마(드로퍼 및 다운로더) 또한 가장 빈번하게 관찰되는 상위 5개 악성코드 유형에 포함됩니다. 즉, 트로이 목마는 여전히 사용자의 컴퓨터 및 조직 네트워크에 대한 초기 액세스 권한을 얻는 데 널리 사용되는 툴이라고 할 수 있습니다.

그 외에 주목해야 할 또 다른 트렌드로는, Android 플랫폼 사용자를 대상으로 하는 악성코드의 사용률이 지속적으로 높게 나타났다는 점입니다. 지난 2년 동안 단발성 위협 목록에서 Android 트로이 목마의 순위는 꾸준히 높아졌습니다. Android 트로이 목마는 2016년에 가장 흔히 확인된 상위 10개 악성코드 유형에도 포함되었습니다. **그림 2**(이전 페이지 참조) 끝자락의 Loki 악성코드는 복제가 가능해 특히 문제가 됩니다.

그림 3에는 Cisco 위협 연구에서 2015년 말부터 관찰된 악성코드의 트렌드입니다. 이를 통해 공격자들의 정찰 방식이 명확하게 변화한 것을 확인할 수 있습니다. 즉, 취약한 브라우저와 플러그인을 구체적으로 찾아내는 위협이 갈수록 잦아지고 있습니다. 이러한 방식의 변화는 공격자들이 멀버타이징을 이용하는 빈도가 계속해서 높아짐을 나타냅니다. 기존의 웹 공격 벡터를 통해서는 많은 사용자를 공격하기가 갈수록 어려워지기 때문입니다. (관련 설명은 다음 섹션인 "웹 공격 벡터: Flash 사용 빈도가 감소하고 있지만 사용자가 경계 상태를 유지해야 하는 이유", **15페이지** 참조)

이러한 상황을 고려할 때 개별 사용자, 보안 전문가 및 기업은 브라우저의 보안을 유지해야 하며, 불필요한 브라우저 플러그인을 비활성화하거나 제거해야 합니다. 해당 조치만으로도 악성코드 감염을 방지하는 데 큰 도움이 됩니다. 간단한 단계를 수행하면 일반적인 웹 기반 위협에 대한 노출을 상당히 줄일 수 있으며, 공격자가 공격 체인의 다음 단계를 수행할 공격 영역을 찾지 못하도록 방지할 수 있습니다.

그림 3 가장 흔히 관찰된 악성코드(2015년 4분기~2016년 3분기)



출처: Cisco Security Research

[6] *Cisco 2016 중기 사이버 보안 보고서*: **http://www.cisco.com/c/m/ko_kr/offers/sc04/2016-midyear-cybersecurity-report/index.html**

정찰 | **공격 수단 구축** | 전송 | 설치

공격자가 전송 가능한 페이로드에 원격 액세스 악성코드를 익스플로잇과 결합

웹 공격 벡터: Flash 사용 빈도가 감소하고 있지만 사용자가 경계 상태를 유지해야 하는 이유

Adobe Flash는 시스템을 공격하고 감염시키려는 공격자가 오랫동안 즐겨 이용한 웹 공격 벡터입니다. 하지만 웹 상의 Adobe Flash 콘텐츠가 감소하고 Flash의 취약점에 대한 인식이 높아짐에 따라, 사이버 범죄자들이 이전과 같은 규모로 사용자를 공격하기 어려워지고 있습니다.

Adobe 역시 Flash 플랫폼의 전체 개발과 지원은 지양하고 있으며, 개발자들에게 HTML5 등의 최신 표준 도입을 장려하고 있습니다.[7] 널리 사용되는 웹 브라우저 제공자 역시 Flash 사용을 최대한 제한하고 있습니다. 예를 들어 Google은 2016년에 Chrome 브라우저에서 Adobe Flash 지원을 중단할 것임을 발표했습니다.[8] Firefox는 기존 Flash 콘텐츠를 지원하기는 하지만, "사용자 환경에 반드시 필요하지 않은 특정 Flash 콘텐츠"는 차단합니다.[9]

이처럼 Flash 사용 범위는 감소하고 있지만, 익스플로잇 킷 개발자들은 여전히 Flash를 공격 벡터로 사용하도록 지원하고 있습니다. Angler 익스플로잇 킷을 이용하는 공격자들은 Flash 취약점을 표적으로 삼아 사용자에게 피해를 입혀 왔습니다. Nuclear 익스플로잇 킷 역시 이와 유사하게 Flash를 집중적으로 공격했습니다. Neutrino는 Flash 파일을 사용하여 익스플로잇을 전송했습니다. 하지만 이러한 추세가 바뀔 수도 있다는 징후가 나타나고 있습니다. 주로 사용되던 세 가지 익스플로잇 킷, 즉 Angler, Nuclear 및 Neutrino가 2016년 들어 더 이상 공격에 사용되지 않게 되었으며, Cisco의 위협 연구 결과에서도 Flash 관련 인터넷 트래픽이 크게 감소한 것으로 확인되었습니다. ("주요 익스플로잇 킷의 소멸로 인한 소규모 및 신규 공격자들의 공격 기회 증가", **20페이지** 참조).

그럼에도 불구하고 사용자는 Flash 사용 시 계속해서 주의해야 하며, 업무상 필요한 경우가 아니면 Flash를 제거해야 합니다. Flash를 사용해야 하는 경우에는 업데이트를 설치하여 최신 상태로 유지해야 합니다. 자동 패치 기능을 제공하는 웹 브라우저를 사용하면 도움이 될 수 있습니다. **13페이지**의 "웹 공격 방법: .공격자의 공격 준비 작업을 지원하는 '단발성' 위협"에 나와 있는 것처럼, 안전한 브라우저를 사용하고 불필요한 브라우저 플러그인을 비활성화하거나 제거하면 웹 기반 위협에 대한 노출을 크게 줄일 수 있습니다.

Java, PDF 및 Silverlight

2016년에는 Java 및 PDF 인터넷 트래픽이 모두 큰 폭으로 감소했습니다. Silverlight 트래픽은 이미 위협 연구에서 정기적으로 추적하지 않아도 될 수준으로 줄어들었습니다.

주요 공격 벡터였던 Java는 최근 수년간 보안 상태가 크게 개선되었습니다. Oracle이 2016년 초에 Java 브라우저 플러그인을 없애기로 결정하면서 Java가 웹 공격 벡터로 사용되는 빈도 역시 낮아졌습니다. PDF 공격 또한 갈수록 줄어들고 있습니다. 이에 Java 및 PDF 공격은 탐지하기가 더 쉬우며, 따라서 대다수의 공격자들은 이제 해당 전략을 이전처럼 즐겨 사용하지 않습니다.

그러나 Flash와 마찬가지로 사이버 범죄자들은 여전히 Java, PDF 및 Silverlight를 통해 사용자를 공격합니다. 따라서 개별 사용자, 기업 및 보안 전문가는 이러한 침해 가능성을 인지하고 있어야 하며 노출 위험을 줄이기 위해 다음 조치를 취해야 합니다.

- **패치 다운로드**
- **최신 웹 기술 사용**
- **위험을 발생시킬 수 있는 웹 콘텐츠 사용 지양**

[7] "Flash, HTML5 and Open Web Standards," Adobe News, November 2015: **https://blogs.adobe.com/conversations/2015/11/flash-html5-and-open-web-standards.html**.
[8] "Flash and Chrome," by Anthony LaForge, The Keyword blog, Google, August 9, 2016: **https://blog.google/products/chrome/flash-and-chrome/**.
[9] "Reducing Adobe Flash Usage in Firefox," by Benjamin Smedberg, Future Release blog, Mozilla, July 20, 2016: **https://blog.mozilla.org/futurereleases/2016/07/20/reducing-adobe-flash-usage-in-firefox/**.

애플리케이션 보안: 앱이 폭증하는 가운데 OAuth 연결 위험 관리

클라우드로 전환하는 기업의 보안 범주는 가상 영역으로 확장됩니다. 하지만 유기적으로 연결된 서드파티 클라우드 애플리케이션을 도입하는 즉시 보안 범주는 대폭 축소됩니다.

작업자는 작업을 수행하는 동안 생산성을 높이고 연결 상태를 유지하고자 합니다. 그러나 이와 같은 섀도 IT 애플리케이션으로 인해 위험이 발생합니다. 이러한 애플리케이션은 사용자가 OAuth(Open Authentication, 개방형 인증)을 통해 액세스 권한을 부여하는 즉시 기업 인프라에 접근하여 기업 클라우드 및 SaaS(Software-as-a-service) 플랫폼과 자유롭게 통신할 수 있습니다. 이러한 앱에는 광범위한(경우에 따라서는 지나친) 액세스 범위가 적용될 수도 있습니다. 기업 데이터를 확인, 삭제, 외부 표시 및 저장할 수 있으며 사용자 대신 작업을 수행할 수도 있으므로 주의를 기울여 관리해야 합니다.

Cisco에서 인수한 클라우드 보안 회사인 CloudLock은 900개 조직으로 구성된 샘플 그룹에 연결된 서드파티 클라우드 애플리케이션의 증가 상황을 추적해 왔습니다. **그림 4**에 나와 있는 것처럼, 2016년 초에 확인된 고유 애플리케이션의 수는 약 129,000개였습니다. 그런데 10월 말에는 애플리케이션 수가 222,000개로 증가했습니다.

2014년부터 계산하면 애플리케이션의 수는 약 11배나 증가했습니다(**그림 5** 참조).

가장 위험한 애플리케이션 분류

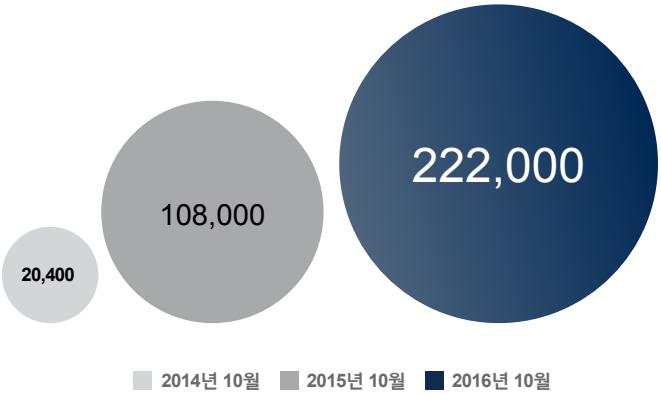
CloudLock은 보안 팀이 가장 취약한 애플리케이션을 현재 연결된 서드파티 클라우드 애플리케이션 내에서 파악할 수 있도록 CARI(Cloud Application Risk Index)를 개발했습니다. 개발 과정에서는 다음과 같은 요인을 평가했습니다.

- **데이터 액세스 요건:** 애플리케이션 인증에 필요한 권한, 데이터 액세스 권한이 부여되는 경우 애플리케이션이 OAuth 연결을 통해 기업 SaaS 플랫폼에 프로그래밍(API) 방식으로 액세스할 수 있는지 여부, 애플리케이션, 나아가 벤더가 사용자 대신 작업할 수 있으며 기업 데이터 보기/삭제 등 데이터를 사용하여 작업을 수행할 수 있는지 여부 등에 대한 질문을 조직에 제시했습니다.
- **커뮤니티 신뢰 등급:** 이 평가 과정에서는 피어 기반 및 크라우드소싱 평가를 사용했습니다.
- **애플리케이션 위협 인텔리전스:** 사이버 보안 전문가가 진행한 이 포괄적인 배경 조사는 보안 인증, 보안 침해 기록, 애널리스트 평가 등 애플리케이션의 다양한 보안 특성을 기반으로 진행되었습니다.

그림 4 연결된 서드파티 클라우드 애플리케이션의 폭증 (2016년)

출처: Cisco CloudLock

그림 5 서드파티 클라우드 애플리케이션의 증가(연도별 비교)



출처: Cisco CloudLock

2017년 그래픽 다운로드: www.cisco.com/go/acr2017graphics

위험 점수 및 예

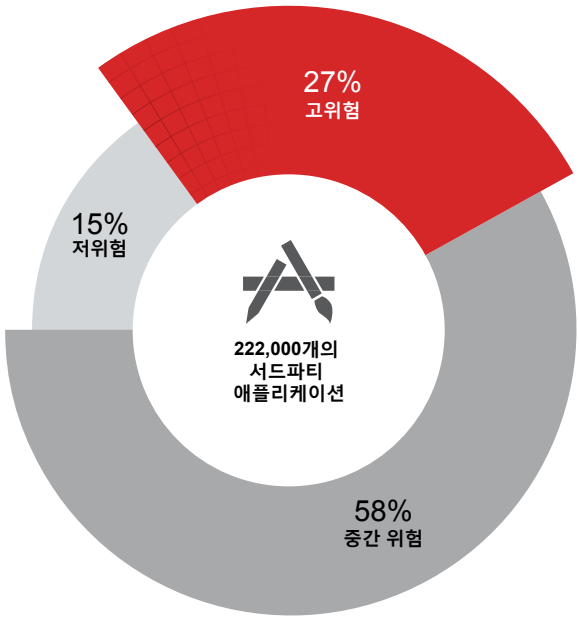
CloudLock은 CARI를 사용하여 서드파티 클라우드 애플리케이션을 분류한 후 각 앱에 대해 1(위험 레벨 최저)에서 5(위험 레벨 최고)까지의 위험 점수를 지정했습니다.

이메일만 확인 가능한 경우와 같이 최소한의 액세스 범위를 적용하고, 커뮤니티의 신뢰 등급이 100%이며 보안 침해 기록이 없는 앱의 경우 1점을 받았습니다.

반면 모든 이메일, 문서, 탐색 기록, 일정 등을 볼 수 있는 전체 어카운트 액세스 권한이 있고, 신뢰 등급이 8%(전체 관리자 중 8%만이 신뢰함)이며 보안 인증을 받지 않은 앱의 경우에는 5점을 받았습니다.

CloudLock는 CARI를 사용하여 샘플에 포함된 900개 조직에서 확인한 222,000개 애플리케이션을 분류했습니다. 전체 애플리케이션 중에 27%가 위험성이 높은 것으로 확인되었으며 대부분의 애플리케이션은 중간 수준의 위험 범주에 포함되었습니다(**그림 6** 참조). 이러한 조직 중 절반은 2016년 여름에 출시된 인기 게임 애플리케이션과 관련된 OAuth 연결을 사용하고 있었습니다.

그림 6 고위험군으로 분류되는 서드파티 애플리케이션

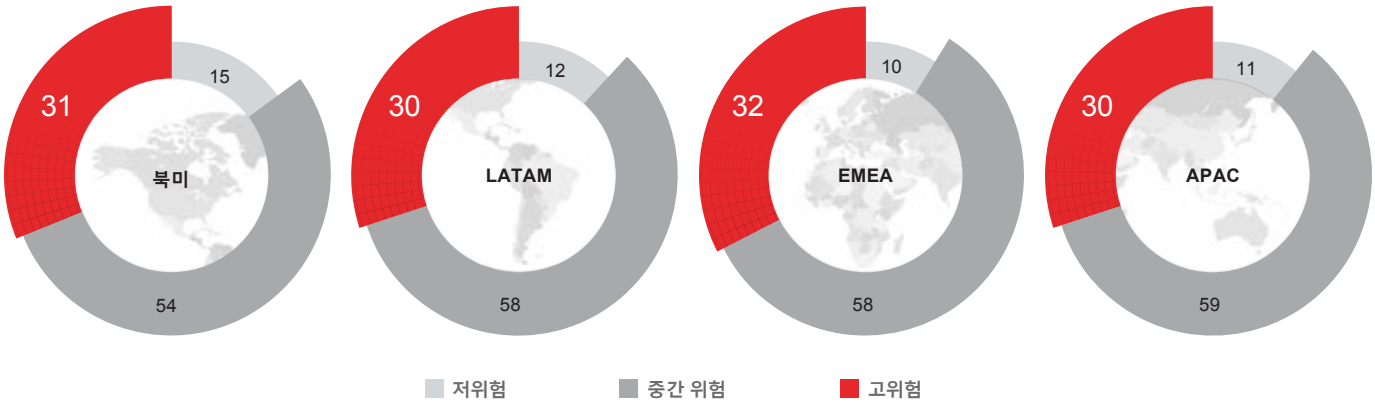


출처: Cisco CloudLock

공유

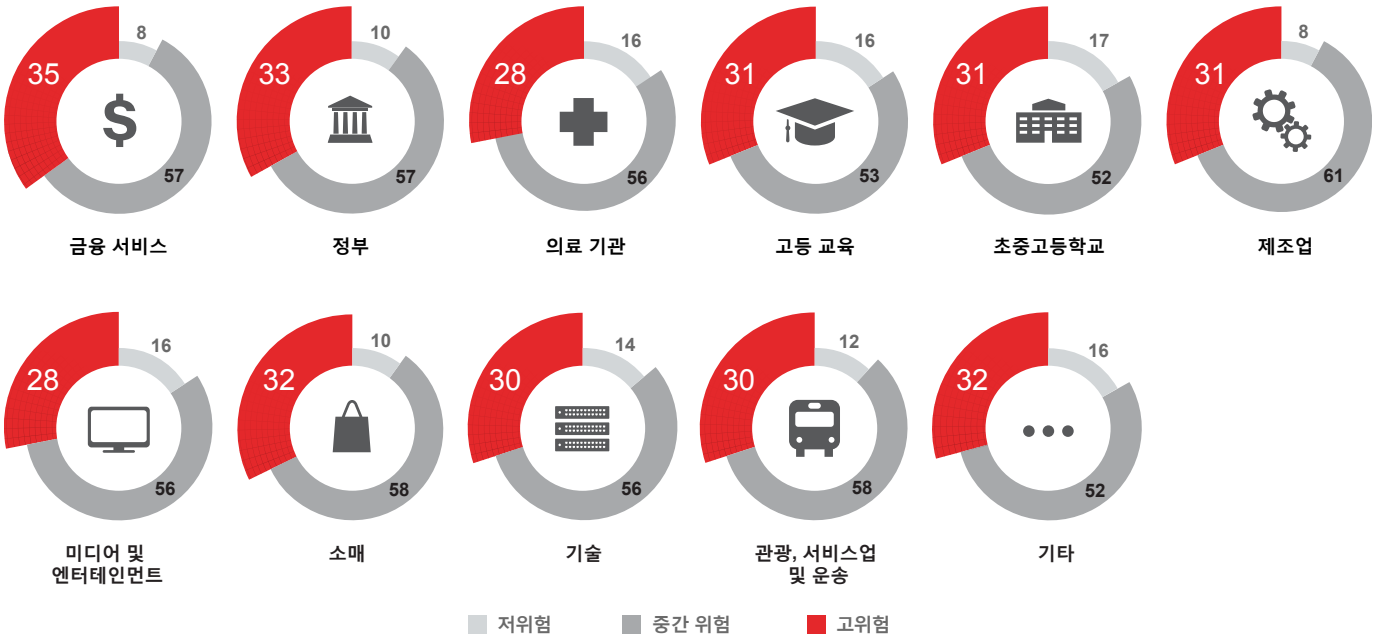
분석 결과 규모, 산업, 지역에 관계없이 모든 조직에서 저위험, 중간 위험, 고위험 애플리케이션이 비교적 균일하게 분포되어 있는 것으로 확인되었습니다(**그림 7** 및 **8** 참조).

그림 7 지역별 저위험, 중간 위험, 고위험 애플리케이션 분포



출처: Cisco CloudLock

그림 8 산업별 저위험, 중간 위험, 고위험 애플리케이션 분포



출처: Cisco CloudLock

2017년 그래픽 다운로드: www.cisco.com/go/acr2017graphics

불필요한 보안 알림 발생 방지

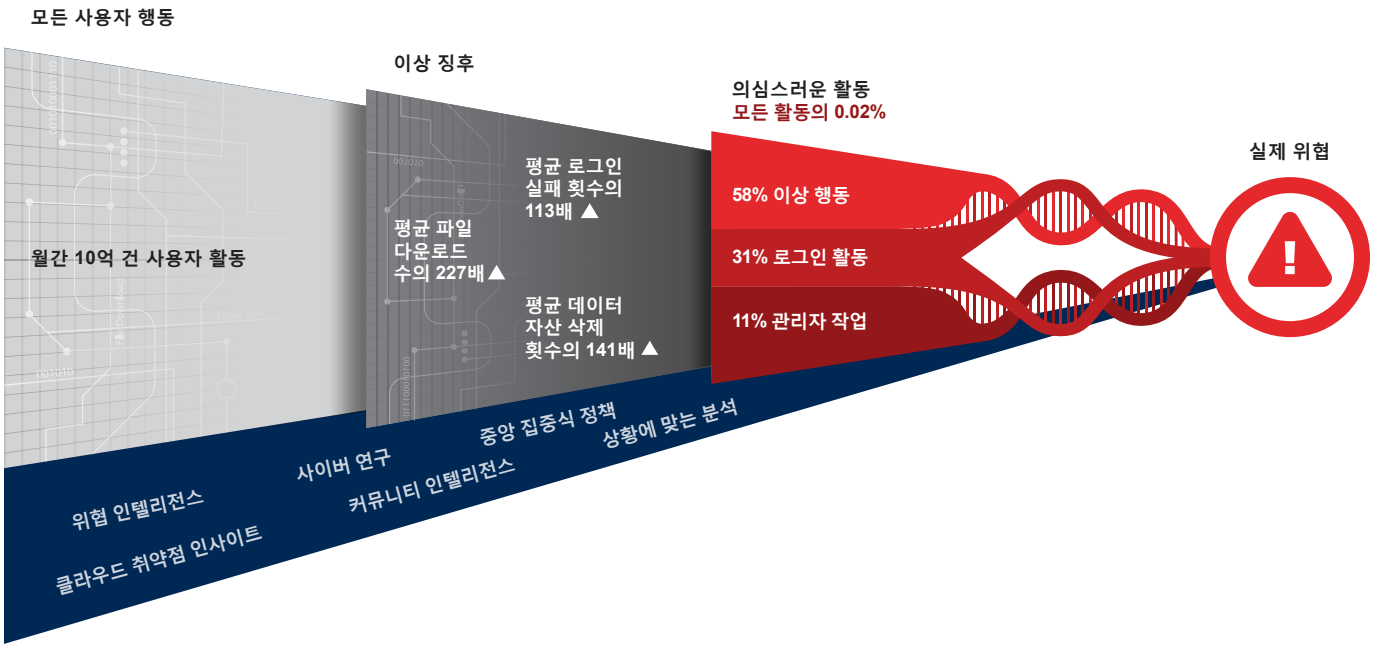
기업 SaaS 플랫폼에서 서드파티 클라우드 애플리케이션을 비롯한 의심스러운 사용자 및 엔터티 행동을 파악하려면 보안 팀은 수십억 건에 달하는 사용자 활동을 면밀하게 파악해 정상 패턴부터 정의해야 할 것입니다. 이러한 작업 후에는 예상 패턴을 벗어나는 이상 징후를 찾아내야 합니다. 마지막에는 의심스러운 활동의 상관성을 분석하여 조사가 필요한 실제 위협을 확인해야 합니다.

의심스러운 활동의 예로는 여러 국가에서 단기간 내에 수행되는 과도한 로그인 활동을 들 수 있습니다. 특정 조직의 정상 사용자 행동이 직원이 매주 1~2개 국가에서 특정 애플리케이션에 로그인하는 것이라고 가정해 보겠습니다. 사용자 한 명이 1주일 동안 68개 국가에서 해당 애플리케이션에 로그인했다면 보안 팀은 해당 활동을 조사해 정상적인 로그인인지를 확인할 수 있습니다.

Cisco의 분석 결과에 따르면 연결된 서드파티 클라우드 애플리케이션과 연관된 사용자 활동 5,000건 중 단 1건(0.02%)만이 의심스러운 활동이라고 합니다. 물론 보안 팀의 당면 과제는 이 1건을 찾아내는 것입니다.

보안 팀은 자동화를 이용해야만 "불필요한" 보안 알림 발생을 방지하고 실제 위협을 조사하는 데 리소스를 집중 투입할 수 있습니다. 앞서 설명한 정상적인 사용자 활동과 의심스러울 수 있는 사용자 활동을 파악하는 다단계 프로세스(**그림9**)의 속도는 각 단계 알고리즘에 자동화가 적용됐는지에 달려 있습니다.

그림 9 자동화를 통한 사용자 행동 패턴 파악(프로세스)



출처: Cisco CloudLock

정찰 | 공격 수단 구축 | **전송** | 설치

공격자들이 이메일, 첨부 파일, 웹사이트 및 기타 툴을 악의적으로 사용하여 사이버 공격 수단을 표적에게 전송

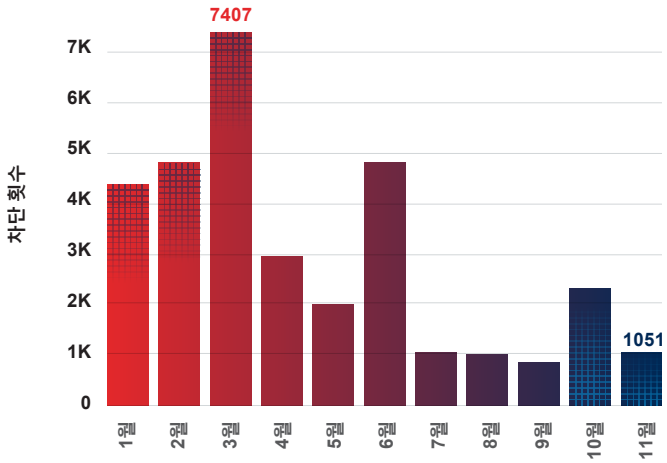
주요 익스플로잇 킷의 감소로 인한 소규모 및 새로운 공격자들의 공격 기회 증가

2016년에는 익스플로잇 킷 환경이 크게 변화했습니다. 2016년 초에 가장 많이 사용되었던 익스플로잇 킷은 Angler, Nuclear 및 RIG였습니다. 11월에는 해당 그룹 중 RIG만이 사용중인 것으로 나타났습니다. **그림 10**에 나와 있듯이, 6월경부터 익스플로잇 킷의 활동이 급감했습니다.

앞선 5월에는 Nuclear의 활동이 갑작스럽게 중단되었습니다. Nuclear 개발자들이 활동을 중지시킨 이유는 아직 확인되지 않았습니다. Flash 파일을 사용하여 취약점을 전송했던 Neutrino 익스플로잇 킷 역시 2016년에 활동을 중지했습니다. (2016년에 확인된 익스플로잇 킷의 상위 취약점 목록은 다음 페이지의 **그림 11** 참조)

Flash는 공격자들이 여전히 즐겨 사용하는 웹 공격 벡터이지만 사용 빈도는 점차적으로 낮아질 전망입니다. Flash를 일부분만 지원하거나 전혀 지원하지 않는 사이트 및 브라우저가 늘어나고 있으며, Flash의 취약점에 대한 인식 역시 높아졌기 때문입니다. (이 항목에 대한 자세한 내용은 "웹 공격 벡터: Flash 사용 빈도가 감소하고 있지만 사용자가 경계 상태를 유지해야 하는 이유", **15페이지** 참조)

그림 10 익스플로잇 킷 랜딩 페이지 차단(2016년 1~11월)



출처: Cisco Security Research

2017년 그래픽 다운로드: www.cisco.com/go/acr2017graphics

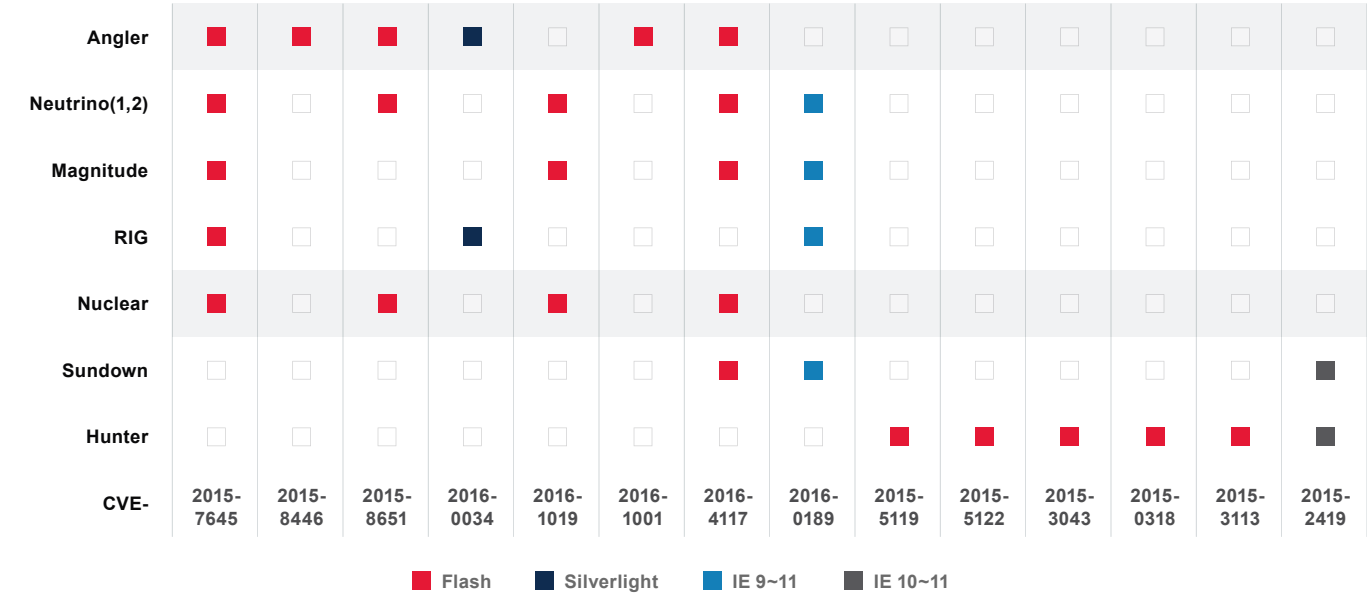
주요 익스플로잇 킷의 퇴장

알려진 익스플로잇 킷 중에 가장 규모가 크고 수준이 높은 Angler 역시 Flash의 취약점을 공격 대상으로 했으며, 다양한 유명 멀버타이징 및 랜섬웨어 공격과 연관되어 있습니다. 하지만 Nuclear 및 Neutrino의 감소와는 달리 Angler의 활동이 중단된 이유는 잘 알려져 있습니다.

2016년 늦은 봄, 러시아 은행을 대상으로 했던 금융 트로이 목마 Lurk 악성코드로 활동하던 약 50명의 해커와 사이버 범죄자들이 러시아에서 검거되었습니다.[10] Cisco 위협 연구에서는 Lurk와 Angler 간의 명확한 연관 관계를 파악했으며, Lurk가 대개 Angler를 통해 러시아 내의 피해자들에게 전송되었다는 점도 확인했습니다. 이 그룹이 검거된 후 Angler는 익스플로잇 킷 시장에서 사라졌습니다.[11]

이처럼 가장 널리 사용되었던 상위 3개 익스플로잇 킷이 사라짐에 따라, 소규모 및 새로운 공격자들이 성장하고 있습니다. 이들의 기술 수준 및 공격 속도 역시 갈수록 높아지고 있습니다. 2016년 말에 증가 추세를 보인 익스플로잇 킷으로는 Sundown, Sweet Orange, Magnitude 등이 있습니다. 이러한 킷과 RIG는 Flash, Silverlight 및 Microsoft Internet Explorer의 취약점을 표적으로 삼는 것으로 알려져 있습니다(**그림 11** 참조). 사용자는 Flash를 제거하고 불필요한 브라우저 플러그인을 비활성화하거나 제거하여 이러한 위협으로 인해 발생하는 위험을 줄여야 합니다.

그림 11 익스플로잇 킷의 상위 취약점



출처: Cisco Security Research

공유

[10] "Russian Hacker Gang Arrested Over $25M Theft," BBC News, June 2, 2016: **http://www.bbc.com/news/technology-36434104**.

[11] 이 항목에 대한 자세한 내용은 2016년 7월 Cisco Talos 블로그 게시물, **Connecting the Dots Reveals Crimeware Shake-Up**을 참조하십시오.

멀버타이징: 브로커를 이용해 공격 속도와 민첩성을 높이는 공격자들의 방식

사용자는 감염된 웹사이트와 멀버타이징의 두 가지 주요 방식을 통해 익스플로잇 킷으로 이동합니다. 공격자는 익스플로잇 킷 랜딩 페이지의 링크를 악성 광고나 감염된 웹사이트에 배치하거나, 브로커라는 중간 링크를 사용합니다. 이처럼 감염된 웹사이트와 익스플로잇 킷 서버 사이에 있는 링크를 "게이트"라고 합니다. 브로커는 사용자에게 악성코드 페이로드를 전송하는 실제 익스플로잇 킷과 초기 리디렉션 간의 매개 역할을 합니다.

공격 영역을 유지하거나 탐지를 피하기 위해서는 더욱 빠르게 이동해야 함을 공격자들이 인지하게 되면서 멀버타이징 전략의 사용률이 높아지고 있습니다. 공격자들은 브로커를 통해 초기 리디렉션을 변경하지 않고도 악성 서버 사이를 빠르게 전환할 수 있습니다. 익스플로잇 킷 공격자는 감염 사슬을 위해 웹사이트나 악성 광고를 지속적으로 수정하지 않아도 되므로 더 오랫동안 공격할 수 있습니다.

ShadowGate: 비용 효율적인 공격

기존의 웹 공격 벡터만으로는 사용자의 보안을 대규모로 침해하기가 갈수록 어려워짐에 따라(15페이지 참조), 공격자들은 사용자를 익스플로잇 킷에 노출시키기 위해 멀버타이징을 점점 더 많이 사용하고 있습니다. Cisco의 연구진은 최근 전 세계적으로 유행했던 멀버타이징 공격에 "ShadowGate"라는 코드명을 지정했습니다. 이 공격은 공격자들이 악성 광고를 통해 대규모 지역에 걸친 사용자를 표적으로 확보하는 방식을 잘 보여 줍니다.

ShadowGate는 대중 문화, 소매, 성인물, 뉴스 등 다양한 분야의 웹사이트를 감염시켰으며 북미, 유럽, 아시아 태평양, 중동 지역 사용자 수백만 명에게 영향을 주었을 가능성이 있습니다. 이 공격은 전 세계적으로 진행되었으며 다양한 언어를 사용한다는 점에서 주목할 만합니다.

도메인 섀도잉(Domain Shadowing) 기법을 사용한 ShadowGate는 2015년 초반에 처음 확인되었습니다. 이 공격은 일정 기간 동안 휴면 상태로 유지되다가 무작위로 다시 가동돼 익스플로잇 킷 랜딩 페이지로 트래픽을 전달합니다. ShadowGate는 원래 Angler 익스플로잇 킷으로만 사용자를 이동시키기 위해 사용되었습니다. 그러나 2016년 여름 Angler가 소멸된 이후에는 사용자가 Neutrino 익스플로잇 킷으로 이동되었고, 몇 개월 후에는 Neutrino 역시 사라졌습니다. (이 사례에 대한 자세한 내용은 "주요 익스플로잇 킷의 소멸로 인한 소규모 및 신규 공격자들의 공격 기회 증가"(20페이지 참조))

ShadowGate는 대량의 웹 트래픽을 생성했지만 사용자가 직접 상호작용을 함으로써 익스플로잇 킷으로 이동하는 경우는 극히 일부에 불과했습니다. 악성 광고는 대부분 페이지에 렌더링되는 이미지 광고였으며 사용자 상호작용은 전혀 필요하지 않았기 때문입니다. 이 온라인 광고 모델을 통해 ShadowGate 공격자는 더욱 효율적인 비용으로 공격할 수 있었습니다.

ShadowGate 연구는 Cisco와 주요 웹 호스팅 업체가 협력하여 진행되었습니다. 이러한 협력을 통해 공격자들이 활동하는 데 사용했던 등록자 어카운트를 회수함으로써 위협을 차단했습니다. 뒤이어 해당하는 모든 하위 도메인도 운영이 중단되었습니다.

ShadowGate 캠페인에 대한 자세한 내용은 2016년 9월 Cisco Talos 블로그 게시물, Talos ShadowGate Take Down: Global Malvertising Campaign Thwarted를 참조하십시오.

조사 결과: 전체 조직 중 75%가 애드웨어 감염 경험

애드웨어는 합법적인 용도로 사용하는 경우 리디렉션, 팝업, 광고 주입을 통해 광고를 다운로드하거나 표시하여 광고 작성자가 수익을 거둘 수 있도록 하는 소프트웨어입니다. 그러나 사이버 범죄자들 역시 수익원을 늘리기 위한 툴로 애드웨어를 사용하고 있습니다. 이들은 광고 주입을 통한 수익 창출과 더불어 DNSChanger 악성코드와 같은 기타 악성코드 공격을 더욱 쉽게 진행하기 위한 첫 단계로 악성 애드웨어를 사용합니다. 악성 애드웨어는 소프트웨어 번들을 통해 전송됩니다. 즉, 게시자는 다수의 악성 애드웨어 애플리케이션과 합법적인 애플리케이션이 함께 포함된 설치 프로그램을 만듭니다.

악의적인 공격자들은 다음과 같이 애드웨어를 활용합니다.

- **광고 주입(익스플로잇 킷에 추가로 감염되거나 노출되는 원인으로 작용할 수 있음)**
- **보안 수준을 낮추도록 브라우저 및 운영 체제 설정 변경**
- **안티 바이러스 또는 기타 보안 제품 손상**
- **다른 악성 소프트웨어를 설치할 수 있도록 호스트에 대한 모든 권한 확보**
- **위치, ID, 사용하는 서비스 및 자주 방문하는 사이트를 기준으로 사용자 추적**
- **개인 데이터, 자격 증명, 인프라 정보(예: 회사의 내부 영업 페이지)와 같은 정보 유출**

기업에 대한 애드웨어 문제의 범위를 평가하기 위해 Cisco 위협 연구진은 80가지 애드웨어 변종을 검사했습니다. 2015년 11월부터 2016년 11월까지 진행된 이 조사에는 여러 업종의 약 130개 조직이 포함되었습니다.

여기서는 각 구성 요소의 기본적인 행동에 따라 애드웨어를 다음과 같은 4개 그룹으로 분류했습니다.

- **애드 인젝터:** 이 애드웨어는 일반적으로 브라우저에 상주하며 모든 운영 체제에 영향을 줄 수 있습니다.
- **브라우저 설정 하이재커:** 이 애드웨어 구성 요소는 브라우저 보안 수준을 낮추기 위해 컴퓨터 설정을 변경할 수 있습니다.
- **유틸리티:** 지속적으로 확대되고 있는 대규모 애드웨어 범주입니다. 유틸리티는 PC 최적화 등 사용자에게 유용한 서비스를 제공하는 웹 애플리케이션입니다. 이러한 애플리케이션은 광고를 주입할 수 있지만 기본적인 용도는 사용자가 유료로 서비스를 이용하도록 하려는 것입니다. 하지만 대부분의 유틸리티는 스캠이며 사용자에게 아무런 이점도 제공하지 않습니다.
- **다운로더:** 이 애드웨어는 툴바 등의 다른 소프트웨어를 전송할 수 있습니다.

연구 대상 조직 중 75%는 애드웨어 감염의 영향을 받았다는 것이 확인되었습니다.

그림 12 애드웨어에 감염된 조직의 비율

출처: Cisco Security Research

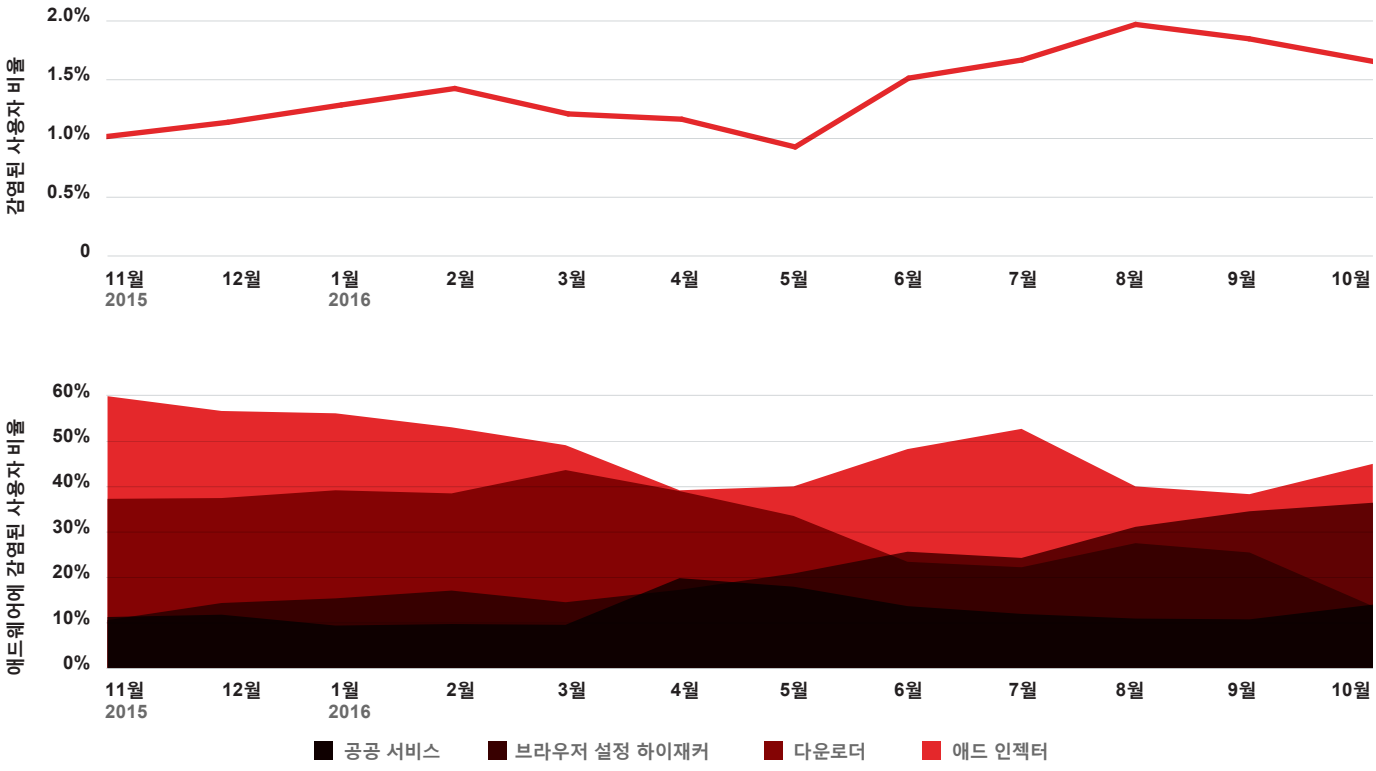
공유

그림 13에는 Cisco의 조사에 포함되었던 조직에서 관찰된 사고 유형이 나와 있습니다. 기본적인 감염 출처는 애드 인젝터였습니다. 사용자 동의 없이 설치된 애플리케이션이 대부분의 웹브라우저를 표적으로 삼는다는 사실을 방증합니다. 또한 지난 수년간 브라우저 기반 감염이 증가했다는 점도 확인되었습니다. 이는 공격자들이 공격 대상 사용자에게 이 전략을 효율적으로 사용하고 있음을 나타냅니다.

