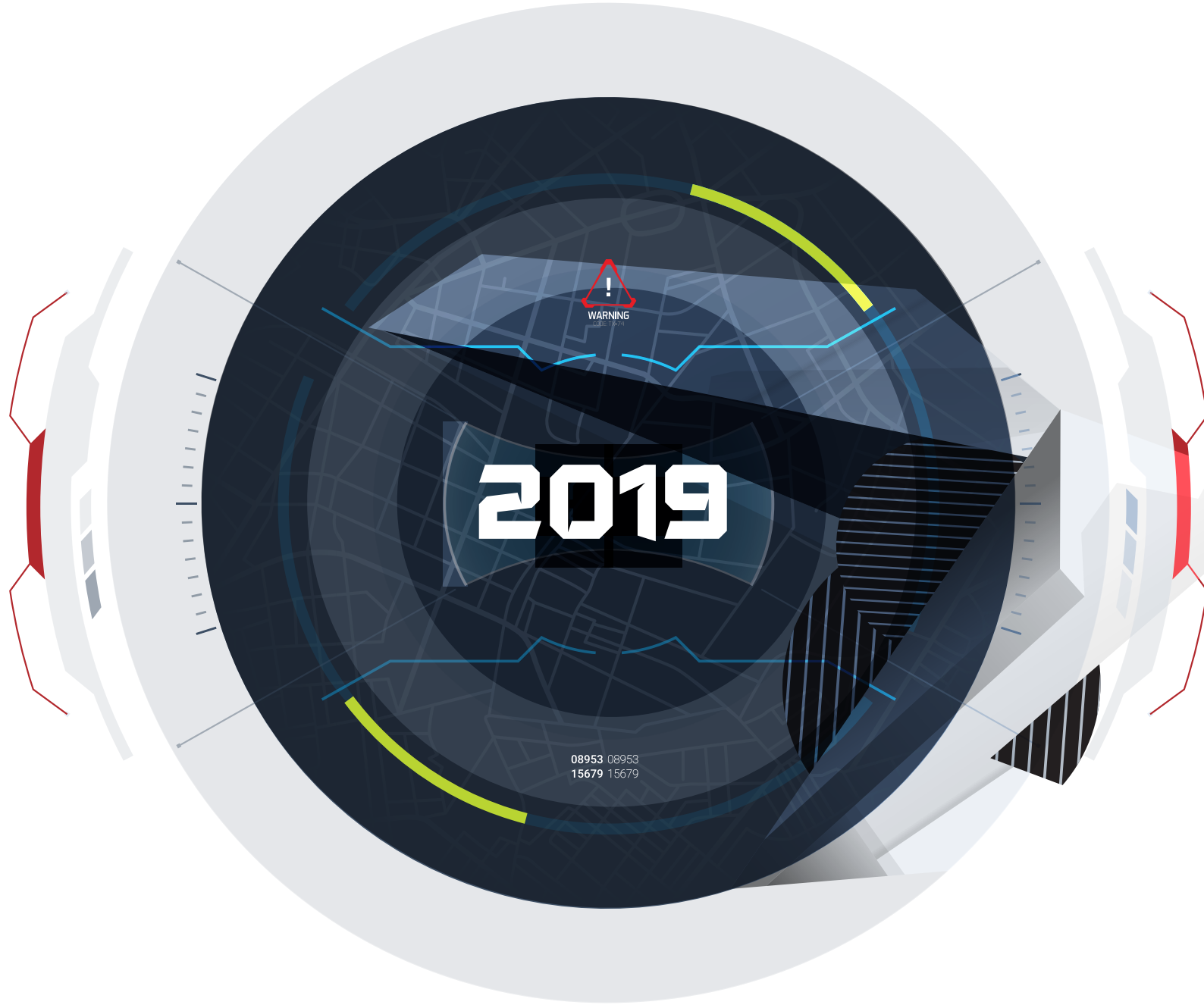
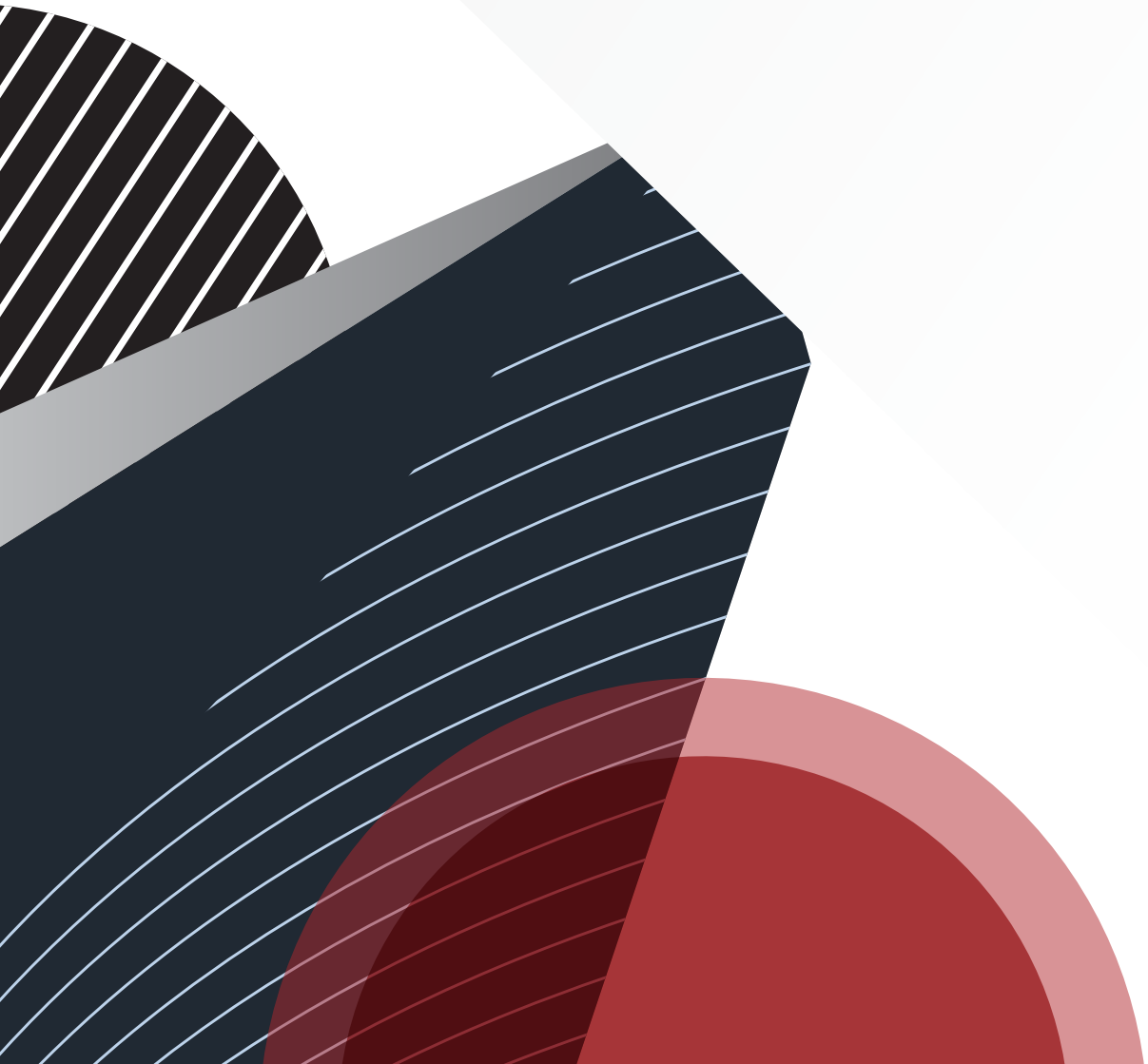
FireEye



향후 전망

2019 년 이후의 사이버 보안



Voices of FireEye

향후 전망

사이버 보안 영역에서는 수일 동안 24시간 내내 작업을 해야 하는 상황이 많이 발생합니다. 그러다 보니 언제 한 해가 끝나고 또 다른 해가 시작되는지 잊어버리는 경우가 많습니다. 이는 매우 안타까운 일입니다. 연말은 지난 12개월 동안 관찰하고 경험한 것을 되돌아보고 문제들을 최상으로 해결할 방법을 고민할 순간이기 때문입니다. 또한 특정한 추세가 있다면 이를 관찰하고, 향후 전개될 추세를 파악해야 하는 순간이기도 하므로 더 중요하다고 할 수 있습니다.

우리 각자가 문제를 해결하기 위해 많은 고민을 하더라도, 결국 가장 중요한 사실은 한 개인이 모든 문제를 해결할 수 없다는 것입니다. 사이버 보안 산업의 현황과 미래의 모습을 전체적으로 적절히 평가하려면 각자의 다양한 전문 분야에서 상세한 통찰력을 제공하는 수천 명의 개인이 필요합니다. 정보에 근거하고 논리 정연하며 방어 가능한 보안 전망을 위해서는 여러 분야의 팀이 필요합니다.

올해의 보안 예측 보고서인 *보안 전망: 2019, 우리가 마주한 미래*를 발간하기 위해 FireEye 각 분야의 전문가 및 지식을 활용하여 2019년 이후에 일어날 상황에 대한 광범위한 의견을 한데 모아 정리했습니다.

2019년에 접어들면서, CEO Kevin Mandia, CSO Steven Booth, 인텔리전스 책임자 Sandra Joyce, 클라우드 전문가 Martin Holste, 항공 전문가 Christopher Porter를 비롯한 당사의 고위 경영진은 다음 사항을 고민하고 있습니다.

- 공격적인 역량을 개발하는 국가
- 귀속관계 및 책임의 부재로 인해 계속되는 침해
- 기술 격차의 확대 및 보안 일자리를 채울 숙련된 전문가의 부족
- 중소기업의 리소스 부족
- 약점으로 작용하는 공급망
- 데이터가 모이는 클라우드를 주목하는 공격자
- 가장 위험한 위협이라고 통용되는 소셜 엔지니어링
- 사이버 스파이, 사이버 범죄 및 기타 항공 산업에 대한 위협

FireEye의 경영진은 사이버 보안에 대한 포괄적인 견해를 가지고 있지만, 최전방에서 자세한 현황을 파악하는 것도 중요합니다. 따라서 3개의 주요 팀 즉, FireEye Threat Intelligence, FireEye Mandiant 및 FireEye Labs의 전문가로부터 조언을 구했습니다. 전문 분석가 및 연구원은 다음을 비롯하여 다양한 주제에 대해 의견을 제시하였습니다.

- 중국 사이버 스파이의 재구성
- 미국에 대한 이란의 위협 활동 증가
- 주요 위협 공격자가 공개적으로 사용 가능한 악성코드 활용
- 명령 및 통제에 대한 합법적인 서비스 남용
- POS(Point of Sale)가 아닌 전자 상거래에 대해 정립된 견해
- 표적이 되는 온라인 뱅킹 포털
- 보안 향상을 위해 Flash 및 Java 사용 감소
- 초기 공격 경로로서 비즈니스 이메일 침해 증가
- 탐지를 피하기 위해 사용되는 새로운 기술

이러한 예측 중 많은 부분은 미국을 기반으로 한 FireEye 전문가가 제시한 것입니다. 따라서 우리는 APAC(아시아 태평양), EMEA(유럽, 중동 및 아프리카) 및 LATAM(라틴 아메리카) 지역을 비롯하여 북미 이외의 지역에 대해 몇 가지 주요 예측을 논의함으로써 올해 보고서를 마무리했습니다.

금년 보안 전망 보고서는 수십 명의 FireEye 리더 및 전문가의 협업을 통해 완성될 수 있었습니다. 2019년으로 나아가는 이때, FireEye 리더 및 전문가들의 협력을 기반으로 완성된 이 보고서를 통해 소중한 통찰력을 얻기 바랍니다.

CEO의 전하는 말

Kevin Mandia, CEO

억제하는 그 무엇도 없다면 **공격자는 네트워크를 계속 표적으로 삼고** 공격에 성공할 것입니다.

