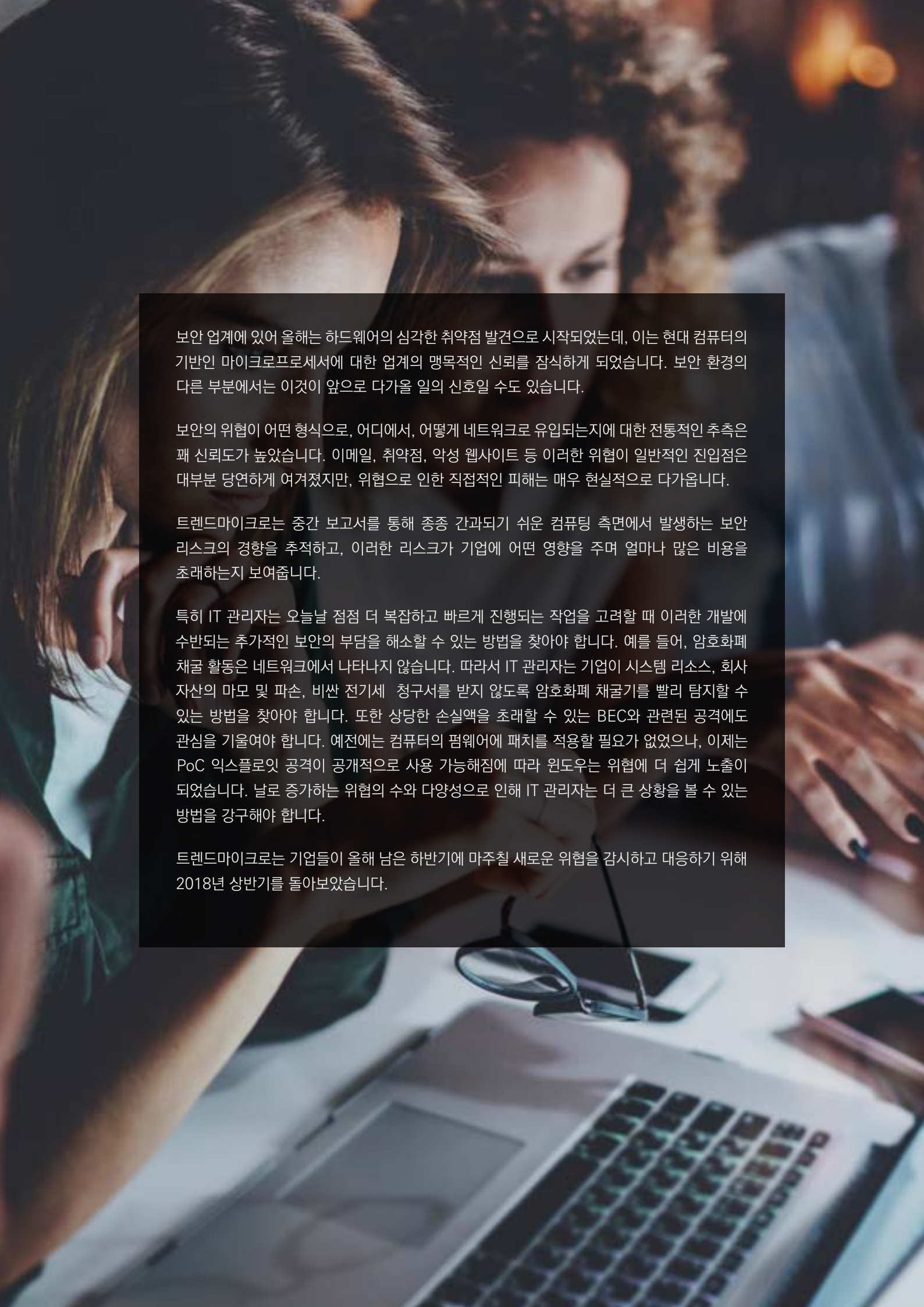
보이지 않는 위협, 잠재적인 손실

트렌드마이크로 2018 중간 위협 보고서

Cover image: SFIO CRACHO/Shutterstock.com

For Raimund Genes (1963-2017)

Contents



보안 업계에 있어 올해는 하드웨어의 심각한 취약점 발견으로 시작되었는데, 이는 현대 컴퓨터의 기반인 마이크로프로세서에 대한 업계의 맹목적인 신뢰를 잠식하게 되었습니다. 보안 환경의 다른 부분에서는 이것이 앞으로 다가올 일의 신호일 수도 있습니다.

