# Cisco 2017
# 중기 사이버 보안 보고서

# 목차

# 요약

10년 동안 시스코는 사이버 위협 및 취약점을 알리고 보안 및 사이버 복구 능력을 개선하기 위해 사이버 보안 보고서를 발표하고 있습니다. 시스코는 이 보고서를 통해 점점 더 정교해지는 보안 위협과 공격자가 침해, 정보 도용, 혼란 야기를 위해 사용하는 기법들을 알리고 있습니다.

시스코는 이 보고서를 통해 보안에 대한 경각심이 한층 더 강화되어야 한다는 점을 확인하였습니다. 전세계 사이버 공격 수법의 진화 속도와 정교함이 고도화되는 사실을 우려하는 보안 팀들의 목소리가 갈수록 커지고 있습니다. 물론 현재 기업들이 위협 감지와 공격 방어를 위한 투자를 하고 있지 않거나 사용자 혹은 관련 조직들이 보다 신속한 해결 및 복구에 노력하지 않는다는 의미는 아닙니다. 그러나 다음과 같은 두 가지 추세로 인하여 보안 팀이 이루어왔던 성과를 무력화하거나, 진보를 어렵게 해 새로운 사이버 위협 시대가 올 수도 있습니다.

### 보안 사고의 여파 증가

대다수 사이버 범죄자들의 최우선 목표는 수익 창출입니다. 일부 사이버 범죄자는 공격 과정에서 시스템을 폐쇄하고 데이터를 파괴하는 공격적 성향을 드러냅니다. Cisco 2017 중기 사이버 보안 보고서 7페이지의 "서론"에서 설명했듯이, 시스코는 이처럼 더욱 악랄해진 활동이 새롭고 치명적인 공격 수법인 '서비스 파괴(DeOS, Destruction Of Service)'로 이어질 가능성에 대하여 우려하고 있습니다.

지난 한 해에는 사이버 범죄자들이 DDoS 공격에 IoT(Internet of Things) 장치를 이용한 점을 파악할 수 있었습니다. IoT 영역에서 활동하는 봇넷의 특성을 관찰해보면 일부 사이버 범죄자들은 인터넷 자체에 혼란을 가져올 수 있는 광범위하고 파괴력 있는 공격의 토대를 마련하는 데 주력하는 것으로 파악됩니다.

### 기술의 속도와 규모

시스코는 모빌리티, 클라우드 컴퓨팅, 기타 기술 발전과 트렌드로 인해 기업이 방어해야 할 보안 영역이 어떻게 넓어지고 잠식되는지 다년간 주시해왔습니다. 특히, 최근 들어 날로 넓어지는 공격 영역을 악의적 공격자가 어떻게 악용하고 있는지 훨씬 더 명확하게 볼 수 있었습니다. 최근 랜섬웨어 공격의 영역과 강도만 보더라도 노련한 사이버 범죄자는 공격 효과를 극대화하기 위해 장치와 네트워크에 존재하는 보안 공백과 취약점을 악용하고 있음을 알 수 있습니다.

급변하는 IT 환경에 대한 가시성 부족, "섀도우 IT"에 내재된 고질적인 위험, 끊임없이 나타나는 보안 경고, IT 보안 환경의 복잡성 등 여러 가지 이유로 인해 자원이 부족한 보안 팀은 날로 교묘하고 강력해지는 오늘날의 사이버 위협에 대처하는 데 어려움을 겪고 있습니다.

### 보고서의 핵심 내용

Cisco 2017 중기 사이버 보안 보고서에서는 앞서 언급한 현상들과 관련하여 다음과 같은 사항에 대하여 설명합니다.

### 공격 수법

시스코는 사이버 범죄자가 사용자를 공격하거나 시스템에 침입할 때 이용하는 전형적인 수법에 대해 연구해 왔습니다. 보안 담당자는 사이버 범죄자의 전술 변화를 파악하여 보안 프랙티스(practice)를 수정하고 사용자를 교육해야 합니다. 이 보고서에서는 새로 개발된 악성 프로그램, 웹 공격 수법과 스팸의 동향, 스파이웨어 같은 잠재적 악성 애플리케이션(PUA)의 위험, BEC(Business Email Compromise) 수법의 위험, 악의적 해킹의 경제적 환경의 변화, 의료 기기 공격 등을 주제로 다룹니다. 또한 사이버 범죄자들의 공격 툴과 수법이 어떻게, 얼마나 빠르게 진화하고 있는지 분석한 결과를 제시하고, 위협 탐지 시간(TTD)을 줄이기 위해 시스코가 진행 중인 프로젝트에 대한 최근 소식도 전합니다.

### 취약점

이 보고서에서는 기업 및 사용자를 공격의 희생양으로 삼는 위협 요인과 기타 취약점에 관해 설명합니다. 또한 파악된 취약점에 대해 미흡한 개선 속도, 소홀한 클라우드 시스템 접근 권한 통제, 인프라 및 엔드포인트의 관리 미흡과 같은 취약한 보안 프랙티스에 대해 설명합니다. 그리고 IoT 보편화와 IT 및 OT(Operational Technology)의 융합으로 인해 기업과 사용자뿐 아니라 소비자가 훨씬 더 큰 위험에 노출된 이유를 설명하고, 통제 불능 상태가 되기 전에 이러한 위험을 해소하기 위해 당장 어떠한 조치를 취해야 하는지도 집중적으로 살펴봅니다.

### 보안 팀의 기회

Cisco 2017 중기 사이버 보안 보고서는 시스코의 최근 보안 역량 벤치마크 연구에서 추가로 파악된 내용을 담고 있습니다. 특히 서비스 제공업체, 공공 부문, 소매, 제조, 공익사업, 의료, 운송, 금융 등 8개 산업 분야의 주요 보안 문제를 심층 분석합니다. 또한 시스코의 산업 전문가들은 관련 분야의 기업들이 보안 상태를 개선할 수 있도록 보안 지식과 인력의 공백을 해소하기 적합한 서비스 활용, IT 환경의 복잡성 최소화, 자동화 기술 도입 권고안을 제시합니다.

보고서의 결론 부분에는 보안 팀이 고위 경영진 및 이사회와 사이버 보안 위험 및 예산에 대해 논의하기 위해 취해야 할 조치와 이러한 대화를 시작하는 방법이 제시되어 있습니다.


## 감사의 말

Cisco 2017 중기 사이버 보안 보고서 제작에 도움을 주신 시스코 보안 전문가와 각 분야 전문가팀 및 기술 파트너들에게 감사의 말씀을 전합니다. 제공해주신 연구 내용과 의견은 앞으로도 시스코가 보안 커뮤니티, 기업 및 사용자에게 오늘날의 복잡하고 광범위한 글로벌 사이버 공격 수법에 대한 통찰력을 전달하고 보안 개선에 도움이 될만한 모범 사례와 지식을 전파하는 데 필수적 역할을 할 것입니다.

특히 시스코의 기술 파트너는 시스코가 기업 IT 환경을 보호하는 데 필요한 통합 솔루션을 단순하고 개방적이면서도 자동화되도록 개발하는 데 중요한 역할을 맡고 있습니다. **85페이지**에는 기술 파트너 이 외에 Cisco 2017 중기 사이버 보안 보고서 제작에 기여한 분들이 소개되어 있습니다.

# 주요 조사 결과

- BEC(Business email compromise)는 사이버 범죄자들에게 수익성이 매우 높은 공격 수법으로 자리잡았습니다. IC3(Internet Crime Complaint Center)에 따르면 2013년 10월부터 2016년 12월까지 BEC 사기로 인한 피해액은 53억 달러에 달한다고 합니다. 참고로, 랜섬웨어로 인한 2016년 피해액은 10억 달러에 불과했습니다.
- PUA를 빙자한 스파이웨어는 악성 프로그램의 일종이며 많은 기업이 과소 평가하거나 무시되지만 위험 요소가 다분한 프로그램입니다. 스파이웨어의 경우 사용자 및 기업의 정보를 수집할 뿐만 아니라 장치의 보안 상태를 약화시켜 악성 프로그램 감염 범위를 확대시킬 수 있습니다. 스파이웨어의 감염률 역시 걷잡을 수 없이 상승하고 있습니다. 시스코 보안 전문가들이 세 가지의 스파이웨어를 조사해본 결과, 300개 기업 중 20%가 이 유형의 스파이웨어에 감염된 것으로 확인됐습니다.
- IoT(Internet of Things)는 기업 간 협업이나 혁신과제에 큰 도움이 됩니다. 하지만 IoT가 보편화되면서 보안 위험 역시 커지고 있습니다. 그 중 한가지 문제점은 미흡한 가시성입니다. 즉, 어떤 IoT 장치가 네트워크에 연결되어 있는지 보안 팀이 제대로 파악하기 어렵다는 것입니다. 이러한 문제뿐만 아니라 IoT 보안의 장애물로 작용할 수 있는 여러 문제에 대응하려면 보안 팀이 발 빠르게 움직여야 합니다. 사이버 범죄자들은 이미 IoT 장치의 보안 취약점을 악용하고 있습니다. 사이버 범죄자는 이런 장치를 거점으로 활용해 은밀하게, 그리고 비교적 손쉽게 네트워크를 활보합니다.
- 시스코는 2015년 11월부터 TTD(Median Time to Detection)를 추적해왔습니다. 그 이후 TTD는 전반적으로 감소하였는데, 조사 시작 시점에 39시간이 넘었던 TTD는 2016년 11월과 2017년 5월 사이에 약 3.5 시간으로 감소하는 등 전반적인 하락세를 이어왔습니다.
- 시스코가 조사한 바에 의하면 2016년 중반 이후 스팸의 수량은 대게 증가했으나, 같은 기간 동안 익스플로잇 킷(Exploit Kit)의 활동은 크게 감소했습니다. 랜섬웨어 유포 시 익스플로잇 킷 의존도가 높았던 사이버 범죄자들은 현재 시스템 감염 후 페이로드를 전송하는 등 사용자의 반응을 유도하거나 샌드박스 기술 대부분을 무력화시킬 악성 매크로 파일이 첨부된 스팸 메일을 선호하고 있습니다.
- 사이버 범죄자들은 우선 한 곳의 취약한 사이트부터 점령한 후 공급망 공격을 통해 여러 기업에 악성 프로그램을 유포해나갑니다. 시스코 파트너인 RSA가 조사한 보안 사고 사례에 따르면 한 소프트웨어 제공 업체의 다운로드 웹페이지가 공격 당해 이 회사의 소프트웨어를 다운로드한 모든 기업이 악성 프로그램에 감염됐습니다.
- 시스코 파트너 Radware에 따르면 지난해 사이버 공격 빈도, 복잡성 및 규모의 급증은 해킹의 경제적 환경이 새로운 국면에 접어들었음을 의미합니다. Radware는 해킹 집단들이 유용하고 저렴한 여러 가지 해킹 자원을 빠르고 손쉽게 입수할 수 있게 됐다고 경고합니다.
- 기업 보안의 경우, 클라우드 보안이 미흡합니다. OAuth(Open Authorization)의 위험과 최고 권한이 부여된 사용자 계정의 미흡한 관리는 사이버 범죄자가 쉽게 악용할 수 있는 보안 공백을 유발합니다. 시스코 보안 전문가들에 의하면 악의적 사이버 범죄자들은 이미 클라우드로 관심을 돌렸으며 집요하게 기업의 클라우드 환경에 침입하려고 시도하고 있습니다.
- 익스플로잇 킷의 경우, 급격한 하향세를 맞으면서 정체기에 접어들었습니다. 해킹 부문의 과거 패턴을 감안하면 이런 현상은 일시적일 가능성이 높습니다. 그러나 Adobe Flash 기술로 제작된 파일의 취약점을 악용하기가 더 어려워지는 등 다른 요인들로 인해 익스플로잇 킷의 적극적인 공격이 늦어질 수도 있습니다.
- 시스코 파트너 Rapid7에 의하면 부적절하게 배포되었거나, 합법적 사용자가 편의를 위해 고의로 배포한 DevOps 서비스는 기업에 심각한 위험을 초래한다고 합니다. 사실, 이러한 사례 중 다수가 벌써 피해를 입은 것으로 관찰됐습니다.
- 해킹 단체 'Fancy Bear'에 소속된 사이버 범죄자들이 사용하는 공동 도메인을 대상으로 한 ThreatConnect의 분석 결과를 보면 사이버 범죄자들의 IP 인프라 전술을 연구해볼 필요가 있습니다. 보안 팀은 이 인프라 연구를 통하여 예방 차원에서 차단할 대량의 도메인, IP 주소, 이메일 주소를 확보할 수 있습니다.
- 시스코는 2016년 말에 Memcached 서버에서 세 가지 원격 코드 실행 취약점을 발견하여 보고한 바 있습니다. 몇 달 후 인터넷을 조사한 결과, 이전에 노출된 것으로 확인된 약 110,000대의 Memcached 서버 중 79 %가 아직 패치를 하지 않아서 이 세 가지 취약점을 여전히 안고 있는 것으로 나타났습니다.

# 서론

# 서론

공격 수법은 꾸준히 변해왔습니다. 그러나 시스코 및 기술 파트너가 최근에 관찰한 위협의 급격한 진화와 공격 규모는 우려할만한 수준입니다. 지하 경제의 주범들은 파급 효과가 크고 복구가 어려운 공격을 감행할 교두보를 주도 면밀하게 마련하고 있을지 모른다는 우려가 제기되고 있습니다.

## 새로운 공격 수법: DeOS(Destruction Of Service)

사이버 범죄자들은 악성 프로그램 유포, 랜섬웨어 공격 또는 심각한 업무 차질을 유발하는 여러 사이버 사고를 겪은 기업이 시스템과 데이터를 복원하는 데 사용하는 "안전망"을 제거하려 합니다. 사이버 범죄자의 핵심적 동기와 창의력 및 능력의 수준에 따라 DeOS 공격의 전개 양상과 결과가 달라질 수도 있습니다.

한 가지 분명한 점은 현재 각광 받고 있는 IoT(Internet of Things)와 더불어 악용하기 좋은 보안 취약점을 가지고 있는 수많은 장치 및 시스템으로 인하여 이러한 공격 수법의 파급 효과가 커질 수 있다는 사실입니다. IoT는 사이버 범죄자와 보안 팀 간의 새로운 전장으로 부각되고 있습니다.

한편, 기존 전장에서 사이버 범죄자들이 활동할 수 있는 시간과 영역은 줄었습니다. 따라서 그들은 탐지를 피하거나 공격 효과를 높이기 위해 지속적이고 신속하게 공격 수법을 쇄신해야 합니다. 랜섬웨어의 효과를 높이기 위해 Bitcoin과 Tor를 활용한 경우가 대표적입니다. 뿐만 아니라 그들은 익스플로잇 킷 같은 수익 창출용 툴의 효용성이 떨어지거나 보안팀의 대응으로 인해 희석되면 악성 이메일 및 사회 공학적 기법 같은 전략을 다시 꺼내 들기도 합니다.

## 관건: 여러 개의 보안 툴 혼용 지양

보안 팀은 승리를 자신할 때조차도 사이버 범죄자가 언제든 보안상의 허점을 찾아낼지도 모른다는 점을 염두에 두어야 합니다. 보안 팀은 사이버 범죄자의 침입 속도를 늦추고 그들의 활동 시간과 영역을 줄이는 데 필요한 대부분의 솔루션을 이미 확보하고 있습니다. 문제는 이를 어떻게 활용하느냐입니다. 기업의 보안 담당자들은 여러 보안 솔루션 제공업체의 다양한 솔루션을 사용하고 있는 것으로 확인됐습니다. 이는 빈틈없고 총체적이어야 하는 보안 관리를 복잡하게 만듭니다.

여러 보안 솔루션들을 부분적으로 사용하면 기업의 위협 관리 능력이 저하됩니다. 또한 인적/물적 자원의 한계를 갖는 보안 팀이 검토해야 할 보안 이벤트 수도 기하급수적으로 늘어납니다. 반면, 솔루션 제공업체를 일원화하고 개방적이며 단순화된 통합 보안 방식을 도입하면 보안 사고 발생률을 줄일 수 있습니다. 또한 급부상 중인 IoT 세계의 보안 문제를 해결하고 2018년 5월부터 시행될 GDPR(General Data Protection Regulation)의 데이터 보호 규정을 더욱 철저히 준비해 준수할 수 있습니다.

# 사이버 범죄자의 행동 변화

# 사이버 범죄자의 행동 변화

이번 섹션에서는 사이버 범죄자가 웹 및 이메일 기반 공격에 이용하는 공격 수법의 진화 및 혁신 동향에 대해 개괄적으로 설명합니다. 시스코와 기술 파트너는 기업 경영층과 보안 팀이 향후 몇 개월 내에 사이버 범죄자들이 회사 공격에 이용할지도 모를 공격 수법을 이해하는 데 도움 될만한 연구, 관찰 및 분석 결과를 제공하고 있습니다. 아울러 시스코는 기업과 사용자의 위험 노출 가능성을 줄일 수 있도록 보안 개선책 관련 권고안도 제시하고 있습니다.

## 익스플로잇 킷: 감소 추세, 그러나 끈질긴 생명력

2016년에 세 가지 대표적인 익스플로잇 킷인 Angler, Nuclear, Neutrino가 사이버 범죄 세계에서 돌연 종적을 감췄습니다.[1] 이후로 Angler과 Nuclear는 다시 나타나지 않았지만 Neutrino는 다시 모습을 드러냈습니다. Neutrino는 여전히 활동 중이지만 모습을 드러냈다 사라지기를 반복합니다. Neutrino 개발자들은 선별된 조직에게만 이 익스플로잇 킷을 독점적으로 빌려줍니다. 이처럼 한정적이고 제한적인 유포 전략으로 인해 쉽게 감지될 우려가 없어 Neutrino의 활동은 명맥을 이어가는 것입니다.

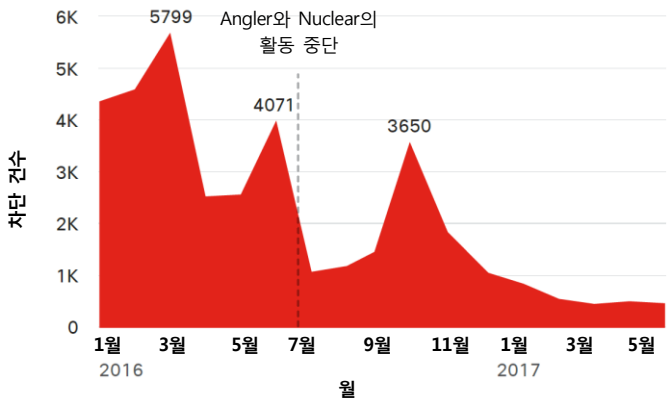
Cisco 2017 연례 사이버 보안 보고서에서 익스플로잇 킷의 이와 같은 극적인 실태 변화가 새로운 공격자에게 어떤 기회로 작용되는지 설명한 바 있습니다. 그러나 2017년 중반까지 이 기회를 살린 공격자는 찾아볼 수 없습니다. 활동중인 소수의 익스플로잇 킷 중 RIG가 지하 경제에서 가장 두드러진 활약으로 한동안 선두를 유지해오고 있습니다. 이 익스플로잇 킷은 Adobe Flash, Microsoft Silverlight, 그리고 Microsoft Internet Explorer 기술의 취약점을 공격하는 것으로 알려져 있습니다.

그림 1에 보이는 것처럼 전반적인 익스플로잇 킷의 활동은 2016년 1월 이후 크게 감소했습니다.

이러한 경향은 널리 유포된 익스플로잇 킷 'Blackhole'의 개발자와 배포자가 러시아에서 체포된 이후에 이러한 감소 추세가 고스란히 드러나고 있습니다.[2]

그 뒤에 Blackhole의 활동 중단은 익스플로잇 킷 시장에 막대한 영향을 미쳤고, 꽤 오랜 시간이 걸린 후에야 새로운 강자가 등장했습니다. 새로운 각축전의 승자는 익스플로잇 킷과 DBD(Drive-By Download) 공격 수법의 정교함을 새로운 수준으로 끌어올렸다고 평가 받은 Angler였습니다.[3]

**그림 1.** 익스플로잇 킷 활동




출처: Cisco Security Research

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

1 시스코 2017 중기 사이버 보안 보고서: cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html.
2 "Meet Paunch: The Accused Author of the Blackhole Exploit Kit", Brian Krebs, KrebsonSecurity 블로그, 2013년 12월 6일: krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/.
3 "Connecting the Dots Reveals Crimeware Shake-Up", Nick Biasini, Talos 블로그, 2016년 7월 7일: blog.talosintelligence.com/2016/07/lurk-crimeware-connections.html.

Angler는 다양한 취약점을 공격했습니다. Angler 개발자들은 혁신적이었고 익스플로잇 킷 세계에 몸담은 그 어떤 개발자들보다 더 신속하게 새로운 취약점을 찾아 본인들의 익스플로잇 킷에 반영했습니다. 그들은 다방면으로 사이버 범죄자들의 기대치를 높였고 다른 개발자들은 경쟁력을 유지하기 위해 데이터와 기술을 도용했습니다. 그러나 지금은 Angler의 시대가 막을 내리면서 익스플로잇 킷의 혁신도 침체기를 맞았습니다.

Angler의 소멸은 이런 침체기의 가장 유력한 원인 중 하나일 뿐입니다. Flash 기술을 악용하기 어려워졌다는 점도 간과할 수 없습니다. Flash 소프트웨어의 취약점은 수년 동안 익스플로잇 킷 시장의 성장과, 유지를 도왔습니다. 그러나 이러한 취약점을 인식한 보안 팀의 신속한 패치로 인해 Flash 소프트웨어를 악용하기가 더 어려워졌습니다. 이제 사이버 범죄자는 여러 취약점을 동시에 공격해야만 시스템을 공격할 수 있다는 점을 인식하고 있습니다.

최신 운영체제와 웹 브라우저의 자동 보안 업데이트도 사용자가 익스플로잇 킷을 막는 데 도움이 되고 있습니다. 익스플로잇 킷 시장의 변화에 따른 대안으로 사이버 범죄자들이 신속하고 경제적 이점을 가지는 랜섬웨어와 기타 악성 프로그램을 유포할 수단으로 다시 이메일을 활용한다는 점도 눈여겨볼 만합니다. 탐지 시스템을 피하는 방법도 창의적으로 진화하고 있습니다.

예를 들어, 시스코가 조사한 바에 의하면 사용자의 반응을 요구하여 시스템을 감염시키고 페이로드를 전송함으로써 다수의 샌드박스 기술을 무력화시킬 수 있는 악성 매크로 파일(예: Word 문서, Excel 파일 및 PDF)을 첨부한 스팸 메일이 증가하는 추세입니다.[4]

### 진화는 은밀히 진행 중?

크라임웨어가 수십억 달러 규모의 산업이라는 점을 감안하면 익스플로잇 킷 시장이 부활하는 건 시간 문제입니다. 악용하기 쉽고 다수의 사용자에게 영향을 미칠 수 있는 새로운 공격 수단이 등장하면 익스플로잇 킷은 곧바로 인기를 회복하고 개발 경쟁과 혁신이 거세질 것입니다.

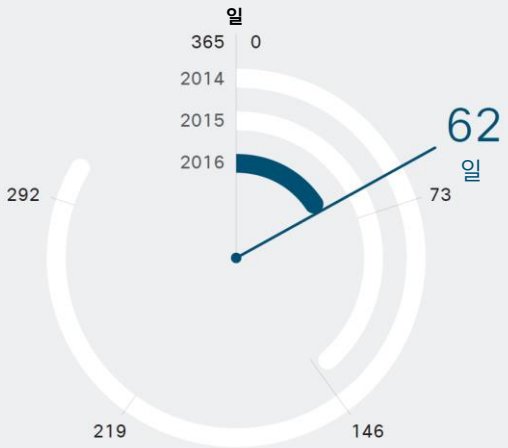
따라서 보안 팀은 절대 경계를 늦추지 말아야 합니다. 많은 익스플로잇 킷이 여전히 활동 중이며 사용자를 공격하거나 시스템을 악성 프로그램에 감염시키는 데 효과적입니다. 따라서 언제, 어디서든 이런 위협이 닥칠 수 있습니다. 하나의 시스템 안에서 악용하기 좋은 취약점 하나만 찾아내도 판도가 바뀝니다. 취약점, 특히 웹 브라우저 및 관련 플러그인의 취약점 패치를 게을리하지 않고 다중 방어 체제를 구현한 기업은 이런 위험을 최소화할 수 있습니다. 보안이 유지되는 브라우저를 사용하고 불필요한 웹 플러그인을 비활성화하거나 제거하도록 사용자를 철저히 교육시키면 익스플로잇 킷의 위협에 노출될 가능성이 크게 낮아집니다.

4 "Threat Spotlight: Mighty Morphin Malware Purveyors: Locky Returns via Necurs," Nick Biasini, Talos 블로그, 2017년 4월 21일: blogs.cisco.com/security/talos/locky-returns-necurs.

## 사이버 공격을 줄일 수 있는 방어 습관

보안 팀이 Flash 소프트웨어의 취약점을 적시에 패치하면 익스플로잇 킷 시장의 성장과 발전을 지연시키는 데 도움을 줄 수 있습니다. 시스코의 이전 사이버 보안 보고서에서 언급했듯이, Flash 소프트웨어는 시스템을 악용하고 공격하려는 사이버 범죄자들에게 오랫동안 매력적인 웹 공격 수단이었습니다. 그러나 보다 적극적인 패치 문화가 자리잡으면서 이를 악용하기가 점차 어려워지고 있습니다.

**그림 2.** Flash 소프트웨어의 취약점 중 80%를 패치하는 데 걸리는 일수




출처: Qualys

네트워크 보안 및 취약점 관리 회사이자 시스코 파트너인 Qualys의 조사 결과에 따르면 보안 팀이 Flash 소프트웨어의 알려진 취약점 중 80%를 패치하는 데 걸리는 평균 시간이 2014년 308일에서 2015년 144일과, 2016년 62일로 현저히 감소했습니다(그림 2 참조). 이 조사 결과는 Qualys가 글로벌 입지를 바탕으로 매년 실시하는 30억 건 이상의 취약점 검사를 통해 얻은 데이터를 근거로 합니다.

보안 팀이 Flash 소프트웨어의 새로운 취약점을 패치하는 시기가 빨라지면 일부 공격 툴 개발자는 오래 전에 발견됐지만 등한시된 취약점을 악용하는 데 집중할지도 모릅니다. 따라서 보안 팀은 Flash 소프트웨어의 알려진 취약점이 모두 해결되었는지 점검하고 기업을 위험에 빠뜨릴 수 있는 주요 취약점을 최우선적으로 패치하는 데 시간을 할애해야 합니다.

또한, Flash 소프트웨어를 표적 삼아 익스플로잇 킷을 동원해 랜섬웨어와 기타 악성 프로그램을 유포하던 일부 사이버 범죄자는 꾸준한 목표액 달성을 위해 한시적으로나마 다른 수법을 사용할 가능성도 있습니다.

이를 증명하듯 시스코의 조사 결과에 의하면 겉보기에 정상이지만 악성 매크로 파일이 첨부된 스팸 메일이 증가했습니다(**23페이지**의 "악성 프로그램의 진화: 6개월간의 관찰 결과" 참조). 공교롭게도 이러한 추세에 맞물려 익스플로잇 킷의 활동이 최근 들어 감소했습니다(이 주제에 대한 자세한 내용은 **9페이지**의 "익스플로잇 킷: 감소 추세, 그러나 끈질긴 생명력" 참조).

## 웹 공격 수법의 변화 - 인터넷 성숙기에 대한 방증

프록시는 인터넷 사용 초창기부터 존재해왔는데, 프록시의 기능성 또한 인터넷 발전 속도에 맞춰 진화했습니다. 사이버 범죄자는 사용자 컴퓨터의 접속 권한을 획득하고, 기업에 침입하며, 공격을 감행할 수 있는 인터넷 인프라나 네트워크의 약점을 노리는데, 이런 잠재적 위협을 감지할 목적으로 보안 팀은 콘텐츠 검사 시 프록시를 사용하고 있습니다.

잠재적 위협의 예로는 다음과 같은 것들이 있습니다.

- 악성 브라우저 확장 프로그램 같은 잠재적 악성 애플리케이션(PUA)
- 트로이 목마(드로퍼 및 다운로더)
- 웹 스팸 및 광고 사기 링크
- JavaScript 및 그래픽 렌더링 엔진 같은 브라우저 관련 취약점
- 악성 웹 콘텐츠로 사용자를 유도하는 데 사용되는 브라우저 리디렉션, 클릭재킹 및 기타 수법

그림 3에는 2016년 11월부터 2017년 5월까지 사이버 범죄자들이 가장 보편적으로 사용한 악성 프로그램의 유형이 나열되어 있습니다. 시스코는 당사의 관리형 웹 보안 로그를 참조하여 해당 목록을 작성했습니다. 그림 3의 목록에는 많은 사용자 집단을 공격하고 컴퓨터와 시스템을 감염시키는 악의적인 여러 가지 공격 수법이 열거되어 있습니다. 대표적인 공격 수법은 다음과 같습니다.

- 사용자 컴퓨터의 초기 감염을 용이하게 하는 트로이 목마 및 유틸리티 같은 "1단계 페이로드" (악성 Word 문서에 포함된 매크로 바이러스가 이런 유형에 해당됩니다.)
- 악성 브라우저 확장 프로그램이 포함된 PUA
- 애드웨어 및 스파이웨어 같은 위협 요소를 전파하는 Windows 바이너리[5]
- 가짜 할인 행사, 미디어 콘텐츠 및 설문조사 사기 같은 페이스북 사기
- 감염된 호스트에 페이로드를 전송하는 랜섬웨어 및 키 입력 도용 에이전트 같은 악성 프로그램

**그림 3.** 2016년 11월과 2017년 5월 사이에 가장 많이 발견된 악성 프로그램(차단율 기준)

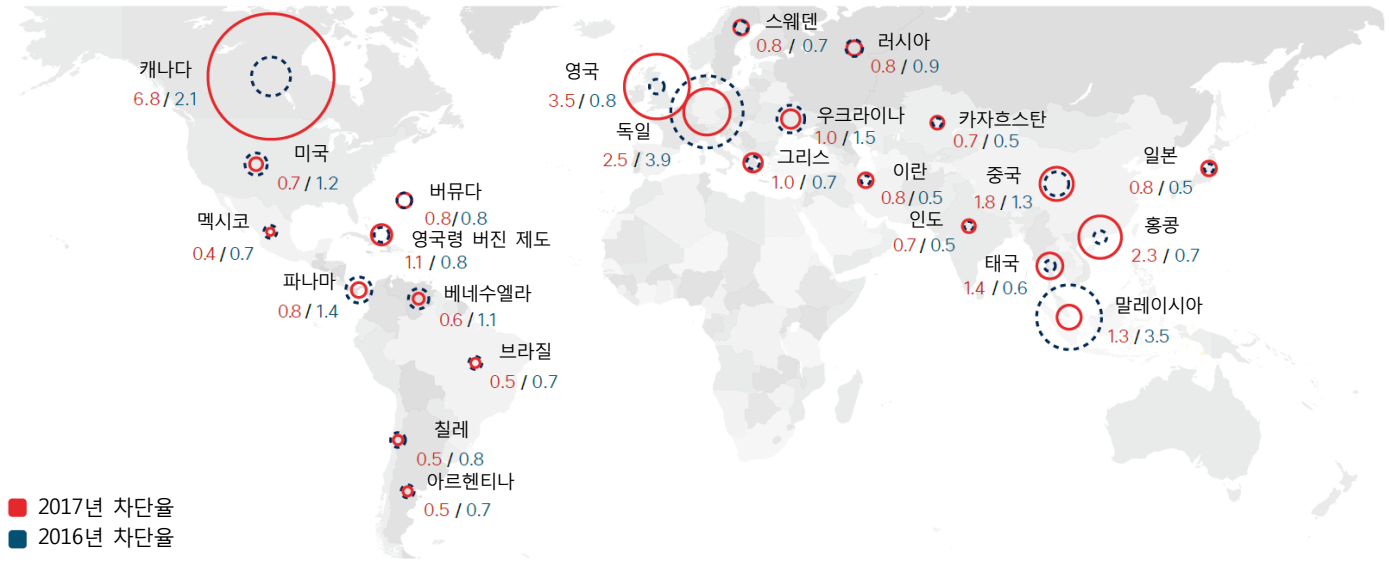

출처: Cisco Security Research

5 참고: Cisco 2017 연례 사이버 보안 보고서(b2me.cisco.com/en-us-annual-cybersecurity-report-2017?keycode1=001464153에서 다운로드 가능), 시스코는 해당 보고서에서 광고 삽입 애드웨어, 브라우저 설정 하이재커, 유틸리티 및 다운로더 같은 악성 애드웨어가 증가하고 있다고 경고했습니다. 보고서 14페이지에는 스파이웨어 같은 PUA가 사용자와 기업에 초래하는 위험이 소개되어 있습니다.

위의 모든 공격 수법은 가장 많이 발견되고 악성 프로그램 목록에도 자주 오르는 수법입니다. 악성 프로그램 목록에 큰 변동이 없다는 것은 인터넷이 성숙기에 접어들면서 사이버 범죄자들이 사용자 공격 시 가장 효과적인 웹 공격 수법을 어느 정도 고착화 시켰다고 해석할 수 있습니다.

한편, 보안이 유지되는 브라우저를 사용하고 불필요한 웹 플러그인을 비활성화하거나 제거하는 방법이야말로 일반적인 웹 기반 공격에 노출될 가능성을 줄이는 데 가장 효과적입니다.

**그림 4.** 2016년 11월~2017년 5월 전세계 웹 차단율




출처: Cisco Security Research

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

## 전세계의 웹 차단 현황

시스코는 국가 또는 지역별 악성 프로그램 차단 현황을 추적하고 있습니다. 사이버 범죄자는 근거지를 자주 변경하며 공격을 감행할만한 취약 인프라를 찾아 다닙니다. 시스코는 전반적인 인터넷 트래픽 규모 및 차단 활동을 조사하여 악성 프로그램의 출처에 대한 분석 정보를 제공합니다.

시스코는 인터넷 트래픽 규모를 토대로 조사 대상 국가를 선택합니다. 1.0이란 수치의 "차단율"은 조사된 차단 횟수가 네트워크 크기에 비례한다는 의미입니다. 차단율이 정상 수치보다 높게 나타난 국가와 지역에는 취약점을 패치하지 않은 다수의 웹 서버 및 호스트가 네트워크에 존재할 가능성이 높습니다. 위의 도표는 전세계 웹 차단 현황을 보여주고 있습니다.

## 여전히 악명 높은 스파이웨어

PUA로 알려진 오늘날의 온라인 광고 소프트웨어 중 다수는 스파이웨어입니다. 스파이웨어 제공업체는 자신들의 소프트웨어가 유용한 서비스를 제공하고 사용자의 사용권 계약을 준수하는 합법적인 툴이라고 주장합니다. 그러나 그들이 아무리 미화하려 애써도 스파이웨어는 악성 프로그램일 뿐입니다.

PUA로 가장한 스파이웨어는 사용자의 컴퓨터 활동 정보를 은밀하게 수집하여 전송하는 소프트웨어입니다. 스파이웨어는 일반적으로 사용자 모르게 컴퓨터에 설치됩니다. 이해를 돕기 위해 이 보고서에서는 스파이웨어를 크게 3개의 범주(애드웨어, 시스템 모니터, 트로이 목마)로 분류했습니다.

기업 환경에서 스파이웨어는 다음과 같은 여러 가지 잠재적 보안 위험을 초래합니다.

- 개인 식별 정보(PII)와 기타 민감한 정보나 기밀 정보와 같은 사용자 및 기업 정보를 몰래 빼냅니다.
- 장치 구성 및 설정을 변경하고, 소프트웨어를 추가로 설치하며, 타인의 접속을 허용하는 방법으로 장치의 보안 상태를 약화시킵니다. 또한 스파이웨어는 공격자가 장치를 완벽하게 제어할 수 있도록 임의의 코드를 실행하기도 합니다.
- 악성 프로그램 감염 위험이 증가합니다. 사용자가 스파이웨어나 애드웨어 같은 PUA에 감염되면 훨씬 더 많은 악성 프로그램에 감염될 가능성이 높아집니다.

스파이웨어 감염 실태를 보다 정확하게 파악하기 위해 시스코는 2016년 11월부터 2017년 3월까지 약 300개 기업의 네트워크 트래픽을 조사하여 어떤 유형의 스파이웨어에 얼마나 감염됐는지 확인했습니다.

그 결과, 모집단 중 20% 이상의 기업이 세 가지 스파이웨어(Hola, RelevantKnowledge, DNSChanger/DNS Unlocker)에 모두 감염된 것으로 조사됐습니다. 그리고 월별 기준으로 모집단 중 25% 이상의 기업은 Hola, RelevantKnowledge 또는 DNSChanger/DNS Unlocker에 감염된 것으로 확인됐습니다(그림 5 참조).

스파이웨어의 종류는 수백 개에 달합니다. 그러나 시스코가 이 세 가지 스파이웨어만 조사한 것은 신종 스파이웨어가 아닌데도 조사 대상 기업의 환경에서 가장 일반적으로 발견된 "브랜드"였기 때문입니다. 다음 페이지에서는 이 세 가지 "브랜드"에 대해 좀 더 구체적으로 살펴보겠습니다.

**그림 5.** 2016년 11월부터 2017년 3월까지 특정 유형의 스파이웨어에 감염된 기업의 비율

월별 기준으로 조사 대상 기업 중 25%가 Hola, RelevantKnowledge 또는 DNSChanger/DNS Unlocker에 감염됐습니다.

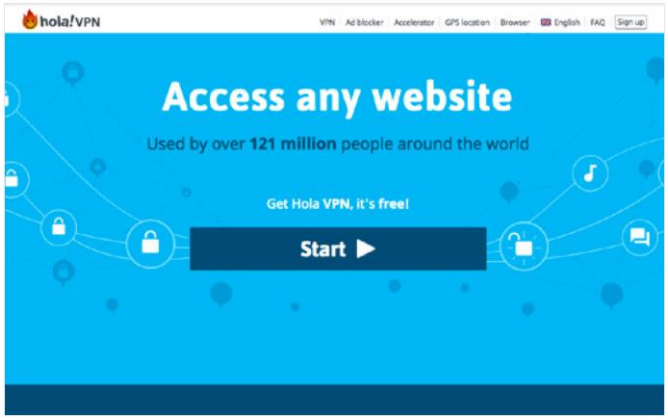
출처: Cisco Security Research

### Hola VPN

Hola(스파이웨어 겸 애드웨어)는 P2P 네트워크를 통해 사용자에게 일종의 VPN을 제공하는 부분 유료(Freemium) 웹이자 모바일 애플리케이션입니다. 또한 Hola는 P2P 캐싱 기술을 이용해 사용자가 다운로드한 콘텐츠를 다른 사용자가 "저장"하게 만듭니다. Hola는 클라이언트 측 브라우저 기반의 애플리케이션으로 배포됩니다. 또한, 브라우저 확장 프로그램이나 독립형 애플리케이션으로 사용할 수 있습니다.

그림 6의 Hola 웹사이트 스크린샷을 보면 스파이웨어 제공업체들은 Hola가 사용자가 "모든 웹사이트에 접속"할 수 있는 유용한 무료 서비스라고 주장합니다. 또한 그들은 "전세계 1억 2천 백만 명 이상이 Hola를 사용"하고 있다고 주장합니다.

**그림 6.** Hola VPN 홈페이지 스크린샷




**스파이웨어로 간주하는 이유:** Hola는 Luminati라는 서비스를 통해 사용자의 대역폭 판매, 사용자 시스템에 자체 코드 서명 인증서 설치, 바이러스 백신 검사를 우회할 수 있는 옵션으로 모든 파일 다운로드, 원격으로 코드 실행 등의 기능을 갖추고 있습니다.

### RelevantKnowledge

RelevantKnowledge(스파이웨어 겸 시스템 모니터)는 인터넷 검색 활동, 인구 통계, 시스템 및 구성에 대한 다량의 정보를 수집합니다. RelevantKnowledge는 경우에 따라 사용자 동의를 받지 않은 채 직접 또는 소프트웨어 번들을 통해 설치됩니다.

**그림 7.** RelevantKnowledge 홈페이지 스크린샷


Hola와 마찬가지로, RelevantKnowledge 홈페이지(그림 7)에는 사용자가 기분 좋게 서비스에 가입하도록 유도하는 홍보 문구가 있습니다. 예를 들어, 스파이웨어 제공업체는 모든 회원을 대표해서 "Trees for Knowledge"에 나무를 기증한다고 주장합니다.

**스파이웨어로 간주하는 이유**: 앞에서 언급했듯 RelevantKnowledge는 사용자의 동의 없이 소프트웨어를 설치할 수 있습니다. 또한 RelevantKnowledge는 "조사"를 목적으로 하는 타사에 데이터를 판매하기 위해 사용자 프로파일을 작성하고 정보를 수집합니다.

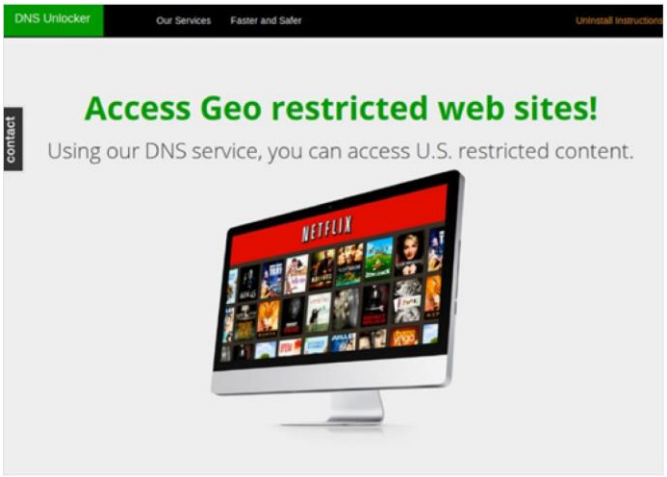
### DNS Changer/DNS Unlocker

DNS Changer와 DNS Unlocker는 동일한 악성 소프트웨어를 두 가지 다른 버전으로 나는 것입니다. DNS Changer는 감염된 호스트의 DNS 설정을 변경하거나 "하이재킹"하는 트로이 목마입니다.[6] DNS Unlocker는 프로그램 제거 옵션을 제공하는 애드웨어 서비스입니다.

DNS Unlocker는 네임 서버를 자체 네임 서버로 대체하여 호스트의 HTTP와 기타 요청을 사이버 범죄자가 제어하는 일련의 서버로 전송합니다. 따라서 사이버 범죄자가 호스트 트래픽을 가로채고, 조사하며, 수정할 수 있습니다. 이 스파이웨어는 브라우저 대신 엔드포인트를 감염시킵니다. DNS Unlocker는 감염된 호스트에서 PowerShell(Microsoft Windows용 개체 지향 프로그래밍 언어 겸 대화형 명령줄 셸)을 사용하여 명령을 실행할 수 있습니다. 덕분에 사이버 범죄자가 원격으로 액세스할 수 있는 교두보가 마련되는 셈입니다.

DNS Unlocker 제공업체는 사용자가 지리적으로 제한되는 콘텐츠(예: 스트리밍 비디오)에 액세스할 수 있게 해주는 서비스라고 이 스파이웨어를 소개합니다.