사이버 보안 업계에서 저의 경력은 1993년 펜타곤에서 시작되었습니다. 당시 대령과의 회의에서 7CG(7th Communications Group)에서 제가 할 수 있는 다양한 역할에 대해 논의했던 것을 기억합니다. 제게 주어진 한 가지 옵션은 JPL 프로그래밍이었고, 또 다른 옵션은 POM(Program Objective Memorandum)과 관련된 업무 수행이었습니다. 그러나 저는 이러한 두 기회 모두에서 특별히 흥미로운 점을 찾지 못했습니다. 대령은 저에게 마지막 옵션을 제시했고, 이를 통해 저는 컴퓨터 보안 책임자가 될 수 있었습니다. 이 직책은 우리가 지금까지 논의한 것 중 가장 흥미로운 업무였습니다. 그리고 당시 그 자리는 딱 한 자리만 남아있었습니다. 저는 당연히 그 직책을 받아들였습니다.

FireEye의 CEO로서 바라볼 때, 오늘날 사이버 보안 환경은 1990년대 중반과 비교해 매우 달라졌습니다. 일반적인 소비자부터 입법자 및 선출 공무원에 이르기까지 많은 사람들도 이러한 변화를 마찬가지로 느낄 것입니다. 제가 생각하기에 현재 사이버 보안 상태에 영향을 주고 있는 주요 추세로는 다음의 세 가지가 있습니다.

국가의 공격적인 활동 증가

공격자에 대한 교전 규칙이나 불이익이 없음

보안 리소스의 부족

출장을 다니면서 저는 영광스럽게도 전 세계 각국의 공무원들과 만날 기회가 있었습니다. 그리고 거의 모든 대화에서 처음 10분 이내에 같은 질문을 받습니다. 공무원들은 자신의 국가를 위해 어떻게 공격 역량을 개발할 수 있는지 질문합니다. 이것은 중동, 유럽, 아시아, 북미 등 모든 지역에 해당합니다.

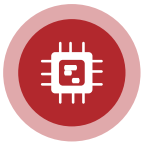
2019년과 그 이후에는 더 많은 국가에서 사이버 공격 역량을 개발할 것으로 예상됩니다. 국가가 공격 역량을 개발해서는 안 된다고 주장하는 사람들이 있지만, 전 세계 대부분의 정부 청사에 근무하는 공무원들은 자신의 국가가 공격적인 작전을 고려할 필요가 있으며 그렇지 않으면 불이익을 당할 것으로 생각합니다.

또한 우리는 사이버 공간상의 국가 차원 공격자 사이에서 공동 개입 규칙이 악화되고 있는 것을 목격하고 있습니다. 수십 년간 컴퓨터 침입에 대응하면서 느끼고 있는 사실은, 최근 들어 국가들이 공격 행동을 바꾸고 있다는 것입니다. 예를 들면 러시아의 위협 공격자들이 공격 표적을 늘리고 과거보다 더 공격적인 사이버 작전을 개시하는 것을 목격했습니다. 오늘날 대부분의 국가는 다음에 대해 질문을 던져야 합니다. "사이버 활동의 경계라는 것이 도대체 무엇입니까? 우리는 무엇을 할 수 있습니까? 무엇이 허용됩니까? 공정한 게임이란 무엇입니까?" 우리는 세계적인 커뮤니티에 살고 있으며, 이 커뮤니티는 앞으로 무슨 일이 일어날지 불확실하므로 그리 편안한 곳은 아닙니다. 우리는 앞으로 몇 년 내에 이 문제를 해결하기 시작해야 합니다.

안타깝게도 침해로 이어지는 공격의 속도는 늦춰지지 않는 것 같습니다. 그 이유 중 하나는 침해를 일으키는 사람들에게 제약이 될 어떤 불이익이나 영향이 여전히 없기 때문입니다. 공격자들은 이메일을 훔치거나 누군가에게서 일정량의 암호 화폐를 갈취하면서도 체포될 것이라는 두려움이나 경각심이 없습니다. 이렇게 그들을 억제하는 무엇인가가 없다면 공격자는 네트워크를 계속 표적으로 삼고 공격 할 것입니다. 또 다른 문제는 대부분의 사이버 공격이 인간의 신뢰를 악용한다는 것입니다. 우리가 인터넷으로 이메일 또는 텍스트를 전달할 때는 항상 취약성이 수반되기 마련입니다. 공격자는 피해자가 링크를 클릭하거나 악의적인 어떤 작업을 실행하게 만들 방법을 찾습니다.

세 번째 문제는 방어 리소스를 확장할 수 있는 수단뿐만 아니라 효과적인 보안 리소스가 부족하다는 점입니다. 충분한 리소스를 보유한 대기업은 많은 툴, 발전된 보안 프로그램, 다양한 프로세스 그리고 레드팀에 맞서 연습한 다수의 숙련된 인력을 보유할 수 있습니다. 그러나 이러한 대기업조차도 여전히 침해 당하고 있습니다. 하물며, 인력이나 리소스가 없는 중소기업은 더욱 많은 위험에 노출되어 있는 것입니다. 결론적으로 오늘날의 위협 환경을 고려해 볼 때 중소기업은 필요한 보안 프로그램을 구축할 역량이 부족합니다. 문제는 공격자에게 "소규모 기업"은 무방비한 표적이며, 더 큰 규모의 조직을 공격하기 위한 공급망의 일부이기도 하다는 점입니다. 이렇게 무방비한 "소규모 기업"이 결국 침해되면 공급망이 손상됩니다. 그 결과 발전된 보안 프로그램을 갖춘 대기업에 진입할 백도어가 생기는 것입니다. 이것이 우리가 2018년에 보아왔던 투쟁이며, 우리는 앞으로 이러한 문제를 해결해야 합니다.

이러한 환경에서 우리는 무엇을 해야 합니까? 우리가 글로벌 커뮤니티로서 보안 환경을 개선하기 위해 추구할 수 있는 영역으로는 다음과 같이 세 가지가 있습니다.



기술

전문가

외교

기술 측면에서 FireEye는 자체적으로 개발한 혁신 주기에 지속적으로 집중할 것입니다. 소프트웨어를 만드는 사람이라면 누구나 소프트웨어가 인간 프로세스의 자동화임을 인식하는 것이 중요하다고 생각합니다. 침해에 대응할 때 매일 최전선에서 해야 할 일은 우리가 모두 사용하는 공통의 보호 장치를 공격자가 어떻게 회피하는지 정확히 파악하는 것입니다. 그런 다음, 그러한 행위를 해결하는 혁신 주기를 만들어야 합니다. 이것이 FireEye에 주어진 사명 중 한 가지 입니다. FireEye는 인간의 프로세스를 자동화하는 솔루션에 최전선에서 파악한 내용을 통합하고 있습니다. 이를 통해 더 크고 효율적인 방어를 제공할 수 있게 되었습니다. 기술도 매우 중요합니다. 따라서 FireEye는 Tier 1 및 Tier 2 SOC(보안 운영 센터) 운영을 자동화하기 위해 최선을 다하고 있습니다. 혁신 주기의 순환 과정에 인간을 완전히 배제하지는 못하겠지만, 소프트웨어 및 자동화를 통해 인간의 개입을 가장 중요한 결정 단계로 집중시킬 수는 있습니다.

두 번째로 할 일은 지식 공유를 통해 역량을 구축하는 것입니다. 우리는 서로 가르치고, 배우고, 사이버 범죄자들이 무엇을 하는지에 관해 토론하고, 어떤 솔루션 및 서비스가 효과가 있으며, 어떤 솔루션 및 서비스가 효과가 없는지 논의해야 합니다. 우리는 업계의 모든 사람들이 자신의 스킬을 향상시키도록 지원 해야 하며 더 중요하게는 차세대 보안 전문가를 양성해야 합니다.

마지막 우선순위는 외교입니다. 사이버 보안은 전 세계적인 문제이며 모두가 이 문제에 직면해 있습니다. 한 국가에 홀로 떨어져 있는 공격자가 다른 국가에 있는 인터넷 상의 모든 컴퓨터를 위협할 수 있다는 사실은 곧 많은 사람들이 협업함으로써 문제를 해결해야 함을 의미합니다. 우리는 앞으로 교전 규칙에 대해 논의해야 합니다. 우리는 이러한 공동 개입 규칙을 시행할 방식과 공격자 또는 공격자들의 행위를 묵인하는 국가에 불이익을 가하는 방법에 대해 논의해야 합니다. 사이버 스파이 행위에 대한 합의에 도달하지 못할 수도 있지만, 원칙을 전달함으로써 사이버 공간에서 공격이 확대되는 위험을 방지해야 합니다. 또한 우리는 허용되지 않는 일련의 행동에 합의하고 그러한 행동을 방지할 억제력을 유지하기 위해 함께 협업하는 글로벌 커뮤니티를 관리할 수 있습니다.

직원 채용, 클라우드 및 통합

Steven Booth, CSO(최고 보안 책임자)

2019년 많은 변화와 혁신의 중심에는 **통합이라는 단어가 있을 것입니다.**

2019년으로 나아가면서 사이버 보안 산업이 어떻게 변화하고 발전할 것인가를 고민할 때 중점으로 두어야 할 핵심 영역은 직원 채용, 클라우드 및 통합입니다.

먼저, 직원 채용부터 살펴보겠습니다. 업계 추정에 따르면 2020년까지 공석으로 남아 있는 사이버 보안 일자리가 2-3백만 개에 이를 것으로 예상됩니다. 이 수치는 연구에 따라 다르지만, 중요한 것은 미국에서 모든 컴퓨터 과학 전공자를 모두 채용한다고 해도 여전히 사이버 보안 일자리를 채우기에 충분하지 않다는 점입니다. 명확한 사실은, 컴퓨터 전공자 중 다수가 보안이 아닌 다른 분야를 선택하며 사이버 보안 업계에 종사하지 않으리라는 것입니다.

우리는 채용과 관련하여 완벽한 균형 지점에 도달하지 못했습니다. 좋은 소식은, 우리의 당면 과제가 인력 공급의 부족이긴 하지만 인식이 바뀌고 있다는 것입니다. 서비스 데스크에서 근무하는 직원에게 보안 이벤트에 대응하는 방법을 교육할 수 있습니까? 저는 그렇게 할 수 있다고 생각합니다. 보안 분야에 근무하지 않는 직원으로부터 보안 가치를 얻을 수 있습니까? 가능성이 있습니다. 역동적으로 변화하는 환경으로 인해 과감한 변화가 필요하기도 합니다. 예를 들어, 업무 능력이 매우 뛰어난 방화벽 담당자가 있는데, 현재 대부분의 비즈니스를 클라우드로 이전하고 있는 상황입니다. 이제 이 담당자는 처음으로 AWS 환경에 대한 정책을 설정해야 합니다. 이때 직원에 대한 관리와 리더십이 중요해집니다. 직원에게 새로운 책임을 부여하지 않고 기술 향상을 위한 교육을 제공하지 않으면 직원이 발전할 수 있는 기회를 놓치게 되고 심지어 직원을 잃게 될 수도 있습니다. 사람에게 투자할 때 최고의 인재를 개발하고 유치할 수 있다는 사실을 항상 기억해야 합니다.

2019년에 정말로 우려되는 또 다른 사항은 클라우드 및 클라우드 문제입니다. 업계의 모든 사람들이 클라우드로의 대단위 마이그레이션을 예상하지만, 대부분의 회사는 자체 데이터 센터를 보호하는 데 투여한 노력만큼 클라우드를 보호하는 데는 열의를 쏟고 있지 않습니다. 그리고 사이버 범죄자들은 이 사실을 알고 있습니다. 우리가 처리하는 사고 대응 및 침해 사례 중 약 20%가 클라우드와 연관되었다는 사실에는 다 이유가 있습니다. 사이버 범죄자들은 돈이나 가치가 있는 곳을 쫓기 마련입니다. 따라서 이제 클라우드에 공격자가 몰릴 가능성이 높아질 것이 명백합니다. 클라우드에는 전체적으로 상당한 공격 표면이 존재하는 반면, 악의적인 활동을 탐지하는 고급 기술은 별로 없습니다. 좋은 소식은 이러한 문제를 해결하기 위해 큰 혁신이 일어나고 있다는 것입니다. 나쁜 소식은 이에 따라 조직에 더 많은 솔루션이 필요하고 더 많은 이벤트가 발생하며 더 많은 워크로드가 부하된다는 점입니다. 이는 결국 복잡성으로 귀결됩니다. 그러나 이러한 상황은 절대 바뀌지 않을 것입니다. 이벤트, 장치, 탐지 플랫폼, 살펴봐야 할 사항, 보안 담당자가 이해해야 할 기술 등은 갈수록 더 많아질 것입니다.