조사 과정에서 확인된 모든 애드웨어 구성 요소는 사용자와 조직에 대한 악성 활동을 수행할 위험성이 있습니다. 보안 팀은 애드웨어 감염으로 인해 발생하는 위협을 인식해야 하며, 조직의 사용자가 위험을 충분히 인지하도록 해야 합니다.

이 항목에 대한 자세한 내용은 2016년 2월 Cisco Security 블로그 게시물 **DNSChanger Outbreak Linked to Adware Install Base**를 참조하십시오.

그림 13 애드웨어 구성 요소별 전체 사고 구분



출처: Cisco Security Research

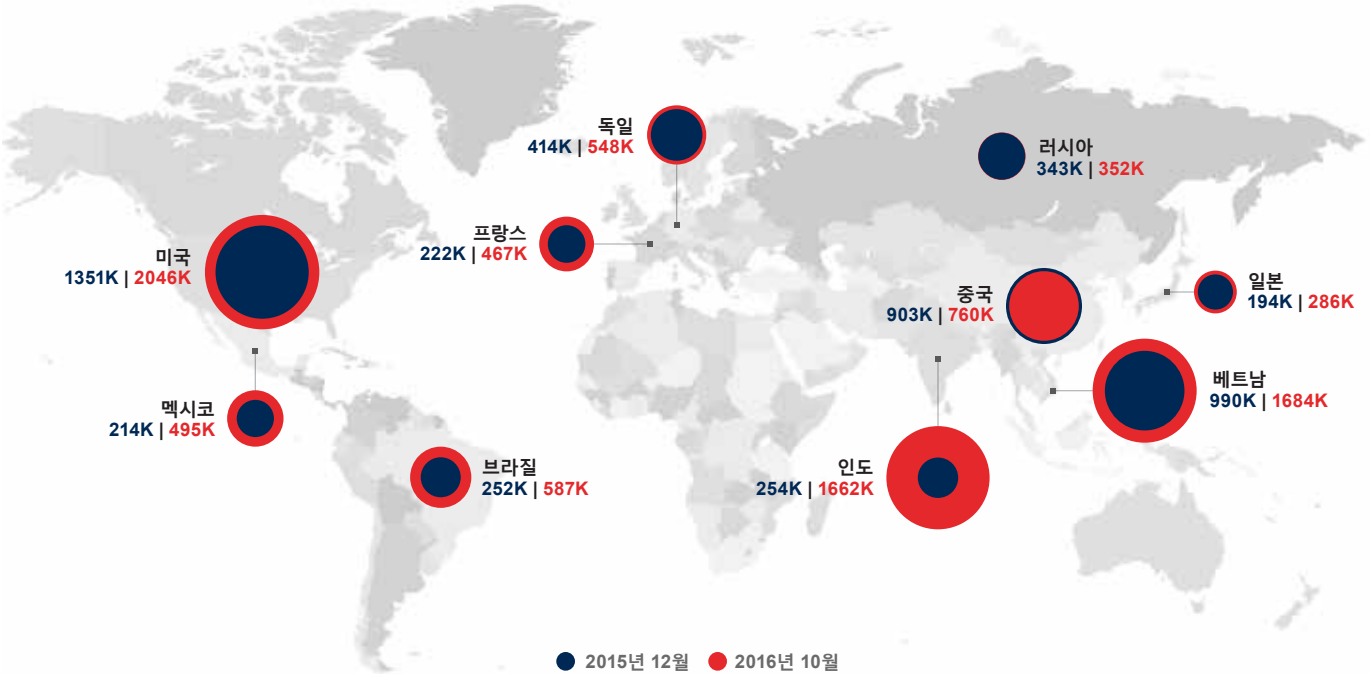
2017년 그래픽 다운로드: www.cisco.com/go/acr2017graphics

전 세계적인 스팸 증가 및 그에 따른 악성 첨부 파일 비율 증가 추세

Cisco 위협 연구진은 옵트인(사전 수신 동의) 고객 텔레메트리를 사용하여 총 이메일 중 스팸의 비율을 예측하기 위한 두 가지 조사를 2016년에 진행했습니다. 그 결과 총 이메일 중 스팸이 거의 2/3(65%)를 차지하는 것으로 나타났습니다. 또한, 전 세계의 스팸량이 계속 증가하고 있다는 것도 확인되었습니다. 이러한 증가 추세의 주된 이유는 Necurs와 같은 대규모 스팸 봇넷이 갈수록 성장하고 있기 때문입니다. 그리고 Cisco의 분석 결과에 따르면 2016년에 확인된 전 세계 스팸 중 약 8~10%는 악성으로 분류되는 것으로 나타났습니다.

2016년 8~10월에는 IP 연결 차단 수가 크게 증가했습니다 (**그림 14**).[12] 이러한 트렌드는 전반적인 스팸량 증가와, 스팸 발신인의 정보에 따라 조정되는 평판 시스템으로 인한 것이라 할 수 있습니다.

그림 14 국가별 IP 차단 횟수(2015년 12월~2016년 11월)



출처: Cisco Security Research

공유

[12] IP 연결 차단은 스팸 발신인의 평판 점수가 낮아 스팸 탐지 기술에 의해 즉시 차단된 스팸 메시지입니다. 확인된 스팸 전송 봇넷 또는 스팸 공격에 참여하는 것으로 알려진 감염된 네트워크에서 생성된 메시지를 예로 들 수 있습니다.

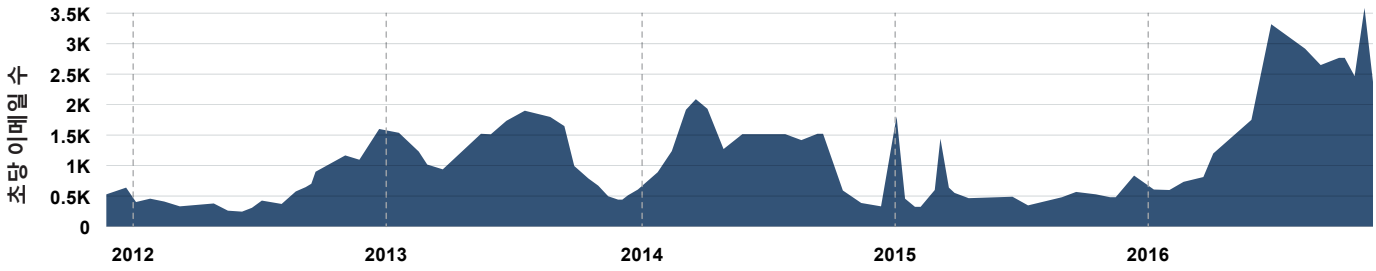
의심스러운 스팸 감염 항목이 포함된 DNS 기반 "블랙홀 목록" CBL(Composite Blocking List)의 5년 주기 그래프[13]에서도 2016년에 총 스팸량이 크게 증가했음을 확인할 수 있습니다(**그림 15**).

CBL의 10년 단위 데이터(그림에는 나와 있지 않음)를 검토한 결과, 2016년의 스팸량은 2010년에 확인되었던 사상 최대 수준의 스팸 수에 거의 근접한 것으로 나타났습니다. 새로운 안티 스팸 기술이 도입되고 스팸 관련 봇넷이 엄격한 처벌을 받으면서 수년 동안 스팸 수준이 낮게 유지되었습니다. Cisco 위협 연구 결과에 따르면, 최근 전 세계 스팸량의 증가 추세는 Necurs 봇넷으로 인한 것으로 보입니다. Necurs는 Locky 랜섬웨어의 주요 벡터이며 Dridex 금융 트로이 목마 등을 배포합니다.

그림 16은 Cisco의 SpamCop 서비스에서 생성한 내부 그래프로, 2016년에 관찰된 스팸 볼륨의 변동을 보여줍니다. 이 그래프에는 2015년 11월부터 2016년 11월까지의 SCBL(SpamCop Block List) 전체 크기가 나와 있습니다. SCBL의 각 행은 고유 IP 주소를 나타냅니다.

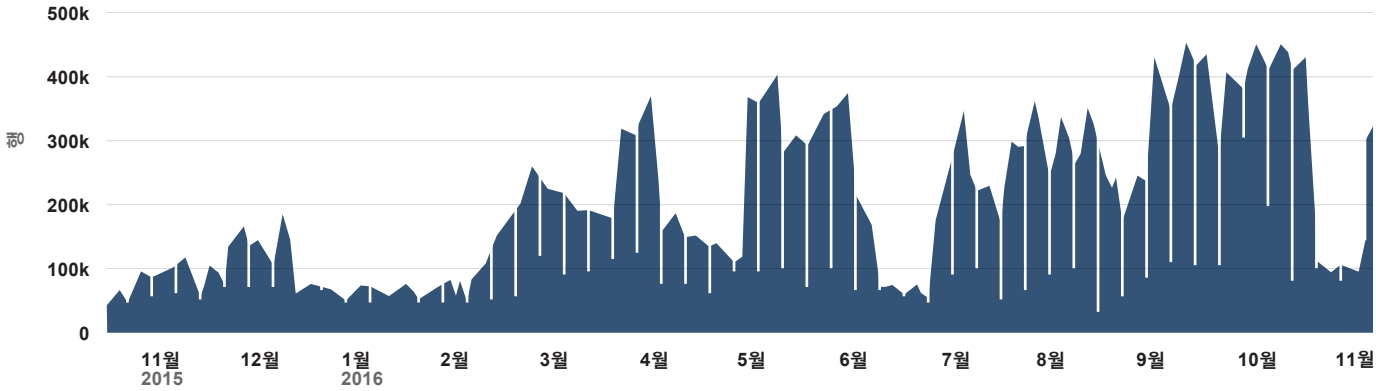
2015년 11월에서 2016년 2월까지의 SCBL 크기는 IP 주소 20만 개 미만이었습니다. 9~10월에는 SCBL 크기가 IP 주소 40만개를 초과했다가 10월에 다시 감소했습니다. Cisco 위협 연구진에 따르면, 이러한 감소는 Necurs 운영자들이 잠시 휴지기를 가졌기 때문일 뿐이라고 합니다. 6월에도 스팸량이 크게 감소했음을 확인할 수 있습니다. 5월 말에 Lurk 금융 트로이 목마 관련 해킹 그룹이 검거되었기 때문입니다(**21페이지 참조**). 이로 인해 Necurs를 비롯해 널리 알려진 다수의 위협이 잠시 소강 상태를 나타냈습니다. 하지만 3주 후부터 Necurs의 활동이 재개되어 2시간만에 SCBL에 IP 주소가 20만 개 이상 추가되었습니다.

그림 15 총 스팸량



출처: CBL

그림 16 SCBL의 전체 크기



출처: SpamCop

공유

[13] CBL에 대한 자세한 내용은 **http://www.abuseat.org/**를 참조하십시오.

Necurs 스팸을 전송하는 대다수의 호스트 IP는 2년 이상 감염된 상태였습니다. Necurs는 봇넷의 전체 범위를 은폐된 상태로 유지하기 위해 감염된 호스트 중 일부에서만 스팸을 전송합니다. 감염된 호스트는 2~3일 동안 사용된 후 2~3주 동안은 다시 사용되지 않을 수도 있습니다. 이러한 행동으로 인해 보안 인력이 스팸 공격에 대응하기가 까다로워집니다. 즉, 보안 직원은 감염된 호스트를 찾아내 올바르게 치료했다고 생각하겠지만 실제로는 Necurs 공격자들이 다른 공격을 실행하기 전까지 잠시 기다리는 것뿐입니다.

2016년 10월에 관찰된 총 스팸 중 75%는 악성 첨부 파일을 포함하고 있었으며 대부분 Necurs 봇넷에서 전송된 것이었습니다(**그림 17** 참조). Necurs는 JavaScript, .hta, .wsf, VBScript 다운로더 등의 임베디드 실행 파일이 포함된 악성 .zip 첨부 파일을 전송합니다. 연구 과정에서 악성 첨부 파일이 포함된 총 스팸 수의 백분율을 계산할 때 "컨테이너" 파일(.zip)과 이 파일 내의 "하위" 파일(예: JavaScript 파일)이 모두 개별 악성 첨부 파일로 계산되었습니다.

다양한 첨부 파일 유형을 사용하여 악성 스팸 공격을 지속적으로 개선하는 공격자

Cisco 위협 연구진은 악성 스팸이 탐지되지 않도록 하기 위해 공격자들이 첨부 파일을 활용하는 방식을 조사했습니다. 조사 결과, 공격자들은 파일 유형을 광범위하게 사용한 뒤, 원하는 결과를 얻지 못할 경우 빠르게 전술을 전환함으로써 공격 전략을 발전시키고 있었습니다.

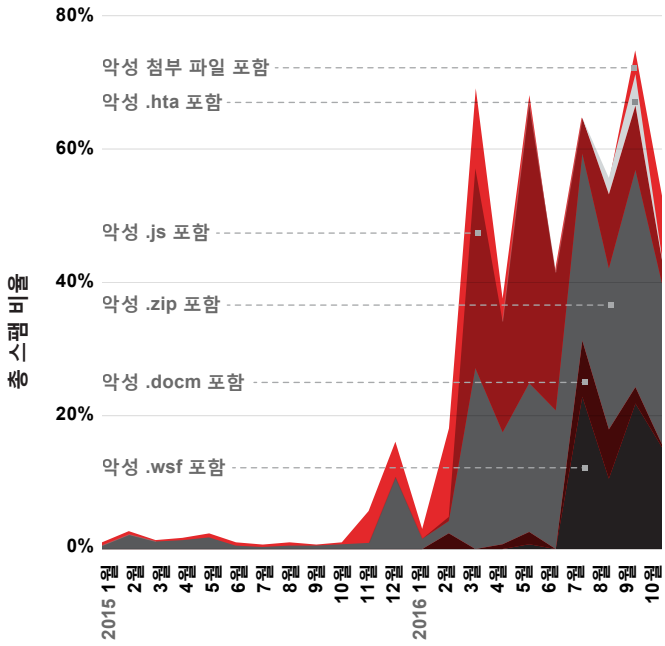
그림 17에는 악성 스팸 공격자들이 관찰 기간 동안 .docm, JavaScript, .wsf 및 .hta 파일을 시범적으로 사용해 본 수치가 나와 있습니다. 앞에서 언급한 것처럼 이러한 파일 유형은 대부분 Necurs 봇넷에서 전송하는 스팸과 연관되어 있습니다. (조사에 포함되었던 기타 파일 유형과 관련된 연구 내용은 부록, 78페이지 참조)

지정된 달에 확인된 악성 첨부 파일을 포함하는 총 스팸 비율을 사용하여 해당 달의 파일 유형별 사용 비율을 계산했습니다. 예를 들어 2016년 7월의 .docm 파일 사용률은 7월에 관찰된 총 악성 첨부 파일 비율 중 8%를 차지합니다.

2016년에 .wsf 파일을 사용한 패턴(**그림 17** 참조)을 살펴보면 공격자들이 점진적으로 악성 스팸 전술을 발전시킨 방식을 파악할 수 있습니다. 이 파일 유형은 2016년 2월 이전에는 악성 첨부 파일로 거의 사용되지 않았습니다. 그런데 Necurs 봇넷의 활동이 활발해지면서 이 파일 유형의 사용률이 높아지기 시작했습니다. 7월에는 모든 악성 스팸 첨부 파일 중 .wsf 파일의 비율이 22%까지 높아졌습니다. 또한, 이 시기쯤에 전 세계의 스팸 활동도 급격히 증가했습니다(이전 섹션 참조). 이러한 현상은 대개 Necurs 봇넷으로 인한 것이라 할 수 있습니다.

8, 9, 10월에는 .wsf 파일의 사용 비율에 심한 변동이 나타납니다. 이 시기에는 해당 파일 유형의 탐지 빈도가 높아져 공격자들이 사용 빈도를 조절한 것으로 보입니다.

그림 17 악성 첨부 파일이 포함된 총 스팸 비율



출처: Cisco Security Research

Hailstorm(헤일스톰) 및 Snowshoe(스노우슈)

방어자에게 있어서 특히 까다로운 두 가지 악성 스팸 공격 유형은 Hailstorm(헤일스톰) 공격과 Snowshoe(스노우슈) 공격입니다. 이 두 가지 유형은 모두 빠른 속도와 표적 지정 요소를 활용하며 효율성이 매우 높습니다.

Hailstorm 공격은 안티 스팸 시스템을 대상으로 합니다. 이러한 공격자는 스팸 공격 실행 시점과 안티 스팸 시스템의 탐지 시점 사이의 매우 짧은 시기를 활용합니다. 공격자들이 공격을 수행할 수 있는 시간은 대개 공격이 탐지되어 차단되기 전까지 몇 초에서 몇 분에 불과합니다.

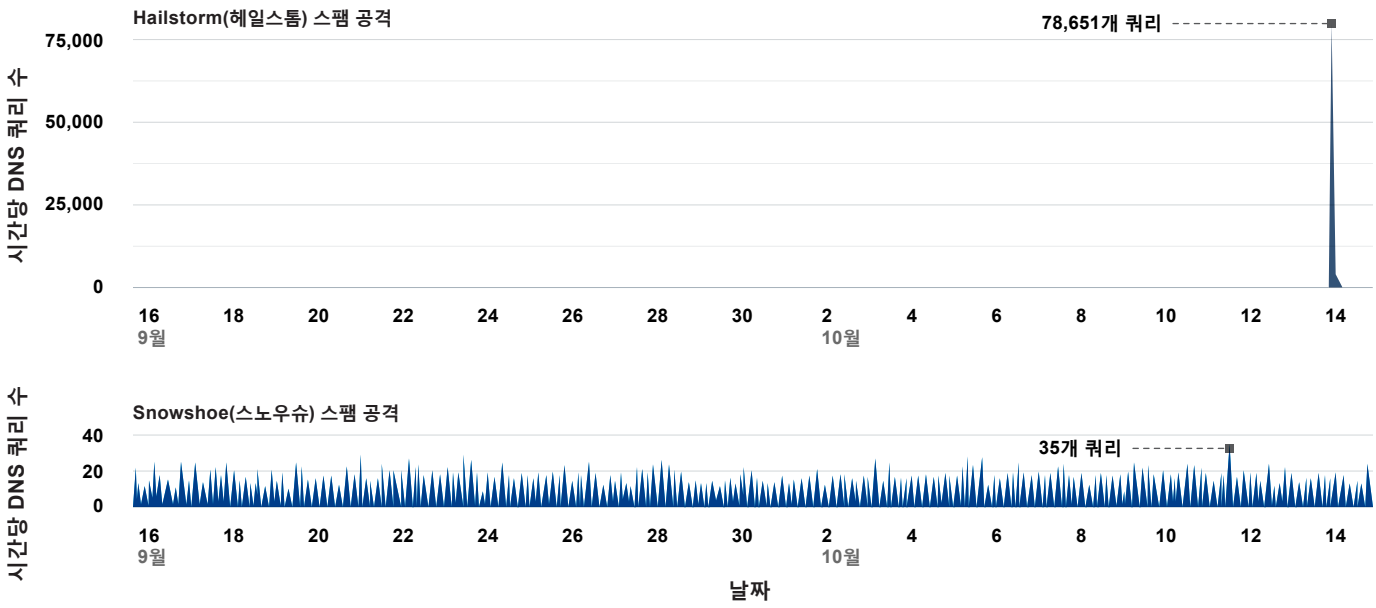
그림 18에서 IP 주소 확인 수가 급증한 날짜가 Hailstorm 공격이 실행된 날짜입니다. 이 활동은 Cisco Investigate 인터페이스에 표시됩니다. 공격 직전까지는 IP 주소를 확인하는 사람이 전혀 없었습니다. 그런데 갑자기 DNS의 도메인을 확인하는 컴퓨터 수가 78,000대 이상으로 급증했다가 다시 0대로 돌아갑니다.

이러한 Hailstorm 공격과는 달리, **그림 18**에 나와 있는 Snowshoe 스팸 공격에서는 공격자가 볼륨 기반 탐지 솔루션의 감시망을 피해 공격을 시도합니다. 그림에 나와 있는 것처럼 DNS 조회 수는 일정하게 유지되지만 시간당 쿼리 수는 25개에 불과합니다. 공격자들은 이처럼 볼륨이 거의 변화하지 않는 공격을 통해 대량의 IP 주소에서 비밀리에 스팸을 배포할 수 있습니다.

이러한 스팸 공격은 서로 다른 방식으로 작동하지만 몇 가지 공통점이 있습니다. 즉, 이러한 방식을 통해 공격자는 다음을 수행할 수 있습니다.

- **정상 IP 및 도메인에서 스팸을 전송하여 악의적인 평판 우회**
- **전문적인 콘텐츠 및 서브스크립션 관리를 제공하는 마케팅 메일 모방**
- **엉성한 스크립트나 스팸 봇 대신 적절하게 구성된 이메일 시스템 사용**
- **전달 확인 역방향 DNS 및 SPF(Send Policy Framework) 레코드를 올바르게 설정**

그림 18 Hailstorm(헤일스톰) 및 Snowshoe(스노우슈) 스팸 공격 비교



출처: Cisco Investigate

공유

공격자들은 텍스트를 변형하고 파일 유형을 번갈아 사용하여 콘텐츠 탐지 기능을 손상시킬 수도 있습니다. (사이버 범죄자들이 방어자들의 탐지를 피하기 위해 위협 방식을 발전시키는 방법에 대한 자세한 내용은 "진화 소요 시간" 섹션, **34페이지** 참조) 사이버 범죄자들이 다양한 악성 첨부 파일을 이용해 스팸 공격 방식을 시도하는 내용은 이전 섹션을 참조하십시오.

그림 19에는 상위 위협 발생 알림이 나와 있습니다. 여기서는 이메일 보안 검사 및 규칙을 우회하기 위해 2016년에 공격자들이 빈번하게 업데이트한 것으로 확인된 스팸 및 피싱 메시지를 대략적으로 보여 줍니다. 악성 메시지로 인한 피해를 입지 않으려면 가장 널리 사용되는 이메일 위협 유형을 파악해 두어야 합니다.

그림 19 상위 위협 발생 알림

버전	게시 식별자	게시 이름 및 URL	메시지 요약	첨부 파일 유형	언어	최종 게시일
96	35656	RuleID4626	청구서, 결제	.zip	영어, 독일어	2016-04-25
87	34577	RuleID10277	구매 발주서	.zip	영어, 독일어	2016-06-02
82	36916	RuleID4400KVR	구매 발주서	.zip	영어	2016-02-01
74	38971	RuleID15448	구매 발주서, 결제, 영수증	.zip, .gz	영어	2016-08-08
72	41513	RuleID18688	주문, 결제, 세미나	.zip	영어	2016-09-01
70	40056	RuleID6396	구매 발주서, 결제, 영수증	.rar	영어	2016-06-07
66	34796	RuleID5118	제품 주문, 결제	.zip	영어, 독일어	2016-09-29
64	39317	RuleID4626(계속)	청구서, 결제, 배송	.zip	영어, 독일어, 스페인어	2016-01-28
64	36917	RuleID4961KVR	확인, 결제/이체, 주문, 배송	.zip	영어	2016-07-08
63	37179	RuleID13288	배달 알림, 법정 출두, 티켓 청구서	.zip	영어, 스페인어	2016-07-21
61	38095	RuleID858KVR	배송, 견적, 결제	.zip	영어	2016-08-01
58	39150	RuleID4961KVR	견적 요청, 제품 주문	.zip	영어, 독일어, 다국어	2016-01-25
47	41886	RuleID4961	이체, 배송, 청구서	.zip	영어, 독일어, 스페인어	2016-02-22

출처: Cisco Security Research

2017년 그래픽 다운로드: www.cisco.com/go/acr2017graphics

정찰 | 공격 수단 구축 | 전송 | **설치**

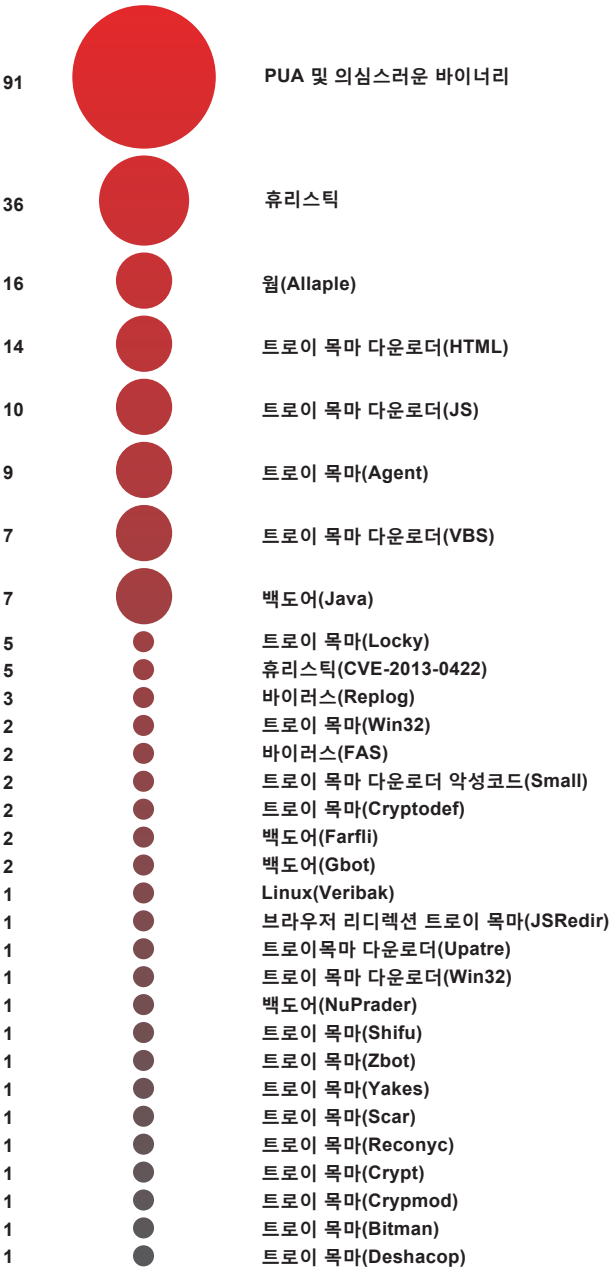
위협이 전송된 후 표적 시스템에 백도어를 설치하여 공격자에게 지속적 액세스 권한을 제공

웹 공격 방법: 사용자가 쉽게 피할 수 있는 위협을 보여주는 "장기적" 공격 기법

"장기적" 웹 공격 방법 스펙트럼(**그림 20**)에는 비교적 적은 수의 악성코드 유형 모음이 포함됩니다. 이 단계에서는 전송된 위협(금융 트로이 목마, 바이러스, 다운로더 또는 기타 익스플로잇)이 대상 시스템에 백도어를 설치합니다. 그러면 공격자에게 영구적 액세스 권한이 제공되며 데이터 유출 및 랜섬웨어 공격과 악의적인 행동이 가능한 기회도 제공됩니다.

그림 20에 나와 있는 위협은 가장 흔히 관찰되는 상위 50개 악성코드 유형 이외에 확인된 악성코드 시그니처 샘플입니다. 길게 나열된 웹 공격 방법들은 공격 성공 후 해당 머신이나 시스템에서 비밀리에 작동하는 위협을 사전에 보여주는 공격 기법입니다. 이러한 감염 중 상당수는 악성 애드웨에 감염되거나 교묘하게 제작된 피싱 스캠에 노출되는 경우 최초로 전파됩니다. 사용자는 이러한 상황을 쉽게 피하거나 빠르게 치료할 수 있습니다.

그림 20 관찰된 양이 적은 악성코드의 샘플



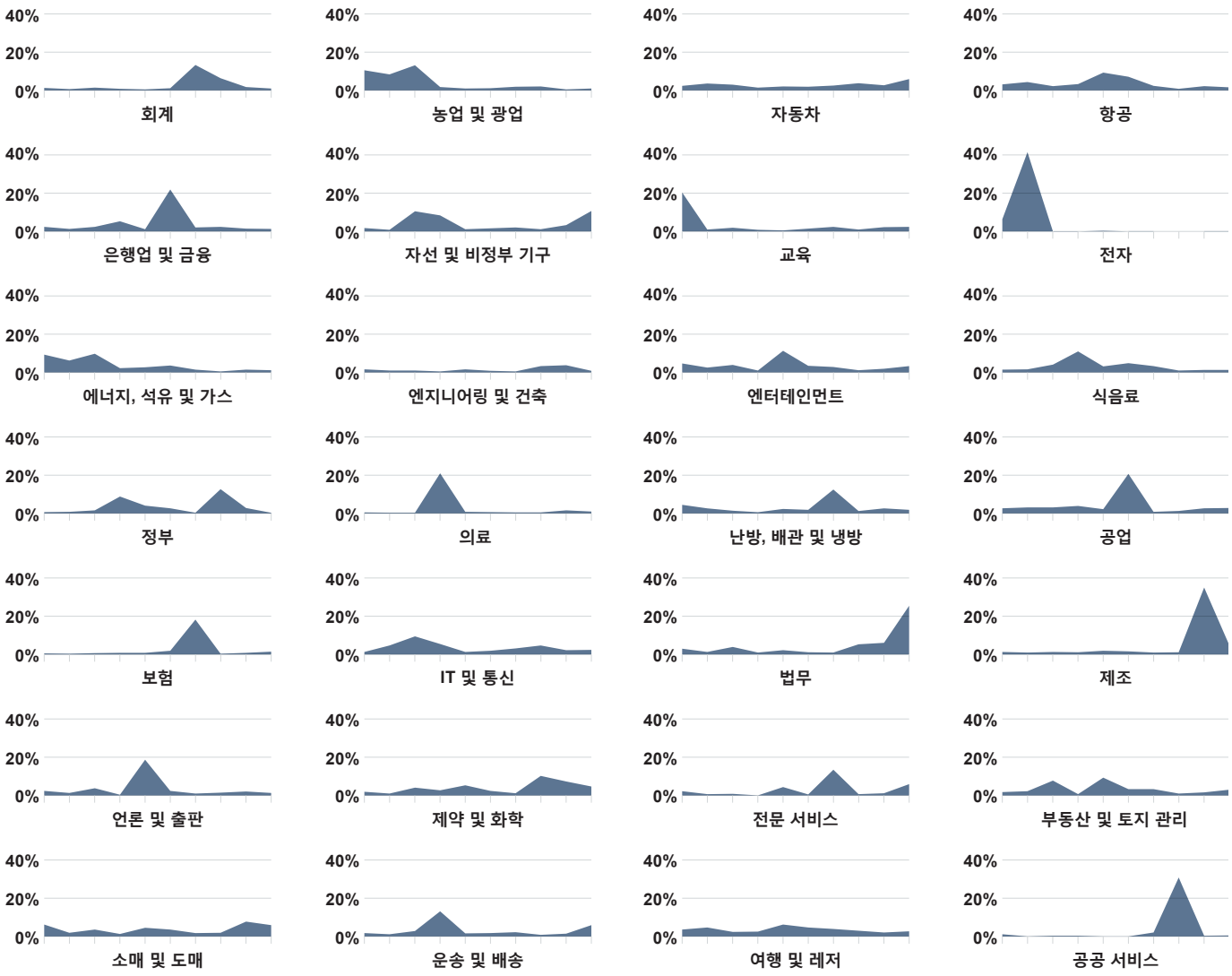
출처: Cisco Security Research

업종별 악성코드 발생 위험: 공격자들의 업종별 공격 현황

*Cisco 2016 중기 사이버 보안 보고서*에는 악성코드의 위험에 대한 중요 메시지, 즉 "안전한 업종은 없다"가 나와 있습니다. Cisco 연구 팀이 시행한 공격 트래픽 "차단율" 및 "정상적인" 트래픽에 관한 업종별 정기 조사에 따르면 2016년 하반기에도 이 메시지는 유효했던 것으로 나타났습니다.

기간별 업종 및 해당 차단율(**그림 21**)을 살펴보면 몇 달 동안 특정 시점에서 모든 업종에 다양한 수준의 공격 트래픽이 발생했음을 확인할 수 있습니다. 공격의 시작과 종료 시기는 업종별로 다르지만 공격이 발생하지 않은 업종은 없음이 명확하게 드러납니다.

그림 21 월간 업종별 차단율



출처: Cisco Security Research

공유

웹 차단 활동에 대한 지역별 개요

공격자는 활동 거점을 빈번하게 옮기며 취약한 인프라를 찾아다닙니다. Cisco 위협 연구진은 전반적인 인터넷 트래픽량과 차단 활동을 분석함으로써 악성코드 최초 발생지 정보를 제공할 수 있습니다.

그림 22에 나와 있는 것처럼, 미국의 트래픽은 ***Cisco 2016 중기 사이버 보안 보고서***에 제공된 차단율보다 약간 증가했습니다. 실제로 미국의 차단율은 훨씬 높지만, 이 수치는 미국의 온라인 트래픽 비율이 타 국가에 비해 훨씬 높다는 점을 고려하여 함수로 계산해야 합니다. 또한, 미국은 세계 최대의 악성코드 공격 대상국 중 하나이기도 합니다.

보안 전문가가 기억해야 할 점은, 업종별 웹 차단 활동과 마찬가지로 지역별 웹 차단 활동에서도 악성코드 트래픽이 보편적인 문제로 나타난다는 것입니다.

그림 22 국가별 웹 차단

출처: Cisco Security Research

공유

탐지 소요 시간(TTD): 방어자의 탐지 소요 시간 측정을 위한 필수 메트릭

Cisco는 TTD 중앙값의 가장 정확한 예상치를 추적 및 보고할 수 있도록 지속적으로 TTD 측정 방식을 개선하고 있습니다. 이 측정 방식이 최근 조정되어, 처음에는 "알 수 없음"으로 분류되었다가 추후 지속적인 분석 및 글로벌 차원의 관찰을 통해 "악성으로 확인됨"으로 보다 정확히 파악할 수 있게 되었습니다. 이처럼 데이터를 더욱 종합적으로 확인함으로써 위협이 처음으로 발생한 시기 및 보안 팀이 해당 사항을 위협으로 확인하는 데 걸린 시간을 더욱 효율적으로 파악할 수 있습니다.

이러한 방식으로 새롭게 확보한 정보를 통해, 2015년 11월의 TTD 중앙값이 39시간임을 확인할 수 있었습니다(**그림 23** 참조). 2016년 1월에는 이 TTD 중앙값이 6.9시간으로 단축되었습니다. Cisco의 위협 연구진은 2016년 10월의 데이터를 수집 및 분석하여 Cisco 제품이 2015년 11월~2016년 10월의 기간 동안 TTD 중앙값 14시간을 달성했음을 확인할 수 있었습니다. 참고로 2016년의 TTD 중앙값 수치는 관찰 기간 동안의 평균 중앙값입니다.

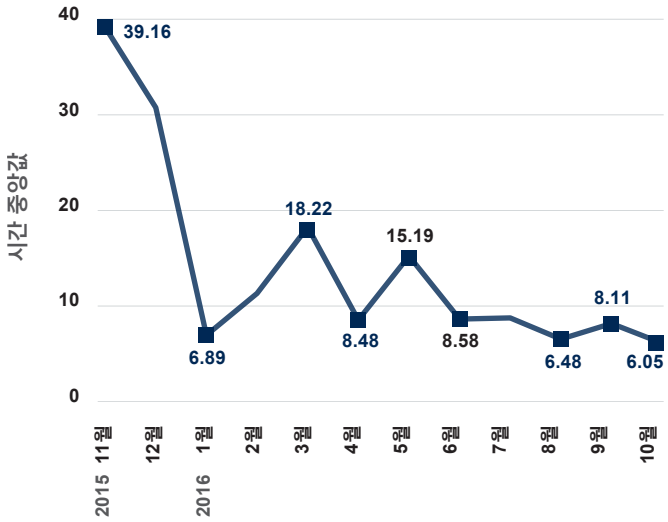
TTD 중앙값은 2016년 한 해 동안 큰 폭으로 변화했지만 전반적으로는 감소하는 경향을 보였습니다. 공격자들이 새로운 위협을 실행하는 시기가 되면 TTD 중앙값이 증가합니다. 그 이후에 방어자들이 방어 방법을 파악하여 위협을 빠르게 식별할 수 있는 시기가 되면 중앙값은 감소합니다.

그림 23에서는 2016년 4월 말경의 TTD 중앙값이 약 15시간이었음을 알 수 있습니다. 이 값은 *Cisco 2016 중기 사이버 보안 보고서*에서 보고되었던 수치인 13시간보다 큽니다.[14] 이 15시간이라는 수치는 2015년 11월~2016년 4월에 수집된 데이터를 기준으로 합니다. 즉, 해당 수치는 파일의 회귀적 정보를 분석해서 얻은 것이 아닙니다. 새로운 중기 TTD 수치를 사용하는 경우에는 2016년 5~10월의 기간 동안 TTD가 약 9시간으로 감소했다고 보고할 수 있습니다.

TTD 중앙값의 보다 정확한 측정치를 확인하는 과정은 물론, 장기적으로 위협이 발전하는 방식을 연구하는 과정에서도 회귀적인 데이터 검토는 중요한 작업입니다. 보안 커뮤니티에 알려져 있다 하더라도 특히 포착하기 어려우며 식별에 오랜 시간이 수반될 위협이 다수 존재합니다.

공격자는 탐지를 피하고 공격 준비 시간을 늘리기 위해 특정 악성코드군을 발전시킵니다. 이러한 전술로 인해 방어자가 다수의 알려진 위협 유형을 효율적으로 탐지하고 유지하기 어려워집니다. (이 항목에 대한 자세한 내용은 "진화 소요 시간: 지속적으로 변화하는 위협", **34페이지** 참조) 그러나 사이버 범죄자들이 위협을 빠르고 빈번하게 발전시키고 있다는 점은 위협을 활동 상태로 유지하고 수익 창출 방법을 찾는 데 큰 부담을 안고 있음을 나타냅니다.

그림 23 월별 TTD 중앙값



출처: Cisco Security Research

Cisco는"탐지 소요 시간(Time To Detection)", 즉 "TTD"를 보안 침해가 발생한 시점부터 위협이 탐지된 시점까지의 시간 범위로 정의합니다. 이 시간 범위는 전 세계에 구축된 Cisco 보안 제품으로부터 수집한 옵트인(사전 수신 동의) 보안 텔레메트리를 통해 결정합니다. Cisco는 글로벌 가시성 및 지속적인 분석 모델을 사용하여 악성코드가 엔드포인트에서 실행되는 시점부터 분류되지 않은 모든 악성코드가 발생할 당시 위협으로 확인되는 시점까지를 측정할 수 있습니다.

[14] *Cisco 2016 중기 사이버 보안 보고서*: **http://www.cisco.com/c/m/ko_kr/offers/sc04/2016-midyear-cybersecurity-report/index.html**.

진화 소요 시간: 지속적으로 변화하는 위협

사이버 범죄자들은 다양한 난독화(obfuscation) 기술을 사용해 악성코드의 강도를 유지하며 이를 통해 수익을 창출하고자 합니다. 여기에 흔히 사용하는 두 가지 방법은 페이로드 전송과, 새로운 파일을 빠르게 생성하여 해시 전용 탐지 방법을 무력화하는 것입니다. Cisco 연구 팀은 공격자들이 이러한 두 가지 전략을 사용하여 널리 알려진 6가지 악성코드군(Locky, Cerber, Nemucod, Adwind RAT, Kryptik, Dridex)이 탐지를 피해 사용자와 시스템을 침해한 방식을 면밀하게 조사했습니다.

이러한 분석을 통해 Cisco는 TTE(Time to Evolve, 진화 소요 시간), 즉 공격자들이 특정 악성코드가 전송되는 방식을 변경하는 데 소요되는 시간과 각 전술 변경 간의 시간차를 측정했습니다. 그리고 다양한 Cisco 출처(구체적으로는 웹 프록시 데이터, 클라우드 및 엔드포인트 지능형 악성코드 제품, 복합적인 악성코드 차단 엔진)의 웹 공격 데이터를 분석했습니다.

Cisco 연구 팀은 사용자 시스템에서 정의된 파일 콘텐츠(MIME) 유형과 악성코드를 전송하는 파일 확장자의 변경 사항을 확인했습니다. 그 결과, 각 악성코드군에 고유한 진화 패턴이 있음을 확인했습니다. 각 악성코드군에 대해 웹 및 이메일 전송 방법의 패턴을 모두 조사했으며 각 악성코드군과 연관된 고유 해시의 사용 기간도 추적하여 공격자들이 새 파일(결과적으로는 새 해시)을 얼마나 빨리 만들 수 있는지를 확인했습니다.

이 연구를 통해 확인된 사항은 다음과 같습니다.