**그림 8.** DNS Unlocker 홈페이지 스크린샷

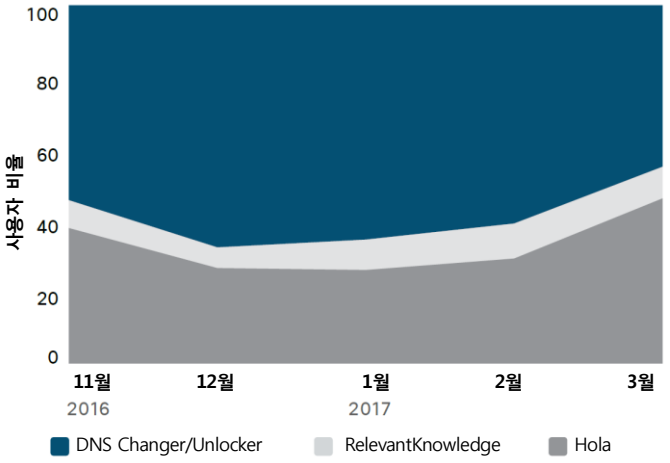



**스파이웨어로 간주하는 이유:** 앞서 거론한 기능과 기타 용도 외에도, DNS Unlocker는 온라인 광고 같은 특정 서비스에 콘텐츠를 삽입하는 수법으로 즉시 PII를 도용하고, 사용자 트래픽을 리디렉션하거나 사용자 콘텐츠를 수정할 수 있습니다.

### 가장 만연한 스파이웨어 - DNS Unlocker

이 보고서에서 집중적으로 다루고 있는 세 가지 스파이웨어 중에서 DNS Unlocker가 가장 널리 퍼져있는 것으로 조사됐습니다. 구체적으로 말하자면, 기업을 대상으로 실시한 월간 감염률 조사에서 40%의 기업이 이 스파이웨어에 감염된 것으로 확인됐습니다.

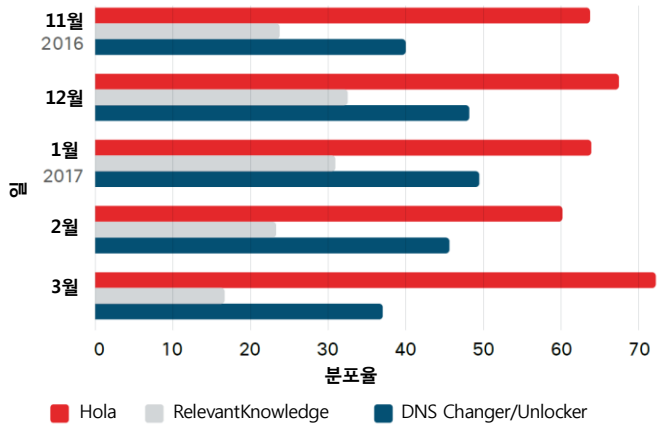
**그림 9.** 각 유형의 스파이웨어에 감염된 사용자 비교




출처: Cisco Security Research

6 "DNSChanger Outbreak Linked to Adware Install Base," Veronica Valeros, Ross Gibb, Eric Hulse, Martin Rehak 공저, Cisco Security 블로그, 2016년 2월 10일: blogs.cisco.com/security/dnschanger-outbreak-linked-to-adware-install-base.

그림 10. 스파이웨어 분포




출처: Cisco Security Research

기업을 대상으로 실시한 분포율 조사에서 세 가지 스파이웨어 중 Hola가 가장 높은 분포율(매달 60% 이상)을 기록했습니다. 이 스파이웨어는 시간이 지날수록 완만해지긴 했으나 꾸준한 증가세를 보였습니다.

한편, DNS Unlocker의 경우, *가장 많은 사용자를 감염시켰음에도 불구하고 기업 단위로 추산하면 Hola보다 적었던 것으로 조사됐습니다*(그림 10 참조). 시스코의 조사 결과에 의하면 1월에 이 스파이웨어에 감염된 기업 수는 11월에 비해 크게 증가했지만 이후 하향세로 돌아섰습니다.

## 더욱 심각성을 인지해야만 하는 스파이웨어 감염

기업 스파이웨어 감염 건수가 급증하고 있지만, 기업들은 이를 중대한 보안 위험으로 여기지 않습니다. 그러나 최근 시스코가 실시한 다른 조사[7]에서 조사 대상 기업 중 3/4이 감염된 것으로 확인된 애드웨어와 마찬가지로, 스파이웨어에 감염된 사용자와 기업은 피해를 입을 수 있습니다.

스파이웨어 제공업체들은 오히려 사용자를 보호하거나 사용자에게 도움을 주는 서비스라고 스파이웨어를 알리지만, 이런 악성 프로그램의 진짜 목적은 (경우에 따라 사용자의 동의를 받거나 사용자에게 알리지도 않은 채) 사용자와 소속 기업에 대한 정보를 추적하고 수집하는 것입니다. 스파이웨어 제공업체는 자사가 수집한 데이터 열람 권한을 유료로 판매하거나 제공하는데, 이를 구매한 자는 익명으로 정보를 수집할 수 있습니다. 그리고 이 정보는 중요 자산을 파악하고, 기업의 인프라 배치 구조를 분석하며, 표적 공격 계획에 악용될 수 있습니다.

브라우저와 엔드포인트가 스파이웨어에 감염되면 신속하게 치료해야 합니다. 보안 팀은 최신 스파이웨어 정보를 꾸준히 입수하고 어떤 유형의 정보가 위험한지 파악해야 합니다. 또한 보안 팀은 스파이웨어, 애드웨어, 리스크웨어[8]에 감염된 경우 이를 치료하고 PUA의 위험을 사용자에게 숙지시킬 수 있도록 적절한 지침서를 가지고 있어야 합니다. 사용자 역시 PUA의 최종 사용자 사용 약관에 동의하기 전에 본인의 정보를 수집, 저장 및 공유하는 방법이 명시된 항목만이라도 꼼꼼히 읽어봐야 합니다.

PUA를 빙자한 스파이웨어를 단순한 악성 프로그램의 일종으로 여겨 경계하지 않으면 감염 및 보안 위험이 더 커질 수밖에 없습니다. 스파이웨어 제공업체가 소프트웨어에 더 많은 악성 기능을 추가하고 기업의 소극적인 대처를 계속 기회로 삼는다면 스파이웨어 문제는 날로 심각해질 것으로 예상됩니다.

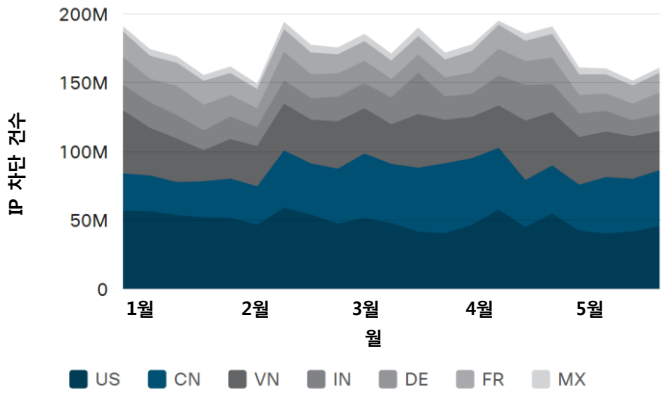
7 이 주제를 다룬 시스코의 이전 보고서를 참조하려면 cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html에서 시스코 2017 연례 사이버 보안 보고서를 다운로드하십시오.

8 리스크웨어는 사이버 범죄자가 수정하여 비도덕적 목적으로 사용할 수 있는 합법적 소프트웨어입니다.

## 익스플로잇 킷 활동 감소에 의한 전세계 스팸 동향

시스코 조사에 따르면, 중국 IP 주소 에서 유입된 IP 차단 건수가 2017년 1월부터 5월 동안 증가한 것으로 확인됐습니다. 2016년 말에 이르러 정점을 찍었던 전체 스팸량이 올해 상반기에 감소한 데 이어 꾸준한 하락세를 보이고 있습니다.

**그림 11.** 국가별 IP 차단 건수




출처: Cisco Security Research

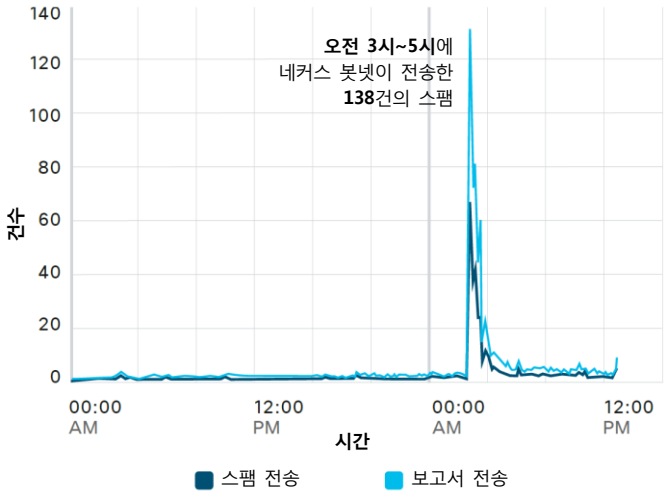
시스코 조사가 나타내듯이, 2016년 8월 이후 전체 스팸량은 증가했지만, 같은 시기 익스플로잇 킷의 활동이 크게 감소한 것으로 확인됐습니다[9]. 사이버 범죄자들은 이메일과 같은 검증된 방법으로 랜섬웨어와 악성 프로그램을 유포하여 수익을 창출하고 있습니다(**9페이지**의 "익스플로잇 킷: 감소 추세, 그러나 끈질긴 생명력" 참조).

시스코는 악성 파일이 첨부된 스팸량이 계속 증가하는 데 반해, 익스플로잇 킷의 활동 규모는 앞으로도 유동적일 것으로 전망합니다. 이메일은 엔드포인트로 곧장 이동할 수 있다는 장점이 있습니다. 또한 사이버 범죄자는 악성 이메일 수신자의 "도움"을 받아 다른 사용자에게도 전파할 수 있습니다. 더불어, 사이버 범죄자는 교묘한 사회 공학적 수법(예: 피싱 스피어 피싱)으로 사용자를 쉽게 속이고 기업에까지 침입할 수 있습니다.

또한 일부 사이버 범죄자는 악성 매크로 파일이 첨부된 스팸 메일을 활용하여 랜섬웨어를 유포하고 있습니다. 이런 유형의 공격 수법은 시스템을 감염시키고 페이로드를 전송하는 데 사용자의 긍정적 반응(예: 대화상자에 있는 "확인" 클릭)이 수반되기 때문에 다수의 샌드박스 기술을 무력화시킬 수 있습니다(**23페이지**의 "악성 프로그램의 진화: 6개월간의 관찰 결과" 참조).

스팸 발송 봇넷, 특히 대규모 봇넷인 네커스(Necurs)도 기승을 부리면서 전세계의 전반적인 스팸량 증가에 일조하고 있습니다. 올해 초, 네커스는 투기성 저가주(penny stock) "주가 조작" 사기 스팸 대량 유포에 성공하자 랜섬웨어 같은 정교한 공격 수법이 포함된 스팸량이 다소 감소했습니다.[10] 그림 12는 시스코의 스팸캅(SpamCop) 서비스 사업부가 작성한 그래프로 네커스의 이 같은 활동 유형 사례를 보여주고 있습니다. 봇넷 소유자가 이와 같은 저급 스팸 작전에 크게 의존하는 이유는 비교적 큰 노력을 들이지 않고서도 성공적으로 수익을 창출할 수 있기 때문인 것으로 추측됩니다.

**그림 12.** 네커스의 "주가 조작" 사기 스팸 활동(24시간 이상)




출처: 스팸캅

좀 더 최근에 네커스 봇넷은 다수의 대규모 악성 스팸 메일 캠페인을 통해 랜섬웨어의 새로운 변종인 재프(Jaff)를 유포했습니다. 이메일에는 재프 랜섬웨어의 임시 다운로드 기능이 부여된 Microsoft Word 문서와 PDF 파일이 첨부되어 있습니다.[11]

9 이 주제를 다룬 시스코의 이전 보고서를 참조하려면 cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html에서 시스코 2017 연례 사이버 보안 보고서를 다운로드하십시오.

10 "Necurs Diversifies Its Portfolio," by Sean Baird, Edmund Brumaghin, Earl Carter 공저, Jaeson Schultz 도움, Talos 블로그, 2017년 3월 20일: blog.talosintelligence.com/2017/03/necurs-diversifies.html.

11 "Jaff Ransomware: Player 2 Has Entered the Game," Nick Biasini, Edmund Brumaghin, Warren Mercer 공저, Colin Grady 도움, Talos 블로그, 2017년 5월 12일: blog.talosintelligence.com/2017/05/jaff-ransomware.html.

## 악성 이메일: 악성 프로그램 개발자가 선호하는 파일 형식의 고찰

주로 이메일을 통해 랜섬웨어와 기타 악성 프로그램을 유포하는 사이버 범죄자가 늘고 있기 때문에 시스코는 악성 프로그램에 가장 많이 사용되는 파일 형식을 추적하고 있습니다. 이 정보는 위협 탐지 시간(TTD)을 줄이고 악성 프로그램 제공업체가 공격 수법을 강화하는 다양한 방법(예: 파일 확장자 변경)을 추적하는 데 유용합니다. (TTD에 대한 자세한 내용은 **26페이지** 참조, **28페이지**의 "진화 동향: 네머코드(Nemucod), Ramnit, Kryptik, 페어릿(Fareit)" 참조).

**그림 13.** 가장 많이 감지된 악성 프로그램

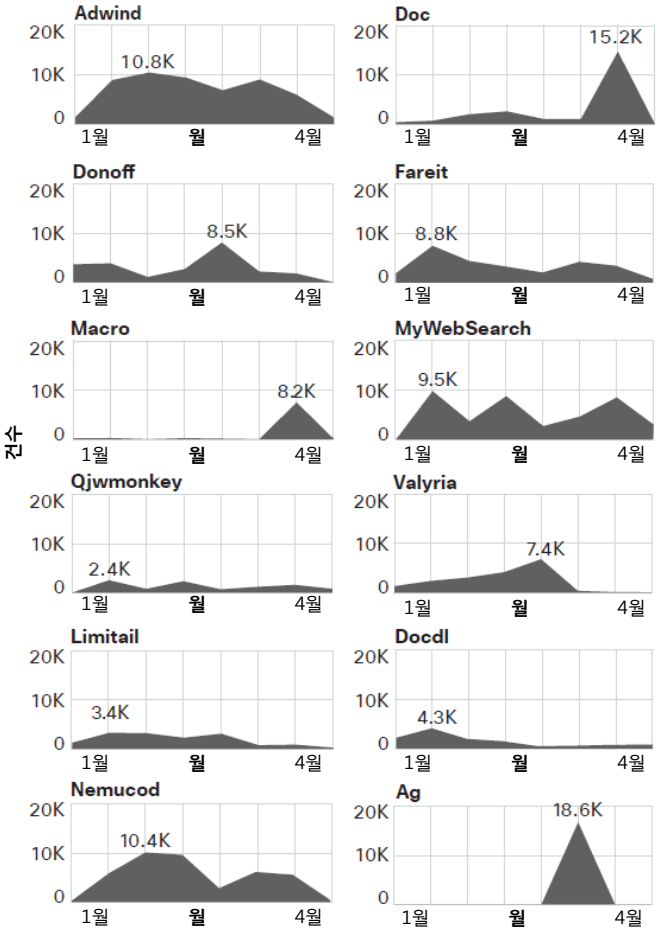

출처: Cisco Security Research

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

시스코는 2017년 1월부터 4월까지 악성 프로그램 감지 횟수를 분석하여 해당 기간 동안 악성 이메일 페이로드에서 가장 많이 감지된 상위 20가지 변종 악성 프로그램을 파악했습니다(그림 13 참조).

그림 14는 '.zip' 또는 '.exe'와 같은 악성 페이로드 파일 확장자가 포함된 프로그램의 감지 횟수를 유형별로 보여주고 있습니다. 미국과 캐나다를 비롯한 여러 국가의 일반적인 납세 기간인 4월에 매크로 관련 악성 프로그램이 급격히 증가했다는 사실에 주목할 필요가 있습니다(매크로 악성 파일이 첨부된 스팸에 대한 자세한 내용은 **23페이지**의 "악성 프로그램의 진화: 6개월간의 관찰 결과" 참조).

**그림 14.** 2017년 상위 악성 프로그램의 패턴

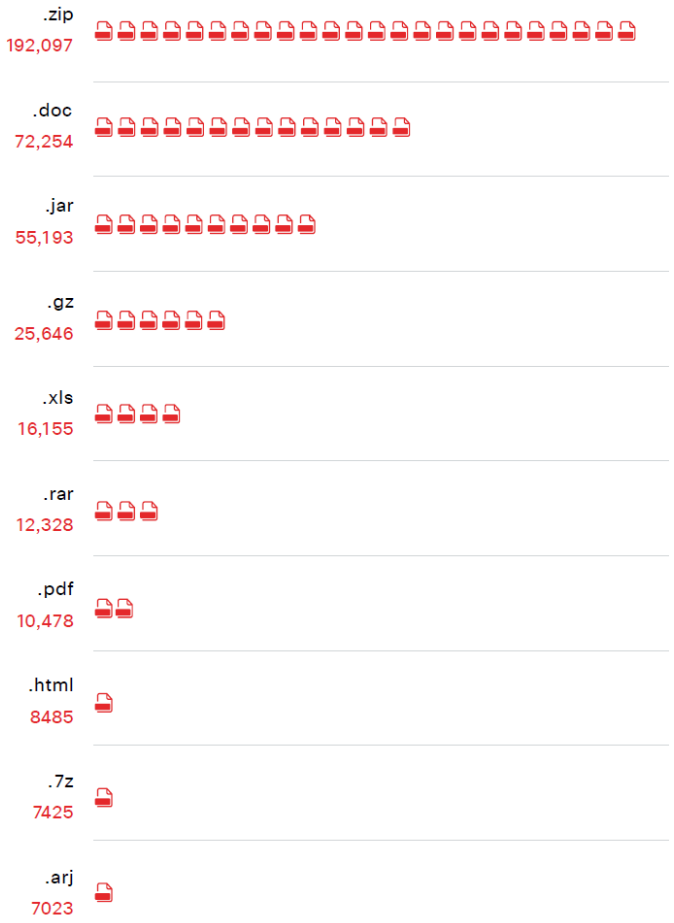



출처: Cisco Security Research

또한 시스코는 이메일에 가장 흔히 사용된 악성 파일 확장자 목록을 작성하기 위해 페이로드 첨부 파일 사용 횟수를 조사했습니다(그림 15 참조). 그 결과, 악성 zip 파일에 이어 Microsoft Word의 '.doc' 확장자가 가장 많이 사용된 것으로 확인됐습니다.

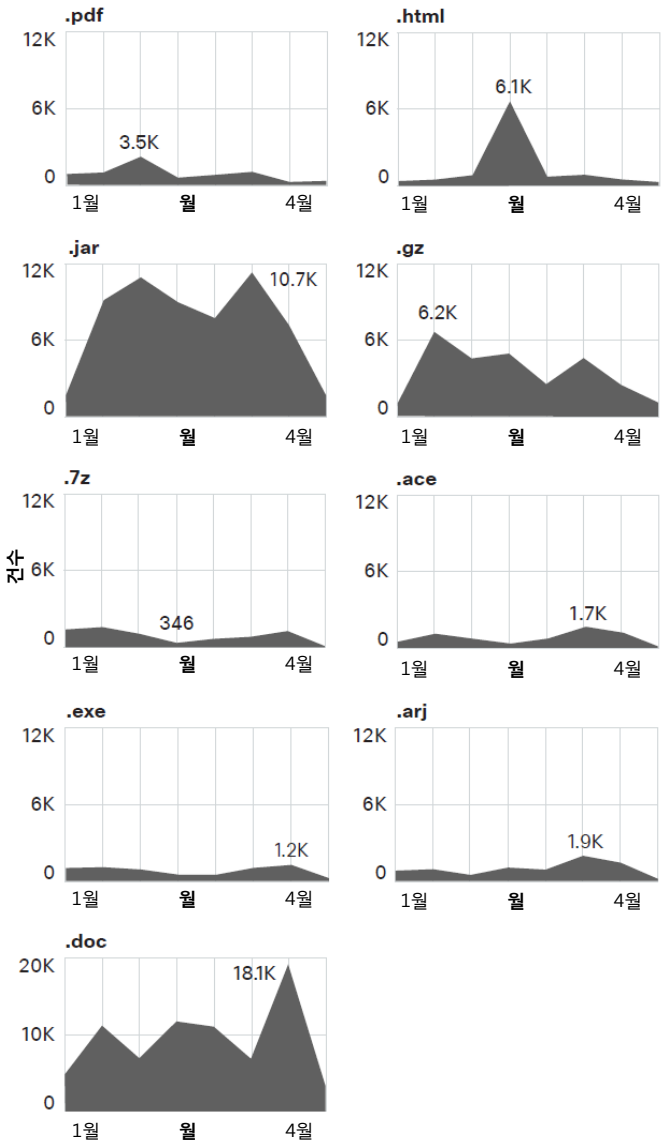
이에 따라 시스코는 확장자 선호도가 시간의 추이에 따라 어떻게 달라졌는지 조사했습니다(그림 16 참조).

**그림 15.** 횟수 기준으로 가장 많이 감지된 악성 파일 확장자




출처: Cisco Security Research

**그림 16.** 2017년 상위 악성 파일 확장자 패턴




출처: Cisco Security Research

### 상위 악성 프로그램에 "자주 사용된" 파일 형식

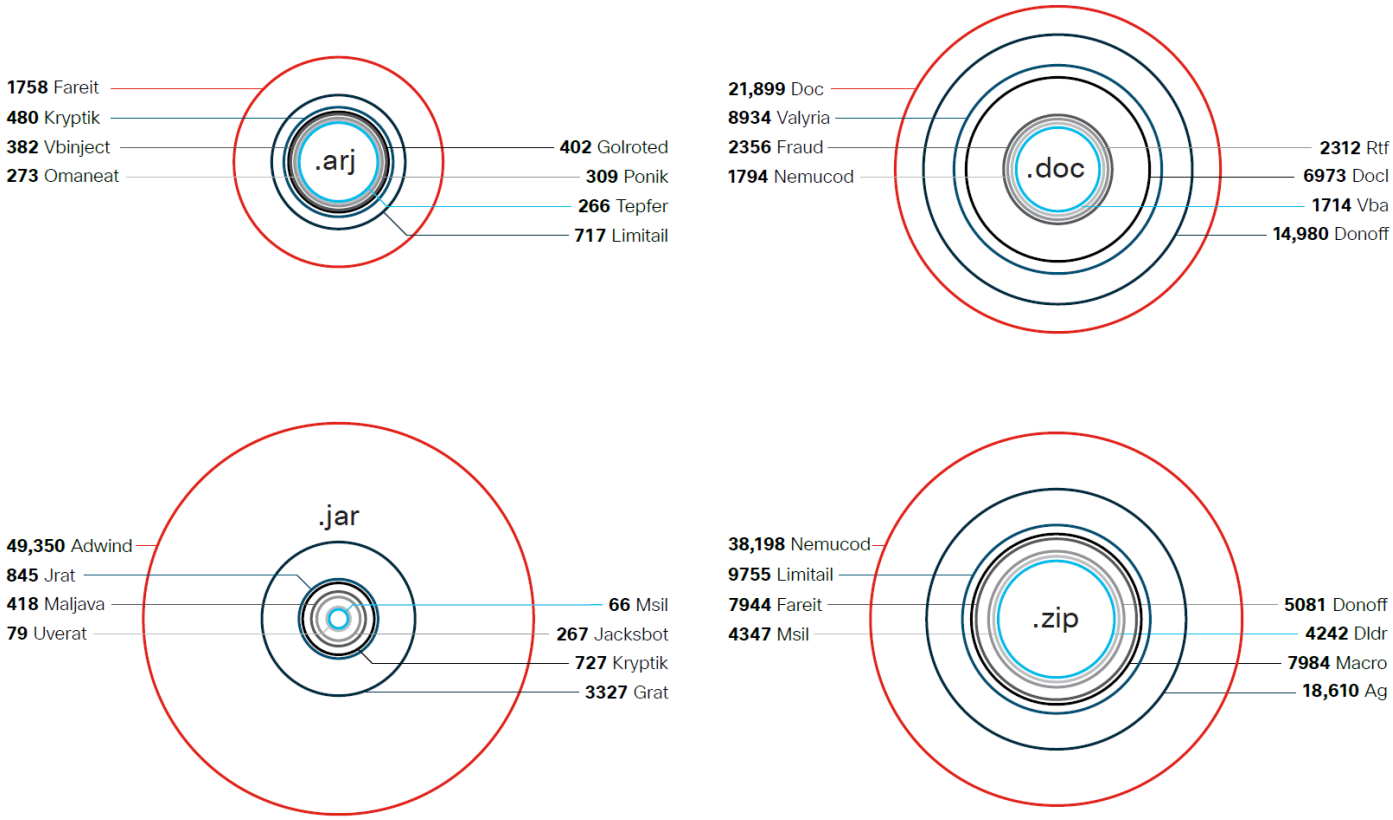
상위 5가지 악성 프로그램을 살펴본 결과, 각 악성 프로그램는 다양한 파일 형식이 사용됐는데, 이 중 일부 확장자는 주기적으로 사용된 것으로 확인했습니다. 예를 들면 다음과 같습니다.

- RAT(Remote Access Trojan)의 일종인 애드윈드(Adwind)에는 '.jar' 파일(Java 아카이브 확장자)이 자주 사용됐습니다.
- 랜섬웨어를 유포하는 트로이 목마 다운로더인 네머코드에는 '.zip'이 파일 확장자로 사용됐습니다.
- 악성 애드웨어인 마이웹서치(MyWebSearch)는 매우 선별적입니다. 마이웹서치 에는 '.exe' 파일 확장자만 사용됐는데 한 달 내내 한가지 파일 형식만 사용되는 경우가 많았습니다.
- 또 다른 RAT인 페어릿에는 다양한 파일 형식이 사용됐지만 주로 '.zip' 및 '.gz' 파일 확장자가 사용됐습니다. ('.gz'는 아카이브 파일 확장자입니다.)
- 악성 매크로를 유포하는 랜섬웨어의 일종인 Donoff 에는 주로 Microsoft Office 문서 파일 형식, 특히 '.doc' 파일 형식이 사용됐습니다.

그림 17은 사용된 파일 확장자와 다양한 악성 프로그램의 관계라는 특이한 관점에서 악성 이메일 패턴을 보여주고 있습니다. 사이버 범죄자들은 '.zip' 및 '.doc' 등 비즈니스 환경에서 널리 사용되는 파일 형식을 네머코드 및 페어릿을 비롯한 여러 상위 변종 악성 프로그램에서 활용하고 있었습니다.

그러나 '.jar' 및 '.arj' 같은 더 오래된 파일 확장자 형식을 사용하는 변종 악성 프로그램도 다수 발견됐습니다. ('.arj'는 압축 파일 형식입니다.)

**그림 17.** 파일 확장자(.arj, .doc, .jar, .zip)와 악성 프로그램의 관계




출처: Cisco Security Research

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

## 랜섬웨어보다 더욱 심각할 수 있는 BEC(Business Email Compromise)

랜섬웨어가 최근 보안 분야에서 가장 주목되고 있지만, 훨씬 더 높은 수준의 위협을 조용히 안겨줄 공격 수법이 있습니다. 다름아닌 BEC(Business Email Compromise) 공격 수법입니다. 시스코 파트너이자 보안 정보 제공업체인 플래시포인트(Flashpoint)는 BEC가 기업으로부터 거액을 탈취하기에 가장 매력적이고 수익성 높은 방법이라는 결론을 내리고 BEC 문제를 연구했습니다. BEC는 사회 공학적 수법을 동원하여 굉장히 손쉽게 금전적 이득을 꾀할 수 있는 공격수법입니다.

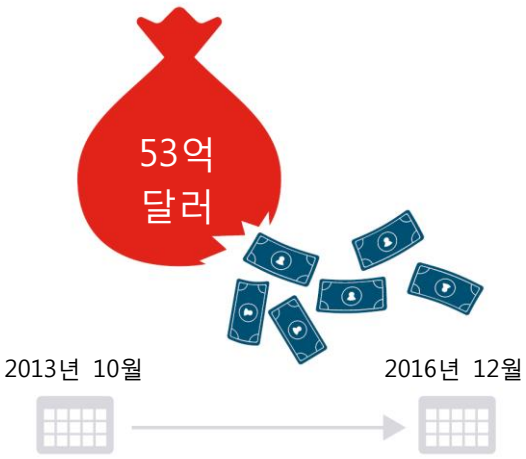
가장 기본적으로 BEC 공격에서는 송금 권한이 있는 회계 담당 직원에게 (때로는 동료 직원이 보낸 것처럼 위장한) 이메일이 발송됩니다. 사이버 범죄자는 일반적으로 그 기업의 조직 구조와 직원에 대한 조사를 마친 상태에서 이루어 집니다(예를 들어, 소셜 네트워크의 프로필을 참조하여 기업의 명령 체계를 추측합니다). CEO 또는 다른 최고 경영자가 보낸 것으로 위장한 이메일을 통해 수신자에게 동업자나 협력업체에 송금을 지시합니다. 수신자가 확인할 시간적 여유 없이 송금하도록 유도하기 위해 메시지에 긴급하다는 표현이 강조되기도 합니다. 그렇게 해서 송금한 돈은 일반적으로 사이버 범죄자 소유의 해외 및 국내 은행 계좌로 들어갑니다.

BEC 사기 수법은 주로 대기업을 표적으로 삼는데, 대기업은– 비교적 체계적인 보안 및 사기 방지 시스템을 갖추고 있음에도 불구하고 희생양으로 전락한 사례를 어렵지 않게 찾아볼 수 있습니다. 페이스북과 구글도 BEC 및 송금 사기의 피해를 입은 적이 있습니다.[12] BEC 메시지에는 악성 프로그램이나 미심쩍은 링크가 포함되어 있지 않기 때문에 아주 정교한 보안 솔루션이 아니라면 어렵지 않게 보안 시스템을 통과합니다.

FBI, 미국 법무부, 국립 화이트 칼라 범죄 센터(National White Collar Crime Center)와 협력 관계에 있는 IC3(Internet Crime Complaint Center)의 조사에 따르면 2013년 10월부터 2016년 12월까지 BEC 사기로 인한 피해액이 53억 달러(연평균 17억 달러)[13]에 달했습니다(그림 18 참조). 이에 비해 랜섬웨어로 인한 2016년 피해액은 약 10억 달러입니다.[14]

2013년 10월부터 2016년 12월까지 미국에서 BEC 사기로 인해 피해를 입은 기업은 22,300개에 육박합니다.

**그림 18.** BEC로 인한 피해액




출처: Internet Crime Complaint Center

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

12 "Exclusive: Facebook and Google Were Victims of $100M Payment Scam," Jeff John Roberts, Fortune.com, 2017년 4월 27일: fortune.com/2017/04/27/facebook-google-rimasauskas/.

13 "Business E-mail Compromise, E-Mail Account Compromise: The 5 Billion Dollar Scam," IC3 및 FBI, 2017년 5월 4일: ic3.gov/media/2017/170504.aspx.

14 "Ransomware Took In $1 Billion in 2016—Improved Defenses May Not Be Enough to Stem the Tide," Maria Korolov, CSOonline.com, 2017년 1월 5일: csoonline.com/article/3154714/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html.

BEC 사기에 맞서려면 보안 솔루션보다 오히려 비즈니스 프로세스를 보완하는 데 힘써야 합니다. 보안 정보 제공업체인 플래시포인트는 사용자 교육을 권장합니다. 예를 들어, 직원이 국내 사업체의 해외 송금 요청같은 비정상적인 송금 요청을 눈치 챌 수 있도록 교육하라는 것입니다. 또한 기업은 가짜 이메일에 속는 일이 없도록 직원 간 송금 시 전화로 확인하는 절차를 거쳐야 한다는 규정을 마련할 수 있습니다.

보안 솔루션의 경우, SPF(Sender Policy Framework) 기능이 허위 주소를 사용한 이메일을 차단하는 데 도움이 되기도 합니다. 그러나 IT 부서에서 제대로 관리하지 않을 경우 SPF가 이따금 정상적인 이메일(예: 마케팅 메시지 또는 뉴스레터)까지 차단하기 때문에 이 기능을 사용하기 꺼려하는 기업도 있습니다.

결과적으로 페이스북이나 구글과 같은 거대 기업부터 수십 명의 직원을 둔 기업에 이르기까지 온라인 시장에 진출한 기업들은 BEC 사기의 잠재적 목표가 됩니다. BEC는 범죄자에게 저비용 고수익 사기 수법이라 더욱 보편화될 가능성이 높습니다.

## 악성 프로그램의 진화: 6개월간의 관찰 결과

시스코는 2017년 상반기에 악성 프로그램의 진화 과정을 관찰해왔으며, 그 과정에서 악성 프로그램 개발자가 유포, 난독화, 회피 등의 전략을 개발할 때 무엇에 가장 주력하는지 짐작할 몇 가지 동향을 발견했습니다.

**동향 1: 사이버 범죄자는 위협이 활성화되도록 사용자에게 특정 방식의 긍정적 행동을 유도하는 악성 프로그램 유포 시스템을 사용하고 있습니다.**

악성 프로그램 자동 탐지 시스템을 우회할 수 있는 악성 이메일 첨부 파일이 증가한 것으로 조사됐습니다. 샌드박스 환경에서 이러한 첨부 파일을 검사하더라도 악성이라는 증거가 나타나지 않습니다. 따라서 다음과 같은 콘텐츠가 사용자에게 전달될 수 있습니다.

- 비밀번호로 보호되는 악성 문서(열람 유도를 위해 이메일 본문에 비밀번호 명시)
- 특정한 방식의 행동을 통해 사용자의 승인을 요청하는 대화상자(예: "'확인'을 클릭하십시오.")가 표시된 문서•• Word 문서의 악성 OLE 개체
- PDF에 포함 된 악성 Word 문서[15]

**동향 2: 사이버 범죄자는 랜섬웨어 코드베이스를 활용합니다.**

사이버 범죄자는 "교육적" 목적으로 랜섬웨어 코드를 공개적으로 배포하는 히든티어(Hidden Tear) 및 EDA2 같은 오픈 소스 코드베이스를 사용하여 악성 프로그램을 효율적· 경제적으로 개발합니다. 사이버 범죄자는 원본과 다르게 보이도록 코드를 수정한 후 악성 프로그램을 유포합니다. 시스코가 최근 몇 달간 파악한 "신종" 악성 프로그램 중 상당수는 교육용 코드베이스의 오픈 소스 코드를 토대로 개발됐습니다.

**동향 3: RaaS(Ransomware-as-a-Service) 플랫폼이 빠른 속도로 성장하고 있습니다.**

Satan 같은 RaaS 플랫폼은 코딩 또는 프로그래밍 작업을 수행하거나 기발한 전술을 개발하는 데 공을 들이지 않고서도 랜섬웨어 시장에 진출하거나 효과적으로 공격을 개시하고 싶어하는 사이버 범죄자들에게 이상적인 플랫폼입니다.

꾸준히 늘고 있는 이 플랫폼 제공업체는 사이버 범죄자들의 수입 중 일부를 가져갑니다. 심지어 일부 플랫폼 제공업체는 랜섬웨어를 배포하고 자사 '고객'의 공격 진행 상황 추적 등의 추가 서비스까지 제공합니다.

15 "Threat Spotlight: Mighty Morphin Malware Purveyors: Locky Returns via 네커스," Nick Biasini, Talos 블로그, 2017년 4월 21일: blogs.cisco.com/security/talos/locky-returns-necurs.

**동향 4: "메모리 상주" 악성 프로그램, 즉 파일이 없는 악성 프로그램이 늘고 있습니다.**

전세계 각지에서 시스템이 이런 유형의 악성 프로그램에 감염되고 있습니다. 사이버 범죄자가 반복적 메커니즘을 적용하지 않는 한, 이런 유형의 악성 프로그램은 파일 시스템이나 레지스트리에 아티팩트를 기록하지 않은 채 PowerShell 또는 WMI를 사용하여 전적으로 메모리에서 실행됩니다.[16] 그로 인해 악성 프로그램을 감지하기 더 어렵습니다. 게다가 포렌식 조사와 사고 대응도 더 까다로워집니다.

**동향 5: 명령과 제어를 감추기 위해 익명화되고 분산된 인프라에 의존하는 사이버 범죄자가 늘고 있습니다.**

시스코 조사에서 Tor 네트워크에 호스팅되는 악성 프로그램과 명령 및 제어 서비스에 쉽게 액세스할 수 있는 "브리징 서비스(Bridging Service)"의 사용률이 증가하고 있는 것으로 확인됐습니다. 일례로 로컬 Tor 클라이언트 애플리케이션을 설치하지 않고서도 인터넷에 연결된 시스템이 Tor에 호스트된 프로그램과 서비스에 액세스할 수 있게 해주는 Tor2web 프록시 서비스가 있습니다.[17]

Tor2web은 사이버 범죄자가 악성 프로그램을 수정하거나 Tor 클라이언트를 악성 프로그램 페이로드에 추가하지 않고서도 Tor를 더욱 손쉽게 사용할 수 있다는 장점이 있습니다. 사이버 범죄자는 본인이 선택한 도메인에서 Tor2web 프록시 서버를 구성할 수 있으므로 악성 프로그램을 유포할 때 Tor2web 프록시 서버를 차단하기 더 어렵습니다.

## Talos의 위협 분석: 공격과 취약점 동향 추적

시스코의 Talos 웹사이트(blog.talosintelligence.com)는 취약점 연구와 공격 수법 동향에 관한 정보 제공을 목표로 합니다. 취약점 연구는 특히 중요합니다. 시간이 흐를수록 사이버 범죄자와 보안 팀 간의 전쟁에 미치는 영향이 크기 때문입니다.

일반적으로 사이버 범죄자는 시간이 충분하기 때문에 유리한 반면, 보안 팀은 그렇지 않기 때문에 불리합니다. 사이버 범죄자가 야기한 피해를 보안 팀이 억제하는 데 소모할 수 있는 시간은 한정되어 있습니다. 취약점을 조사하면 사이버 범죄자가 취약점을 악용하기 전에 보안 팀이 활로를 차단할 수 있습니다. 제로데이 취약점을 찾아내고 패치를 개발해서 배포할 수 있도록 소프트웨어 제공업체와 협력하면 이러한 공백에 따른 피해를 최소화하는 데 도움이 되기도 합니다.

보안 업계는 랜섬웨어의 대응에 보다 기민해졌습니다. 익스플로잇 킷 활동의 감소로 Talos의 전문가들이 다른 위협을 분석하는 데 주력할 수 있게 됐습니다. 이에 따라 정보 보안 업계가 랜섬웨어의 작동 방식을 이해하고 새로운 변종 랜섬웨어를 찾아내기가 한결 수월해졌습니다.

Talos 블로그에서 논의된 또 다른 주요 동향은 사이버 범죄자가 익스플로잇 킷에서 탈피하여 이메일 기반의 공격 수법으로 관심을 돌렸다는 점입니다. 한때 주종을 이뤘던 Angler 익스플로잇 킷이 2016년에 자취를 감추게 되면서 시스코는 두각을 나타내는 다른 공격 수법이 있는지 또는 다른 주목할만한 동향이 있는지 관찰해왔습니다(**9페이지**의 "익스플로잇 킷: 감소 추세, 그러나 끈질긴 생명력" 참조). 시스코의 조사에서 Flash 또는 Java 소프트웨어를 동원한 공격 수법이 감소하고 있는 것으로 확인됐습니다. 브라우저 개발사가 관련 플러그인을 차단하면 사이버 범죄자는 이를 공격 수단으로 사용할 가능성이 줄어듭니다.

16 이 주제에 관한 상세 정보 참조: "Covert Channels and Poor Decisions: The Tale of DNSMessenger," Edmund Brumaghin, Colin Grady 공저, Talos 블로그, 2017년 3월 2일: blogs.cisco.com/security/talos/covert-channels-and-poor-decisions-the-tale-of-dnsmessenger.

17 이 주제에 관한 상세 정보 참조: "Go RAT, Go! AthenaGo Points 'TorWords' Portugal," Edmund Brumaghin, Angel Villegas 도움, Talos 블로그, 2017년 1월 8일: blog.talosintelligence.com/2017/02/athena-go.html.

다음은 특정 공격 수법에 대한 연구 결과를 중점적으로 다루고 사이버 범죄자가 보안 팀보다 앞서가기 위해 어떻게 변화할지 전망한 Talos 블로그의 최근 게시물입니다.

**새로운 게이머 'WannaCry'님이 게임에 입장하셨습니다.** - 이 게시물에는 널리 알려진 변종 랜섬웨어인 WannaCry에 대한 소개와 함께 네트워크를 위협으로부터 보호하는 방법이 제시되어 있습니다.

**MBRFilter: 어떻게 해볼 도리가 없군!** - 이 게시물에서는 Talos 전문가들이 시스템에 연결된 모든 디스크 장치의 0번 섹터에 악성 프로그램의 쓰기를 방지하는 디스크 필터인 *'MBRFilter'*를 발표했습니다. 이 전술은 Petya 같은 변종 악성 프로그램이 사용하는 것과 동일합니다. Petya는 감염된 시스템의 마스터 부트 레코드(MBR)를 덮어쓰고 부트 로더를 악성 코드로 대체하려고 시도합니다.

**Sundown 익스플로잇 킷: 좀 더 조심해야 해.** - 이 게시물에서는 Sundown 익스플로잇 킷을 다룹니다. 이와 관련된 공격은 지금까지 소수의 IP 주소에서만 진행됐지만, Talos 전문가들은 다양한 등록자 계정을 사용하여 500개 이상의 도메인과 관련된 80,000개 이상의 악성 하위 도메인을 찾아냈습니다. 따라서 이 공격 수법은 전통적인 블랙리스트 솔루션을 피할 수 있는 것으로 추정됩니다.

**네커스가 없으면 Locky는 무용지물** - 네커스 봇넷이 한시적으로 활동을 중단하자 변종 랜섬웨어인 Locky의 활동도 감소한 이유를 Talos 전문가들이 설명합니다. Talos 전문가들은 네커스 봇넷의 활동을 면밀히 주시하고 있습니다. 네커스 봇넷이 활동을 재개하면 Locky뿐만 아니라 뱅킹 악성 프로그램인 Dridex, Locky를 유포하는 스팸이 엄청나게 늘어날 수도 있습니다.

**RAT 출동! AthenaGo가 포르투갈을 노린다.** - 이 게시물에서는 Talos 전문가들이 악성 Word 문서를 통해 유포되고, 포르투갈에서 공격대상을 찾는 악성 프로그램인 AthenaGo를 조사합니다. Talos 전문가들은 감염된 시스템에서 추가 바이너리를 다운로드하고 실행할 수 있는 RAT(Remote Access Trojan)를 사용한다는 점에서 독특하다고 얘기합니다. 특이하게도 이 악성 프로그램은 Go 프로그래밍 언어로 작성되었습니다. 또한 이 악성 프로그램에 사용되는 명령 및 제어 통신은 탐지를 회피할 목적으로 사용하는 Tor2web 프록시에 의존합니다.

**은밀한 채널과 잘못된 판단: DNSMessenger 이야기** - Talos 전문가들이 DNS TXT 레코드 쿼리 및 응답을 사용하여 양방향 명령 및 제어 채널을 구현하는 악성 프로그램을 분석하고 그 결과를 공개합니다. 양방향 명령 및 제어 채널을 구현하는 수법은 DNSMessenger가 공격 대상 환경에서 실행되는 동안 탐지를 피하는 데 목적을 둔 보기 드문 회피 수법입니다.