20%

우리가 처리하는 사고 대응 및 침해 사례 중 약 20%가 클라우드와 연관되었다는 사실에는 다 이유가 있습니다.

저는 2019년 일어날 많은 혁신에는 통합이 있다고 생각합니다. 보안 담당자가 집중할 수 있는 범주는 한정되어 있습니다. 따라서 현재 역량으로는 이 변화를 모두 감당할 수 없습니다. 여러분은 현재 직원들과 함께 통합을 이뤄야 하며, 누구든지 그 일을 할 수 있어야 합니다. 이 부분은 상당히 희망적입니다. 보안팀에 근무하지 않는 직원이 들어오는 위협 중 일부를 처리할 수 있는 방법을 발견할 수 있다면 엄청난 발전을 이룰 수 있습니다.

사이버 보안 시장에서 사람들은 다음과 같이 생각하는 경향이 있습니다. 마법과 같은 기술이 존재합니까? 안타깝게도, 그런 것은 없습니다. 질문은 다음과 같아야 합니다. 보유하고 있는 제어 기능과 시스템은 어떤 것들이며 이를 어떻게 사용합니까? 다양한 툴 및 기술을 구매한 사람(저와 같은 직책을 가진 사람)은 많지만, 사용법을 제대로 아는 사람은 거의 없습니다. 그들은 콘솔을 통해 어떤 이벤트가 가장 많이 발생하는지 보고 있지만, 무엇이 가장 중요한지는 파악하지 못합니다.

저와 같은 역할에 있는 대부분의 사람은 시대에 맞지 않게 방화벽이 있으니 안전할 거라고 생각합니다. 그러나 많은 기술을 구매했으므로 안전하다고 생각한다면 그것은 큰 오산입니다. 다음과 같이 자문해볼 필요가 있습니다. 내가 제어할 대상은 무엇인가? 이 질문에 접근하는 한 가지 방법은 모든 것을 똑같이 보호할 수는 없다는 점을 받아들이는 것입니다. 악성 링크를 클릭한 사용자의 노트북보다 조직의 중요 자산을 보관하는 새로운 클라우드 인프라를 더 높은 우선순위로 다루어야 합니다. 우리는 지금까지와는 완전히 다른 제어 기능을 보유해야 합니다. 그리고 이 문제는 간단히 다음과 같은 질문으로 요약됩니다. 보유하고 있는 자산이 무엇인지 알고 있습니까? 실제로 보호하려고 하는 것이 무엇인지 알고 있습니까? 보이는 것보다 어려운 질문이지만, 2019년에 그 답을 알아내야 합니다. 그리고 "이 자산을 보호할 수 있는 상당히 견고한 아키텍처가 있습니다."라고 말할 수 있을 정도로 역량을 구축하면, 이러한 베이스를 재사용하고 적용할 수 있습니다. 이 때가 되면 신뢰할 수 있는 일련의 제어 기능을 갖춘 것이며, 다양한 요구에 따라 그 용도를 바꿀 수 있습니다.

...**특히 우리가 인터넷에서 보는 내용에 대해서**는 **항상** 의심해 보아야 합니다.

인텔리전스 기밀 해제

Sandra Joyce, 글로벌 인텔리전스 운영 부문 VP 겸 책임자

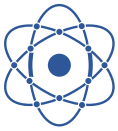
2019년으로 나아가면서 우려되는 사항 중 하나는 공급망 공격입니다. FireEye는 작년 한 해만 5건 이상의 소프트웨어 공급망 침해사고를 목격했으며, 이 수치는 과거와 비교했을 때 엄청난 증가입니다. 공급망은 공격자에게 높은 가치의 여러 표적에 접근하여 광범위한 정보를 포착할 수 있는 수단을 제공합니다. 또한, 공격자가 공급망에서 충분히 깊숙한 곳의 표적을 정한 경우 눈에 띄지 않게 작전을 펼칠 수 있습니다.

FireEye는 ICS(산업 제어 시스템) 공격이 더욱 정교해지는 것을 목격했습니다. 가장 주목할 만한 것은 최근 발표한 TRITON 악성코드입니다. 이 악성코드는 중요한 인프라 조직의 안전 시스템을 실제로 공격하고 있습니다. 이 악성코드는 정찰을 위한 것이 아니라, 실제 안전 시스템을 공격하는 케이스라는 점이 특히 불안감을 줍니다. 이러한 공격의 지속성과 사용된 리소스의 유형을 보면, 국가기반의 공격자들이 수행 할 수 있는 수준의 고도화된 공격이라고 할 수 있습니다. 그러나 주목할 만한 점은 ICS 공격을 할 수 있는 기술 수준의 격차가 공격자들 사이에서도 점점 줄어들고 있다는 점입니다. 특히 침입 및 공격 툴이 지하 시장에서 점점 더 많이 제공되고 있습니다. 그리고 이것은 큰 변화입니다. 이러한 변화가 보안 경보를 직접적으로 울리지는 않지만, 우리가 2019년으로 나아가면서 확실히 주의 깊게 살펴보아야 할 사항입니다.

2019년에 접어들면서 우려할 만한 또 하나의 영역은 모바일 악성코드의 사용 증가입니다. 모바일 악성코드는 새로운 것이 아닙니다. 그러나 이 엄청난 속도로 발전하고 있습니다. 주된 통신 수단으로 모바일을 사용하는 동남아시아, 아프리카 및 중동의 개발 도상국에서 사이버 공격자가 등장하고 있고 이러한 추세가 훨씬 더 심화될 것으로 예상됩니다.

이러한 위협에 관련해서는 모든 산업이 위험에 처해 있으며 누구도 안심하지 못합니다. 2019년에 계속 지켜봐야 하는 주목할만한 산업 중 하나는 제조업으로, 자동차 조립 회사에서 의약품을 제조하는 제약회사에 이르기까지 모든 산업을 포함합니다. 주된 이유는 IoT(사물 인터넷)의 확장으로 인해 연결성이 증가하고 제조 프로세스의 공급망에 대한 의존성이 증가함에 따라 제조 작업이 매우 광범위한 공격 표면에 노출되었기 때문입니다. 공격자들은 제조와 관련된 다양한 조직을 침해함으로써 많은 이득을 얻을 수 있기 때문에 이 산업을 더욱 매력적인 표적으로 삼을 수 있습니다.

물론, 이는 쉽지 않은 싸움이 될 것입니다. 모든 조직이 직면한 가장 큰 문제는 전문 지식의 부족입니다. 많은 조직은 보안 격차를 해소하고 침해를 완화하려는 충분한 의지가 있지만, 이를 위한 인력이 부족합니다. FireEye가 2019년에 추진할 프로젝트 중 하나는 고객이 요청하는 즉시 전문 서비스를 제공함으로써 조직에서 20-30명의 인력을 고용하지 않고도 문제를 해결할 수 있도록 지원하는 것입니다. 조직은 필요할 때 그리고 상황에 따라 FireEye의 전문 지식을 간단히 활용할 수 있습니다. 이러한 유형의 지원은 미래에 모든 조직 특히, 자체 보안 팀을 완전히 구성할 수 있는 리소스가 마련되지 않은 조직에 큰 도움이 될 것입니다.



5~20년

다른 기술은 양자 컴퓨팅입니다. 양자 컴퓨팅(그리고 이미 진행 중인 양자 키 배포)은 지금부터 5년에서 20년 내에 엄청난 도약을 할 것으로 추정됩니다.

2019년과 그 이후에 걸쳐 장기적으로, 모두가 알고는 있지만 그다지 심각하게 받아들이지 않는 두 가지 주요 기술이 있습니다. 하나는 AI(인공지능)로, 한동안 유행처럼 번지던 화두였습니다. 인공지능은 위협 환경을 실제로 변화시킬 것입니다. 인공 지능이 탐사에 사용될 뿐만 아니라 조직 및 기타 표적에 대한 공격을 구체적으로 맞춤화하는 데 활용되는 것을 상상해보십시오. 딥페이크와 같은 기술이 바로 그러한 것들입니다. 즉, 사람의 목소리와 버릇을 복제하여 실제 사람이 말한 것처럼 보이는 무언가를 만들 수 있는 능력이 실제로 구현되고 있습니다.

또 다른 기술은 양자 컴퓨팅입니다. 양자 컴퓨팅(그리고 이미 진행 중인 양자 키 배포)은 지금부터 5년에서 20년 내에 엄청난 도약을 할 것으로 추정됩니다. 이 기술을 사용하면 기존의 암호화를 해독하는 데 필요한 시간을 몇 주 또는 몇 분으로 단축할 정도로 계산의 범위가 극적으로 증가합니다. 즉, RSA와 같이 오늘날 사용 중인 일부 기본적인 암호화를 해제한다는 것을 의미합니다. 현재 물리학자 및 수학자들은 양자 저항 알고리즘을 찾아 위협을 피하려고 시도하고 있지만, 이 알고리즘을 먼저 찾아내는 사람이 현재 다루는 데이터의 암호화뿐만 아니라 기록 정보를 보호하는 모든 레거시 암호화를 무력화할 기회를 얻게 될 것입니다. 따라서 양자 기술을 개발하는 사람은 정보상의 엄청난 이점을 얻게 될 것입니다.

오늘날 전 세계의 많은 국가가 양자 컴퓨팅에 막대한 투자를 하고 있으며, 먼저 이러한 양자 기술을 선취하기 위해 경쟁을 펼치고 있습니다. 이 목표는 향후 20년 동안 아무도 달성하지 못할 수 있고 지금 당장 중요한 사항이 아닐 수도 있지만, 한 가지 사실은 오늘날 사이버 공격 및 스파이 행위를 수행하는 일부 공격자들도 이 기술에 막대한 투자를 하고 있다는 것입니다. 그들은 이미 양자 키 배포라고 하는 관련 기술(동일한 기술은 아니지만)을 사용하고 있습니다. 양자 키 배포는 현재 본질적으로 해독할 수 없는 암호화입니다. 중국과 같은 나라들은 이미 이 기술에 막대한 투자를 하고 있으므로, 우리가 멀리 내다보고 있다면 지금 이 기술에 대비해야 합니다.

우리가 2019년으로 나아갈 때 마지막 고려할 사항은 인터넷에서 읽은 내용에 대해 계속 의심하라는 것입니다. 역사적으로 영향력 작전 및 사람들이 생각하는 방식에 영향을 줄 수 있는 선전(소셜 미디어를 통해 또는 다른 유형의 조작 캠페인을 통해)에 대해 생각할 때 러시아가 떠오를 것입니다. 러시아는 비단 사이버 영역뿐만 아니라 오랜 기간 동안 영향력 작전을 수행해 왔습니다. 러시아는 이런 분야에서 매우 능숙합니다. 주목할 점은, 현재 러시아의 성공 사례를 배워 발전하고 있는 위협자들이 등장하고 있다는 점입니다. 예를 들어, FireEye는 최근 친이란적인 사회적 의제를 전파하는 데 사용된 이란인 소유의 가짜 계정을 다수 발견했습니다. 앞으로는 러시아와 이란에 그치지 않고 점점 더 많은 국가에서 이러한 사이버 작전을 펼치게 될 것입니다. 국가들이 이 전술이 얼마나 효과적인지 알기 때문입니다. 모든 사람이 대화에 참여할 수 있다는 것이 소셜 미디어의 긍정적인 측면이지만 이는 반대로 부정적으로 이용될 수 있습니다.

클라우드의 전망

Martin Holste, 클라우드 부문 CTO(최고 기술 책임자)

클라우드에서 벌어지는 일들에 대한 가시성을 확보하고 있습니까? SOC(보안 운영 센터)를 설립하여 발생하는 상황에 대응할 수 있습니까?