보안의 위협이 어떤 형식으로, 어디에서, 어떻게 네트워크로 유입되는지에 대한 전통적인 추측은 꽤 신뢰도가 높았습니다. 이메일, 취약점, 악성 웹사이트 등 이러한 위협이 일반적인 진입점은 대부분 당연하게 여겨졌지만, 위협으로 인한 직접적인 피해는 매우 현실적으로 다가옵니다.

트렌드마이크로는 중간 보고서를 통해 종종 간과되기 쉬운 컴퓨팅 측면에서 발생하는 보안 리스크의 경향을 추적하고, 이러한 리스크가 기업에 어떤 영향을 주며 얼마나 많은 비용을 초래하는지 보여줍니다.

특히 IT 관리자는 오늘날 점점 더 복잡하고 빠르게 진행되는 작업을 고려할 때 이러한 개발에 수반되는 추가적인 보안의 부담을 해소할 수 있는 방법을 찾아야 합니다. 예를 들어, 암호화폐 채굴 활동은 네트워크에서 나타나지 않습니다. 따라서 IT 관리자는 기업이 시스템 리소스, 회사 자산의 마모 및 파손, 비싼 전기세 청구서를 받지 않도록 암호화폐 채굴기를 빨리 탐지할 수 있는 방법을 찾아야 합니다. 또한 상당한 손실액을 초래할 수 있는 BEC와 관련된 공격에도 관심을 기울여야 합니다. 예전에는 컴퓨터의 펌웨어에 패치를 적용할 필요가 없었으나, 이제는 PoC 익스플로잇 공격이 공개적으로 사용 가능해짐에 따라 윈도우는 위협에 더 쉽게 노출이 되었습니다. 날로 증가하는 위협의 수와 다양성으로 인해 IT 관리자는 더 큰 상황을 볼 수 있는 방법을 강구해야 합니다.

트렌드마이크로는 기업들이 올해 남은 하반기에 마주칠 새로운 위협을 감시하고 대응하기 위해 2018년 상반기를 돌아보았습니다.

심각한 취약점이 하드웨어에서 발견됨에 따라 취약점 패치는 더욱 어려워졌습니다

CPU 펌웨어의 고질적인 결함들로 패치의 적용 문제가 가중됩니다.

지난 1월, 구글은 공격자들이 이전에는 접근하기 어렵다고 생각했었던[1] 민감한 정보에 액세스할 수 있도록 길을 열어주는 심각한 마이크로프로세서의 취약점을 발견했다고 발표했습니다. 멜트다운 (CVE-2017-5754) 및 스펙터 (CVE-2017-5753, CVE-2017-5715)가 악용하는 취약점은 특정 마이크로프로세서[2]의 CPU 명령어 사용과 관련된 결함입니다. 멜트다운은 1995년 출시된 모든 Intel 프로세서를 사용하는 데스크톱 및 노트북 (2013년 이전 Intel® Itanium® 및 Intel Atom® 프로세서 제외)을 비롯한 컴퓨팅 장치에 영향을 미칩니다.[3] 스펙터의 경우 x86 (Intel 및 AMD) 및 ARM 기반의 프로세서를 실행하는 장치가 영향을 받습니다.[4]

특정 운영 체제나 특정 소프트웨어 버전에 한정되고 하나의 공급업체에서 해결할 수 있는 일반적인 소프트웨어 취약점과 달리, 멜트다운과 스펙터는 대규모의 기업 네트워크에 또 다른 과제를 제시합니다.

해당 결함의 발견은 전체 컴퓨팅의 에코시스템이 오랫동안 취약해 있었음을 의미합니다. 또한 설계 결함은 현대 컴퓨터의 기능에 매우 기본적이고 필수적인 부분에서 일어났으므로 이와 함께 유사한 유형의 취약점이 또 존재할 가능성이 높습니다. 사실상 취약점이 발표된 5개월 후 스펙터와 유사한 취약점인 Speculative Store Bypass 결함이 공개되었습니다.[5] 따라서 앞으로의 컴퓨터 산업은 이러한 결함의 지속적인 발견을 겪게 될 것입니다.