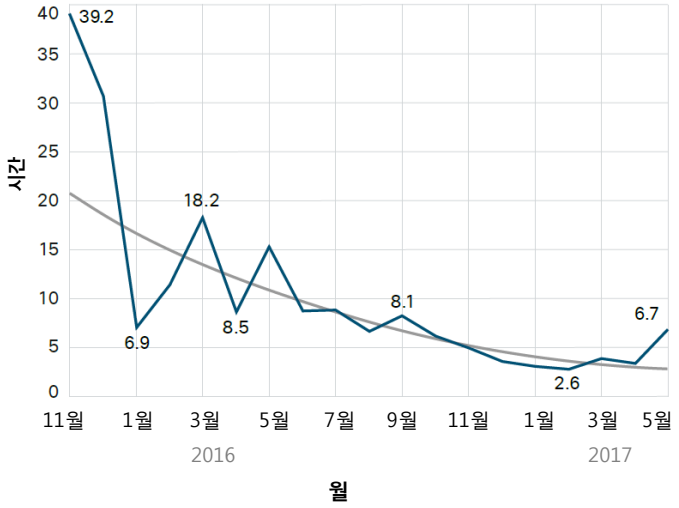
**네커스의 포트폴리오 다양화** - 이 게시물에서는 Talos 전문가들이 스팸 유포 수법을 다양화하고 투기성 저가주 주가 관련 허위 메시지를 추가한 네커스 봇넷의 새로운 활동을 진단합니다.

**위협 집중 조명: 마약 같은 악성 프로그램 제공업체** - Talos 전문가들이 조사한 바에 의하면 한시적으로 활동을 중단했던 네커스 봇넷이 다시 돌아오자, 스팸을 대량 살포하는 Locky의 활동량도 다시 크게 늘었습니다.

## 탐지 시간: 사이버 범죄자와 보안 팀의 팽팽한 줄다리기

시스코는 2015년 11월부터 탐지 시간(TTD) 중앙값을 면밀히 주시해왔습니다. 조사 이후 전반적인 동향은 감소세를 보였습니다. 특히, 조사 초기에 39시간을 살짝 웃돌았던 탐지 시간 중앙값은 2016년 11월과 2017년 5월 사이의 평균이 약 3.5시간에 불과할 정도로 대폭 감소했습니다(그림 19 참조).

**그림 19.** 월별 탐지 시간 중앙값




출처: Cisco Security Research

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

사이버 범죄자가 새로운 공격 수법을 선보이면 탐지 시간 중앙값이 증가합니다. 보안 팀이 알려진 위협을 빠르게 감지하는 기간에는 탐지 시간 중앙값이 감소합니다. 사이버 범죄자가 우위를 점한 후 이를 지키려고 애쓰면 얼마 안 가 보안 팀이 다시 기세를 되찾기를 반복하던 팽팽한 줄다리기는 2016년 여름 이후 소강 국면에 접어들었습니다.

시스코가 정의한 탐지 시간(TTD, time to detection)이란 취약점 노출 시점부터 위협 탐지까지 걸리는 시간을 말합니다. 시스코는 전 세계에 배치된 시스코 보안 제품에서 수집한 자체 보안 원격 측정 통계를 토대로 이 시간차를 산정합니다. 시스코는 글로벌 모니터링 능력과 지속적 분석 모델을 동원하여 초기에 위협으로 분류되지 않았던 모든 악성 코드가 엔드포인트에서 실행된 순간부터 위협으로 판명된 시점까지의 시간을 측정할 수 있습니다.

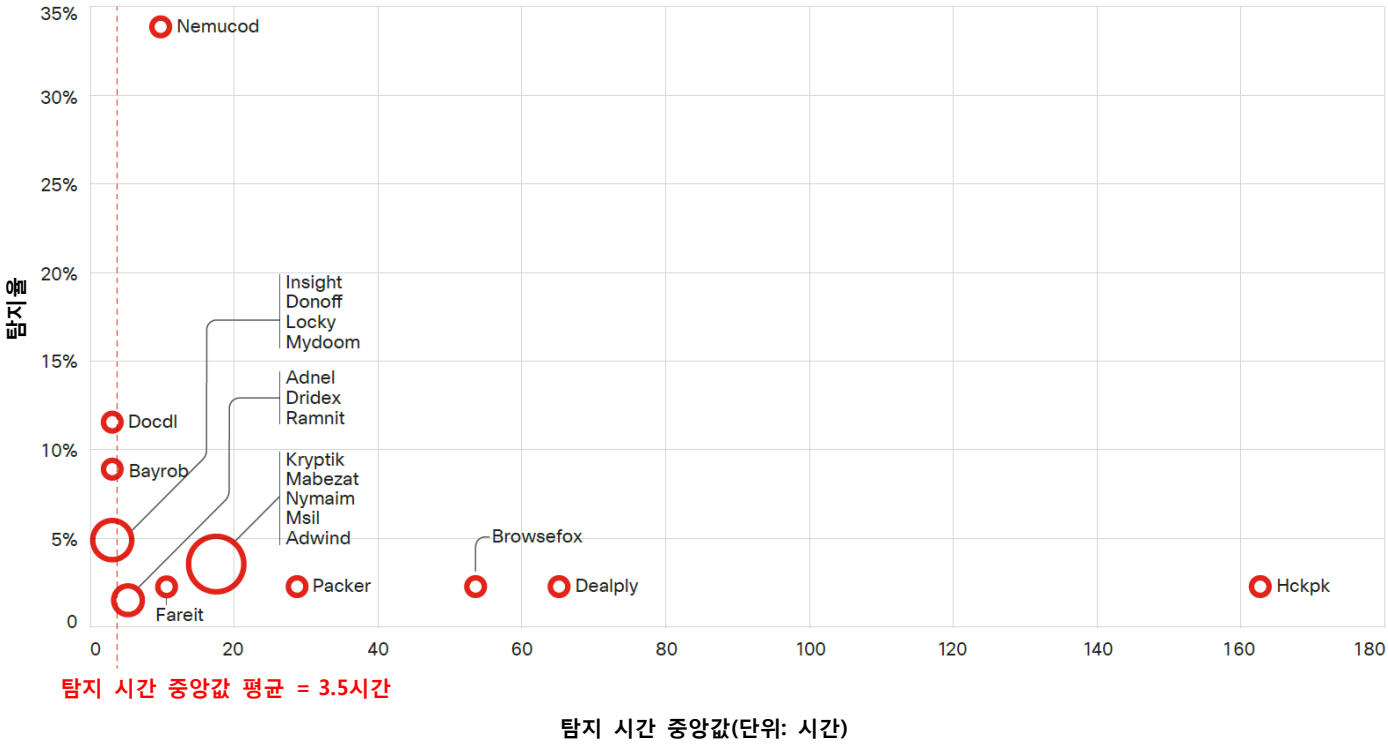
(특히 지난 6개월간의) 위협 상황의 전개 양상을 보면 공격 수법을 보완해서 탐지를 피하고 새로운 기술을 개발해야 한다는 사이버 범죄자의 압박감이 훨씬 더 커진 것을 알 수 있습니다.

그림 20에는 시스코가 2016년 11월부터 2017년 4월까지 조사한 탐지율 상위 20위 악성 프로그램의 탐지 시간 중앙값이 제시되어 있습니다. 시스코 제품이 탐지 시간 중앙값(3.5시간) 이내에 감지한 악성 프로그램 중 다수는 급격히 확산되는 위협, 즉 산업화된 위협입니다. 널리 퍼져 있는 오래된 위협 역시 일반적으로 탐지 시간 중앙값보다 짧은 시간 내에 감지됩니다.

많은 악성 프로그램은 보안 커뮤니티에 노출되더라도 보안 팀이 감지하기까지 여전히 많은 시간이 걸립니다. 그 이유는 이런 위협의 배후가 악성 프로그램의 효과와 수익성을 유지하기 위해 다양한 난독화 기법을 사용하기 때문입니다. 다음 절에서는 네 가지 특정 악성 프로그램(Fareit(RAT), Kryptik(RAT), Nemucod(다운로더 트로이 목마), Ramnit(뱅킹 트로이 목마))이 보안 팀을 따돌리기 위해 어떤 전략을 사용하는지 살펴봅니다.

이들의 전략은 효과적입니다. 그림 20에 보이는 것처럼 이 모든 악성 프로그램은 탐지 시간 중앙값인 3.5시간을 벗어나 있는데 Kryptik이 특히 그렇습니다. 심지어 상위 악성 프로그램 중 가장 빈번히 감지되는 Nemucod조차 빠르게 진화하기 때문에 감지에 많은 시간이 걸립니다.

**그림 20**. 상위 20위 악성 프로그램의 탐지 시간 중앙값




출처: Cisco Security Research

## TTE(Time To Evolve) 동향: Nemucod, Ramnit, Kryptik, Fareit

시스코는 악성 프로그램 개발자가 페이로드 전송 방식을 보완하는 방법, (해시 전용 탐지 방식을 무력화하기 위해)새 파일을 작성하는 속도, 사용자와 시스템을 효과적으로 공격하기 위해 도메인 생성 알고리즘(DGA)을 사용하는지 여부와 그 방법을 면밀히 모니터링합니다. 일부 악성 프로그램은 많은 수의 DGA 도메인을 생성하는데, 트래픽을 감추고 감지를 피하려는 방편의 일환으로 관련 도메인 이름을 살짝 바꾼 DGA 도메인이 사용됩니다(DGA 도메인에 대한 자세한 내용은 **33페이지**의 "DGA 도메인의 늘어난 수명과 중복 현상" 참조).

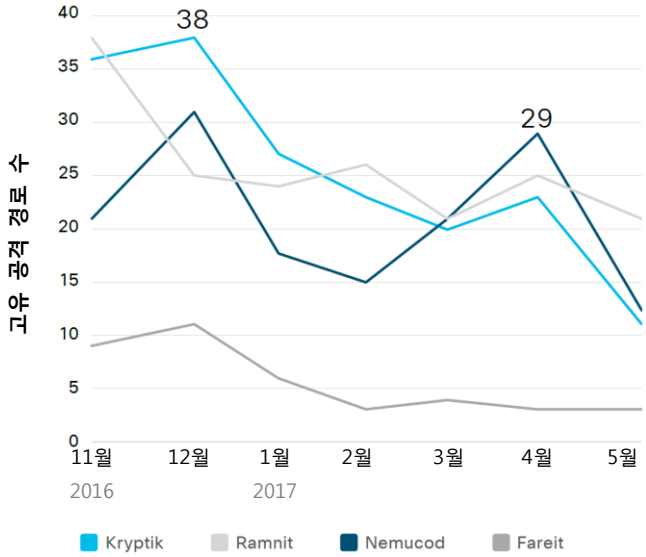
시스코는 웹 프록시 데이터, 클라우드 및 엔드포인트용 고급 악성 프로그램 차단 솔루션, 복합 악성 프로그램 차단 엔진 등 다양한 출처에서 웹 공격 데이터를 수집하여 분석합니다. 분석 결과로 얻은 데이터를 토대로 TTE(Time To Evolve)를 측정할 수 있습니다. TTE란 사이버 범죄자가 특정 악성 프로그램의 유포 방식을 변경하기까지 걸린 시간, 즉 유포 방식의 변경 주기를 뜻합니다.

각 악성 프로그램 고유의 진화 패턴과 더불어 사이버 범죄자가 보안 팀을 따돌리려고 새로운 혹은 기존의 툴과 전술을 사용하는 방법을 분석하면 보안 대책과 기술을 보완하여 지속적으로 탐지 시간을 단축할 수 있습니다(탐지 시간에 대한 자세한 내용은 **26페이지**의 "탐지 시간: 사이버 범죄자와 보안 팀의 팽팽한 줄다리기" 참조).

시스코는 2016년 11월부터 2017년 5월까지 잘 알려진 4가지 악성 프로그램(Nemucod, Ramnit, Kryptik, Fareit)을 집중 분석했습니다. 그리고 사용자 시스템에 의해 지정된 대로 파일 콘텐츠(MIME) 형식과 악성 프로그램을 유포하는 파일 확장자의 변화 추이를 지켜봤습니다. 아울러 웹 및 이메일을 통한 유포 방식의 패턴도 악성 프로그램 유형별로 조사했습니다.

그림 21에는 관찰 기간 동안 4가지 악성 프로그램이 웹 공격에 사용한 고유 공격 경로의 수가 제시되어 있습니다.

**그림 21.** 웹 이벤트에서 발견된 월별 고유 공격 경로 수



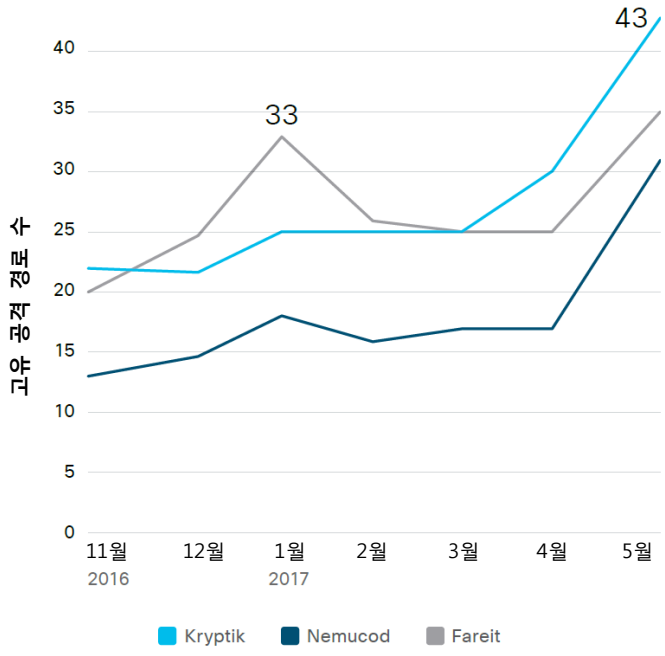

출처: Cisco Security Research

그림 22에는 관찰 기간 동안 각 유형의 악성 프로그램이 이메일 공격에 사용한 고유 공격 경로의 수가 제시되어 있습니다. 참고로, 시스코의 조사에서 Ramnit 관련 파일이 연루된 보안 이벤트(차단)는 소수만 발견됐기 때문에 Ramnit 악성 프로그램은 분석 결과에서 제외됐습니다.

TTE 분석에는 차단 시점에 악성 프로그램이 사용했던 해시의 연령에 대한 (월별) 조사도 포함됩니다. 이를 통하여 해시 기반의 탐지를 피하기 위해 악성 프로그램이 얼마나 자주, 얼마나 빨리 업그레이드되는지 파악하기 용이합니다.

그러면 4가지 악성 프로그램에 대한 분석 결과를 간추려 설명하겠습니다.

**그림 22**. 이메일 이벤트에서 발견된 월별 고유 공격 경로 수




출처: Cisco Security Research

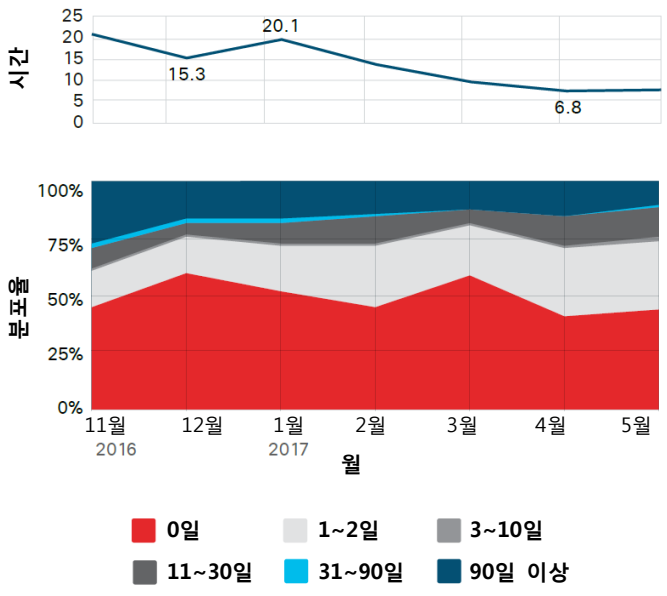
## TTE 분석: Kryptik

(GozNym으로도 알려진) Kryptik 악성 프로그램은 소스 코드가 공공연하게 유출된 고급 뱅킹 트로이 목마와 다운로더의 통합으로 탄생한 결과물입니다.[18] 시스코가 최근 TTE 연구의 일환으로 조사한 Kryptik 악성 프로그램 관련 웹 이벤트 중 약 1/3(35%)에는 JavaScript가 사용된 반면, 26%에는 .php 파일 확장자가 사용된 것으로 확인됐습니다. 그리고 MIME 형식에는 MS Word, octet-stream 또는 HTML이 사용된 것으로 조사됐습니다. 또한 Kryptik RAT 관련 이메일 이벤트에는 대부분 .zip, .js 또는 실행 파일이 사용됐습니다.

또한 Kryptik 악성 프로그램은 관찰 기간 동안 다양한 연령의 해시를 사용하고 있는 것으로 확인됐습니다(그림 23 참조).

Kryptik의 탐지 시간 동향(그림 23)을 보면 최근 몇 달 새에 시스코 제품의 위협 감지 속도가 빨라졌는데도 불구하고 악성 프로그램은 여전히 감지하기 어렵다는 사실을 알 수 있습니다. 2017년 4월 말을 기준으로 Kryptik RAT의 탐지 시간 중앙값은 전체 탐지 시간 중앙값인 3.5시간의 약 2배였습니다(탐지 시간 계산 방법에 대한 자세한 내용은 **26페이지** 참조). 그러나 이 수치는 2016년 11월 시스코가 Kryptik를 대상으로 측정한 21.5시간이란 탐지 시간에는 크게 못 미칩니다.

**그림 23**. Kryptik 악성 프로그램의 월별 탐지 시간과 해시 연령




출처: Cisco Security Research

18 "Visualizing 2016's Top Threats," Austin McBride/Brad Antoniewicz, Cisco Umbrella 블로그, 2017년 2월 8일: umbrella.cisco.com/blog/blog/2017/02/08/visualizing-2016s-top-threats/

### TTE 분석: Nemucod

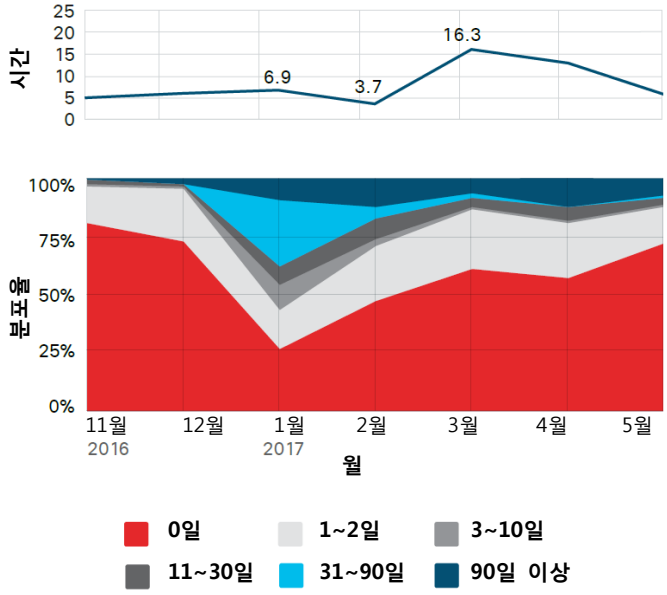
Nemucod는 2017년 내내 가장 많이 발견된 악성 프로그램으로 군림했습니다. 이 다운로더 악성 프로그램은 랜섬웨어와 기타 위협(예: 신원 도용이나 클릭 사기를 조장하는 백도어 트로이 목마)을 유포하는 데 사용됩니다. 일부 변종은 Nemucod 악성 프로그램 페이로드를 전파하는 툴 역할도 합니다.

Nemucod의 진화 양상은 이 악성 프로그램의 거듭된 성공과 밀접한 연관이 있습니다. 그림 24에서와 같이 Nemucod는 15가지가 넘는 파일 확장자와 파일 콘텐츠 형식의 조합을 사용합니다. 예를 들어, 시스코가 발견한 Nemucod 웹 이벤트에는 JavaScript가 70%로 가장 많이 사용됐고 .php(16%)와 .zip 파일 확장자(9%)가 뒤를 이었습니다. 또한 이메일의 차단 기능에 감지되는 Nemucod 이벤트는 주로 .zip, .wsf(Windows script file) 또는 .js 파일이었습니다.

그림 24를 보면 Nemucod는 보안 팀을 따돌리기 위해 앞서 하루도 안 된 해시를 주로 사용한다는 것을 알 수 있습니다.

그런데 최근 몇 달 새에 하루를 넘은 해시를 사용하는 악성 프로그램이 늘었습니다. 이 이유는 보안 커뮤니티가 Nemucod의 새로운 인스턴스를 더 철저히 감지할 수 있게 되면서 악성 프로그램 개발자가 효과적이라고 검증된 오랜 연령의 해시를 다시 사용하기 때문인 것으로 추정됩니다. 그런데도 그림 24에서 볼 수 있듯 3월과 4월에 Nemucod의 탐지 시간은 증가하면서 사이버 범죄자와 보안 팀 사이의 긴장감이 고조되고 있습니다. 사이버 범죄자가 해시 연령, 유포 방법 또는 기타 난독화 수법을 바꾼 이유와 무관하게, Nemucod 개발자는 감지하기 더 어려운 유포 수법을 개발한 것으로 보입니다.

**그림 24**. Nemucod 악성 프로그램의 월별 탐지 시간과 해시 연령




출처: Cisco Security Research

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

### TTE 분석: Ramnit

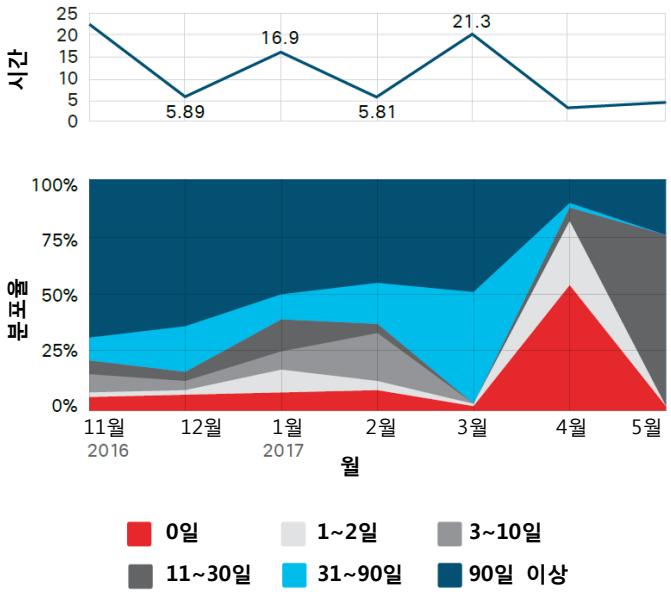
Ramnit는 2010년 자가 복제 웜으로 처음 등장했습니다. 후에 Ramnit 개발자는 악명 높은 Zeus Trojan의 유출된 소스 코드를 사용하여 데이터 도용 기능을 추가하고 기타 기능을 보완했습니다. 오늘날 Ramnit은 알려진 뱅킹 트로이 목마 중 가장 끈질긴 악성 프로그램으로 손꼽힙니다.

시스코가 최근 실시한 TTE 연구에서 Ramnit 악성 프로그램과 관련된 웹 이벤트 중 거의 대부분(99%)에 텍스트 또는 HTML MIME 형식이 사용된 것으로 확인됐습니다. 파일 확장자는 다양했지만 주로 HTML(41%)이 사용된 것으로 조사됐습니다.

시스코가 조사한 바에 의하면 사이버 범죄자들은 Ramnit에 90일 이상 된 해시를 주로 사용하여 수개월간 보안 팀을 따돌리는 데 성공했습니다(그림 25 참조).

그러나 그림 25에 보이는 것처럼 4월 전후로 Ramnit에 주로 새로운 해시가 사용됐는데, 하루도 안 된 해시가 절반을 넘었습니다. 그 이유는 보안 팀이 오래된 해시를 사용한 Ramnit의 인스턴스를 비교적 쉽게 감지하기 때문인 것으로 추정됩니다. 실제로, 3월에 21시간을 웃돌던 Ramnit의 탐지 시간 중앙값은 5월 초에 5시간 가량으로 감소했습니다.

**그림 25.** Ramnit 악성 프로그램의 월별 탐지 시간과 해시 연령



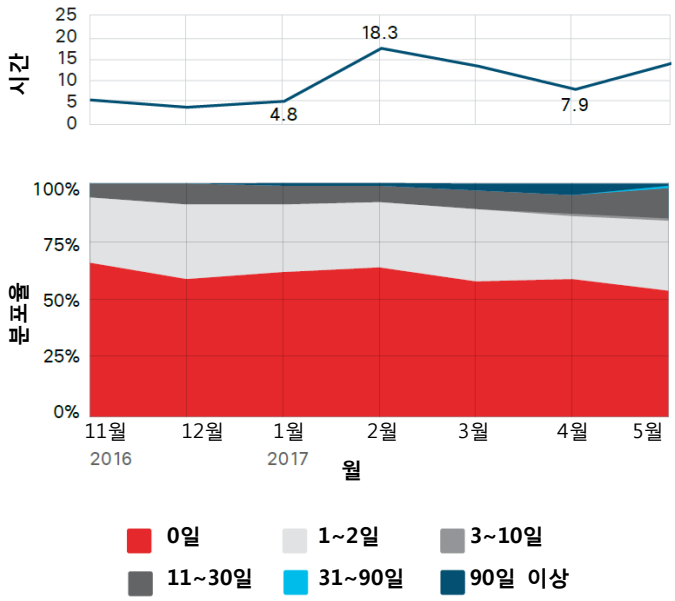

출처: Cisco Security Research

### 탐지 시간 분석: Fareit

Fareit 역시 잘 알려지고 널리 퍼져 있는 악성 프로그램입니다. Fareit RAT는 자격 증명을 빼내고 다양한 유형의 악성 프로그램을 유포합니다. 시스코의 조사에 의하면 웹 공격에 동원된 변종 Fareit 악성 프로그램 중 대다수(95%)에 .dll 파일 확장자가 사용됐습니다. 파일 콘텐츠 형식의 경우, msdos-program MIME 형식이나 msdownload MIME 형식이 84%를 차지했습니다. 이메일 공격에 동원된 Fareit 파일 확장자의 경우, Word 문서가 대부분이었고 ACE(압축 아카이브), 실행 파일 또는 .zip 파일도 사용됐습니다.

Fareit은 Kryptik 악성 프로그램과 마찬가지로 감지를 피하기 위해 해시를 자주 변경합니다(그림 26 참조). Fareit의 탐지 시간 중앙값은 2월과 3월에 눈에 띄게 치솟았습니다. 그 기간 동안 Fareit에 새로운 해시가 사용된 경우가 약간 늘었고 꽤 오래된 해시(90일 이상)도 보이기 시작했습니다.

**그림 26.** Fareit 악성 프로그램의 월별 탐지 시간과 해시 연령




출처: Cisco Security Research

### 도메인 활동: Nemucod와 Ramnit

시스코는 최근 TTE 연구의 일환으로 두 가지 악성 프로그램(Nemucod, Ramnit)과 관련된 도메인 활동을 분석했습니다. 분석 목적은 이러한 특정 악성 프로그램이 도메인을 사용하여 악성 프로그램을 유포하는 방법을 구체적으로 파악하는 것이었습니다.

관찰 기간(2016년 11월~2017년 3월) 동안 Nemucod는 Ramnit보다 더 다양한 웹사이트에 침입한 후 악용한 것으로 확인됐습니다.

한편, Ramnit은 수백 개의 DGA(Domain-Generation Algorithm) 도메인을 사용하는 것으로 조사됐습니다(DGA 도메인과 악성 프로그램 개발자가 DGA 도메인을 사용하는 이유에 대한 자세한 내용은 **33페이지**의 "DGA 도메인의 늘어난 수명과 중복 현상" 참조).

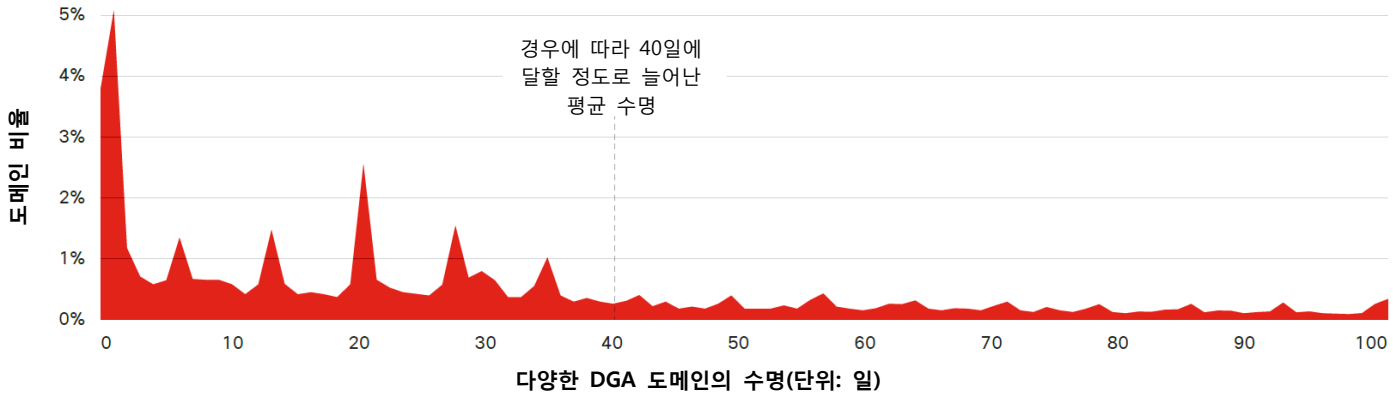
## DGA(Domain-Generation Algorithm) 도메인의 늘어난 수명과 중복 현상

널리 알려진 악성 프로그램 중 다수는 임의의 도메인 이름을 신속하게 생성하고 DGA를 사용하여 감지를 피합니다. DGA 도메인은 일반적으로 수명이 짧지만 이따금 수 개월간 유지되기도 하므로 보안 팀이 휴리스틱 탐지 기법으로 차단하기가 상대적으로 더 어렵습니다.

시스코의 파트너이자 위협 정보 제공업체인 Anomali가 다양한 악성 프로그램과 관련된 의심스러운 DGA 도메인의 수명을 추적했습니다. Anomali의 위협 연구 전문가들에 따르면 약 5년 전에 발견됐던 DGA 도메인의 수명은 대부분 3일 이하였습니다. 그 이후 DGA 도메인의 평균 수명이 경우에 따라 40일에 달할 정도로 크게 늘었습니다(그림 27 참조). 심지어 일부 DGA 도메인은 40일을 넘기기도 합니다.

참고: 모집단에 속한 약 45가지의 악성 프로그램

**그림 27.** DGA 수명




출처: Anomali

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

이러한 동향이 나타나는 이유는 사이버 범죄자가 이미 침입에 성공한 기업의 시스템에서 더 오랫동안 발각되거나 차단되지 않기 위해 더 자주 공격 수법을 업그레이드해야 한다는 부담감이 커졌기 때문인 것으로 추측됩니다(이 주제에 대한 자세한 내용은 **28페이지**의 "TTE 동향: Nemucod, Ramnit, Kryptik, Fareit" 참조). 악성 프로그램 개발자는 발 빠르게 변화를 꾀해야 차단 목록에 오르는 불상사를 막을 수 있지만, 여의치 않다 보니 오히려 우위를 점한 보안 팀이 새 도메인을 모조리 차단하는 데 성공합니다.

대부분의 경우, DGA 도메인을 생성하는 악성 프로그램의 알고리즘은 도메인을 만들 때 두 가지 요소만 수정합니다. 도메인 이름의 길이와 해당 도메인이 사용할 수 있는 최상위 도메인이 다름아닌 그것입니다. (참고: 거의 모든 알고리즘은 다양한 방식을 동원하여 2단계 도메인에 사용할 문자를 무작위로 선택합니다.)

이런 제약이 새 DGA 도메인을 지속적으로 생성해야 하는 현재의 실정과 맞물리면서 악성 프로그램이 중복된 DGA 도메인을 생성해서 등록하는 경우도 종종 발생합니다. 예를 들어, 8~10자로 이뤄진 .com 도메인처럼 문자 조합이 이미 포화된 DGA 도메인은 서로 충돌하기도 합니다. 이처럼 포화 상태에 이른 경우, 보안 팀에 의해 이미 감지된 사이버 범죄자의 DGA 도메인과 유사한 다른 사이버 범죄자의 도메인까지 덩달아 차단 목록에 등재할 수 있습니다.

## 인프라 분석을 통해 사이버 범죄자의 공격 툴에 대한 폭넓은 지식 확보

"보안 역량 벤치마크 연구: 중요 수직 산업 위주의 분석" (**77페이지** 참조)에서 언급했듯, 많은 보안 팀이 매일 수천 건에 달하는 보안 알림의 원인을 파악하느라 골머리를 앓고 있습니다. 사이버 범죄자의 등록 및 호스팅 전술(특히 사이버 범죄자가 운영하는 인프라)을 제대로 파악한 보안 전문가는 위협의 진원지를 찾아내서 차단할 수 있습니다.

시스코 파트너이자 업계 유일의 확장형 인텔리전스 기반 보안 플랫폼 제공업체인 ThreatConnect의 연구 팀은 해킹 단체인 Fancy Bear의 인프라를 분석함으로써 보안 팀이 사이버 범죄자의 네트워크 침입을 방지하는 데 도움이 되는 잠재적 악성 도메인, IP 주소 및 별칭을 파악했습니다.[19] 덕분에 기업들이 사이버 범죄자에 대한 정보를 수집함으로써 사전 대책을 강구할 수 있을 뿐만 아니라 범죄 수법도 미리 예측할 수 있습니다.

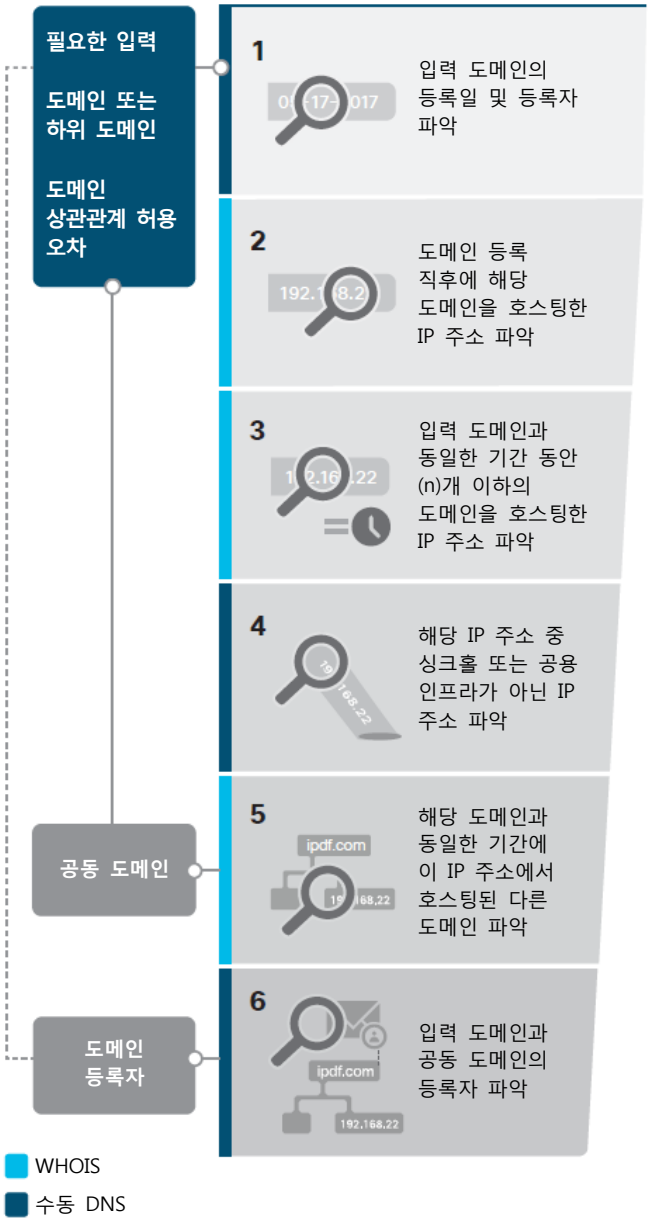
도메인과 IP 주소를 분석하자 Fancy Bear가 시민 기자 단체인 Bellingcat을 표적으로 삼고 APT를 동원한 스피어 피싱 공격을 감행한다는 사실이 드러났습니다. ThreatConnect는 몇몇 사이버 범죄자가 이미 일부 IP 인프라에 침입했기 때문에 그들이 장악한 인프라에 두 개 이상의 도메인을 호스팅할 것이라고 예견했습니다. 이러한 공동 도메인을 분석한 보안 전문가들은 사이버 범죄자가 장악할 수 있는 (도메인 및 IP 주소 같은) 인프라를 추가로 파악하고 사전에 이를 차단하거나 방어 전략에 반영할 수 있었습니다.

19 자세한 내용은 "How the ThreatConnect Research Team Used the Platform to Investigate Incidents, Identify Intelligence, and Conduct Pertinent Analysis Regarding Fancy Bear"(threatconnect.com/blog/how-to-investigate-incidents-in-threatconnect/)를 참조하십시오.

ThreatConnect의 분석 작업은 다음과 같은 과정을 거쳐 진행됐습니다.

- Bellingcat이 러시아 정부의 지원을 받은 해커로부터 발송된 것으로 추정되는 스피어 피싱 메시지의 이메일 헤더를 제보했습니다. 이후, ThreatConnect는 Fancy Bear의 이전 작전에 대한 분석 정보를 토대로 Fancy Bear가 Bellingcat을 상대로 동원할 가능성이 가장 높은 작전을 분석했습니다.
- ThreatConnect는 WHOIS 등록 정보를 사용하여 스피어 피싱 메시지의 도메인이 등록된 시간과 도메인을 등록한 이메일 주소를 파악한 후 조사 계획을 수립했습니다.
- ThreatConnect는 수동 DNS를 사용하여 도메인을 등록하고 호스팅한 IP 주소를 파악했습니다. 사이버 범죄자와 연관 있어 보이는 IP 주소를 찾아낸 것입니다.
- ThreatConnect는 다수의 고객을 위해 다수의 도메인을 호스팅하는 IP를 제외하기 위해 한 번 더 DNS를 사용하여 주어진 임의의 개수보다 적은 수의 도메인을 호스팅한 IP 주소를 파악했습니다.
- ThreatConnect는 WHOIS와 수동 DNS를 사용하여 사이버 범죄자의 전유물로 추정되는 IP 주소의 하위 집합을 파악함으로써 APT에 활용될 가능성이 높은 IP 주소 목록을 추출했습니다.
- 그런 다음 ThreatConnect는 수동 DNS를 사용하여 최초 도메인과 동일한 시기와 동일한 IP 주소에서 호스팅된 다른 도메인을 IP 주소의 하위 집합에서 추려냈습니다. (해당 도메인의 IP 주소가 최초 도메인과 동일한 경우, 동일한 APT에 장악 당한 도메인일 가능성이 있는 것으로 판단합니다.)
- 또한 ThreatConnect는 최초 도메인을 등록하는 데 사용된 것과 동일한 이메일 주소를 통해 등록된 다른 도메인도 파악했습니다. 이메일 주소가 APT 활동과 관련된 도메인을 등록하는 데 사용된 경우, 해당 이메일 주소로 등록된 다른 도메인 역시 APT 활동에 연루되어 있을 수 있습니다.
- ThreatConnect는 새로 파악한 도메인(동일한 이메일 주소를 사용하여 등록된 도메인, 최초 도메인과 IP 주소가 동일한 도메인)을 대상으로 추가 분석을 실시했습니다.
- 그런 다음 ThreatConnect는 수동 DNS를 사용하여 파악된 도메인과 관련된 하위 도메인을 파악했습니다. 이 정보는 파악된 도메인과 동일한 IP에서 호스팅되지 않은 메일 서버 또는 다른 하위 도메인을 찾아내는 데 도움이 되고 추가 조사의 근거로 삼기에도 적합합니다.

**그림 28.** 공동 도메인 분석 방식




출처: ThreatConnect

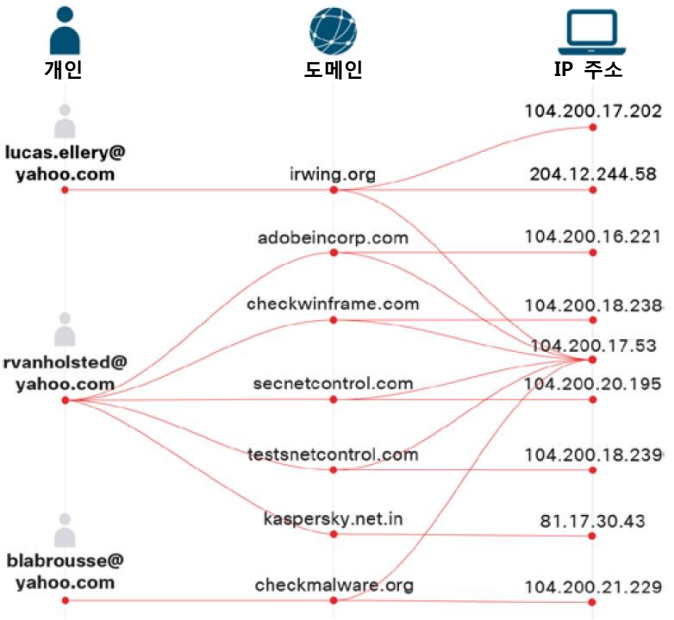
**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

그림 28에 보이는 것과 같은 분석 방법을 사용하면 당면한 위협과 관련이 있거나 의심스러워 보이는 대량의 이메일 주소, IP 주소, 도메인 그룹을 파악하는 데 도움이 될 수 있습니다. 위에서 설명한 조사는 Bellingcat에서 제보한 이메일 헤더를 통해 6개의 도메인, 5개의 IP 주소, 3개의 이메일 등록자를 파악하면서 시작됐습니다.

그리고 앞서 개괄적으로 설명한 과정을 거쳐 Fancy Bear APT 공격과 관련된 32개의 이메일 주소와 별칭, 180개 이상의 도메인, 50개 이상의 IP 주소를 파악할 수 있었습니다. 그림 29는 도메인, 이메일 주소, IP 주소 간의 상관관계 및 Bellingcat 스피어 피싱 사건과 이들의 연관성을 간추린 결과입니다.

이와 유사한 분석을 실시하는 기업은 공격의 진원지일지도 모를 도메인, IP 주소, 이메일 주소를 예방 차원에서 차단할 수 있습니다. 인프라를 조사해서 파악하는 기업은 일상적 사고 대응에 활용할 전술 정보를 확보하고, 사이버 범죄자가 기업을 공격하는 데 활용할 인프라를 미리 인지하며, 인프라와 사이버 범죄자의 과거 배경이나 연관성을 추정할 수 있습니다.

**그림 29.** APT 그룹에 의한 사용된 인프라의 연관성




출처: TheartConnect

## 공급망 공격: 한 곳만 뚫려도 전체가 위험

기업이 시간과 비용을 절약하는 데 힘쓰듯, 사이버 범죄자는 작전을 보다 효율적으로 진행할 방법을 모색합니다. 시스코 파트너인 RSA의 조사에서 밝혀진 것처럼 사이버 범죄자 입장에서 공급망은 최소한의 노력만으로 최상의 효과를 거둘 수 있는 공격 대상입니다. RSA가 조사한 경우에서 사이버 범죄자는 기업 시스템 관리자가 주로 Windows 시스템 이벤트 로그를 분석하는 데 사용하는 합법적인 소프트웨어에 트로이 목마를 삽입했습니다.[20]

감염된 소프트웨어는 업데이트 파일과 함께 소프트웨어 제공업체의 웹사이트에서 다운로드할 수 있었습니다. 결과적으로, 소프트웨어 제공업체의 웹사이트에서 단지 소프트웨어와 자동 업데이트를 제공한 것뿐인데 더 많은 기업 네트워크로 트로이 목마가 유포된 것입니다.