- **랜섬웨어군은 유사한 신규 바이너리 순환을 포함하는 것으로 나타났습니다. 그러나 Locky는 페이로드를 전송하기 위해 더 많은 파일 확장자 및 MIME 조합을 사용합니다.**
- **몇 가지 파일 전송 방법만을 사용하는 악성코드군도 있고 10가지 이상의 방법을 사용하는 악성코드군도 있습니다. 공격자는 장기간에 걸쳐 효율적인 바이너리를 사용하는 경향이 있습니다. 그리고 특정 파일이 단기간 동안 급격하게 사용되다가 빠르게 사라지는 경우도 있는데, 이는 악성코드 개발자들이 전술 전환의 압박을 받고 있음을 나타냅니다.**
- **Adwind RAT 및 Kryptik 악성코드군은 TTD 중앙값이 높은 편입니다. (TTD에 대한 자세한 내용은 33페이지 참조) 이러한 악성코드군의 경우 파일 사용 기간도 더욱 다양합니다. 이는 공격자들이 탐지가 어려운 것으로 확인된 효율적인 바이너리를 재사용했음을 나타냅니다.**
- **Dridex 악성코드군의 파일 사용 기간을 살펴보면 이전에는 널리 사용되었던 이 금융 트로이 목마를 더 이상 사용하지 않는 것으로 보입니다. 2016년 말에는 Dridex 탐지량이 줄어들었으며 이 악성코드를 전송하는 새로운 바이너리의 개발도 감소했습니다. 이 트렌드는 Dridex 악성코드 개발자들이 더 이상 이 위협을 발전시킬 가치가 없다고 판단했거나, 탐지하기가 더 어려운 새로운 방식으로 해당 악성코드를 패키징했음을 나타냅니다.**

TTE 및 TTD

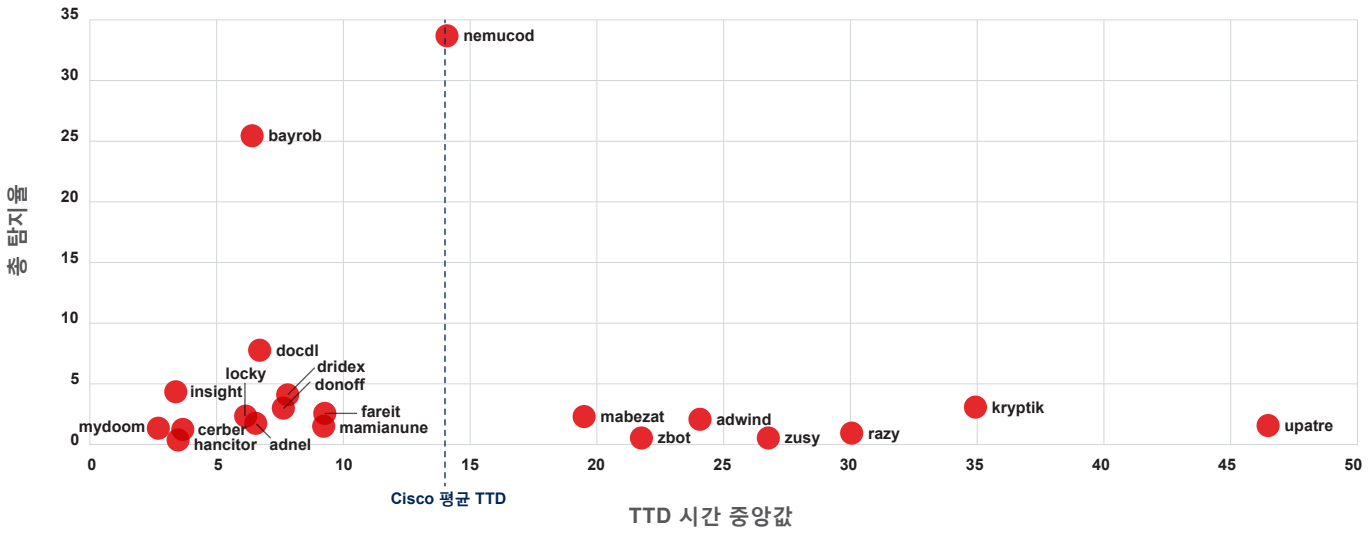
그림 24에는 Cisco의 TTE 조사에서 분석한 6개 악성코드군이 나와 있습니다. 이 차트에서는 Cisco 연구 팀이 2015년 11월부터 2016년 11월까지 관찰한 상위 20개 악성코드군을 탐지 수별로 보여 줍니다. 해당 기간 동안의 평균 TTD 중앙값은 약 14시간이었습니다. (TTD 계산 방식에 대한 자세한 내용은 **33페이지** 참조)

Cisco 제품이 TTD 중앙값 이내에 탐지하는 대다수의 악성코드군은 빠르게 확산되므로 보다 널리 활용되는 산업화된 위협입니다. 랜섬웨어 유형인 Cerber 및 Locky를 예로 들 수 있습니다.

공격자들이 거의 또는 전혀 발전시키지 않았지만 널리 퍼져있는 위협 역시 대개 TTD 중앙값 이내에서 탐지됩니다. 이러한 위협의 예로는 Bayrob(봇넷 악성코드), Mydoom(Microsoft Windows에 영향을 주는 컴퓨터 웜), Dridex(금융 트로이 목마) 등의 악성코드군이 있습니다.

다음 섹션에서는 Locky, Nemucod, Adwind RAT 및 Kryptik 악성코드군의 TTE와 TTD에 대한 주요 연구 결과를 소개합니다. Cerber 및 Dridex와 관련하여 확인된 상세한 결과는 부록(**78페이지**)에 포함되어 있습니다.

그림 24 상위 악성코드군의 TTD 중앙값(탐지 횟수를 기준으로 한 상위 20개 악성코드군)



출처: Cisco Security Research

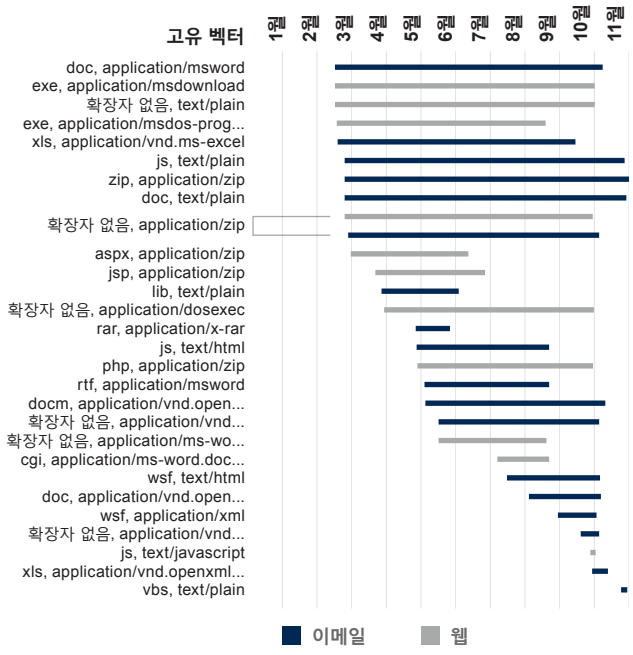
TTE 분석: Locky

Cisco는 TTE 연구를 통해 Locky와 Cerber가 제한된 수의 파일 확장자 및 MIME 조합을 사용하여 웹이나 이메일을 통해 악성코드를 전송함을 확인했습니다(**그림 25** 참조). 이 연구에서는 Microsoft Word 관련 파일 콘텐츠 유형(msdownload, ms-word)을 포함하는 다양한 조합을 관찰했습니다. 그러나 관련 파일 확장자(.exe 및 .cgi)가 Word 파일을 다시 가리키지는 않았습니다. Cisco는 또한 악성 .zip 파일을 가리킨 콘텐츠 유형도 파악했습니다.

Locky 및 Cerber는 파일 기반 탐지를 피하기 위해 새로운 바이너리를 빈번하게 사용하는 것으로 보입니다. Locky 악성코드군의 파일 사용 기간은 **그림 26**에 나와 있습니다. 차트 위쪽에는 특정 달에 관찰된 파일 사용 기간이 나와 있고, 아래쪽에는 새로 관찰된 파일과 이전에 관찰된 파일에서 Locky 관련 해시 볼륨의 월별 변화가 나와 있습니다.

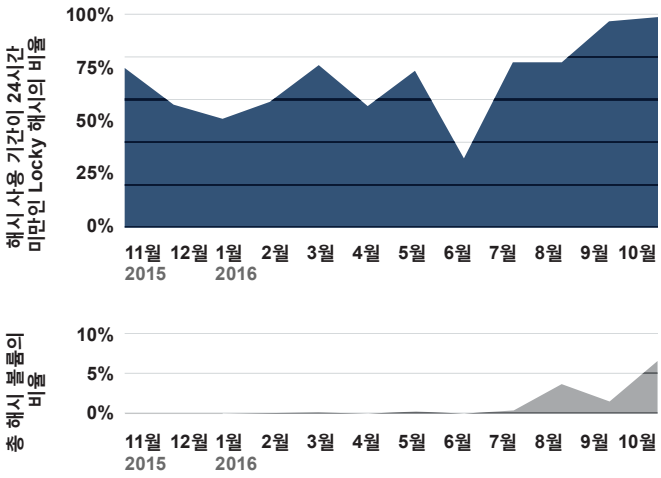
그림 26에서는 파일 볼륨과 파일 사용 기간 분포가 6월에 감소했다는 점도 확인할 수 있습니다. Locky를 제공하는 것으로 알려진 Necurs 봇넷은 6월에 활동을 중단했습니다. 이로 인해 악성코드 개발자가 악성코드를 최신 상태로 유지하는 작업을 수행하지 못한 것으로 보입니다. 하지만 Necurs 봇넷은 바로 복구되었습니다. 이에 7월에 해당 악성코드는 표준 파일 사용 기간 조합으로 다시 돌아왔으며, 대다수의 파일(74%)은 처음 탐지될 때 사용 기간이 1일 미만이었습니다.

그림 25 Locky 페이로드를 발생시키며 Locky 페이로드를 포함하는 위협 및 지표군의 파일 확장자 및 MIME 조합(웹 및 이메일 벡터)



출처: Cisco Security Research

그림 26 별로 관찰된 Locky 악성코드군의 해시 사용 기간 및 총 해시 볼륨의 비율



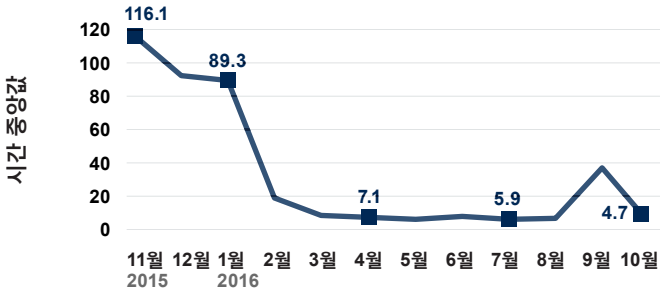
출처: Cisco Security Research

공유

이 랜섬웨어의 빠른 바이너리 순환은 당연한 현상이라 할 수 있습니다. Locky 및 Cerber 인스턴스는 도입된 당일이나 1~2일 후에 탐지되는 경우가 많으므로, 공격자는 위협을 활성 상태로 유지하고 효율성을 높이기 위해 위협을 지속적으로 발전시켜야 하기 때문입니다. 앞에서도 언급한 것처럼, **그림 24**에는 Cisco 제품이 2016년의 TTD 중앙값 이내에 Locky 및 Cerber 랜섬웨어를 모두 탐지한 사실이 나와 있습니다.

그림 27은 Locky 랜섬웨어의 TTD 중앙값을 보여 줍니다. 2015년 11월에는 이 수치가 약 116시간이었는데 2016년 10월에는 5시간 미만으로 대폭 감소했습니다.

그림 27 Locky 악성코드군의 TTD

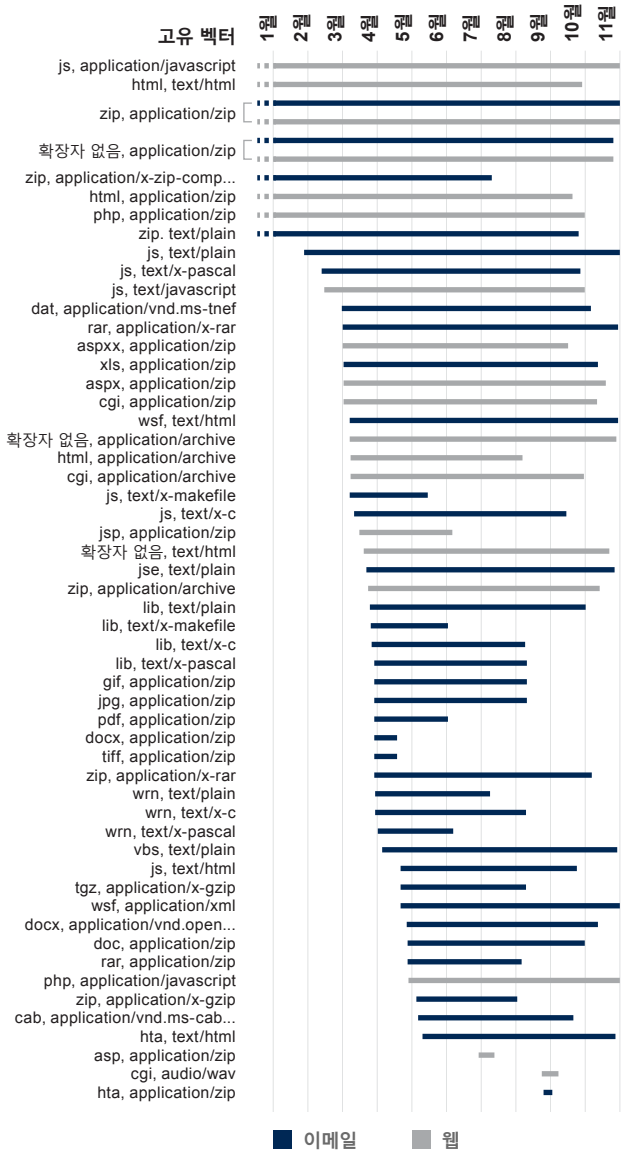


출처: Cisco Security Research

TTE 분석: Nemucod

그림 24에 나와 있는 상위 20개 악성코드군 중에서 Nemucod는 2016년에 가장 자주 탐지된 악성코드였습니다. 공격자는 이 다운로더 악성코드를 사용하여 백도어 트로이 목마(클릭 유도를 용이하게 할 수 있는)같은 기타 위협과 랜섬웨어를 배포합니다. 일부 Nemucod 변종은 Nemucod 악성코드 페이로드를 전송하기 위해 사용됩니다.

그림 28 Nemucod의 파일 확장자 및 MIME 조합(웹 및 이메일 벡터)



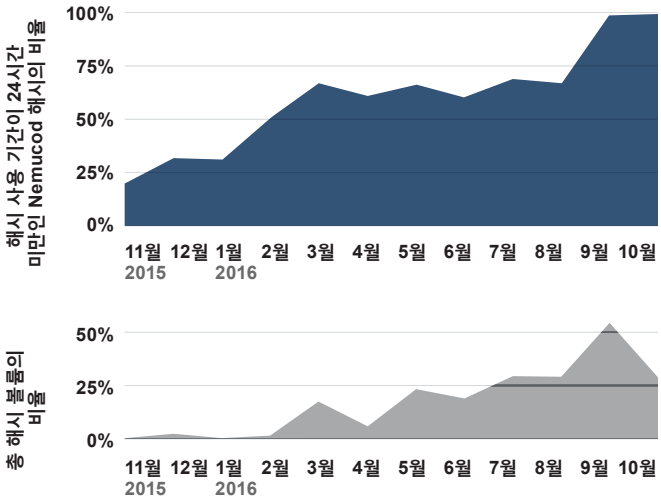
출처: Cisco Security Research

Cisco 위협 연구진에 따르면, Nemucod 악성코드가 2016년에 매우 광범위하게 사용되었던 이유 중 하나는 이 악성코드의 개발자들이 해당 위협을 지속적으로 발전시켰기 때문입니다. Cisco는 Nemucod 악성코드군과 연관된 15가지 이상의 파일 확장자 및 MIME 조합이 웹 상에서 악성코드를 전송하는 데 사용되었음을 파악했습니다. 그리고 더욱 많은 조합이 이메일을 통해 사용자에게 위협을 전송하는 데 사용되었습니다(**그림 28**).

다수의 파일 확장자 및 MIME 조합(웹 및 이메일)은 사용자에게 악성 .zip 파일 또는 아카이브를 안내하도록 설계되었습니다. 또한, 공격자는 관찰 기간 동안 여러 가지 조합을 재사용했습니다.

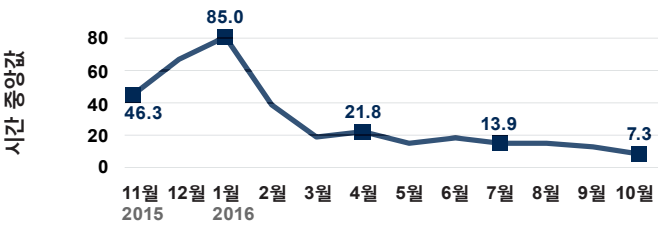
그림 29에 나와 있는 것처럼, 대다수의 Nemucod 해시는 탐지 당시 사용 기간이 2일 미만이었습니다. 2016년 9월과 10월에 차단되었던 Nemucod 악성코드군과 관련된 거의 모든 바이너리의 사용 기간은 1일 미만이었습니다.

그림 29 월별로 관찰된 Nemucod 악성코드군의 해시 사용 기간 및 총 해시 볼륨의 비율



출처: Cisco Security Research

그림 30 Nemucod 악성코드군의 TTD



출처: Cisco Security Research

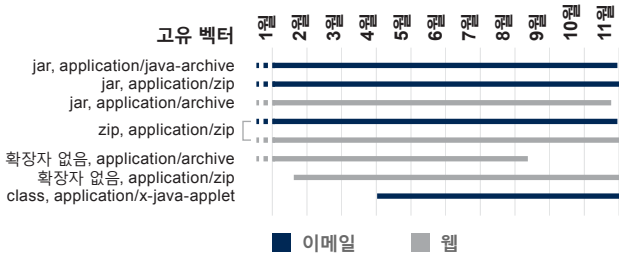
TTE 분석: Adwind RAT

Cisco 위협 연구진에 따르면, Adwind RAT(원격 접속 트로이 목마) 악성코드는 .zip 또는 .jar 파일을 포함하는 파일 확장자 및 MIME 조합을 통해 전송된다고 합니다. 이러한 방식은 악성코드가 전송되는 수단(이메일 또는 웹 공격 벡터)에 관계없이 적용됩니다(**그림 31** 참조).

Adwind RAT는 2016년에 매우 다양한 사용 기간의 해시를 사용했습니다. 단, 9월과 10월에는 확인된 대다수 파일의 사용 기간이 1~2일이었습니다(**그림 32**).

또한, Adwind RAT의 TTD 중앙값은 분석 대상이었던 기타 악성코드군의 TTD 중앙값에 비해 지속적으로 높게 나타났습니다(**그림 33**). 이는 악성코드 개발자들이 탐지하기 어려운 전송 메커니즘을 개발했기에 Adwind RAT의 공격이 계속 성공했던 것으로 보입니다. 따라서 다른 악성코드군 개발자들처럼 빠르게 또는 빈번하게 새로운 해시를 순환할 필요가 없었던 것입니다. Adwind 트로이 목마는 JSocket, AlienSpy 등의 다른 이름으로도 알려져 있습니다.

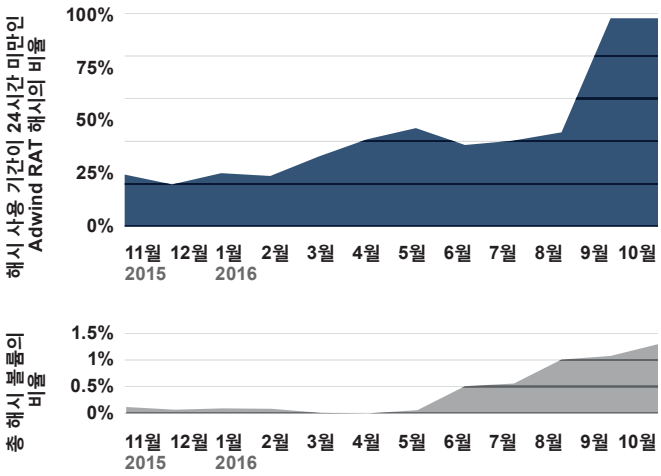
그림 31 Adwind RAT의 파일 확장자 및 MIME 조합(웹 및 이메일 벡터)



출처: Cisco Security Research

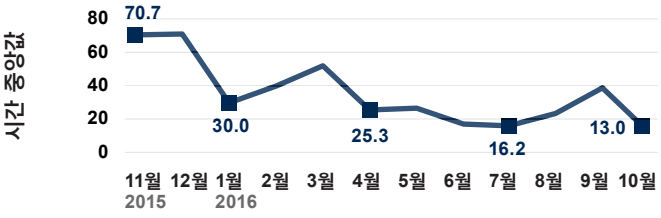
2017년 그래픽 다운로드: www.cisco.com/go/acr2017graphics

그림 32 월별로 관찰된 Adwind RAT 악성코드군의 해시 사용 기간 및 총 해시 볼륨의 비율



출처: Cisco Security Research

그림 33 Adwind RAT 악성코드군의 TTD



출처: Cisco Security Research

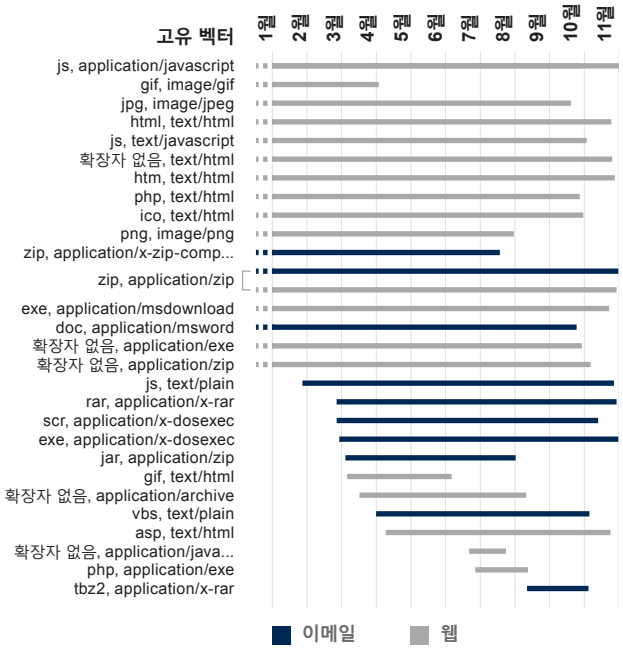
TTE 분석: Kryptik

Adwind RAT 악성코드와 같이 Kryptik는 Cisco에서 2015년 11월부터 2016년 10월까지 분석한 다른 악성코드군보다 TTD 중앙값이 지속적으로 높게(약 20시간) 나타났습니다(**그림 36**). 그러나 10월에 Cisco 제품은 Kryptik 악성코드의 TTD 중앙값을 9시간 미만으로 단축했습니다(**그림 36**).

Kryptik 악성코드군 역시 분석 대상이었던 다른 악성코드군에 비해 특히 2016년 상반기에 다양한 해시를 사용했습니다. Kryptik 개발자들이 이처럼 오랜 기간 동안 오래된 해시를 사용할 수 있었던 것은 방어자들이 이 악성코드 유형을 탐지하기 힘들었다는 사실을 시사합니다.

관찰 대상 기간 동안 Kryptik 개발자들은 웹 공격 벡터를 통해 폭넓은 페이로드 전송 방법을 활용했습니다. 그리고 웹 및 이메일 둘 다에 대해 파일 확장자 및 MIME 조합에서 .zip 파일과 같은 JavaScript 파일 및 아카이브 파일을 사용했습니다(**그림 34** 참조). 일부 조합의 경우 2011년에 개발된 것도 있었습니다.

그림 34 Kryptik의 파일 확장자 및 MIME 조합(웹 및 이메일 벡터)

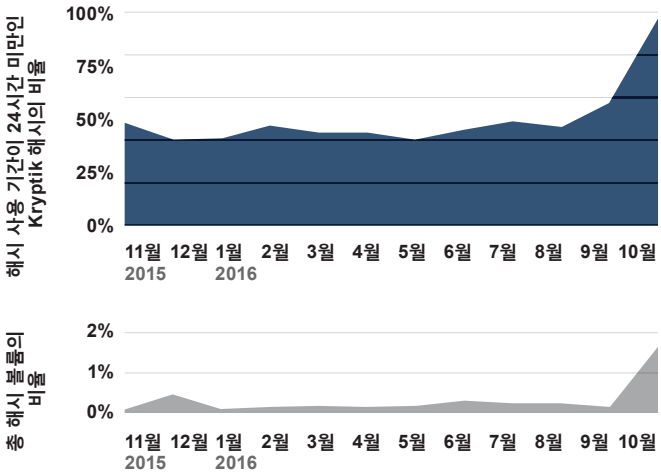


출처: Cisco Security Research

6가지 악성코드군을 분석한 결과, 공격자들은 전술을 빈번하게 전환해야 한다는 점을 알 수 있었습니다. 성공적으로 활동할 수 있는 기간이 단기간에 그치기 때문에 이를 활용해야 했던 것입니다. 이는 방어자들의 악성코드 탐지 능력이 위협이 진화한 후에도 향상되고 있음을 나타냅니다. 따라서 공격자는 탐지를 피하고 지속적으로 수익을 창출할 수 있는 새로운 공격 방식을 찾아내야 한다는 부담을 느끼고 있습니다.

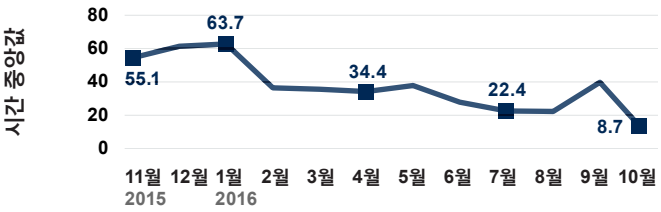
이처럼 빠르게 진화하며 모든 악성코드군이 각기 다른 방식으로 행동하는 복잡한 위협 환경에서 전문가의 지식과 포인트 솔루션만으로는 위협을 빠르게 식별하고 대응할 수 없습니다. 즉, 위협에 대한 실시간 인사이트를 제공하는 통합 보안 아키텍처와 자동화된 탐지 및 방어 기능을 함께 사용해야 TTD를 개선하고 감염 발생 시 신속하게 치료할 수 있습니다.

그림 35 월별로 관찰된 Kryptik 악성코드군의 해시 사용 기간 및 총 해시 볼륨의 비율



출처: Cisco Security Research

그림 36 Kryptik 악성코드군의 TTD



출처: Cisco Security Research

방어자 행동

방어자 행동

2016년의 취약점 감소 현황

Cisco의 연구 결과에 따르면 2016년 하반기에 벤더가 공개한 취약점은 2015년에 비해 크게 감소했습니다(**그림 37**). **National Vulnerability Database**에서도 이와 유사한 취약점 감소 추세를 확인할 수 있습니다. 공개된 취약점 보고 수의 감소 이유는 명확하지 않습니다.

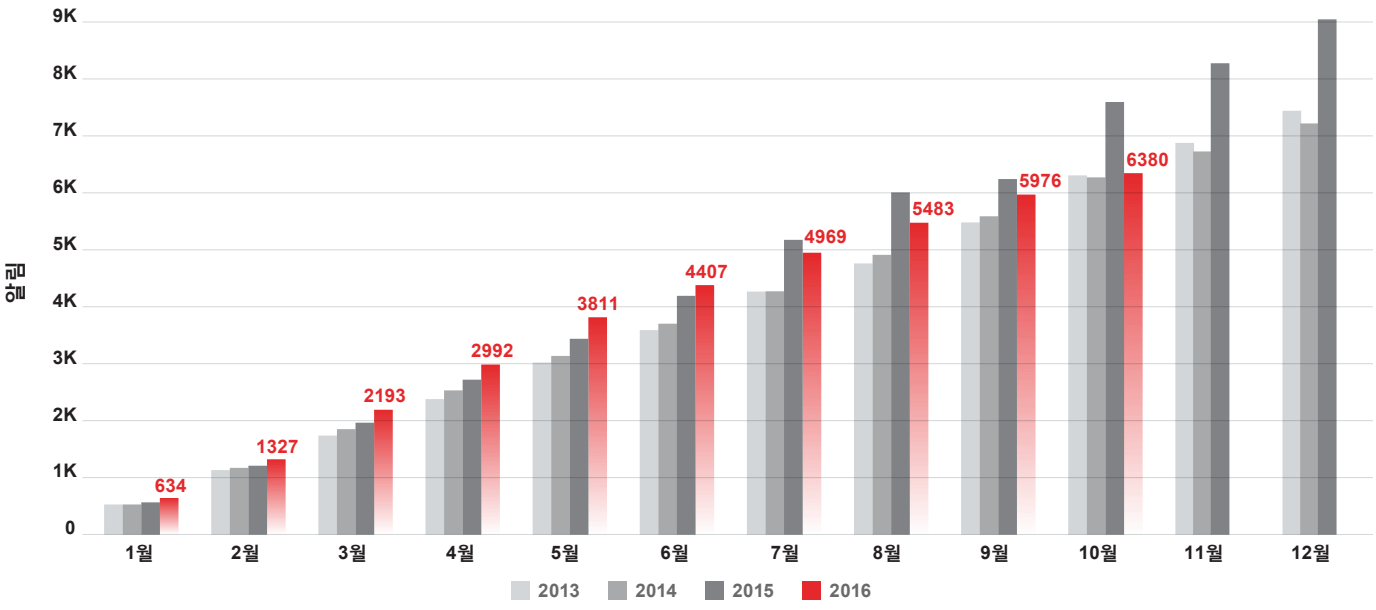
2015년은 취약점이 비정상적으로 많이 확인된 해였기 때문에 2016년의 수치는 정상적인 취약점 보고 수를 반영하는 것일 수 있습니다. 2015년 1~10월의 총 알림 수는 7,602건이었습니다. 반면 2016년 같은 기간의 총 알림 수는 6,380건이었고 2014년에는 총 알림 수가 6,272건이었습니다.

2015년에 취약점이 많이 보고된 이유는 벤더가 기존 제품과 코드를 보다 면밀하게 확인했고, SDL(secure development lifecycle, 보안 개발 수명 주기) 업무를 더욱 철저하게 구현했으며, 취약점을 식별한 다음 수정했기 때문일 수 있습니다. 보고된 취약점이 감소한 것은 이러한 노력의 결과가 나타난 것이라 할 수 있습니다. 즉, 벤더는 이제 제품이 출시되기 전부터 취약점을 식별하여 수정하는 데 주력하고 있습니다.

2016년에 취약점이 가장 크게 감소한 것으로 나타나는 벤더는 Apple이었습니다. Apple이 보고한 취약점 수는 2015년에는 705건이었던 반면 2016년에는 324건으로 54%나 감소했습니다. 마찬가지로 Cisco가 보고한 취약점 수는 2015년의 488건에서 2016년에는 310건으로 36% 감소했습니다.

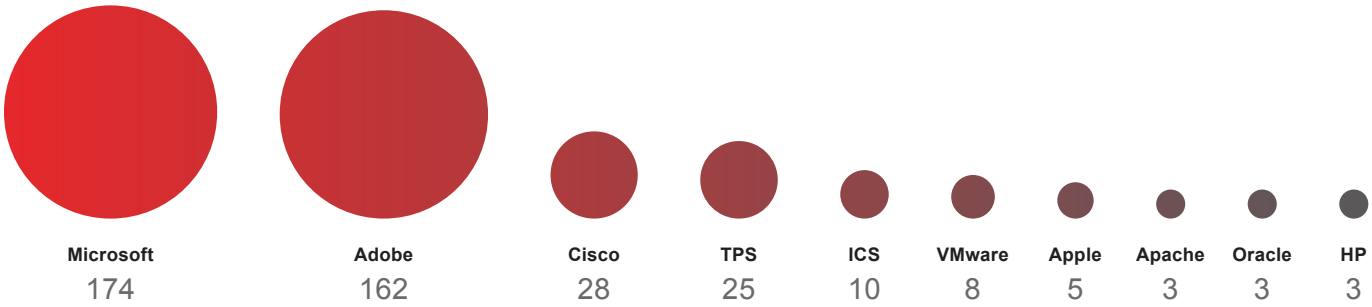
보안 연구 팀에서 흔히 발생하는 문제 중 하나는, 보안 전문가들이 처리해야 하는 취약점 처리 관련 업무가 과도하다는 것입니다. 최근 몇 개월 동안에는 2014년의 Heartbleed 사례에서와 같이 업계 전체에 큰 파란을 일으킨 주요 취약점 관련 발표가 없었습니다. 실제로 Heartbleed의 경우와 같이 "알려진" 취약점과 관련한 과도한 반응과 2015년의 취약점 증가 현상이 모두 취약점 관련 업무 증가에 영향을 주었을 가능성이 높으며, 그렇지 않더라도 최소한 취약점 보고의 필요성 감소에는 영향을 주었음이 분명합니다.

그림 37 연간 누적 알림 합계



출처: Cisco Security Research

그림 38 벤더 및 유형별 중요 취약점 보고



출처: NVD(National Vulnerability Database)

Cisco에서 현재 사용 중인 SIR(Severity/Impact Ratings, 심각도/영향 등급)의 등급 레벨은 "중요", "높음", "중간", "낮음"입니다. 이러한 등급은 CVSS(Common Vulnerability Scoring System)의 간소화된 우선순위 지정 방식을 반영합니다. 또한, Cisco는 CVSS v2.0의 후속 버전인 CVSS v3.0을 도입했습니다. 이러한 변화로 인해 일부 취약점의 경우 이전보다 점수가 높아졌으므로 보안 전문가가 취약점을 확인할 때 등급이 "중간" 및 "낮음" 대신 "중요" 및 "높음"으로 다소 높게 표시될 수도 있습니다. 이러한 배점 방식 변경에 대한 자세한 내용은 Cisco Security 블로그 게시물, The Evolution of Scoring Security Vulnerabilities: The Sequel을 참조하십시오.

Cisco 2017 보안 기능 벤치마크 조사(**49페이지**)에 따르면, 보안 운영 환경 구축에 동의하는 보안 전문가가 다소 감소한 것으로 나타났습니다. 이러한 감소 추세 역시 지속적인 업그레이드 및 패치 구현 필요성에 관한 부담감이 적용됐을 것입니다. 예를 들어 2016년에는 보안 전문가 중 53%가 보안 방식을 정기적, 공식적, 전략적으로 검토하고 개선하는 데 매우 동의한다고 답변한 반면, 2014년과 2015년의 경우 매우 동의한다고 답변한 보안 전문가의 비율은 56%였습니다.

물론 취약점의 감소가 위협 환경에 대한 안일함으로 이어져서는 안 됩니다. 즉, 널리 알려진 취약점이 없더라도 위협에 대한 경계를 늦춰도 된다고 생각해서는 안 됩니다.

이전 보고서에서도 언급했지만, 보안 전문가는 협력을 통한 패치를 우선적으로 적용해야 합니다. 인력과 기타 리소스가 부족하여 사용 가능한 모든 패치를 제때 설치할 수 없는 경우에는 네트워크 안전에 가장 중요한 패치를 평가한 다음 작업 목록에서 해당 패치를 최상위에 배치해야 합니다.

2017년 그래픽 다운로드: www.cisco.com/go/acr2017graphics

그림 39 선별된 중요 취약점 보고

보고 제목	발행일
Adobe Acrobat 및 Acrobat Reader 메모리 손상 코드 실행 취약점	2016년 7월 28일
Adobe Acrobat 및 Acrobat Reader 메모리 손상 원격 코드 실행 취약점	2016년 7월 28일
Adobe Acrobat 및 Acrobat Reader 메모리 손상 취약점	2016년 7월 21일
Adobe Acrobat 및 Acrobat Reader 정수 오버플로 취약점	2016년 5월 23일
Adobe Acrobat 및 Acrobat Reader 메모리 손상 원격 코드 실행 취약점	2016일 2월 8일
Adobe Acrobat 및 Acrobat Reader 메모리 손상 취약점	2016년 7월 28일
Adobe Acrobat 및 Acrobat Reader 메모리 손상 취약점	2016년 7월 18일
Adobe Acrobat 및 Acrobat Reader 메모리 손상 취약점	2016년 7월 23일
Adobe Acrobat 및 Acrobat Reader 메모리 손상 취약점	2016년 5월 24일
Adobe Acrobat 및 Acrobat Reader 메모리 손상 취약점	2016년 5월 23일

출처: Cisco Security Research

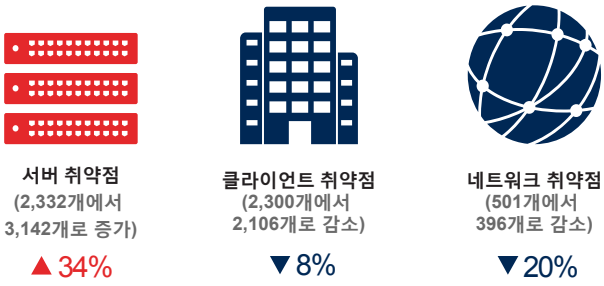
위에 나와 있는 보고는 익스플로잇 코드가 공개적으로 제공되거나 현재 실제로 이용되고 있는 것으로 여러 출처에서 보고된 2016년의 중요 등급 취약점 관련 보고 중 선별된 것입니다.

서버 및 클라이언트 취약점

*Cisco 2016 중기 사이버 보안 보고서*에 설명되어 있는 것처럼, 공격자들은 서버 솔루션 내에서 공격할 수 있는 영역과 시기를 모색합니다. 공격자는 서버 소프트웨어에서 공격을 실행함으로써 더 많은 네트워크 리소스 제어권을 확보할 수 있고 다른 중요 솔루션으로 내부 이동할 수도 있습니다.

Cisco 연구 팀은 벤더별 클라이언트 및 서버 취약점을 추적했습니다(**그림 40**).

그림 40 클라이언트-서버 취약점 구분(2015~2016년)



출처: National Vulnerability Database

미들웨어: 패치가 적용되지 않은 소프트웨어에서 기회를 모색하는 공격자

*Cisco 2016 중기 사이버 보안 보고서*에는 서버 시스템에 대한 공격 관련 데이터가 포함되어 있습니다. 2017년에는 공격자들이 방어자의 대응 및 인식 속도가 느린 미들웨어, 즉 플랫폼이나 애플리케이션을 연결해주는 곳을 공격 지점으로 모색할 가능성이 높습니다.

Cisco 연구 팀은 서드파티 소프트웨어의 취약점을 찾는 과정에서 매월 소프트웨어별로 평균 14개의 신규 취약점을 확인했습니다. 이러한 취약점 중 대부분(62개)은 미들웨어 사용으로 인한 것이었습니다. 이 62개 취약점 중 20개는 PDF를 처리하는 코드 내에서, 12개는 이미지를 처리하는 코드에서, 10개는 흔히 사용되는 사무 생산성 솔루션용 코드에서, 9개는 압축용 코드에서, 그리고 11개는 기타 라이브러리에서 발견되었습니다(**그림 41**).

미들웨어에 취약점이 있으면 고유한 보안 위협이 발생합니다. 미들웨어의 라이브러리는 대개 클라이언트 대상 소프트웨어(즉 생산성 솔루션과 같이 사용자가 일상적으로 직접 상호작용하는 소프트웨어)처럼 신속하게 업데이트되지 않기 때문입니다. 미들웨어 라이브러리는 소프트웨어 감사에서 제외될 수 있으므로 취약점이 그대로 유지됩니다.

그림 41 미들웨어 라이브러리에서 확인된 취약점

출처: Cisco Security Research

공유

조직은 미들웨어가 위험 부담이 있음에도 불구하고 안전한 것으로 생각하여 솔루션 업데이트에 주력할 수도 있습니다. 그러나 아직은 알려지지 않은 미들웨어 경로로 공격자들이 침입할 가능성이 낮다는 가정은 틀릴 수 있습니다. 따라서 미들웨어는 방어자들의 보안 사각 지대가 되는 동시에 공격자들에게는 공격 기회를 제공하게 됩니다.

미들웨어 라이브러리 업데이트 관련 당면 과제는 ***Cisco 2015 중기 보안 보고서***에서 설명하는 오픈 소스 소프트웨어 문제와 밀접하게 관련되어 있습니다. 대다수의 미들웨어 솔루션은 오픈 소스 개발자가 제공하는 것이기 때문입니다. 그러나 현재 발생하고 있는 문제는 오픈 소스 개발자와 전용 미들웨어 개발자에게 모두 영향을 줄 수 있습니다. 그러므로 대부분의 개발자는 미들웨어 라이브러리를 지속적으로 업데이트해야 합니다. 과중한 업무에 시달리고 있는 IT 또는 보안 팀이 관리해야 하는 작업 중 미들웨어 라이브러리 업데이트의 우선순위는 높지 않을 수도 있지만, 이러한 업데이트에 더욱 신경 써야 합니다.

다음으로는 공격자가 미들웨어 취약점을 공격하는 경우의 잠재적 영향에 대해 살펴보겠습니다. 이메일이나 메시징과 같은 기타 중요 시스템과 미들웨어가 서로 연결되는 경우 공격자는 이러한 시스템으로 내부 이동하여 피싱 메시지나 스팸을 전송할 수 있습니다. 또는 인증된 사용자로 가장하여 사용자 간의 신뢰 관계를 악용해 추가 액세스 권한을 획득할 수도 있습니다.

미들웨어 취약점을 통해 실행되는 공격의 피해를 입지 않으려면 다음과 같은 조치를 취해야 합니다.

- **사용 중인 애플리케이션에서 알려진 종속성 및 라이브러리 목록을 적극적으로 유지 보수**
- **이러한 애플리케이션의 보안을 적극적으로 모니터링하고 위험을 최대한 차단**
- **소프트웨어 벤더와의 계약에 패치를 제때 제공하기 위한 서비스 레벨 계약 삽입**
- **소프트웨어 종속성 및 라이브러리 사용을 정기적으로 감사 및 검토**
- **소프트웨어 벤더에 제품 유지 보수 및 테스트 방법에 대한 세부사항 요청**

요약하자면, 패치 적용이 지연될수록 공격자가 공격할 수 있는 영역은 늘어나며 중요 시스템 제어권을 확보할 수 있는 시간도 길어집니다. 다음 섹션에서는 웹 브라우저 등 흔히 사용되는 솔루션의 패치 적용과 영향 및 트렌드에 대해 설명합니다.

패치 적용까지 걸리는 시간: 복구 기간 단축

대부분의 사용자는 패치를 제때 다운로드하여 설치하지 않습니다. 공격자는 이처럼 패치가 적용되지 않은 취약점을 이용하여 네트워크에 진입할 수 있습니다. 최신 연구 결과에 따르면, 효과적인 사용자의 패치 다운로드 및 설치 장려 방안은 벤더가 소프트웨어 업데이트를 정기적으로 제공하는 것입니다.

보안 패치가 릴리스된다는 것은 공격자가 공격할 수 있는 취약점이 있음을 명확하게 나타내기 때문입니다. 수준 높은 공격자들은 해당 취약점을 일정 시간 동안 공격해 왔을 가능성이 높지만, 대다수의 공격자들은 패치 알림이 제공되면 이전 버전을 공격할 수 있음을 알게 됩니다.

소프트웨어 벤더가 정기 일정에 따라 새 버전을 릴리스하면 사용자는 규칙적으로 업데이트를 다운로드하여 설치할 수 있습니다. 반면 벤더 업그레이드 릴리스 일정이 규칙적이지 않으면 사용자가 업그레이드를 설치할 가능성은 낮아집니다. 따라서 공격 가능한 취약점이 포함되어 있을 수 있는 오래된 솔루션을 계속 사용하게 됩니다.

업그레이드 주기에 영향을 주는 또 다른 행동은 다음과 같습니다.

- **알림 환경의 작동 수준**
- **옵트아웃(사후 수신 거절)의 편의성 수준**
- **소프트웨어 사용 빈도**

벤더 측이 릴리스한 업그레이드를 사용자가 설치할 때까지의 기간은 각기 다릅니다. Cisco 연구 팀은 고객의 엔드포인트에 설치되는 소프트웨어를 확인했습니다. 고객의 소프트웨어는 아래의 3가지 범주로 구분되었습니다.