2018년 내내 클라우드와 관련된 많은 문제가 있었습니다. 2019년으로 나아가면서 이러한 문제는 계속되고 심화될 것으로 예상됩니다. 먼저, 많은 데이터가 클라우드로 전환되고 있으며 이에 따라 공격자도 함께 이동하고 있습니다. 우리는 클라우드와 관련된 케이스의 숫자가 엄청나게 증가하는 것을 목격하고 있습니다. 이 수치는 실제로 공격자들은 데이터를 따라다님을 증명합니다. 그렇다고 클라우드의 안전성 자체에 문제가 있는 것은 아닙니다. 저는 이러한 현상에 대해 고객과 많이 이야기합니다. 즉, 공격자는 항상 데이터가 있는 곳으로 찾아갑니다. 현재 클라우드와 관련된 많은 지능형 공격이 등장하고 있고, 일부 지능적이지 못한 공격 사례도 보이고 있습니다. 어떤 수준의 공격이든 공격이 활발히 일어나고 있다는 것은 조직이 방심하지 않아야 한다는 것을 의미합니다. 따라서 실제로 물어봐야 할 질문은 다음과 같습니다. 클라우드에서 일어나는 일들에 대한 가시성을 확보하고 있습니까? SOC(보안 운영 센터)를 설립하여 발생하는 상황에 대응할 수 있습니까?

클라우드의 가장 큰 문제는 모든 것이 공격의 표면이라는 점입니다. 조직은 클라우드 보안에 관해 여전히 수행할 일이 많습니다. 따라서 2019년에는 올바른 질문을 던져야 합니다. 현재 누가 귀사의 인프라에 로그인하고 있는지 알고 있습니까? 누가 인프라에 액세스하고 있는지 알고 있습니까? 누군가 파일을 다운로드하는 경우 그들이 그 파일을 다운로드해도 되는지 알고 있습니까? 비트 및 바이트 단위의 문제(버퍼 오버플로우 등)에는 덜 집중하면서 비즈니스 논리에 더 많은 중점을 두고 다음을 이해해야 합니다. 현재 진행되고 있는 것들이 예정되어있던 일들입니까? 이례적인 상황이 있습니까? 또한, 보안 운영 센터에서 이러한 사항을 조사할 시간이 있습니까? 이러한 질문의 답에 따라 자동화를 적용합니다. 클라우드에 대한 작업은 더 쉽게 자동화할 수 있어야 합니다. 즉, 취약성을 관리하고, 방화벽 규칙을 수행하며, 모든 일을 쉽게 진행할 수 있어야 합니다. 그러면 보안 운영 환경에서 비정상적인 활동을 발견하고 모든 것이 정상인지 확인하는 데 자원을 집중할 수 있게 됩니다.

클라우드에서 발생하는 많은 공격 중에는 우연히 클라우드에서 일어나는 것들도 있습니다. 공격의 표적인 가상 머신이 온프레미스에서 실행될 수 있지만, 클라우드에서 실행 될 수도 있습니다. 어떤 경우에는 공격자가 온프레미스 네트워크에 침투한 후 그곳에서 클라우드로 옮겨갈 수 있으며, 그 반대의 경우도 가능합니다. 이러한 것들이 2019년에 염두에 두어야 할 사항입니다. 따라서 온프레미스에 있는 하이브리드 데이터 센터와 클라우드 간 연결을 모니터링하는 것은 매우 중요합니다.

클라우드 보안에서 가장 유의해야 할 사항은 이메일 보안일 것입니다. 피싱을 방어하는 일이 그만큼 어렵기 때문입니다. 피싱은 공격자가 침투하는 가장 주된 방법이며, 2019년에 그 사실이 바뀔 것으로 예상되지는 않습니다. 기본적으로 클라우드는 버퍼 오버플로우, SQL 삽입 공격 등에 대해서는 훨씬 더 안전합니다. 5년 전에는 검증된 많은 공격이 클라우드에서는 별 효과가 없다는 것이 밝혀지고 있습니다. 반면에, 기술 지원을 요청하면서 사칭하는 것과 같은 방법은 효과적입니다. 이러한 전술은 계속 사용될 것입니다. 공격자는 크리덴셜을 탈취하는 일로 시작하여 점차 내부로 이동합니다. 이러한 이유로 가시성과 작업의 자동화가 매우 중요합니다. 알려진 악성 패턴을 찾는 일과는 다르게, 현재 일어나고 있는 일들이 적정한 것인지 아니면 보안상 문제가 될 수 있는지는 실제 조사를 통해 판단할 수 있기 때문입니다.

우리가 2019년으로 나아가면서 마주하게 될 커다란 혁신은 비즈니스 논리 및 가시성에 대한 집중이라고 생각합니다. 공격자로부터 방어하기를 원한다면 항상 누가 무엇을 하고 있는지 알아야 한다고 생각합니다. 조직은 비즈니스 내에서 일어나는 일을 파악하고 있어야 합니다. 이는 재무적인 측면만을 의미하지 않습니다. 즉, 다운로드되고 있는 파일, 부팅되고 있는 가상 머신, 2단계 인증의 사용 등을 파악하고 있어야 합니다.

...클라우드 보안에서 가장 유의해야 할 사항은 이메일 보안입니다. 피싱을 방어하는 일이 너무 어렵기 때문입니다.

공격자가 2단계 인증을 우회하는 데 사용하는 기술 중 하나가 SIM 카드 스푸핑입니다. 보통 새 전화를 구매하면, 판매사원이 전화번호가 인식된 새로운 SIM 카드를 개통시켜줍니다. 누군가에게 전화번호가 인식되지 않은 카드를 달라고 설득할 수 있다면 해당 방식으로 여러 2단계 인증을 우회할 수 있습니다. 우리는 이 기법을 사용하여 소셜 미디어 계정을 훔치는 사례를 목격했습니다. 이 경우 공격자는 인기 있는 계정을 소유한 누군가의 전화번호를 알아내고 그 계정에 접근하여 나중에 계정을 판매할 수 있습니다. 이러한 공격자는 부티크 매장에 들어가서 소셜 엔지니어링을 사용하여 새로운 SIM 카드를 구하거나 뇌물을 주고 SIM 카드를 만들기도 합니다.

2019년에도 조직이 클라우드로의 마이그레이션을 계속 진행함에 따라 적절한 질문을 던져야 합니다. 저는 조직들이 "클라우드에서도 온프레미스와 동일한 보안을 구현하고 싶습니다."라고 말하는 것을 종종 듣습니다. 하지만 이것은 적절한 생각이 아닙니다. 시작은 좋지만 다음과 같은 추가 질문을 해야 합니다. "좋습니다. 클라우드는 다릅니다. 누가 무엇을 하고 있는지에 대해 훨씬 더 많은 정보를 알 수 있습니다. 예를 들어, 시스템이 부팅된 이유를 파악할 수 있습니까? 관리자가 로그인할 때마다 알 수 있습니까? 그리고 누가 정기적으로 그것을 점검합니까?" 운영 센터에서 이러한 질문에 대응할 수 있으려면, 그동안 덜 집중했던 모든 작업을 자동화해야 합니다. 그러면 조사 과정에서 실제 인력을 더 집중할 수 있습니다.

분석은 간단한 작업을 자동화하는 좋은 방법이 될 수 있습니다. 그러나 인적 요소가 모두 자동화되지는 않을 것입니다. 전화 통화를 한다거나 사람이 반드시 개입해야 할 영역이 분명 존재하기 때문입니다. 기계가 항상 모든 일을 올바르게 수행하도록 만드는 것은 정말 어렵습니다. 따라서 사람이 이를 검토하고 후속 조치를 취하는 것이 중요합니다. 물론 여기에 AI(인공 지능)을 사용할 수 있습니다. AI를 이용하면, 이상하거나 특이한 점들을 빠르게 찾을 수 있기 때문입니다. 하지만 결국 문제를 해결하기 위해서는 인간이 필요합니다. 그리고 저의 가장 큰 관심사 중 하나도 여기에 있습니다. 즉, SOC에서는 모든 탐색 활동이 실제로 일어나고 있는지 확인하는 데 충분한 시간을 쏟고 있지 않다는 것입니다.

항공기에 대한 위협

Christopher Porter, 최고 정보 전략가

사이버 스파이는 그 위험이나 영향의 범위가 매우 광범위합니다. **따라서 최상의 방어는 상황과 맥락과 관련된 상세한 정보를 빠르게 공유하는 것입니다.**

2018년 9월 6일 저는 미국 국토안보위원회에서 증언할 기회가 있었는데 이 자리에서 미국 항공 산업 부문 관련 위협에 대한 FireEye의 통찰력을 공유했습니다. 위원들과 그들의 참모들이 저와 제 동료들에게 던진 몇 가지 중요한 질문에 대해 활발한 대화를 나눌 수 있어서 큰 영광이었습니다. 우리의 목표는 위협의 "규모를 설정"하는 것이었습니다. 즉, 미국 및 항공 부문에 대한 실질적인 위협을 알려주는 것이었습니다.

먼저, 모든 사람 앞에서 질문에 대답했습니다. 누군가 비행기를 해킹할 수 있습니까? 저는 절대 안 되는 건 없다고 배웠습니다. 그리고 가장 정교한 사이버 위협 그룹은 물리적 시스템에 대한 불능화를 비롯해 여러 부문에 걸쳐 기술 및 운영상의 불시 공격을 반복적으로 수행했습니다. 그러나 이 질문은 FireEye의 전문 지식 범위를 벗어난 사항입니다. FireEye는 공항, 항공기 제조업체의 개발 및 생산 네트워크 그리고 항공 산업 부문의 규제 및 보호를 담당하는 연방 기관을 방어합니다. FireEye는 현재 항공기 자체를 방어하고 있지 않습니다. 따라서 이 건에 대해서는 DHS 소속 전문가들의 의견에 따르겠습니다. 이 전문가들은 2017년에 발표한 연구에서 그러한 위협이 적어도 기술적으로 실현 가능하다고 했습니다.

우리는 항공기 및 항공지원 시스템에 대한 사이버 기반 물리적 위협에 적절히 대응해야 하지만, 항공 산업의 보안 팀이 대비해야 하는 훨씬 더 일반적인 위협은 사이버 스파이입니다. 사이버 스파이는 그 위험이나 영향력의 범위가 매우 광대합니다. 따라서 상황과 맥락이 담긴 상세한 정보를 빠르게 공유하는 것이 매우 중요합니다. FireEye는 실시간으로 고객에게 경보를 보내며, 같은 산업에 속한 그룹 사이에 정보를 공유합니다. 알다시피, 하나의 위협은 보통 모두에게 동일하게 위협이 되기 때문입니다.

항공 산업은 미국의 주요 수출 산업 중 하나입니다. 특히 중국은 모든 국력을 활용하여 아시아 및 전 세계의 군사력과 경제력에서 미국을 견제합니다. 지적 재산 도용을 막기 위한 미국과 중국의 성공적인 협정 체결에도 불구하고, 저는 앞으로 10년 동안 양국 간 국방 경쟁이 더 격렬해짐에 따라 사이버 스파이도 더 늘어날 것으로 예상합니다. 따라서 미국 항공 우주 연구원, 제조업체 및 항공 운영을 지속적인 표적으로 삼을 것으로 예상하는 편이 안전합니다.

마찬가지로 사이버 범죄자는 항공 산업 부문 및 해당 고객에게 경제적 위협을 가합니다. 수년 동안 공격자들은 불법적인 경로를 통해 항공권을 재판매하기 위해 항공사 및 항공권 판매자에게 익스플로잇 공격을 가하는 것을 관찰했습니다. 항공사는 고객의 신뢰를 기반으로 민감한 개인 데이터를 광범위하게 사용하므로, 사기 행위를 하려고 데이터를 수집하려는 사이버 범죄자들의 표적이 됩니다.

지난 2년간 당사 어플라이언스는 항공사 발권 및 지원 운영을 일시적으로 무력화시키는 랜섬웨어 활용 사례의 급격한 증가를 탐지했습니다. 항공 여행은 시간이 중요한 비즈니스입니다. 그리고 사이버 범죄자들은 항공사가 시스템이 해독될 때까지 승객을 운송할 수 없게 된다면, 공격자에게 빠른 금전 지불의 압박을 받게 된다는 사실을 알고 있습니다.