RSA는 "Kingslayer"라는 해킹 단체를 조사하는 과정에서 한 URL을 노린 미심쩍은 징후가 포착되자 감염된 소프트웨어를 추적했습니다.

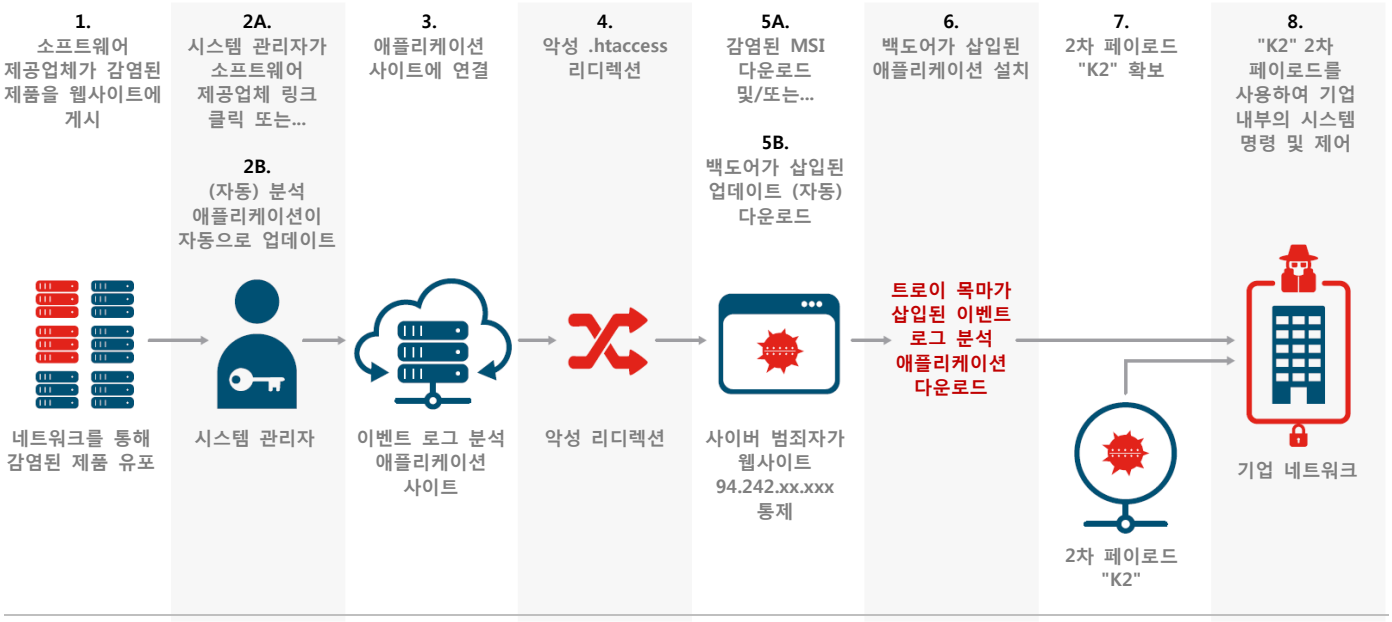
그리고 한 IP 주소를 찾아냈는데, 후에 이 주소는 악성 도메인으로 판명됐습니다. 도메인에서 발견된 악성 프로그램(PGV_PVID의 변종)의 진원지를 추적하던 RSA 팀은 그에 감염된 것으로 보이는 기업을 발견했고 악성 프로그램이 시스템 관리 소프트웨어를 통해 유포됐다는 사실까지 확인했습니다.

RSA의 조사에서 소프트웨어 다운로드 페이지뿐 아니라 소프트웨어 제공업체의 업데이트 페이지도 감염된 것으로 밝혀졌습니다(다음 페이지의 그림 30 참조). 따라서 정상적인 버전의 소프트웨어를 다운로드했던 기업까지도 자동 업데이트를 활성화한 경우 이후의 업데이트 과정에서 악성 프로그램에 감염될 우려가 있었습니다.

20 조사에 대한 자세한 내용은 RSA 보고서 "Kingslayer—A Supply Chain Attack"(rsa.com/en-us/resources/kingslayer-a-supply-chain-attack)을 다운로드하십시오.

악성 프로그램이 유포된 기간은 2주에 불과합니다. 그러나 소프트웨어 제공업체가 몇 개월 뒤에야 그 사실을 고객에게 알렸기 때문에 각 기업이 자체적으로 악성 프로그램을 감지하기 전이나 소프트웨어 제공업체가 사실을 공표하고 치료 대책을 마련할 때까지 악성 프로그램이 활개칠 수 있었습니다.

**그림 30.** Kingslayer의 악성 프로그램 감염 경로




출처: RSA

cisco.com/go/mcr2017graphics에서 2017년 그래프를 다운로드할 수 있습니다.

RSA 분석가들로서는 악성 프로그램 문제를 소프트웨어 제공업체에 알리기 전까지 얼마나 많은 기업이 감염된 소프트웨어를 설치했는지 알 길이 없습니다. 다만, 소프트웨어 제공업체의 웹사이트에 고객 명단이 공개되어 있고 이 고객들은 이벤트 로그 정보 포털 서비스에 가입한 상태입니다. 적어도 이 명단에 오른 다음과 같은 기업이 잠정적 피해자이기도 합니다.

- 4개의 글로벌 통신 서비스 제공업체
- 10개 이상의 군 부대
- 24개 이상의 Fortune 500대 기업
- 5개의 주요 방위 산업 도급업체
- 24개 이상의 은행 및 금융 기관
- 45개 이상의 고등 교육 기관

기업이 공급망 위협을 차단하는 데 힘쓰더라도 악성 프로그램을 감지하기가 쉽지 않습니다. 엔드포인트 보안은 보안 팀에게 소프트웨어의 구성요소가 다른 구성요소와 통신하고 있다는 것을 알려주기 때문에 아마도 최고의 방어 수단일 것입니다. 실시간 모니터링 역시 미심쩍은 활동을 감지하는 데 도움이 될 수 있습니다.

RSA는 Kingslayer의 최종 목표를 단언할 수 없지만 이 기업들의 규모와 전문성을 감안하면 대단히 탐나는 표적임이 분명합니다. 사이버 범죄자가 마음만 먹는다면 금융 서비스 기관에서 고객 로그인 정보를 빼내거나 정부의 혼란을 야기할 수 있기 때문입니다.

여러 가지 이유로 보안 팀은 공급망 공격 전략을 예의 주시해야 합니다. 사이버 범죄자가 공급망 중 한 부분만 공격하는 데 성공하면 다수의 표적을 감염시킬 수 있기 때문입니다. 더욱이 이런 공격은 본래 은밀하게 이뤄지므로 사이버 범죄자가 발각되지 않은 채 작전을 진행하기에 충분한 시간을 확보할 수 있습니다. 또한 시스템, 네트워크 또는 보안 관리자가 감염되지 않은 소프트웨어를 주로 사용하더라도, 사이버 범죄자는 대기업을 체계적으로 공격하기에 이상적인 교두보를 확보할 가능성이 높습니다.

### 학계 네트워크를 노리는 인프라 하베스팅(Infrastructure Harvesting) 수법

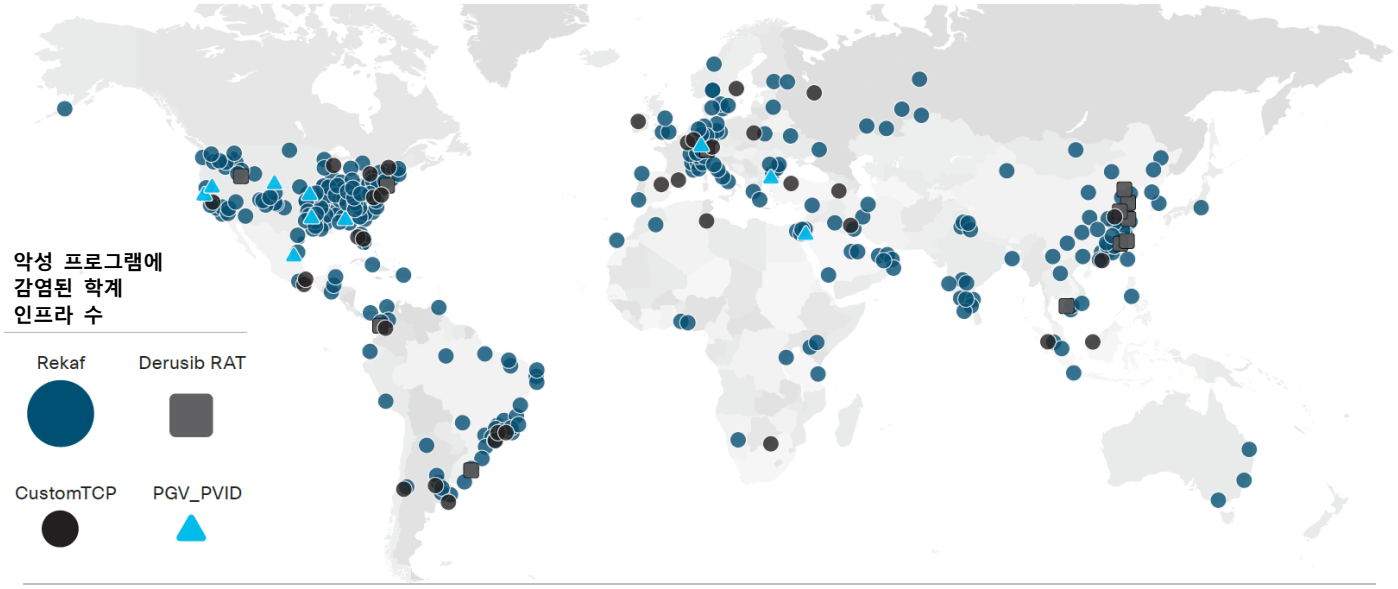
Kingslayer 사례에 동원된 사이버 범죄자의 인프라 하베스팅 수법은 합법적 하드웨어에 숨어서 소프트웨어 사용자에게 '깨끗한' 제품이라는 인상을 줬기 때문에 네트워크에 침입하는 데 성공했습니다. Schoolbell 봇넷[21]의 경우, 네트워크 자원은 사용자의 경계심을 거의 또는 전혀 유발하지 않으며 겉보기에 안전한 공간이기 때문에 사이버 범죄자가 인프라를 공격의 기폭제로 삼습니다. 두 경우에서 모두 사이버 범죄자는 네트워크 서비스 제공업체의 명성과 입지를 활용합니다.

엔드포인트 보안과 실시간 모니터링은 위에서 설명한 공급망 공격을 막는 데 도움이 될 뿐만 아니라 RSA가 "인프라 하베스팅"으로 칭한 공격 수법을 감지하는 데 도움이 되기도 합니다. 이러한 유형의 공격에서 사이버 범죄자는 대규모 공격에 이를 활용하기 위해 기업의 인프라를 장악하려고 시도합니다.

학계의 인프라를 표적으로 삼는다고 해서 명명된 Schoolbell 봇넷은 이런 공격 수법의 대표적인 예입니다. RSA의 조사에 의하면 Schoolbell 봇넷의 활동이 절정에 달한 시기에 2천 건에 육박하는 인프라 감염 사고가 발생했습니다(그림 31 참조).

Schoolbell 봇넷과 인프라 하베스팅 수법은 탐낼만한 데이터가 없기 때문에 사이버 공격을 받을 리 없다고 안심하는 곳들에 경고장을 던집니다. 교육 기관은 금융 서비스처럼 다른 산업에 종사하는 비슷한 규모의 조직에 비해 네트워크 보안에 소홀하기 쉽습니다. 따라서 학계의 네트워크는 사이버 범죄자가 손쉽게 "침입"할 수 있을 뿐만 아니라 발각되지 않은 채 은밀하게 작전을 펼칠 시간적 여유가 충분하다는 점에서 매력적인 표적이 될 수 있습니다. 학계는 더 많은 인프라 자원을 구하려는 사이버 범죄자에게 이상적인 먹잇감이 되기도 합니다.

**그림 31.** Schoolbell 악성 프로그램 전 세계 감염 추세




출처: RSA

21 Schoolbell 봇넷과 인프라 하베스팅 수법에 대한 자세한 내용은 "Schoolbell: Class Is in Session"(Kent Backman/Kevin Stear, RSA, 2017년 2월 13일: blogs.rsa.com/schoolbell-class-is-in-session/)을 참조하십시오.

## 이제 막 각광 받기 시작한 IoT와 달리, 이미 만연한 IoT 봇넷

2016년은 오랫동안 우려를 낳았던 DDoS 공격이 위세를 떨친 해였습니다. 다수의 연결 장치가 봇넷으로 돌변하면서 DDoS 공격이 시작된 것입니다. 9월에 보안 블로거인 브라이언 크렙스(Brian Krebs)를 표적으로 삼은 665Gbps 공격이 일어났습니다.[22] 그에 이어 얼마 뒤 프랑스 호스팅 회사인 OVH를 대상으로 1TBps의 공격이 시작됐습니다.[23] 그리고 10월에는 DynDNS가 DDoS 공격으로 몸살을 앓으면서 수백 개의 유명 웹사이트가 마비됐습니다(세 건의 사물 인터넷(IoT) DDoS 공격 중 최대 규모의 피해).[24]

이 세 건의 공격이 신호탄이 되어 1TBps DDoS 시대에 돌입했습니다. 그 이 세 건의 공격으로 전통적인 DDoS 보호 패러다임이 흔들리고 IoT DDoS 봇넷 공격이 현실화되자 기업도 그에 대비해야 한다는 의식을 갖게 되었습니다.

시스코 파트너인 Riskware는 최근 3대 IoT 봇넷(Mirai, BrickerBot, Hajime)의 활동을 조사하고 다음과 같은 결론을 내렸습니다.

### IoT 봇넷의 공통적 특성

- 설치가 빠르고 쉽습니다. 실제로, 1시간 내에 설치를 완료할 수 있습니다.
- 유포가 빠릅니다. 감염 재발 메커니즘 때문에 봇넷의 규모가 기하급수적으로 비대해집니다. 실제로, 사이버 범죄자가 24시간 만에 10만 대 이상의 장치를 봇넷에 감염시킬 수 있습니다.
- 감지하기 어렵습니다. 악성 코드가 장치의 메모리에 상주하고 장치를 재시작하면 삭제되므로 샘플을 확보하기가 대단히 어렵습니다.

### Mirai

DynDNS 공격에 동원된 Mirai 봇넷은 수십만 대의 IoT 장치를 감염시킨 후 강력한 대규모 DDoS 공격에 착수할 수 있는 "좀비 군대"로 탈바꿈시킵니다. 보안 전문가들은 수백만 대의 취약한 IoT 장치가 이와 같은 합동 공격에 적극 연루되어 있는 것으로 추정합니다. Mirai 악성 프로그램의 소스 코드는 2016년 말에 공개됐습니다.[25]

### 작동 원리

1. Mirai는 60개 이상의 BusyBox 소프트웨어용 기본 자격 증명을 사용하여 Telnet 서버를 대상으로 한 무차별 대입 공격을 통해 피해 시스템에 연결됩니다.
2. 감염된 모든 장치는 다른 봇을 스스로 차단합니다.
3. Mirai가 피해 시스템의 IP와 자격 증명을 중앙집중식 ScanListen 서비스에 전송합니다.[26]
4. 피해 시스템이 자기 복제 패턴을 양산하여 새로운 봇넷을 포섭하는 데 일조합니다.

### Mirai에 관한 추가 정보

Mirai의 특징은 1TBps 이상의 트래픽 볼륨을 생성한다는 점 외에, 미리 지정된 10가지 공격 수법 중 택일할 수 있다는 점입니다(그림 32 참조). 일부 공격 수법은 서비스 제공업체 및 클라우드 서비스 제공업체의 보호 계층을 공격함으로써 그 회사의 인프라를 장악하는 데 효과적인 것으로 밝혀졌습니다.

**그림 32.** Mirai의 공격 수법 메뉴


출처: Radware

10가지 공격 수법 중 GRE 플러드, TCP STOMP 및 Water Torture 공격처럼 대단히 정교한 공격 수법도 있습니다. Mirai DDoS 공격이 등장하면서 GRE 트래픽 또는 재귀적 DNS 쿼리의 적법성을 모니터링하는 일이 대단히 중요해졌습니다.

22 "KrebsOnSecurity Hit with Record DDoS," Brian Krebs, KrebsOnSecurity 블로그, 2016년 9월 21일: krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
23 "150,000 IoT Devices Abused for Massive DDoS Attacks on OVH," Eduard Kovacs, SecurityWeek, 2016년 9월 27일: securityweek.com/150000-iot-devices-abused-massive-ddos-attacks-ovh
24 "DDoS Attack on Dyn Came from 100,000 Infected Devices," Michael Kan, IDG News Service, for ComputerWorld, 2016년 10월 26일: computerworld.com/article/3135434/security/ddos-attack-on-dyn-came-from-100000-infected-devices.html
25 "Source Code for IoT Botnet 'Mirai' Released," Brian Krebs, KrebsOnSecurity 블로그, 2016년 10월 1일: krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/
26 "BusyBox Botnet Mirai—the Warning We've All Been Waiting For?" Pascal Geenens, Radware, 2016년 10월 11일: blog.radware.com/security/2016/10/busybox-botnet-mirai/

### BrickerBot

PDoS(Permanent Denial of Service) 공격은 장치 하드웨어의 기능을 마비시키도록 설계된 고속 봇 공격입니다. 이러한 형태의 사이버 공격은 점차 보편화되고 있습니다.[27]

"플래싱(Phlashing)" 공격으로 불리기도 하는 PDoS 공격을 당한 시스템은 하드웨어를 다시 설치하거나 교체해야 할 정도로 심각하게 손상됩니다. PDoS 공격은 보안 허점이나 잘못된 구성을 악용하여 펌웨어와 시스템의 기본적인 기능을 마비시킬 수 있습니다.

BrickerBot의 특징:

- **장치 침입**: BrickerBot의 PDoS 공격은 Mirai와 동일한 Telnet 무차별 대입 공격 수법을 동원하여 사용자의 장치에 침입합니다.
- **장치 손상**: BrickerBot가 장치에 침입하는 데 성공하면 일련의 Linux 명령을 실행하여 스토리지를 손상시킵니다. 그리고 나서 인터넷 연결 및 장치 성능을 마비시키는 명령을 실행하고 장치에 저장된 모든 파일을 삭제합니다.

그림 33은 BrickerBot의 정확한 명령 실행 순서를 보여주고 있습니다.

### Hajime

Hajime는 대단히 흥미로운 악성 프로그램으로서 위협 정보 분석 전문가들도 이를 면밀히 주시하고 있습니다. 그 이유는 수십만 대의 장치가 Hajime에 감염됐는데도 지금까지 아무 일도 일어나지 않았기 때문입니다. 감염 규모가 굉장히 크기 때문에 우려의 목소리도 큽니다. 한편, Hajime 개발자들은 스스로를 선량한 해커라고 주장하고 있습니다(그림 34 참조).

**그림 33.** BrickerBot의 명령 실행 순서


출처: Radware

**그림 34.** Hajime 개발자의 메시지


출처: Radware

### 작동 원리

Hajime는 정교하고 유연하며 신중하게 설계된 미래 지향적 IoT 봇넷입니다. Hajime는 자체 업데이트를 실시할 수 있으며 새로 추가된 기능을 효율적이고 빠르게 다른 동종 봇들에게 유포할 수 있습니다. Hajime는 다른 많은 IoT 봇넷과 마찬가지로 인터넷을 검색하여 TCP 23(Telnet) 포트와 TCP 5358(WSDAPI) 포트가 개방되어 있는 새로운 희생양을 찾아 감염시킵니다. 이 악성 프로그램은 무차별 대입 공격 수법을 사용하여 장치에 로그인하고 통제권을 확보합니다.

흥미롭게도, Hajime는 감염시키고자 하는 장치에서 다른 악성 프로그램을 제거할 수 있습니다. 그리고 나서 해당 장치의 Telnet 통신을 통제함으로써 새로 침입하는 악성 프로그램을 차단할 수 있습니다. 그렇게 해서 장치는 다시 중립 상태가 되지만, Hajime 개발자가 원한다면 언제든 장치에 로그인할 수 있습니다.

보안 전문가들은 Hajime가 Mirai에 감염된 장치에서 Mirai를 제거하는 사례를 발견했습니다.[28] (반면에 BrickerBot는 Mirai나 Hajime에 감염된 장치를 파괴합니다.)

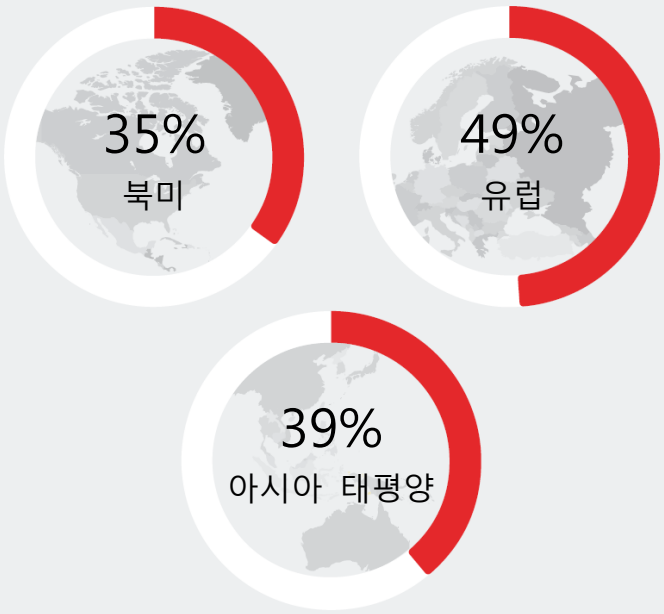
27 이 주제에 대한 자세한 내용은 "BrickerBot PDoS Attack: Back With A Vengeance"(Radware, 2017년 4월 21일: security.radware.com/ddos-threats-attacks/brickerbot-pdos-back-with-vengeance/)를 참조하십시오.

28 이 주제에 대한 자세한 내용은 "Hajime – Sophisticated, Flexible, Thoughtfully Designed and Future-Proof"(Pascal Geenens, Radware, 2017년 4월 26일: blog.radware.com/security/2017/04/hajime-futureproof-botnet/)을 참조하십시오.

## 사이버 인질극: RDoS(Ransom Denial of Service)

기업 중 거의 절반(49%)이 한 건 이상의 '사이버 인질' 사고(랜섬웨어 공격(39%) 또는 RDoS 공격(17%))을 당했습니다.[29] 그림 35는 2016년에 세계 각지에서 사이버 인질 사고를 겪은 기업의 비율을 보여주고 있습니다.[30]

**그림 35.** 2016년 국가별 사이버 인질 사고 분포도




출처: Radware

Radware는 Armada Collective라는 사이버 범죄 단체를 현재까지 발생한 대다수 RDoS 공격의 주범으로 지목합니다. 이 범죄 단체가 일반적으로 요구하는 몸값은 10~200비트코인(현행 환율로 약 3,600~70,000달러)입니다. 일반적으로 간단한 '시범' 또는 '맛보기' 공격에 몸값 요구서를 동반합니다. 몸값 지불 기한이 만료되면 사이버 범죄자는 100Gbps 이상의 트래픽 볼륨으로 공격 대상의 데이터센터를 마비시킵니다.

이제는 모방 범죄자들이 Armada Collective를 사칭하고 있습니다. 3개의 그리스 은행을 상대로 약 720만 달러를 갈취하려던 사건이 대표적입니다.[31] 이런 사이버 범죄자는 최소한의 노력으로 빠른 시일 내에 돈이 들어오기를 바라면서 가짜 몸값 요구서를 보냅니다. 여기서 가짜 몸값 요구서를 구분하는 데 유용한 팁을 소개합니다.

1. **요구액에 주목하십시오.** Armada Collective는 일반적으로 20비트코인을 요구합니다. 다른 범죄자들은 이와 꽤 차이 나는 액수를 요구합니다. 실제로, 몸값 요구액이 적은 경우 액수에 부담을 느끼지 않은 잠재적 피해자가 별다른 조치 없이 요구액을 지불하기를 바라는 모방 범죄자일 확률이 매우 높습니다.
2. **네트워크를 검사하십시오.** 진짜 해커는 간단한 공격을 감행하면서 몸값을 요구합니다. 네트워크 트래픽이 평소와 다른 경우 몸값 요구서와 협박이 진짜일 가능성이 높습니다.
3. **체계를 잘 살펴보십시오.** 진짜 해커는 체계를 제대로 갖추고 있습니다. 반면에 가짜 해커는 웹사이트 링크나 공식 계좌를 갖추고 있지 않습니다.
4. **다른 기업의 상황을 살펴보십시오.** 진짜 해킹 단체는 동일 부문에 종사하는 다수의 기업을 표적으로 삼는 경우가 많습니다. 따라서 다른 기업도 동일한 협박을 받았는지 확인해야 합니다.

29 한 시장 조사 회사가 Radware의 의뢰를 받아 전 세계 약 600명의 응답자를 대상으로 실시한 설문조사 결과
30 상동
31 "Greek Banks Face DDoS Shakedown," Mathew J. Schwartz, BankInfoSecurity.com, 2015년 12월 2일: bankinfosecurity.com/greek-banks-face-ddos-shakedown-a-8714

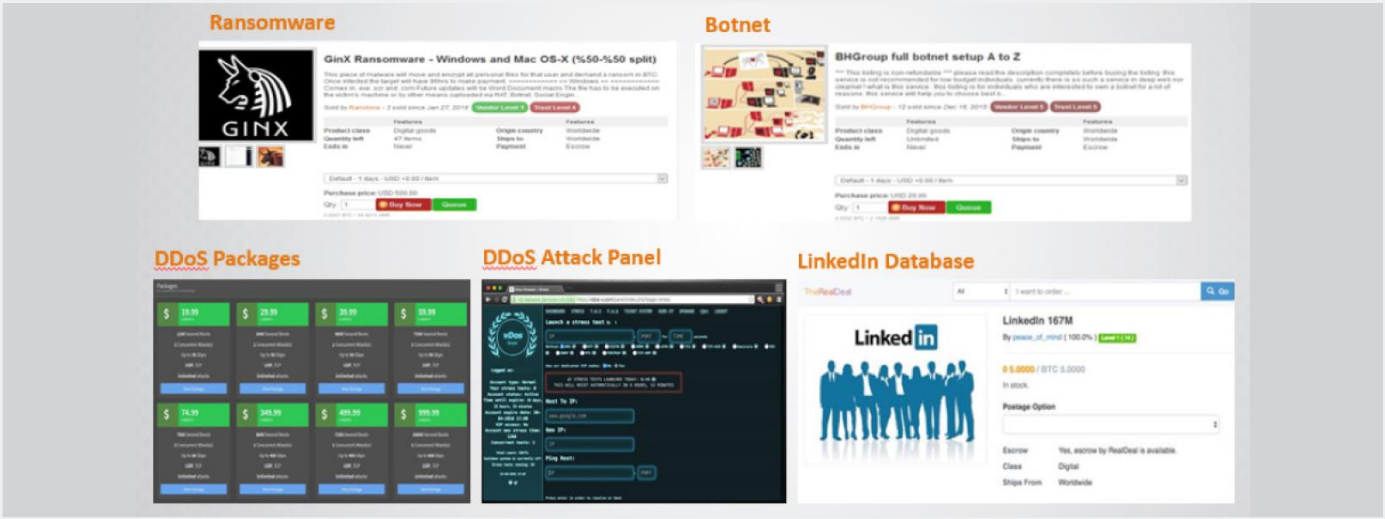
## 해킹의 경제적 변화

지난 해 사이버 공격 빈도, 복잡성, 규모가 급증했는데 이는 해킹의 자본 환경이 새로운 국면에 접어들었음을 방증합니다. Radware의 분석에 의하면 해킹 커뮤니티가 다음과 같은 혜택을 누릴 수 있게 됐습니다.

- 유용하고 저렴한 여러 가지 해킹 자원을 빠르고 손쉽게 입수(그림 36 참조)
- 온라인으로 취급하는 주요 정보는 날로 늘어나는데도 보안은 오히려 더 취약해진 '영양가 있는' 기업 급증
- 사이버 범죄자에게 효율성, 보안 및 익명성을 지원하기 적합한 수준까지 발전한 인터넷과 지하 경제

*참고: 그림 36에 제시된 소프트웨어 중 일부 툴은 더 이상 존재하지 않습니다.*

**그림 36.** 사이버 공격 툴 및 패널의 예




출처: Radware

## 인질로 잡히는 의료 기기: 실제 사건

의료 산업을 비롯한 여러 산업이 갈수록 더 촘촘히 연결되는 세상에서 효과적으로 비즈니스를 운영하려면 IT(Information Technology)와 OT(Operational Technology)를 통합해야 합니다. 그러나 운영 구조가 점점 더 촘촘하게 뒤얽히면서 과거에 서로 "차단"되어 있었던 장치와 시스템의 알려진 보안 취약점이 이제 기업에 훨씬 더 큰 위험 요소로 작용하게 됐습니다. 예를 들어, 사이버 범죄자는 사용자를 공격하는 데 피싱 이메일 같은 검증된 수법을 동원함으로써 네트워크에 침입하고, 오래된 운영체제가 설치된 장치를 교두보 삼아 네트워크에서 은밀하게 이동하면서 정보를 훔치며, 랜섬웨어 공격의 기틀을 마련합니다.

최근 발생한 WannaCry 랜섬웨어 공격은 서로 연결된 건강 관리 시스템과 취약한 보안 대책이 어떻게 조직과 환자를 위험에 빠뜨릴 수 있는지 보여주는 대표적인 사례입니다.

의료 기관을 대상으로 한 최초의 랜섬웨어 공격은 아니었지만 두 개의 미국 병원에서 사용하는 Windows 기반의 방사선 장비가 피해를 입었다는 점에서 주목할 만합니다.[32]

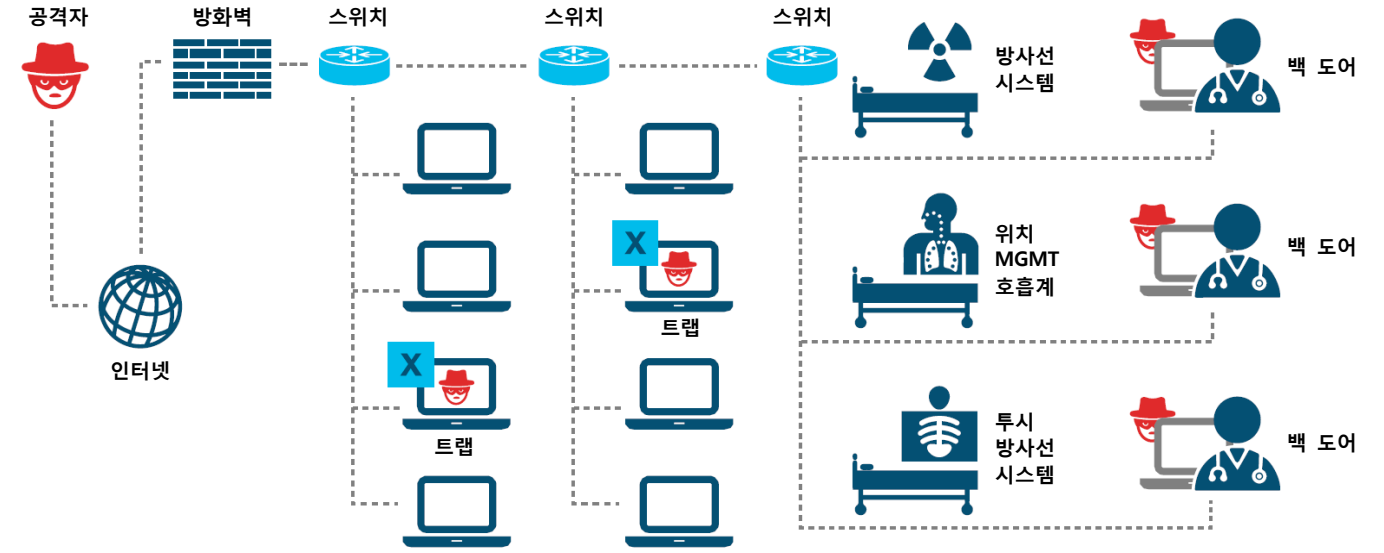
시스코 파트너이자 교란 작전 중심의 사이버보안 방어 시스템을 개발한 TrapX Security의 보안 전문가들은 랜섬웨어와 기타 악성 프로그램을 이용한 의료 기기 공격이 증가할 것이라고 경고합니다. 이런 공격 수법을 "의료 기기 하이재킹(MEDJACK)"이라고 합니다.

대여섯 개의 병과를 둔 중소 규모의 병원에서 평균 12,000~15,000대의 의료 기기를 사용한다는 점을 고려하면 잠재적 피해는 심각한 수준입니다. TrapX에 따르면 이런 의료 기기 중 10~12% 정도는 IP에 연결되어 있습니다.

32 "#WannaCry Hits Medical Devices in US," Tara Seals, InfoSecurity Magazine, 2017년 5월 18일: infosecurity-magazine.com/news/wannacry-hits-medical-devices-in-us/

오늘날 사용되고 있는 많은 다른 IoT 장치와 마찬가지로 의료기기는 과거에도 그랬고 현재도 보안을 염두에 두고 설계되거나 제작되지 않습니다. 의료기기는 패치되지 않은 오래된 시스템을 기반으로 하는 경우가 많고 병원 IT 직원이 모니터링하는 경우도 거의 없습니다. 보안 팀이 취약점을 인지하더라도 제조업체만 해당 제품에 액세스할 수 있기 때문에 조치를 취할 수 없습니다. 중요 장비의 가동을 잠깐 동안이라도 중단할 여유가 없거나 기기의 성능이 저하될 우려가 있기 때문에 보안 팀이 패치를 보류해야 하는 경우도 있습니다. 그리고 때로는 제조업체나 정부 기관 같은 다른 조직으로부터 의료기기 개량을 승인 받아야 하는데 그 과정에만 수년이 걸리기도 합니다. 게다가 의료기기의 개량 비용도 상당히 많이 드는 편입니다.

**그림 37.** 방사선 시스템 공격




출처: TrapX

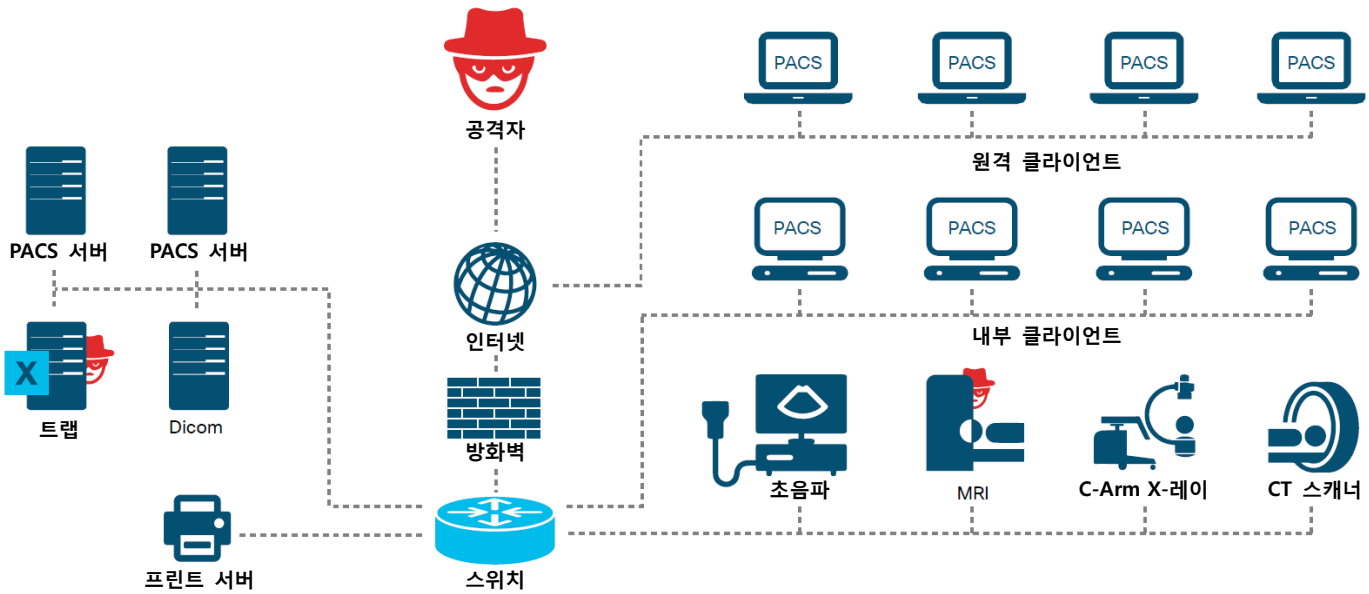
**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

많은 사이버 범죄자들이 의료기기를 공격하려고 시도합니다. TrapX의 전문가들은 사이버 범죄자가 병원 네트워크에서 은밀히 이동하는 데 의료기기가 중추적인 역할을 하기 때문이라고 설명합니다. 또한 사이버 범죄자들은 생명을 살리는 데 필요한 의료기기를 볼모로 잡는 랜섬웨어 공격으로 큰 소득을 올릴 수 있다는 사실을 알고 있습니다. 심지어 좀 더 부도덕한 범죄자는 이식용 장치 같은 의료기기를 장악하고 환자에게 피해를 입히는 것도 마다하지 않습니다.

최근에 TrapX의 전문가들은 방사선 시스템의 알려진 Windows XP 취약점을 악용한 사례를 조사했습니다. 사이버 범죄자는 3대의 컴퓨터(그 중 한 대는 강력 레이저 제어용)를 감염시킨 후 한 대를 병원 네트워크 전역에 악성 프로그램(Conficker의 변종)을 전파하는 마스터 봇넷으로 탈바꿈시켰습니다(그림 37 참조).

TrapX가 최근 조사한 또 다른 MEDJACK 사고는 MRI 시스템 감염과 관련이 있습니다. 이번에도 Windows XP의 취약점이 악용됐습니다. 사이버 범죄자는 시스템에서 환자 데이터를 발견했지만, 곧바로 방화벽을 우회하면 병원의 PACS 시스템을 장악할 수 있다는 사실을 깨달았습니다(이 시스템은 환자 기록 및 기타 중요한 정보를 중앙집중식으로 보관하고 관리하는 데 사용됩니다). 포렌식 조사를 실시한 결과, 사이버 범죄자가 병원 네트워크에서 10개월 이상 활동한 것으로 밝혀졌습니다.

**그림 38.** MRI 시스템 공격




출처: TrapX

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

Windows XP는 의료, 에너지, 제조 및 기타 산업에서 널리 사용되는 운영 체제입니다. 사이버 범죄자들은 Microsoft가 더 이상 적극 지원하지 않는 탓에 기업이 Windows XP를 기반으로 하는 중요한 장치를 업데이트하기가 매우 어렵고 많은 비용을 부담해야 하기 때문에 이 운영 체제가 약점이라는 것을 알고 있습니다. 이런 장치가 랜섬웨어를 애용하는 사이버 범죄자에게 특히 매력적인 표적이 되는 이유도 그 때문입니다. 사이버 범죄자들은 기업이 기계의 가동이 중단되거나, 최악의 경우 완전히 고장 나는 상황을 감수하느니 차라리 몸값을 지불하는 편을 택할 것이란 사실을 잘 알고 있습니다.

### 당면 과제 해결

TrapX의 전문가들은 의료 기관이 의료기기 및 기타 중요한 OT 기술을 표적으로 삼은 랜섬웨어 공격의 발생 가능성과 피해를 줄일 수 있도록 다음과 같은 조치를 취해야 한다고 충고합니다.

- 현재 IP에 연결된 의료 장비의 종류와 대수를 파악하십시오.
- 제조업체와 체결한 계약서 내용을 다시 검토하고 소프트웨어, 장치 및 시스템 업데이트 또는 교체에 관한 계약 조항이 제대로 이행되고 있는지 확인하십시오.
- 고위 경영진 및 이사회 차원에서 이 문제를 논의하여 관련 절차에 대한 관심과 지원을 유도하십시오.
- 네트워크를 모니터링하고 자동으로 위협을 감지 및 차단하는 기술 툴을 배치하십시오.

# 취약점

# 취약점

이번 섹션에서는 기업 및 사용자가 공격 또는 공략의 희생양으로 전락하는 원흉으로 작용할 수 있는 취약점 및 기타 위험 요인을 개괄적으로 설명합니다. 그리고 알려진 취약점 패치에 대한 소극적 자세, 클라우드 시스템에 대한 접근 권한 통제 소홀, 인프라 및 엔드포인트를 관리 미흡 같은 취약한 보안 대책을 논의합니다. 또한 지정학적 환경의 변화로 인해 솔루션 제공업체와 기업에게 어떤 과제와 기회가 주어지는지도 살펴봅니다.

## 각자의 임무: 악용될만한 취약점에 관한 정보 공유에 소극적인 경우 어떤 사태가 벌어지는지 엿볼 수 있었던 WannaCry 공격 사례

5월 중순에 대규모 WannaCry 랜섬웨어 공격이 발생하기 전부터 세계적으로 사이버보안에 대한 논의가 급격히 활발해졌고 우려의 목소리도 훨씬 더 커졌습니다. WannaCry 랜섬웨어 공격 사례를 되짚어보면 글로벌 커뮤니티가 사이버 범죄자와 정부의 지원을 받는 해커에 의한 악의적 공격에 따른 위험과 피해를 줄이기 위해 아직도 해야 할 일이 얼마나 많이 남아 있는지 알 수 있습니다.

시스코는 최근 발생한 이 글로벌 공격에서 다음과 같은 세 가지 교훈을 얻었습니다.

1. **정부는 소프트웨어 결함을 적시에 소프트웨어 제공업체에 고지하는 한편, 결함이 악용될만한 범위 내에서 독자적으로 해당 소프트웨어를 감독하고 검토할 수 있는 결정권을 갖는다는 내용을 성문화해야 합니다.**

악용될만한 취약점을 더욱 철저히 모니터링해야만 악용 가능성과 세계적인 피해를 최소화할 수 있습니다. 또한 정부는 악용될만한 취약점에 대한 정보를 처리할 방법과 이 정보를 기술 개발 회사와 일반 대중에게 공개할 시기에 대해 위험 기반의 결정을 내릴 수 있는 체계적이고 지속적인 프로세스를 정립해야 합니다.

2. **기술 개발 회사는 알려진 취약점, 패치, 위험 완화 및 해결 대책의 가용 또는 부재에 대한 정보를 수신, 처리 및 공개할 수 있는 개방형 위험 기반 메커니즘을 갖춰야 합니다.**

기술 개발 회사는 제품의 정상적 수명 주기 내내 보안을 지원하는 한편, 취약점 처리 방법, 툴, 이유, 시기를 대중에게 알려야 합니다. 기술 개발 회사는 공동 개발 프로세스에 대한 투명성을 제고하는 데 힘써야 합니다. 또한 기술 개발 회사는 공개하고 해결해야 할 취약점을 사용자가 누구에게 신고해야 하는지 정확히 알 수 있도록 연락 창구를 고지해야 합니다.