- **새 버전:** 엔드포인트가 사용 가능한 최신 버전 소프트웨어를 실행함
- **최근 버전:** 엔드포인트가 최신 버전이 아닌 이전 3개 버전 소프트웨어 중 하나를 실행함
- **오래된 버전:** 엔드포인트가 최신 릴리스로부터 4개 버전 이상 지난 소프트웨어를 실행함

예를 들어 소프트웨어 벤더가 2017년 1월 1일에 버전 28을 릴리스한 경우에는 버전 28이 새 버전, 버전 26이 최근 버전, 버전 23이 오래된 버전입니다. 다음 페이지의 그림에는 하나 이상의 소프트웨어 버전이 릴리스된 주 단위 기간을 나타내는 설명선이 포함되어 있습니다.

Adobe Flash 사용자에 대한 조사(**그림 42**)에서는 업데이트가 릴리스된 첫 주에 거의 80%의 사용자가 최신 버전의 소프트웨어를 설치한 것으로 확인되었습니다. 즉, 사용자층이 최신 버전을 설치하여 작업 속도를 높이는 데 소요된 시간은 약 1주에 불과했습니다. 이 1주 동안의 "복구" 기간은 해커가 공격할 수 있는 기회이기도 합니다.

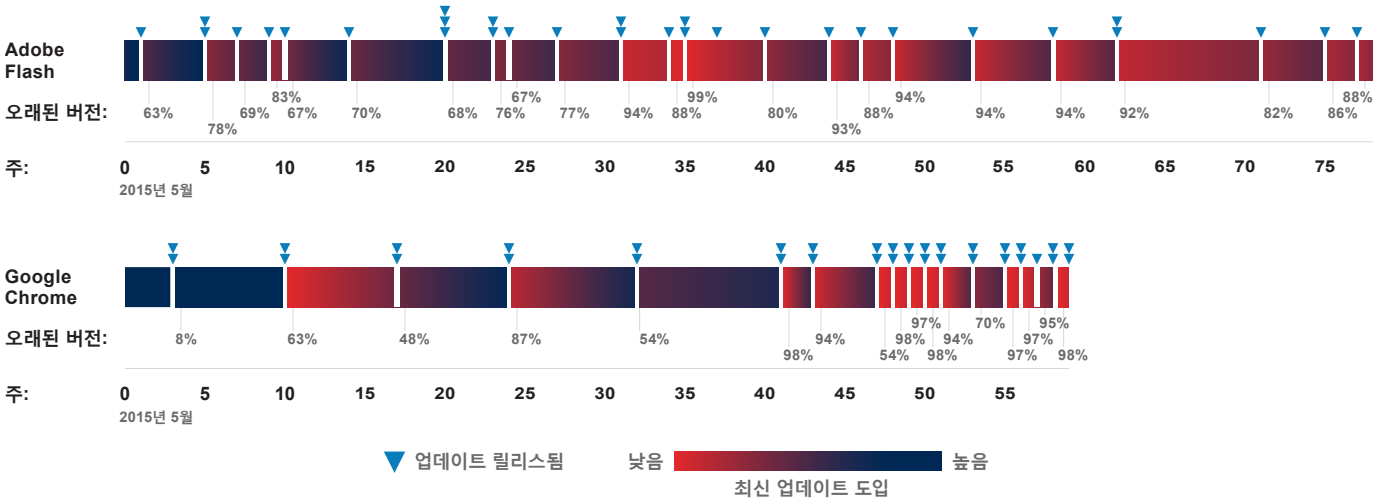
반면 Adobe Flash 그래픽의 2015년 4분기 말을 살펴보면 최신 버전의 솔루션 사용자 수가 급격히 감소함을 확인할 수 있습니다. 조사 기간 동안 Adobe는 다양한 추가 기능, 버그 수정, 보안 업데이트가 포함된 5개 Flash 버전을 빠른 속도로 끊임 없이 릴리스했습니다. 이처럼 업데이트가 많이 릴리스되면 사용자가 혼란을 느낄 수 있습니다. 즉, 사용자는 과연 그렇게 많은 업데이트를 다운로드해야 하는지 의문을 느낄 수도 있고, 업그레이드 알림 수가 과도한 탓에 모두 확인하기 어려울 수 있습니다. 심지어 중요 업데이트를 이미 다운로드했다고 생각하여 새 알림을 무시할 수도 있습니다. 사용자가 업데이트 설치를 간과하는 요인이 무엇이든, 방어자들에게는 불리한 환경이 조성되는 것입니다.

Google Chrome 웹 브라우저의 업그레이드를 조사하는 과정에서는 다른 패턴이 확인되었습니다. 이 패턴은 정기적인 업그레이드와 사용자가 업데이트 알림을 무시하기 어렵게 만드는 강력한 옵트아웃(사후 수신 거절) 정책을 반영합니다. **그림 42**에 나와 있는 것처럼, 최신 버전을 실행하는 엔드포인트의 수는 장기간 비교적 일정하게 유지되었습니다.

Chrome 데이터에 따르면 사용자의 복구 속도도 다소 빠른 것으로 나타났습니다. 정기 업데이트의 경우 복구 타임라인은 대략 1주일입니다. 그러나 2016년 2분기와 3분기에 걸친 9주 동안에는 7개의 업데이트가 릴리스되었습니다. 이 기간에 사용자층의 복구는 완료되었지만 업그레이드 메시지 확인 부담은 증가했습니다. 이로 인해 대다수의 사용자층이 복구를 마쳤음에도 이전 버전을 계속 사용하는 사용자의 비율 또한 꾸준히 높아졌습니다.

Mozilla의 Firefox 브라우저도 정기 일정에 따라 업데이트를 제공하지만, 업데이트가 릴리스된 후의 복구 기간은 최대 1개월까지 걸린 것으로 나타났습니다. 다시 말해, Firefox 사용자는 Chrome 사용자들처럼 업데이트를 자주 다운로드하여 설치하지 않는 것입니다. 그 이유 중 하나는 일부 사용자가 브라우저를 규칙적으로 사용하지 않아 업데이트를 확인 및 다운로드하지 않기 때문일 수 있습니다(다음 페이지의 **그림 43** 참조).

그림 42 Adobe Flash 및 Google Chrome의 패치 적용 시간



출처: Cisco Security Research

공유

Firefox는 대개 격주 단위로 버전을 업데이트했으며 관찰 기간 동안 업데이트 빈도는 갈수록 잦았습니다. 이처럼 업데이트 빈도가 누적됨에 따라 사용자층 내에서 이전 Firefox 버전 사용자도 증가했습니다. 복구 기간은 약 1.5주였지만 이 기간은 중복 계산된 것입니다. 최신 버전을 유지하려는 사용자 수는 사용자층의 30%까지 떨어졌습니다. 특정 시점에서는 최신 버전보다 5개 이상 이전의 버전을 계속 실행하는 사용자가 2/3나 되었습니다. 즉, Firefox는 신속하게 문제를 해결하고 버그를 수정하지만 사용자층은 그와 동일한 빈도로 브라우저를 업데이트하거나 재시작 하지는 않습니다.

소프트웨어의 경우에는 사용 수준이 취약점을 나타낸다고도 할 수 있습니다. 사용자가 소프트웨어에 자주 액세스하지 않아 소프트웨어를 패치하고 업그레이드할 필요성을 느끼지 못하면, 공격자가 공격할 수 있는 영역과 시간이 늘어납니다.

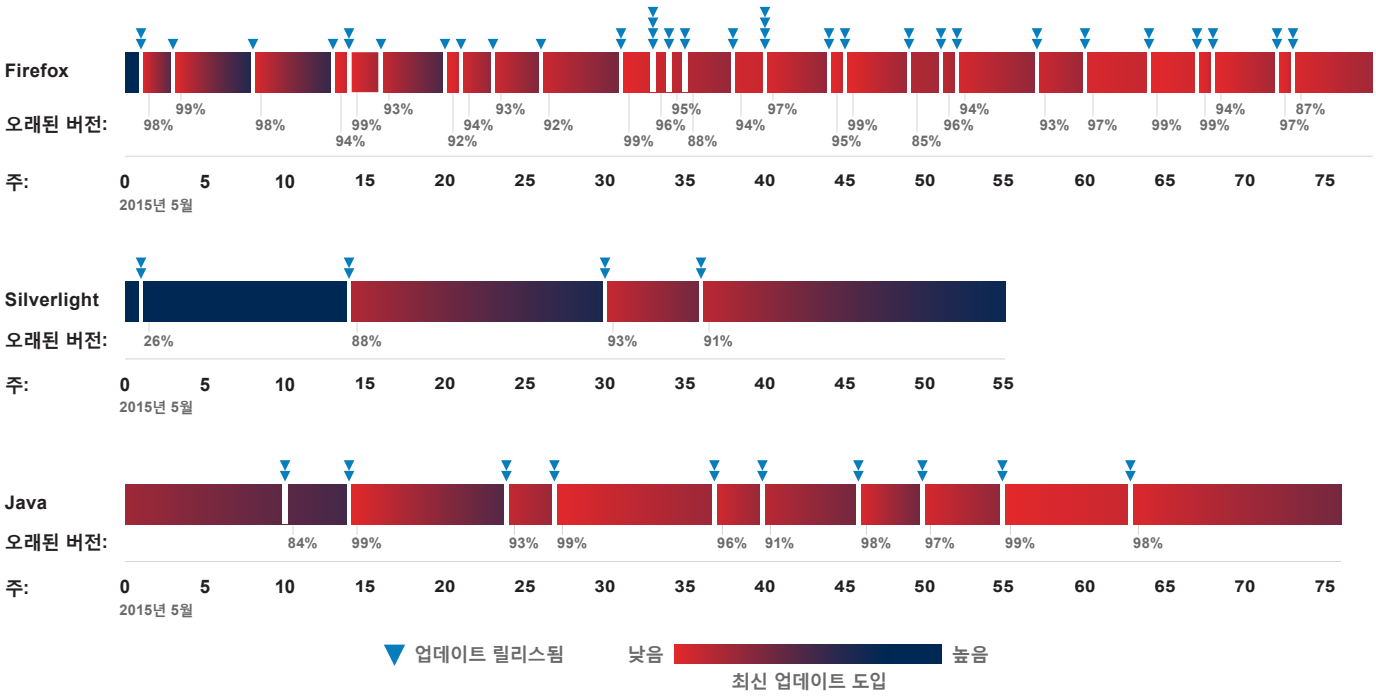
Microsoft Silverlight에 대한 연구에서는 이러한 상황을 확인할 수 있으며, 릴리스 이후에 사용자가 업그레이드를 설치하는 복구 기간이 최대 2개월까지 걸리는 것으로 나타났습니다. 2015년 4분기와 2016년 1분기 사이의 기간에 확인할 수 있는 것처럼, 특정 시점에서는 5주 동안 2개 버전이 릴리스되어 3개월이 넘는 기간 동안 사용자층에게 영향을 주기도 했습니다.

Microsoft는 2012년에 Silverlight의 단종을 발표했지만 패치와 버그 수정은 지속적으로 릴리스되고 있습니다. 하지만 이로 인해 Internet Explorer와 동일한 문제가 발생하고 있습니다. 패치가 적용되지 않은 오래된 소프트웨어는 공격자가 쉽게 공격할 수 있는 것입니다.

Java 사용자의 복구 기간을 확인한 결과, 대부분의 사용자는 최신 릴리스에서 1~3개 이전 버전 소프트웨어를 사용하고 있었습니다. 복구 시간은 약 3주입니다. Java의 특이한 패턴은, 대다수의 사용자층이 최근 버전을 사용한다는 것입니다. Java 업데이트 주기는 1~2개월입니다.

결국 패치 적용까지 소요되는 시간 전반에 걸쳐 확인할 수 있는 사항은 두 가지 입니다. 업그레이드 릴리스 패턴이 사용자 보안 상태에 영향을 줄 수 있으며, 네트워크 역시 위험하게 만든다는 점입니다.

그림 43 Firefox, Silverlight 및 Java의 패치 적용 시간



출처: Cisco Security Research

2017년 그래픽 다운로드: www.cisco.com/go/acr2017graphics

Cisco 2017 보안 기능 벤치마크 조사

Cisco 2017 보안 기능 벤치마크 조사

보안 전문가의 조직 내 보안 상태 인식을 평가하기 위해 Cisco는 여러 국가와 조직에 소속된 CSO(Chief Security Officer, 최고 보안 책임자) 및 보안 업무(SecOps) 관리자에게 해당 조직의 보안 리소스와 절차에 대해 질문했습니다. Cisco 2017 보안 기능 벤치마크 조사에서는 현재 사용되고 있는 보안 업무 및 보안 방식의 성숙도에 대한 인사이트를 제공하고, 그 결과와 2016년 및 2015년 보고서의 결과를 비교하고 있습니다. 이 조사는 13개국의 2,900명이 넘는 응답자를 대상으로 진행되었습니다.

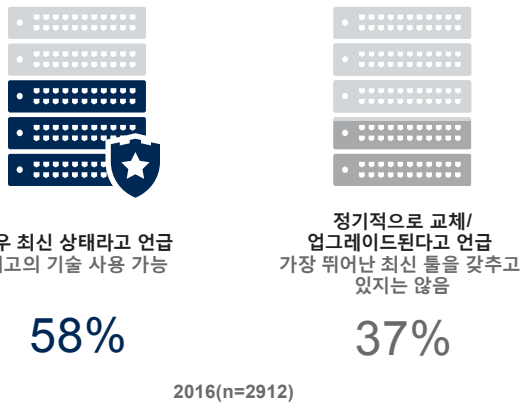
보안 전문가는 공격자의 복잡한 위협 환경과, 공격 영역을 확장하려는 시도에 대응하는 방식으로 조직의 보안을 강화하고자 합니다. 많은 조직이 여러 벤더가 제공하는 다양한 솔루션을 사용합니다. 이러한 전술은 인터넷 속도를 상승시키지만, 연결되는 디바이스와 트래픽이 증가하여 보안 대상 네트워크가 상당히 복잡해지거나 혼란을 초래합니다. 따라서 자체 네트워크를 보호하려는 조직은 단순한 환경과 통합 솔루션 도입을 목표로 해야 합니다.

인식: 툴은 확실히 신뢰하지만 현재 해당 툴이 효과적인지는 확신할 수 없는 보안 전문가

대부분의 보안 전문가는 현재 적절한 솔루션을 보유하고 있으며 보안 인프라가 최신 상태라고 생각합니다. 그러나 Cisco의 조사에 따르면 이러한 신뢰는 다소 불확실한 것으로 나타났습니다. 즉, 이러한 전문가들이 주어진 예산과 인력을 활용하여 현재 보유하고 있는 기술을 항상 효율적으로 활용한다고 확신할 수 없는 것입니다.

조직에 대한 위협은 다각도로 유입됩니다. 공격자들은 독창적이며 신속한 방식을 활용해 방어 기능 회피를 시도할 수 있습니다. 이처럼 항상 경계를 늦춰서는 안 되는 환경이지만 대다수의 보안 전문가들은 보안 인프라가 최신 상태라고 신뢰하고 있습니다. 다만 이러한 신뢰도가 몇 년 전에 비해 다소 낮아지기는 했습니다. 2016년에는 응답자의 58%가 자사의 보안 인프라가 최신 상태이며 최신 기술을 통해 꾸준히 업그레이드되고 있다고 답했습니다. 그리고 37%는 보안 기술을 정기적으로 교체하거나 업그레이드하고는 있지만 가장 뛰어난 최신 툴을 갖추고 있지는 않다고 답했습니다(**그림 44**).

그림 44 자사의 보안 인프라가 최신 상태라고 생각하는 보안 전문가의 비율



출처: Cisco 2017 보안 기능 벤치마크 조사

그러나, 2/3가 넘는 보안 전문가가 자사의 보안 툴이 매우 효과적이거나 최고로 효과적이라고 생각하고 있습니다. 예를 들어, 자사의 툴이 보안 위협 차단 효과에 매우 혹은 가장 뛰어나다고 생각하는 보안 전문가가 74%에 달하며, 자사의 툴이 대응형 위협 방식으로 변화하는 공격을 동적으로 방어하고 네트워크 이상 징후를 탐지하는 데 효과적이라고 응답한 비율도 71%입니다(**그림 45**).

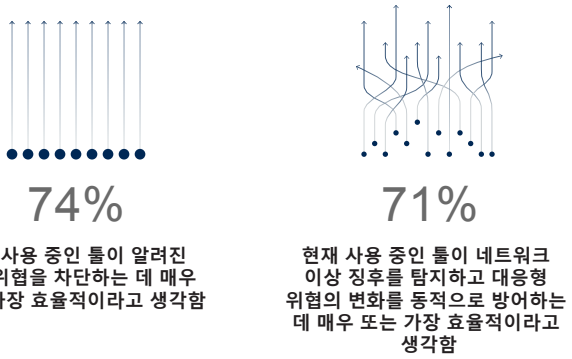
문제는 툴을 신뢰한다고 해서 효율적으로 보안할 수 있다는 뜻은 아니라는 겁니다. 조사 결과에서도 확인할 수 있듯이, 보안 부서는 여러 벤더의 복잡한 툴을 사용하는 데 어려움을 겪고 있으며 인력도 부족한 상황입니다. 이러한 상황을 요약하자면 "의도와 현실의 차이" 문제라 할 수 있습니다. 보안 전문가는 단순하고 효과적인 보안 툴을 사용하고자 하지만 실제로 이러한 비전을 실현하는 데 필요한 통합 방식은 마련되어 있지 않습니다.

보안은 대부분의 조직에서 여전히 최우선으로 해결해야 하는 과제입니다. 경영진 역시 조직의 핵심 목표에서 보안을 우선적으로 고려해야 합니다. 물론 당면 과제는 보안 관련 작업을 지원할 인재와 기술을 경영진이 적절하게 지원하는 것입니다.

자사의 경영진 리더십이 보안을 높은 우선 순위로 고려한다고 응답한 보안 전문가의 수는 2016년의 경우 59%였습니다. 이는 2015년의 61%, 2014년의 63%에서 약간 하락한 수치입니다(**그림 46**). 보안 역할과 책임이 조직의 경영진에게 귀속돼 있다고 응답한 보안 전문가가 2016년 55%에 불과한 반면, 2015년과 2014년에는 58%였습니다.

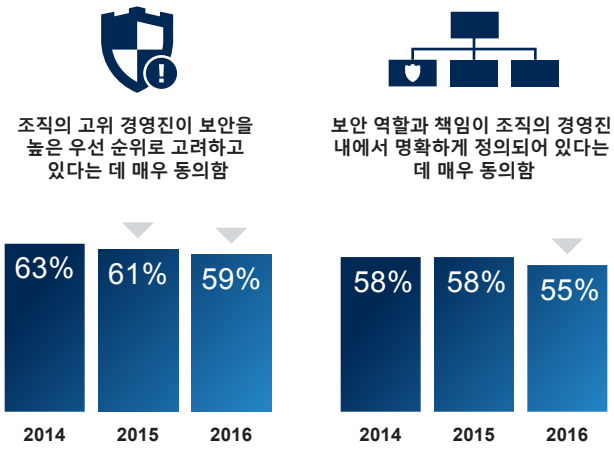
요컨대, 보안 전문가 대부분은 현재 보유하고 있는 툴을 신뢰하고 있으며, 기업의 리더들이 보안 문제 해결과 관련하여 보안 전문가의 의견을 존중하고 있다고 생각합니다. 하지만 이러한 신뢰도는 다소 낮아졌습니다. 즉, 갈수록 확대되는 공격 범위를 관리하는 까다로운 작업과 공격자의 공격 성공에 대한 보안 전문가의 인식이 높아지고 있습니다.

그림 45 다양한 보안 툴이 매우 효과적이라고 생각하는 보안 전문가의 비율



출처: Cisco 2017 보안 기능 벤치마크 조사

그림 46 경영진이 보안을 높은 우선 순위로 고려하고 있다고 생각하는 보안 전문가의 비율(2014~2016년)



출처: Cisco 2017 보안 기능 벤치마크 조사

공유

제약: 위협 대응 능력에 영향을 주는 시간, 인재 및 예산

비교적 많은 보안 전문가가 위협을 탐지하고 피해를 완화하는 데 필요한 툴을 보유하고 있는 것으로 신뢰한다면, 목표 달성을 어렵게 하는 특정 구조적 제약이 있다는 점도 인지하고 있을 것입니다. 지속적으로 해결해야 하는 당면 과제 중 하나는 한정된 예산입니다. 그러나 기타 보안 관련 제약 역시 보안을 간소화하고 자동화하는 문제에 영향을 줍니다.

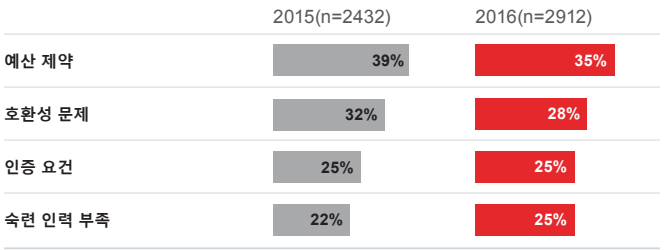
그림 47에 나와 있는 것처럼, 2016년에 보안 전문가 중 35%는 강화된 보안 프로세스 및 기술을 도입하는 데 가장 큰 장애 요소가 예산이라고 답했습니다. 이는 2015년의 동일 답변 비율인 39%보다 약간 낮아진 수치입니다. 또한 2015년과 마찬가지로, 예산 다음으로 부각되는 장애 요소는 기존 시스템과의 호환성 문제였습니다. 2016년에는 2015년의 32%에 비해 다소 낮아진 28%가 호환성을 장애 요소로 선택했습니다.

비용은 문제의 일부분일 뿐입니다. 예를 들어 호환성 문제는 통합할 수 없으며 연결되지 않은 시스템 문제에 영향을 줍니다. 게다가 숙련된 인력 부족 문제로 인해 보안 환경에서 발생하는 상황을 완벽하게 파악할 수 없는 상황이 더욱 부각됩니다.

표적 공격과 지속적으로 변화하는 공격 전술에 대응하는 데 필요한 전문 지식 및 의사 결정 능력을 고려할 때, 인재를 찾기가 어려운 것은 중요한 문제라 할 수 있습니다. 적절한 리소스가 투입되는 전문적인 IT 보안 팀을 구성하고 올바른 툴을 제공하면 기술과 정책을 연동할 수 있으며 보안 작업에서 원하는 결과를 얻을 수 있습니다.

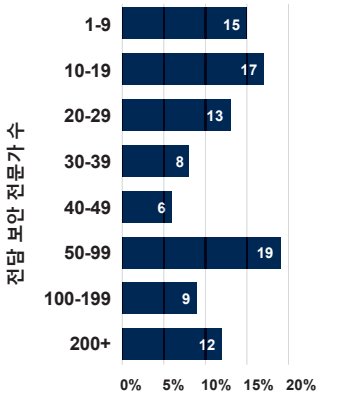
조사 대상 조직의 보안 전문가 수 중앙값은 2015년의 25명에 비해 증가한 33명이었습니다. 2016년에는 조직 중 19%가 50~99명의 전담 보안 전문가를 보유했으며, 9%는 100~199명의 보안 전문가를, 12%는 200명 이상의 보안 전문가를 보유하고 있었습니다(**그림 48**).

그림 47 보안 유지의 최대 장애 요소



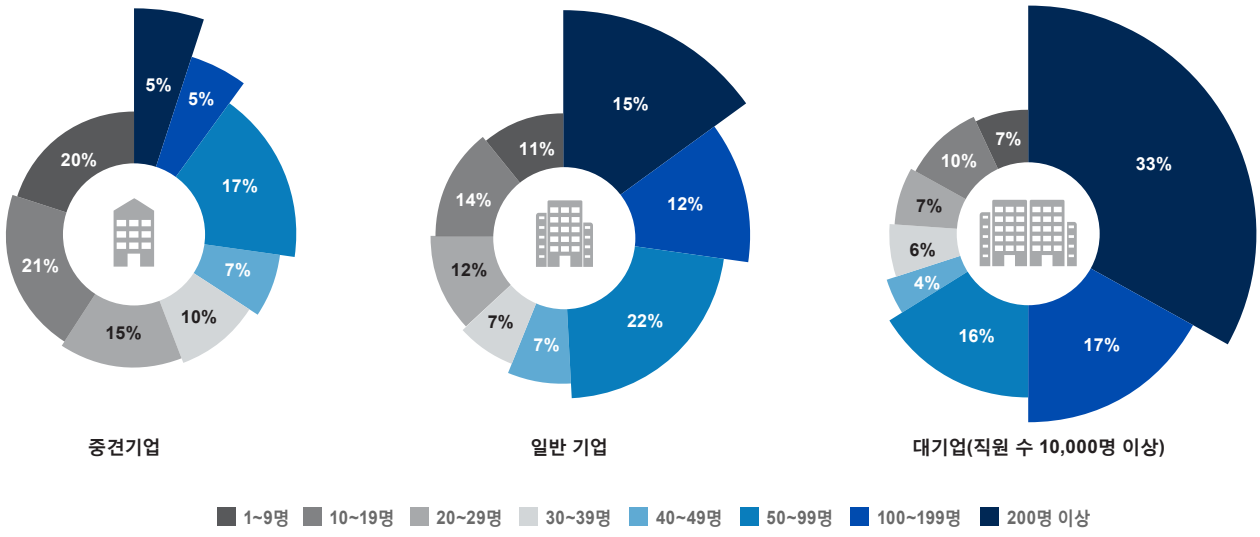
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 48 조직 소속 보안 전문가의 수



출처: Cisco 2017 보안 기능 벤치마크 조사

그림 49 조직 규모별 보안 전문가의 수



출처: Cisco 2017 보안 기능 벤치마크 조사

보안 전문가 수는 조직 규모에 따라 다릅니다. **그림 49**에 나와 있는 것처럼, 직원 수가 10,000명이 넘는 대기업 중 33%에는 200명 이상의 보안 담당 직원이 있었습니다.

어떠한 제약이 있든, 보안 전문가는 위협 대응 능력을 제한하는 장애 요소와 관련하여 어려운 질문을 해야 합니다.

우선 예산과 관련하여 충분한 예산이란 실제로 어느 정도인지를 파악해야 합니다. 설문조사 응답자들의 설명에 따르면 보안 팀은 IT 환경 내에서조차 기업 내 여러 요소보다 높은 우선 순위를 차지하기 위해 경쟁해야 합니다. 툴을 추가로 구매할 수 있는 자금을 확보하지 못한다면 기존에 확보한 예산을 훨씬 더 효율적으로 사용해야 합니다. 예를 들어 자동화를 활용해 인력 제한 문제를 어느 정도 보완할 수 있습니다.

소프트웨어 및 하드웨어 호환성 문제와 관련해서도 비슷한 질문을 해야 합니다. 호환성 문제가 증가하는 경우 관리해야 하는 소프트웨어 및 하드웨어의 각기 다른 버전 수(대다수의 버전은 효과적으로 작동 중이지 않을 수 있음)를 파악해야 합니다. 그리고 보안 팀이 필요한 여러 인증 요건을 처리하는 방법도 확인해야 합니다.

아웃소싱과 클라우드를 통한 효율적 예산 활용

벤치마크 조사에 참여한 대다수의 보안 전문가는 보안 관련 제품을 구매할 때 예산이 부족하다고 느낀 적이 있다고 합니다. 이에 따라 일부 작업을 아웃소싱하거나 클라우드 솔루션 및 자동화를 활용함으로써 예산 활용도를 높였습니다.

보안 전문가는 이러한 제한 사항 외에 보안 운영 환경 구축도 다소 간과할 수 있습니다. 이로 인해 보안 전문가가 최적의 상태가 아닌 보안 인프라를 구축하게 되는 문제가 발생할 수 있습니다. 운영 환경 구축이 허술해지는 징후는 갈수록 확장되는 공격 환경을 조직 차원에서 방어할 준비가 덜 됐음을 나타낼 수 있습니다.

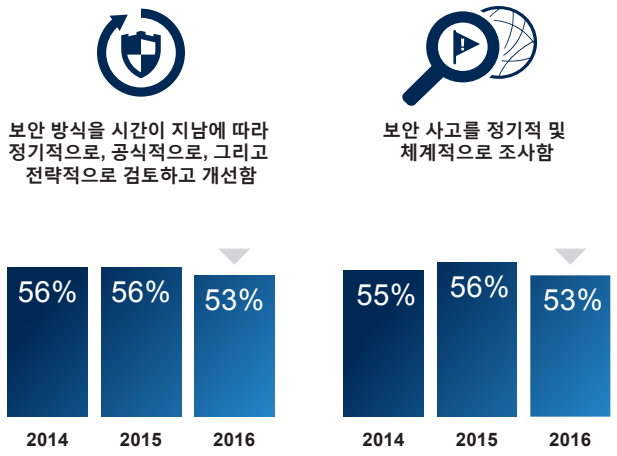
예를 들어 2016년에는 응답자 중 53%가 보안 방식을 정기적, 공식적, 전략적으로 검토하고 개선하는 데 매우 동의한다고 답변한 반면, 2014년과 2015년의 경우 매우 동의한다고 답변한 보안 전문가의 비율은 56%였습니다. 마찬가지로, 2016년에는 응답자 중 53%가 보안 사고를 정기적 및 체계적으로 조사한다는 데 매우 동의한다고 답변한 반면, 2014년과 2015년에는 이와 같이 답변한 응답자가 각각 55%, 56%였습니다(**그림 50**).

보안 전문가가 보안 기능 활용이라는 목표를 달성하지 못한다면 새 툴을 추가할 수 없음은 물론 현재 보유 중인 툴조차 효율적으로 구축하지 못할 수 있습니다. 조사 응답자들이 답변한 것처럼, 이미 보유하고 있는 기술을 사용할 수 없다면 보안 프로세스를 자동화하는 보다 간소화된 툴이 필요합니다. 그리고 이러한 툴은 현재 네트워크 환경에서 발생하고 있는 상황에 대한 정보를 종합적으로 제공해야 합니다.

보안을 통합할 수 없는 경우 공격자들이 공격을 시작할 수 있는 시간과 영역이 발생할 수 있습니다. 보안 전문가가 여러 벤더의 솔루션과 플랫폼을 사용하는 데 어려움을 겪는 경향은 원활한 방어 환경 구축을 더욱 힘들게 합니다. **그림 51**에 나와 있는 것처럼, 대부분의 조직 환경에서는 6개 이상의 보안 벤더에서 제공하는 6가지 이상의 보안 제품을 사용하고 있습니다. 보안 전문가 중 55%는 6개 이상의 벤더를, 45%는 1~5개 벤더를, 그리고 65%는 6개 이상의 제품을 사용하고 있습니다.

2017년 그래픽 다운로드: www.cisco.com/go/acr2017graphics

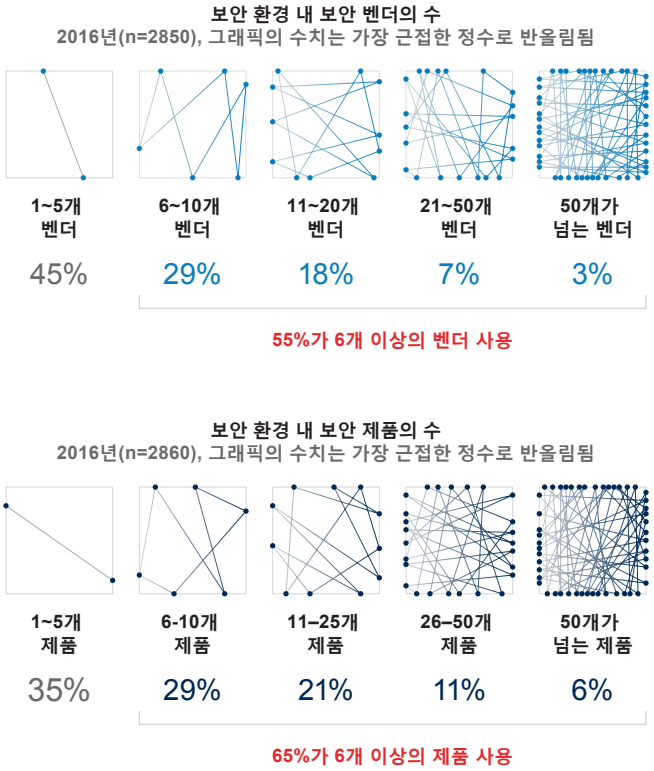
그림 50 보안 운영 환경 구축 설명에 매우 동의하는 응답자의 비율



2014년(n=1738), 2015년(n=2432), 2016년(n=2912)

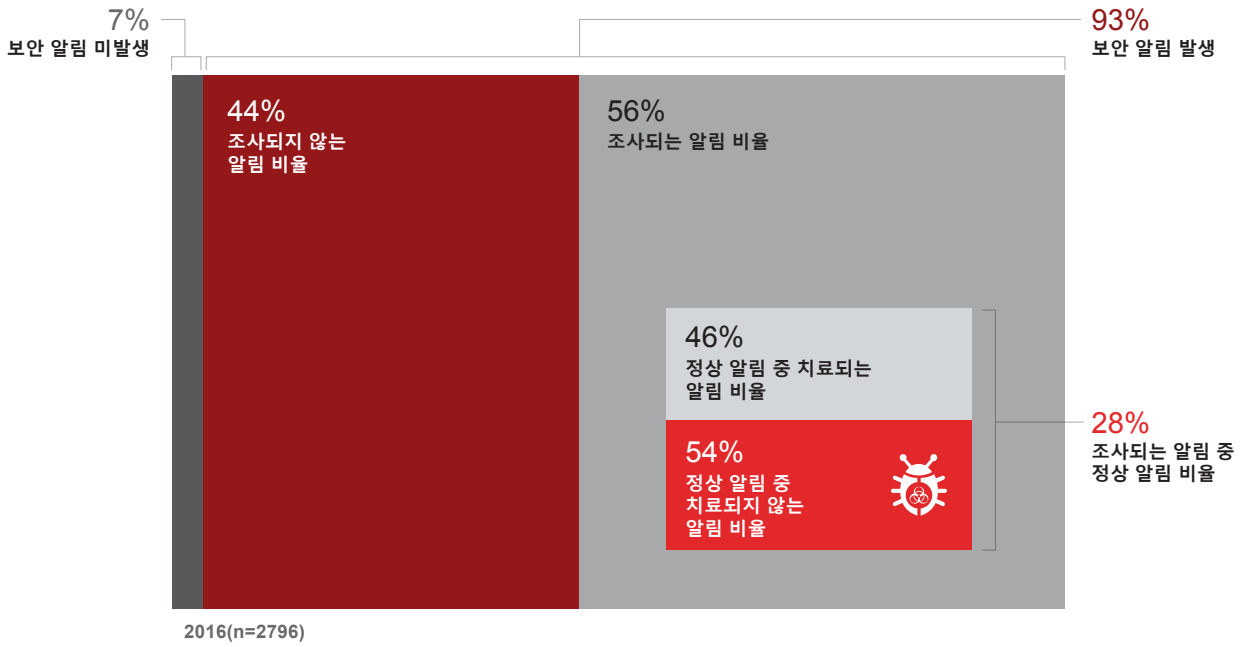
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 51 조직에서 사용 중인 보안 벤더와 제품의 수



출처: Cisco 2017 보안 기능 벤치마크 조사

그림 52 조사 또는 치료되지 않는 보안 알림의 비율



출처: Cisco 2017 보안 기능 벤치마크 조사

운영 환경 구축 목표를 달성하지 못하고, 툴을 최대한 효율적으로 사용하지 못하고, 능력을 갖춘 인력을 확보하지 못한다면 보안 수준은 낮아집니다. 보안 전문가는 중요한 알림 및 이러한 알림이 발생하는 이유를 확인하는 데 사용할 수 있는 인재, 툴 또는 자동화된 솔루션이 없다는 이유만으로 알림 조사를 건너뛸 수밖에 없습니다.

통합 방어 시스템의 부재나 직원의 시간 부족 등 여러 가지 요인으로 인해 조직은 특정일에 수신하는 보안 알림 중 절반을 약간 넘는 수만 확인할 수 있습니다. **그림 52**에 나와 있는 것처럼 조사되는 알림은 전체 알림의 56%이며, 나머지 44%는 조사되지 않습니다. 그리고 조사되는 알림 중 28%는 정상 알림이며, 이 중 46%만이 치료됩니다.

이 문제를 보다 명확하게 이해하기 위해 구체적인 수치를 적용해 보겠습니다. 조직에서 매일 5,000개의 알림을 기록하는 경우에는 다음 사항이 적용됩니다.

- **2,800개의 알림(56%)이 조사되며 2,200개의 알림(44%)은 조사되지 않음**
- **조사되는 알림 중 784개(28%)는 정상 알림이고 2,016개(72%)는 잘못된 알림임**
- **정상 알림 중 360개(46%)가 치료되고 424개(54%)는 치료되지 않음**

이처럼 알림 중 절반에 가까운 수가 조사되지 않으므로 문제가 발생하게 됩니다. 치료되지 않는 알림 그룹에 포함되는 알림은 단순히 스팸을 전송하는 낮은 수준의 위협일 수도 있지만 랜섬웨어 공격을 야기하거나 네트워크를 마비시킬 수 있는 위협일 수도 있습니다. 위협 환경을 더 많이 조사하고 파악하려면 조직은 자동화 시스템 및 적절하게 통합된 솔루션을 모두 활용해야 합니다. 자동화를 도입하면 중요한 리소스의 활용 범위를 넓히고 보안 팀의 부담을 해소할 수 있습니다.

앞에서도 설명한 것처럼, 알림 수가 너무 많아 일일이 확인할 수가 없기 때문에 조직 전체의 적절한 보안 유지와 관련하여 의문점이 생기게 됩니다. 즉, 이처럼 조사되지 않는 위협이 기업의 생산성, 고객 만족 및 신뢰도에 어떤 영향을 줄 수 있는지에 대한 의문이 제기될 수 있습니다. 응답자들의 답변에 따르면, 단시간의 네트워크 중단이나 보안 침해가 발생하더라도 기업 수익에 장기적인 영향을 줄 수 있습니다. 손실이 상대적으로 경미하고 영향을 받은 시스템을 비교적 쉽게 식별하여 격리할 수 있다 하더라도, 보안 리더는 조직에 미치는 부담으로 인해 보안 침해를 심각한 문제로 간주합니다.

이러한 부담은 여러 가지 방식으로 조직에 영향을 줄 수 있습니다. 보안 팀은 시간을 할애하여 보안 침해 이후 발생하는 네트워크 중단을 관리해야 합니다. 이러한 중단의 절반 가량은 최대 8시간까지 지속되었습니다. 즉, 네트워크 중단의 45%는 1~8시간(**그림 53**), 15%는 9~16시간, 11%는 17~24시간 동안 계속되었습니다. 그리고 이러한 중단 중 41%는 조직 시스템의 11~30%에 영향을 주었습니다.

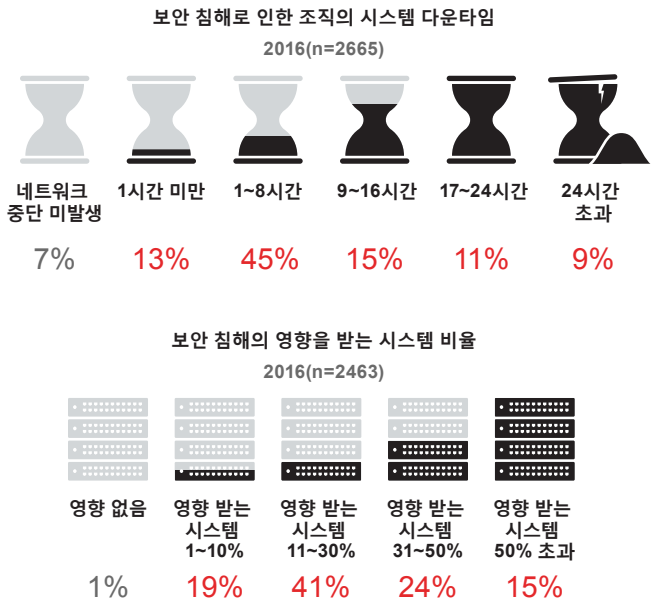
영향: 보안 침해로 인한 손실을 경험하는 조직 증가

보안 침해로 인한 피해는 네트워크 중단에 국한하지 않습니다. 즉, 보안 침해가 발생하는 경우에는 비용, 시간 및 평판에서도 손해를 보게 됩니다. 이러한 피해를 방지할 수 있다고 생각하는 보안 팀은 데이터와 관련된 현실을 무시하고 있다고 해도 과언이 아닙니다. Cisco의 조사 결과에서도 확인할 수 있듯이, 거의 절반에 가까운 조직이 보안 침해 이후 공개 조사를 받아야 했습니다. 공격자의 공격 능력 및 전술 범위를 고려할 때 문제는 보안 침해 발생 여부가 아니라 시기입니다.

벤치마크 조사에서 나타난 것처럼, 보안 전문가는 보안 침해가 발생해야 현실을 자각하게 됩니다. 즉, 보안 침해가 발생한 후에야 보안 전략을 변경하거나 방어를 강화하는 경우가 많습니다. 아직 공격자로 인한 네트워크 보안 침해를 경험하지 않은 조직은 공격을 피하는 데 성공했다고 안심할 수도 있습니다. 하지만 이러한 신뢰는 잘못됐을 가능성이 높습니다.

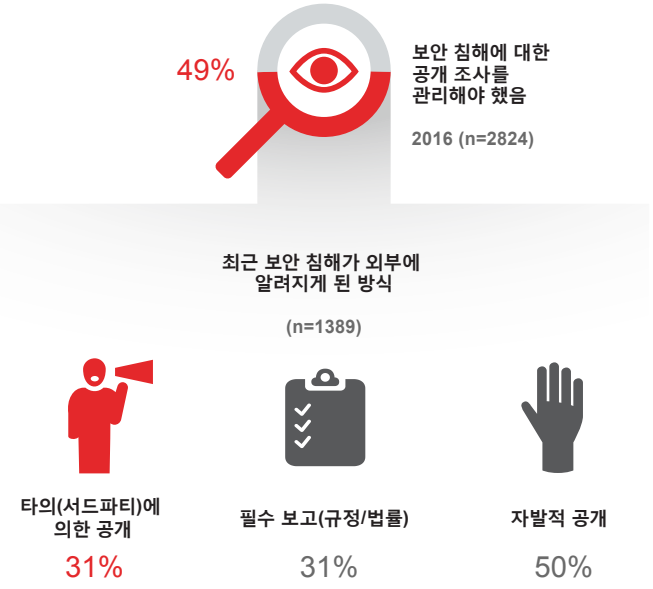
설문조사 대상 보안 전문가 중 49%는 조직에서 보안 침해가 발생한 후 공개 조사를 관리해야 했다고 답변했습니다. 이러한 조직 중 49%는 보안 침해 사실을 자발적으로 공개한 반면 31%는 서드파티에 의해 보안 침해가 공개되었다고 답변했습니다(**그림 54**). 즉, 조사 대상 조직의 약 1/3은 타의에 의해 공개된 보안 침해 관련 사안을 처리해야만 했습니다. 보안 침해를 비밀리에 처리할 수 있었던 시대는 지나갔습니다. 보안 침해를 공개할 수 있는 규제 기관, 언론 및 소셜 미디어 사용자들이 너무 많기 때문입니다.