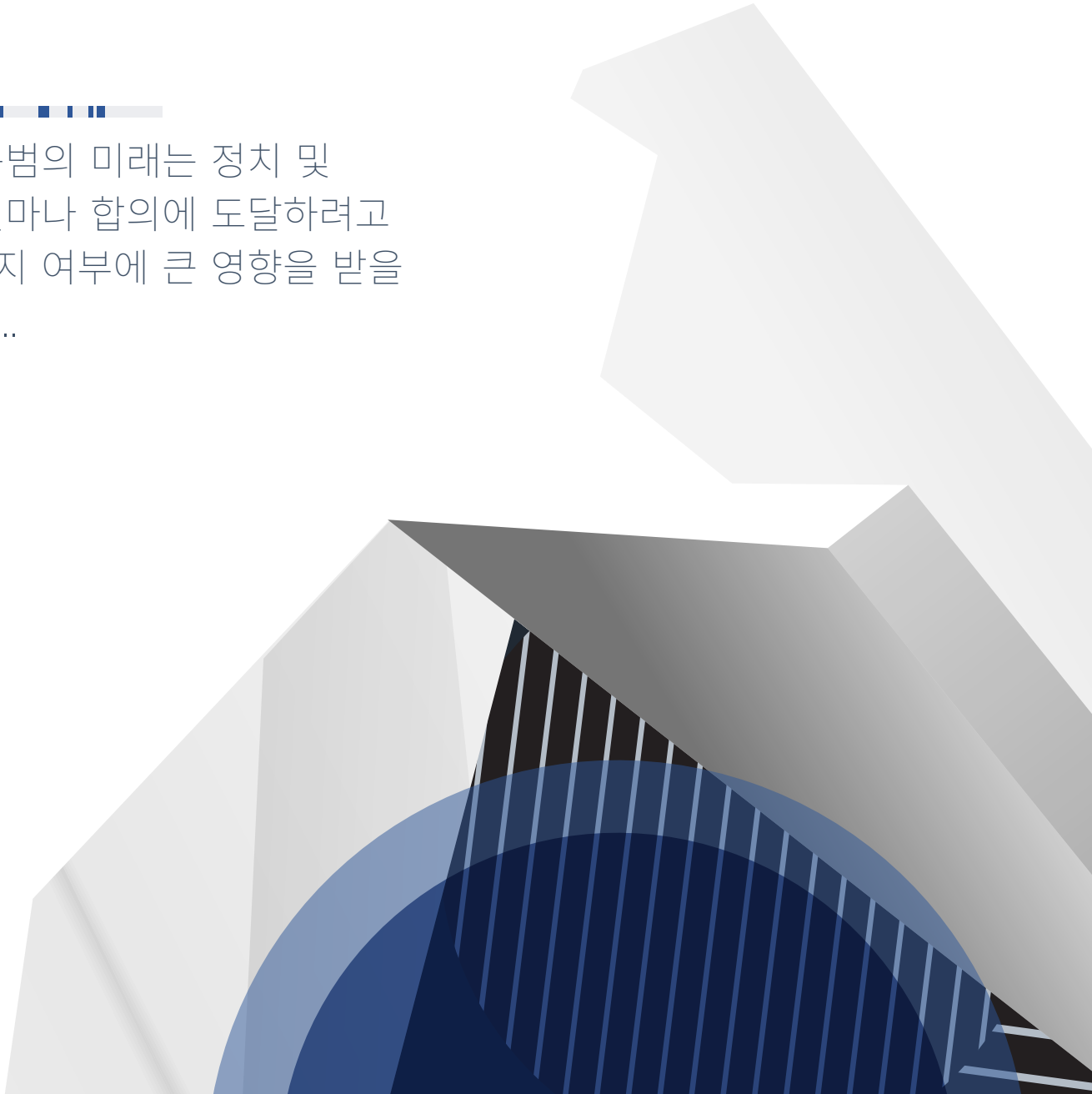
공항 자체가 피해 대상일 경우 위협에 대응할 책임이 있는 주체가 명확하지 않을 수 있습니다. 일부 항공 인프라는 민간 소유이고 일부는 주 정부 또는 지방 정부가 소유하거나 세 주체 모두가 함께 소유하기도 합니다. 공격자가 외국의 군사적 지원을 받는 위협 그룹인 경우 공항이 미군 또는 미국 연방 정부가 방어 책임이 있다고 생각하는 것도 합리적인 추론입니다. 저는 이미 제기된 위협뿐만 아니라 사이버 공격에 직접 노출 되었을 때 이에 대처하고 회복하기 위한 준비 수준에 대해서도 우려가 됩니다. 공격을 해결하는 사이에 생기게 될 혼란은 분명히 많은 리스크를 가져올 것입니다. FireEye가 고객을 대상으로 실습 훈련을 주최할 때 다양한 이해 관계자를 참여시켜 사이버 공격으로 인한 위기에 대응하는 방법을 시뮬레이션하지만, 이는 사실 쉽지 않은 일입니다.

많은 항공 시스템이 실제로 공격자의 의도와 달리 공격 당할 수 있습니다. 범죄자가 빠른 이익을 내려고 하는 와중에, 자신도 모르는 사이에 더 심각한 혼란을 일으킬 수도 있습니다. 저의 공개 증언과 같은 날 오후에 영국 공항에 일어난 상황이 바로 이런 경우입니다. 테러리스트 그룹은 혼란을 초래하여 자신들에게 이목을 끌기 위해 항공 산업을 사이버 공격 표적으로 삼기도 합니다.

가장 중요한 것은 이러한 상황에서 주된 피해자는 일반인들로서, 자신이나 사랑하는 사람이 위험에 빠질 것을 과도하게 두려워할 수 있고, 비행에 대해 점점 불신을 갖게 될 수 있다는 점입니다. 따라서 정확한 커뮤니케이션이 중요합니다. 일반 대중이 비행기 운항 및 탑승자 안전을 직접 지원하는 시스템과 장애 발생 시 이용에 불편을 유발하는 시스템은 분명히 서로 다른 두 가지임을 인지하는 데서 시작합니다.

FireEye 위협 인텔리전스 파일 활용

사이버 규범의 미래는 정치 및 기업이 얼마나 합의에 도달하려고 노력하는지 여부에 큰 영향을 받을 것입니다...



중국 사이버 스파이의 재구성

우리는 2016년부터 중국 사이버 스파이 조직의 재구성이 진행되었으며 그 결과 스파이 활동이 활발히 재개되고 있다고 생각합니다. 또한 이러한 조직 개편이 2020년 이후까지 중국 사이버 스파이 활동의 성장 및 지리적 확장에 영향을 미칠 것이라고 평가합니다. 이러한 변화는 점차적으로 이루어졌습니다. 중국의 위협 활동을 지적 재산 도용에서 사이버 스파이 활동으로 전환시킨 오바마-시진핑 합의를 비롯하여 세간의 이목을 끈 몇몇 이벤트와 공식적인 합의에 의해 촉진되었습니다. 즉, 중국 인민 해방군(PLA)은 새롭게 구성된 SSF(Strategic Support Force)의 지휘 아래에 사이버 관련 기능을 대부분 통합했으며 중국의 13차 5개년 계획(2016-2020)에 따라 시작한 목표는 국가의 우선순위를 공식적으로 바꿔놓았습니다.

미국에 대한 중국의 사이버 스파이 활동이 감소한 이후 **Red Line Drawn 보고서**에 발표된 대로 일부 그룹이 서서히 활동을 재개한 것으로 확인되었습니다. 이러한 사례의 대부분에서 해당 그룹은 새로운 악성코드, 수정된 TTP(전술, 기법 및 절차) 및/또는 다양한 지리적 표적 설정 패턴을 가지고 다시 모습을 드러냈습니다. 경우에 따라서 활동을 중단한 그룹에 속한 공격자가 새로운 작전 팀에 재편되거나 기존의 알려진 그룹에 재배정 되었을 것입니다.

2018년 이후의 사이버 스파이 활동을 주도하는 중국의 BRI(Belt and Road Initiative)

BRI(Belt and Road Initiative)는 아시아, 유럽, 중동 및 아프리카 전역에서 진행되는 야심 찬 장기 프로젝트로, 전 세계적으로 중국의 영향력을 반영할 육로(실크로드 경제 벨트 및 해상 실크로드) 및 해상 무역 네트워크를 개발합니다. 우리는 BRI가 사이버 위협 활동의 추진 요인이 될 것으로 예상합니다.

BRI와 관련된 사이버 스파이 활동에는 새로운 그룹 및 국가 지원 공격자의 출현이 포함될 것입니다. BRI의 지정학적 이해관계의 범위를 고려할 때, 이 이니셔티브는 새로운 국가 지원 사이버 공격자가 자신의 역량을 활용하는 촉매제가 될 수 있습니다. 특히, 해당 무역 경로에 있는 지역과 정부는 스파이 활동의 표적이 될 가능성이 높습니다. BRI 진행 상황에 대한 미디어 발표, 새로 체결한 계약 및 관련 개발 회의는 사이버 작전의 동인 역할을 하고 향후 침입을 위한 미끼 자료로 활용될 것입니다.

미국 조직에 대한 이란의 사이버 위협 활동은 미국의 JCPOA 탈퇴 이후 증가할 가능성이 크며, 파괴적이거나 파멸적인 공격을 포함할 수 있습니다

2015년 JCPOA(Joint Comprehensive Plan of Action)에 서명한 후, 이란 연계 사이버 활동의 속도 및 특성은 두 가지 주요 방식에서 바뀌었습니다. 첫 번째, 파멸적이고 파괴적인 작전이 상당히 감소했습니다. 두 번째, 중요한 인프라를 탐색하는 이란 연계 활동의 축소가 관찰되었습니다.

작년에 우리는 미국이 JCPOA에서 탈퇴하면 이란이 사이버 위협 활동을 통해 미국에 대해 보복할 것으로 생각한다고 보고했습니다. 이러한 보복은 잠재적으로 미국의 민간 기업에 대한 파괴적인 공격의 형태를 취할 수 있으며, 실제로는 이란 당국에 의해 통제되지만 독립적인 핵티비스트라고 주장하는 가짜 인물에 의해 수행될 수 있습니다. 이러한 공격이 즉각적이거나 단기간에 행해질 것으로 예상되지는 않지만, 초기에 이란 연계 공격자들이 장래의 작전에 대비하여 중요한 인프라 네트워크에 대한 탐색을 재개할 것으로 생각합니다. 미국의 모든 중요한 인프라 부문의 조직 및 자산 운영자는 파괴적이고 파멸적인 공격에 중점을 둔 이란의 위협 그룹으로부터 방어할 준비가 되어 있어야 합니다.

사이버 규범이 가까운 미래에 국가 지원 사이버 작전을 제한할 가능성은 없습니다

사이버 공간에서 책임 있는 국가에게 적용되는 행동 규범은 여전히 초기 단계에 머물러 있습니다. 그러나 장기적으로는 국가 혹은 그 대리인에 의해 수행되는 미래의 사이버 작전에 상당한 영향을 미칠 것입니다. 규범은 긍정적이거나 부정적일 수 있습니다. 구체적으로 행동을 용인하거나 비판할 수 있습니다. 사이버 규범의 미래는 정치 및 기업 사이에서 합의점에 도달하기 위해 얼마나 노력하는지에 많은 영향을 받을 것입니다. 궁극적으로는 한 국가에서 사이버 작전 수행 시 규범에 따를 것인지 무시할 것인지에 따라 그 효력이 달라질 것입니다.

사이버 외교에서 활발하게 활동하는 국가들과 다국적 기업들은 점점 더 복잡해지는 사이버 위협을 관리하기 위한 규범을 모색하고 있습니다. 그러나 상업적 이익을 목적으로 사이버 지적 재산 도용을 하지 않기로 한 합의를 제외하고는 국가 간에 명시적인 합의를 이룬 규범이 없습니다. 반면에 기업들은 신뢰의 헌장 및 **사이버 보안 기술 협약** 등 몇 가지 새로운 발의를 하는 등 진전을 보이고 있습니다.