3. **기업 지도자는 사이버보안을 최우선 과제로 삼아야 합니다.**

오래 전부터 시스코는 기업 IT 관리자가 가능할 때마다 악의적 공격이 기업, 직원, 고객, 브랜드 평판에 미칠 수 있는 악영향에 대하여 고위 경영진 및 이사회에 인식시키도록 권고해왔습니다. 지금은 메시지를 공유하고, 메시지에 귀 기울이며, 메시지를 토대로 행동해야 할 때입니다. 기업의 경영층은 사이버보안을 최우선 과제로 삼고 사이버보안의 중요성을 전사적으로 강조해야 합니다. 또한 기업 지도자는 자사의 IT 인프라가 최신 상태를 유지하고 정기적으로 업데이트되는지 확인하고 충분한 예산을 이러한 프로젝트에 편성해야 합니다(이 주제에 대한 자세한 내용은 **83페이지**의 "보안 관리자: 보안을 중시해야 하는 시대" 참조).

정부가 세계와 취약점 정보를 공유하는 방법과 시기에 대해 제대로 논의해야 합니다. 그러나 WannaCry, Shadow Brokers, WikiLeaks Vault 7 및 Year Zero 사례에서 보았듯이 정부가 악용될만한 취약점을 아무리 감추려 애써도 언젠가 유출되기 마련입니다. 그리고 이는 다른 정부의 후원을 받는 해커와 사이버 범죄자에게 엄청난 기회로 작용합니다.

사이버 범죄자들은 급부상한 사물 인터넷(IoT)에서 거점을 확보하려고 벌써 발 빠른 행보를 보이고 있습니다. IoT에 수많은 알려진 취약점과 알려지지 않은 취약점이 존재하기 때문입니다. 정부는 기술 개발 회사가 보다 안전한 IoT 세계를 구축하는 것을 도울 확실한 기회를 얻었지만 관행을 바꾸고 투명성을 개선하는 일이 선행돼야 합니다.

한편, 기술 개발 회사는 취약점 악용 사례가 제대로 수집될 수 있도록 정부에 신고자 포상 제도를 마련할 것을 꾸준히 촉구해야 할뿐만 아니라 적시 보고 및 정보 공유에 힘써야 합니다.

사용자 역할도 그에 못지않게 중요합니다. 사용자는 적극적으로 소프트웨어를 패치하고 최신 상태로 유지하며 더 이상 지원되지 않는 제품을 최신 제품으로 업그레이드해야 합니다.

## 취약점 관련 최근 동향: 중요한 취약점 노출 직후 공격 증가

이전의 시스코 보안 보고서에서 다룬 OpenSSL 취약점 같은 중대 취약점 노출 빈도는 최근 몇 개월간 평범한 수준이었습니다(그림 39 참조). 그러나 시스코가 조사한 바에 따르면 Microsoft Windows에 영향을 미치는 취약점 악용 방법을 누설한 Shadow Brokers[34], 관리 서비스 제공업체를 대상으로 피싱 공격을 감행한 Operation Cloud Hopper 사례[35], 인기 있는 소프트웨어 솔루션과 운영체제가 어떻게 공격 당할 수 있는지 설명할 목적으로 제작된 미국 중앙정보국의 문서를 공개한 WikiLeaks Vault 7[36] 등 중대 취약점 정보가 유출되면 이를 악용한 공격이 크게 증가합니다.

대중이 인지하지 못하고 있을 뿐 취약점은 존재하고 악용될 수 있다는 사실을 유념해야 합니다. 예를 들어, Shadow Brokers가 공개한 취약점은 이미 수년 전부터 활발하게 악용됐습니다. 취약점이 공개되면 더 많은 사람들이 이를 악용할 수 있지만, 대신 보안 팀도 방어 대책을 마련할 수 있습니다.

**그림 39.** 해커 단체 주요 활동(2016년 11월~2017년 5월)

| 날짜 | 활동 | 날짜 | 활동 |
|---|---|---|---|
| **05/24/17** | Samba Insecure Library Loading 취약점 CVE-2017-7494 공개 | **03/06/17** | Apache Struts2 원격 코드 실행 취약점 CVE-2017-5638 공개 |
| **04/11/17** | Microsoft Office CVE-2017-0199 (Dridex 악용) 공개 | **02/06/17** | OpenSSL 취약점 CVE-2017-3733 공개 |
| **04/08/17** | 해킹 단체인 Shadow Brokers가 Equation Group 공격 방법 공개 | **01/26/17** | OpenSSL 취약점 공개 |
| **04/06/17** | Operation Cloud Hopper 공격 전 세계에 횡행 | **01/18/17** | Oracle CPU Oracle OIT 취약점 공개(Talos) |
| **03/29/17** | Microsoft Internet Information Services(IIS) WebDav CVE-2017-7269 | **01/03/17** | PHPMailer 무작위 명령 삽입 CVE-2016-10033 CVE-2016-10045 |
| **03/21/17** | 네트워크 시간 프로토콜 | **11/22/16** | 네트워크 시간 프로토콜 |
| **03/14/17** | Microsoft Windows 그래픽 CVE-2017-0108 | **11/10/16** | BlackNurse - ICMP DOS |
| **03/07/17** | WikiLeaks Vault 7 공개 | **11/04/16** | 모바일 OAuth 2.0 구현 원리 공개 |

출처: Cisco Security Research

33 Cisco 2015 연례 보안 보고서: cisco.com/web/offer/gist_ty2_asset/Cisco_2015_ASR.pdf
34 "Cisco Coverage for Shadow Brokers 2017-04-14 Information Release," Cisco Talos 블로그, 2017년 4월 15일: blog.talosintelligence.com/2017/04/shadow-brokers.html
35 "Operation Cloud Hopper: China-Based Hackers Target Managed Service Providers," Kevin Townsend, SecurityWeek.com, 2017년 4월 6일: securityweek.com/operation-cloud-hopper-china-based-hackers-target-managed-service-providers
36. "The WikiLeaks Vault 7 Leak – What We Know So Far," Omar Santos, Cisco Security Blog, 2017년 3월 7일: blogs.cisco.com/security/the-wikileaks-vault-7-leak-what-we-know-so-far

WikiLeaks에 의해 공개된 취약점을 살펴봄으로써 드러난 우려할만한 부분은 정부 기관이 취약점 정보를 입수하고도 이를 제대로 공개하지 않는다는 점입니다. 따라서 보안 팀들로서는 아직 공개되지 않았을 뿐 다른 취약점이 존재하는 건 아닐까 염려할 수밖에 없습니다.

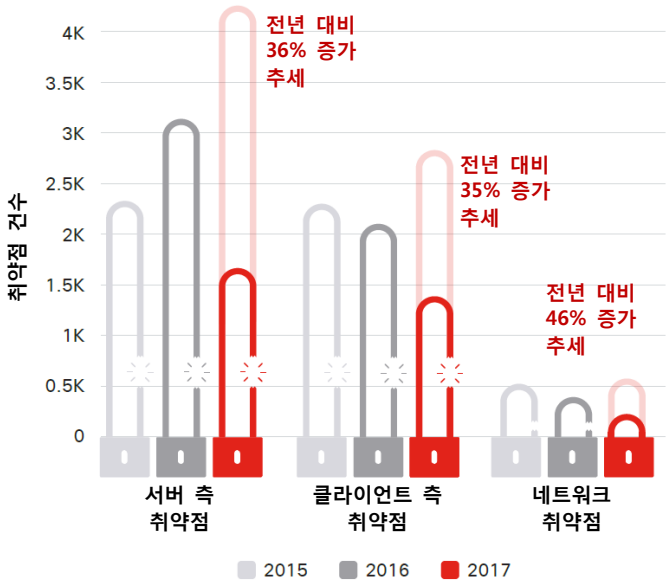
그림 39의 목록도 눈여겨볼 필요가 있습니다. Microsoft Office의 취약점이 노출되자 Dridex 봇넷이 재빨리 이를 악용했습니다.[37] 시스코의 조사에 의하면 악성 파일을 첨부한 이메일 기반 공격으로 Microsoft Office의 취약점을 악용했습니다. 또한 Apache Struts2 취약점도 공개 직후부터 악용되기 시작됐습니다.[38]

### 클라이언트-서버 취약점 증가

Cisco 2016 중기 사이버보안 보고서에서 언급했듯 서버 측 취약점이 증가했습니다. 사이버 범죄자들은 서버 소프트웨어의 취약점을 악용하면 기업 네트워크에 한결 수월하게 침입할 수 있다는 사실을 발견했습니다.[39] 2017년 초반 몇 개월간 발견된 서버 측 취약점 건수가 2016년에 비해 36%, 클라이언트 측 취약점 건수는 35% 증가한 것으로 조사됐습니다(그림 40 참조).

서버 측 취약점이 증가한 이유 중 하나는 타사의 소프트웨어에서 취약점이 발견된 경우 수동으로 패치해야 하기 때문입니다. 제때 수동 패치를 실시하지 않으면 서버 측 취약점을 악용할 기회가 커집니다. 클라이언트 측 취약점도 증가했지만 자동 업데이트를 통해 패치를 완료할 수 있으므로 악용될 여지를 없애기가 훨씬 수월합니다.

**그림 40.** 클라이언트 측 취약점




출처: Cisco Security Research

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

37 "Cisco Coverage for CVE-2017-0199," Cisco Talos 블로그, 2017년 4월 14일: blog.talosintelligence.com/2017/04/cve-2017-0199.html
38 "Content-Type: Malicious - New Apache Struts2 0-Day Under Attack," Nick Biasini, Cisco Talos 블로그, 2017년 3월 8일: blog.talosintelligence.com/2017/03/apache-0-day-exploited.html
39 "Adversaries See Value in Server-Based Campaigns," 시스코 2016 중기 사이버보안 보고서: cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html

### 익스플로잇 킷 활동 대폭 감소

익스플로잇 킷을 사용하는 사이버 범죄자의 전반적인 감소세에 맞물려 취약점을 악용하는 익스플로잇 킷의 활동은 눈에 띄게 줄고 있습니다. 소프트웨어 제공업체, 특히 웹 브라우저가 Adobe Flash와 Java로 작성된 콘텐츠 같은 일반적인 공격 매개체를 차단하자 랜섬웨어, DDoS, BEC(Business Email Compromise) 같은 한결 손쉬운 공격 수법으로 관심을 돌리는 사이버 범죄자가 늘고 있습니다(**22페이지** 참조).

### 취약점 범주: 여전히 선두를 유지 중인 버퍼 오류

CWE(Common Weakness Enumeration) 취약점 범주 조사에서 이번에도 버퍼 오류가 사이버 범죄자에 의해 악용되는 가장 일반적인 유형의 코딩 오류로 확인됐습니다(그림 41 참조). 소프트웨어에서 여전히 코딩 오류가 사라지지 않고 있습니다. 버퍼 오류를 방지하려면 이를 악용할 수 없도록 소프트웨어 개발사가 버퍼를 제한해야 합니다.

**그림 41.** 취약점 범주 악용 순위(2016년 11월~2017년 5월)


출처: Cisco Security Research

## DevOps 기술이 야기할 수 있는 보안 위험

2017년 1월 사이버 범죄자들이 공개 MongoDB 인스턴스를 암호화하고 암호 해독용 키와 소프트웨어를 제공하는 대가로 몸값을 요구하기 시작했습니다. 이후 사이버 범죄자들은 서버를 노리는 랜섬웨어의 공격 대상을 CouchDB와 Elasticsearch 같은 다른 데이터베이스로 확대했습니다.[40] 이런 DevOps 서비스가 빈번하게 공격에 노출되는 이유는 합법적인 사용자의 편의를 위해 적절한 절차를 거치지 않은 채 배포되거나 일부러 개방해두기 때문입니다.

시스코 파트너이자 보안 데이터 및 분석 솔루션 제공업체인 Rapid7은 MongoDB, CouchDB, Elasticsearch를 노린 공격을 "DevOps 랜섬웨어 공격"으로 분류했습니다. Rapid7은 Docker, MySQL, MariaDB, 널리 사용되는 기타 DevOps 구성 요소 같은 기술을 DevOps 랜섬웨어 공격 대상으로 지목했습니다.

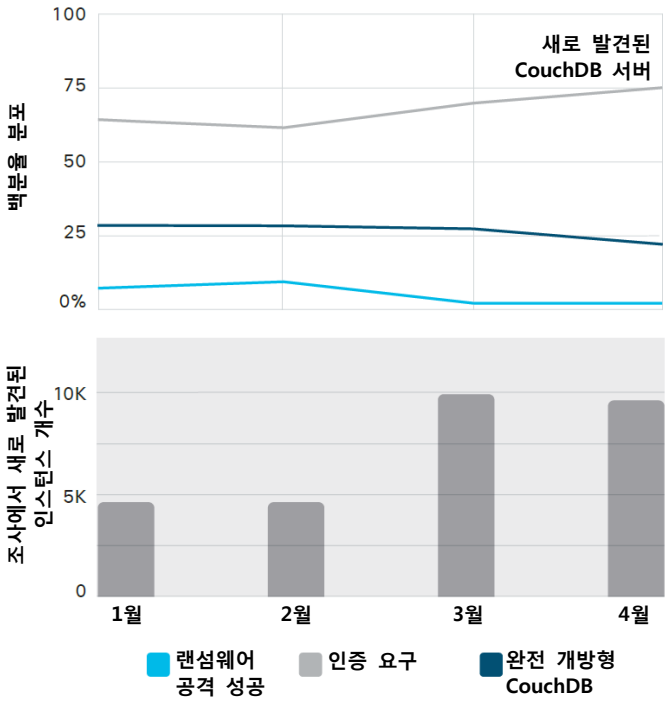
2017년 1월부터 Rapid7은 이러한 기술을 정기적으로 조사하고 개방형 인스턴스와 랜섬웨어 공격 대상 인스턴스로 분류하고 있습니다. 인터넷에 공개된 테이블의 이름으로 미루어 보아 일부 DevOps 서비스에는 개인 식별 정보(PII)가 포함되어 있습니다.

Rapid7의 조사 결과를 갖추려 소개하자면 다음과 같습니다.

### CouchDB

CouchDB 서버 중 약 75%는 (인터넷에 공개되어 있고 인증 절차를 전혀 거치지 않는) 완전 개방형 서버로 분류할 수 있습니다. 인증(최소한의 자격 증명)을 요구하는 CouchDB 서버는 1/4도 채 되지 않습니다. 약 2~3%는 사이버 범죄자의 '인질'로 잡힌 적이 있을 것으로 추정됩니다. 그리 많지 않아 보이는 수치이지만 Rapid7이 조사한 CouchDB 서버 중 약 2%에 개인 식별 정보가 저장되어 있다는 사실을 염두에 둬야 합니다. 더군다나 이런 개인 식별 정보에는 임상 약물 시험 정보, 신용카드 번호 및 개인 연락처 정보가 포함되어 있습니다.

**그림 42.** CouchDB 상태 분포도



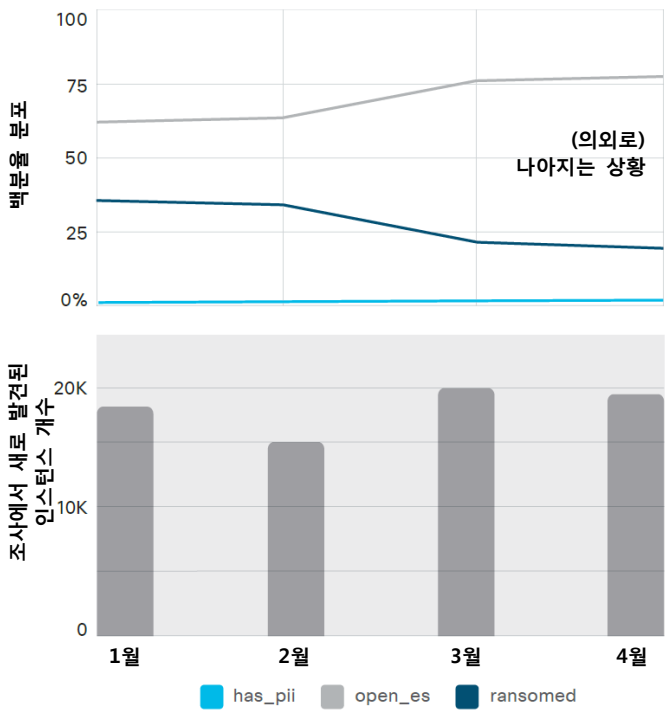

출처: Rapid7

### Elasticsearch

CouchDB와 마찬가지로 Elasticsearch 서버 중 약 75%는 완전 개방형 서버로 분류할 수 있습니다. 약 20%는 사이버 범죄자의 먹잇감이 된 적이 있을 것으로 추정됩니다. 다행스러운 소식이 있다면 Rapid7의 분석에 따르면 PII가 저장된 Elasticsearch 서버는 매우 적다는 점입니다.

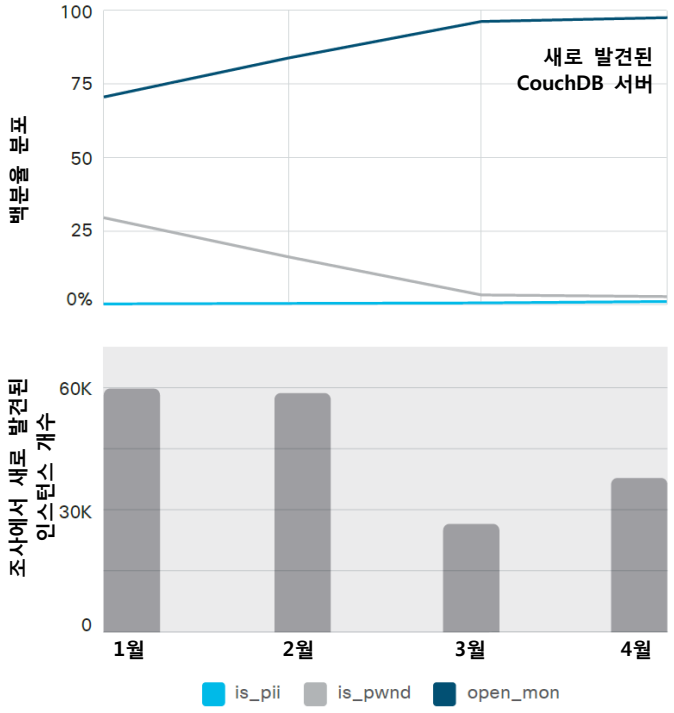
40 "After MongoDB, Ransomware Groups Hit Exposed Elasticsearch Clusters," Lucian Constantin, IDG News Service, 2017년 1월 13일: pcworld.com/article/3157417/security/after-mongodb-ransomware-groups-hit-exposed-elasticsearch-clusters.html

**그림 43.** Elasticsearch 상태 분포도




출처: Rapid7

**그림 44.** MongoDB 상태 분포도



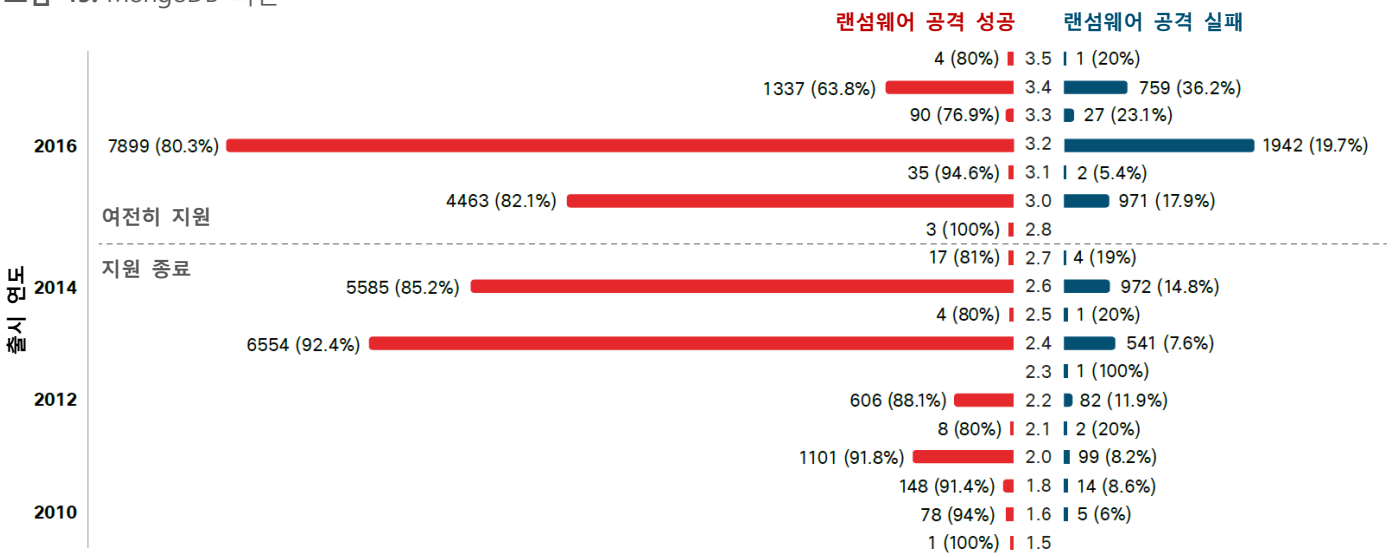

출처: Rapid7

### MongoDB

지난 1월 수천 대의 MongoDB 서버를 노린 랜섬웨어 공격이 발생했는데도 이 서버의 보안 체제는 여전히 개선해야 할 여지가 남아 있습니다. Rapid7가 조사 기간 동안 새로 발견한 서버 중 거의 100%를 완전 개방형 서버로 분류할 수 있습니다. 한가지 다행인 것은 이 중에서 민감한 정보가 저장된 서버는 극소수란 점입니다.

또한 Rapid7의 조사에서 랜섬웨어가 공격에 성공한 것으로 추정되는 MongoDB 서버 중 대부분이 지원 중단 단계에 있었던 것으로 확인됐습니다. 그러나 상당한 비율의 서버는 비교적 최신 서버이거나 여전히 지원되는 버전의 서버인데도 업데이트나 패치가 제대로 이뤄지지 않은 것으로 조사됐습니다(다음 페이지의 그림 45 참조).

**그림 45.** MongoDB 버전

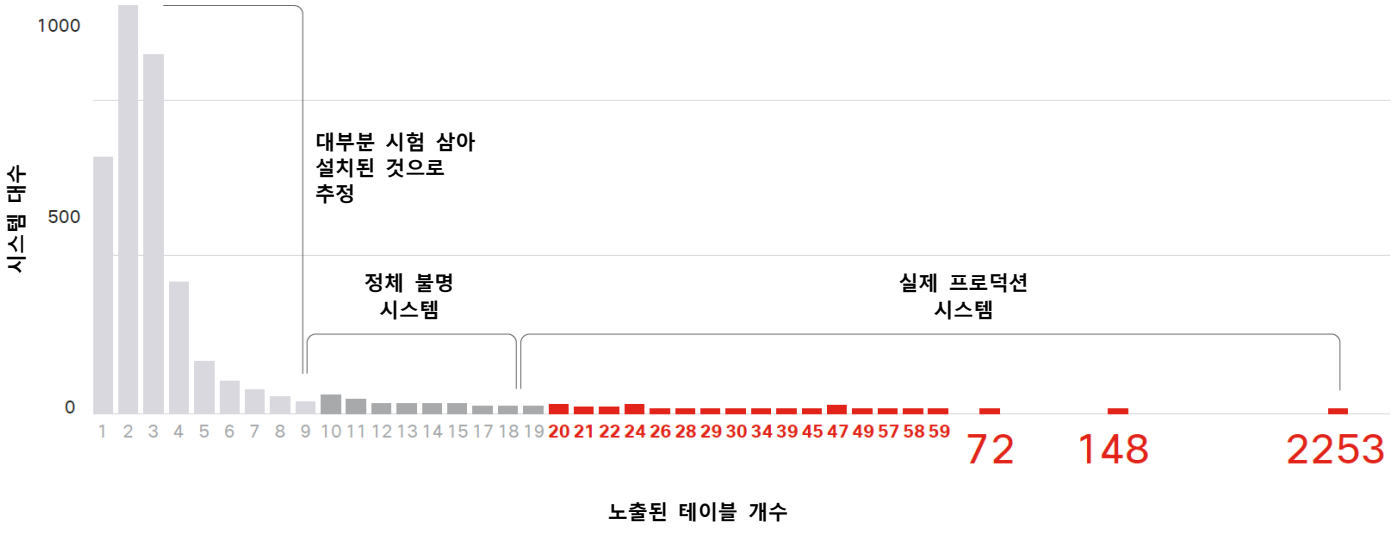



출처: Rapid7

그림 46은 Rapid7의 조사에서 노출된 것으로 확인된 MongoDB 서버의 테이블 개수를 보여주고 있습니다. 대다수 MongoDB 서버는 테이블이 10개 미만인 점을 감안하면 시험 삼아 설치된 것으로 보입니다.

그러나 일부 서버에는 20개 이상의 테이블이 존재하는 것으로 미뤄보아 실제 프로덕션 시스템으로 추정됩니다. 한편, 인터넷에 노출된 서버 한 대에는 2,200개 이상의 테이블이 존재하는 것으로 확인됐습니다.

**그림 46.** 노출된 테이블 개수에 따른 MongoDB 데이터베이스 규모 분포도(2017년 1월~4월)




출처: Rapid7

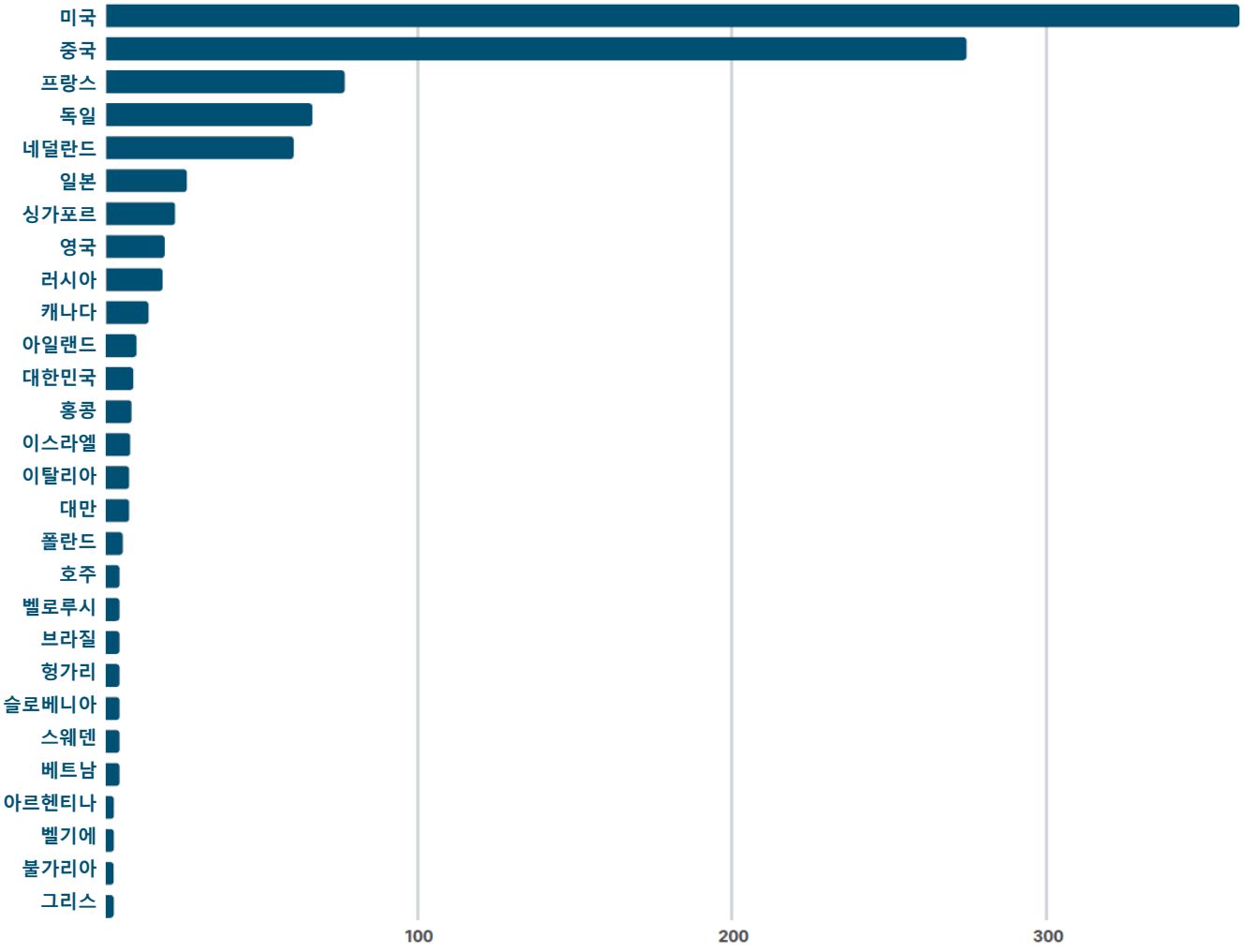
**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

### Docker

Rapid7은 운영 회사가 처음부터 보안에 철저히 신경 쓴 오케스트레이션 프레임워크인 Docker도 조사했습니다. 그러나 Rapid7의 분석에 따르면 운영 회사가 쏟은 정성이 무색하게도 1,000개 이상의 Docker 인스턴스가 완전히 공개된 상태입니다. 대부분의 Docker 인스턴스는 미국 또는 중국에 존재하는 것으로 확인됐습니다(그림 47 참조).

공개된 Docker 인스턴스 중 다수는 방치되거나 잊혀진 테스트 시스템으로 추측됩니다. 그러나 1,000개의 개방형 인스턴스 중 245개에는 최소 4GB의 메모리가 할당되어 있는 것으로 봤을 때 실제 프로덕션 시스템으로 추정됩니다(다음 페이지의 그림 48 참조).

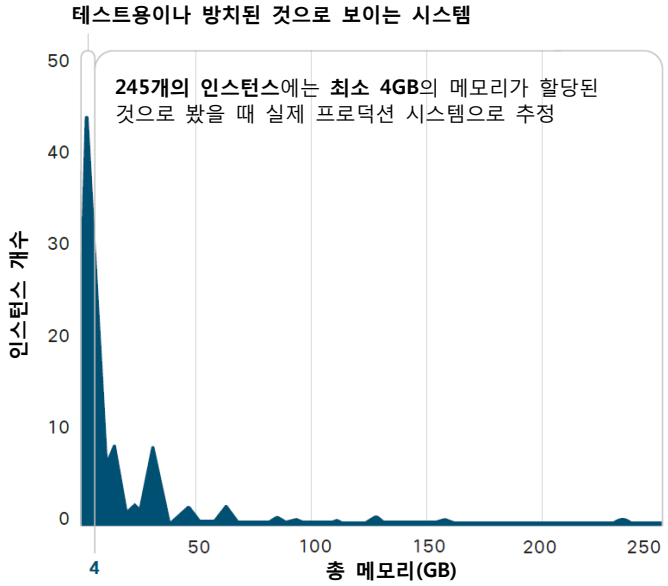
그림 47. 국가별 Docker 인스턴스 분포도(2017년 1월~4월)




출처: Rapid7

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

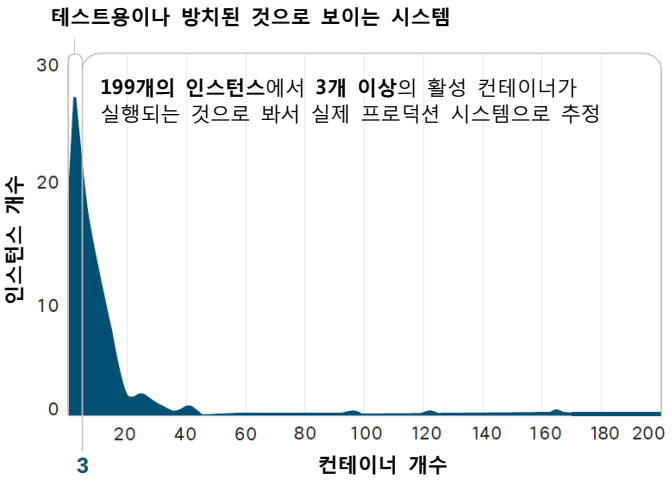
**그림 48.** Docker에 할당된 총 메모리 분포도 (2017년 1월~4월)




출처: Rapid7

또한 Rapid7의 조사에 따르면 199개의 완전 개방형 Docker 인스턴스에서 최소 3개의 활성 컨테이너가 실행되고 있습니다. 일부 Docker 인스턴스에서는 최대 160개의 컨테이너가 실행되고 있습니다(그림 49 참조). 이처럼 보안이 유지되지 않는 프로덕션 시스템을 사용하는 기업은 엄청난 위험에 노출되어 있는 셈입니다. 사이버 범죄자는 인터넷에서 이런 시스템으로 이동할 수 있는 쉘을 구현하여 시스템을 장악할 수 있습니다.

**그림 49.** 인스턴스에서 실행되는 컨테이너 개수 분포도(2017년 1월~4월)




출처: Rapid7

다양한 DevOps 기술의 공개 인터넷 인스턴스를 사용하는 기업은 위험을 해소하는 데 필요한 조치를 취해야 합니다. 보안팀이 해야 할 일은 다음과 같습니다.

- DevOps 기술을 안전하게 배포할 수 있는 체계적인 기준을 마련해야 합니다.
- 회사 소유의 공개 인프라를 지속적으로 모니터링해야 합니다.
- DevOps 기술을 상시 최신 상태로 유지하고 지속적으로 패치해야 합니다.
- 취약점을 조사해야 합니다.

## 알려진 Memcached 서버의 취약점을 패치하는 데 소극적인 기업들

사이버 범죄자들은 침입해서 데이터를 훔치거나 몸값을 요구할 심산으로 인터넷에 노출된 안전하지 않은 데이터베이스를 적극적으로 찾아 나섭니다. 수천 대의 MongoDB 데이터베이스에 피해를 입힌 랜섬웨어 공격이 지난 1월에 발생한 이후 데이터베이스 보안 사고가 급증했습니다.[41]

MongoDB 같은 서비스는 일반적으로 아무런 (또는 강력한) 인증 절차가 갖춰져 있지 않기 때문에 신뢰할 수 없는 환경에 노출하지 않아야 합니다. 시스코는 이와 유사한 서비스의 취약점을 연구하고 있습니다. 한 예로 시스코는 2016년 말에 Memcached 캐싱 서버의 보안을 평가할 목적으로 코드를 분석했습니다. 기업은 Memcached 서버를 사용하여 웹 서비스 및 애플리케이션의 속도와 성능을 개선합니다.

41 "MongoDB Databases Actively Hijacked for Extortion," Ionut Arghire, SecurityWeek, 2017년 1월 4일: securityweek.com/mongodb-databases-actively-hijacked-extortion

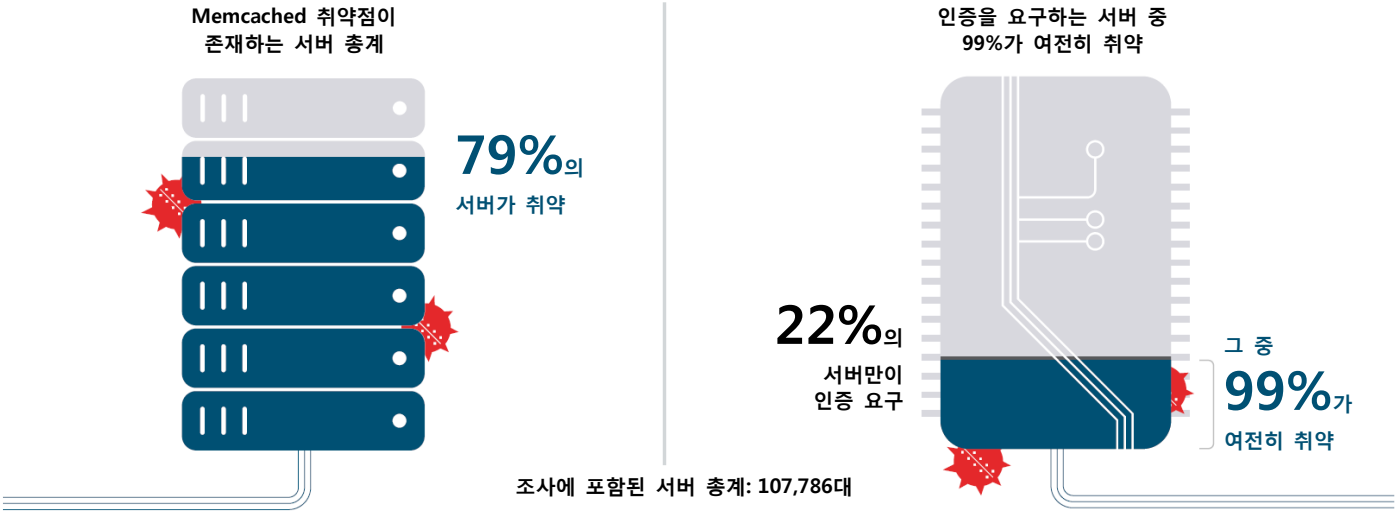
시스코는 조사 과정에서 세 가지 원격 코드 실행 취약점을 발견했습니다.[42] 한 가지 취약점은 서버의 인증 메커니즘에 있기 때문에 인증 절차가 갖춰진 서버조차도 여전히 사이버 범죄자의 마수에서 자유로울 수 없습니다. 시스코는 인증 소프트웨어 제공업체에 취약점을 알렸고 해당 기업은 서둘러 패치를 배포했습니다.

취약점을 알린 지 몇 달 뒤, 시스코는 패치 배포의 상황을 파악하고자 인터넷 전수 검사를 실시했습니다. 인증 소프트웨어 제공업체가 서둘러 패치를 개발하고 Linux 유통업체는 신속하게 업데이트를 배포했지만, 노출된 약 110,000대의 Memcached 서버 중 79%에 여전히 원격 코드 실행 취약점이 패치되지 않은 것으로 조사됐습니다(그림 50 참조).

게다가 인증 절차가 활성화된 서버는 22%에 불과했습니다. 또한 인증을 요구하는 거의 모든 서버(23,907대 중 23,707대)가 여전히 취약합니다(그림 50 참조). 시스코의 조사 대상에 포함된 서버는 전 세계 국가에 분포되어 있지만 미국과 중국이 대부분을 차지합니다. 가장 최근의 조사 시점인 3월을 기준으로 해도 이 두 국가에 취약한 서버가 편중되어 있습니다(그림 51 참조).

결론을 말하면, 시스코는 이 세 가지 취약점 때문에 피해를 입은 서버는 전혀 발견되지 않았지만 그것도 시간 문제일 가능성이 큽니다. 취약점 및 관련 패치에 대한 정보는 이미 수개월 전에 공개된 상태입니다.

**그림 50.** 취약점: Memcached




출처: Cisco Security Research

42 자세한 내용은 다음 2016년 Talos 취약점 보고서 참조: "Memcached Server Append/Prepend Remote Code Execution Vulnerability," talosintelligence.com/vulnerability_reports/TALOS-2016-0219, "Memcached Server Update Remote Code Execution Vulnerability," talosintelligence.com/vulnerability_reports/TALOS-2016-0220, "Memcached Server SASL Authentication Remote Code Execution Vulnerability," talosintelligence.com/vulnerability_reports/TALOS-2016-0221

## 클라우드로 관심을 돌린 사이버 범죄자들

해커 입장에서 클라우드는 완전히 새로운 개척지이며 그들은 공격 경로로서 클라우드의 잠재력을 본격적으로 타진하고 있습니다. 해커들은 많은 기업에서 클라우드 시스템이 중추적인 역할을 한다는 사실을 잘 알고 있습니다. 또한 그들은 클라우드 시스템을 공격하는 데 성공하면 연결된 다른 시스템에 더욱 빠르게 침입할 수 있다는 사실을 알고 있습니다.

시스코의 조사에 의하면 2016년 말부터 다양한 수준의 정교함이 뒷받침되는 수법으로 클라우드 시스템을 공격하는 해커의 활동이 증가했습니다.

2017년 1월 시스코는 유효한 기업 사용자 로그인 정보를 물색하는 해커를 조사했습니다. 무차별 대입 공격을 동원한 해커들은 인터넷에 노출된 계정 목록을 토대로 유효한 기업 사용자 자격 증명(사용자 ID 및 비밀번호) 라이브러리를 만들었습니다. 그들은 매우 의심스러운 20개의 IP를 사용하는 서버를 통해 여러 기업의 클라우드 환경에 로그인하려고 시도했습니다.

시스코는 2016년 12월부터 2017년 2월 중순까지 행동 분석 기술과 기타 툴을 사용하여 수천 개에 달하는 기업 고객의 클라우드 환경을 분석했습니다. 그 결과, 시스코의 조사 대상에 포함된 기업 중 17% 이상의 기업에서 유사한 로그인 시도 패턴이 나타났습니다. 해커들은 탐지를 피하기 위해 20개의 IP를 무작위로 번갈아 사용했습니다.

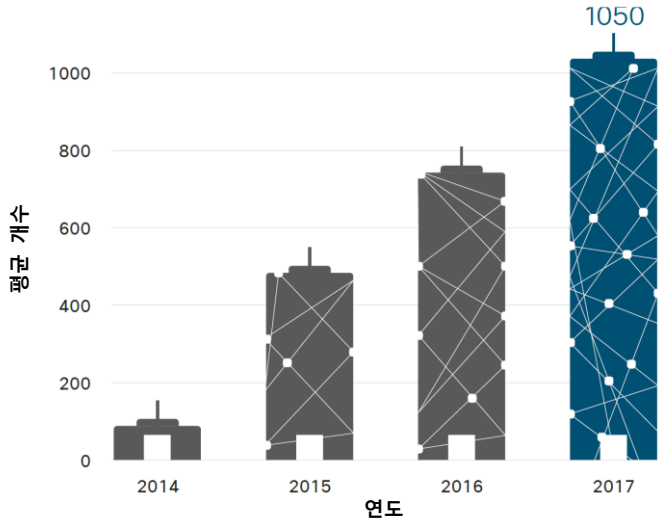
시스코는 고객에게 이 문제를 경고하고 미심쩍은 IP를 블랙리스트에 추가했습니다. 해커가 유효한 기업 사용자 자격 증명 라이브러리를 어떤 목적으로 사용하려 했는지는 밝혀지지 않았습니다. 다만, 스피어 피싱이나 사회 공학적 공격을 감행하려고 준비했다는 설이 유력합니다. 사이버 범죄자가 사용자 ID 및 비밀번호 조합을 판매하거나, 자격 증명을 직접 사용하여 사용자 계정에 로그인한 후 민감한 데이터를 빼내거나 다른 동료 직원들을 공격하려 했다는 설도 설득력이 있습니다. 명확히 밝혀진 사실은 해커가 기업 클라우드 시스템에 접속하는 데 사용하려고 했던 대부분의 자격 증명이 이전의 보안 사고에서 유출된 법인 계정과 관련되어 있다는 점입니다.

### 클라우드의 장점을 배가하지만 위험도 야기하는 OAuth

시스코는 직원이 기업에 설치하는 타사의 네트워크 기반 클라우드 애플리케이션의 위험성을 조사한 후 그 결과를 Cisco 2017 연례 사이버보안 보고서에 수록한 바 있습니다. 이런 애플리케이션은 기업의 인프라에 연결되며 사용자가 OAuth(Open Authorization)를 통해 접속 권한을 획득한 순간 기업 클라우드 및 SaaS(Software-as-a-Service) 플랫폼과 자유롭게 통신할 수 있습니다.

그림 52에서 볼 수 있듯 2014년 이후 기업에서 사용하는 네트워크 기반 클라우드 애플리케이션의 개수가 급격히 증가한 것으로 확인됐습니다. 기업 환경에 설치되는 애플리케이션 개수는 평균 1,000개 이상이고 한 기업의 설치 횟수를 도합하면 20,000회가 넘습니다.