그림 53 보안 침해로 인한 네트워크 중단 발생 기간 및 범위



출처: Cisco 2017 보안 기능 벤치마크 조사

그림 54 공개 보안 침해를 경험한 조직의 비율



출처: Cisco 2017 보안 기능 벤치마크 조사

그림 55 공개 보안 침해의 영향을 받을 가능성이 가장 높은 기능

출처: Cisco Security Research

보안 침해로 인한 조직의 피해는 상황을 해결하는 데 걸리는 시간 이외에도 훨씬 많습니다. 피해로 인한 영향은 막대하므로 기업은 피해 방지에 최대한 노력해야 합니다.

그림 55에 나와 있는 것처럼, 보안 전문가 중 36%는 가장 영향을 받을 가능성이 높은 기능으로 운영을 선택했습니다. 즉, 운송, 의료, 제조 등 여러 산업에 영향을 주는 생산성 유지를 위한 핵심 시스템의 속도가 느려지거나 작동이 중단될 수 있는 것입니다.

운영 다음으로 영향을 받을 가능성이 높은 요소는 재무(응답자의 30%가 언급함)이며, 브랜드 평판과 고객 유지(둘 다 26%)가 그 뒤를 잇따랐습니다.

사업을 확장하고 목표를 달성하려는 조직이라면 핵심 부서가 보안 침해의 영향을 받지 않도록 해야 할 것입니다. 보안 전문가는 자사 조직의 현실을 반영하여 설문조사 결과를 파악해야 하며, 자사 조직에서 보안 침해로 인해 이러한 종류의 손실을 입는 경우 실무에는 어떤 영향이 발생하는지를 고려해야 합니다.

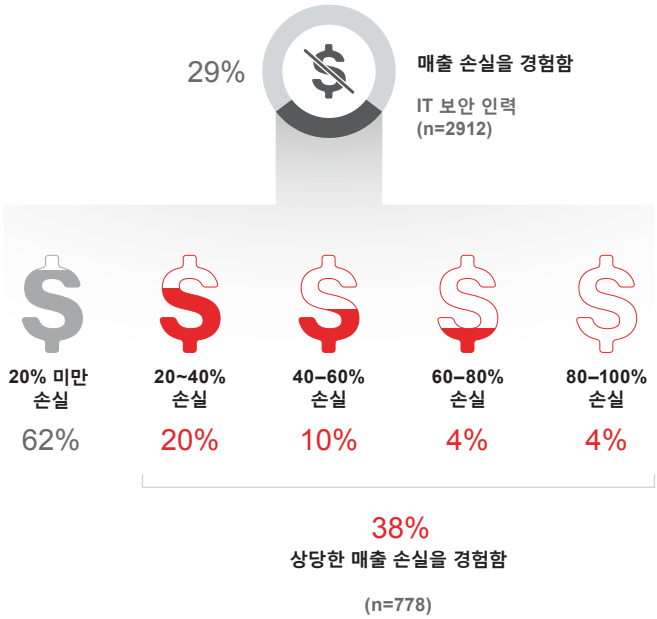
온라인 공격을 받는 회사에는 심각한 기회 상실이 발생할 수 있습니다. 설문조사 대상 보안 전문가 중 23%는 2016년에 자사 조직이 공격으로 인한 기회 상실을 경험했다고 답했습니다(**그림 56**). 이 보안 전문가 그룹 중 58%는 상실한 총 기회의 비율이 20% 미만, 25%의 전문가는 20~40%, 9%의 전문가는 40~60%라고 답했습니다.

많은 조직에서는 공개 보안 침해로 발생하는 매출 손실을 수치로 산출할 수 있습니다. **그림 57**에 나와 있는 것처럼, 보안 전문가의 29%는 공격으로 인한 매출 손실을 경험했다고 답했습니다. 해당 그룹 중 38%는 매출 손실이 20% 이상이라고 답했습니다.

온라인 공격을 받으면 고객도 줄어듭니다. **그림 58**에 나와 있는 것처럼, 조직 중 22%는 공격으로 인해 고객 이탈을 경험했다고 답했습니다. 이 중 39%는 20% 이상의 고객을 잃었다고 답했습니다.

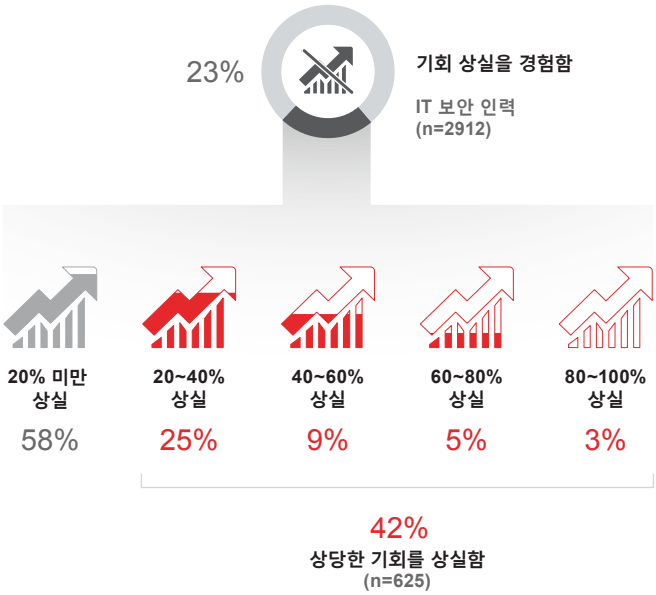
2017년 그래픽 다운로드: www.cisco.com/go/acr2017graphics

그림 57 공격으로 인해 손실된 조직의 매출 비율



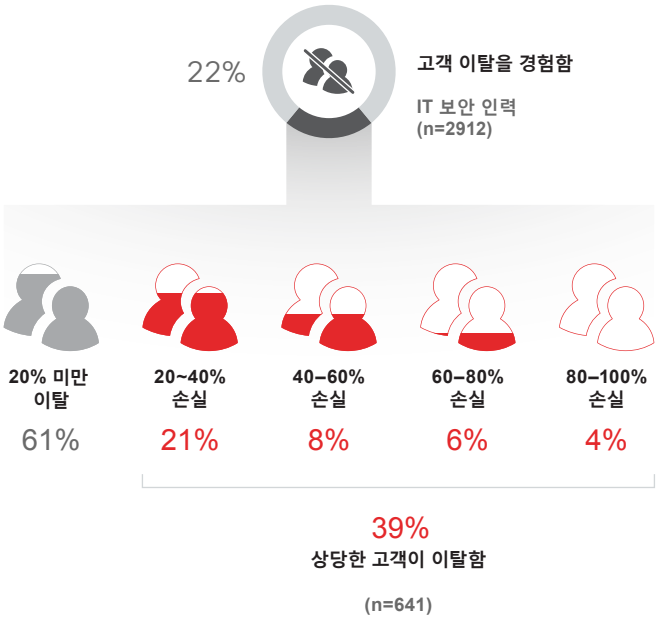
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 56 공격으로 인해 상실된 비즈니스 기회 비율



출처: Cisco 2017 보안 기능 벤치마크 조사

그림 58 공격으로 인해 이탈한 회사의 고객 비율



출처: Cisco 2017 보안 기능 벤치마크 조사

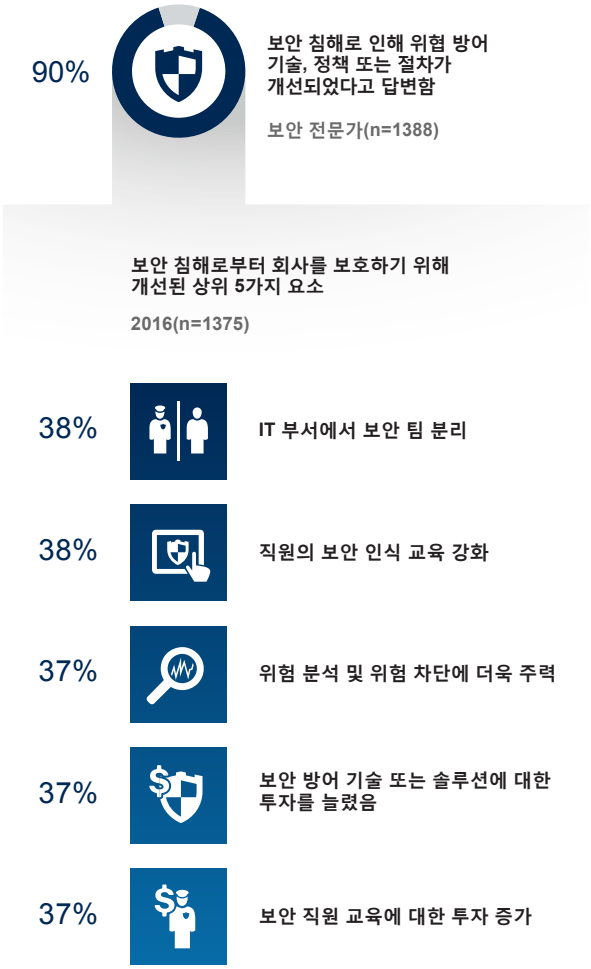
결과: 추가적인 조사를 통해 보안 개선

설문조사 결과처럼, 보안 침해는 장기적이고 광범위한 영향을 줄 수 있습니다. 일정 시점 동안, 조직이 보안 침해로 인한 피해를 받는다면 그 이후에는 어떤 상황이 이어질지 의문이 발생할 것입니다. 그럼 이제 보안 침해의 발생 가능성을 낮추기 위해 경영진이 새롭게 주목해야 하는 영역과 리소스를 투입해야 하는 부분에 대해 살펴보겠습니다.

보안 침해가 발생하면 교훈을 얻을 기회가 생깁니다. 이러한 기회를 낭비하지 않고 보다 나은 방식에 투자를 할 수 있도록 해야 합니다.

그림 59에 나와 있는 것처럼, 보안 전문가 중 90%는 보안 침해가 위협 방어 기술과 프로세스 개선의 원동력이 되었다고 답했습니다. 보안 침해의 영향을 받은 조직 중 38%는 IT 부서에서 보안 팀을 분리하는 방식으로 대응했다고 답했습니다. 그리고 직원에 대한 보안 인식 교육을 강화했다는 답변도 38%였으며, 37%는 위험 분석 및 차단을 보다 중점적으로 다루기 시작했다고 답했습니다.

그림 59 보안 침해로 인한 방어 개선



출처: Cisco 2017 보안 기능 벤치마크 조사

조직은 인재, 기술 호환성 및 예산에 구애받지 않고 독창성을 발휘해야 함을 알고 있습니다. 이를 위한 전략 중 하나로 아웃소싱 서비스를 도입해 예산을 보다 효율적으로 활용하고 외부의 인재를 확보해야 합니다.

2016년에 보안 전문가 중 51%는 아웃소싱 자문/컨설팅 서비스를 이용했으며 45%는 아웃소싱 사고 대응 서비스를 이용했습니다(**그림 60**). 응답자의 52%는 비용 절약 차원에서 아웃소싱했다고 답변한 반면 48%는 편견 없는 시각을 얻기 위해 아웃소싱한다고 답했습니다.

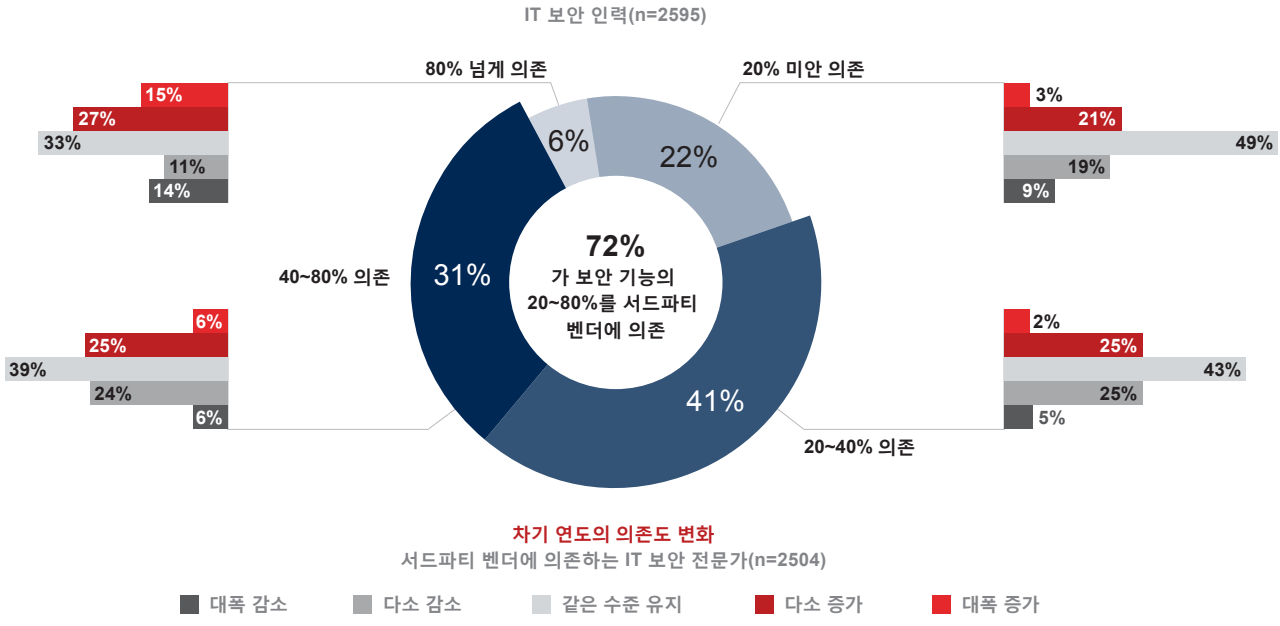
아웃소싱 서비스를 이용하는 조직은 서드파티 벤더를 통해 방어 전략을 보완하기도 합니다. 보안 에코시스템에서는 보안에 대한 책임을 공유하는 방식을 제공합니다.

그림 61에 나와 있는 것처럼, 보안 전문가 중 72%는 보안 기능의 20~80%를 서드파티 벤더에 맡기고 있다고 답했습니다. 보안과 관련하여 외부 서비스를 많이 사용하는 조직의 경우 앞으로도 서드파티 벤더 사용률이 증가할 것이라고 답한 경우가 많았습니다.

그림 60 조직의 아웃소싱 의존도

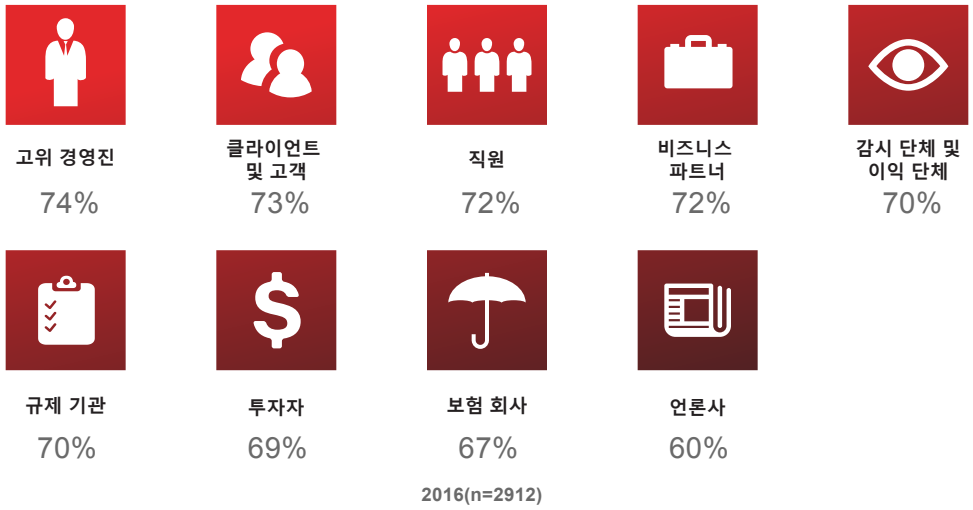
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 61 조직의 아웃소싱 의존 비율



출처: Cisco 2017 보안 기능 벤치마크 조사

그림 62 조사 증가의 원인

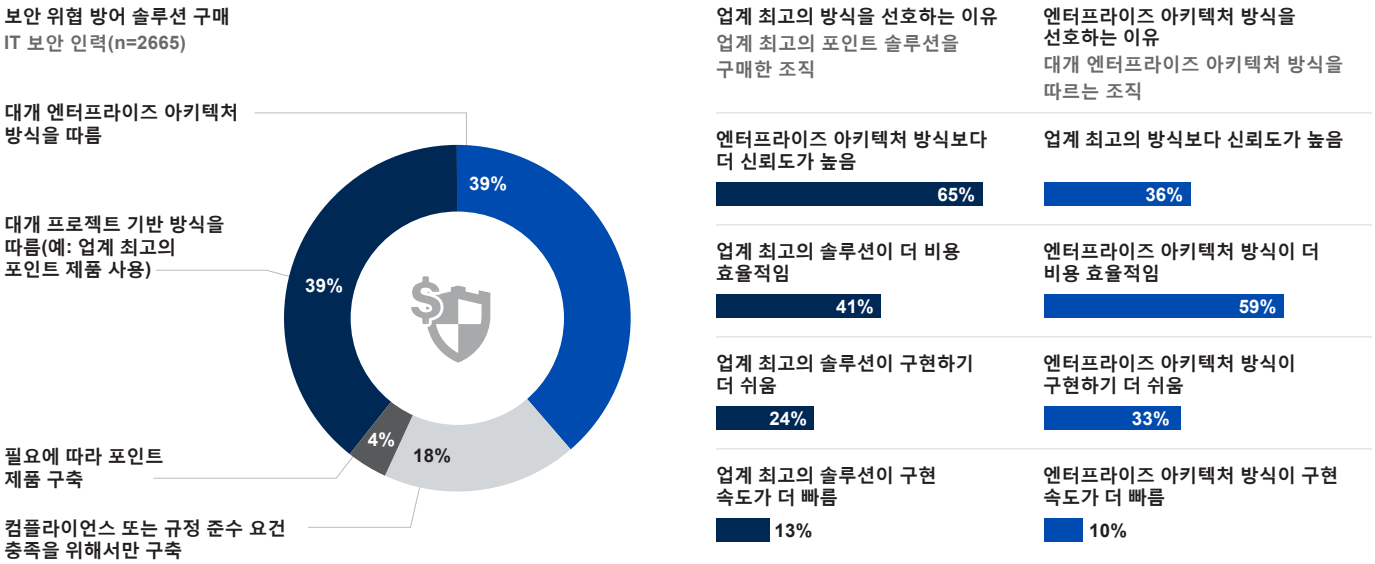


출처: Cisco 2017 보안 기능 벤치마크 조사

조직이 보안 상태를 강화하기 위한 단계를 수행하게 되면 보다 철저한 주의를 기울일 것입니다. 이러한 조사는 영향력 있는 대상이 진행하는 것이므로 무시할 수 없으며, 해당 대상의 문제 해결 방식은 방어 능력에 큰 영향을 줄 것입니다.

그림 62에 나와 있는 것처럼, 보안 전문가 중 74%는 이러한 조사를 고위 경영진이 진행한다고 답했으며 73%는 고객이, 72%는 직원이 진행한다고 답했습니다.

그림 63 신뢰와 비용 효율성이 보안 관련 결정에 영향을 주는 방식



출처: Cisco 2017 보안 기능 벤치마크 조사

신뢰와 비용: 보안 솔루션 구매 요인

보안 전문가는 조직 보호를 위한 최고의 솔루션을 사용하고자 합니다. 하지만 이상적인 보안 환경을 구축하는 방식에 대한 인식은 서로 다릅니다. 다양한 벤더에서 제공하는 솔루션을 구매할 수도 있고, 통합 아키텍처 방식이 비용 대비 효율적이라 판단해 해당 아키텍처를 도입할 수도 있습니다. 이처럼 여러 방안이 있지만, 간소화는 모든 조직에 공통적으로 도움될 수 있습니다.

그림 63에 나와 있는 것처럼, 보안 전문가는 업계 최고의 솔루션과 아키텍처형 솔루션 중 어떤 쪽을 선택할지를 결정할 때 신뢰와 비용을 모두 중요하게 고려하는 것으로 나타났습니다. 보안 전문가 중 65%는 엔터프라이즈 아키텍처 방식보다 신뢰도가 높은 업계 최고의 솔루션을 선호한다고 답했습니다. 반면 59%는 보다 비용 효율적인 아키텍처형 방식을 선호한다고 답했습니다.

하지만 이 두 가지 방식 중 어느 하나만 선택할 수 있는 것은 아닙니다. 즉, 조직에는 업계 최고의 솔루션과 통합 보안 솔루션이 모두 필요합니다. 이 두 가지 방식은 모두 이점을 제공하고 보안을 간소화하는 동시에 자동화된 대응 툴을 제공합니다(**그림 63**).

보안 팀은 통합 방식과 업계 최고의 솔루션을 함께 활용하여 더욱 단순하면서도 효율적인 보안 기능을 구축하기 위한 단계를 추진할 수 있습니다. 통합 방식을 사용하는 경우 보안 전문가가 모든 방어 단계에서 발생하는 상황을 파악할 수 있습니다. 이러한 방식에서는 공격자가 공격할 수 있는 영역이 감소합니다. 또한, 단순한 방식이므로 팀이 원하는 규모로 솔루션을 구축할 수 있으며, 개방적이라 필요에 따라 업계 최고의 솔루션도 함께 사용할 수 있습니다. 게다가 자동화 방식이므로 더욱 빠르게 위협을 탐지할 수 있습니다.

요약: 벤치마크 조사에서 확인된 사항

보안 툴을 확보하는 것과 실제로 그러한 툴을 사용하여 위험을 줄이고 공격자들이 공격할 수 있는 영역을 없애는 능력을 갖추는 것은 별개의 문제입니다. 벤치마크 조사의 응답자들은 공격자를 무력화할 수 있는 툴을 보유하고 있다고 생각합니다. 하지만 인력 부족, 제품 호환성 불량 등의 제약으로 인해 아무리 좋은 툴을 확보하더라도 원하는 만큼 효율적으로 활용할 수 없다는 점도 인지하고 있습니다.

보안 침해의 영향과 관련하여 확인된 조사 결과는 보안 전문가에게 프로세스 및 프로토콜 개선 필요성에 대한 충분한 증거를 제시합니다. 매출 손실 및 고객 이탈 등의 현실적이고 즉각적인 영향을 고려할 때 조직은 더 이상 이상적인 보안 기능이 현실화되기를 기대할 수 없습니다. 문제는 보안 침해 발생 여부가 아닌, 발생 시기에 있기 때문입니다.

벤치마크 조사에서 확인된 사항 중 하나는, 신속하고 효율적인 보안을 제약하는 요인은 항상 존재한다는 것입니다. 보안 전문가들은 필요한 만큼 충분한 예산과 인재를 확보할 수 없습니다. 이러한 제약을 고려하면 보안을 간소화하고 자동화된 솔루션을 구축해야 하는 이유를 이해할 수 있습니다.

보안 간소화 과정에서는 업계 최고의 솔루션과 통합 아키텍처를 모두 사용해야 합니다. 조직에서는 이 두 가지 방식의 이점을 모두 활용해야 하기 때문입니다.

업계 동향

업계 동향

가치 사슬(value chain) 보안: 서드파티 관련 위험 차단을 통해 디지털 환경의 보안 유지

가치 사슬(value chain) 보안은 상호 연계된 경제 환경에서 보안을 효율적으로 유지하기 위한 필수 요소입니다. 가치 사슬 전반, 즉 하드웨어, 소프트웨어, 서비스의 엔드 투 엔드 라이프사이클에 걸쳐 적절한 보안 기능을 제때 올바른 영역에서 활용해야 합니다.

그림 64에는 가치 사슬의 8개 단계가 나와 있습니다.

디지털 환경에서는 정보 기술과 운영 기술이 통합되고 있습니다. 따라서 조직은 내부 비즈니스 모델, 솔루션 및 인프라 보호에만 주력해서는 안 됩니다. 즉, 가치 사슬을 종합적으로 파악하여 비즈니스 모델에 적용하거나 각 서드파티의 서비스 이용 환경으로 인해 위험이 발생하는지 고려해야 합니다.

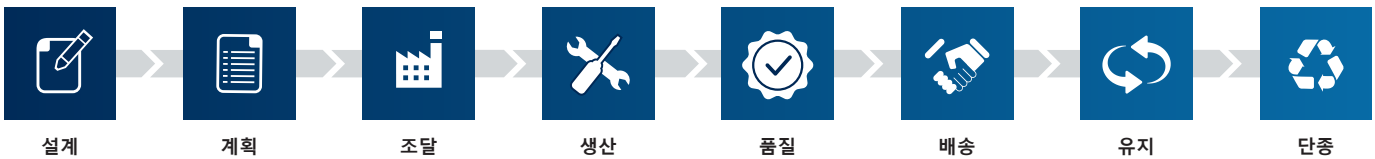
결론부터 이야기하자면, 서드파티는 위험을 발생시킬 가능성이 높습니다. SANS Institute의 연구 결과에 따르면, 데이터 보안 침해 중 80%는 서드파티에서 발생한 것으로 나타났습니다.[15] 이러한 위험을 줄이려면 조직은 확고한 신뢰를 바탕으로 모든 관련자가 보안에 책임을 지는 가치 사슬(value chain)을 조성해야 합니다. 이러한 목표 달성을 위한 기초 단계로 조직은 다음과 같은 조치를 취해야 합니다.

- **서드파티 에코시스템의 핵심 관련자 확인 및 해당 서드파티에서 제공하는 서비스 파악**
- **해당 에코시스템의 여러 서드파티와 공유할 수 있으며 이러한 서드파티에 구축할 수 있는 유연한 보안 아키텍처 개발**
- **서드파티가 조직의 보안 아키텍처에 의해 설정된 허용 수준 내에서 운영되고 있는지 평가**
- **디지털화의 보편화로 인해 에코시스템에서 발생할 수 있는 새로운 보안 위협 경계**

또한, 조직은 서드파티 에코시스템이 개입해야 하는 비즈니스 모델이나 해당 에코시스템에 별도의 영향을 줄 수 있는 새로운 솔루션을 도입하기 전에 보안을 우선적으로 고려해야 합니다. 이를 위해 가치 및 생산성 개선 가능성과 잠재적 위험(특히 데이터 보안 및 개인정보 보호 관련 위험)을 비교 평가해야 합니다.

전 세계적으로, 그리고 특정 산업 분야에서 가치 사슬(value chain)의 중요도에 대한 인식이 높아지고 있습니다. 최근 미국의 IT 조달 관련 법안에서는 정보 기술 및 사이버 보안 기술 조달 분야의 개방형 기술 표준과 관련하여 미국 국방부의 1년 의무 평가 기간을 규정했습니다.[16] 고도로 통합된 에너지 분야의 경우 NERC(North American Electric Reliability Corporation)에서는 사이버 가치 사슬의 문제 해결책을 활발하게 개발 중입니다.[17]

그림 64 가치 사슬(value chain)의 단계



출처: Cisco

공유

[15] *Combatting Cyber Risks in the Supply Chain,* SANS Institute, 2015: **https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252**.
[16] Public Law 114-92 §
[17] NERC는 미 연방 에너지 규제 위원회 18 CFR Part 40 [Docket No. RM15-14-002; Order No. 829]을 통해 이러한 요구 사항을 충족하도록 명령함.

조직은 서드파티와 함께 "데이터를 생성하는 방식은 무엇이며 생성 주체는 누구인가?" 및 "데이터 디지털 마이닝이 필요한가?" 등의 질문에 답할 필요가 있습니다. 보다 명확히 하자면 "조직에서 수집하거나 생성하는 디지털 자산의 소유자는 누구인가?" 및 "조직에서 해당 정보를 공유해야 하는 대상은 누구인가?" 조직에서 수집하거나 생성하는 디지털 자산의 소유자는 누구인가?" 및 "조직에서 해당 정보를 공유해야 하는 대상은 누구인가?"와 같은 질문에도 답할 수 있어야 합니다. 또한, "보안 침해 발생 시 누가 어떤 책임을 지는가?" 보안 침해 발생 시 누가 어떤 책임을 지는가?"라는 중요한 질문에 대한 답변도 확보해야 합니다.

이러한 가치 사슬 중심 방식을 도입하면 솔루션 라이프사이클의 모든 단계에서 보안을 고려할 수 있게 됩니다. 적합한 아키텍처를 도입하고 올바른 보안 표준을 준수하면 전체 가치 사슬에서 광범위하게 보안 요소를 적용할 수 있을 것입니다.

지정학적 업데이트: 암호화, 신뢰 및 투명성 보장

이전 사이버 보안 보고서에서 Cisco의 지정학 전문가들은 인터넷 거버넌스 환경의 불확실성, 개인의 권리와 국가의 권리 간 충돌, 정부와 민간 기업이 데이터 보호 관련 문제를 해결할 수 있는 방식을 연구한 바 있습니다. 이러한 논의에서 공통적으로 등장한 주제는 암호화였습니다. 암호화는 머지 않아 사이버 보안 관련 논의에서 지속적으로 등장할 것으로 예상되며 핵심 사안이 될 가능성도 높습니다.

국가 및 지역별로 데이터 프라이버시 관련 법이 널리 확산됨에 따라, 이러한 법을 파악하고자 하는 벤더와 사용자의 우려도 커졌습니다. 이렇게 불확실한 환경에서 데이터 주권, 데이터 현지화 등의 문제가 표면화되었으며, 기업이 갈수록 발전하는 복잡한 개인정보 보호 규정을 준수할 수 있는 독창적인 솔루션을 모색하는 과정에서 클라우드 컴퓨팅 및 현지화된 데이터 스토리지가 확산되었습니다.[18]

그와 동시에 데이터 보안 침해 및 APT(Advanced Persistent Threat)가 증가하고, 미국 대선 등의 주요 행사 중에 진행된 해킹과 같이 국가 주도 해킹이 언론에 보도되면서 민감한 데이터와 개인정보 보호에 대한 사용자들의 신뢰도는 더욱 낮아지고 있습니다.

스노든의 정보 폭로 이후, 각국 정부는 더욱 철저한 디지털 통신 관련 규정을 제정하고 필요시 데이터에 접근할 수 있도록 하고 있습니다. 하지만 사용자 역시 철저한 개인정보 보호를 요구하고 있습니다. 테러리스트 소유의 iPhone과 관련하여 최근 벌어졌던 FBI와 Apple 간의 충돌로 인해 사용자의 개인정보 보호에 대한 우려는 한층 높아졌습니다. 특히 미국의 디지털 세대는 엔드 투 엔드 암호화의 중요성을 자각하게 되었습니다. 현재 대부분의 사용자들은 기술 제공 업체로부터 엔드 투 엔드 암호화 적용을 요구하고 있으며 암호화 키를 보유하고자 합니다.

사이버 보안 환경이 과거와는 근본적으로 달라진 것입니다. 따라서 조직은 상충하는 과제를 파악하고 적절히 대응할 수 있는 환경을 구축해야 합니다.

이처럼 환경이 변화함에 따라 제조업체, 통신사 또는 사용자에게 알리지 않고 암호화나 기술적인 보호 조치를 우회 또는 해제할 수 있는 권리를 법으로 제정하는 정부가 증가하고 있습니다. 이로 인해 관계 당국과 기술 업체 간에, 그리고 타국 기관의 자국민 데이터 액세스 요청을 원치 않는 정부 간에 긴장 상태가 조성되고 있습니다. 대부분의 정부는 벤더 소프트웨어에서 발견된 제로 데이 익스플로잇과 취약점에 대한 정보를 수집합니다. 그러나 정부가 소유한 정보를 항상 벤더에게 투명하게 제공하거나 제때 공유하는 것은 아닙니다.

이처럼 중요한 정보를 확보해 두고 공유하지 않으면 벤더는 제품의 보안을 개선하거나 사용자를 위협으로부터 효율적으로 보호할 수 없게 됩니다. 정부에도 이러한 정보를 보유해야 하는 합당한 이유가 있을 수 있지만, 전 세계 사이버 보안 환경의 투명성과 신뢰도 역시 높여야 합니다. 따라서 정부는 제로 데이 익스플로잇 관련 정보 확보에 대한 현재 정책을 솔직하게 평가해야 합니다. 그리고 벤더와 정보를 공유함으로써 모든 사용자에게 훨씬 더 안전한 디지털 환경을 창출할 수 있다는 기본적인 자세를 견지해야 합니다.

[18] 이 항목에 대한 자세한 내용은 "Data Localization Takes Off as Regulation Uncertainty Continues"(Stephen Dockery, 2016년 6월 6일, *The Wall Street Journal*)을 참조하십시오. **http://blogs.wsj.com/riskandcompliance/2016/06/06/data-localization-takes-off-as-regulation-uncertainty-continues/**

고속 암호화: 전송 중에 데이터를 보호하는 확장형 솔루션

65페이지의 지정학 섹션에서 설명한 것처럼, 엔드 투 엔드 암호화는 당분간 정부와 업계 간에 많은 논란과 충돌을 야기할 주제가 될 것입니다. 하지만 이 문제로 인해 야기되는 긴장 상태에 관계없이 엔드 투 엔드 데이터 암호화에 대한 사용자 수요는 갈수록 증가하고 있습니다.

Cisco 지정학 전문가들의 전망에 따르면, 일부 데이터 스트림 및 풀은 적어도 단기적으로 벤더가 관리하는 키로 암호화된 상태로 유지될 것이라고 합니다(특히 광고 중심 비즈니스 모델의 경우). 그러나 그 외의 분야에서는 고객이 소유한 키를 사용하는 엔드 투 엔드 암호화가 갈수록 대세로 자리잡을 것으로 예상됩니다.

한편, 전송 중인 데이터(특히 데이터 센터 간을 고속으로 이동하는 데이터)를 보호하는 방식을 더 철저하게 제어하려는 조직도 증가하고 있습니다. 이전에는 기존 기술의 제약 및 네트워크 성능에 대한 영향으로 인해 이러한 작업을 기업에서 수행하기가 매우 어려웠습니다. 하지만 새로운 방식이 등장함으로써 이 프로세스를 더욱 쉽게 수행할 수 있게 되었습니다.

이러한 작업을 위한 솔루션 중 하나는 데이터 암호화를 위해 애플리케이션을 수정하는 애플리케이션 레이어 보안입니다. 이러한 보안 유형을 구축하는 데는 조직에서 사용하는 애플리케이션의 수에 따라 리소스가 매우 많이 사용되고, 구현이 복잡하며, 운영비도 많이 들 수 있습니다.

또 다른 방식으로 전송 중에 데이터를 보호할 수 있도록 네트워크나 클라우드 서비스에 내장되어 있는 암호화 기능도 최근 많이 사용되고 있습니다. 이러한 방식은 기존의 게이트웨이 VPN 모델이 진화한 것으로, 데이터 센터 트래픽의 빠른 전송 속도, 네트워크의 동적 특성 관련 문제에 대한 솔루션이라 할 수 있습니다. 기업은 해당 환경 내 애플리케이션에서 생성되는 데이터가 다른 위치로 고속 전송될 때 해당 데이터 보호 기능에서 제공되는 운영 및 비용 효율성을 활용하고 있습니다.

하지만 네트워크 기반 암호화는 데이터 보호를 위한 툴 중 하나일 뿐입니다. 따라서 전송 중이거나 휴면 중인 데이터를 보호하려는 조직은 당면 과제를 종합적으로 파악해야 합니다. 그러려면 먼저 기술 벤더에 다음과 같은 기본적이지만 중요한 사항을 확인하는 것이 좋습니다.

- 전송 데이터 보호 방법
- 휴면 데이터 보호 방법
- 데이터에 액세스할 수 있는 사람
- 데이터가 저장되는 위치
- 데이터 삭제 시기 및 데이터를 삭제해야 하는지 여부에 대한 정책

이러한 질문 역시 데이터 보호와 관련된 논의를 시작하는 내용에 불과하므로 이후에는 데이터 복원력 및 사용 가능성과 같은 주제에 대한 논의를 비롯하여 더욱 폭넓은 사안을 파악해야 합니다.

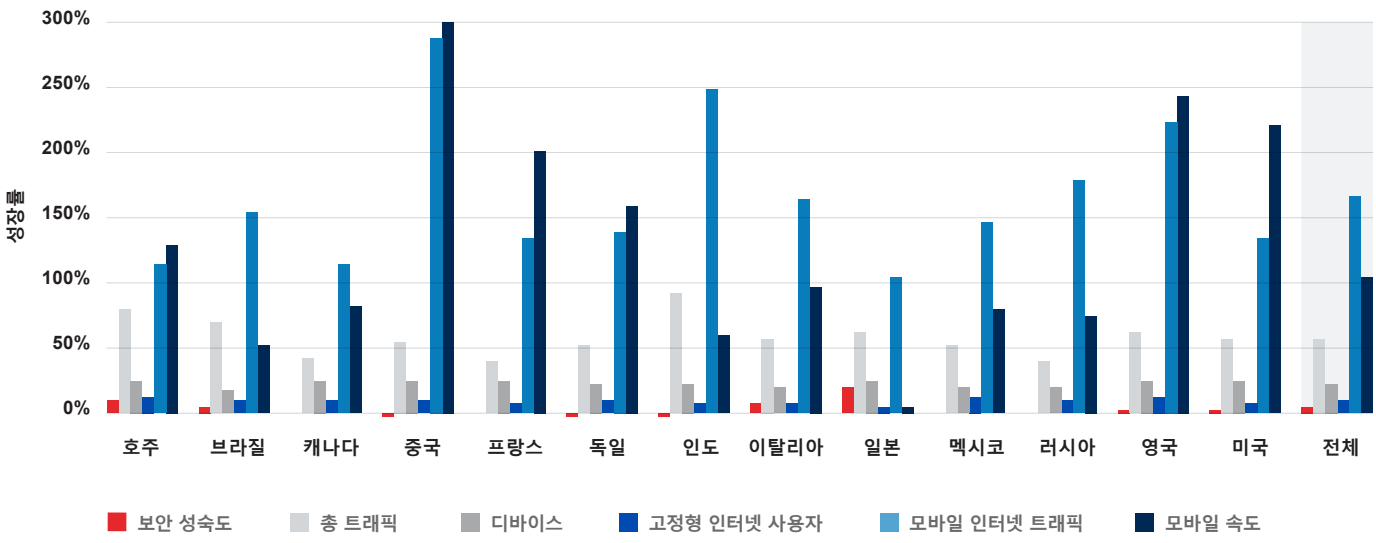
네트워크 성능과 도입 및 보안 성숙도: 동일한 속도로 개선되지 않는 온라인 속도, 트래픽 및 준비도

방어자는 공격을 받기 전에 미리 대비하고자 합니다. 뒤늦게 방어하는 경우 위험한 상황이 발생할 수 있기 때문입니다. 하지만 방어자들은 공격자들의 공격 영역 및 시간 확보 속도에 맞춰 보안 상태를 개선할 수 없다고 우려합니다. 전 세계의 유선 및 모바일 인터넷 트래픽이 빠른 속도로 증가하고 있음을 고려할 때, 방어자들은 이처럼 증가하는 트래픽에 맞게 보안 인프라의 성숙도를 높여야 합니다.

Cisco VNI Forecast는 모바일 및 Wi-Fi 트래픽을 포함한 전 세계의 IP 트래픽에 대한 연간 조사를 진행하고 있습니다. 이 조사에서는 향후 5년 동안의 예상 IP 트래픽량, 인터넷 사용자 수, IP 네트워크에서 지원할 개인용 디바이스 및 M2M(machine-to-machine) 연결 수를 제공합니다. VNI Forecast에 대해 자세히 알아보려면 **여기를 방문**하십시오. 예를 들어 이 조사에서 추정한 바에 따르면 2020년에는 전체 IP 트래픽 중 30%가 스마트폰에서 생성될 것으로 전망됩니다.

Cisco는 VNI Forecast의 조사 결과를 방어자의 보안 성숙도와 비교하는 연구를 진행했습니다. 이 자료는 Cisco의 연례 보안 기능 벤치마크 조사(**49페이지**)에서 발췌한 것입니다. **그림 65**에 나와 있는 것처럼, 2015, 2016, 2017년 벤치마크 보고서의 성숙도 성장률 조사에 따르면 인터넷 트래픽의 증가 속도에 비해 보안 성숙도는 크게 낮은 것으로 확인되었습니다. 심지어 중국 및 독일과 같은 일부 국가의 경우 조사 기간 동안 성숙도가 약간 낮아지기도 했습니다. 특히 광대역 속도는 **그림 65**에 나와 있는 다른 네트워킹 변수에 비해 훨씬 빠른 속도로 개선되며 높아지고 있습니다. 이처럼 속도가 빨라지고 연결된 디바이스 수가 늘어나면서 트래픽도 증가하는 데 비해, 조직은 이와 비슷한 속도로 보안 조치 및 인프라를 강화하는 데 어려움을 겪고 있습니다.

그림 65 보안 성숙도 및 성장률



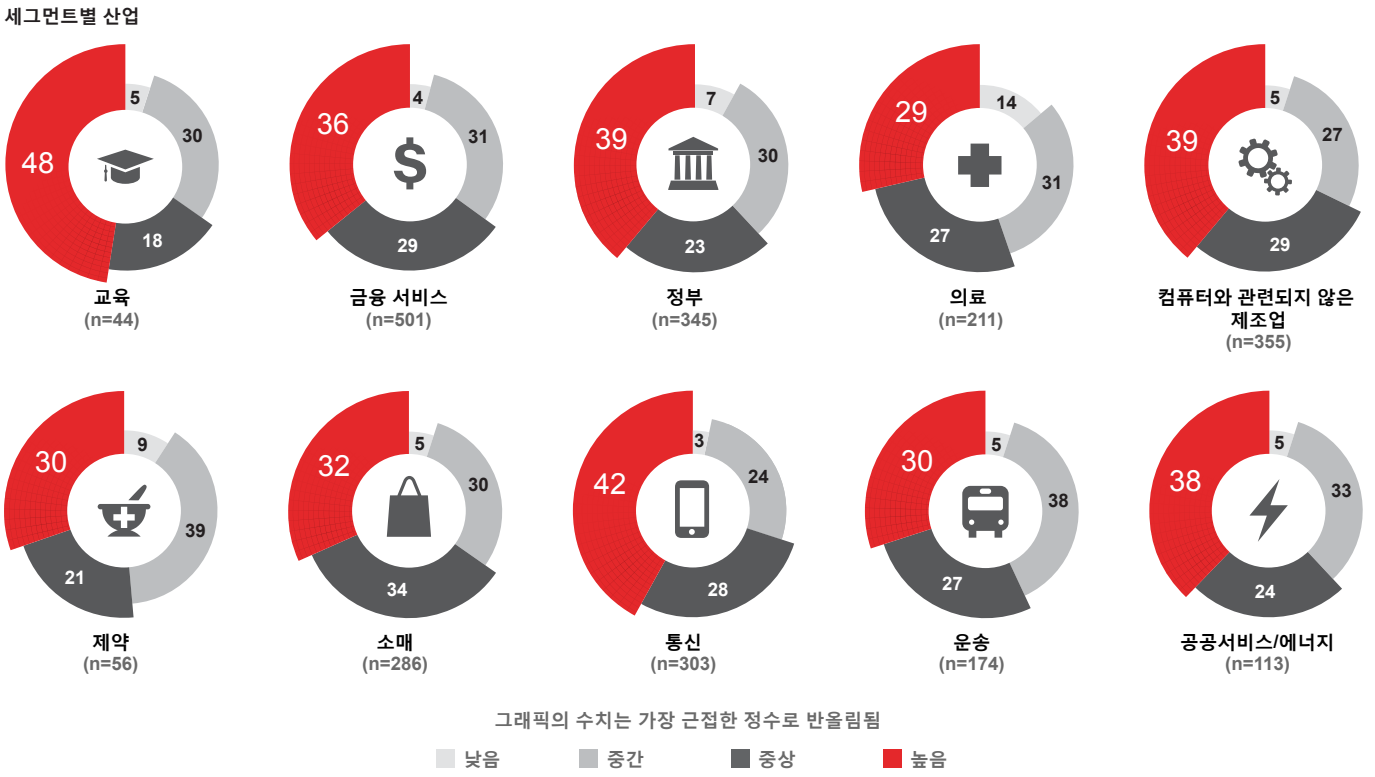
출처: Cisco Security Research, Cisco VNI 및 Cisco 2017 보안 기능 벤치마크 조사

그림 66에 나와 있는 것처럼 특정 산업 또한 보안 성숙도가 타 산업에 비해 낮았습니다. 특히 제약, 의료, 운송 분야의 성숙도가 다른 산업에 비해 뒤처졌습니다.