FIN 및 APT 그룹의 공개적으로 사용 가능한 악성코드 사용

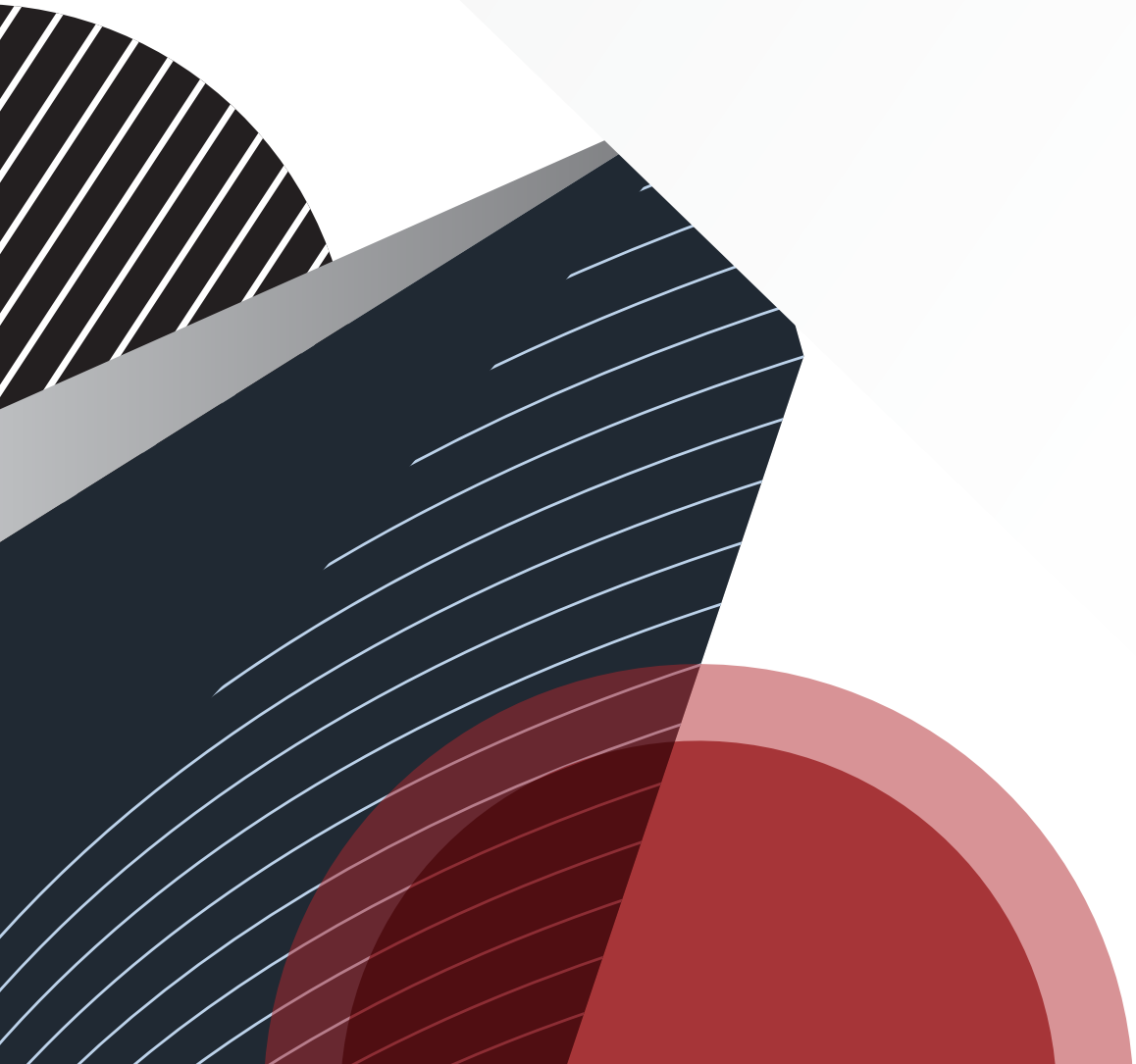
새로운 변화라고는 할 수 없지만, 스파이와 재정적 동기가 있는 공격자에 의한 오픈 소스 악성코드 사용이 계속 증가할 것으로 예상됩니다. 지능형 공격자가 공개적으로 사용 가능한 툴을 활용하는 이유는 다양하지만, 크게 두 가지를 들 수 있습니다. 첫 번째는 추적을 피하기 위한 의도이며, 두 번째는 개발 비용 절감입니다. 또한 Cobalt Strike와 같은 침투 테스트 프레임워크의 모듈 특성을 통해 공격자는 그들이 배포하는 페이로드에서 유연성을 구현할 수 있습니다. APT 및 FIN 그룹에서 사용하는 오픈 소스 악성코드의 예로는 NETWIRE, TRINITY, GHOST RAT, METERPRETER, ASPXSPY 등이 있습니다. 최근 몇 달 동안 특히 공격자들 사이에서 인기가 상승하고 있는 두 가지 플랫폼은 Cobalt Strike와 PowerShell입니다.

C&C에 대한 합법적인 서비스 남용

사이버 스파이와 경제적 동기가 있는 공격자는 적어도 2008년부터 사이버 작전 중 C2(명령 및 제어)를 목적으로 합법적인 인터넷 서비스를 남용했습니다. 대개 화이트리스트에 있는 합법적인 서비스를 활용하면 C2 트래픽을 탐지하기가 더 어려워지며, 공격자 측에서 추가 개발 및 인프라 오버헤드가 발생하지만 공격자와 악의적인 활동 사이에 또 다른 난독화 레이어를 확보할 수 있습니다. 2006년부터 2016년까지 C2에 합법적인 서비스를 사용한 악성코드 샘플의 비율을 FireEye에서 분석한 결과, 2008년 약 4%에서 2016년 약 9%로 증가했으며, 2019년 이후에도 계속 증가할 것으로 예상됩니다.

FireEye Mandiant와 협업

전자 상거래 웹사이트 및 기프트 카드를 표적으로 삼는 경제적 동기의 공격자가 급증할 것으로 예상됩니다.



신흥 국가들이 서로를 따라잡기 위해 각축을 벌이는 동안 러시아는 표적을 넓히고 있습니다

러시아의 공격자들이 ICS를 공격하려는 새로운 시도가 드러날 것입니다. 이러한 시도는 사실상 파괴적인 공격이라기 보다 툴의 테스트 또는 사전 작업일 수도 있지만, 지정학적 사건으로 인해 일부 지역 특히, 우크라이나 또는 다른 전 소련 공화국에서의 실제 공격이 일어날 가능성도 배제할 수 없습니다.

러시아는 미디어를 통해 불화의 씨를 뿌리거나, 전술적으로 데이터를 유출하고 해킹하는 등 더 은밀한 작전을 통해 영향력 작전을 계속 수행할 것입니다. 그러한 작전의 중점 지역 중 한 곳은 중동으로, 러시아는 GCC(걸프 협력 회의) 국가들(즉, 사우디아라비아 및 UAE)과 카타르, 미국 동맹국들 간에 분열을 만들어 내려는 목적을 가지고 있습니다.

우리가 지난 몇 년 동안 이란, 북한 및 베트남의 부상에서 보았듯이 2019년에는 다른 많은 사이버 국가들이 새롭게 부상할 것으로 예상합니다. 이들의 부상을 가속화시키는 주된 이유는 다른 나라들을 따라잡으려는 압박과 전통적인 군사 능력과 비슷한 수준의 사이버 프로그램을 개발해야 한다는 압박 입니다.

현재 이란 정부를 지원하는 것으로 드러난 새로운 공격 그룹의 능력이 다소 떨어지는 것을 확인하긴 했지만 이란의 많은 공격자들은 여전히 계속 역량을 향상시킬 것입니다. 따라서 이란의 정교함과 대량 공격의 성장 추세가 계속될 것을 예상할 수 있습니다.

POS(Point of Sale)에서 전자 상거래 환경으로의 지속적인 전환

기프트 카드 사기뿐만 아니라 전자 상거래 웹사이트에 대한 공격이 증가할 것으로 예상됩니다. 미국의 유통업계에서는 칩, 서명 및 모바일 결제(예: Apple Pay)로의 전환으로 인해 해커가 신용 카드 데이터를 도용하여 수익을 올리기가 더 어려워졌습니다. 당사가 협업한 여러 POS(Point of Sale) 침해 사례에서 은행들은 놀라울 정도로 낮은 사기 비율을 리포트했는데, 이는 공격자가 전체 마그네틱 선(트랙 2 데이터)을 보유하지 못했기 때문입니다.

전자 상거래 웹사이트 및 기프트 카드를 표적으로 삼는 경제적 동기의 위협 공격자가 급증할 것으로 예상됩니다. 2018년의 당사 조사에서 우리는 이미 공격자가 전자 상거래 "스키머"를 설치하여 PII(개인 신원 확인 가능 정보), 결제 카드 번호 및 CVV를 도용하는 것을 보았습니다. 범죄자가 이 데이터를 확보하면 불법 경로를 통해 정보를 구매 또는 판매하는 것이 상대적으로 쉬워집니다.

공격자의 표적이 되는 온라인 뱅킹 포털

온라인 뱅킹 포털 및 애플리케이션에 대한 공격은 더욱 정교해지고 있으며 2019년에는 사이버 범죄자들에게 더욱 매력적인 대상이 될 것입니다. 북미의 뱅킹 포털 2곳에 대한 최근의 공격을 보면, 공격자가 계정 등록 및 인증 워크플로우를 리버스 엔지니어링하는 데 상당한 시간을 투자한 것으로 드러났습니다. 그런 다음, 공격자는 카드 열거, 세션 손상, 무차별 대입(brute force) 및 암호 스프레이 기법을 결합하여 뱅킹 크리덴셜을 침해하고 단계별 인증을 우회하는 정교한 공격을 설계했습니다.

공격자가 계정에 액세스하면 온라인 이체를 시작하고 수표장을 주문하고 기존 거래 대상을 수정할 수 있었습니다. 대부분의 경우 일반적인 취약성 평가 실행에서는 이러한 취약성을 알아채지 못합니다. 해당 취약성을 파악하려면 보안 툴을 통해 사용할 수 있는 자동화된 방법보다 훨씬 더 집중적이고 사용자 지정된 접근 방식이 필요하기 때문입니다.

우리는 온라인 포털에 대한 대규모 계정 탈취 공격이 증가할 것으로 예상하며, 대규모 사기 사례를 관찰하게 될 것이라 예상합니다.

표적: 공급망

2019년에는 국가가 후원하고 금전적 동기를 가진 공급망 공격이 증가할 것으로 예상됩니다. 조직이 보안 환경을 향상시키고 전면 방어를 구축함에 따라 공격자는 표적 네트워크에 대한 접근 권한을 확보하려는 목적으로 타사 벤더, 고객 또는 파트너를 침해하는 방향으로 공략을 바꿀 것입니다.

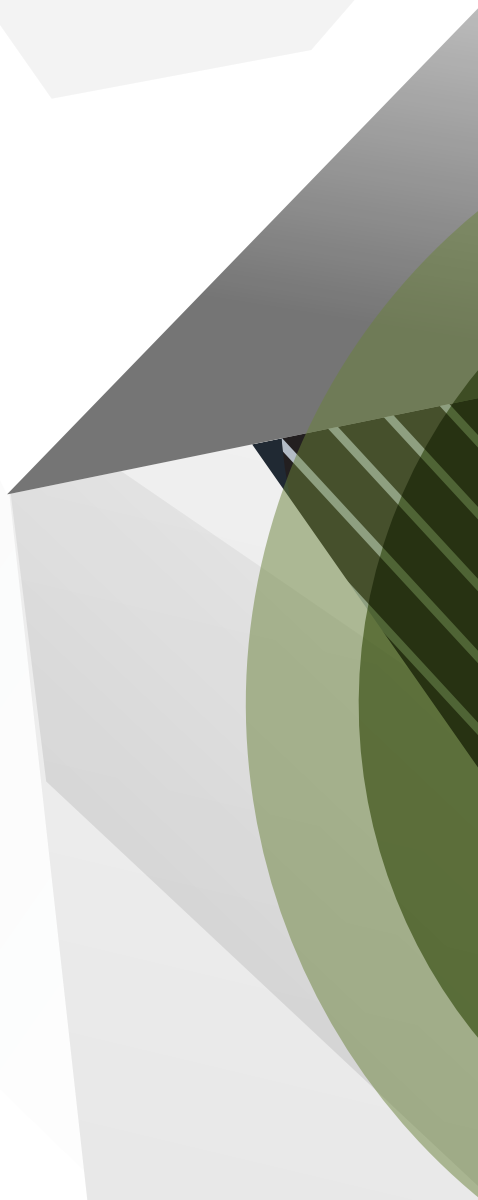
우리는 최근에 중국 스파이 그룹인 APT10이 캐나다와 미국의 서비스 제공업체를 침해하여 표적 네트워크에 대한 액세스 권한을 확보하는 것을 확인했습니다. 우리는 APT10이 오바마-시진핑 합의를 위반하지 않으면서, 비사이버 수단으로 비즈니스에 중요한 정보를 도용하고 표적 기술 절도하기 위해 미국 주요 기업의 공급망을 침해하는 데 집중하고 있다고 평가합니다. 또한 우리는 재정적 동기가 있는 공격자뿐만 아니라 북한의 라자루스(Lazarus) 및 중국의 APT31과 같이 국가가 후원하는 그룹에서 알려진 소프트웨어 개발 회사에 대한 대중들의 신뢰를 악용하여(인증서 도용) 탐지 컨트롤을 우회하는 데 사용하는 소프트웨어 기반 공급망 공격도 발견했습니다.