**그림 52.** 한 기업에서 사용하는 네트워크 기반 클라우드 애플리케이션의 개수




출처: Cisco Security Research

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

Gmail 사용자를 공격하고 OAuth 인프라를 악용하려는.피싱 공격이 최근 급증하면서 OAuth 보안 위험이 심화됐습니다.[43] 사이버 범죄자는 사용자의 이메일 계정을 장악한 후 연락처 목록에 있는 다른 사용자에게 피싱 웜을 전파하려고 시도했습니다. Google의 발표에 따르면 10억 명의 줄잡아 30만 개 이상의 기업이 이 웜에 감염되었던 것으로 추정합니다.[45]

### 클라우드 보안: 단 한 명의 최상위 권한 소유 클라우드 사용자에 의해 초래될 수 있는 엄청난 위험

역대 최대 규모의 보안 사고는 가장 많은 권한을 가진 계정 하나가 사이버 범죄자의 손에 넘어가면서 시작되는 경우도 꽤 있습니다. 최상위 권한의 사용자 계정에 대한 접속 정보를 확보한 해커는 "왕국으로 들어가는 만능열쇠"를 거머쥔 채 마음껏 탈취하고 심각한 피해를 입힐 수 있습니다. 그러나 대다수 기업은 이런 위험에 충분한 주의를 기울이지 않고 있습니다.

이와 같은 보안 문제의 상황을 더욱 정확히 파악하기 위해 시스코가 495개 기업에서 사용 중인 최상위 권한의 사용자 계정 494개를 조사한 결과, 클라우드 플랫폼 사용자 계정 100개 중 6개가 최상위 권한의 사용자 계정으로 확인됐습니다(그림 53 참조). 그러나 대다수 기업에서 최상위 권한의 사용자 계정을 보유한 사용자 중 평균 2명이 대부분의 관리 업무(88%)를 책임지고 있습니다. 또한 기업이 기존의 관리자 계정 중 75%에서 "최고 관리자" 권한을 회수하더라도 업무에 거의 혹은 전혀 지장이 없는 것으로 조사됐습니다.

**그림 53.** 과도하게 많은 최상위 권한의 사용자 계정


출처: Cisco Security Research

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

43 "Google Docs Phishing Attack Underscores OAuth Security Risks," Michael Kan, IDG News Service, 2017년 5월 5일: pcworld.com/article/3194816/security/google-docs-phishing-attack-underscores-oauth-security-risks.html

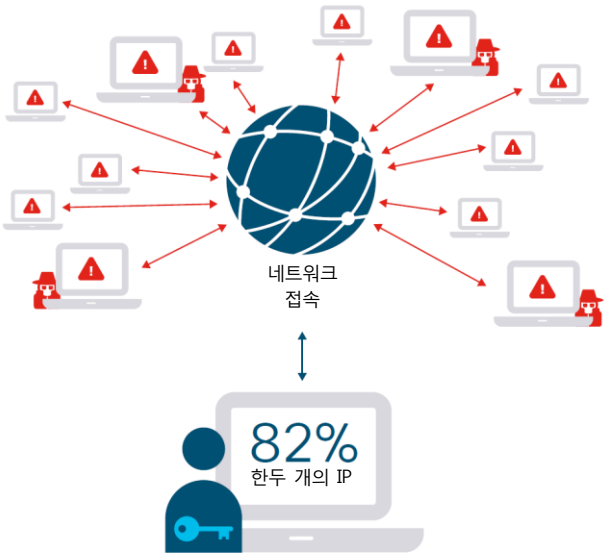
44 "A Massive Google Docs Phish Hits 1 Million Gmail Accounts—UPDATED," Thomas Fox-Brewster, Forbes, 2017년 5월 3일: forbes.com/sites/thomasbrewster/2017/05/03/massive-google-gmail-phish-many-victims/#219602e142a1

45 시스코의 추정
수치는 Google의 클라우드 기반 생산 툴을 유료로 사용하는 기업의 수("More than 3M businesses now pay for Google's G Suite," Frederic Lardinois, TechCrunch, 2017년 1월 26일: techcrunch.com/2017/01/26/more-than-3m-businesses-now-pay-for-googles-g-suite/ )와 현재 시스코의 CASB(Cloud Access Security Broker) 솔루션을 사용하고 과거에 Gmail 사용자를 노린 피싱 공격의 피해를 입었던 고객의 수(약 10%)를 근거로 함.

시스코의 조사에 따르면 최상위 권한을 지닌 사용자 중 약 85%는 월평균 한두 개의 IP 주소에서 로그인합니다. 따라서 평소와 다른 접속 패턴이 나타나면 조사해볼 필요가 있습니다.

또한 최상위 권한을 지닌 사용자 중 60%는 상시 로그인 상태를 유지하므로 다른 사용자가 무단으로 접속 권한을 획득한 후 발각되지 않은 채 활동하기가 한결 수월합니다(그림 55 참조). 사용자는 관리 작업을 수행해야 할 때만 로그인하고 작업을 마치면 즉시 로그아웃하는 습관을 일상화해야 합니다.

**그림 54.** 최상의 권한을 지닌 사용자 활동(특정 IP 주소를 사용한 월간 로그인 활동)




출처: Cisco Security Research

### 클라우드 보안에 대한 공동 책임 정책 시행

클라우드 활용 범위를 넓히려는 기업은 각자의 역할을 정확히 이해하여 클라우드 보안을 확립해야 합니다. 클라우드 서비스 제공업체는 물리적, 법적, 운영적 측면에서 자사가 판매하는 인프라 보안을 책임져야 합니다. 그러나 기본적인 클라우드 서비스를 이용하는 데 수반되는 보안에 대한 책임은 사용 기업의 몫입니다. 온프레미스 환경의 보안을 유지하는 데 추구하는 것과 동일한 모범 사례를 클라우드 시스템에도 적용하면 클라우드 시스템에 대한 무단 접속을 방지하는 데 많은 도움이 됩니다.

**그림 55.** 최상위 권한을 지닌 사용자 중 60%가 상시 로그인 상태 유지

출처: Cisco Security Research

## 기업을 위험에 빠뜨리는 인프라와 엔드포인트

오늘날의 개방형 네트워크로 인해 새로운 보안 공백과 위험이 발생하고 가시성이 감소하여 공격 영역이 넓어지기 쉽습니다. 클라우드는 이런 문제의 주요 원인입니다. 기업의 허가를 받지 않은 이른바 "섀도우 IT" 장치와 애플리케이션도 마찬가지입니다. 네트워크 및 자산 관리 솔루션의 통제 범위를 벗어난 네트워크와 엔드포인트 역시 기업이 제대로 파악하거나 관리할 수 없는 보안 공백을 유발합니다.

많은 기업이 엔터프라이즈 네트워크, 엔드포인트 및 클라우드 인프라에 존재하는 사각 지대의 (수와) 위험을 과소평가합니다. 사이버 상황 인식 기술을 제공하는 시스코 파트너인 Lumeta의 조사에 따르면 가시성이 부족하면 기업이 평균 20~40%의 네트워크 및 엔드포인트 인프라를 제대로 파악하거나 관리할 수 없습니다. 정부, 의료, 금융 서비스 및 IT를 비롯한 여러 분야의 기업들이 이와 같은 고민을 안고 있습니다.

기업의 관리 범위를 벗어난 네트워크 인프라와 엔드포인트가 존재할 경우 기업의 방화벽을 우회하려는 사이버 범죄자가 쉽게 공격할 수 있으며, 데이터를 빼내거나 또는 승인 받지 않은 Tor 트래픽을 전송하는 데 악용되거나 봇넷으로 사용될 수 있습니다. 심지어 단순한 라우터, 네트워크 방화벽 또는 새그먼트 구성 오류도 사이버 범죄자가 인프라에 침입하여 중요한 데이터에 접근할 수 있는 기회로 작용하기도 합니다.

기업이 가시성을 유지하려면 실시간 상황 중심 보안 정보를 확보할 수 있어야 합니다. 실시간 모니터링 및 유출 경로 탐지를 지원하는 솔루션을 설치하지 않으면 사이버 범죄자가 발각되거나 저지당하지 않은 채 마음껏 네트워크를 누빌 수 있습니다. 또한 기업은 자사의 세그먼트 정책을 검토하고 정책의 효과를 테스트할 수 있는 강력한 툴을 도입해야 합니다.

뿐만 아니라 기업은 어떤 장치와 시스템이 네트워크에 연결되는지 파악할 수 있어야 합니다. 보안 팀이 간단한 정보나 오래된 관리 대상 장치 목록만 확인할 수 있는 경우, 실제로 네트워크에 연결된 하드웨어 중 20% 이상이 보안 팀의 관리 범위를 벗어나게 됩니다. 엔터프라이즈 네트워크, 엔드포인트 및 클라우드 인프라가 지속적으로 바뀌고 보안 담당자만으로는 효과적으로 모니터링하기 어려우므로 인프라와 엔드포인트를 정기적으로 자동으로 조사할 수 있어야 합니다.

# 보안 팀의
# 과제와 기회

# 보안 팀의 과제와 기회

이번 섹션에서는 시스코의 최근 보안 역량 벤치마크 연구에서 추가로 밝혀진 각 산업의 조사 결과를 일련의 사례 연구에 중점을 두고 살펴봅니다. 그리고 기업이 구매하는 보안 솔루션 제공업체의 수를 줄임으로써 보안을 개선하는 방안을 제시하고 회사 규모가 보안에 어떤 영향을 미칠 수 있는지 논의합니다. 마지막으로, 보안 책임자가 사이버 보안에 대한 논의에서 기업 경연진을 설득하고 "리더십"을 발휘할 방법도 탐구합니다.

## 보안 역량 벤치마크 연구: 업종별 분석

시스코는 2017년 연구 결과를 토대로 업종별 조사를 했습니다.[46] 조사 결과는 고객 데이터 보호, 규제로 인한 제약에 대응, 최신 네트워크 기반 시스템을 기존 소프트웨어와 통합 등의 주요 과제 결과와 직결됩니다.

각 산업이 저마다 독특한 보안 과제에 직면해 있으며 보안 체제의 완성도는 산업마다 다르지만 모든 산업의 공통적인 관심사가 있습니다. 모든 업계의 보안 전문가들은 날로 정교해지는 공격 수법과 사이버 범죄자보다 한발 앞서갈 필요성을 인지하고 있습니다. 많은 기업은 데이터 유출 사실이 대중에 알려지면 (고객 이탈 같은) 피해를 줄이고 유사한 보안 사고를 예방하는 일을 최우선 과제로 삼습니다.

기업들은 정보 기술(IT)과 운영 기술(OT)을 통합하고, 특히 통합 시스템을 보호하는 데 전력을 기울여야 합니다. 최근 WannaCry 랜섬웨어 공격으로 유럽에 위치한 Renault-Nissan 자동차 공장의 가동이 중단됐는데, 이는 커넥티드 시스템(Connected System)이 보안 공격으로 어떤 피해를 입을 수 있는지 극명히 드러난 사례입니다. 연결 상태가 안전하고 적절하게 유지되지 않으면 심지어 랜섬웨어의 무작위 공격에도 OT 시스템이 타격을 입을 수 있습니다.[47]

과거에 IT와 OT는 연동하지 않았고 담당 팀들도 각기 따로 작업했습니다. 요컨대, OT 인력은 장비와 공장을 관리한 반면, IT 인력은 업무용 애플리케이션을 관리했습니다. 오늘날에는 많은 OT 센서와 시스템이 비즈니스 차원에서 사용되고 있습니다. 예를 들어, 제조 실행 시스템(MES)은 센서의 원격 측정 정보를 확보하여 작업을 최적화하고 더욱 정확하게 예측하는 데 사용합니다.

커넥티드 시스템이 OT 세계에 도입되면서 IT와 OT의 경계가 무너졌습니다. 이제는 커넥티드 시스템은 분석용 데이터를 공유함으로써 안전과 제품 품질을 개선하는 데 일조할 수 있습니다. 또한 커넥티드 시스템은 서로 연동하여 사이버 보안 위협을 억제할 수 있습니다. 그러나 이를 위해서는 멀티레이어 방어 능력을 개발해야 합니다. 단절된 폐쇄형 시스템은 IT와 OT를 포괄적으로 모니터링할 수 없기 때문입니다.

> IT와 OT 통합에 대한 자세한 내용은 시스코의 백서 "IT/OT 통합: 디지털 제조 방식으로 진화(IT/OT Convergence: Moving Digital Manufacturing Forward)"를 참조하십시오.

46 Cisco 2017 연례 사이버보안 보고서, 49페이지: b2me.cisco.com/en-us-annual-cybersecurity-report-2017?keycode1=001464153

47 "Renault-Nissan Is Resuming Production After a Global Cyberattack Caused Stoppages at 5 Plants," Laurence Frost/Naomi Tajitsu, BusinessInsider.com, 2017년 5월 15일: businessinsider.com/renault-nissan-production-halt-wannacry-ransomeware-attack-2017-5

## 회사 규모에 따라 달라져야 하는 보안 전략

사이버 범죄자의 네트워크 침입으로 정보가 유출된 경우, 중소기업은 대기업보다 피해 복구에 더 큰 어려움을 겪습니다. 데이터 유출 소식이 대중에 공개되는 바람에 평판이 하락하고 고객이 경쟁사로 넘어간 경우, 중소기업은 대기업에 비해 그로 인한 타격을 감당하기가 더 어렵습니다. 중소기업 역시 위협과 데이터 유출로 인한 피해를 최소화하는 보안 프로세스와 툴을 갖춤으로써 입지를 강화할 필요가 있습니다.

2017년 보안 역량 벤치마크 조사 결과를 검토해보면 (250~499명의 직원을 둔 기업으로 규정된) 중소기업은 대기업에 비해 보안 대책이 미흡한 실정입니다. 중소기업은 근본적으로 더 적은 자원과 부족한 전문 인력으로 조직을 보호해야 하기 때문에 사이버 공격에 상대적으로 더 취약할 수밖에 없습니다. 자신들에게 중대한 보안 위협 요소를 묻는 질문에 10,000명 이상의 직원을 둔 기업 중 21%가 랜섬웨어라고 답한 데 반해, 랜섬웨어를 손꼽은 중소기업은 29%였습니다. 또한 규제 준수의 제약을 중대 위험 요소로 생각하는 중소기업은 30%에 달하는 것과 대조적으로, 대기업은 20%에 불과했습니다(그림 56 참조).

**그림 56.** 기업 규모별 위험 요소 인식

| 위험: 귀사의 보안을 위협하는 중대 위험 요소는 다음 중 무엇이라고 생각하십니까? | 기업 규모 비율 | | | |
|---|---|---|---|---|
| | 250~499 | 500~999 | 1000~9999 | 10,000+ |
| BYOD 및 스마트 기기 보편화 | 29 | 28 | 29 | 25 |
| 재해 복구 및 비즈니스 연속성 실행 능력 | 28 | 25 | 26 | 21 |
| 규제 준수 제약 | 30 | 25 | 24 | 20 |
| APT(Advanced Persistent Threat) | 34 | 33 | 34 | 30 |
| 랜섬웨어 | 29 | 25 | 25 | 21 |

출처: 2017년 시스코 보안 역량 벤치마크 연구

더 적은 예산과 전문 인력 때문에 핵심 보안 인프라를 구축할 여유가 있는 중소기업도 상대적으로 더 적습니다. 예를 들어, 이메일 보안을 사용하는 대기업은 45%인데 반해 중소기업은 34%(그림 57 참조)에 불과하고, 대기업 중 52%가 데이터 유출 방지 솔루션을 사용하는 반면 중소기업은 40%(그림 57 참조)만이 데이터 유출 방지 솔루션을 사용하고 있는 것으로 확인됐습니다.

**그림 57.** 기업 규모별 핵심 보안 인프라 구축 여부

| 복잡성: 귀사가 사용 중인 위협 차단용 보안 솔루션은 다음 중 무엇입니까? | 기업 규모 비율 | | | |
|---|---|---|---|---|
| | 250~499 | 500~999 | 1000~9999 | 10,000+ |
| 데이터 유출 방지 | 40 | 43 | 47 | 52 |
| DDoS 방어 | 33 | 35 | 42 | 39 |
| 이메일/메시징 보안 | 34 | 41 | 45 | 45 |
| 암호화/개인정보/데이터 보호 | 39 | 38 | 49 | 52 |
| 엔드포인트 보호/바이러스 및 악성 프로그램 차단 | 36 | 37 | 45 | 45 |
| 패치 및 구성 | 26 | 28 | 32 | 35 |
| 웹 보안 | 37 | 39 | 44 | 45 |
| 무선 통신 보안 | 32 | 35 | 40 | 42 |

출처: 2017년 시스코 보안 역량 벤치마크 연구

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

보안 전략을 명문화해서 시행하는 대기업이 중소기업에 비해 많고(66% 대 59%), 협력업체에 ISO 27018 인증을 요구하는 대기업도 중소기업보다 많습니다(36% 대 30%).

보안 능력을 강화하려는 중소기업은 보안 정책 및 절차를 개선하고 일반적인 위협 방어 체제를 보다 광범위하게 적용하여 공격으로 인한 악영향을 최소화하는 데 주력할 수 있습니다. 타사의 보안 서비스를 이용하면 모범 사례를 확립하는 데 효과적인 공식적 보안 전략을 구현함과 동시에, 직원의 전문적인 모니터링 및 사고 대응 능력을 강화하는데 필요한 노하우를 제공 받을 수 있습니다.

비즈니스 요건과 예산에 부합하는 보안 인프라를 도입하려면 보안 팀이 통합을 통해 관리하기 용이하면서도 효과적인 수준으로 보안 환경을 간소화할 수 있는 솔루션을 물색해야 합니다. 또한 성장 중인 기업은 NIST 사이버 보안 프레임워크 같은 표준을 준수하여 보안을 강화할 수 있습니다. 기업의 규모에 관계없이 보다 거시적인 보안 전략을 추구하는 기업은 진화하는 위협에 보다 효과적으로 대응할 수 있습니다.

## 서비스의 이용을 통한 전문 지식 및 인력 부족 문제의 완화

보안 팀 내부에서는 동급 최강의 솔루션과 통합 아키텍처 중 어떤 방어 체제가 최선인가를 놓고 논란이 끊이지 않습니다. 그러나 보안 팀은 모든 보안 결정에 영향을 미치는 또 다른 어려움이 있다고 호소합니다. 다름아닌 보안 전문성이 부족하다는 점입니다. 나날이 공격 수법이 발전하고 기업에서 사용되는 기술 또한 다양해지고 있기 때문에 기업은 보안 서비스에 대한 의존도를 높여서 인재 부족 문제를 해소해야 합니다.

적합한 인재를 확보해서 유지하는 데 얼마나 공을 들이느냐에 따라 보안 팀의 성과가 달라질 수 있습니다. 시스코의 보안 역량 벤치마크 연구에 따르면 많은 산업 분야에서 숙련된 인력이 부족한 탓에 향상된 보안 프로세스 및 기술을 도입하는 데 어려움을 겪습니다. 사실, 인재 부족은 전 세계 국가의 공통된 고민입니다. 거듭 강조하지만 타사의 보안 서비스로 인재 부족 문제를 완화할 수 있습니다.

시스코의 보안 서비스 전문가에 따르면 보안 동향에 대한 정보가 방어 체제에 반영되지 않는 경우가 종종 있습니다. 노련한 보안 전문가의 전문성은 제품, 심지어 최고의 자동화 솔루션조차 지원하지 못하는 수준의 분석력을 발휘합니다.

사내 보안 팀에게 "알림 피로"는 고질적인 문제입니다. 2017년 보안 역량 벤치마크 연구 보고서에서 업종별로 다룬 다수의 글에서 이미 언급했듯, 조사할 시간이 턱없이 부족할 정도로 많은 알림이 발생되기 때문에 보안 인력이 심각한 위협을 놓치기 십상입니다. 사소한 알림이 자주 발생되는 경우, 알림 처리 프로세스를 자동화하면 부족한 인력이나 기술 때문에 제대로 활용하지 못했던 기회가 발생할 수 있습니다. 가급적 많은 수의 사소한 알림을 자동으로 처리하는 시스템을 구축한 기업은 더 큰 영향을 미칠지도 모를 보다 중요한 문제에 집중할 수 있습니다.

알림 피로의 원인은 다양합니다. 서로 단절된 시스템 때문에 알림이 중복으로 발생되기도 하고, 보안 팀이 사소한 알림과 심각한 알림을 구분하거나 잘못된 알림을 구별할만한 지식이 없는 경우도 있습니다. 잠재적 위협의 근원을 파악하는 데 필요한 툴이 부족한 탓에 알림 피로가 누적될 수도 있습니다. 외부 서비스 팀의 독창적인 사고 능력이야말로 이러한 "피로"를 떨쳐버리고 대응해야 할 위협에 관한 조언을 얻기에 더없이 적합합니다.

제품에 대한 지식 부족으로 보안 팀이 새로 구매한 솔루션을 제대로 활용하지 못하는 경우도 있습니다. 종종 보안 솔루션은 보안 전문가가 아니라 해당 솔루션 전문가에 의해 구현됩니다. 그와 같은 경우, 보안 팀이 제품을 통합하여 위협에 대한 총체적 가시성, 다시 말해서 보안 효과를 정확히 파악할 수 있는 "단일 인터페이스"를 확보하는 방법을 이해하기 어렵습니다. 또한 타사의 숙련된 보안 팀은 기업의 보안 전문가가 클라우드 솔루션을 관리하고 데이터 보호 방법을 이해하는 데 필요한 도움을 줄 수 있습니다. 클라우드 제공업체가 2단계 인증 같은 보안 체제를 적용하지 않는 경우가 있는데, 이때도 기업은 전문가의 도움을 받아 SLA와 계약 약관을 검토하여 해당 클라우드 공급업체가 사용하는 방어 수단을 확인할 수 있습니다.

## 국가별 타사 서비스 이용률과 보안 알림 데이터 처리

국가별 타사 서비스 이용 실태를 조사한 결과, 일부 국가에서는 타사의 서비스에 의존하는 중소기업이 대기업보다 많은 것으로 확인됐습니다. 예를 들어, 호주에서 타사의 사고 대응 서비스를 이용하는 대기업은 41%인 데 반해, 중소기업은 65%에 달합니다. 일본의 경우 타사의 모니터링 서비스에 의존하는 중소기업은 54%로, 41%인 대기업과 상당한 격차가 있습니다(그림 58 참조).

알림 발생 시 조사에 착수하는 기업을 지역 및 회사 규모에 따라 조사한 결과, 인도, 브라질, 미국의 중소기업이 가장 높은 비율을 보였습니다. 그리고 알림 발생 시 실제로 치료까지 완료하는 중소기업의 비율은 중국, 러시아, 영국이 가장 높은 것으로 확인됐습니다.

**그림 58.** 타사의 서비스를 이용하는 각국의 중소기업 및 대기업 비율

| 보안과 관련해서 (해당되는 경우) 다음 중 어떤 유형의 서비스를 타사에 의뢰해서 이용하고 있습니까? | 미국 | | 브라질 | | 덴마크 | | 이탈리아 | | 영국 | | 호주 | | 중국 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 컨설팅 | 49 | 47 | 40 | 44 | 41 | 47 | 45 | 44 | 43 | 51 | 63 | 52 | 50 | 57 |
| 감사 | 51 | 48 | 48 | 56 | 45 | 49 | 40 | 44 | 49 | 48 | 39 | 30 | 28 | 44 |
| 사고 대응 | 43 | 46 | 43 | 32 | 45 | 41 | 61 | 42 | 45 | 40 | 65 | 41 | 32 | 42 |
| 모니터링 | 54 | 44 | 44 | 38 | 38 | 41 | 50 | 39 | 46 | 41 | 47 | 36 | 33 | 35 |
| 치료 | 34 | 34 | 26 | 21 | 45 | 42 | 32 | 23 | 30 | 34 | 38 | 28 | 46 | 47 |
| 위협 정보 분석 | 43 | 40 | 33 | 37 | 38 | 40 | 44 | 36 | 29 | 42 | 54 | 34 | 28 | 42 |
| 해당 항목 없음 | 14 | 15 | 7 | 13 | 6 | 15 | 2 | 10 | 11 | 20 | 5 | 14 | 20 | 12 |
| | 49 | 47 | 40 | 44 | 41 | 47 | 45 | 44 | 43 | 51 | 63 | 52 | 50 | 57 |
| | **인도** | | **일본** | | **멕시코** | | **러시아** | | **프랑스** | | **캐나다** | | | |
| 컨설팅 | 56 | 62 | 60 | 59 | 58 | 63 | 46 | 50 | 52 | 51 | 48 | 50 | | |
| 감사 | 43 | 50 | 35 | 25 | 57 | 64 | 37 | 43 | 44 | 56 | 44 | 50 | | |
| 사고 대응 | 53 | 55 | 69 | 55 | 39 | 41 | 37 | 35 | 54 | 42 | 49 | 45 | | |
| 모니터링 | 42 | 51 | 54 | 41 | 44 | 46 | 34 | 44 | 51 | 57 | 49 | 50 | | |
| 치료 | 44 | 43 | 40 | 28 | 12 | 24 | 31 | 50 | 34 | 35 | 36 | 45 | | |
| 위협 정보 분석 | 50 | 60 | 41 | 31 | 36 | 38 | 39 | 39 | 43 | 45 | 45 | 42 | | |
| 해당 항목 없음 | 6 | 5 | 1 | 6 | 5 | 5 | 6 | 7 | 2 | 5 | 10 | 11 | | |

**그림 59.** 국가별 알림 관련 통계

| | 미국 | | 브라질 | | 덴마크 | | 이탈리아 | | 영국 | | 호주 | | 중국 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 알림 발생 시 조사에 착수하는 비율은 얼마나 됩니까? | 59.7 | 62.8 | 61 | 65.5 | 44.4 | 52 | 45.8 | 61.3 | 47.4 | 44.2 | 55.6 | 60.8 | 44.8 | 42.5 |
| 조사한 알림 중 실제 사고는 몇 %입니까? | 30.6 | 25.7 | 27.1 | 26.2 | 20.2 | 28.2 | 22.8 | 15.2 | 26.3 | 23 | 27.2 | 28.6 | 30.6 | 44.5 |
| 실제 사고 중 치료를 완료하는 비율은 얼마나 됩니까? | 40.9 | 45.3 | 35.4 | 46.3 | 43.7 | 50.4 | 34.8 | 40.9 | 47.3 | 45.6 | 40.6 | 46.2 | 53.5 | 67.9 |
| | **인도** | | **일본** | | **멕시코** | | **러시아** | | **프랑스** | | **캐나다** | | | |
| 알림 발생 시 조사에 착수하는 비율은 얼마나 됩니까? | 60.5 | 65.1 | 50.6 | 58.1 | 59.1 | 60.6 | 59.3 | 65.9 | 49.1 | 51.3 | 49.3 | 48.8 | | |
| 조사한 알림 중 실제 사고는 몇 %입니까? | 37.1 | 39.7 | 25.4 | 33.8 | 27.8 | 20.5 | 23.4 | 33.2 | 21.8 | 25.5 | 22.2 | 23.8 | | |
| 실제 사고 중 치료를 완료하는 비율은 얼마나 됩니까? | 45.8 | 48.3 | 44.3 | 38.4 | 43.8 | 48.6 | 47.3 | 60.5 | 41.6 | 52.4 | 35.8 | 37.6 | | |

**기업 규모** 중소기업(직원 수 299~500명) 대기업(직원 수 1,000명 이상)

출처: 2017년 시스코 보안 역량 벤치마크 연구

## IoT 보안 위험: 현재와 미래에 대비

시스코가 정의한 IoT(Internet of Things)란 데이터를 수집하고 교환할 수 있는 전자 부품, 소프트웨어, 센서, 액추에이터 및 네트워크 통신 기능이 내장된 전자 기기, 전자 장치 및 기타 장치가 내장 된 실제 장비, 차량, 건물, ("커넥티드 디바이스" 및 "스마트 장치"로도 불리는) 기타 사물이 서로 연결된 네트워크입니다. 시스코의 이론에서 IoT는 정보 기술(IT), 운영 기술(OT) 및 소비자 기술(CT)이란 세 가지 핵심 요소로 구성되어 있습니다.

한편, 산업용 사물 인터넷(IIoT)은 기업 IT 네트워크나 데이터센터와 달리, 산업용 제어 네트워크 내의 연결된 장치들을 지칭하는 용어입니다.

IoT는 비즈니스 협업 및 혁신의 밝은 미래를 보장합니다. 하지만 IoT가 비대해지면서 기업과 사용자의 보안 위험도 커지고 있습니다.

가시성 부족을 문제의 원인으로 손꼽을 수 있습니다. 대부분의 보안 팀은 네트워크에 연결되는 IoT 장치를 제대로 파악하지 못합니다. 카메라부터 온도 조절기와 스마트 미터에 이르기까지 각종 IoT 장치는 일반적으로 보안을 염두에 두고 설계되지 않습니다. 이러한 장치 중 상당수는 보안이 데스크톱의 보안 기능에 훨씬 못 미치는 수준이며 해결하는 데 몇 달 또는 심지어 몇 년이 걸릴 수 있는 취약점 문제를 안고 있습니다. IoT 장치는 일반적으로 다음과 같은 특징을 보입니다.

- CVE 보고 또는 업데이트 기능을 거의 또는 전혀 갖추고 있지 않습니다.
- 특수 아키텍처에서 실행됩니다.
- Windows XP처럼 패치 또는 업데이트 서비스가 중단되어 공격에 취약한 애플리케이션을 사용합니다.
- 패치가 거의 이뤄지지 않습니다.

또한 IoT 장치는 소유자가 액세스하기 어렵거나 아예 액세스할 수 없으므로 악성 프로그램에 감염되더라도 치료하기 어렵거나 불가능합니다. 요컨대, IoT 장치는 사이버 범죄자가 거점으로 삼기에 안성맞춤입니다(이와 같은 상황의 예는 **42페이지**의 "인질로 잡히는 의료 기기: 실제 사건" 참조).

보안 팀이 IoT 장치에서 발생한 알림의 성격을 이해하기 어려운 현실 때문에 IoT 장치의 보안 문제가 가중됩니다. 또한 IoT 장치의 보안 사고를 책임져야 할 사람이 불분명한 경우도 있습니다. 기업으로부터 요청을 받은 IoT 장치 제조업체의 팀은 구현 작업만 책임지기 때문에 기업이 직접 프로젝트를 마무리해야 합니다.

사이버 범죄자가 랜섬웨어 공격을 감행하고, 민감한 정보를 빼내며, 네트워크에서 은밀히 이동할 목적으로 IoT 취약점을 집중 공격하기 마련이므로 보안 팀은 잠재적인 IoT 취약점에 관심을 기울여야 합니다. IoT 장치는 사이버 범죄자가 쉽게 악용할 수 있는 취약점을 지닌 "낮은 가지에 달린 열매"인 셈입니다.

거시적으로 봤을 때 이러한 장치가 대대적으로 공격 받을 경우 기업과 정부, 그리고 인터넷 자체가 심각한 혼란에 빠질 가능성도 있습니다. IoT 장치를 노린 DDoS 공격은 이미 발생한 전례가 있으며, IoT 봇넷(**39페이지** 참조)의 등장으로 사이버 범죄자가 전례 없는 규모의 공격을 개시할 준비도 진행되고 있는 것으로 짐작됩니다.

급격히 성장하고 모니터링 및 관리가 점점 어려워지는 공격 영역인 IoT의 보안 문제를 해결하려면 보안 팀이 다음과 같은 작업을 수행해야 합니다.

- 오래된 서명 계속 사용
- IPS 방어 체제로 IoT 장치 보호
- 네트워크 트래픽 면밀히 모니터링(네트워크 트래픽 패턴을 쉽게 예측할 수 있는 IoT 환경에서 특히 중요합니다.)
- IoT 장치가 네트워크에 접속하고 다른 장치와 통신하는 방법 추적(예를 들어, IoT 장치를 할 경우 사이버 공격이 시작되는 불길한 징후일 가능성이 높습니다.)
- 적시에 패치 실시
- 기본적인 제품 보안을 지원하고 보안 권고안을 제시하는 제품 제조업체와 공조

IoT 장치를 감염 또는 공격으로부터 보호하거나 불가피하게 일부 IoT 장치가 사이버 범죄자에게 공격 당한 경우라도 그로 인한 영향을 최소화하려면 예방 중심의 탄력적인 보안 정책과 다단계 방어 전략이 필수적입니다.

## 보안 역량 벤치마크 연구: 업종별 분석

### 서비스 제공업체

#### 산업의 핵심 과제

시스코의 조사에 의하면 서비스 제공업체 시장은 통신, 클라우드/웹 기반 인프라 및 호스팅, 미디어 회사, SaaS(Software-as-a-Service) 모델로 제공되는 애플리케이션 등 다양하게 구성된 산업입니다. 또한 서비스 제공업체는 관리형 보안 서비스를 상품으로 판매하기도 합니다. 조사 대상 서비스 제공업체 중 71%는 고객에게 관리형 보안 서비스를 제공하고 있다고 답했습니다.

서비스 제공업체는 IT 및 프러덕션 인프라와 고객 데이터 보호를 비롯한 수많은 과제를 안고 있습니다. 서비스 제공업체의 보안 전문가 중 59%는 자사의 데이터센터나 핵심 프러덕션 네트워크 보호가 최우선 과제라고 답했습니다.

하지만 이러한 과제는 서비스 제공업체의 비즈니스 규모 때문에 상황이 더욱 어려워 지고 있습니다. 보안 전문가들은 회사의 규모가 커지고 위협에 노출되는 범위가 넓어지면 사이버 범죄자가 핵심 비즈니스(고객에게 서비스 제공)를 공격할 가능성도 커진다고 우려합니다. 고객 이탈률이 높은 산업에서 고객 정보 유출 사고는 매출에 타격을 입힐 수 있습니다. 실제로, 34%의 서비스 제공업체가 지난 해 보안 사고로 인해 수익 손실을 입었다고 밝혔습니다.

많은 서비스 제공업체의 핵심 과제는 보안 툴과 프로세스를 통합하여 그 효과를 극대화할 방법을 강구하는 한편, 현재 운영 중인 서비스와 툴이 무분별하게 확산되는 현상을 억제하는 것입니다.

관리형 서비스 제품으로 판매하지 않는 한, 보안은 수익의 중심점이 아닌 비용 발생의 원천이 되기 십상이므로 비대해지는 것을 경계해야 하지만, 거세진 경쟁과 위협 상황 때문에 어쩔 수 없이 보안에 더욱 치중할 수밖에 없는 것이 서비스 제공업체의 경제적 현실입니다.

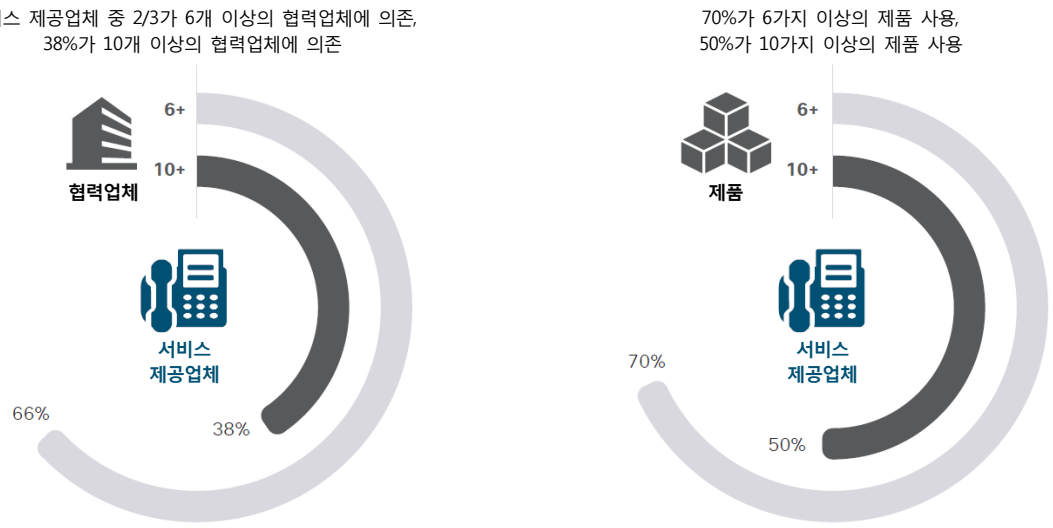
#### 어려움을 가중시키는 서비스 제공업체 규모

모든 산업이 난립하는 보안 서비스 제공업체와 툴때문에 골머리를 앓고 있습니다. 그러한 난립으로 솔루션이 통합되지 않고 실효성 있는 위협 정보를 제공하지 못할 때가 많기 때문입니다. 서비스 제공업체 시장에서는 시장 규모로 인해 이런 문제가 심화되고 있습니다. 서비스 제공업체의 보안 전문가 중 2/3는 자신들이 6개 이상의 협력업체에 의존하고 있다고 답했습니다. 더욱이 10개 이상의 협력업체에 의존한다고 답한 보안 전문가가 38%에 달합니다(그림 60 참조).

사용 중인 제품의 수에 대해 묻는 질문에 70%는 적어도 6가지의 보안 제품을 사용하고 50%는 10가지 이상의 제품을 사용한다고 답했습니다. 이 시장에 대한 시스코의 전문가에 따르면 제품이 제대로 통합되지 않아서 단계적으로 보안을 강화할 때마다 복잡성은 기하급수적으로 심화되는 경우가 많습니다.

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

**그림 60.** 6개 이상의 협력업체 솔루션과 제품을 사용하는 서비스 제공업체 비율




출처: 2017년 시스코 보안 역량 벤치마크 연구

### 보안 사고 이후 고객 이탈률 상승

서비스 제공업체 중 절반 이상(57%)이 데이터 유출 사고 때문에 공개 조사를 받은 적이 있다고 답했습니다. 개인정보 유출 사고를 겪은 서비스 제공업체 중 거의 절반이 유출 사고를 계기로 보안을 대폭 강화했다고 밝혔으며, 90%는 유출 사고 이후 보안 체제를 조금이라도 개선한 것으로 조사됐습니다. 이 조사 결과로 미루어 봤을 때, 서비스 제공업체의 보안 전문가들은 유출 사고를 통해 얻은 교훈을 서둘러 보안 체제에 반영하는 것으로 보입니다.

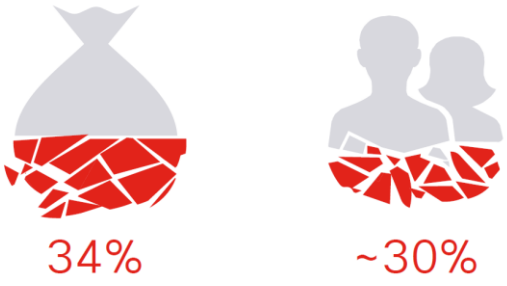
지난 해 서비스 제공업체 중 34%가 사이버 공격으로 인해 수익에 타격을 입었고, 약 30%는 사이버 공격 때문에 고객이나 비즈니스 기회를 잃은 것으로 나타났습니다(그림 61 참조). 서비스 제공업체들은 개인정보 유출 사고로 인해 가장 큰 타격을 입은 부분으로 비즈니스 운영, 브랜드 평판, 고객 유지를 손꼽았습니다.

규모가 크고 경쟁이 치열한 시장일수록 서비스 제공업체가 보안 사고로 인해 입을 수 있는 피해도 커집니다. 고객은 선택의 폭이 넓기 때문에 기존의 서비스 제공업체에게 자사의 데이터나 고객을 보호할 능력이 부족하다고 생각되면 즉시 다른 서비스 제공업체에게 발길을 돌립니다.

### 높은 표준 채택률

서비스 제공업체의 표준 채택률이 다른 산업에 비해 훨씬 높은 것으로 조사됐는데, 비즈니스의 범위와 규모를 관리할 수 있는 차이가 이와 같은 결과로 이어진 것으로 관측됩니다. 서비스 제공업체 중 약 2/3는 명문화된 공식 보안 전략을 갖춘 채 표준화된 정보 보안 정책을 추구하는 것으로 확인됐습니다. 또한 조사 대상의 거의 모든 서비스 제공업체는 이구동성으로 보안 프로세스 및 절차가 확립되어 있으며 그에 관한 직원들의 이해도 역시 높다고 답했습니다.

**그림 61.** 사이버 공격으로 인한 수익 손실




지난 해 서비스 제공업체 중 34%가 사이버 공격으로 인해 수익 손실 발생

약 30%가 사이버 공격 때문에 고객이나 비즈니스 기회 상실

출처: 2017년 시스코 보안 역량 벤치마크 연구

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

## 공공 부문

### 산업의 핵심 과제

여러 가지 제약 때문에 공기업은 보안 대책에 있어 사전 예방보다 사후 대응에 더 치중하는 경향이 있습니다. 한정된 예산, 인재 확보의 어려움, 위협에 대한 가시성 부족이 공공 부문의 네트워크 방어 능력에 영향을 미칩니다.

그러나 공공 부문은 일반적으로 민간 부문보다 더 엄격한 사이버 위험 관리 규정을 준수해야 합니다. 이를테면, 미국의 연방 기관은 연방 정보 보안 관리법(FISMA)에 따라 미션 크리티컬 정보 시스템의 기밀성과 무결성을 유지해야 합니다. 주 정부와 지방 정부 차원에서 유사한 규정도 마련되어 있습니다. 실제로, 제공하는 서비스에 따라 엄청나게 많은 새 규정과 오래된 규정이 주 정부 및 지방 정부 산하의 공기업에 적용됩니다.

또한 공기업은 규정의 영향을 받는 '클라우드로의 전환 프로세스'를 관리하기 위해 노력하고 있습니다. 연방 정부 차원에서 마련된 FedRAMP(Federal Risk and Authorization Management Program)는 클라우드 제품 및 서비스 사용에 관한 기준을 제시합니다. 또한 주 정부와 지방 정부는 정부 데이터를 보관하는 클라우드 서비스 제공업체에 인증을 요구합니다.

### 클라우드의 데이터 관리

일관적인 사이버 공격 방어 체제를 유지해야 하는 공기업 입장에서 클라우드로 이전하면 많은 효과를 거둘 수 있지만 그에 못지않게 다양한 문제도 해결해야 합니다. 공기업 중 1/3은 표적형 공격, APT 및 내부자의 데이터 유출을 중대 보안 위험으로 손꼽았습니다. 또한 공공 부문 보안 전문가들은 퍼블릭 클라우드 스토리지와 클라우드 인프라가 보호하기 가장 어려운 요소라고 답했습니다.

### APT(Advanced Persistent Threat)

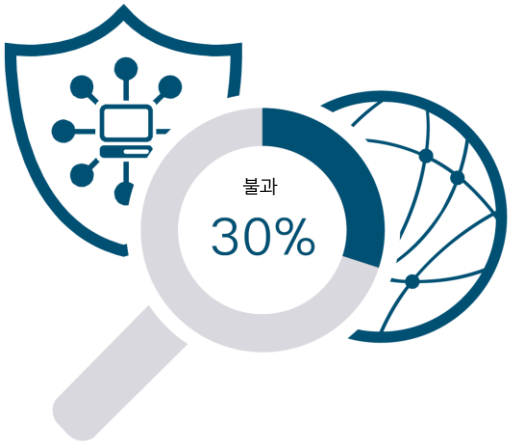
APT는 사이버 범죄자가 작전 시간을 벌 목적으로 감행하는 공격입니다. 이 공격 수법은 사이버 범죄자가 (일반적으로 데이터를 빼낼 의도로) 오랜 시간 동안 발각되지 않은 채 네트워크에 잠복할 수 있도록 설계되어 있습니다.