모바일 속도가 크게 빨라진 것은 통신 사업자들이 4G 및 LTE 네트워크를 광범위하게 도입했기 때문입니다. 2020년 말까지 5G 네트워크가 대규모로 구축되면 모바일 속도는 유선 네트워크 속도와 비슷해질 것으로 예상됩니다. 최신 Mobile VNI Forecast에 따르면 5G가 광범위하게 도입되는 경우 전체 IP 트래픽 중에서 전 세계 모바일 트래픽이 차지하는 비율은 더욱 높아질 것으로 보입니다. VNI Forecast에 따르면 전 세계 모바일 트래픽은 2015년에는 전체 IP 트래픽의 5%에 불과했지만 2020년에는 전체 IP 트래픽의 16%에 달할 것으로 전망됩니다.

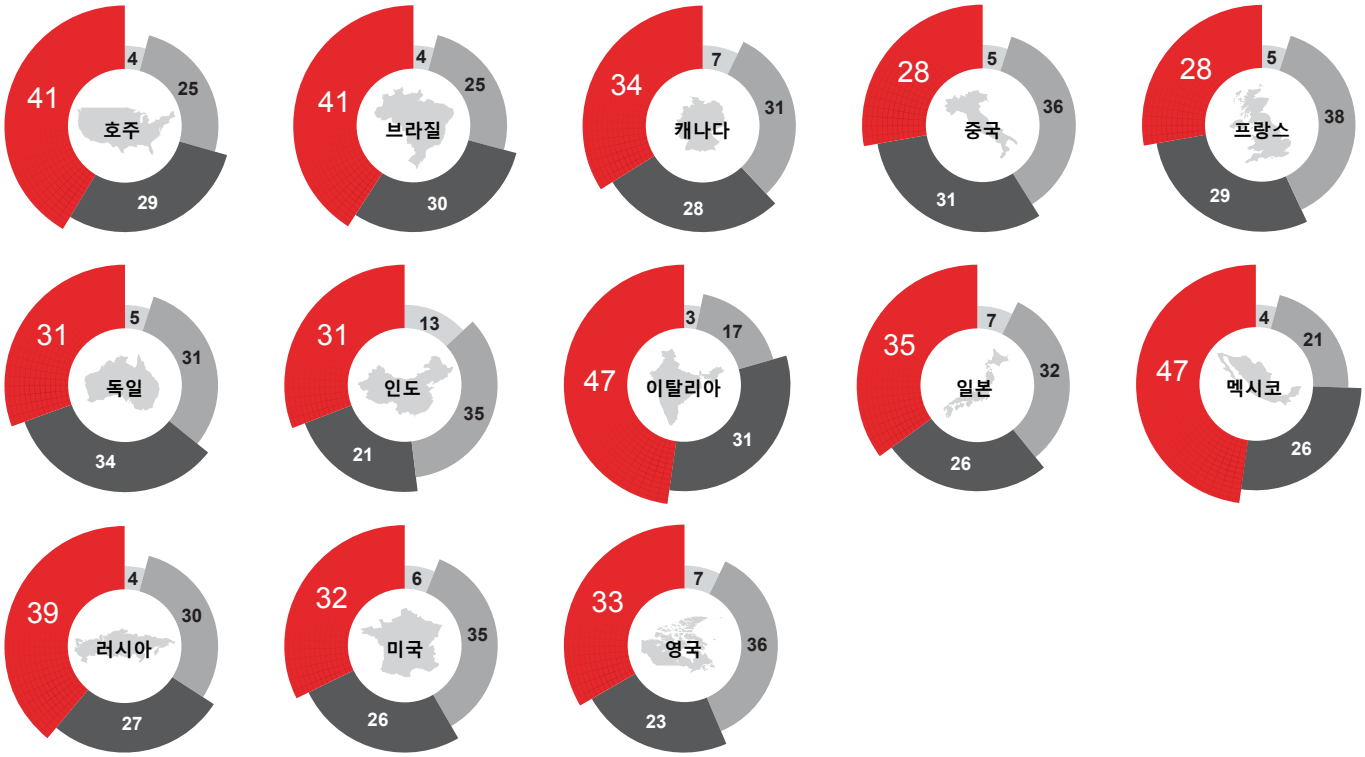
보안 조직은 인터넷 트래픽 증가 속도에 맞게 보안 성숙도를 빠르게 높여야 합니다. 인터넷 트래픽이 증가하면 잠재적 공격 범위도 확장될 것이기 때문입니다. 또한, 조직은 기업 네트워크에 고정되어 있거나 유선으로 연결되지 않은 엔드포인트 사용 증가 추세에도 대응해야 합니다. 뿐만 아니라, 작업자들이 기업 데이터에 액세스하는 데 개인용 디바이스를 더 광범위하게 사용하는 상황에도 대비해야 합니다.

그림 66 산업 업종별 보안 성숙도



출처: Cisco 2017 보안 기능 벤치마크 조사

그림 67 국가별 보안 성숙도



출처: Cisco 2017 보안 기능 벤치마크 조사

인터넷 트래픽의 증가를 촉진하는 요인은 빨라진 속도뿐만이 아닙니다. IoT로 인해 인터넷에 연결되는 디바이스의 수가 늘어남에 따라 트래픽도 증가할 뿐 아니라 공격자들의 공격 경로도 다양해졌습니다.

Cisco VNI Forecast에 대한 자세한 내용을 확인하려면 **Cisco 웹사이트** 또는 **2015~2020년 연례 VNI Forecast**의 Cisco 블로그 게시물을 확인하십시오.

결론

결론

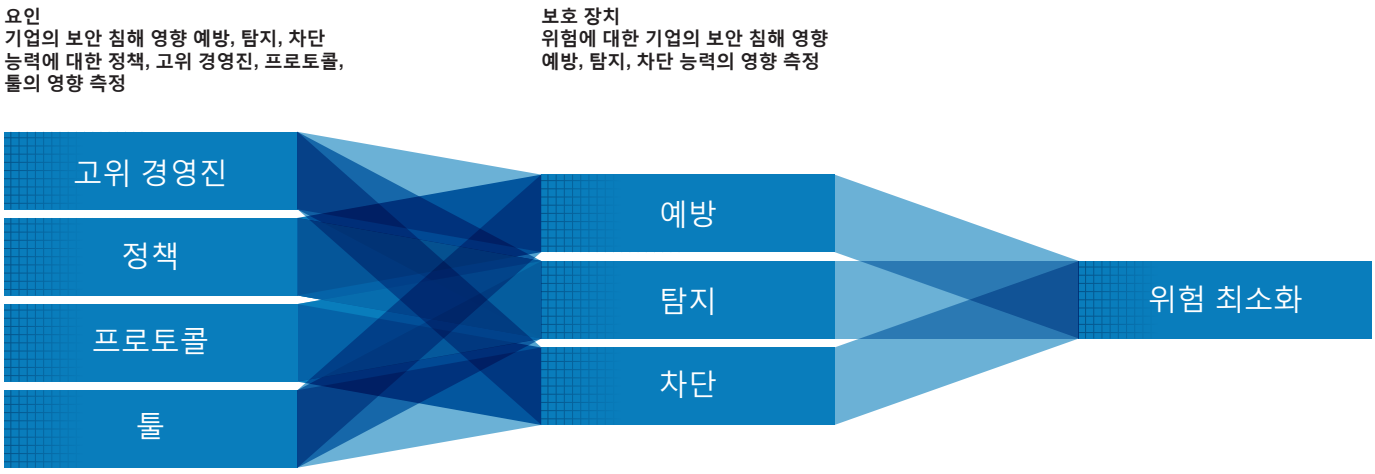
공격 범위가 빠르게 확장됨에 따라 상호 연결된 통합 보안 방식의 필요성 대두

Cisco의 보안 기능 벤치마크 조사(49페이지)에서 확인했듯이, 데이터 분석 과정에서 조직이 위험을 최소화할 방안과 관련 결정 사항을 파악할 수 있었습니다. 이를 통해 조직이 위험에 관한 노출을 크게 줄일 수 있는 보안 관련 투자 영역을 확인할 수 있었습니다. Cisco는 시스템 중단 비율 및 보안 침해 기간을 파악하여 위험을 측정했습니다(보안 침해 기간 및 영향을 받는 시스템에 관해서는 55페이지의 **그림 53** 참조).

조직이 위험에 대해 효과적인 보호 장치를 마련하는 방법을 파악하려면 조직이 위험을 예방하거나 탐지 및 차단하는 능력에 영향을 주는 요인부터 조사해야 합니다(**그림 68** 참조). 이러한 요인에는 다음과 같은 요소가 포함되어야 합니다.

- **고위 경영진:** 최고 경영진이 보안을 우선적으로 고려해야 합니다. 그래야 공격을 차단할 수 있을 뿐 아니라 예방도 가능합니다. 또한 경영진은 보안 프로그램 효율성 평가를 위한 측정 기준을 명확하게 수립해야 합니다.
- **정책:** 정책은 위험 차단과 긴밀하게 연관되어 있습니다. 네트워크, 시스템, 애플리케이션, 기능 및 데이터에 대한 액세스 권한 제어는 보안 침해로 인한 피해를 완화하는 데 도움이 됩니다. 또한, 보안 방식을 정기적으로 검토하도록 하는 정책을 통해 공격을 예방할 수 있습니다.
- **프로토콜:** 적합한 프로토콜을 적용하면 보안 침해를 방지 및 탐지할 수 있을 뿐 아니라 이를 차단하는 데도 큰 도움이 됩니다. 특히 네트워크의 연결 활동을 정기적으로 검토하여 보안 조치가 수행되고 있는지를 확인하는 것은 보안 침해 방지와 차단 모두를 위한 핵심 작업입니다. 장기간에 걸쳐 보안 방식을 정기적, 공식적, 전략적으로 검토 및 개선하는 방식도 도움이 됩니다.
- **툴:** 보안 침해의 피해를 완화하려면 툴을 신중하고 적절하게 적용하는 것이 가장 중요합니다. 사용자는 현재 보유 중인 툴을 통해 보안 침해 탐지 및 방지와 차단에 핵심적인 피드백을 검토하고 제공할 수 있습니다.

그림 68 위험 최소화를 위한 요인 및 보호 장치



출처: Cisco 2017 보안 기능 벤치마크 조사

2017년 그래픽 다운로드: www.cisco.com/go/acr2017graphics

조직에서 사용하는 예방, 탐지, 차단 등의 보안 관련 보호 장치는 조직이 위험을 최소화할 수 있는 능력에 영향을 미칩니다(**그림 68** 참조).

이러한 보호 장치는 다음 요소를 포함해야 합니다.

- **예방:** 보안 침해로 인한 피해를 최소화하려면 직원들이 보안 장애와 문제를 보고해야 합니다. 또한, 보안 프로세스와 절차를 명확하게 정의하고 철저하게 파악하는 것이 중요합니다.
- **탐지:** 보안 침해로 인한 피해를 최소화하기 위한 최고의 탐지 방법은 큰 보안 사고로 발전하기 전에 보안 취약점을 조직에서 찾아낼 수 있도록 하는 방법입니다. 이러한 목표를 달성하려면 사고 관련 정보를 분류하는 효과적인 시스템이 반드시 필요합니다.
- **차단:** 보안 침해를 효율적으로 차단하려면 사고 대응 및 추적에 대해 명확하게 문서화된 프로세스와 절차가 있어야 합니다. 또한, 조직은 강력한 프로토콜을 통해 위기 대응 방식을 관리해야 합니다.

보안 전문가는 한 두 가지 동인과 보호 장치만 적용하여 보안 문제를 해결했다고 확신해서는 안 됩니다. 즉, 모든 동인을 고려하고 모든 보호 장치를 활용해야 합니다. 보안 팀은 조직의 약점(예: 관리자의 지원 수준이 낮음, 보안 침해 차단을 위한 툴 부재)을 분석하고 보안 관련 투자 영역을 판단해야 합니다.

핵심 목표: 공격자가 공격할 수 있는 영역 축소

방어자가 최우선으로 취해야 하는 조치는 공격자가 아무런 제약 없이 공격을 수행할 수 있는 영역을 줄이고(완전히 없애는 것이 가장 좋음) 공격자의 존재를 파악하는 것입니다. 실제로 모든 공격을 중지하거나 모든 보호 대상을 보호할 수는 없습니다. 하지만 공격 수행 영역을 완벽히 없애는 것만으로도 사이버 범죄자들이 탐지를 피한 채 중요 시스템과 데이터에 접근하는 상황을 효율적으로 막을 수 있습니다.

이 보고서에서는 공격자들이 사용자와 시스템을 공격하는 데 사용하는 여러 가지 방식을 분류했습니다. 이러한 공격 방식의 범주(정찰, 공격 수단 구축, 전송, 설치)를 지정할 때는 공격 체인에서 공격이 일반적으로 전개되는 영역을 기준으로 했습니다. 공격자들이 취약점 및 기타 약점을 이용해 디바이스나 시스템에 접근하여 공격을 실행한 다음 원하는 목적을 달성하는 시기, 방법 및 위치를 설명하기 위해 이러한 방식이 사용되었습니다.

방어자는 공격자들이 기본적으로 사용하는 프로세스를 사전에 파악할 수 있도록 보안 방식을 조정하는 것이 좋습니다. 예를 들어 정찰 단계 중에 공격자의 능력을 약화시키려는 보안 팀은 다음 조치를 취해야 합니다.

- **최신 위협 및 취약점 관련 정보 수집**
- **네트워크에 대한 액세스를 제어하고 있는지 확인**
- **확장되는 공격 범위에 대한 조직의 노출 제한**
- **컨피그레이션 관리**
- **이 작업을 통해 알림을 받는 일관된 대응 방식과 절차 개발**

공격 수단으로 구축된 위협이 전송되면 방어자들은 확보한 모든 툴을 적용해 위협의 확산 및 악화를 방지해야 합니다. 그러려면 통합 보안 아키텍처가 반드시 필요합니다. 통합 보안 아키텍처에서는 위협을 실시간으로 파악할 수 있을 뿐 아니라 자동화된 탐지와 방어도 실행할 수 있습니다. 위협 탐지를 개선하려면 이러한 기능이 필수적입니다.

설치 단계에서 보안 팀은 피해 대응 및 조사를 진행하면서 환경 상태를 지속적으로 파악해야 합니다. 해당 환경이 단순하고 자동화된 개방형 환경이며 방어자들이 앞서 언급한 기타 사전 대응 단계를 수행했다면 보안 팀은 리소스를 집중 투입하여 기업이 다음과 같은 핵심 질문에 답할 수 있도록 지원할 수 있습니다.

- **공격자가 액세스한 대상은 무엇인가?**
- **공격자가 액세스 권한을 확보할 수 있었던 이유는 무엇인가?**
- **공격자의 이동 경로는 어떠한가?**
- **공격자가 네트워크에서 계속 작업 중인가?**

보안 팀은 이러한 정보를 파악함으로써 추가 공격에 대한 적절한 조치를 취할 수 있을 뿐 아니라, 경영진과 이사회에 위험 노출 가능성 및 공개해야 하는 사안을 알릴 수 있습니다. 이러한 과정 이후, 기업은 피해 당시 확인된 보안 격차, 즉 공격자들에게 공격 영역을 제공했던 취약점을 해결하고자 포괄적 제어 및 차단 기능 여부를 확인하는 과정을 시작할 수 있습니다.

회사 소개

Cisco는 지능형 사이버 보안을 현실 세계에 제공하여 사이버 공격에 대해 광범위한 보호 포트폴리오 솔루션을 제공하는 업체입니다. 보안에 대한 Cisco의 위협 대응형, 조직적 접근 방식은 복잡성과 프래그멘테이션을 줄이는 동시에 공격 전, 중, 후에 뛰어난 가시성, 일관된 제어, 지능형 위협 차단을 제공합니다.

CSI(Collective Security Intelligence) 에코시스템의 위협 연구진은 다양한 디바이스와 센서, 공개 및 비공개 피드, 오픈 소스 커뮤니티에서 얻은 텔레메트리를 사용하여 업계 최고의 위협 인텔리전스를 하나로 결합했습니다. 이 정보의 양은 매일 수십억 건의 웹 요청, 수백만 개의 이메일, 악성코드 샘플, 네트워크 침입에 해당합니다.

Cisco의 정교한 인프라와 시스템은 이 텔레메트리를 사용하여 머신 러닝 시스템 및 연구진들이 네트워크, 데이터 센터, 엔드포인트, 모바일 디바이스, 가상 시스템, 웹, 이메일 전반을 비롯해, 클라우드에서 위협 정보를 추적하여 침입 경로를 식별하고 사건 발생을 억제할 수 있도록 합니다. 이를 통해 얻은 인텔리전스는 Cisco 제품 및 서비스에 대한 실시간 보호로 변환되어 전 세계 Cisco 고객에게 즉시 전달됩니다.

Cisco의 위협 대응형 보안 접근법에 대한 자세한 내용은 **www.cisco.com/go/security**에서 확인하십시오.

Cisco 2017 연례 사이버 보안 보고서에 도움 주신 분들

CloudLock

Cisco의 회사인 CloudLock은 조직이 클라우드를 안전하게 사용할 수 있도록 지원하는 CASB(Cloud Access Security Broker) 솔루션을 제공하는 최고의 보안업체로, 사용자, 데이터 및 애플리케이션 전반에 걸쳐 SaaS(Software-as-a-service), PaaS (Platform-as-a-service) 및 IaaS(Infrastructure-as-a-service) 환경에 대한 가시성과 제어 기능을 제공합니다. 또한, 데이터 과학자들이 이끄는 CyberLab 및 크라우드소싱 보안 분석을 통해 실제로 활용 가능한 사이버 보안 인텔리전스도 제공합니다. 자세한 내용은 **https://www.cloudlock.com**을 참조하십시오.

Security and Trust Organization

Cisco의 Security and Trust Organization은 이사회 및 전 세계 리더들의 마음속에 있는 가장 중요한 문제 두 가지를 해결하겠다는 Cisco의 약속에 역점을 두고 있습니다. 이 조직의 핵심 임무에는 Cisco의 공공 및 민간 부문 고객을 보호하는 일, Cisco의 제품 및 서비스 포트폴리오 전반에 걸쳐 Cisco Secure Development Lifecycle 및 Trustworthy Systems를 지원하고 보장하는 일, 그리고 계속해서 진화하는 위협으로부터 Cisco 기업을 보호하는 일이 포함됩니다. Cisco는 사람, 정책, 프로세스, 기술을 포함해 널리 퍼져 있는 보안과 신뢰에 대한 전체적인 접근 방식을 취하고 있습니다. Security and Trust Organization은 InfoSec, Trustworthy Engineering, Data Protection and Privacy, Cloud Security, Transparency and Validation, Advanced Security Research and Government 등에 초점을 맞춰 운영 효율성을 추진하고 있습니다. 자세한 내용은 **http://trust.cisco.com**을 참조하십시오.

Global Government Affairs

Cisco는 기술 부문을 지원하는 공공 정책과 규정 마련을 돕고 정부의 목표 달성을 돕기 위해 다양한 레벨에서 일하고 있습니다. Global Government Affairs 팀은 기술 지향적 공공 정책과 규정을 개발하고 있습니다. 업계 이해관계자들 및 협회 파트너들과 함께 협력하여 업무를 수행하면서 정부 지도자들과 관계를 형성하여 Cisco의 비즈니스 및 전반적인 ICT 도입과 관련한 정책에 영향을 미치고, 세계적, 국가적, 지역적 레벨 등에서 정책 결정의 틀을 마련하는 방안을 모색합니다. Government Affairs 팀은 전직 선출직 공무원, 국회 의원, 규제 담당자, 미 정부 고위 공직자, 정부 업무 전문가들로 구성되어 있는데, 이들은 Cisco가 전 세계에서 기술 사용을 촉진하고 보호하도록 돕는 사람들입니다.

Cognitive Threat Analytics

Cisco Cognitive Threat Analytics는 클라우드 기반 서비스로서 네트워크 트래픽에 대한 통계 분석을 통해 보안 사고, 보호 대상 네트워크에서 활동하는 악성코드, 기타 보안 위협을 찾아냅니다. 행동 분석 및 이상 징후 탐지를 통해 악성코드 감염이나 데이터 보안 침해의 증상을 파악하여 경계 기반 방어의 허점을 보완합니다. Cognitive Threat Analytics는 고급 통계 모델링 및 머신 러닝을 사용하여 독자적으로 새로운 위협을 식별하고 파악한 내용을 학습하며 시간을 두고 조정합니다.

IntelliShield Team

IntelliShield 팀은 Cisco Security Research and Operations 및 외부 소스로부터 수집한 데이터와 정보를 대상으로 취약점 및 위협 조사, 분석, 통합, 상관관계 분석을 수행하여 각종 Cisco 제품과 서비스를 지원하는 IntelliShield Security Intelligence Service를 제공합니다.

Talos Security Intelligence and Research Group

Talos는 Cisco의 위협 인텔리전스 조직으로, Cisco의 고객과 제품 및 서비스를 위해 탁월한 보호를 전담하는 엘리트 보안 전문가 그룹입니다. 최고의 위협 연구진이 첨단 시스템을 활용하여 알려진 혹은 새로운 위협을 탐지, 분석, 차단하는 Cisco 제품을 위해 위협 인텔리전스를 구축합니다. Talos는 Snort.org, ClamAV, SenderBase.org, SpamCop의 공식 규칙 세트를 관리하며 Cisco CSI 에코시스템에 위협 인텔리전스를 제공하는 주요 팀입니다.

SR&O(Security Research and Operations)

SR&O(Security Research and Operations)는 업계 최고의 PSIRT(Product Security Incident Response Team)를 포함한 Cisco의 모든 제품과 서비스에 대한 위협 및 취약점 관리를 맡고 있습니다. SR&O는 Cisco 및 업계 기업들과의 협업을 통해, 그리고 Cisco Live나 Black Hat 등의 행사를 통해 진화하고 있는 위협 양상을 고객들이 이해할 수 있도록 돕고 있습니다. 또한, SR&O는 Cisco의 CTI(Custom Threat Intelligence)와 같은 새로운 서비스를 제공하고 있습니다. CTI 서비스는 기존의 보안 인프라에서 탐지되거나 차단된 적이 없는 침해 지표를 파악합니다.

Cisco VNI(Visual Networking Index)

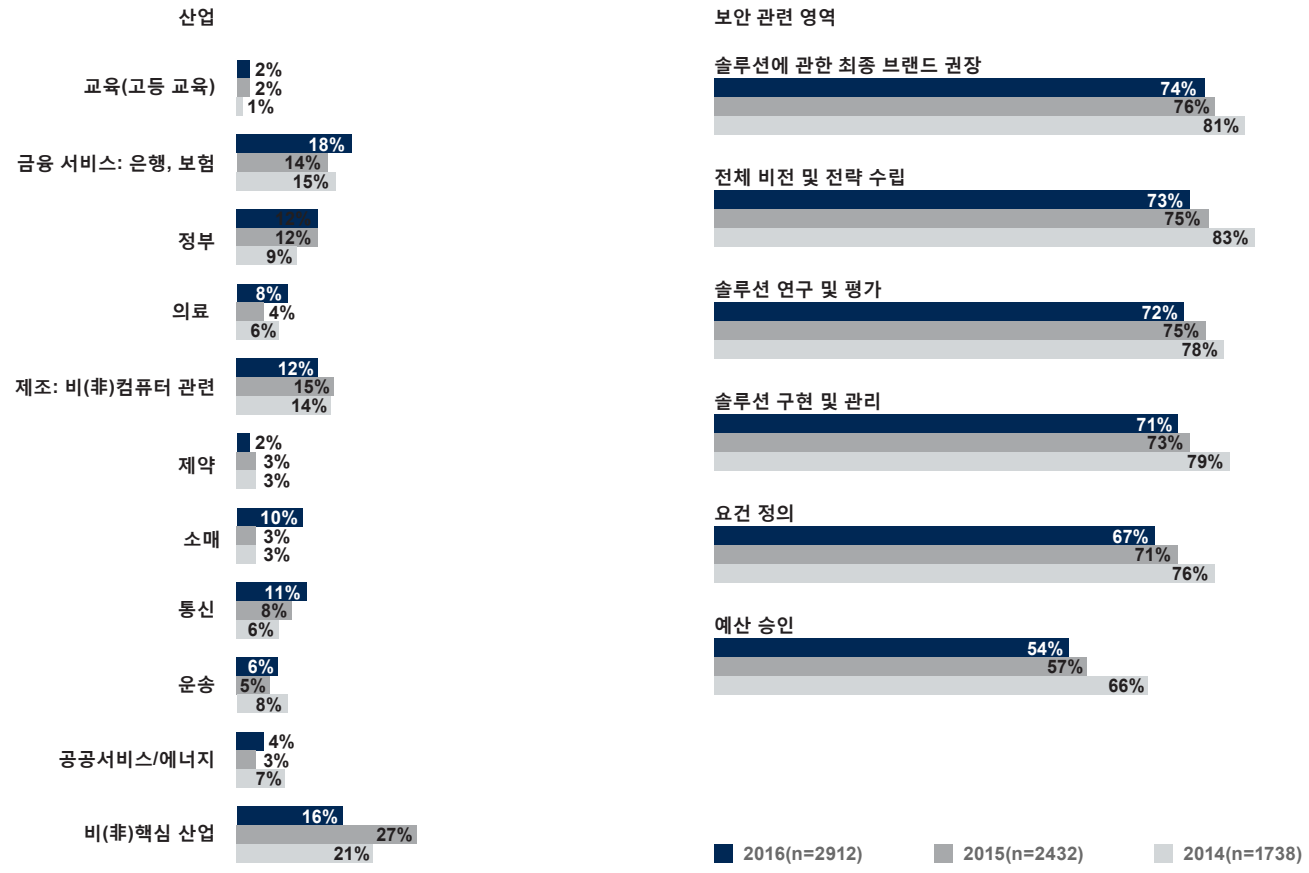
Cisco VNI Global IP Traffic Forecast(2015~2020년)는 독립 분석 전망 및 실제 네트워크 사용 데이터를 기반으로 합니다. 이 기초 데이터에 Cisco 자체의 글로벌 IP 트래픽 및 서비스 도입 예측 데이터를 접목시킵니다. 방법론에 대한 자세한 내용은 보고서 전문을 참조하십시오. 지난 11년간 Cisco VNI 연구 조사는 인터넷의 성장을 평가하는 지표로 신뢰받고 있습니다. 각국의 정부 기관, 네트워크 규제 기관, 학계, 통신 기업, 기술 전문가, 산업 및 비즈니스 미디어, 분석가들이 디지털 미래를 계획하고 대비하는 데 이 연례 조사를 활용하고 있습니다.

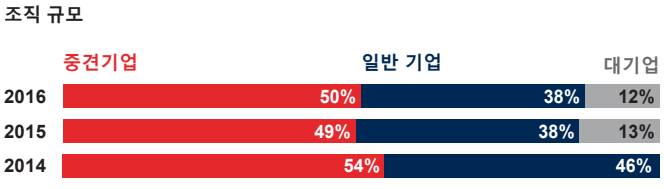
부록

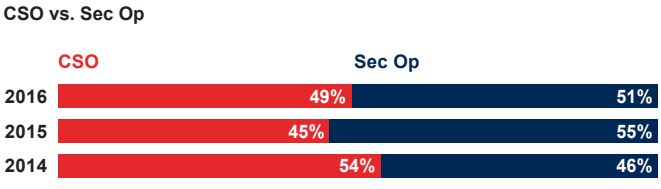
부록

Cisco 2017 보안 기능 벤치마크 조사

그림 69 보안 기능 벤치마크 조사







출처: Cisco 2017 보안 기능 벤치마크 조사

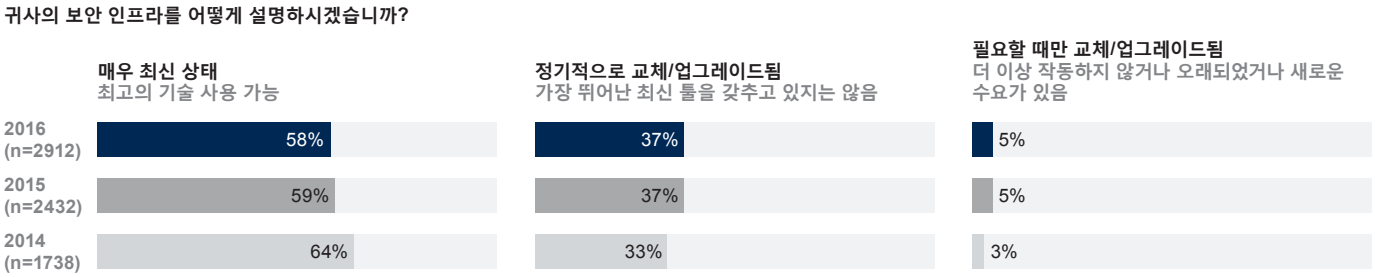
그림 70 전담 보안 전문가 수

	2014(n=1738)	2015(n=2432)	2016(n=2912)
1-9	18%	17%	15%
10-19	16%	18%	17%
20-29	12%	17%	13%
30-39	8%	9%	8%
40-49	4%	4%	6%
50-99	19%	16%	19%
100-199	9%	9%	9%
200 이상	15%	10%	12%
보안 전담 전문가 수 중앙값	30	25	33

출처: Cisco 2017 보안 기능 벤치마크 조사

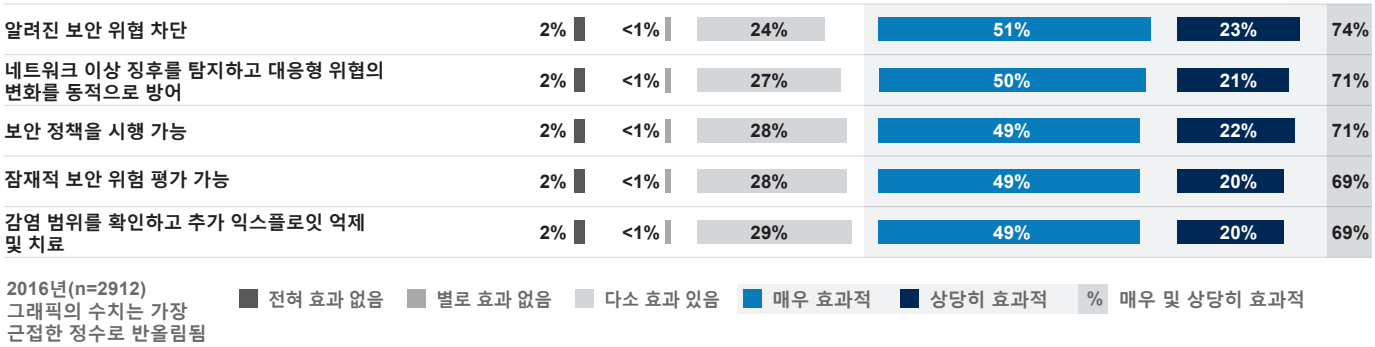
인식

그림 71 보안 전문가 대부분이 보안 인프라가 최신 상태라고 생각함



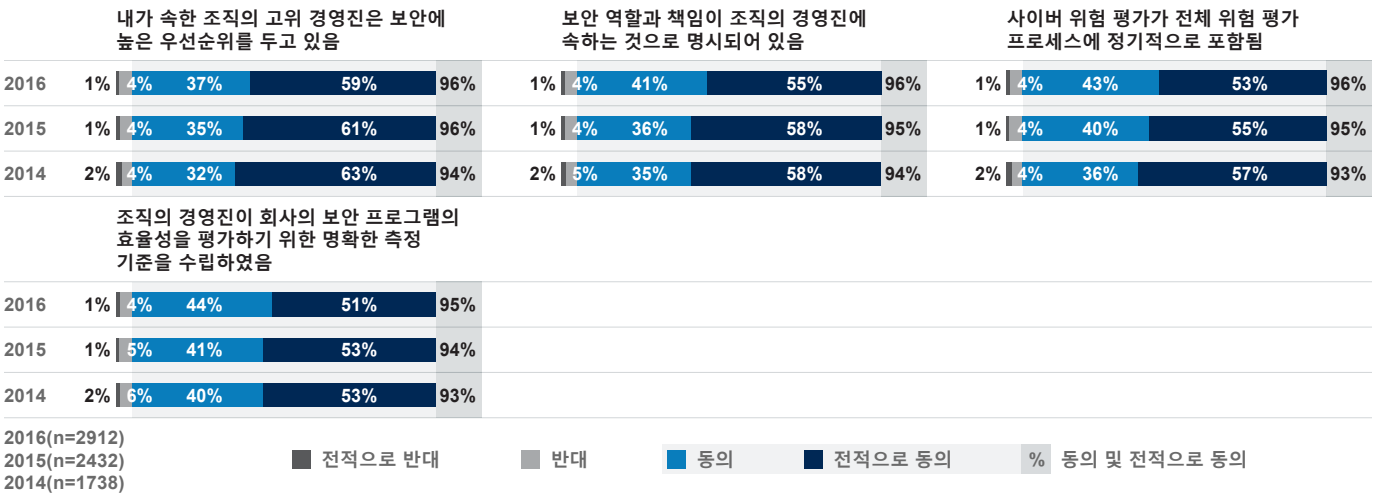
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 72 다양한 보안 툴이 매우 효과적이라고 생각하는 보안 전문가의 비율



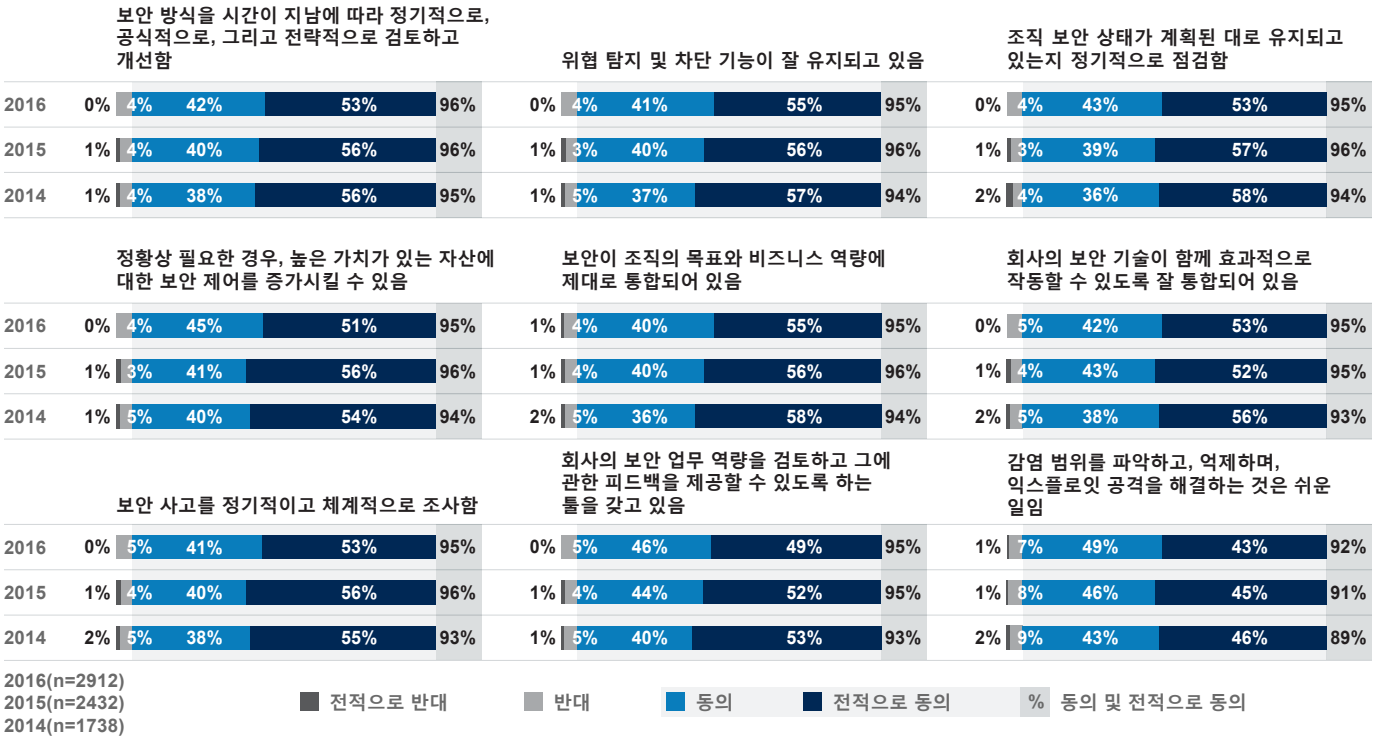
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 73 경영진이 보안을 높은 우선 순위로 고려하고 있다고 생각하는 보안 전문가의 비율



출처: Cisco 2017 보안 기능 벤치마크 조사

그림 74 보안 운영 환경 구축 설명에 매우 동의하는 응답자의 비율



출처: Cisco 2017 보안 기능 벤치마크 조사

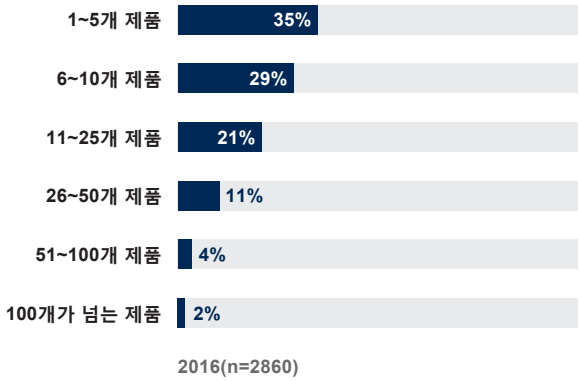
제약

그림 75 보안 유지의 최대 장애 요소

	2015(n=2432)	2016(n=2912)
예산상의 제약	39%	35%
호환성 문제	32%	28%
인증 요건	25%	25%
숙련 인력 부족	22%	25%
우선순위 경쟁	24%	24%
과중한 현재 업무량	24%	23%
지식 부족	23%	22%
검증될 때까지의 구매 주저	22%	22%
조직 문화/태도	23%	22%
해당 조직은 공격자들에게 높은 가치가 있는 표적이 아님	해당 없음	18%
보안이 경영진의 우선 순위가 아님	해당 없음	17%

출처: Cisco 2017 보안 기능 벤치마크 조사

그림 76 조직에서 사용 중인 보안 벤더와 제품의 수



출처: Cisco 2017 보안 기능 벤치마크 조사

그림 77 조직 규모별로 사용 중인 보안 벤더의 수

보안 환경에서 사용 중인 보안 벤더(브랜드, 제조업체)의 수	중견기업 (직원 수 250~1,000명)	일반기업 (직원 수 1,000~10,000명)	대기업 (직원 수 10,000명 이상)
1-5	46.9%	43.4%	39.9%
6-10	28.4%	30.9%	21.3%
11-20	17.6%	15.8%	23.1%
21-50	5.6%	7.1%	8.7%
50곳 초과	1.4%	2.8%	6.9%
전체 조직 수	1435	1082	333

출처: Cisco 2017 보안 기능 벤치마크 조사

그림 78 조직 규모별로 사용 중인 보안 제품의 수

보안 환경에서 사용 중인 보안 제품의 수	중견기업 (직원 수 250~1,000명)	일반기업 (직원 수 1,000~10,000명)	대기업 (직원 수 10,000명 이상)
1-5	37.9%	32.7%	25.1%
6-10	29.0%	30.1%	22.5%
11-25	19.8%	20.4%	23.7%
26-50	9.6%	10.5%	15.6%
51-100	3.0%	4.3%	7.8%
100 개초과	0.8%	1.9%	5.4%
전체 조직 수	1442	1084	334

출처: Cisco 2017 보안 기능 벤치마크 조사

그림 79 IT 예산 범위 내에서 제공되는 보안 예산의 연도별 감소

보안 예산이 IT 예산에 포함되어 있습니까? (IT 부서 구성원)	2014(n=1673)	2015(n=2374)	2016(n=2828)
모두 IT에 포함됨	61%	58%	55%
일부만 IT에 포함됨	33%	33%	36%
완전히 분리됨	6%	9%	9%

출처: Cisco 2017 보안 기능 벤치마크 조사

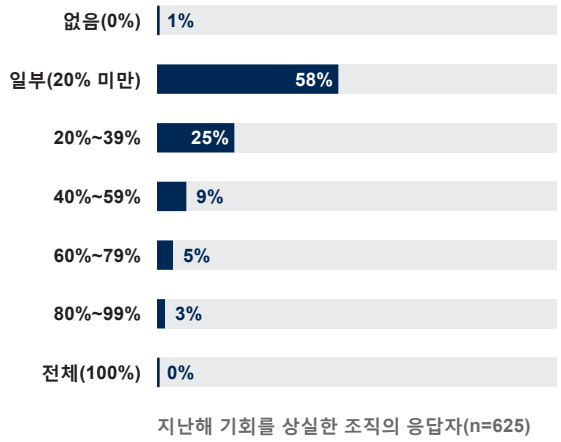
그림 80 보안 관련 지출의 연도별 감소(IT 예산 중 차지하는 비율)