작년에 공개된 중요한 소프트웨어 공급망 이벤트는 7건이 있었습니다. 이러한 공격에는 합법적인 소프트웨어에 백도어를 포함하거나, 탐지를 우회하기 위해 훔친 인증서를 사용하여 악성 파일에 서명하거나, 소프트웨어의 업데이트 프로세스를 손상시켜 업데이트 프로세스 중에 악성 코드를 다운로드 및 실행하는 것이 포함될 수 있습니다.

공급망 공격은 탐지가 어렵기 때문에 대부분의 조직에서 제대로 관리하지 못하고 있으며, 현재 적용 중인 관행보다 훨씬 더 효과적인 리스크 관리가 필요합니다.

FireEye Labs의 시각

소셜 엔지니어링은 효과가 좋기 때문에 **가장 일반적으로 사용되는 공격 기법이며**, 연말은 항상 경각심을 가져야 할 시기입니다.



위협 환경이 진화함에 따라 보안도 발전함

기술이 끊임없이 진화하고 IoT가 시시각각으로 성장함에 따라 위협 환경이 기하급수적으로 팽창하고 있습니다. 결과적으로 이러한 위협에 맞서기 위한 기술 아키텍처의 일부로 새로운 방어 전략이 나타날 것입니다.

활성 코드를 악용 및/또는 실행하는 데 사용할 수 있는 코드 전송 및 기능의 활용은 최소화될 것입니다. Flash 및 Java와 같은 기능의 사용이 줄어듦에 따라 이미 진행 중에 있다고 볼 수 있습니다. 매크로는 물론, 문서 공유조차도 확실히 사라질 수 있습니다. 이러한 경향은 클라우드에 의해 활성화되고 "앱", "컨테이너" 서비스 등의 개념과 관련된 장치들로 보호됩니다. 본질적으로 비즈니스 생산성 및 협업은 그 어느 때보다 공개적으로 보이는 환경이지만 실제로는 고립된 가상 환경에서 이루어지며, 정보 및 콘텐츠의 흐름은 늘어날 것입니다.

또한 앞으로 IoT는 정보를 보다 적게 보유하고 리소스와 실제 기능을 보다 적게 활용할 것으로 예상됩니다. 미래의 IoT를 활용하는 공격은 매우 복잡하고 탐지 및 방어하기가 어려울 것입니다. 물론, 도움이 되는 차세대 엔드포인트, 네트워크, 클라우드 및 기타 보안 기술이 항상 새로 등장하겠지만, 힘겨운 싸움이 될 것입니다.

표적 공격에 활용되는 비즈니스 이메일 침해

소셜 엔지니어링은 효과가 좋기 때문에 가장 일반적으로 사용되는 공격 기법이며, 연말은 이를 특히 주의해야 하는 시기입니다. 우리는 모든 종류의 피싱 및 스피어 피싱 전술이 표적 공격에 활용되는 것을 목격할 것입니다. 구체적으로 말하면 CEO 사기 또는 BEC(비즈니스 이메일 침해) 사례가 더 많이 발생할 것으로 예상됩니다. 오늘날의 솔루션이 피싱 공격 및 기타 이메일 사기를 점점 더 성공적으로 탐지함에 따라 BEC가 급격히 증가할 것으로 예상됩니다. 따라서 직원들은 주요 인물로부터 이메일을 받을 때 특히, 이메일에서 특정한 행동을 지시 받을 때 더 경계해야 합니다.

새로운 기술을 사용하여 탐지 회피

작년의 FireEye 보안 전망 보고서에서 논의했듯이, 우리는 정교한 공격을 수행하기 위해 클라우드 기반 인프라를 선택하는 사이버 범죄자가 꾸준히 증가하고 있음을 보아왔습니다. 이는 2018년 내내 사실로 증명되었습니다. 그리고 2019년 이후에는 사이버 범죄자가 블록체인 및 AI와 같은 새로운 기술을 사용하여 공격을 탐지하기 어렵게 만들 것으로 예상됩니다.

또한 조직에 배포된 AI 기반 사이버 보안 제품의 수가 증가하고 보안 벤더들이 혁신을 통해 AI 기반 보안 신제품을 시장에 출시함에 따라 공격자는 그에 맞춰 행동을 조정하기 시작할 것입니다. 내년에는 공격자가 AI 솔루션을 회피하기 위해 정상 트래픽과 섞여 있는 위협 및 오해의 소지가 있는 데이터를 제공하여 머신 러닝 모델에 혼란을 주는 등의 새로운 기법을 사용할 것으로 예상됩니다.

기타 회피 기법

공격자는 2018년 내내 공격에 독특하고 독창적인 다양한 회피 기법을 활용했으며, 2019년에도 몇몇 새로운 획기적인 회피 방법들과 함께 해당 기법을 다시 사용할 것으로 예상됩니다. 기존에 성공하여 앞으로도 증가할 가능성이 있는 기술 중 하나는 암호로 보호된 공격입니다. 2018년에 우리는 암호화된 악성 첨부 파일과 해당 암호가 이미지로 함께 첨부되어있는 이메일을 보았습니다. 아무 의심 없이 이메일 상의 지시 사항을 따르고 첨부 파일을 열어본 사용자는 침해 당했습니다.

이렇게 암호화된 공격은 일단 뿌려놓고 잘 되기를 바라는 방법 중 하나이긴 하지만, 이와 유사한 경향이 표적 공격의 트렌드를 지배하게 될 것입니다. 공격자는 보안 벤더의 탐지를 회피하기 위한 새로운 방법을 지속적으로 도입할 것입니다. WMI 기반 쿼리를 사용하여 실행 환경을 프로파일링하는 것은 올해 표적 공격에서 자주 등장했습니다. 이 방법은 많은 성공을 거두었기 때문에 내년에도 다시 사용될 것임이 분명합니다. 또한 공격자는 해당 공격에서 GeoIP 및 사용자 에이전트 기반 회피는 물론, 보안솔루션을 피하기 쉬운 새로운 파일 형식을 계속 사용할 것입니다. 마지막으로, 공격자는 샌드박스 환경을 타파할 새롭고 획기적인 방법을 찾을 것으로 예상됩니다.

글로벌 통찰력

APAC

기술을 보유하고 있지만
리소스가 부족한 국가
지원 공격자 및 숙련된
개별 공격자의 영향은
**보안의 발전 속도를
따라잡지 못한 조직에서
더욱 강력하게 느껴질
것입니다.**

2020년 도쿄 올림픽에 대한 시각

지금까지의 경향으로 보았을 때, 일본의 기업 및 조직을 표적으로 삼는 위협 활동이 2019년 내내 증가하며, 2020년 도쿄 올림픽이 개최될 때까지 지속될 것으로 예상됩니다. 표적이 될 것으로 예상되는 산업에는 중요한 인프라, 미디어 및 방송, 정부, 관광 및 숙박, 지역 및 국제 올림픽 조직위원회 등이 포함됩니다. 우리가 경계하고 있는 위협 활동으로는 피싱 및 가짜 티켓 웹사이트부터 DDoS(분산된 서비스 거부) 공격, 랜섬웨어 배포 및 지적 재산 도용에 이르기까지 다양합니다.

또한 북한 및 중국과 같은 국가는 일본에 관심이 많으므로 이러한 국가의 공격자가 주요 이벤트 이전에 정찰을 수행하고 방어를 테스트할 것으로 예상할 수 있습니다. 2012년 런던 하계 올림픽은 표적이 되었고, 2016년 리우데자네이루 올림픽도 마찬가지였으므로 이러한 패턴이 지속될 가능성이 큽니다.

위협의 진화

2019년에는 숙련도가 떨어지는 공격자도 더 나은 소셜 엔지니어링 및 더 우수한 툴을 사용하여 광범위한 표적에 액세스할 것으로 예상됩니다. 현금 없는 사회로의 지속적인 전환으로 낮은 가치의 절도를 탐지하기 더 어려워지며, 대형 은행 조직은 낮은 가치의 절도를 막기 위해 큰 노력을 기울이기보다 그 비용을 갚아줌으로써 문제를 관리하는 것이 더 저렴하다는 사실을 알게 될 것입니다. 보안이 강화된 조직이 아니라 개인을 표적으로 삼는 데서 계속 이익을 추구하는 범죄자도 등장할 것입니다.

기술을 보유하고 있지만 리소스가 부족한 국가 지원 공격자 및 숙련된 개별 공격자의 영향은 보안의 발달 속도를 따라잡지 못한 조직에서 더욱 강력하게 느껴질 것입니다. 이러한 조직에서 대량의 데이터를 탈취해가는 사례가 증가할 것으로 예상됩니다.

고도로 숙련되고 경험 많은 공격자는 성숙한 스파이/범죄 계층으로 이동합니다. 이들은 탐지 및 저지가 훨씬 더 어렵습니다. 중국 및 러시아의 공격자들은 작전을 두드러지게 확장할 것입니다. 그러나 상용 소프트웨어의 사용과 시스템에 대한 액세스를 유지하고자 하는 움직임은 자신이 누구이며 무엇을 원하는지를 숨기는 데 더욱 중점을 둘 것임을 의미합니다.

글로벌 통찰력

EMEA

공격자에 대한 추적으로 사이버 범죄 활동은 실행하기가 더 어려워지며 **이로 인해 어느 정도의 억제력이 생길 수 있습니다.**

소셜 미디어의 어두운 면

2017년 및 2018년 우리는 소셜 미디어가 개인, 정당 및 국가가 주도하는 정보 작전 및 허위 정보 유포를 위한 플랫폼으로 사용되는 것을 목격했습니다. 이와 관련하여 미국 의회, EU 및 영국에서 많은 토론과 청문회가 진행되었지만 그다지 성과를 거두지 못했습니다.

2018년 하반기에 FireEye는 소셜 미디어와 관련된 광범위한 정보 작전 네트워크(이란의 정치적 이익에 의해 추동되는 것으로 추정됨)를 발표했습니다. 우리는 2019년 EMEA 전역에서 예정된 선거에서 특정 국가 또는 지역에 전략적 관심이 있는 국가가 정보 작전을 펼칠 것이며, 이때 소셜미디어를 중요한 플랫폼으로 사용할 것으로 예측합니다. 정보 작전의 목표는 특정한 외교 정책에 대해 우호적인 특정 정당을 홍보하거나 정치적 담화를 촉진하여 국가 내부의 갈등을 일으키는 것일 수 있습니다.

2019년에는 주요 국가에 대해 정보 작전이 대규모로 수행되는 것은 물론, APAC뿐만 아니라 동유럽에서까지 미디어 및 소셜 네트워크에 지역 갈등에 대한 영향력이 행사될 것으로 예상됩니다. 이러한 유형의 캠페인은 그 특성으로 인해 탐지가 더 어려우며 사이버 보안 회사 및 정부가 작성자를 탐지 및 저지하기는 어려울 것입니다. 귀속관계 추적이 핵심이 될 것입니다.

리소스 부족이 위험을 초래

EMEA에 대한 지난해의 예측에서 우리는 보안 리소스 부족의 심화에 대해 이야기했습니다. 기업은 자격을 갖춘 보안 전문가를 고용하는 데 계속 어려움을 겪고 있습니다. 따라서 우리는 조직이 계속 아웃소싱 또는 외부 기업 고용을 통해 보안 강화에 도움을 받는 것을 볼 수 있습니다.

아웃소싱 및 타사 관리 서비스 제공자와의 제휴는 기업이 자체 사이버 방어 역량을 완성하는 데 도움이 될 수 있지만 벤더 또는 보안서비스 제공자의 역량을 평가하지 않으면 침해의 위험이 커질 수 있습니다. 최근 몇 년간 우리는 조직력이 다소 떨어지는 사이버 범죄자뿐만 아니라 사이버 스파이 위협 그룹이 임무를 수행하기 위해 (관리) 서비스 제공자, 보안 제공업체, 계약업체 및 아웃소싱 회사를 표적으로 삼는 데 관심이 증가하는 것을 보았습니다.