시스코의 공공 부문 보안 전문가에 따르면 클라우드 스토리지마다 각기 다른 데이터 보호 툴 세트를 지원하기 때문에 보안 팀이 데이터를 보호할 툴과 프로세스의 구성 방법을 재고할 수 밖에 없다는 데 문제가 있습니다. 예를 들어, NetFlow 분석 툴의 기능은 클라우드 서비스의 분석 툴에 정확하게 매핑되지 않으므로 프로세스와 결과가 동일하지 않습니다.

### 위협 분석의 걸림돌이 되는 예산 및 인재 부족

예산, 전문 인력 및 규정에 따른 제약도 공공 부문이 보안 목표를 달성하는 데 걸림돌로 작용합니다. 예를 들어, 공기업에서 툴을 설치하고 결과를 분석하기 위해서는 지식이 풍부한 직원이 필요하기 때문에 특정 툴을 도입하기가 여의치 않을 수 있습니다. 실제로, 공공 부문 보안 전문가 중 30%만이 침입테스트 및 엔드포인트 또는 네트워크 포렌식 툴을 사용한다고 밝혔습니다(그림 62 참조). 이러한 툴은 다양한 방어 보안 전략의 핵심 요소이므로 도입하지 않을 경우 보안이 우려될 수밖에 없습니다. 보안에 이런 서비스를 활용하지 않는 기업에서는 네트워크 침입 사고가 거듭해서 발생할 수 있습니다.

**그림 62.** 다양한 방어 솔루션을 사용하는 공기업 비율




30% 정도만이 침입 테스트 및 엔드포인트 또는 네트워크 포렌식 툴 사용

출처: 2017년 시스코 보안 역량 벤치마크 연구

또한 충분한 수의 보안 전문가를 확보하지 못한 공기업은 위협을 제대로 조사하기 어려울 수 있습니다. 공기업 중 거의 40%가 하루 평균 수천 건의 알림이 발생되는데 그 중 조사하는 알림은 65%에 불과하다고 답했습니다. 그리고 조사한 알림 중 32%가 실제 보안 사고로 판명되지만 그 중 치료까지 완료되는 사고는 47%에 그치는 것으로 조사됐습니다.

조사하지 않은 채 지나치는 알림 건수만 봐도 알림 관련 정보 공유 및 분석 기능을 지원하는 툴이 필요하다는 사실을 알 수 있습니다. 이런 툴은 경고에 대한 성격과 구체적인 정보(즉, 보다 의미 있는 정보)를 제공하므로 담당 인력이 어떤 알림에 즉각적인 관심이 필요한지 판단하기 용이합니다. 한편, 자동화는 일부 위협을 해소하므로 보안 팀의 부담을 줄이는 데 도움이 되기도 합니다.

시스코의 보안 전문가에 따르면 공기업에서 일상적으로 발생되는 다수의 알림을 제대로 조사하려면 경우에 따라 수십 명의 보안 인력이 필요하지만 그만큼의 인력을 보유한 공기업은 찾아보기 힘듭니다. 공기업 중 35%는 보안 전담 인력이 30명 미만이라고 답했습니다. 또한 27%는 숙련된 인력 부족이 향상된 보안 프로세스 및 기술을 도입하는 데 중대한 장애 요인으로 작용한다고 밝혔습니다. 자동화 툴이 일상적으로 발생되는 보안 알림을 처리할 수 있는 보안 방어 시스템을 반드시 구축해야 하는 또 다른 이유입니다.

**유출 사고를 계기로 한 보안 강화**

인력 및 검증된 보안 툴의 부족 현상이 공공 부문의 보안에 영향을 미칩니다. 공기업 중 53%가 데이터 유출 사고 때문에 공개 조사를 받은 적이 있다고 답했습니다. 지금까지 사고를 겪지 않은 기업도 운이 좋아서 피해를 입지 않았을 뿐 언제든 사고가 발생할 수 있다는 생각을 가져야 합니다. 사고가 발생할 경우 재빨리 대응하면 그만이라는 안일한 자세를 지양하고 예방 중심의 포괄적 보안 전략을 추구해야 합니다. 사고가 발생할 때마다 임시방편으로 대응하다 보면 너무나도 많은 자원이 소모되기 때문에 거시적인 계획을 세우는 데 필요한 자원이 턱없이 부족해집니다.

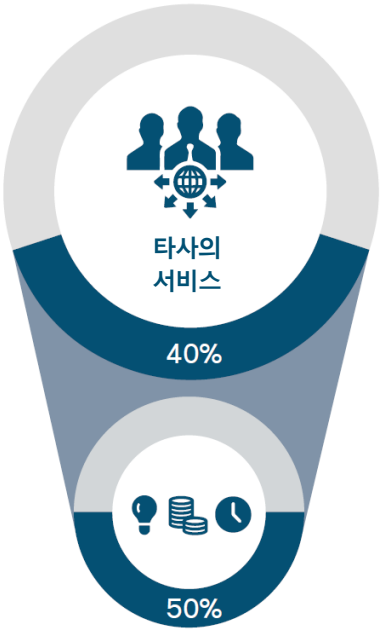
공기업의 보안 팀은 보안 사고가 발생하면 이를 교훈으로 삼는 것으로 조사됐습니다. 46%는 데이터 유출 사고를 계기로 보안이 크게 개선됐다고 답했습니다. 그러나 기업은 위험을 최소화하고 보안 시스템을 보다 효과적으로 관리할 수 있도록 보안 사고를 미연에 방지하기 적합한 기술에 투자하는 일도 게을리하지 말아야 합니다.

**효율적이지만 자체적인 노하우 축적에는 도움이 되지 않는 외주**

더 많은 자원을 확보하려는 공기업이 주로 택하는 전략은 외주입니다. 40% 이상의 공기업이 모니터링이나 감사 같은 타사의 서비스에 완전히 또는 부분적으로나마 의존한다고 답했습니다. 절반 가량의 공기업이 타사의 보안 서비스에 의존하는 가장 큰 이유로 편견 없는 통찰력, 경제성, 적시의 사고 대응을 손꼽았습니다(그림 62 참조).

침해 테스트 및 기타 감사는 외부 조직에 맡겨도 되지만 타사의 서비스에 전적으로 의존할 경우 단점도 있습니다. 그렇게 될 경우 공공 서비스 기관은 세월이 흘러도 자체적으로 노하우를 축적할 수 없습니다. 이런 노하우는 정교한 공격으로부터 네트워크를 방어하는 데 중요합니다. 자동화된 솔루션은 경제적으로 적시에 대응할 수 있다는 장점이 있지만, 매우 중요한 통찰력과 분석력을 확보하려면 외부 인력과 사내 전문가가 균형을 이뤄야 합니다.

**그림 63.** 큰 비중을 차지하는 타사의 서비스




**편견 없는 통찰력, 경제성, 적시의 사고 대응**

출처: 2017년 시스코 보안 역량 벤치마크 연구

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

## 소매업

### 업종별 핵심 과제

소매업에서 보안 사고가 발생하면 뉴스가 순식간 대대적으로 보도됩니다. 소매업체를 노린 공격은 고객의 금융 정보나 기타 개인 정보가 유출되는 경우가 빈번하기 때문에 언론의 주목을 받고 소비자까지 피해를 입습니다. 소매업에서 발생한 보안 사고 및 데이터 유출 사고는 의료 또는 공익사업 같은 다른 산업보다 훨씬 더 실질적으로 브랜드 평판에 영향을 미칩니다. 고객에게 주어지는 선택의 폭이 넓기 때문에 소매업체가 보안을 소홀히 한다고 여겨지면 고객은 주저 없이 등을 돌립니다.

고객 신용카드 데이터를 빼낼 목적으로 악성 프로그램을 동원하는 등 유수의 소매업체를 노린 공격이 세간의 주목을 받자 보안 전문가들은 자신의 기업들도 같은 상황에 처하지 않을까 노심초사합니다. 그렇다고 해서 소매업체들이 투철한 보안 의식을 갖고 있다고 생각하기는 어렵습니다. 소매업체 경영진은 단순히 자사의 방화벽 안에서 신용카드 데이터를 보호하면 정보가 안전하다고 믿고 있을지도 모릅니다. 그러나 암호화되지 않은 데이터를 은행이나 다른 협력업체에 전송하는 경우 유통 업체의 네트워크 보호 체제는 무용지물이나 다름없습니다.

### 미흡한 안전 의식

보안 사고가 연일 언론에 다뤄지는 현실이 무색하게도 소매업체는 보안에 대해 다소 안일한 입장을 보입니다. 예를 들어, PCI를 철저히 준수해야 한다는 데 전적으로 동의하는 소매업의 보안 전문가는 61%에 그치고, 고객의 기밀 데이터를 유효기간 내내 보호해야 한다는 입장에 전적으로 동의하는 보안 전문가 역시 63%에 불과합니다.

(특히 기술 도입이 더딘 미국에서) 데이터 보호에 주력하려는 소매업체는 신용카드 및 직불카드로 결제하는 고객을 위해 칩 앤 핀(Chip-and-PIN) 기술을 전면 도입해야 합니다. 은행과 신용카드 기업이 칩 앤 핀 시스템으로 이뤄진 구매에 한하여 사기 피해 보상을 보장하기 때문에 소매업체는 이 결제 기술을 도입해야 합니다. 그렇지 않을 경우 소매업체가 피해액을 책임져야 합니다.[48]

### 가장 심각한 보안 위험 - 표적형 공격과 내부자의 데이터 유출

소매업의 보안 전문가들은 매출 손실 및 브랜드 평판 훼손과 직결되는 가장 심각한 보안 위험으로 표적형 공격(38%)과 내부자의 데이터 유출(32%)을 손꼽았습니다(그림 64 참조). 그 이유로는 공격이 조직 내부에서 시작되는 경우도 있기 때문입니다. 말하자면, 침해지표(Indicators Of Compromise: IOC) 검사를 중심으로 보안 체제를 구축하는 것만으로는 충분하지 않습니다. 또한 소매업체는 공격지표를 검토할 수 있는 툴도 갖춰야 합니다.

또한 APT나 피싱 공격처럼 정교한 표적형 공격을 감지하려면 매일, 매주 또는 쇼핑 시즌마다 달라질 수 있는 정상/비정상 트래픽 패턴을 구분해야 합니다.

**그림 64.** 가장 심각한 보안 위험은 표적형 공격과 내부자의 데이터 유출


출처: 2017년 시스코 보안 역량 벤치마크 연구

48 "New Credit Card Chips Shift Liability to Retailers," Andrew Cohn, Insurance Journal, 2015년 12월 7일: insurancejournal.com/news/national/2015/12/07/391102.htm

### 전문 인력 부족 문제 해결

소매업체는 인력과 툴 같은 보안 자원을 확보하는 데 어려움을 겪습니다. 소매업의 보안 전문가 중 24%는 숙련된 인력 부족이 향상된 보안 프로세스 및 기술을 도입하는 데 중대한 장애 요인으로 작용한다고 답변했습니다. 전문 인력 부족 현상에 맞물려 소매업에서는 빠짐없이 해결하기에 너무나도 많은 보안 알림이 꾸준히 발생되고 있습니다. 소매업의 보안 전문가 중 45%는 매일 수천 건의 알림이 발생되지만 그 중 53%만 조사를 실시한다고 답했습니다. 그리고 조사한 알림 중 27%가 실제 보안 사고로 판명되지만 그 중 치료까지 완료되는 사고는 45%에 그치는 것으로 나타났습니다.

인력 부족 문제가 대두되면서 자동화된 보안 솔루션의 역할이 더욱 중요해졌습니다. 자동화된 솔루션은 인력 부족으로 생기는 공백을 메우는 데 도움이 되기도 합니다. 예를 들어, 감염된 장치를 자동으로 격리 장소에 배정하는 솔루션으로 감염이 확산되거나 장치가 기밀 정보에 액세스되는 것을 막을 수 있습니다.

또한 자동화는 소매업의 분산 환경에 내재된 고질적인 문제를 해결(예: 담당 인력이 조사해서 치료해야 하는 보안 알림 발생 횟수 최소화)하는 데 도움이 될 수 있습니다. 사업장(결과적으로, 데이터)이 지리적으로 분산되어 있기 때문에 보안 책임자는 모든 매장이 본사와 동일한 보안 정책을 준수한다고 짐작(또는 기대)할 수밖에 없습니다. 매장이 다른 매장이나 사업장과 지속적으로 소통하지 않으면 몇 년이고 패치/업데이트하지 않는 채 보안 솔루션을 사용할 우려도 있습니다.

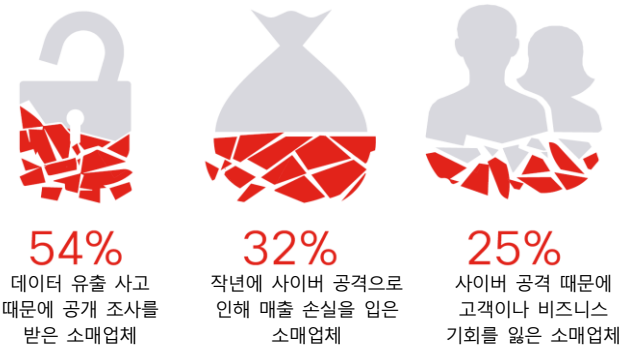
소매업체는 인력 부족 문제를 해결하기 위해 적어도 부분적으로나마 외주에 의존할 수 있습니다. 약 절반에 해당되는 소매업의 보안 전문가가 (부분적으로라도) 타사의 컨설팅 서비스에 의존한다고 밝혔습니다. 45%는 외주를 통해 보안 감사에 수반되는 부담을 덜고 있다고 답했습니다. 절반 가량의 소매업체가 외주에 의존하는 가장 큰 이유로 경제성, 편견 없는 통찰력, 적시의 사고 대응을 손꼽았습니다.

### 개인정보 유출 사고 직후 수익 및 브랜드 평판 하락

소매업체는 보안 사고가 실제로 비즈니스에 영향을 미친다는 사실을 잘 알고 있습니다. 소매업의 보안 전문가들은 운영, 재무 및 브랜드 평판이 보안 사고로 가장 큰 타격을 입는 비즈니스 영역이라고 답했습니다. 54%가 데이터 유출 사고 때문에 공개 조사를 받은 적이 있다고 밝혔습니다. 또한 작년에 사이버 공격으로 인해 매출 손실을 입은 소매업체도 34%에 달하는 것으로 조사됐습니다(그림 65 참조). 그리고 약 25%는 사이버 공격 때문에 고객이나 비즈니스 기회를 잃은 것으로 확인됐습니다.

데이터 유출 사고는 소매업체의 보안 태도에 변화를 가져 오는 전환점이 되기도 합니다. 소매업체 중 29%만이 개인정보 유출 사고를 계기로 보안을 "대폭" 강화했다고 밝혔는데, 거의 90%는 보안 사고 이후 보안 체제를 "조금이라도" 개선한 것으로 조사됐습니다.

**그림 65.** 데이터 유출 사고로 인해 다양한 피해를 입은 소매업체 비율




출처: 2017년 시스코 보안 역량 벤치마크 연구

## 제조

### 업종별 핵심 과제

미국 공장 중 80%는 가동을 시작한지 20년[49]이 넘어 최신 방어 시스템을 갖추고 있는지 여부에 대하여 우려하는 목소리가 커지고 있습니다. 사무용 시스템과 달리 생산 장비는 흔히 오랜 세월에 거쳐 단계적으로 도입되기 때문에 알려지지 않은 취약점이 수년 동안 잠복해 있다가 지금에서야 실체를 드러내기도 합니다. 제조업체가 이러한 구형 시스템에 네트워크 기반의 장치를 추가하자 보안 전문가들은 사이버 범죄자가 악용하기 좋은 조합을 찾아낼 수 있다는 우려를 제기합니다.

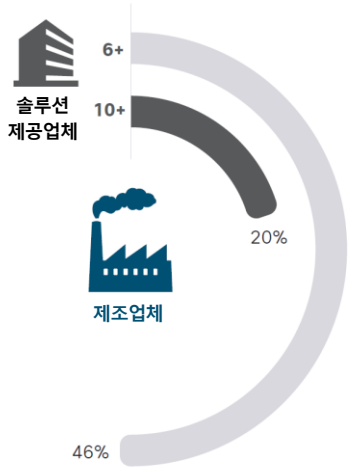
취약한 시스템으로 인해 공장 가동이 중단될 수 있다고 우려하는 자동화 전문가들의 목소리도 만만치 않습니다. 제조업체는 악성 프로그램에 감염된 시스템이 정상적으로 작동하는 탓에 발생할 수 있는 제품 품질 문제와 계획에 없던 가동 중단을 어떻게 해서든 막으려 합니다.

제조업체 보안 전문가의 당면 과제는 노후한 시스템을 업그레이드하여 사이버 범죄자가 손쉽게 침입하는 것을 막고 IoT 시스템 같은 기술을 통합하는 것입니다. 다행인 것은 제조업체가 간단한 단계적 조치만으로도 보안을 개선할 수 있다는 것입니다. 한 번에 모든 위협을 해소하는 것이 아니라 점진적으로 보안을 강화하는 데 힘써야 합니다. 예를 들어, 보안 정책을 명문화하면 보안 강화의 기준으로 삼을 수 있습니다. 안타깝게도, 시스코의 설문조사에서 제조 산업의 보안 전문가 중 40%는 공식적인 보안 전략을 갖추고 있지도, ISO 27001이나 NIST 800-53 같은 표준화된 정보 보안 정책을 따르지도 않는다고 답했습니다. 이와 같은 보안 정책을 추구하다 보면 자사의 보안 체제에서 개선할 부분을 알 수 있을 것입니다.

### 시스템 복잡성의 극복

제조 시스템을 업데이트 및 통합하려는 제조업체는 보안 솔루션의 복잡성 문제부터 해결해야 합니다. 제조 산업의 보안 전문가 중 46%는 6개 이상의 보안 솔루션 제공업체와 거래하고 있다고 답했습니다. 10개 이상의 보안 솔루션 제공업체에 의존한다고 답한 보안 전문가도 20%에 달합니다(그림 66 참조). 구체적으로 몇 가지 제품을 사용 중이냐고 묻는 질문에 63%의 보안 전문가는 6가지 이상의 제품을 사용한다고 답했으며 30%는 10가지 이상의 제품을 사용한다고 밝혔습니다.

**그림 66.** 6개 이상의 보안 솔루션 제공업체에 의존하는 제조업체 비율




출처: 2017년 시스코 보안 역량 벤치마크 연구

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

제조업체가 수많은 솔루션 및 솔루션 제공업체를 이용하다 보니 보안 전문가에게 혼란스러운 상황이 발생합니다. 복잡성을 극복하려면 일단 IT 팀과 OT 팀이 관심을 기울여야 할 보안 문제부터 줄여야 합니다. 예를 들어, 가장 시급한 문제부터 해결할 수 있는 제품들만 사용하는 방안을 고려해 볼만합니다. 물리적 자산에 대한 간단한 보호 조치(예: 비관리형 스위치의 포트 폐쇄 또는 공장 네트워크 인프라에 관리형 스위치 사용)가 포함된 다단계 방어 정책을 시행하는 데 힘쓰는 것도 바람직합니다.

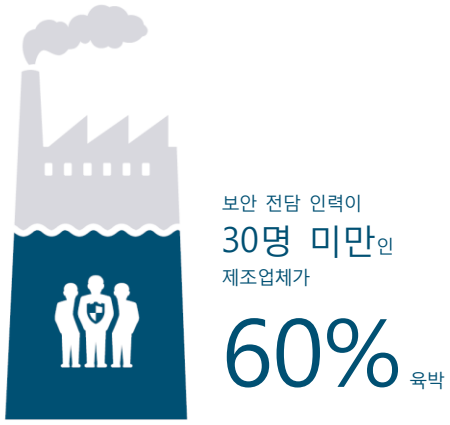
49 "America Is Aging in More Ways Than One," Sho Chandra/Joran Yadoo, Bloomberg, 2016년 10월 6일: bloomberg.com/news/articles/2016-10-06/america-is-aging-in-more-ways-than-one

### IT 팀과 OT 팀의 전문성 접목

제조 현장의 자산을 보호하려면 보안 팀을 적절히 구성해야 합니다. 자체 개발한 제조 시스템에 정통한 전문가가 퇴직한 경우 마땅한 대체 인력을 찾지 못해 전문성에 공백이 생길 수 있습니다. 제조업체 중 거의 60%가 보안 전담 인력이 30명 미만이라고 답했습니다(그림 67 참조). 또한 25%는 숙련된 인력 부족이 향상된 보안 프로세스 및 기술을 도입하는 데 중대한 장애 요인으로 작용한다고 밝혔습니다.

제조업체는 사내 보안 전문 인력을 보강하는 하는 한편, IT 부서와 OT 부서가 지식을 공유하는 문화를 조성해야 합니다. 전통적으로 IT 부서는 OT 부서가 담당하는 생산 현장에도 개입하는데, 갈등이 적잖게 발생합니다. 예를 들어, IT 부서의 패치 프로세스로 인해 구형 네트워크에서 가동되는 장비가 의도치 않게 멈추면서 생산은 중단되고 OT 인력은 곤란한 상황에 처합니다. 미래 지향적인 제조업체들은 IT 팀과 OT 팀을 통합하여 보안 위협에 대한 이해를 높이고 IoT 및 스마트 장치 같은 최신 기술 관리 정책을 강화하고 있습니다.

**그림 67.** 제조업체의 숙련된 보안 인력 수




출처: 2017년 시스코 보안 역량 벤치마크 연구

### 보안 사고 예방으로 경쟁력 상승 효과 창출

제조업체는 제조 산업에서 노후화된 시스템이 차지하는 비중을 감안하면 보안상의 이유뿐만 아니라 경쟁력 강화를 위해서라도 이를 개선하고 업그레이드해야 한다는 사실을 인식하고 있습니다. DBT Center(Global Centre for Digital Business Transformation)의 연구 결과[50]에 의하면 향후 5년간 10개 제조업체 중 4곳은 인프라 현대화를 소홀히 하여 첨단 기술을 도입한 경쟁업체에 대적하기가 어려워져 어려움을 겪을 것으로 전망됩니다. 보안은 브랜드 평판을 유지하고 매출 하락과 고객 이탈을 막는 데 도움이 되므로 경쟁 우위를 점하는 데 있어 중대한 역할을 합니다.

시스코의 조사 결과에 따르면 고객 정보 유출 사고는 제조업체 브랜드에 부정적인 영향을 미칠 수 있습니다. 제조업체 중 40%가 데이터 유출 사고 때문에 공개 조사를 받은 적이 있다고 답했습니다. 또한 28%의 제조업체는 지난 해 보안 사고 때문에 수익이 감소했다고 밝혔습니다. 그러나 보안 사고는 보안 강화 의식을 고취하는 데 일조하기도 합니다. 95%의 제조업체가 개인정보 유출 사고를 계기로 보안을 조금이라도 개선한 것으로 조사됐습니다.

50 "Life in the Digital Vortex: The State of Digital Disruption in 2017," Global Center for Digital Business Transformation: imd.org/dbt/digital-business-transformation

## 공익사업

### 업종별 핵심 과제

2016년 러시아 해커에 의한 우크라이나의 전력망 마비 사태는 공익사업체가 사이버 공격으로부터 핵심 인프라를 보호하는 데 주력해야 한다는 경각심을 일깨운 대표적 사례입니다.[51] 공익사업체는 더 이상 폐쇄형 SCADA(Supervisory Control And Data Acquisition) 네트워크를 운영하지 않습니다. 전력 생산, 송전 및 배전 장비를 원격으로 모니터링하고 제어하는 제어 센터 워크스테이션이 비즈니스 네트워크와 IT 시스템에 동시에 연결됩니다. 물리적 프로세스를 모니터링하고 제어하는 이러한 OT 시스템은 알려진 사이버 보안 취약점이 존재하고 물리적 손상을 입히기 용이하다는 점 때문에 사이버 범죄자의 표적이 되고 있습니다.

2017년 6월 시스코는 이 공격에 한층 더 정교해진 익스플로어킷이 사용됐다는 사실을 발견했습니다. 사이버 범죄자는 제어 프로토콜을 직접 활용하는 특수 모듈을 동원했습니다. 이전 공격에서는 원격 제어 툴을 수동으로 조작하는 수법이 사용됐습니다. 그런데 우크라이나 전력망 공격에서는 사이버 범죄자가 새로운 확장 모듈을 통해 원하는 대로 공격 시기를 설정하고 공격을 감행할 수 있었습니다.

설치된 OT 펌웨어 및 소프트웨어의 보안 취약점에 최신 IT 및 OT 시스템이 연결되고 복잡해져서 보호해야 할 공격 범위가 넓어졌습니다. 비즈니스 디지털화의 일환으로 인간의 개입 없이도 물리적 프로세스를 감지, 모니터링 및 실행하는 최신 소프트웨어 기술을 도입하는 공익사업체가 늘고 있습니다. 이와 같은 사이버 세계와 실제 세계의 융합(소프트웨어와 내장형 시스템을 장치에 통합)으로 인해 보안 전문가의 어려움이 가중되고 있습니다.

사이버 세계와 실제 세계의 융합에 수반되는 보안 위험이 공급망으로 확대되고 있습니다. FERC(Federal Energy Regulatory Commission)는 최근 NERC(North American Energy Reliability Corporation)에 (특히, 공익사업체 공급망의) 중요 인프라 보호에 관한 새로운 표준 개발을 지시한 바 있습니다. 이 표준은 대규모 전기 시스템 운영과 관련된 산업 제어 시스템 하드웨어, 소프트웨어, 그리고 컴퓨팅 및 네트워킹 서비스의 공급망 위험 관리에 적용될 것으로 예상됩니다.[52]

### 중대 보안 위험 - 표적형 공격과 APT

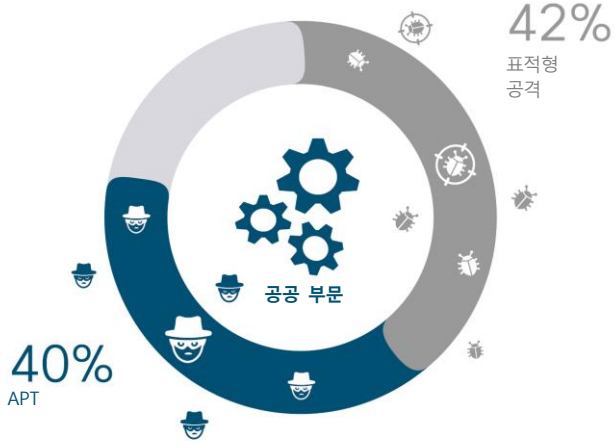
표적형 공격을 우려하는 보안 전문가들의 목소리가 높습니다. 전력 및 에너지 산업의 보안 전문가들은 가장 심각한 보안 위험으로 표적형 공격(42%)과 APT(40%)를 손꼽았습니다(그림 68 참조). 또한 보안 전문가들은 방어 전략에 반영해야 할 중대 항목으로 모바일 장치, 사용자 행동 패턴, 퍼블릭 클라우드 스토리지 및 고객 데이터를 언급했습니다.

APT를 경계해야 하는 이유는 오랜 시간 동안 중요 네트워크에서 발각되지 않은 채 사이버 범죄자가 더 큰 피해를 야기하는 데 활용될 수 있기 때문입니다. 데이터 네트워크가 통합되고 스마트 장치가 증가하면서 공익사업체의 인프라가 마비되는 등 피해 규모가 유례없이 커지고 있습니다.

공익사업이 대중에 미치는 중대한 영향 때문에 보안 팀은 현존하는 공격 수법에 정통합니다. 그래도 APT 및 표적형 공격을 효과적으로 차단할 수 있도록 최신보안기술을 적절히 통합하는 방법을 확립하는 데 힘써야 합니다. 공공 부문의 보안 전문가들은 보안이 중요한 이유를 잘 알고 있습니다. 이제 그들은 물리적 보안 및 사이버 보안 표준 같은 요소를 반영한 다단계 보안 체계를 구현할 "방법"을 보안 솔루션 제공업체에 요구해야 합니다.

네트워크의 복잡성 때문에 전력 및 에너지 회사가 보안 알림의 영향을 평가하고 자원을 집중 투입할 알림을 구분하는 데 어려움을 겪습니다. 전력 및 에너지 산업의 보안 전문가 중 거의 절반은 하루 평균 수천 건의 알림이 발생되는데 그 중 조사하는 알림은 63%에 불과하다고 답했습니다. 그리고 조사한 알림 중 41%가 실제 보안 사고로 판명되며 그 중 치료까지 완료되는 사고는 63%로 나타났습니다.

**그림 68.** 가장 심각한 보안 위험인 표적형 공격과 APT




출처: 2017년 시스코 보안 역량 벤치마크 연구

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

51 "Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks," Jamie Condliffe, MIT Technology Review, 2016년 12월 2일: technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/

52 "Revised Critical Infrastructure Protection Reliability Standards," U.S. Federal Energy Regulatory Commission: ferc.gov/whats-new/comm-meet/2016/072116/E-8.pdf

실제 알림 중 일부만 조사까지 이뤄지고 있는 것으로 확인됐지만, 그나마 전력 및 에너지 산업이 조사 대상 산업 중 가장 높은 해결 비율을 보였습니다. 또한 알림이 발생됐다고 해서 반드시 공격이 시작된 건 아닙니다. 보안 전문가는 네트워크 안전에 심각한 영향을 미칠 수 있는 위협을 치료하는 데 자원을 집중하는 것이 바람직합니다.

**엄격한 예산 규제로 인한 외주 의존도 상승**

전력 및 에너지 회사는 엄격한 규제를 받기 때문에 보안에 사용할 예산을 증액하기가 여의치 않습니다. 예산을 늘리려면 복잡하고 많은 시간이 걸리는 승인 절차를 거쳐야 합니다. 이러한 현실은 외부의 보안 서비스에 대한 의존도에서도 엿볼 수 있습니다. 공익사업체의 보안 전문가 중 60% 이상이 외부의 보안 컨설팅 서비스에 어느 정도 의존한다고 밝혔습니다. 또한 거의 절반이 외부의 모니터링 및 위협 분석 서비스를 이용하고 있다고 답했습니다. 절반 이상의 보안 전문가가 외부의 보안 서비스에 의존하는 가장 큰 이유로 경제성과 편견 없는 통찰력을 손꼽았습니다.

공익사업체는 엄격한 규제 하에 운영되기 때문에 공식적인 보안 정책과 표준화된 절차를 충실히 이행하는 경향을 보입니다. 공익사업체의 보안 전문가 중 거의 2/3가 명문화된 공식 보안 전략을 갖추고 있으며 ISO 27001 또는 NIST 800-53 같은 표준화된 정보 보안 정책을 추구하고 있다고 답했습니다.

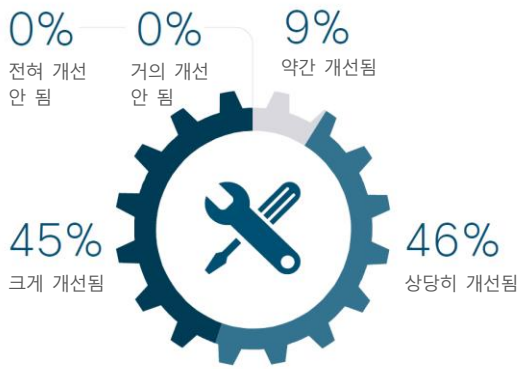
**개인정보 유출 사고를 계기로 한 보안 강화**

공익사업체에서 개인정보 유출 사고가 발생하면 세간의 주목을 받습니다. 공익설비는 대단히 중요한 인프라이며 보안 사고가 발생하면 중요 서비스가 제대로 이뤄지지 않을 수도 있다고 대중들이 생각하기 때문입니다. 한편, 공익사업체 중 61%가 데이터 유출 사고 때문에 공개 조사를 받은 적이 있다고 답했습니다.

다행인 것은 보안 사고가 보안 강화의 계기로 작용하기도 한다는 점입니다. 91%의 공익사업체가 개인정보 유출 사고를 계기로 보안을 조금이라도 개선한 것으로 조사됐습니다(그림 69 참조). "위기를 전화위복의 기회로 삼은" 셈입니다. 보안 전문가가 사고 분석을 통해 사이버 범죄자의 구체적인 네트워크 침입 방법과 침입 경로를 파악하여 방화벽 위치를 조정할 수 있습니다.

보안 사고는 공익사업체의 수익과 고객 충성도에도 영향을 미칠 수 있습니다. 지난 해 보안 사고 때문에 29%의 보안 전문가는 수익이 감소했다고 답했고 21%는 고객이 이탈했다고 밝혔습니다. 일반적으로 지역마다 한 공익사업체만 서비스를 제공하기 때문에 대다수 소비자에게 선택의 여지가 없어 경쟁이 심한 다른 산업에 비해 이탈 고객(결과적으로, 수익 손실)이 그리 많지 않습니다.

**그림 69.** 보안 사고를 계기로 보안이 크게 개선됐다고 답한 보안 전문가 비율




출처: 2017년 시스코 보안 역량 벤치마크 연구

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

**활발한 공격 시뮬레이션 및 분석**

공익사업체의 보안 전문가들은 보안 인프라의 취약점을 찾아내려고 훈련과 시뮬레이션을 자주 실시한다고 밝혔습니다. 92%는 사고 대응 계획을 테스트할 목적으로 매년 한두 차례씩 훈련을 실시한다고 답했습니다. 그리고 84%의 공익사업체가 보안 협력업체와 공동으로 훈련을 실시하는 것으로 조사됐습니다.

또한 78%의 공익사업체는 적어도 분기에 한 번씩 공격 시뮬레이션을 자체적으로 실시합니다. 절반 이하(45%)의 보안 전문가들은 공격 시뮬레이션 결과를 토대로 보안 정책, 절차 및 기술 등을 크게 개선했다고 답했습니다. 공격 시뮬레이션을 실시하는 공익사업체 중 다수는 보안 전문가가 자동화된 툴을 사용하기 때문에 더 적은 시간과 인력으로 시뮬레이션을 완료할 수 있다고 밝혔습니다.

전력 및 에너지 산업은 가장 복잡한 사이버 보안 문제를 안고 있지만 사이버 보안 전략, 정책 및 보안 통제 기술 도입 측면에서 가장 선진적인 산업으로 손꼽힙니다. 공격 수법이 진화하고 있기 때문에 핵심 인프라 제공업체도 공격을 식별, 감지, 차단, 치료하고, 보안 사고 발생 시 신속히 복구할 수 있는 솔루션을 개발해야 합니다.

## 의료

### 업종별 핵심 과제

의료 산업에서 보안과 관련된 대부분의 결정은 규제 요건, 자사의 자산 보호, 그리고 무엇보다도 환자의 안전에 중점을 두고 이뤄집니다. 의료 기관 경영진은 미션 크리티컬 장비를 마비시킬 수 있는 공격을 극도로 경계합니다. 환자의 생사가 걸려 있기 때문입니다. 또한 그들은 온라인 트래픽을 모니터링하고 위협을 감지하도록 설계된 보안 체제 때문에 중요한 시스템의 데이터 송수신 속도가 저하되어 의료진이 환자를 진단하고 치료하는 데 악영향을 미치지 않을까 우려합니다. 또한 의료 기관은 중요한 의료 활동 외에도 (예를 들어, 미국의 건강보험 이전 및 책임에 관한 법(Health Insurance Portability and Accountability Act: HIPAA)에 의거하여) 개인 의료 정보 보호에 중점을 둔 보안 시스템을 운영해야 한다는 사실을 인식하고 있습니다.

의료 기관의 네트워크에 연결되는 설비와 기기가 늘어나자 보안 책임자들은 통합 네트워크의 안전에 우려를 제기하기 시작했습니다. 과거에 PACS(Picture Archiving Collection System), 주입펌프, 환자 모니터링 장비 같은 복잡한 의료 기기는 일반적으로 제조업체가 직접 관리하는 데이터 네트워크와 함께 제공됐기 때문에 의료 기기가 다른 네트워크와 사실상 단절된 상태였습니다. 그런데 오늘날에는 가용 대역폭이 충분해지면서 의료 기관이 하나의 네트워크를 통해 데이터를 송수신하고 논리적 분할 방식을 사용하여 임상 기기, 관리자용 무선 네트워크, 사용자용 무선 네트워크 같은 다양한 유형의 네트워크 트래픽을 분리하는 것이 오히려 실용적이라고 판단하게 됐습니다. 그러나 이와 같은 논리적 분할이 제대로 이뤄지지 않으면 사이버 범죄자가 중요한 데이터나 기기를 장악할 위험이 커집니다.

### 의료기관의 중대 보안 위험 - 표적형 공격

의료 기관은 이미 랜섬웨어 공격으로 피해를 입고 있습니다. 의료 기관은 환자의 안전을 지키기 위해서라면 어떠한 대가라도 치를 것이기 때문에 온라인 범죄자에게 매력적인 표적입니다. 시스코의 설문조사에서 37%의 의료 기관이 표적형 공격을 가장 우려할만한 보안 위험 요소로 손꼽았습니다(그림 70 참조). 또한 표적형 사이버 공격은 감지하고 치료하는 데 더욱 정밀한 방법을 요하기 때문에 하드웨어 손상 또는 도난으로 인한 데이터 유출 사고보다 더 심각한 위험 요소로 간주됩니다.

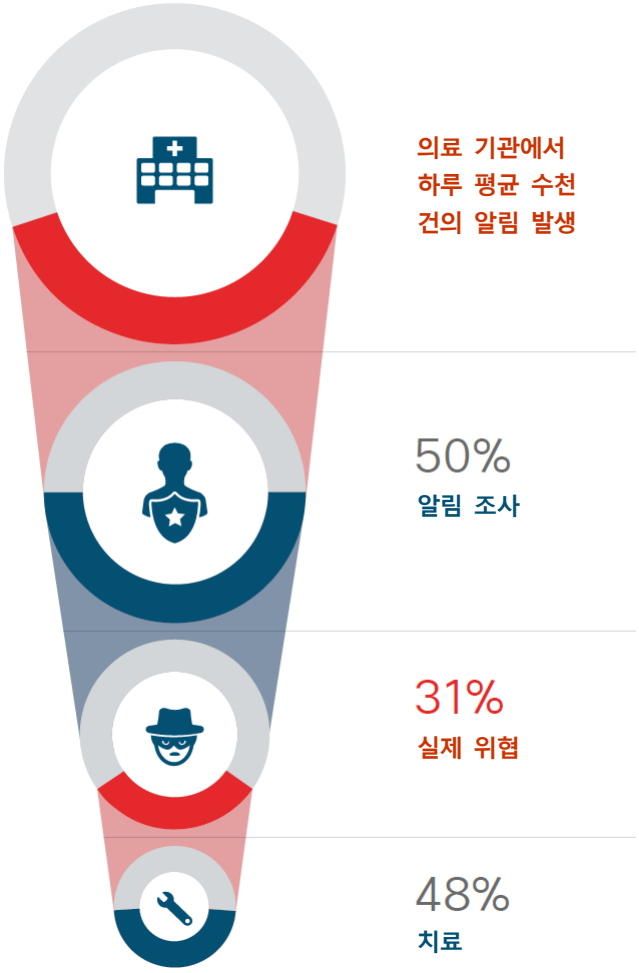
**그림 70.** 중대 보안 위험 요소인 표적형 공격


출처: 2017년 시스코 보안 역량 벤치마크 연구

유감스럽게도 많은 산업과 마찬가지로 의료업계도 모든 위협을 조사할 시간과 인력이 부족합니다. 의료 기관 중 40% 이상이 하루 평균 수천 건의 알림이 발생되는데 그 중 조사하는 알림은 50%에 불과하다고 답했습니다(다음 페이지의 그림 71 참조). 그리고 의료 기관의 보안 팀이 조사한 알림 중 31%가 실제 사고로 판명되지만 그 중 치료까지 완료하는 사고는 48%에 그치는 것으로 조사됐습니다.

시스코 보안 전문가에 따르면 실제로 조사하는 알림은 의료 기관의 보안 책임자가 생각하는 것보다 훨씬 더 적을 수 있으며, 단순히 네트워크에 침입하려는 위협을 차단하고선 위협이 해소됐다고 믿고 있을 가능성도 있습니다. 또한 많은 수의 알림을 일일이 조사하면 과도한 보안 및 IT 작업으로 인해 트래픽 속도가 크게 저하되고 다른 비즈니스 업무에 지장이 생기기 때문에 의료 기관이 면밀히 조사해야 할 알림까지 놓치는 경우가 빈번할 것으로 짐작됩니다.

**그림 71.** 수천 건의 알림이 발생되지만 치료까지 완료되는 알림은 절반 이하




출처: 2017년 시스코 보안 역량 벤치마크 연구

### 관리 문제: 숙련된 인력 부족과 솔루션의 복잡성

많은 의료 기관이 여러 가지 보안 솔루션을 혼용하고 있습니다. 60%에 가까운 의료 기관이 6개 이상의 보안 솔루션 제공업체를 이용하고 있다고 답했으며, 10개 이상의 보안 솔루션 제공업체에 의존한다고 답한 의료 기관도 29%에 달합니다. 보안 전문가 중 2/3는 6가지 이상의 보안 제품을 사용한다고 답했으며 41%는 10가지 이상의 제품을 사용한다고 밝혔습니다.

다수의 보안 솔루션 제공업체와 제품을 이용하다 보면 의료 기관의 보안 전문가가 현재 설치된 툴을 정확하게 파악하기 어려워질 수 있습니다. 보안 역량 벤치마크 연구의 전반적인 조사 결과에서 밝힌 바와 같이, 보안 툴에 대한 최고 정보 보안 책임자(CISO)와 보안 정책 관리자의 의견이 서로 엇갈리는 경우가 종종 있습니다. 계급 구조의 최상위에 있는 최고 보안 책임자들은 일상적인 보안 관리 실무에 어둡기 때문에 자사의 네트워크에 설치된 모든 툴에 정통하지 못할 수도 있습니다.

숙련된 인력이 부족한 탓에 복잡하게 얽혀 있는 솔루션을 관리하면서 일상적인 위협에 대처하기가 한층 더 어렵습니다. 보안 전문가 중 절반 정도는 보안 전담 인력이 30명 미만이라고 답했으며, 21%는 숙련된 인력 부족이 향상된 보안 프로세스 및 기술을 도입하는 데 중대한 장애 요인으로 작용한다고 밝혔습니다.

가장 큰 규모의 극소수 의료 기관을 제외하고 대규모 보안 팀을 갖춘 의료 기관은 흔치 않습니다. 시스코의 의료 산업 전문가에 따르면 보안 요원의 정의는 의료 기간마다 다르고, 그로 인해 보안 팀의 규모에 대한 인식도 다를 수 있습니다. 예를 들어, IT 인력이 보안 팀의 일원으로 간주되거나 한시적으로 보안 팀에 합류하는 경우도 있습니다.

### 트래픽 분할 효과

특정 시스템이나 기기가 각기 다른 보안 절차를 따르는 것을 허용하는 의료 기관의 이례적 상황이 환자의 안전에 지대한 우려를 낳고 있습니다. 의료 기기는 값이 비싸고 수년간 본래의 상태를 유지해야 합니다. 따라서 안정적인 작동을 우선시하느라 이례적으로 소프트웨어 및 운영 체제를 자주 업데이트하지 않습니다. 네트워크와 미션 크리티컬 장치 간의 트래픽을 격리하고 분할하는 것이 의료 환경에 더 효과적이라고 보안 전문가들은 충고합니다. 또는 의료 기관은 보완통제(Compensating Control)가 필요한 이례적 상황에 보다 효과적으로 대응할 수 있도록 보안 인프라와 네트워크 분할 방식을 개선해야 합니다.