보안 기능에 대한 IT 예산 지출 비율	2014(n=1673)	2015(n=2374)	2016(n=2828)
0%	7%	9%	10%
1-5%	4%	3%	4%
6-10%	12%	11%	16%
11-15%	23%	23%	27%
16-25%	29%	31%	26%
26%-50%	21%	19%	15%
51% 이상	5%	4%	2%

출처: Cisco 2017 보안 기능 벤치마크 조사

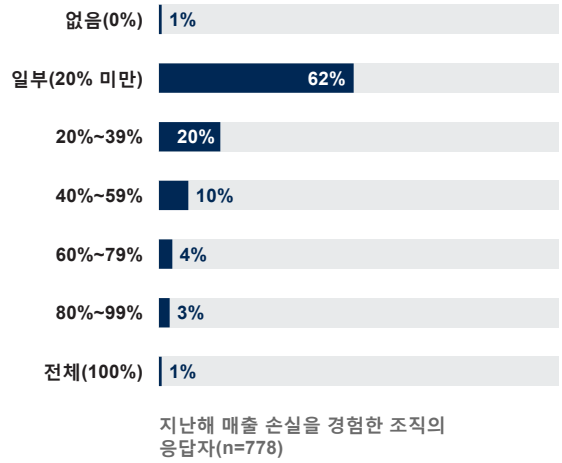
영향

그림 81 공격으로 인해 상실된 조직의 비즈니스 기회 비율



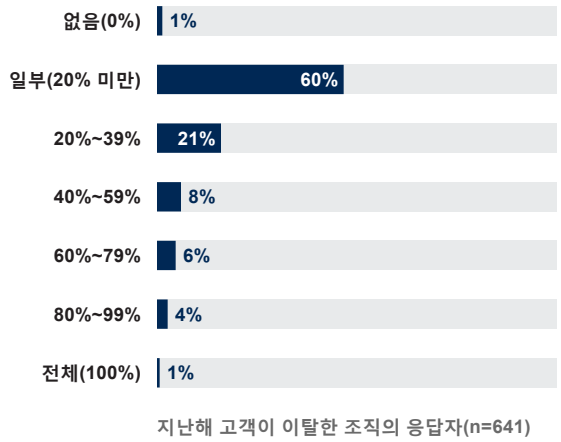
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 82 공격으로 인해 손실된 조직의 매출 비율



출처: Cisco 2017 보안 기능 벤치마크 조사

그림 83 공격으로 인해 이탈한 조직의 고객 비율



출처: Cisco 2017 보안 기능 벤치마크 조사

성과

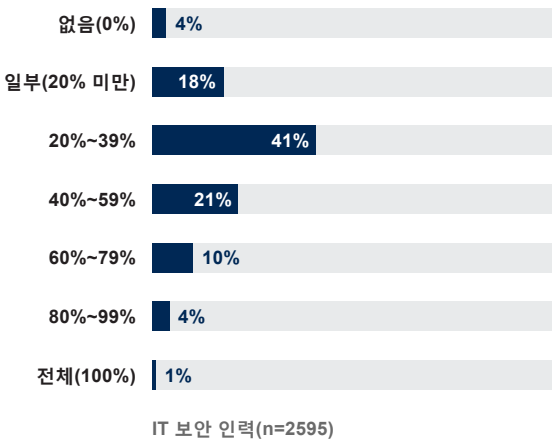
그림 84 조직의 아웃소싱 의존 비율

어떤 보안 서비스를 아웃소싱합니까?	2014 (n=1738)	2015 (n=2432)	2016 (n=2912)
자문 및 컨설팅	51%	52%	51%
감사	41%	47%	46%
사고 대응	35%	42%	45%
모니터링	42%	44%	45%
위협 인텔리전스	해당 없음	39%	41%
침해 복구	34%	36%	35%
없음/모두 내부 처리	21%	12%	10%

왜 서비스를 아웃소싱합니까?	2015 (n=2129)	2016 (n=2631)
비용 효율성이 높아서	53%	52%
편견 없는 시각을 원하므로	49%	48%
사고에 대해 더 시의적절하게 대응하기 위해서	46%	46%
내부 전문성이 부족해서	31%	33%
내부 리소스가 부족해서	31%	33%

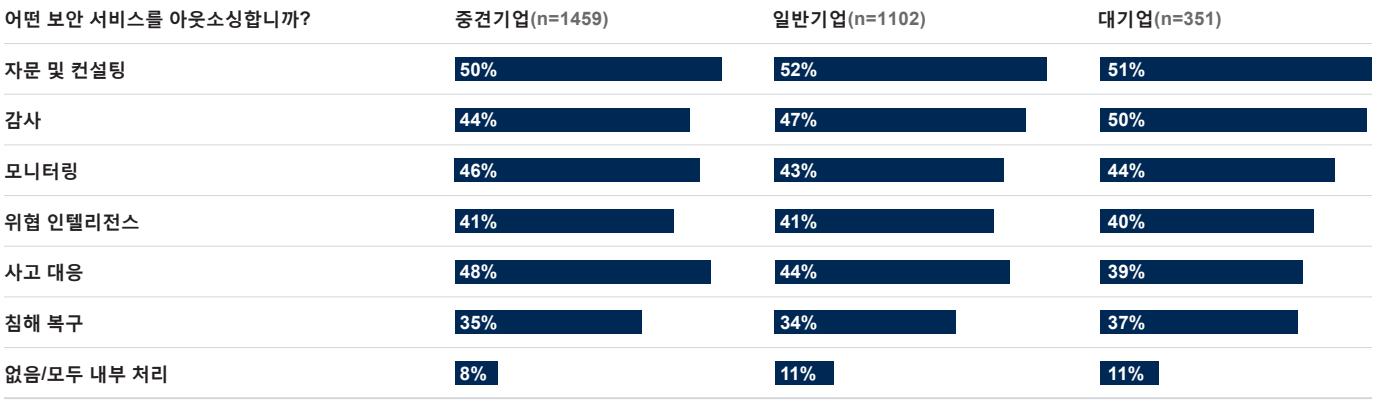
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 85 조직이 보안을 서드파티 벤더에 의존하는 비율



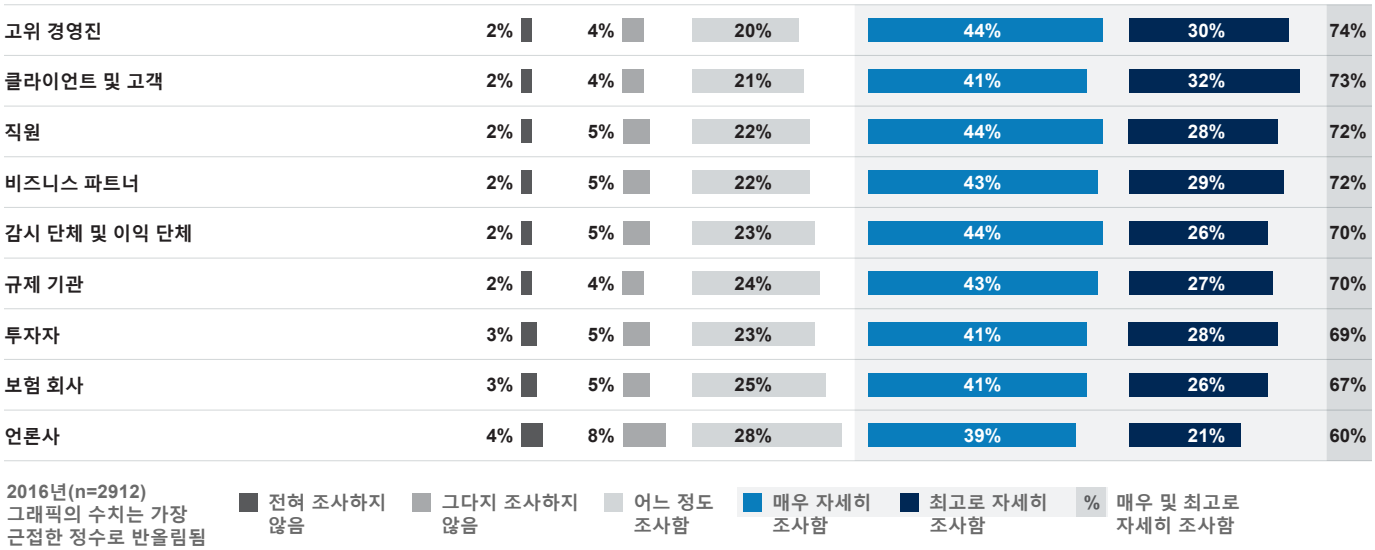
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 86 조직 규모별 보안 서비스 아웃소싱 비율



출처: Cisco 2017 보안 기능 벤치마크 조사

그림 87 조사 증가의 원인



출처: Cisco 2017 보안 기능 벤치마크 조사

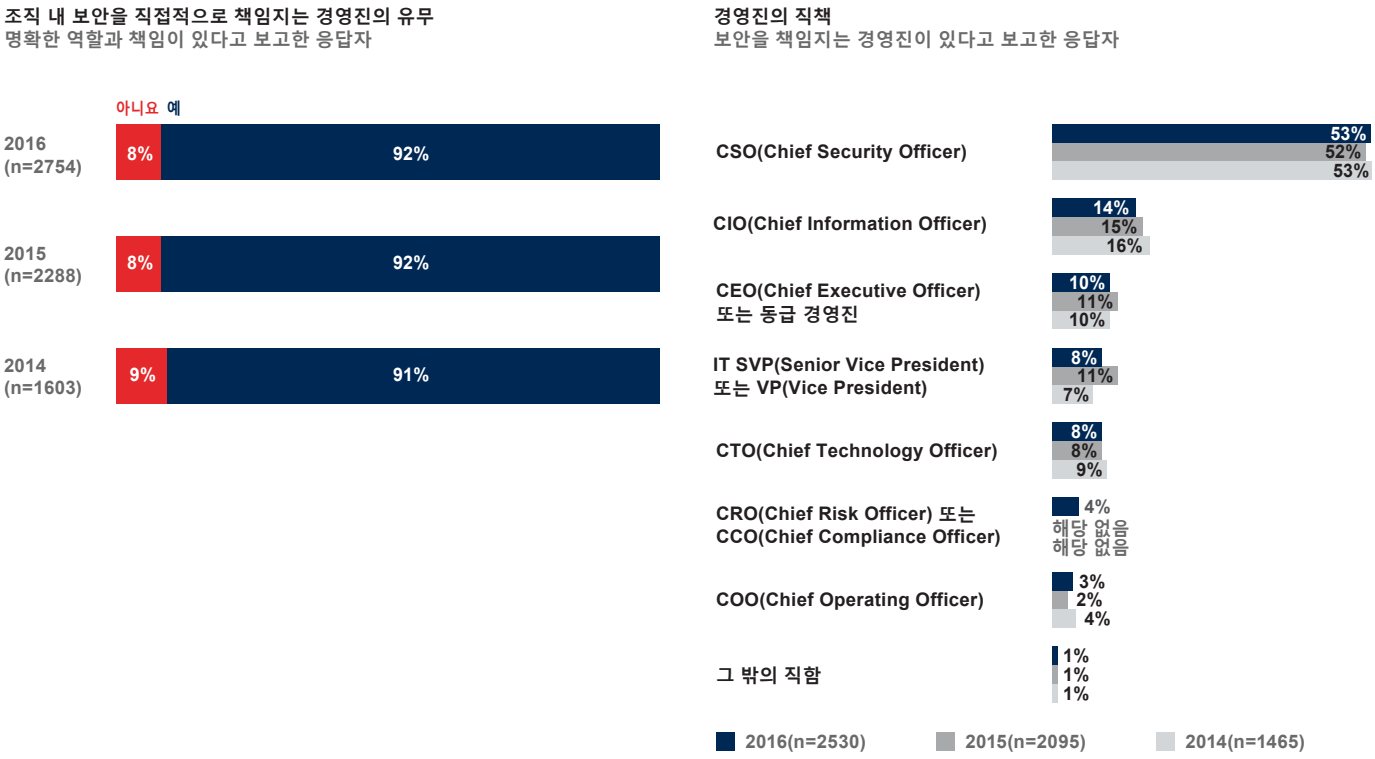
그림 88 오프프레미스 프라이빗 클라우드 및 서드파티 관리 온프레미스 호스팅의 증가

네트워크가 호스팅 되는 위치	2014(n=1727)	2015(n=2417)	2016(n=2887)
프라이빗 클라우드의 일환으로서의 온프레미스	50%	51%	50%
온프레미스	54%	48%	46%
외부 서드 파티가 관리하는 온프레미스	23%	24%	27%
오프프레미스 프라이빗 클라우드	18%	20%	25%
오프프레미스 퍼블릭 클라우드	8%	10%	9%

출처: Cisco 2017 보안 기능 벤치마크 조사

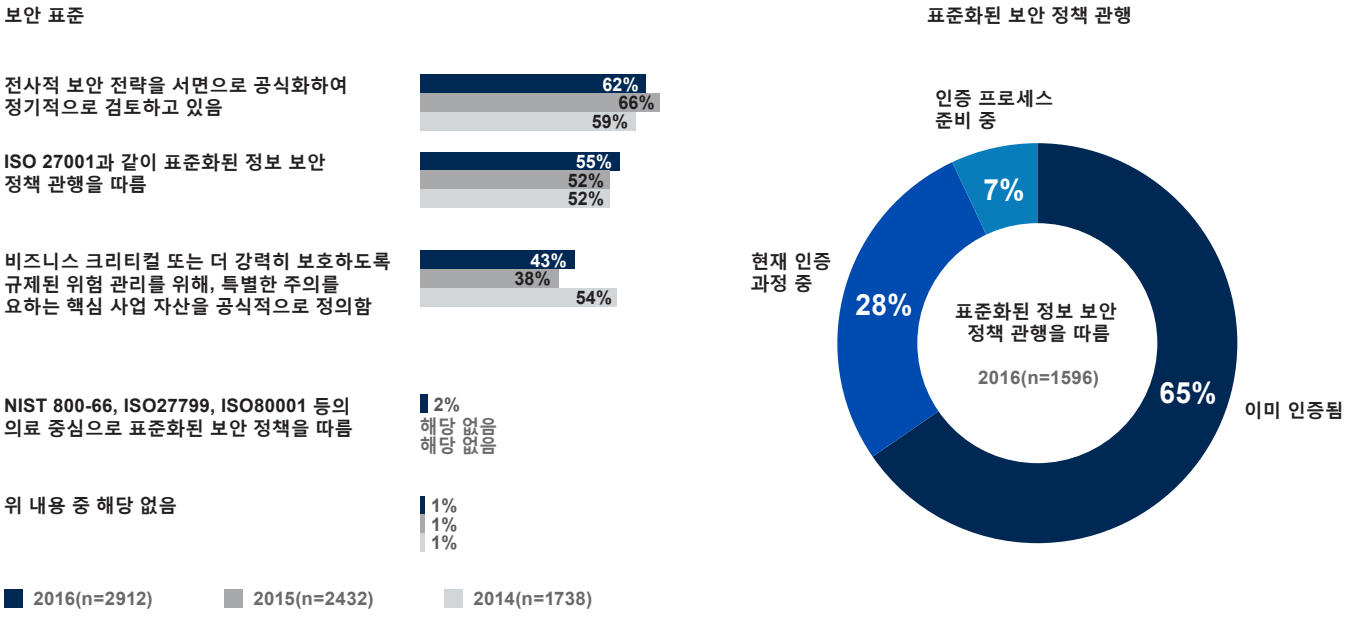
운영, 정책, 절차 및 기능

그림 89 보안 경영진이 있는 회사의 비율



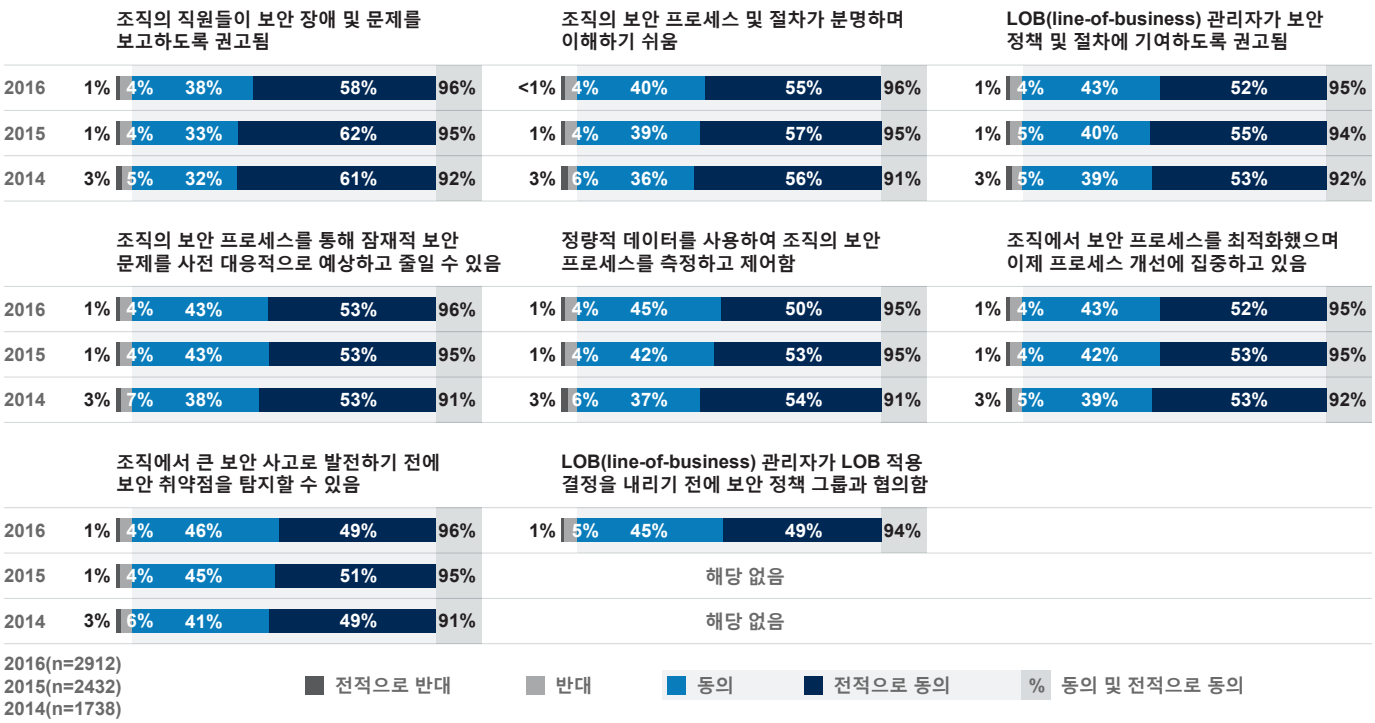
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 90 전사적인 공식 보안 전략이 있으며 표준화된 보안 정책 관행을 따르는 회사의 비율



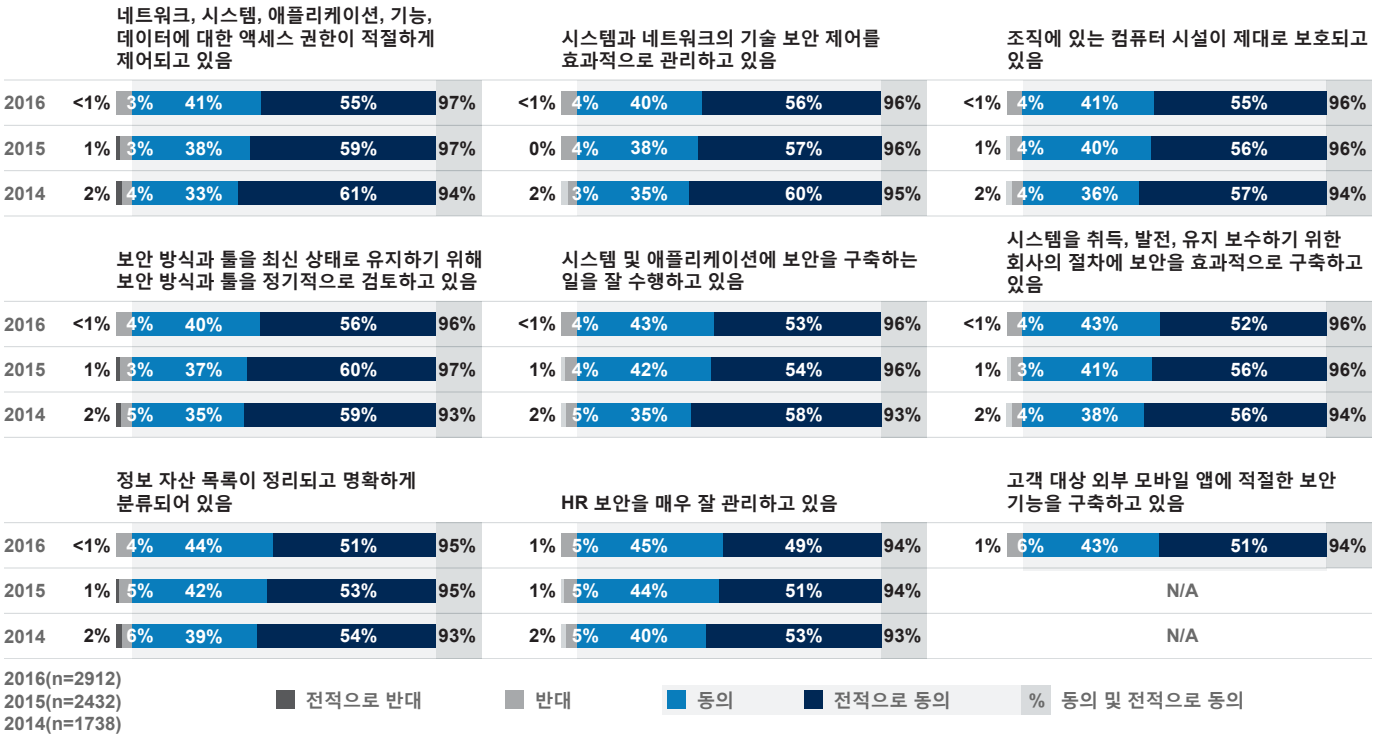
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 91 보안 프로세스 설명에 매우 동의하는 응답자의 비율



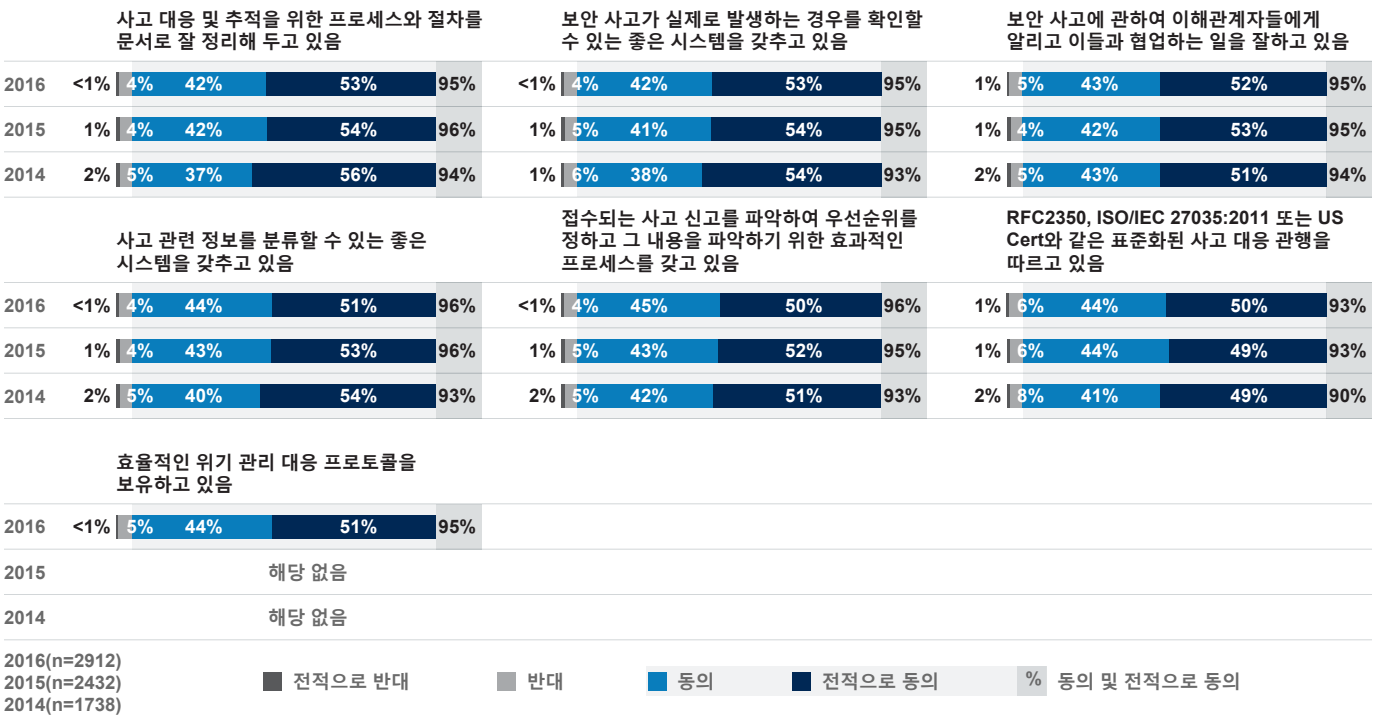
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 92 보안 프로세스 설명에 매우 동의하는 응답자의 비율



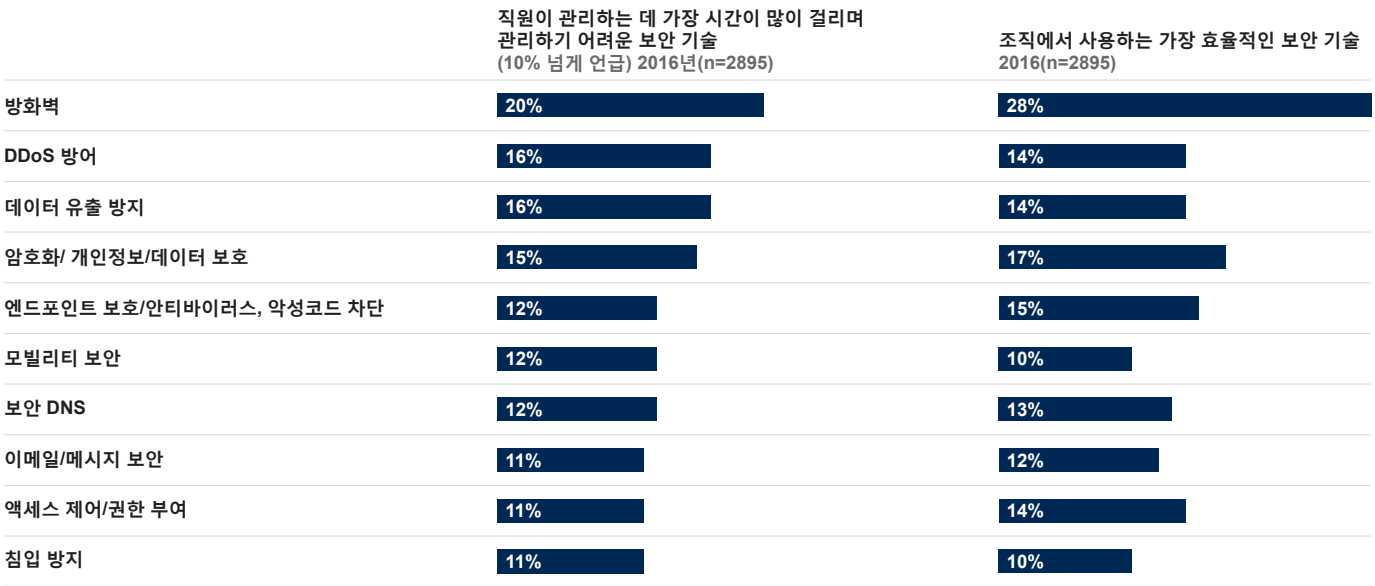
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 93 보안 제어 설명에 매우 동의하는 응답자의 비율



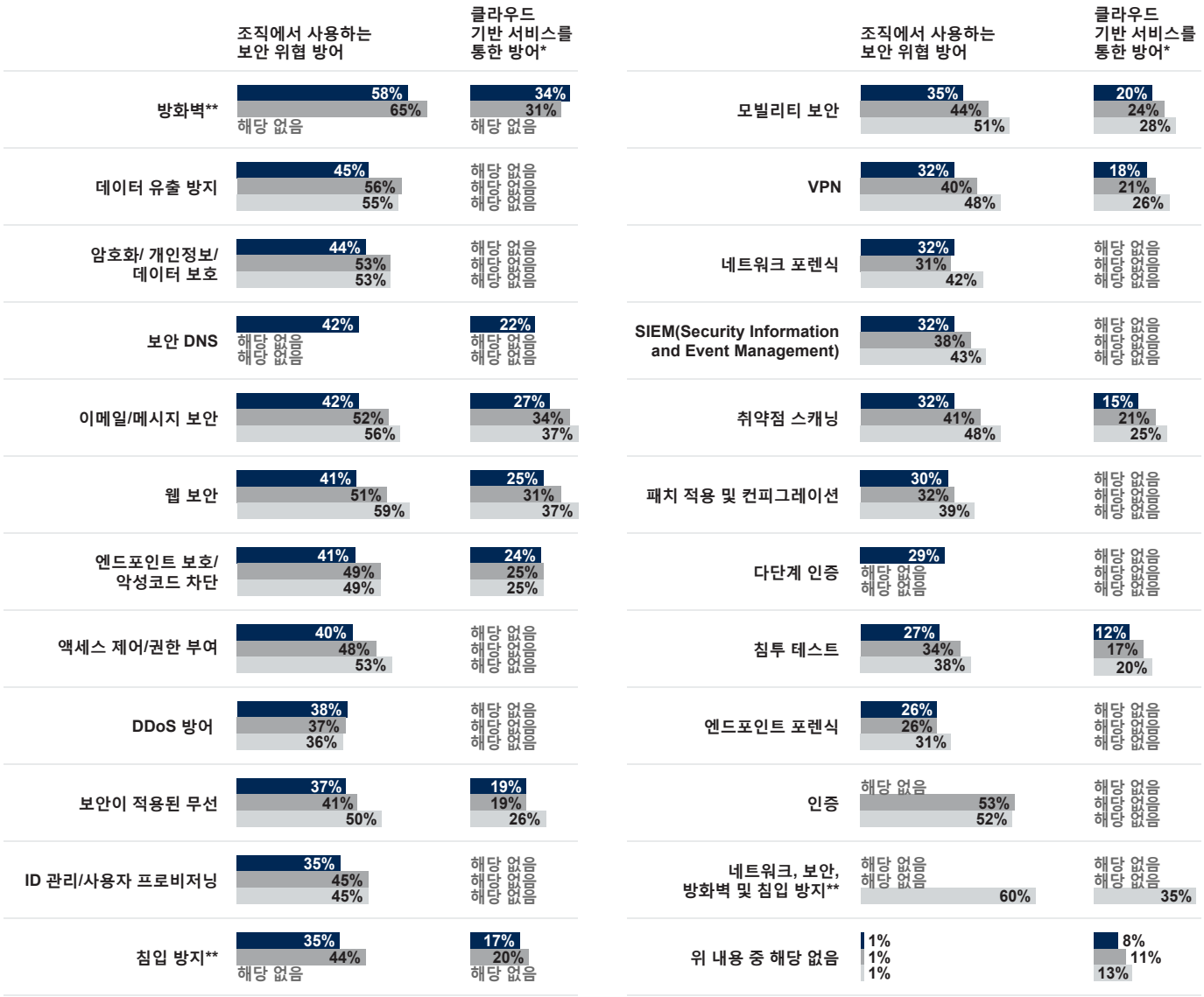
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 94 보안 기술 관리 및 효율성



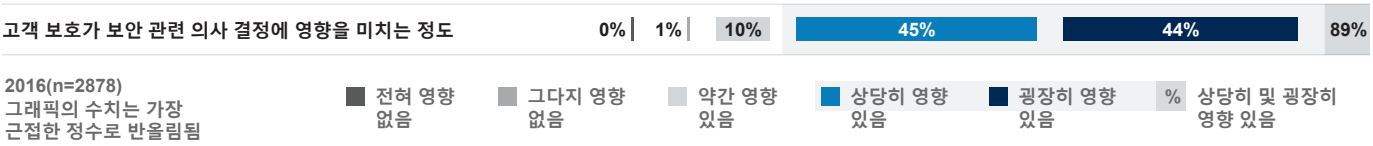
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 95 연도별 보안 위협 방어 사용 비율



출처: Cisco 2017 보안 기능 벤치마크 조사

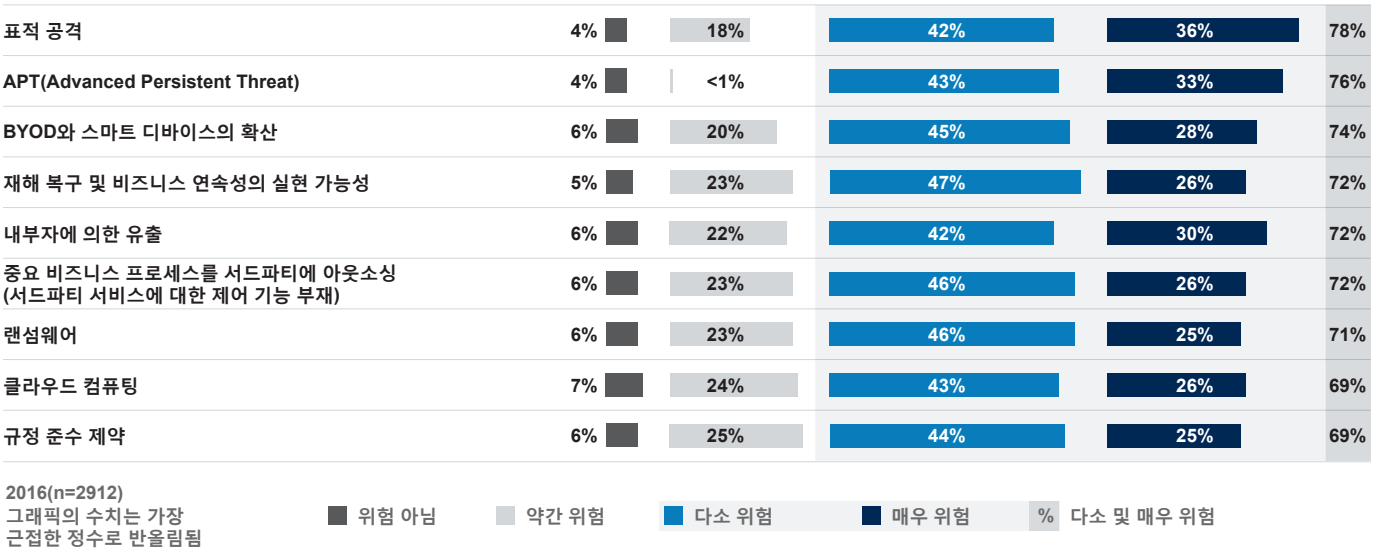
그림 96 고객 보호가 보안 관련 의사 결정에 영향을 미치는 정도



출처: Cisco 2017 보안 기능 벤치마크 조사

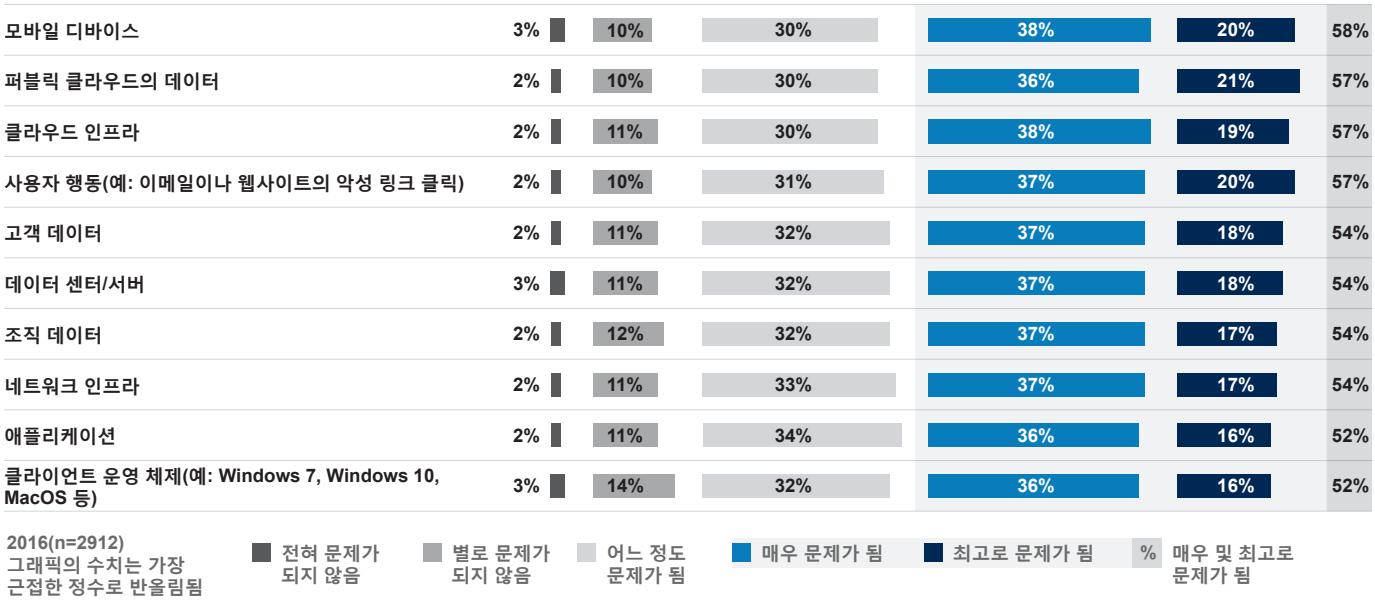
위험 및 취약점

그림 97 IT 보안 직원이 생각하는 사이버 공격 관련 주요 문제 발생 원인



출처: Cisco 2017 보안 기능 벤치마크 조사

그림 98 보안 전문가가 생각하는 사이버 공격 관련 주요 문제 발생 원인



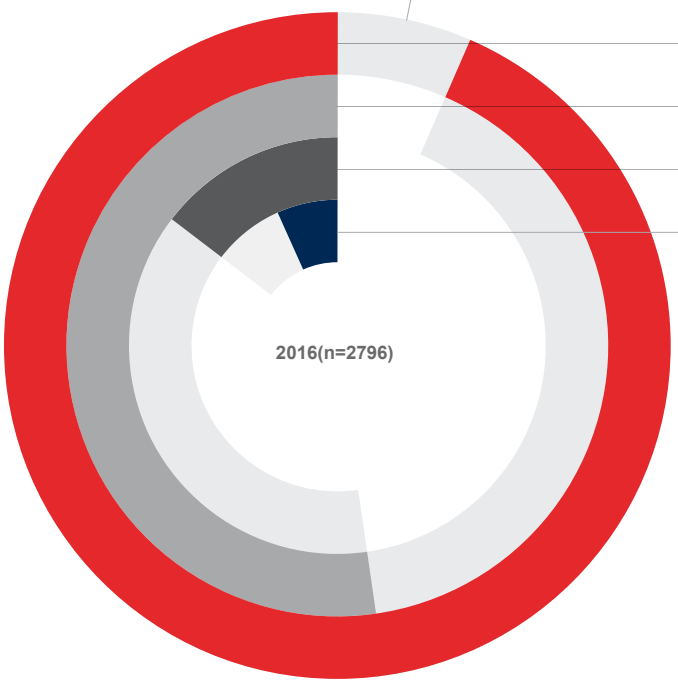
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 99 보안 팀의 업무 분포

출처: Cisco 2017 보안 기능 벤치마크 조사

사고 대응

그림 100 조사 또는 치료되는 보안 알림의 비율



7%	보안 알림 미발생
93%	보안 알림 발생
56%	확인된 알림 중 조사되는 알림 비율
28%	조사되는 알림 중 정상 알림 비율
46%	정상 알림 중 치료되는 알림 비율

조직에서 매일 확인되는 평균 알림 수	
5,000개 미만	50%
5,000~10,000개	15%
10,000~50,000개	11%
50,000~100,000개	8%
100,000~150,000개	6%
150,000개 초과	4%

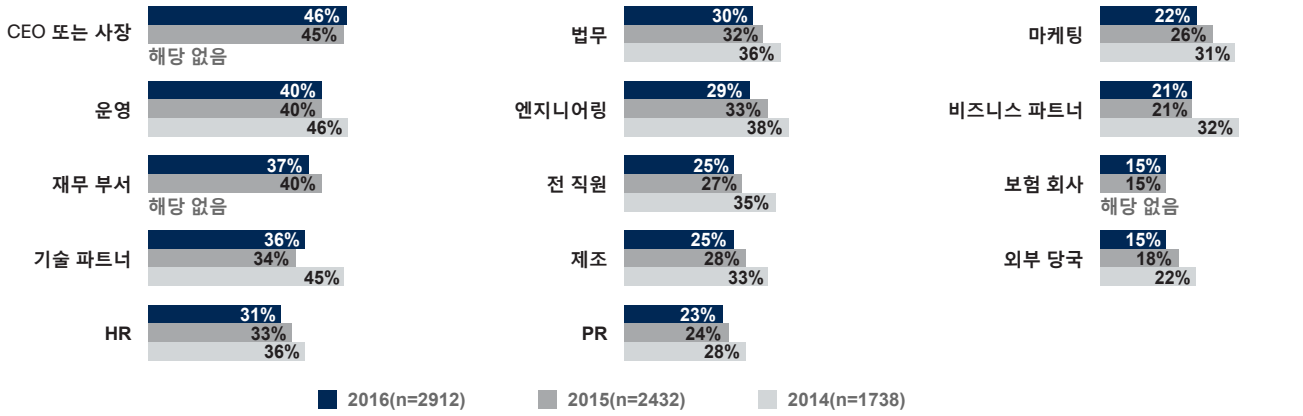
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 101 평균 보안 침해 탐지 소요 시간

	2016(n=2860)
8시간 이하	43%
9~24시간	25%
25~48시간	15%
2일 초과~1주 미만	7%
1~2주	5%
3주~1개월	3%
1~3개월	1%
3개월 초과~1년 미만	1%
1년 이상	0%

출처: Cisco 2017 보안 기능 벤치마크 조사

그림 102 사고 발생 시 보고를 받는 그룹



출처: Cisco 2017 보안 기능 벤치마크 조사

그림 103 보안 성능 평가를 위해 조직에서 사용하는 KPI

출처: Cisco 2017 보안 기능 벤치마크 조사

그림 104 보안이 침해된 시스템 분석을 위한 연도별 프로세스 사용 비율

감염 시스템 분석 프로세스	2014(n=1738)	2015(n=2432)	2016(n=2912)
방화벽 로그	61%	57%	56%
시스템 로그 분석	59%	53%	50%
네트워크 흐름 분석	53%	49%	49%
악성코드 또는 파일 회귀 분석	55%	48%	47%
레지스트리 분석	50%	47%	43%
풀패킷 캡처 분석	47%	38%	40%
IOC 탐지	38%	35%	38%
디스크 포렌식	40%	36%	36%
상호 연관된 이벤트/로그 분석	42%	37%	35%
메모리 포렌식	41%	34%	34%
외부 사고 대응/분석 팀	37%	33%	34%
위 내용 중 해당 없음	2%	1%	1%