공급망(벤더와 소프트웨어 모두)을 표적으로 삼는 이러한 추세는 계속될 것으로 예상되므로, 기업은 제품, 제공업체 및 잠재적 소프트웨어에 대한 보안 평가를 수행하여 제공자, 벤더 또는 공급업체 내부의 사이버 보안 성숙도를 평가 및 이해하는 것이 좋습니다.

전투는 귀속관계 추적으로 시작

2018년 8월, 미국 법무부(Department of Justice)는 FIN7의 멤버 3명을 구금했다고 발표했습니다. 침입 데이터의 적절한 수집, 위협 연구, 사고 대응 및 보안 회사 간 공유가 귀속관계 추적을 어떻게 개선하여 결과적으로 사이버 범죄자를 실제로 체포할 수 있는지에 대한 중요성을 강조했기 때문에 **FIN7 멤버의 체포는 특별한 의미가 있습니다**.

특히 동유럽은 강력한 사이버 범죄의 오랜 역사를 지니고 있습니다. 사이버 범죄는 실제로 국경이 없지만, 체포를 수행하는 데 관심이 적거나 다른 나라에 범인을 인도하는 국제 협약이 없는 국가들은 분명 존재합니다.

귀속관계 추적으로 사이버 범죄 활동은 점점 실행하기가 더 어려워지며 이로 인해 일정 수준의 억제력이 생길 수 있습니다. 2019년에는 신뢰할 수 있고 정확한 귀속관계를 기반으로 사이버 범죄 에코시스템에서 더 많은 검거가 이루어질 것으로 예상됩니다. 사이버 범죄자와 맞서 싸우는 지속적인 활동에서 사이버 보안(특히, 사이버 위협 인텔리전스)이 귀속관계를 제공함으로써 기업, 정부 및 법 집행 기관을 지원하는 것이 중요합니다.

중요한 인프라 공격이 예상됨

2017년 말에 우리는 "**TRITON**"이라고 하는 새로운 ICS 공격 프레임워크의 발견을 발표했습니다. TRITON은 주요 기반시설에 대한 지속적인 위협을 보여주기 때문에 이 보고서에서 다룰만한 가치가 있습니다.

주요기반시설에는 다양한 것들이 포함되는데, EMEA의 경우에는 국가 간 인프라이기도 하며, 에너지, 전력 또는 자원 채굴도 포함합니다. 2019년에는 주요 기반시설에 대한 위협이 증가할 것으로 예상됩니다. 이러한 환경에는 정보 기술과 운영 기술을 통합하는 보안 전략이 없기 때문에 사이버 공격이 주요 기반시설 내에서 서비스의 중단 또는 파괴를 일으킬 수 있습니다.

또한 우리는 공격자가 비즈니스를 방해하거나, 금전을 요구하거나, 지정학적인 동기를 가지고 있거나, 자신의 능력을 과신하기 위해서 운영 기술 네트워크에 직접적인 방해를 시도하는 것을 계속 경험하게 될 것입니다. 그 다양성과 대륙 전체에 걸쳐 설치된 공장의 규모로 인해, 2019년에 유럽은 이러한 공격의 표적이 될 것입니다. 우리는 보안 및 포렌식을 수행하기 어려운 매우 오래된 플랫폼에서 공격자를 보게 됩니다.

ICS에 크게 의존하는 국가 및 회사는 위협을 발견해서 복구하는 데까지의 시간을 줄이고, 적절한 보안 대책을 마련하여 가능한 한 빨리 위험을 파악하는 것이 매우 중요합니다.

글로벌 통찰력
LATAM

라틴 아메리카 및 아프리카와 같은 지역은 보다 영향력이 큰 공격의 표적이 될 것이며 전 세계 언론 매체에 보도될 만큼 주요한 공격이 발생할 수 있습니다.

한눈에 보는 LATAM 위협 환경

사이버 범죄, 사이버 스파이 및 핵티비즘은 이 지역에 영향을 미치는 주요 위협 중 일부로, 2019년까지 지속될 것으로 예상됩니다. 내년에는 라틴 아메리카를 공격하는 그룹이 TTP를 개선하여 다양한 캠페인을 실행할 것으로 예상됩니다. 스피어 피싱은 지속적인 주요 공격 경로일 것입니다. 그러나 통신 장치 및 IoT 장치에 중점을 둔 공급망 공격과 최종 사용자 공격 역시 증가할 것으로 예상됩니다.

발전된 TTP는 금융 및 제조 산업에 대한 공격에 사용될 가능성이 매우 큽니다. 그러나 정부, 하이테크, 및 서비스 산업도 공격 범위 내에 있으며 특히, 하이테크 및 서비스 산업은 공급망 공격의 표적이 될 가능성이 높습니다.

중국에서 제조되어 변조된 하드웨어와 관련된 사고들을 생각하면, 중국이 라틴 아메리카에 분명한 위협을 불러일으킬 것임을 알 수 있습니다. 북한, 러시아, 이란은 일반적인 활동을 계속할 것이며, 아프리카 및 라틴 아메리카의 사이버 범죄 그룹이 더 발전할 것입니다.

라틴 아메리카 및 아프리카와 같은 지역은 보다 타격이 큰 공격의 표적이 될 것이며 이러한 사실은 전 세계 언론 매체에 보도될 만큼 충분히 의미가 있을 것입니다. 이로 인해 해당 지역에 진출해 있는 회사는 보안 투자를 증대하게 되고 현지 정부는 더 많은 법률 및 규정을 시행하게 됩니다. 더 새로운 공격 그룹이 프로파일링될 가능성이 있고, 그로 인해 위협이 감소할 수도 있습니다.

2019년에 위협보다 앞서 대처하려면 **조직은 준수 기반 접근 방식에서 보안 기반 접근 방식으로 전환하기 시작해야 합니다.**

현재 과제 및 앞으로의 과제

보안 업체로부터 조언을 받는데도 불구하고 기업은 실제로 보안 환경을 완성하기보다는 준수하는 데 더 중점을 둘 것으로 예상됩니다. 조직의 수장의 역할을 하는 리더가 미디어에 보도되는 공격의 증가에 점점 더 관심을 갖게 되기만을 바랄 뿐입니다. 이를 통해 조직이 그러한 공격에 맞설 준비가 되었는지에 대한 질문을 제기하게 될 것입니다.

보안에 정통한 조직이 새로운 위협에 대해 이해하고 맞서며 신속하게 적응할 수 있는 인력을 채용하는 데 더 적극적으로 나서서 선점하기 때문에 일반적인 조직이 경험하고 있는 보안 전문가의 부족은 내년에도 계속 심화될 것입니다. 이러한 인력 부족 현상은 더 많은 조직들이 보안 태세를 제대로 완성하고자 함에 따라 계속 악화 일로를 달릴 것입니다.

또한 2019년에는 공격자가 임무를 완수하는 데 필요한 시간을 훨씬 초과하는 기간(체류 시간)에도 환경에서 탐지되지 않은 채 계속 작전을 벌일 것으로 예상됩니다. 이뿐만 아니라, 데이터 보호, 사고 대응, 보안 인식 및 교육 등이 조직 내부에서 가장 취약한 역량임을 고려하면 공격자는 시스템에 더 쉽게 숨어있을 수 있습니다. 이 추세는 2019년에도 계속될 것입니다.

위협에 앞서 나아감

2019년에 위협보다 앞서 대처하려면 조직은 준수 기반 접근 방식에서 보안 기반 접근 방식으로 전환하기 시작해야 합니다. 여기에는 공격 라이프사이클의 다양한 단계에서 공격을 탐지하는 기능을 구현 및 활성화하고, 사고에 맞춰 신속하게 조정하고 대응하는 전략을 개발하여 비즈니스 영향을 최소화하는 것이 포함됩니다.

또한 조직은 공격자를 차단하는 제어 기능을 구현하는 방법을 고민하지 말고 공격자가 네트워크 및 환경에 있을 때 즉시 해당 공격자를 탐지하는 제어 기능을 구현하는 방법을 고민하기 시작해야 합니다. 그런 다음, 보안 팀은 적절히 대응하여 영향을 최소화하는 교육을 받아야 합니다. 사고가 해결되면 조직은 해당 사고의 핵심 사항을 기반으로 자체 역량을 가다듬는 데 집중해야 합니다. 예를 들어, 신뢰할 수 있는 일련의 제어 기능을 다른 유사한 프로세스에 적용할 수 있어야 합니다.

조직은 2019년 내내 엔드포인트 보호 개선을 위해 노력하고 그로 인한 이점을 활용해야 합니다. 솔루션은 더 많은 행동 기반 탐지를 가능하게 합니다. 하지만 이를 위해서는 인텔리전스를 공급해야 합니다. 사용 가능한 대량의 인텔리전스가 있는 조직과의 협력은 위협과 맞서는 데 상당한 이점을 제공합니다.

2019년과 그 이후

우리는 2019년에 기대할 것이 많습니다. 하지만, 해결해야 할 것도 많으며 CEO인 Kevin Mandia 씨가 말씀했듯이 명확하게 이해해야 할 내용도 많습니다.

귀속관계 및 책임은 사이버 공간상의 전쟁에서 승리하기 위해 극복해야 하는 난제 중 가장 큰 두 가지 요소입니다. 인터넷에서 악의적인 활동을 수행하는 데 위험 및 영향이 없으면 공격자는 공격을 계속하고 조직은 계속 침해 당할 것입니다. 해킹에 대한 최근의 기소로 앞으로 일어날 상황에 대해 약간의 희망을 품게 되었지만, 해마다 발생하는 침해의 수를 줄이기 위해서는 이런 면에서 더 많은 진전이 이루어져야 합니다.

클라우드는 조직에 상당한 기회를 제공합니다. 2019년으로 나아가면서 클라우드로의 마이그레이션은 계속 확대될 것입니다. 또한 클라우드를 표적으로 삼는 공격도 더 많이 일어날 것으로 예상됩니다. 클라우드의 보안이 다소 미흡하기 때문이 아니라 공격자는 그야말로 데이터가 있는 곳이면 어디든 따라가기 때문입니다. Martin Holste 씨가 이야기했듯이, 클라우드 보안은 적절한 질문을 하는 것과 관련된 문제입니다. 클라우드에서 원격으로 일어나는 의심스러운 행동 및 활동에 대해 추가 조치를 취하는 것도 도움이 됩니다.

항공기 해킹이 실현 가능하다고 간주하는 것을 상상하기 힘들지만, 항공 산업에는 사이버 스파이, 고객 정보 도용, 불법 티켓 판매, 랜섬웨어 및 DoS(서비스 거부) 공격을 통한 강탈을 비롯하여 고려해야 할 많은 사이버 문제가 있습니다. 아마도 이러한 모든 문제로 인한 가장 큰 결과는 신뢰 약화 및 항공 여행에 대한 두려움이며, 이는 항공 산업에 침해보다 더 심각한 영향을 끼칠 수 있습니다.

안타깝게도 모든 것을 위한 빠른 해결책은 없습니다. 있다면, 전 세계의 수백만 사이버 보안 전문가가 고군분투할 필요가 없을 것입니다. 우리는 한 번에 한 걸음씩 걸어야 합니다. 즉, 적절한 기술을 개발하여 간단한 작업을 자동화하고, 숙련된 보안 직원을 육성하여 중요한 경보에 대해 후속 조치를 취하며, 사이버 공간에서의 공동 개입 규칙에 관한 원칙을 발표해야 합니다.

우리는 이러한 비전을 완전히 수용하고 2019년 이후에도 이러한 책임을 다할 것이라 기대합니다.

FireEye에 대한 자세한 정보: **www.FireEye.com**

FireEye Korea
서울 특별시 강남구 테헤란로 534 글라스타워 20층
02.2092.6580 korea.info@fireeye.com

FireEye, Inc. 소개

FireEye는 인텔리전스 기반의 보안 회사입니다. FireEye는 혁신적인 보안 기술, 국가 수준의 위협 인텔리전스 및 세계적으로 유명한 Mandiant® 컨설팅을 결합한 단일 플랫폼을 제공하여 고객 보안 운영의 완벽한 확장을 지원합니다. 이를 통해 FireEye는 사이버 공격에 대비하고 이를 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 줄이고 간소화합니다.

SP-EXT-RPT-KO-KR-000088-01