의료 기관은 평균 34건의 중요한 보안 관리 예외를 두고 있으며, 이 예외 중 47%에는 보안방안이 적용되고 있습니다. 의료 기관은 보안 체제에 약점이 생길 수 있으므로 예외를 요하는 보안방안을 최소화하는 데 힘써야 합니다.

## 운송

### 업종별 핵심 과제

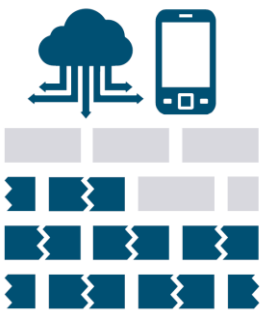
운송 산업의 기술 인프라는 전통적으로 폐쇄형 독점 시스템을 기반으로 구축됐습니다. 운송업에서는 현대식 스마트 네트워크로 전환하는 프로젝트가 활발하게 진행되고 있지만 보안 책임자들은 과도기에 사이버 범죄자에게 노출되지 않을까 우려합니다. 하지만 증가하는 유지비와 기존 시스템의 복잡성을 고려하면 스마트 IP 시스템으로의 교체는 필수입니다.

또한 소비자들은 기존의 통신 인프라로 감당할 수 없는 새로운 안전 및 모바일 서비스를 요구하고 있습니다. 예를 들어, 고객은 소셜 네트워크를 통해 공항, 항공, 여객 및 화물 철도, 도로 또는 지하철 및 교통 관할 기관과 소통하거나, 모바일 기기를 사용하여 승차권을 구매하거나 차량에서 모바일 애플리케이션을 사용할 수 있기를 원합니다. 운송 회사 직원들은 스마트 시스템을 손쉽게 사용할 수 있기를 원합니다. 더욱이 밀레니얼 세대가 운송 회사에 대거 유입되면서 이러한 요구가 갈수록 거세질 전망입니다.

### 운송업의 중대 보안 위험 - APT와 스마트 기기

운송 회사가 네트워크 기반의 복잡한 인프라를 구축하면서 네트워크 공격 범위가 넓어지자 다양한 공격 수법이 잇따라 등장하고 있습니다. 운송업의 보안 전문가 중 1/3 이상이 가장 심각한 보안 위험으로 APT와 최근 보편화된 BYOD 및 스마트 기기를 손꼽았습니다. 또한 59%의 보안 전문가는 클라우드 스토리지와 모바일 기기가 보호하기 가장 어려운 요소라고 답했습니다(그림 72 참조).

**그림 72.** 보호하기 가장 어려운 요소인 클라우드 스토리지와 모바일 기기



59%의
보안 전문가가 보호하기 가장 어려운 요소로 클라우드 스토리지와 모바일 기기 지목

출처: 2017년 시스코 보안 역량 벤치마크 연구

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

정보 접근성에 관한 요구에 부응하려면 네트워크 에지에 데이터를 보관하되, 실시간으로 정보에 접근할 수 있는 환경을 지원해야 한다는 것이 보안 전문가들의 입장입니다. 데이터 접근을 통제하고 필요로 하는 사람에게만 접근을 허용하는 것이 보안 전문가들의 주요 과제입니다.

또한 폐쇄형 독점 시스템만 사용하던 시대가 끝나면서 이런 목표를 달성하기가 오히려 더 어려워진 와중에, 더욱 복잡하고 더욱 다양한 위협에 대비해야 할 것으로 보입니다. 운송 산업의 보안 전문가 중 35%는 하루 평균 수천 건의 알림이 발생되는데 그 중 조사하는 알림은 44%에 불과하다고 답했습니다. 그리고 조사한 알림 중 19%가 실제 보안 사고로 판명되지만 그 중 치료까지 완료되는 사고는 33%에 그치는 것으로 확인됐습니다.

### 보안 인력 부족 문제를 외주로 해결

숙련된 보안 인력을 확보하면 보안 문제를 해결하기 수월하지만 운송 회사들은 적합한 인재를 확보하는 데 어려움을 겪고 있습니다. 운송업의 보안 전문가 중 절반 이상은 보안 전담 인력이 30명 미만이라고 답했습니다. 보안 전문가들은 부족한 보안 전담 인력의 여파를 토로합니다. 실제로, 29%는 숙련된 인력 부족이 향상된 보안 프로세스 및 기술을 도입하는 데 중대한 장애 요인으로 작용한다고 밝혔습니다.

보안 운영 기술이 더 정교하고 전문화됐기 때문에 운송 회사가 그에 적합한 인재를 확보하기 어려워졌습니다. 도로공사는 중요한 국가 및 지역 인프라를 보호하는 데 필요한 고급인력을 채용, 보충 및 보유할 수 있어야 합니다.

충분한 전문 인력을 자체적으로 확보하지 못한 운송 회사 중 다수가 외부의 도움을 받고 있습니다. 절반에 육박하는 운송 회사가 일부 또는 모든 보안 업무를 외주로 해결하고 있는 것으로 조사됐습니다. 외주에 의존하는 가장 큰 이유로 경제성(52%)과 편견 없는 통찰력(44%)을 손꼽은 기업이 많았습니다.

ISO 27001 또는 NIST 800-53 같은 표준화된 정보 보안 정책을 추구하는 운송 회사는 한결 수월하게 기존의 보안 벤치마크를 지향할 수 있습니다. 운송 산업의 보안 전문가 중 54%가 표준화된 정보 보안 정책을 추구한다고 밝혔고, 2/3는 명문화된 공식 보안 전략을 갖추고 있다고 답했습니다(그림 73 참조).

운송 회사는 필요할 때마다 포인트 솔루션을 구입하는 근시안적인 태도를 지양한 채 보안을 전사적으로 확립하는 데 따르는 효과를 잘 알고 있는 것으로 보입니다. 75%의 운송 회사가 보안 관제 센터(SOC)를 갖추고 있으며, 14%는 조만간 SOC를 발족할 계획이라고 밝혔습니다. 또한 거의 90%의 운송 회사가 PT-ISAC 또는 ST-ISAC 같은 보안 표준 기관 또는 산업 단체에 가입해 있는 것으로 확인됐습니다.

**그림 73.** 표준화된 보안 정책을 추구하는 운송 회사 비율

운송 산업의 보안 전문가 중 54%가 표준화된 정보 보안 정책 추구

운송 산업의 보안 전문가 중 2/3가 명문화된 공식 보안 전략 확립

출처: 2017년 시스코 보안 역량 벤치마크 연구

**공격 시뮬레이션을 토대로 보안 강화**

엄격한 규제를 받는 다른 산업과 마찬가지로 교통이 매우 중요한 인프라라는 사실이 운송 회사의 보안 방침에 직접적인 영향을 미칩니다. 예를 들어, 운송 산업의 보안 전문가 중 거의 80%는 적어도 분기에 한 번씩 공격 시뮬레이션을 자체적으로 실시합니다. 또한 절반에 가까운 보안 전문가가 공격 시뮬레이션 결과를 토대로 보안 정책, 절차 및 기술을 크게 개선할 수 있었다고 답했습니다.

개인정보 유출 사고는 보안 강화의 계기로 작용하기도 합니다. 운송 산업의 보안 전문가 중 48%가 데이터 유출 사고 때문에 공개 조사를 받은 적이 있다고 답했습니다. 34%만이 유출 사고를 계기로 보안을 "대폭" 강화했다고 밝혔지만, 83%는 보안 사고 이후 보안 체제를 "조금이라도" 개선한 것으로 조사됐습니다.

또한 보안 사고에 휘말린 기업은 후속 대책을 마련하더라도 충격에서 벗어나는 데 많은 시간이 걸립니다. 31%의 보안 전문가는 지난 해 보안 사고 때문에 수익이 감소했다고 답했는데, 평균 수익 손실은 9%로 확인됐습니다. 또한 보안 사고 때문에 22%는 고객이 이탈했고 답했고, 27%는 비즈니스 기회를 상실했다고 답했습니다.

## 금융

### 업종별 핵심 과제

금융 기관은 온라인 범죄자들이 탐낼만한 표적입니다. 풍부한 고객 재무 데이터와 사용자 계정 ID 및 비밀번호에 고무된 사이버 범죄자는 금융 기관을 대상으로 잇따른 공격을 감행합니다. 실제로, 일부 악성 프로그램 개발자는 금융 서비스 네트워크를 공격하도록 특화된 악성 프로그램을 설계합니다. 자격 증명을 도용하는 악성 프로그램인 Dridex[53]와 Zeus Trojan[54]이 그와 같은 경우에 해당됩니다.

이와 같은 상황에서 금융 서비스 보안 전문가는 사이버 범죄자의 정교한 악성 프로그램을 효과적으로 저지할 방어 체제가 필요하다는 데 공감합니다. 그러나 여러 보안 솔루션 제공업체와 거래하고 다수의 제품을 혼용하다 보니 통찰력을 얻는 건 고사하고 혼선만 초래되는 상황을 비판적으로 보는 시각도 만만치 않습니다. 또한 어떠한 보안 공백도 용납하지 않은 채 기존의 애플리케이션을 신기술과 통합해야 하는 부분도 보안 팀의 몫입니다.

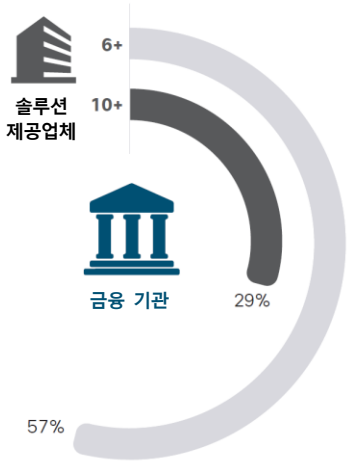
일부 금융 기관은 핀테크(금융 기술) 회사와 제휴하는데, 그로 인해 방어해야 할 범위가 넓고 복잡해집니다. 즉, 고객 데이터를 적절히 보호하려면 제휴 관계를 어떻게 활용해야 하는가? 엄격한 규제 요건을 준수하면서 다른 기업과 제휴 관계를 유지하려면 어떻게 해야 하는가? 이러한 질문을 바탕으로 금융 기관은 향후 몇 년간 보안 문제에 어떻게 대처할 것인지 고민해야 합니다.

또한 금융 기관은 "규정 준수"와 "보안"에 전력을 기울여야 합니다. 엄격한 규제를 받는 여러 산업에는 규제 요건을 준수하면 보안 문제가 해결된다는 인식이 만연해 있습니다. 망분리 같은 규제 요건을 준수하면 데이터를 보호하는 데 확실히 도움이 되지만, 이 역시 사이버 공격을 저지하고 위협을 분석할 수 있는 솔루션의 일환일 뿐입니다.

### 다양한 솔루션 혼용으로 혼란만 가중

금융 기관은 다수의 솔루션 제공업체의 제품을 사용하는 것이 보편적입니다. 금융 기관의 보안 전문가 중 57%는 6개 이상의 보안 솔루션 제공업체를 이용하고 있다고 답했습니다. 10개 이상의 보안 솔루션 제공업체에 의존한다고 답한 보안 전문가도 29%에 달합니다(그림 74 참조). 보안 전문가 중 2/3는 6가지 이상의 보안 제품을 사용한다고 답했으며 33%는 10가지 이상의 제품을 사용한다고 밝혔습니다.

**그림 74.** 6개 이상의 보안 솔루션 제공업체에 의존하는 금융 기관 비율




출처: 2017년 시스코 보안 역량 벤치마크 연구

시스코 보안 전문가에 따르면 금융업계에서는 최대 30개의 보안 솔루션 제공업체의 제품을 사용하는 금융 기관을 쉽게 찾아볼 수 있습니다. 위협에 신속하고 효과적으로 대처하려면 보안 아키텍처를 단순화하는 데 주력해야 합니다. 즉, 사용하는 툴의 종류를 줄이고 통합에 치중해야 합니다. 여러 가지 제품이 서로 단절된 채 실행되는 경우가 흔합니다. 개별적으로는 효과적일 수 있으나 여러 제품이 보안 정보를 공유하고 비교하지 못하면 상충하는 알림과 보고서 때문에 보안 팀이 골머리를 앓아야 합니다.

또한 사용하는 제품의 종류가 늘어나면 보안 전문가가 위협 조사 방법을 제대로 결정하기 어렵습니다. 금융 기관의 보안 전문가 중 46%는 하루 평균 수천 건의 알림이 발생되는데 그 중 조사하는 알림은 55%에 불과하다고 답했습니다. 그리고 조사한 알림 중 28%가 실제 보안 사고로 판명되지만 그 중 치료까지 완료되는 사고는 43%에 그치는 것으로 확인됐습니다.

필요 이상으로 많은 알림이 발생되는 이유가 여러 보안 솔루션 제공업체의 통합되지 않는 제품 때문일 가능성도 배제할 수 없습니다. 어떤 알림이 중복인지 또는 우선적으로 조사해야 할 알림은 어떤 것인지 사고 대응 팀이 파악하기가 쉽지 않습니다. 통합이 이뤄지지 않으면 보안 팀이 위협을 비교 분석하는 데 어려움을 겪을 수밖에 없습니다.

53 "Dridex Attacks Target Corporate Accounting," Martin Nystrom, Cisco Security 블로그, 2015년 3월 4일: blogs.cisco.com/security/dridex-attacks-target-corporate-accounting

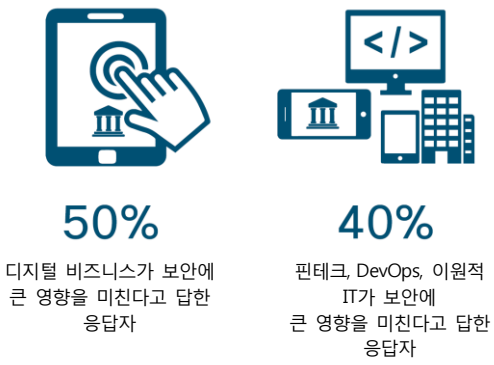
54 "Zeus Trojan Analysis," Alex Kirk, Cisco Talos 블로그: talosintelligence.com/zeus_trojan

### 보안 강화의 계기로 작용하는 디지털 비즈니스

금융 기관은 핀테크 회사와 협력 관계를 유지하면서 새로운 보안 개선 전략(예: 데이터 보안의 책임 소재 명문화)을 모색합니다. 절반에 가까운 금융 기관의 보안 전문가들은 디지털 비즈니스가 보안에 큰 영향을 미친다고 답했습니다. 또한 핀테크, DevOps, 이원적 IT가 보안에 큰 영향을 미친다고 답한 보안 전문가도 약 40%에 달합니다(그림 75 참조).

예를 들어, 핀테크 회사와 협력 중인 금융 기관은 (특히, 클라우드 환경에서) 고객 데이터를 보호하는 방법을 확립해야 합니다. 또한 협력 관계에 있는 두 기업은 보안 사고를 방지하고 보안 사고가 발생할 경우 각자 어떻게 대응할 것인지 구체적으로 명시된 공동 프로세스를 수립해야 합니다.

**그림 75.** 디지털 비즈니스가 보안 미치는 영향




출처: 2017년 시스코 보안 역량 벤치마크 연구

**cisco.com/go/mcr2017graphics**에서 2017년 그래프를 다운로드할 수 있습니다.

### 좀 더 발 빠른 표준 채택

금융 기관이 디지털 세계에서 보안을 유지한 채 고객의 요구를 부응하려면 새로운 정책과 프로세스를 도입하는 데 박차를 가해야 합니다. 현재 명문화된 공식 보안 전략을 갖춘 금융 기관은 63%에 그칩니다. 그리고 48%의 금융 기관만이 ISO 27001이나 NIST 800-53 같은 표준화된 정보 보안 정책을 추구합니다. 금융 산업은 보수적이라 보안 및 IT 책임자가 새로운 표준과 기존 보안 전략의 적합성을 평가할 때 신중한 행보를 보입니다.

금융 기관은 거래 중인 보안 솔루션 제공업체에게 확립된 보안 정책을 추구할 것을 좀 더 적극적으로 요구해야 합니다. 예를 들어, 37%의 금융 기관만이 공동 방어 체제를 구축할 수 있도록 ISO 27001를 도입하라고 보안 솔루션 제공업체에 요구하는 것으로 조사됐습니다.

시스코 보안 전문가에 따르면 보안 솔루션 제공업체에 얼마나 엄격한 요구 조건을 제시하느냐에 따라 금융 기관의 보안 성숙도가 달라질 수 있습니다. 이러한 측면에서 입지를 굳힌 대형 금융 기관이 중소 금융 기관보다 보안 솔루션 제공업체의 실태를 점검하기에 일반적으로 더 유리합니다.

# 결론

# 결론

시스코는 약 10년 전부터 연례 사이버 보안 보고서와 중기 사이버 보안 보고서를 발간해왔습니다. 발간 목적은 보안 팀과 보안 팀의 지원을 받는 사업 부문이 기존의 위협 요소와 새로운 위협 요소를 파악하고 자사의 사이버 보안과 복구 능력을 개선하기 위해 취할 수 있는 방안을 소개하는 데 있습니다.

시스코 보안 전문가 및 기술 파트너들이 이 보고서에 제시한 다양한 정보는 오늘날 위협 상황이 그만큼 복잡하다는 방증입니다. 조사 결과에 따르면 보안 팀은 과거에 비해 사이버 범죄자의 공격 수법과 경로를 훨씬 더 정확하게 이해하고 있을 뿐만 아니라 사이버 공격에도 적절히 대처하고 있습니다.

그러나 IoT가 보편화되면서 보안 팀이 우세를 유지하기가 쉽지 않을 것으로 전망됩니다. 이 보고서의 도입부에 언급했듯 유례없이 악랄하고 치명적인 새로운 유형의 공격 수법이 개발되고 있는 것으로 짐작됩니다. 사이버 범죄자들은 모든 규모의 기업을 마비시키도록 설계된 파급력 있고 치밀한 공격 수법을 개발하고 있습니다. 사이버 범죄자들은 어떤 기업도 IT 또는 OT를 처음부터 재건하는 방안을 골자로 한 비즈니스 연속성 계획을 갖추고 있지 않다는 사실에 주목하고 이런 약점을 주저 없이 악용합니다.

모든 기업이 사이버 보안을 최우선 과제로 삼는 것이 그 어느 때보다 더 중요해진 것도 이 때문입니다. 따라서 기업은 보안 팀이 경계 상태를 유지하고, 가변적인 네트워크를 모니터링 및 관리하며, 진짜 위협을 신속하게 감지해서 대응할 수 있는 자동화된 툴을 도입해야 합니다. 그리고 자사의 IT 환경에 유입되는 모든 것을 예외 없이 정확하게 파악하는 한편, IT 환경에 모든 보안 솔루션을 빈틈없이 배치하고 지속적으로 업데이트하는 데 시간과 자원을 아끼지 말아야 합니다.

한편, 보안 솔루션 제공업체는 고객이 가장 적합한 보안 솔루션을 구현하고 기존의 투자를 최대한 활용할 수 있는 개방형 에코시스템을 구축하는 방법에 대해 보다 폭넓게 사고하고 대화해야 합니다. 이와 같은 에코시스템을 구축하면 모든 보안 솔루션이 사용자와 기업을 보호하기 위해 서로 소통하고 연동할 수 있습니다. IoT 세계를 혼란에 빠뜨리고 기업의 내부 조직에 치명적인 영향을 미칠 수 있는 강력한 위협을 저지하려면 보안 팀의 단결이 필요합니다.

## 보안 관리자: 보안을 중시해야 하는 시대

시스코의 최근 보안 역량 벤치마크 연구에 따르면 많은 기업의 경영진은 보안을 중시합니다. 보안 전문가들 역시 경영진이 보안을 중대 과제로 삼아야 한다고 믿습니다. 그러나 2016년 조사에서 최고 경영자가 보안을 최우선 과제로 삼아야 한다는 점에 강력히 동의한 보안 전문가는 2015년 61%, 2014년 63%에 비해 소폭 하락한 59%였습니다.

그러나 이와 같은 수치 하락은 바람직하지 않은 현상입니다. 고위 경영진과 이사회가 사이버 보안을 비즈니스의 최우선 과제로 여기고 있을 뿐만 아니라 이 사안에 대해 더 많은 의견을 듣고 싶어한다는 사실을 최고 정보 보안 책임자(CISO)는 인식해야 할 것입니다. 실제로 경영진은 더 정확하고 더 다양한 정보를 원하는 것으로 확인됐습니다.

NACD(National Association of Corporate Directors)의 2016~2017년 공공 기업 지배구조 설문조사[55]에 따르면 1/4에 가까운 이사회는 경영진이 제출하는 사이버 보안 보고서 내용에 만족하지 못합니다. 이사회가 받는 보고서는 벤치마킹하기에 효과적이지 않고, 문제를 일목요연하게 다루지 않는 데다, 이해하기도 어려운 것으로 조사됐습니다. 같은 설문조사에서 응답자 중 14%만이 사이버 위험에 대한 이사회의 이해도가 높다고 답했습니다.

보안 솔루션 제공업체이자 시스코 파트너인 SAINT Corporation의 보안 전문가에 따르면 CISO가 그와 같은 지식 공백을 메우는 데 일조할 수 있습니다. 이를 위해 CISO가 취해야 할 태도는 다음과 같습니다.

- 구체적이고 실용적인 방법으로 정보를 전달하는 데 힘써야 합니다. 자사의 사이버 위험 또는 보안 요건에 관한 보고서가 지나치게 전문 기술적인 내용에 치중하지 않아야 합니다. 이러한 사안을 논의할 때 자사가 직면한 위험을 반영하고 비즈니스 우선 순위 및 기대한 결과와 결부시켜 설명해야 합니다. 또한 사이버 보안을 비즈니스의 성장 동력이자 경쟁 차별화 요인으로 활용할 수 있는지 강조해야 합니다.
- 사이버 공격에 대한 경영진과 이사회의 경각심을 일깨울 때 사이버 공격으로 인한 자사의 피해(예: 영향을 받는 직원 또는 고객 수, 유출될 수 있는 중요 정보의 유형), 위협을 차단하고 조사하기 위해 보안 팀이 취할 수 있는 조치, 그리고 정상화하는 데 소요되는 시간을 구체적인 수치와 통계를 동원하여 설명해야 합니다.
- 기술 부서 외에도 다른 여러 부서 책임자의 협조를 구하는 데 힘써야 합니다. 최고 정보 책임자(CIO), 최고 기술 책임자(CTO), 최고 감사 책임자(CAE), 최고 위험 관리 책임자(CRO)를 비롯한 사내 여러 지도자들과 정기적으로 소통함으로써 고위 경영진 및 이사회에 직접 보고할 수 있는 창구를 마련해야 합니다. 또한 이와 같은 직통 창구가 마련되면 CISO가 사이버 보안 전략을 논의하고 전사적인 종합 보안 프로그램을 개발할 때 "주도권"을 쥐는 데도 유리합니다.

CISO는 종종 보안 프로젝트에 필요한 자금을 확보하는 데 어려움을 겪습니다. 안타깝게도 지금이야말로 경영진과 보안 예산을 논의하기에 더없이 좋은 시기라는 사실을 미처 깨닫지 못한 CISO가 많습니다. SIM(Society for Information Management)의 2017년 IT 동향 연구에 따르면 사이버 보안은 세 번째로 큰 기업의 투자 영역입니다.[56] 참고로, 2013년에는 14위에 그쳤습니다. SIM 설문조사에서 IT 분야 중 더 많은 투자가 이뤄져야 할 분야로 사이버 보안을 손꼽은 응답자(IT 책임자)가 두 번째로 많았으며, 가장 많은 응답자가 "개인적으로 가장 우려하는" 정보 기술 분야로 사이버 보안을 지목했습니다.[57]

55 NACD의 동의 하에 2016~2017년 공공 기업 지배 구조 설문조사에서 직접 발췌한 데이터, 정보, 콘텐츠입니다. 설문조사 결과는 NACD 웹사이트 nacdonline.org/Resources/publicsurvey.cfm?ItemNumber=36843에서 다운로드할 수 있습니다.

56 Society for Information Management IT Trends Study, Kappelman, L. A. 등(2017년) - 설문조사 결과는 SIM 웹사이트 simnet.org/members/group_content_view.asp?group=140286&id=442564에서 다운로드할 수 있습니다.

57 상동

# 시스코 소개

# 시스코 소개

업계에서 가장 포괄적이고 지능적인 시스코의 첨단 사이버 보안 솔루션 포트폴리오는 가장 다양한 공격 수법을 감지하여 차단합니다. 시스코는 위협 중심의 체계적 보안 전략을 토대로 복잡성과 단편화를 최소화하면서 공격 이전, 도중, 이후에 뛰어난 가시성, 일관적인 통제, 신종 위협 차단을 지원합니다.

Cisco CSI(Collective Security Intelligence) 에코시스템의 일원인 시스코 보안 연구원들은 다수의 장치 및 센서, 공개 자료 및 기밀 자료, 오픈 소스 커뮤니티에서 수집한 통계를 토대로 업계에서 가장 정확한 위협 정보를 산출합니다. 이를 목적으로 취합되는 양이 하루에만 웹 요청 수십억 건 외에도 이메일, 악성 프로그램 샘플, 그리고 네트워크 침입알림이 수백만 건에 달합니다.

시스코의 정교한 인프라와 시스템은 이와 같은 정보를 분석함으로써 머신러닝 시스템과 연구원이 네트워크, 데이터센터, 엔드포인트, 모바일 기기, 가상 시스템, 웹, 이메일 및 클라우드를 넘나드는 위협을 추적하여 공격의 근원지와 확산 범위를 파악하는 데 일조합니다. 그렇게 확보한 분석 정보는 전 세계 고객이 이용하는 시스코의 제품 및 서비스의 실시간 보호 기능에 즉시 반영됩니다.

시스코의 위협 중심 보안 전략에 대한 자세한 내용은 cisco.com/go/security에서 확인하실 수 있습니다.

## Cisco 2017 중기 사이버 보안 보고서 제작에 도움을 주신 분들

### Cisco Cloudlock

Cisco Cloudlock은 기업이 클라우드의 보안을 유지하는 데 효과적인 CASB(Cloud Access Security Broker) 솔루션을 제공합니다. CASB 솔루션은.SaaS(Software-as-a-Service), PaaS(Platform-as-a-Service), IaaS(Infrastructure-as-a-Service) 환경의 사용자, 데이터, 애플리케이션을 모니터링하고 제어하는 데 유용합니다. 또한 Cisco Cloudlock은 데이터 분석가 중심의 CyberLab와 크라우드소싱 기반의 보안 분석을 통해 실효성 있는 사이버 보안 분석 정보도 제공합니다.

### CSIRT(Cisco Computer Security Incident Response Team)

Cisco CSIRT는 Cisco Corporate Security Program Office의 조사부 소속입니다. CSIRT는 시스코의 사이버 조사 및 포렌식 팀으로 활동하면서 사이버 공격으로부터 시스코의 지적 자산을 보호하는 맞춤형 보안 모니터링 서비스를 제공합니다. CSIRT의 주요 임무는 컴퓨터 보안 사고를 철저히 조사함으로써 기업, 시스템, 데이터를 보호하고, 예방 차원의 위협 평가, 치료 계획, 사건 동향 분석, 보안 아키텍처 점검을 통해 보안 사고 예방에 일조하는 것입니다.

### CSIRS(Cisco Security Incident Response Services)

세계 정상급 사고 대응 전문가들로 구성된 CSIRS 팀은 보안 사고 발생 이전, 도중, 이후에 시스코 고객을 돕는 데 전력을 기울입니다. CSIRS는 세계 최고의 인력, 엔터프라이즈급 보안 솔루션, 최첨단 대응 기술, 그리고 수년간 사이버 범죄자와의 전쟁을 통해 축적한 노하우를 활용하여 고객이 보안 사고를 예방하고 모든 공격에 신속하게 대응하고 복구할 수 있도록 지원합니다.

### Cognitive Threat Analytics

시스코의 Cognitive Threat Analytics는 네트워크 트래픽 데이터의 통계 분석을 통해 침입 시도, 보안 네트워크 내부에서 실행되는 악성 프로그램, 그리고 기타 보안 위협 요소를 찾아내는 클라우드 기반 서비스입니다. Cognitive Threat Analytics는 행동 분석 및 이상 징후 감지를 통해 악성 프로그램 감염 또는 데이터 유출 증상을 식별함으로써 경계 기반 방어 체제의 공백을 해소합니다. Cognitive Threat Analytics는 향상된 통계 모델링 및 머신러닝을 이용하여 새로운 위협을 독자적으로 인지하고 자가 학습을 통해 나날이 진화합니다.

### Commercial West Sales

Commercial West Sales는 시스코 고객과의 보안에 관한 대화 수준을 높이고, 고객을 위한 SAFE 워크샵을 개최하며, 기업의 보안 책임자에게 자사를 보다 철저히 보호하고 전반적인 위험을 줄이는 방법을 조언하는 데 주력하고 있습니다.

### Global Government Affairs

시스코는 여러 정부 기관과 협력하여 정부가 기술 부문을 지원하는 공공 정책 및 규정을 수립하고 목표를 달성하는 데 일조하고 있습니다. Global Government Affairs 팀은 기술 위주의 공공 정책과 규정을 직접 개발하거나 개발하는 데 영향력을 행사합니다. Global Government Affairs 팀은 업계 관계자 및 협력 파트너와 긴밀히 공조함으로써 세계적, 국가적, 그리고 지역적 차원에서 정책을 결정하는 데 일조하는 한편, 시스코의 비즈니스 및 모든 ICT 도입과 직결되는 정책에 영향력을 행사하기 위해 정부 지도자들과 유기적인 관계를 형성하고 있습니다. 전직 공무원, 국회의원, 규제 기관 중역, 미국 정부 관료 및 국정 전문가로 구성된 Global Government Affairs 팀은 시스코가 전 세계에 기술을 보급하고 기술을 보호하는 일을 돕고 있습니다.

### Global Industrial Marketing

시스코의 Global Industrial Marketing 팀은 주로 제조, 전력, 석유 및 가스 산업을 담당하고 있습니다. Global Industrial Marketing 팀은 산업에 따라 차별화된 가치 제안 메시지, 솔루션 및 시장 진출 전략을 통해 글로벌 Thought Leadership을 실현하여 고객이 디지털 방식으로 비즈니스를 혁신하는 데 일조하고 있습니다. 또한 Global Industrial Marketing 팀은 고객, 동료, 고객 관리 팀, 분석가, 언론, 내외부의 기타 관계자와 소통하는 한편, 실시간 분석 기술을 활용하여 시스코 산업별 전략, 시장 진출 전략, 계획 및 타겟 마케팅을 주도하고 있습니다.

### IPTG Connected Car

IPTG Connected Car 팀은 자동차 OEM(Original Equipment Manufacturer)이 차량 내 네트워크를 IP에 연결 및 통합하고 차량 내 네트워크를 보호 및 디지털화하는 일을 돕는 데 앞장서고 있습니다.

### IoT

Security Technology Group은 네트워크에 연결된 환경에서 위협을 감지해서 제거하는 데 유용한 툴, 프로세스, 콘텐츠를 개발하고 있습니다.

### Portfolio Solutions Marketing

Portfolio Solutions Marketing 팀은 Cisco Security 포트폴리오를 통합형 토털 보안 솔루션으로 소개하고 홍보하는 보안 메시지와 콘텐츠를 제작하여 배포하는 데 주력하고 있습니다.

### U.S. Public Sector Organization

Cisco Public Sector Organization은 시스코 고객인 정부 기관이 미국 국민을 보호하고 교육하며 국민에게 봉사하는 방법을 쇄신합니다. 연방 정부, 주 정부, 지방 정부 및 교육 기관에 주요 고객으로 하는 Cisco Public Sector Organization은 직원과 기술을 연결하고 고객 만족도부터 운영 효율성 및 임무 달성에 이르기까지 업무의 모든 면에서 혁신을 실현합니다. Cisco Public Sector Organization은 고객의 비즈니스 과제 이해, 고객의 독특한 필요사항을 반영한 맞춤형 솔루션 개발, 관계 유지, 기술 간소화, 미국과 전 세계에서 고객이 목표를 완수하는 데 일조 등을 통해 고객을 선도합니다.

### Security Business Group Technical Marketing

Security Business Group Technical Marketing 팀은 시스코의 보안 제품 의사결정권자에게 기술 및 산업 분야에 관한 심층적인 전문 지식을 제공합니다. 고도로 숙련된 기술 전문가로 구성된 Technical Marketing 팀은 엔지니어링, 마케팅, 영업 및 서비스 분야의 수많은 시스코 팀을 지원하며 시스코 고객을 보호하는 데 수반되는 가장 어렵고 복잡한 기술 과제를 설명하고 해결합니다. 지식 탐구열이 남다른 팀원들은 수많은 출판과 강연에 기여하고 있습니다.

### SR&O(Security Research and Operations)

SR&O는 업계를 선도하는 PSIRT(Product Security Incident Response Team)를 비롯한 모든 시스코 제품 및 서비스의 위협 및 취약점 관리를 책임지고 있습니다. SR&O는 시스코 및 업계 동료들과의 협력을 통해 고객을 지원하는 한편, Cisco Live 및 Black Hat과 같은 이벤트를 통해 진화하는 위협 상황에 대한 고객의 이해를 돕고 있습니다. 또한 SR&O는 기존의 보안 인프라로 탐지하거나 치료할 수 없는 공격의 징후를 포착하는 시스코의 CTI(Custom Threat Intelligence) 같은 새로운 서비스도 제공합니다.

### Security and Trust Organization

시스코의 Security and Trust Organization은 기업 경연진과 세계 지도자들이 가장 중시하는 두 가지 문제를 해결하겠다는 시스코의 약속에 역점을 두고 있습니다. 이 조직의 핵심 임무는 시스코의 고객인 공기업과 사기업을 보호하고, 시스코의 모든 제품 및 서비스 포트폴리오에 SDL(Secure Development Lifecycle) 프로세스와 TS(Trustworthy Systems) 기술을 지원하고 보장하며, 지속적으로 진화하는 위협으로부터 시스코 사업을 보호하는 것입니다. 시스코는 사람, 정책, 프로세스 및 기술을 포함해 보편적 보안과 신뢰에 총체적 접근 방식을 취합니다. Security and Trust Organization은 정보 보안, 정밀 엔지니어링, 데이터 보호 및 프라이버시, 클라우드 보안, 투명성 및 인증, 첨단 보안 연구 및 정부 등에 중점을 두고 운영 효율성을 개선하고 있습니다. 자세한 내용을 보려면 trust.cisco.com을 방문하십시오.

### Talos Security Intelligence and Research Group

시스코의 위협 정보 분석 조직인 Talos는 시스코의 고객, 제품, 서비스를 철저히 보호하는 데 전력을 기울이는 엘리트 보안 전문가 단체입니다. Talos의 선도적인 보안 연구원들은 정교한 시스템을 이용하여 시스코 보안 솔루션이 알려진 위협과 새로운 위협을 감지, 분석, 차단하는 데 필요한 위협 정보를 산출합니다. Talos는 Snort.org, ClamAV, SpamCop의 공식 규칙 세트를 관리하며 시스코 CSI 에코시스템에 위협 정보를 제공하고 있습니다.

## Cisco 2017 중기 사이버 보안 보고서 제작에 도움을 주신 기술 파트너

ANOMALI™

Anomali 위협 정보 분석 솔루션 제품군은 보안 팀이 은밀하게 활동 중인 사이버 보안 위협을 감지 및 조사하여 적절히 대응하는 데 이상적입니다. 수상 경력을 자랑하는 ThreatStream 위협 정보 분석 플랫폼은 수백만 개의 위협 지표를 통합하고 최적화하여 "사이버 블랙리스트 목록"을 산출합니다 Anomali는 내부 인프라와 통합되어 새로운 공격 수법을 식별하고, 지난 1년간 발생한 데이터 유출 사고를 과학적으로 조사하며, 보안 팀이 위협을 신속하게 파악해서 차단하는 데 필요한 정보를 제공합니다. 또한 Anomali는 위협 정보를 수집하고 공유할 수 있는 툴인 STAXX와 위협 정보 전송 서비스인 Anomali Limo를 무료로 제공하고 있습니다. 자세한 내용은 anomali.com이나 트위터(@anomali)를 통해 확인하실 수 있습니다.

FLASHPOINT

Flashpoint는 기업의 모든 사업 부문과 부서가 보다 적절한 의사결정을 내리고 위험을 완화하는 데 효과적인 비즈니스 위험 요소(BRI)를 제공합니다. 이 회사의 독창적인 Deep & Dark Web 데이터, 전문 지식, 기술을 이용하는 고객은 운영 환경을 보호하고 사용자에게 위험을 경고하는 데 필요한 정보를 수집할 수 있습니다. 자세한 내용은 flashpoint-intel.com에서 확인하실 수 있습니다.

LUMETA
DETECT WITH A HIGHER SENSE

Lumeta는 보안 및 네트워크 팀이 보안 사고를 방지하는 데 도움이 되는 사이버 상황 인식 플랫폼을 제공합니다. Lumeta는 동적 네트워크 요소, 엔드포인트, 가상 시스템, 그리고 클라우드 기반 인프라에 응용할 수 있는 세분화 분석 기술과 실시간 네트워크 및 엔드포인트 모니터링 기능뿐 아니라 모든 네트워크 인프라를 예외 없이 찾아내는 기술도 지원하고 있습니다. 자세한 내용은 lumeta.com에서 확인하실 수 있습니다.

QUALYS®
CONTINUOUS SECURITY

Qualys, Inc.(나스닥 상장명: QLYS)는 Forbes 글로벌 100대 기업 및 Fortune 100대 기업에 여러 차례 선정된 선구적이고 선도적인 기업으로서 100여 개 국가에서 9300개 이상의 기업 고객에게 클라우드 기반 보안 및 규정 준수 솔루션을 제공하고 있습니다. Qualys Cloud Platform과 통합 솔루션 제품군은 필요할 때 중요한 고급 보안 정보를 제공하고 IT 시스템 및 웹 애플리케이션의 모든 감사, 규정 준수 및 보호 프로세스를 자동화하므로 보안 운영을 간소화하고 규정 준수 비용을 절감하는 데 효과적입니다. 1999년에 창립한 Qualys는 전 세계 여러 굴지의 관리형 서비스 제공업체 및 컨설팅 회사와 전략적 제휴를 맺고 있습니다. 자세한 내용은 qualys.com에서 확인하실 수 있습니다.

radware
Every second counts

Radware(나스닥 상장명: RDWR)는 가상 데이터센터, 클라우드 기반 데이터센터, 소프트웨어 정의 데이터센터용 애플리케이션 및 사이버 보안 솔루션 분야에서 세계 선두를 달리는 기업입니다. 수상 경력을 자랑하는 Radware의 솔루션 포트폴리오는 전 세계 10,000개 이상의 기업과 통신 서비스 제공업체에 SLA(Service-Level Assurance)를 제공하고 있습니다. 추가적인 전문 보안 자료와 정보를 보려면 DDoS 공격 툴, 동향 및 위협에 관한 종합 분석 정보를 제공하는 Radware의 온라인 보안 센터(security.radware.com)를 방문하십시오.

Rapid7(나스닥 상장명: RPD)은 위험을 관리하고, 현대식 IT 환경의 복잡성을 최소화하며, 혁신을 촉진하려는 전 세계 IT 전문가와 보안 전문가의 전폭적인 신뢰를 받고 있는 기업입니다. Rapid7의 분석 기술은 오늘날의 방대한 보안 및 IT 데이터에서 정교한 IT 네트워크 및 애플리케이션을 안전하게 개발하고 운영하는 데 필요한 해답을 도출합니다. Fortune 1,000대 기업 중 39%를 포함하여 120여개 국가에 위치한 6,300개 이상의 기업이 Rapid7의 연구, 기술 및 서비스를 이용해 취약점 관리, 침입 테스트, 애플리케이션 보안, 사고 감지 및 대응, 로그 관리 프로세스를 개선하고 있습니다. 자세한 내용은 rapid7.com에서 확인하실 수 있습니다.

RSA의 비즈니스.보안 솔루션은 고객이 보안 사고를 종합적이고 신속하게 비즈니스 상황에 결부시켜서 공격에 효과적으로 대응하고 가장 중요한 자산을 보호하는 데 이상적입니다. 수상 경력을 자랑하는 RSA의 솔루션을 이용하는 고객은 신속한 감지 및 대응, 신원 및 접속 인증, 소비자 사기 방지, 비즈니스 위험 관리를 통해 불확실하고 위험한 사이버 세상에서 안전할 수 있습니다. 자세한 내용은 rsa.com에서 확인하실 수 있습니다.

차세대 통합 취약점 관리 솔루션 분야의 선두 기업인 SAINT Corporation은 기업 및 공공 기관이 전사적으로 보안 위험을 정확히 찾아내는 데 일조하고 있습니다. SAINT는 만인을 위해 접근성, 보안 및 개인정보 보호를 동시에 실현합니다. 또한 SAINT와 함께 하는 고객은 총소유비용을 줄임과 동시에 정보 보안 체제를 강화할 수 있습니다. 자세한 내용은 saintcorporation.com에서 확인하실 수 있습니다.

ThreatConnect®는 기업 고객에게 강력한 사이버 위협 차단 솔루션과 전략적으로 비즈니스 결정을 내릴 수 있는 자신감을 동시에 선사합니다. 업계에서 유일하게 지능화된 확장형 보안 플랫폼을 기반으로 하는 ThreatConnect는 모든 보안 팀이 위협 정보 취합, 분석 및 자동화와 관련한 필요사항을 충족하도록 설계된 제품군을 제공하고 있습니다. 전 세계 1,600개 이상의 기업과 기관이 보안 기술, 팀, 프로세스를 실효성 있는 위협 정보와 완벽하게 통합할 수 있는 ThreatConnect 플랫폼을 구축하여 감지부터 대응까지 걸리는 시간을 줄이고 자산 보호 능력을 개선하고 있습니다. 자세한 내용은 threatconnect.com에서 확인하실 수 있습니다.

TrapX Security는 위협을 실시간으로 포착하고 즉시 공격을 차단하는 데 필요한 분석 정보를 제공하는 적응형 사기 방지용 자동 보안 그리드를 구현합니다. TrapX DeceptionGrid™를 이용하는 기업은 세계에서 가장 효과적인 APT 개발자들이 사용하는 제로데이 악성 프로그램을 감지, 포착 및 분석할 수 있습니다. 다양한 산업에 종사하는 기업들이 IT 에코시스템을 강화하고 값비싼 대가를 치러야 하는 치명적인 보안 사고, 데이터 유출, 규정 위반의 위험을 줄이기 위해 TrapX를 활용하고 있습니다. TrapX Security는 별도의 에이전트나 구성을 필요로 하지 않으며 네트워크와 미션 크리티컬 인프라의 중추부에 설치됩니다. 단일 플랫폼이 최신 악성 프로그램 감지, 위협 정보 분석, 포렌식 분석, 치료를 모두 지원하므로 복잡성과 비용을 최소화하는 데 유용합니다. 자세한 내용은 trapx.com에서 확인하실 수 있습니다.

## 그래프 다운로드

이 보고서에 수록된 모든 그래프는 cisco.com/go/mcr2017graphics에서 다운로드하실 수 있습니다.

## 업데이트 및 수정

이 보고서에 수록된 정보의 업데이트 및 수정 내역은 cisco.com/go/errata에서 확인할 수 있습니다.


**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

Cisco는 전 세계에 200여개의 사무소를 두고 있습니다. 주소, 전화 번호 및 팩스 번호는 Cisco 웹사이트(www.cisco.com/go/offices)를 참조하십시오.



2017년 7월 발간