출처: Cisco 2017 보안 기능 벤치마크 조사

그림 105 보안 사고 원인 제거를 위한 연도별 프로세스 사용 비율

보안 사고 원인 제거 프로세스	2014(n=1738)	2015(n=2432)	2016(n=2912)
악성 애플리케이션 격리 또는 제거	58%	55%	52%
침입 경로 분석	55%	55%	51%
악성 소프트웨어 통신 중단	53%	53%	48%
추가 모니터링	52%	48%	48%
정책 업데이트	51%	47%	45%
감염된 애플리케이션 통신 중단	48%	47%	43%
장기적 해결 방법 개발	47%	40%	41%
이미지로 재설치하여 시스템을 이전 상태로 복원	45%	41%	39%
위 내용 중 해당 없음	2%	1%	1%

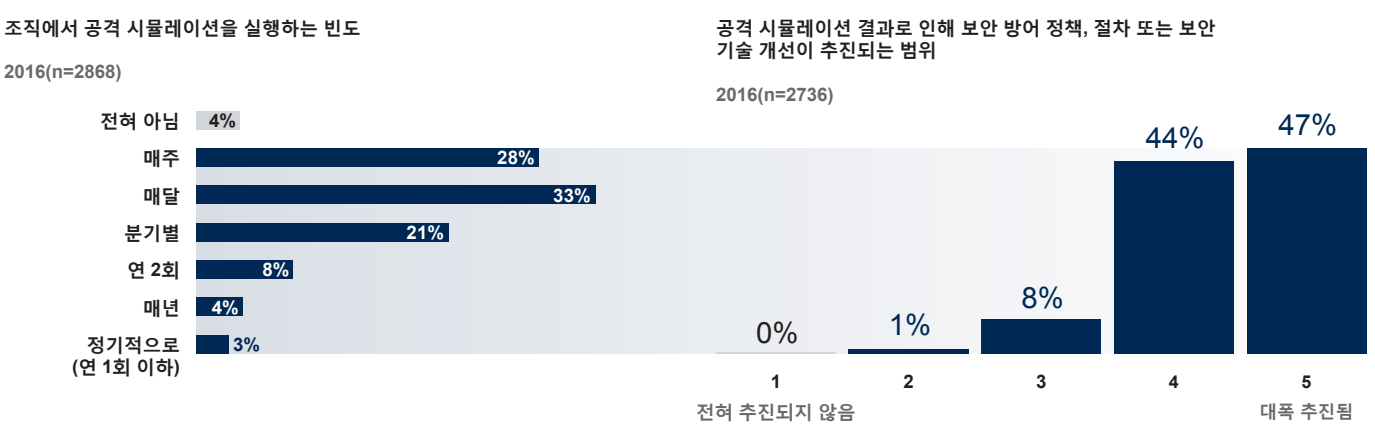
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 106 영향 받는 시스템 복원을 위한 연도별 프로세스 사용 비율

침해된 시스템의 복원 프로세스	2014(n=1738)	2015(n=2432)	2016(n=2912)
사고 후 식별된 약점에 근거한 추가적이거나 새로운 탐지 및 제어의 구현	60%	56%	56%
사고 이전의 백업에서 복원	57%	59%	55%
취약한 것으로 간주되는 애플리케이션에 대한 패치 및 업데이트	60%	55%	53%
차등 복원(사고로 인해 야기된 변경 사항 제거)	56%	51%	50%
골드 이미지 복원	35%	35%	34%
위 내용 중 해당 없음	2%	1%	1%

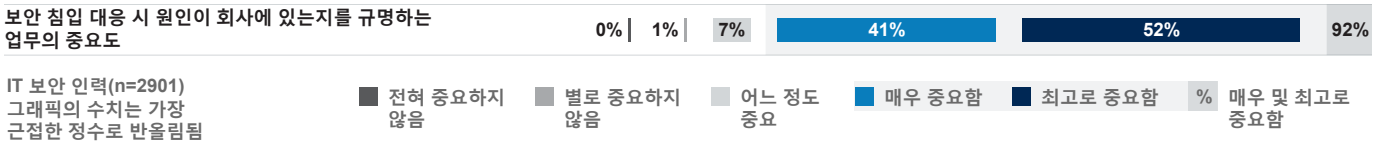
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 107 공격 시뮬레이션: 보안 방어 개선을 추진하는 빈도 및 범위



출처: Cisco 2017 보안 기능 벤치마크 조사

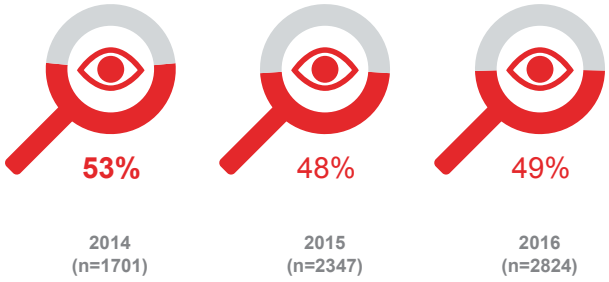
그림 108 보안 침해 원인 규명의 중요도



출처: Cisco 2017 보안 기능 벤치마크 조사

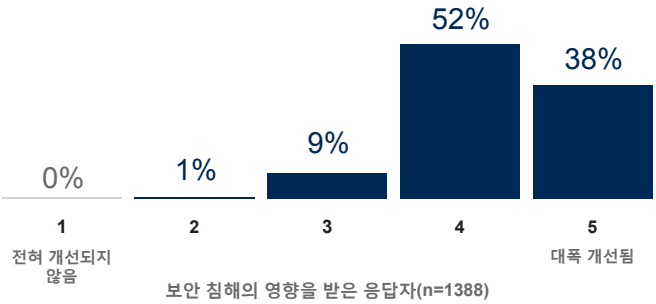
보안 침해 및 해당 영향

그림 109 공개 보안 침해를 경험한 조직의 비율



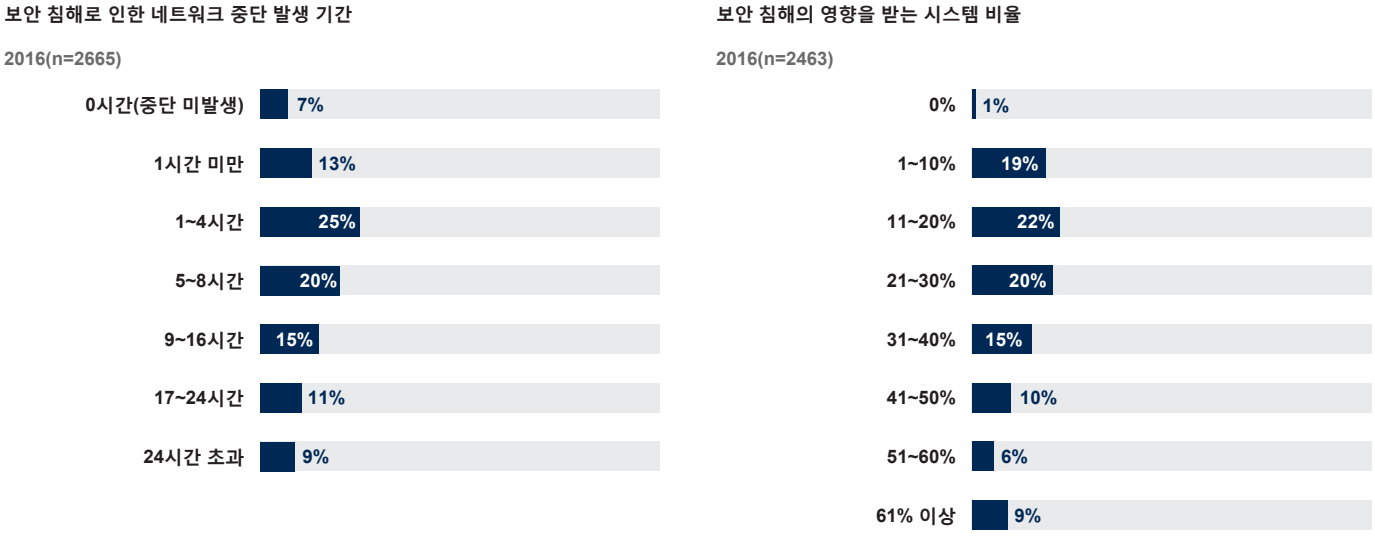
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 110 보안 침해로 인해 귀사의 보안 위협 방어 정책, 절차 또는 기술이 얼마나 많이 개선됐습니까?



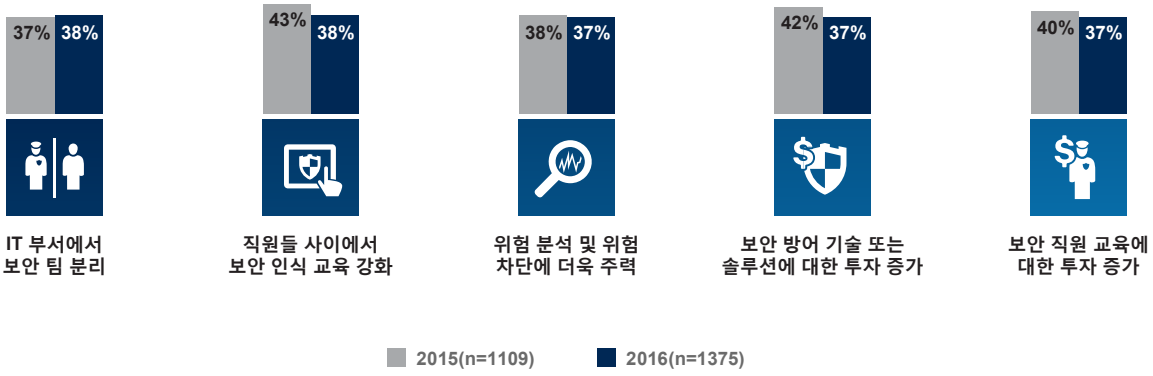
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 111 보안 침해로 인한 네트워크 중단의 발생 기간 및 범위



출처: Cisco 2017 보안 기능 벤치마크 조사

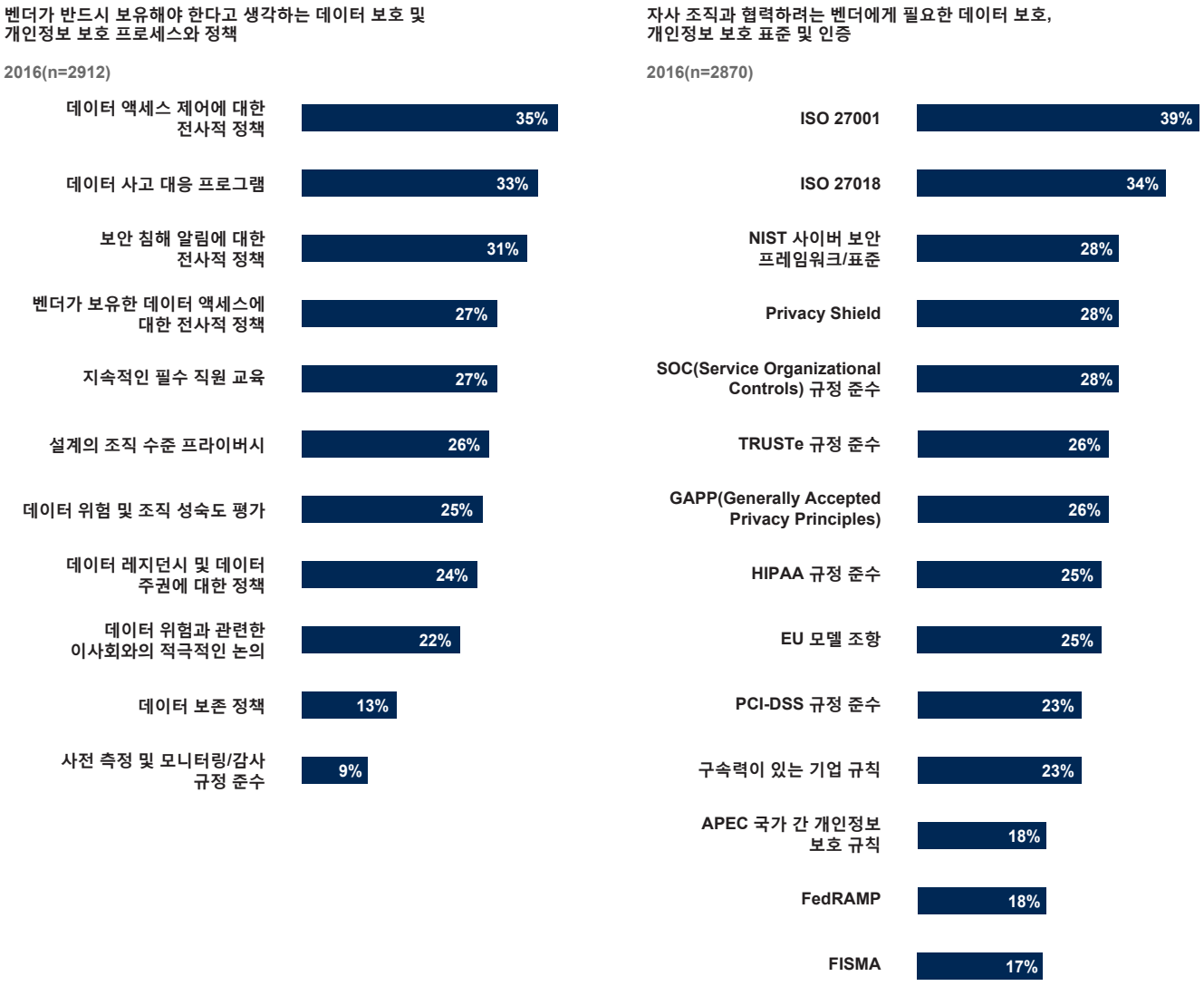
그림 112 보안 침해로부터 회사를 보호하기 위해 개선된 요소



출처: Cisco 2017 보안 기능 벤치마크 조사

벤더 선택 및 기대치

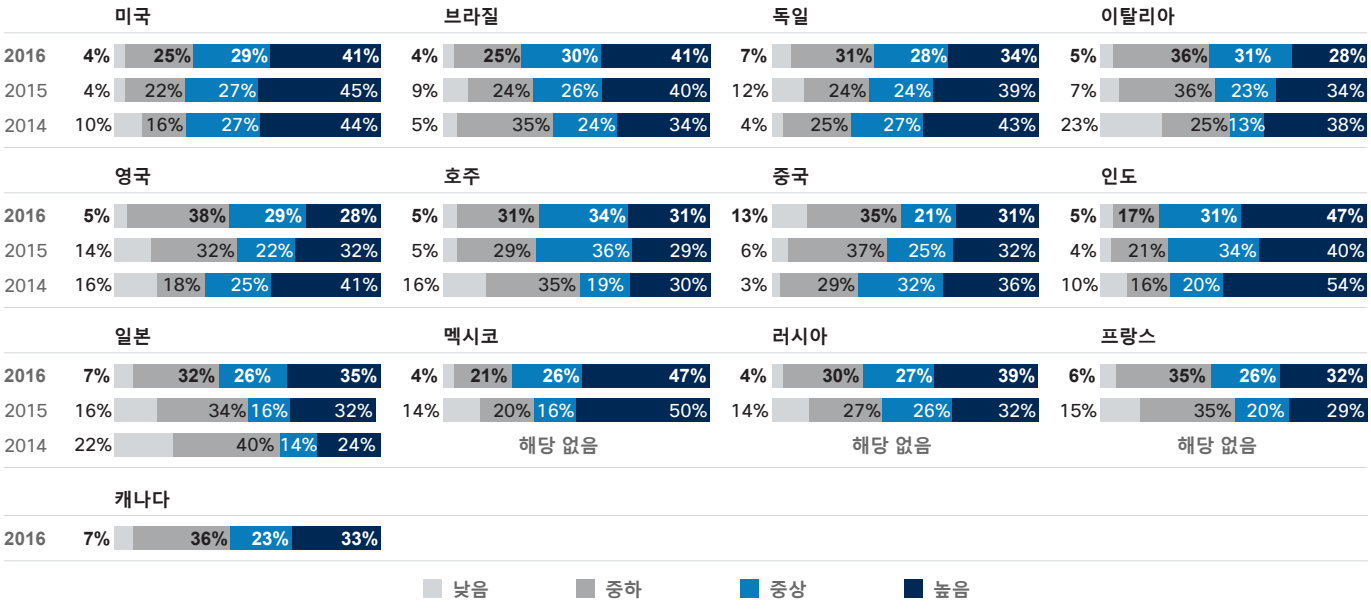
그림 113 벤더에 필요한 데이터 보호 및 개인정보 보호의 중요도



출처: Cisco 2017 보안 기능 벤치마크 조사

보안 기능 성숙도 모델

그림 114 국가별 보안 성숙도

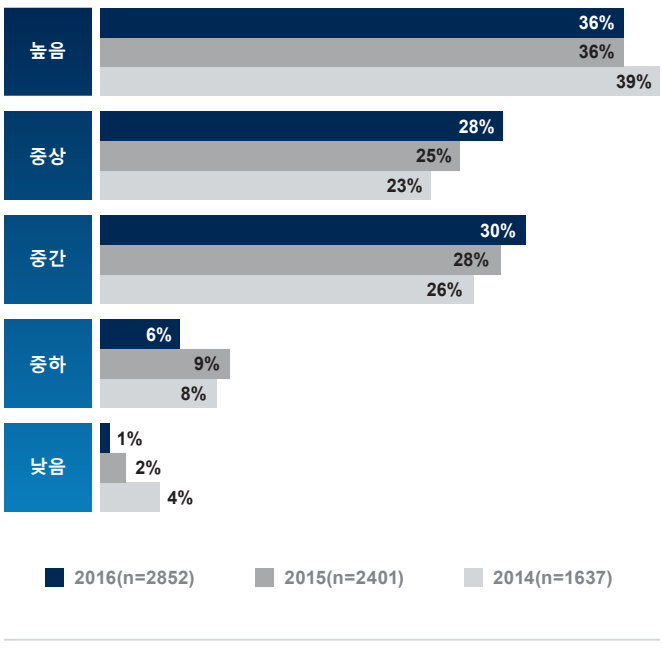


출처: Cisco 2017 보안 기능 벤치마크 조사

그림 115 보안 프로세스를 기준으로 성숙도 모델이 조직 순위 결정

출처: Cisco 2017 보안 기능 벤치마크 조사

그림 116 성숙도 모델의 세그먼트 크기

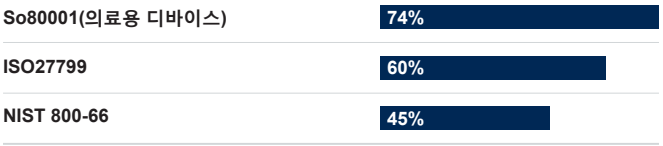


출처: Cisco 2017 보안 기능 벤치마크 조사

산업별

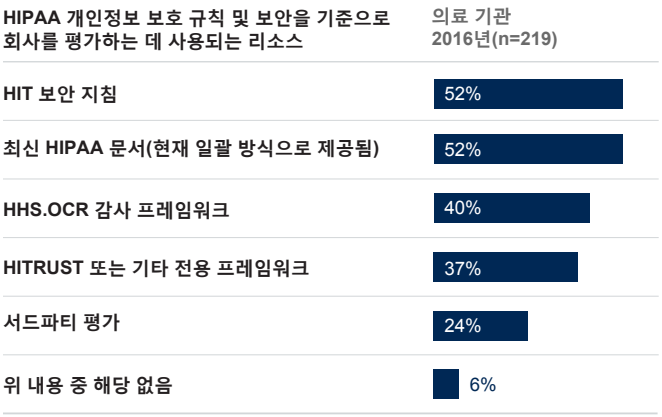
그림 117 표준화된 보안 정책을 구현한 의료 기업 비율

표준화된 보안 정책 구현
의료 기관이 준수하는 의료 관련 정보 보안 정책 관행, 2016년(n=65)



출처: Cisco 2017 보안 기능 벤치마크 조사

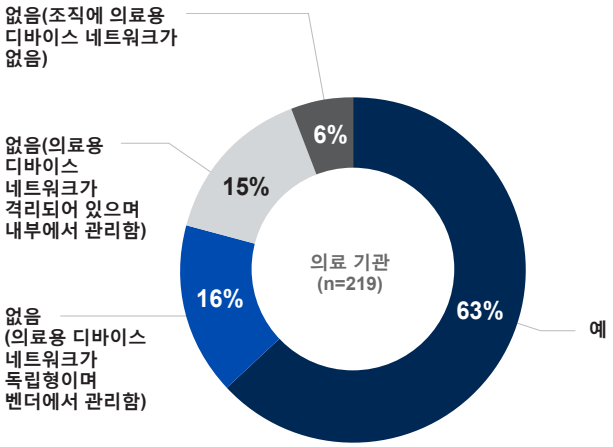
그림 118 의료 기관이 HIPAA 개인정보 보호 규칙을 기준으로 자사를 평가하는 데 사용하는 리소스



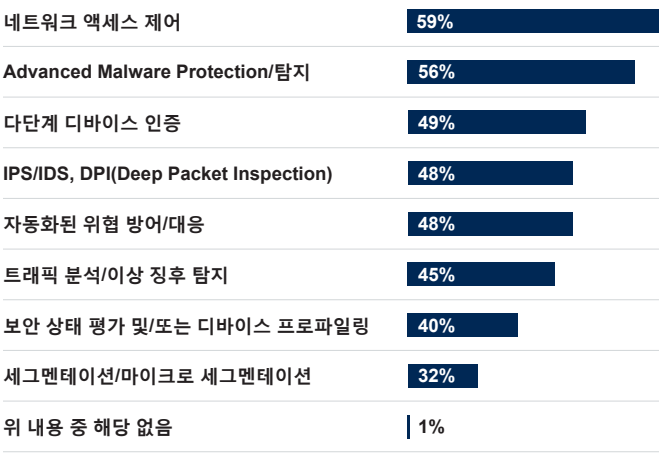
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 119 의료 디바이스 네트워크를 보유한 의료 기관에서 흔히 사용되는 보안 조치

조직 내 주요 병원 네트워크와 통합된 의료용 디바이스 네트워크의 유무



회사에서 의료용 디바이스 네트워크 보호 및 보안을 위해 구현한 보안 조치(있는 경우)
조직에 의료용 디바이스 네트워크가 있는 회사(n=207)



출처: Cisco 2017 보안 기능 벤치마크 조사

그림 120 통신용 샘플 프로파일

조직이 기본적으로 속하는 통신 하위 부문
통신 기업(n=307)

통신 장비	47%
통신 사업자(기존)	33%
케이블/위성 사업자	11%
미디어/방송	7%
인터넷 콘텐츠 사업자(Netflix, Hulu 등)	2%

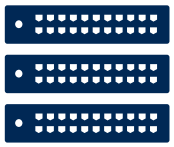
회사에서 고객에게 제공하는 서비스
통신 기업(n=308)

최종 고객에게 제공되는 관리형 보안 서비스	71%
IP(TV 포함), 모바일 등의 핵심 프로덕션 네트워크	60%
엔터프라이즈 환경	59%
데이터 센터	57%

출처: Cisco 2017 보안 기능 벤치마크 조사

그림 121 통신용 보안 전략 요소

보안 전략과 프로토콜에 대한 상대적 우선 순위
통신 기업(n=308)



사용 가능성의 평균 비율

34%

사용 가능성: 데이터에 대한 안정적 액세스 보장

신뢰성의 평균 비율

36%

신뢰성: 적절한 당사자만 데이터에 액세스할 수 있도록 보장

무결성의 평균 비율

31%

무결성: 데이터가 정확함을 보장

출처: Cisco 2017 보안 기능 벤치마크 조사

그림 122 통신용 보안 우선 순위

조직의 보안 우선 순위 랭킹

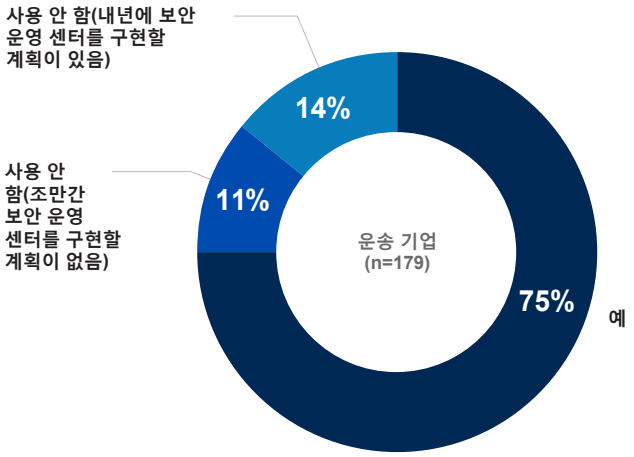
통신 기업(n=308)

	1순위	2순위	3순위	4순위
데이터 센터 보안 유지	34%	21%	24%	22%
고가용성 IP 및/또는 모바일 서비스를 제공하는 핵심 프로덕션 네트워크	26%	21%	29%	24%
관리형 보안 서비스 제공	21%	30%	19%	30%
엔터프라이즈 네트워크 및 내부 데이터	20%	28%	29%	24%

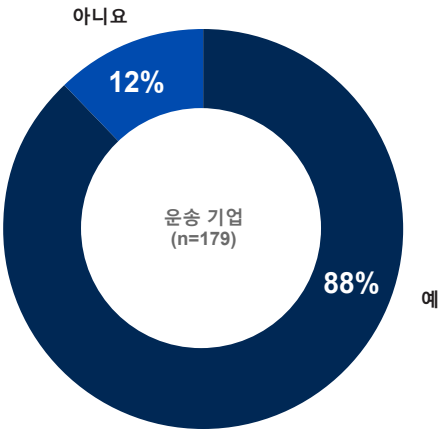
출처: Cisco 2017 보안 기능 벤치마크 조사

그림 123 운송용 샘플 프로파일

회사의 SOC(Security Operations Center, 보안 운영 센터) 사용 여부



회사의 보안 표준 단체 또는 업계 조직 참여 여부



조직이 기본적으로 속하는 운송 하위 부문
운송 기업(n=180)

운송 및 물류	54%
대중교통	11%
철도	9%
도로	9%
항공	7%
해양	5%
차량	5%

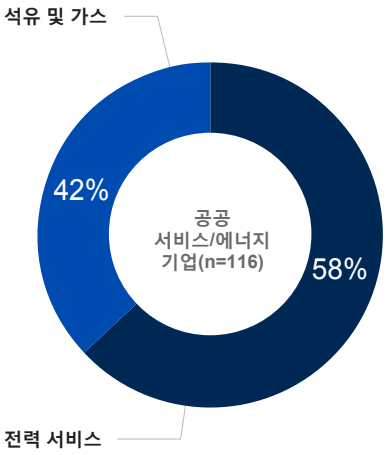
담당하는 보안 영역
운송 기업(n=180)

운영 기술 보안	84%
핵심 인프라 보안	71%
차량 보안	43%

출처: Cisco 2017 보안 기능 벤치마크 조사

그림 124 공공 서비스/에너지용 샘플 프로파일

조직이 기본적으로 속하는 공공 서비스/에너지 하위 부문



사이버 보안 사고에 대한 회사의 대응 계획을 테스트하기 위해 조직에서 훈련이나 연습을 수행하는 빈도

6개월에 한 번	55%
1년에 한 번	37%
2년에 한 번	6%
거의 아님	2%
전혀 아님	0%

공공 서비스/에너지 기업(n=116)

훈련이나 연습 수행 시의 참여 당사자

보안 파트너	84%
보안과 관련이 없는 내부 인력	69%
사업 파트너	64%
최초 대응자	33%
지역 또는 지방 정부 기관	31%
중앙 정부 기관	26%
기타 공공 서비스 사업자	20%
위 내용 중 해당 없음	1%

공공 서비스/에너지 기업(n=116)

출처: Cisco 2017 보안 기능 벤치마크 조사

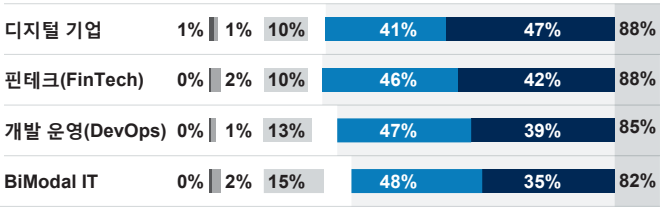
그림 125 금융 서비스용 샘플 프로파일

조직이 기본적으로 속하는 금융 서비스 하위 부문

금융 시장	52%
소매금융	25%
보험	23%

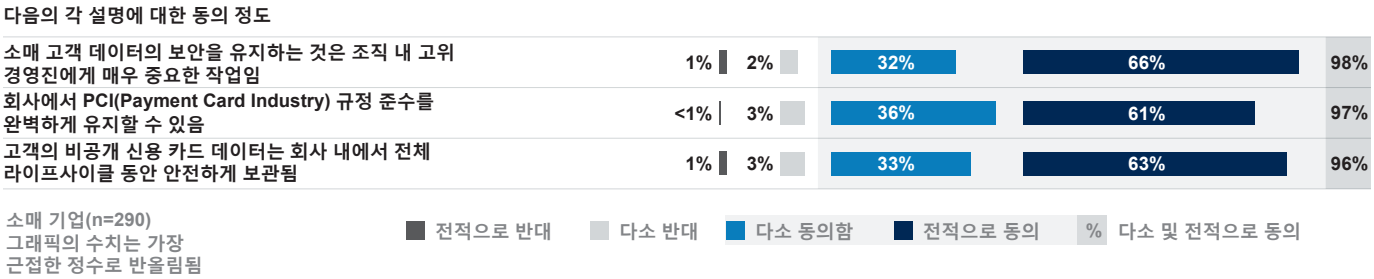
금융 서비스 기업(n=509)
그래픽의 수치는 가장 근접한 정수로 반올림됨

다음과 같은 트렌드에 보안이 영향을 받는다고 생각되는 정도



출처: Cisco 2017 보안 기능 벤치마크 조사

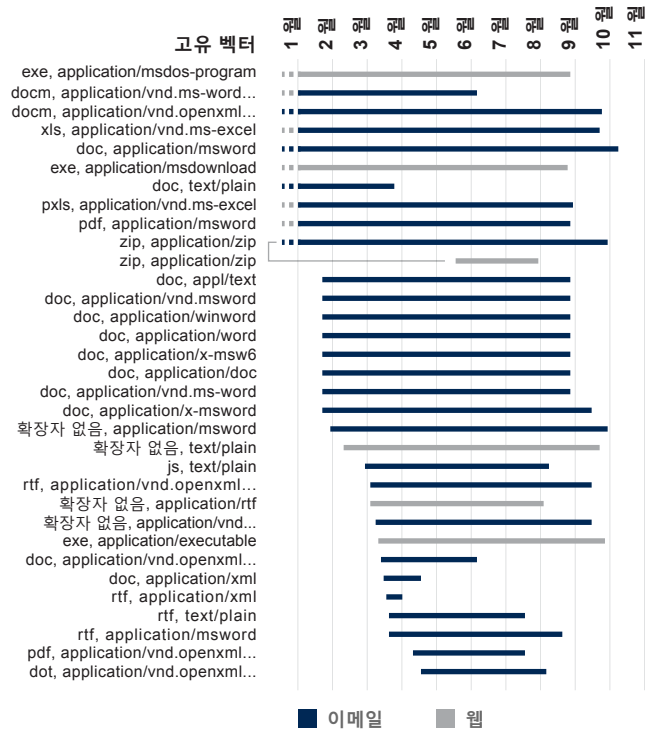
그림 126 소매용 데이터 보안



출처: Cisco 2017 보안 기능 벤치마크 조사

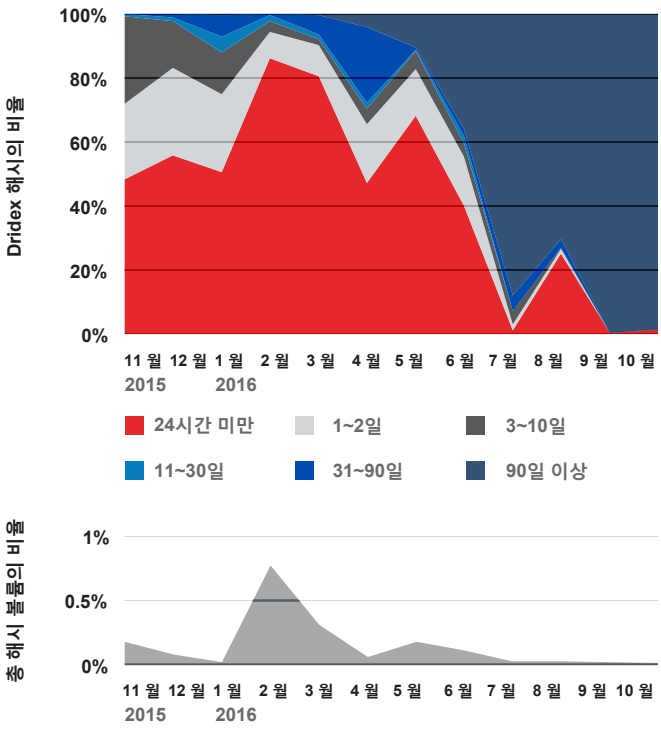
악성코드군

그림 127 Dridex의 파일 확장자 및 MIME 조합(웹 및 이메일 벡터)



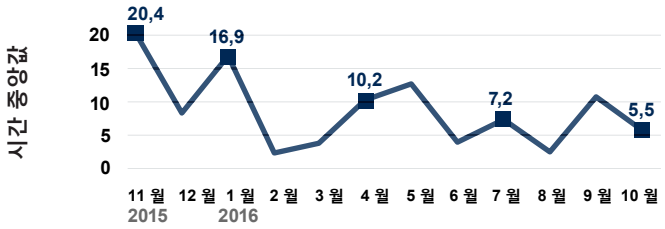
출처: Cisco Security Research

그림 128 월별로 관찰된 Dridex 악성코드군의 해시 사용 기간 및 총 해시 볼륨의 비율



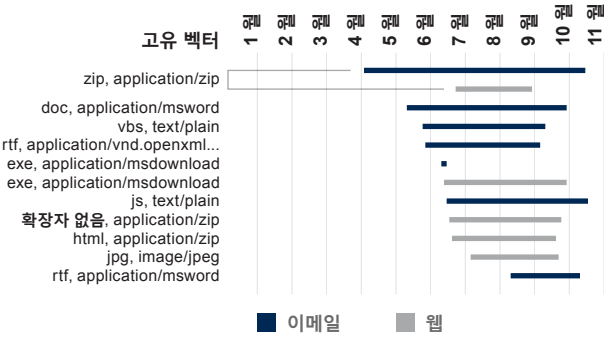
출처: Cisco Security Research

그림 129 Dridex 악성코드군의 TTD



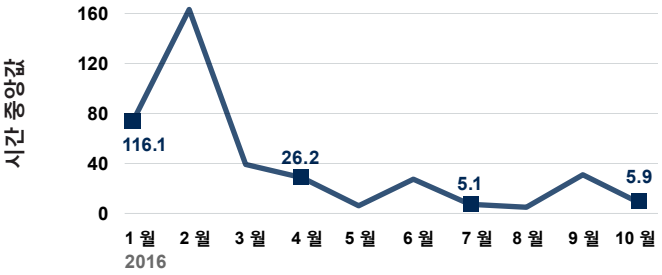
출처: Cisco Security Research

그림 130 Cerber 페이로드를 발생시키며 Cerber 페이로드를 포함하는 위협 및 지표군의 파일 확장자 및 MIME 조합(웹 및 이메일 벡터)



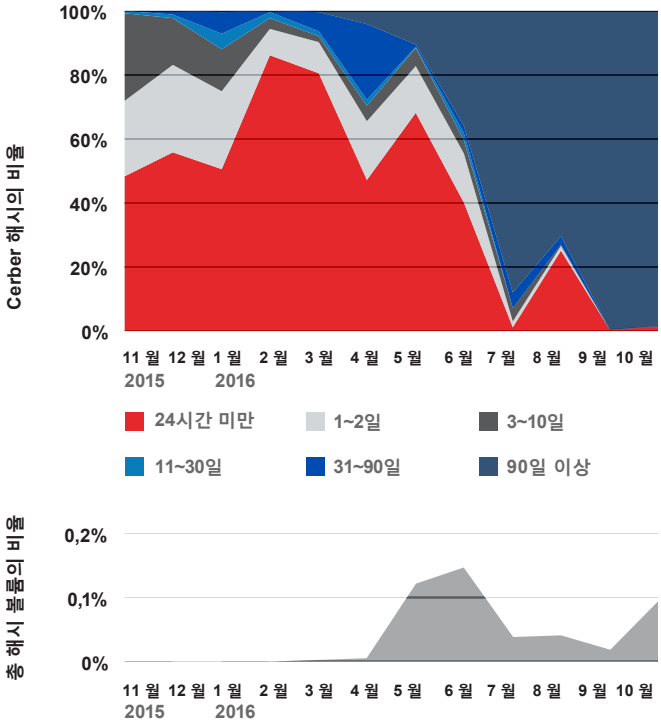
출처: Cisco Security Research

그림 131 Cerber 악성코드군의 TTD



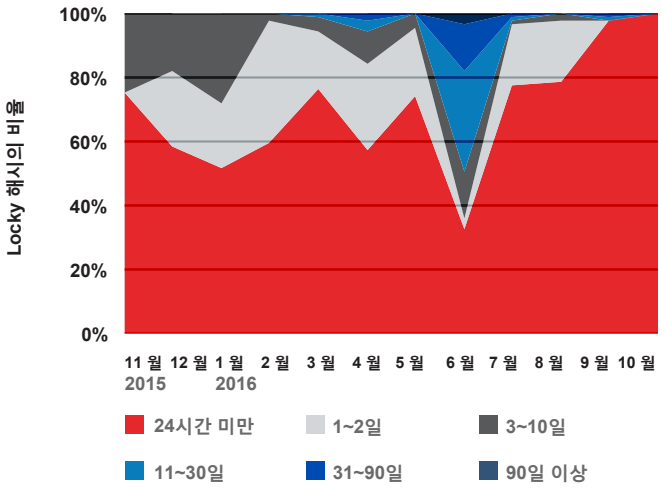
출처: Cisco Security Research

그림 132 월별로 관찰된 Cerber 악성코드군의 해시 사용 기간 및 총 해시 볼륨의 비율



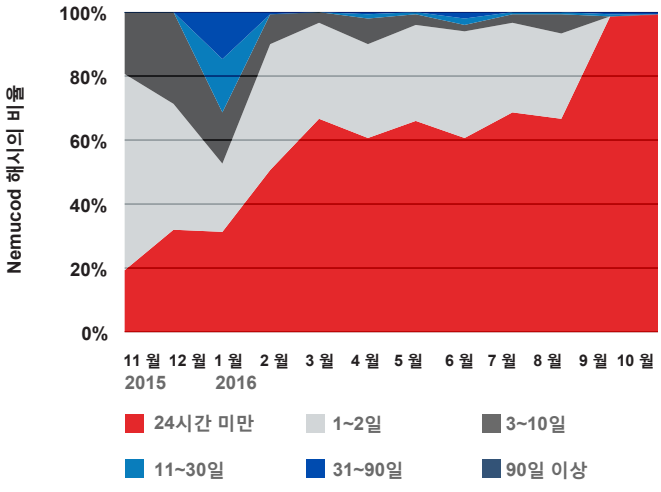
출처: Cisco Security Research

그림 133 월별 Locky 악성코드군의 해시 사용 기간



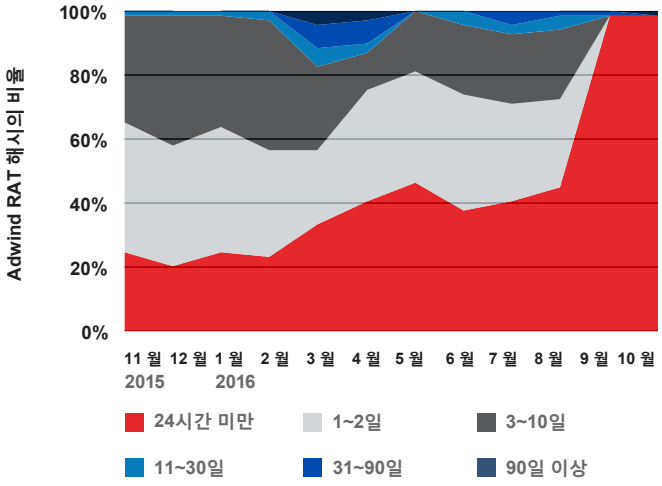
출처: Cisco Security Research

그림 134 월별 Nemucod 악성코드군의 해시 사용 기간



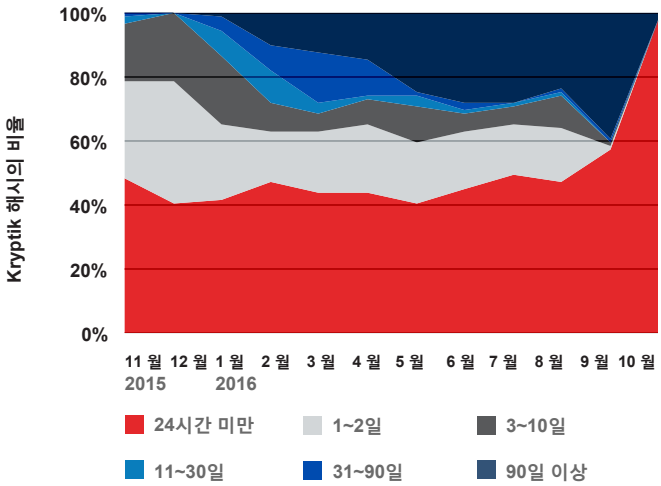
출처: Cisco Security Research

그림 135 월별 Adwind RAT 악성코드군의 해시 사용 기간



출처: Cisco Security Research

그림 136 월별 Kryptik 악성코드군의 해시 사용 기간



출처: Cisco Security Research

그래픽 다운로드

이 보고서의 모든 그래픽은 아래 페이지에서 다운로드할 수 있습니다.
www.cisco.com/go/acr2017graphics

업데이트 및 수정 사항

이 보고서에 수록된 정보의 업데이트 및 수정 사항을 보려면 다음 페이지를 방문하십시오.
www.cisco.com/go/acr2017errata

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. 주소, 전화번호 및 팩스 번호는 Cisco 웹사이트 **www.cisco.com/go/offies**에서 확인하십시오.

Published January 2017