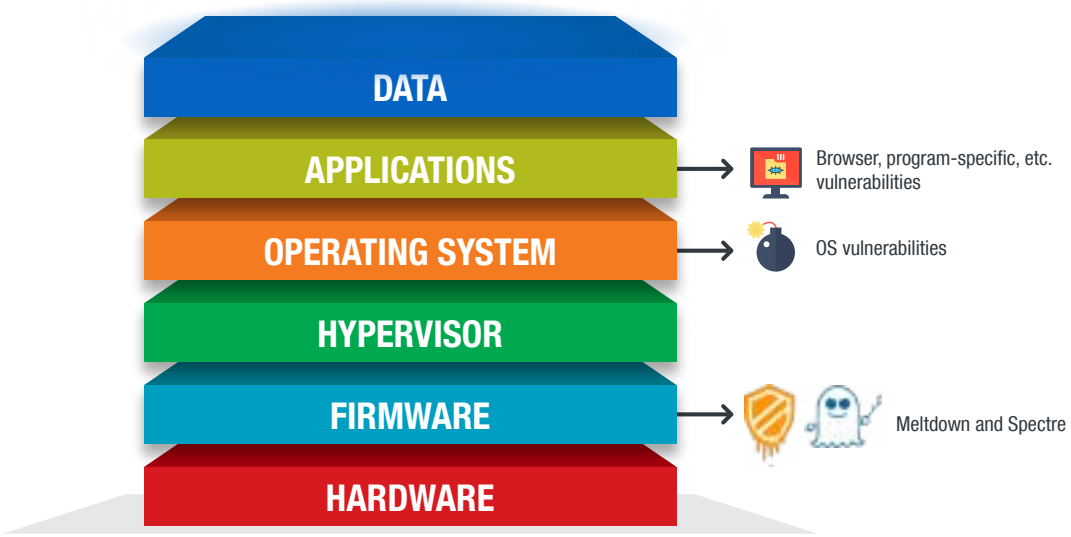


그림 1. 샘플 컴퓨팅 스택의 다이어그램 및 취약점:
멜트다운 및 스펙터는 일반적인 소프트웨어 취약점보다 컴퓨팅 스택에 더 깊이 존재합니다.

그러나 공급업체들이 어떠한 공격도 발견되지 않았다고 거듭 주장해 왔음에도 불구하고 이제 공격자들은 이전보다 더 면밀하게 컴퓨팅 스택의 취약점 측면을 살펴봐야 한다는 점을 알게 되었다는 것이 더욱 우려되는 부분입니다. 이러한 우려점에 대한 증거는 안티바이러스 테스트 회사의 멀웨어 데이터베이스에 멜트다운 및 스펙터에 관련된 샘플이 출현했다는 점입니다.[6] 비록 샘플의 수가 적지만 해당 공격의 영향을 받는 공급업체의 거대한 시장 점유율을 놓고 본다면, 결코 무시할 수 없는 사실입니다.

IT 관리자의 입장에서 네트워크의 모든 컴퓨팅 장치를 패치하는 것은 필수이지만 이는 절대 쉽지 않은 일입니다. 여러 마이크로프로세서 공급업체, 운영 체제 개발자 및 심지어 결함의 해결 방법이나 부분적인 완화를 제공할 수 있는 브라우저 제조업체까지 관여되어 있어 각기 다른 롤아웃 전략 및 일정으로 인해 모두 관리하는 것은 힘든 일입니다.

또한 IT 관리자는 패치를 설치하기 전 보안과 시스템 성능 중 어떤 것에 더 중점을 두어야 하는지 결정해야 합니다. 멜트다운 및 스펙터에 대한 패치 적용 후 마이크로소프트의 시스템 성능 연구처럼 구형 운영 체제를 실행하는 컴퓨터는 시스템 성능이 현저히 저하되는 경우가 있습니다.[7] 심지어 최신 시스템 또한 부팅이 가능하지 않게 될 수 있습니다.[8]

레거시 시스템과 구형 시스템 또한 위험에 노출되어 있습니다. 따라서 시스템 업그레이드가 필요한 의료 기관을 비롯하여 사용 편의성이나 실용성을 유지하기 위한 경향이 있는 업계에서는 내부의 보안 전략을 검토해야 합니다.

Adobe, Foxit, Microsoft가 차지하는 취약점 권고 건수

취약점 조사는 보안 환경의 전반적인 상태를 확인하기 위해 매우 중요합니다. 취약점 연구원들은 영향을 받는 소프트웨어 공급업체의 즉각적인 솔루션과 반응을 이끌어낼 플랫폼을 보유하고 있습니다. 2018년 상반기의 경우 ZDI (Zero Day Initiative)에 기여하는 3,000명 이상의 연구원들이 602건의 취약점 권고를 발행하였으며 (전년도 하반기의 수는 578건), 이 중 단 23개의 건수만 공급업체의 조정 일정을 초과하여 공급업체의 정식 패치나 대응책 없이 발행이 되었습니다.

취약점 권고를 가장 많이 받은 업체는 SCADA (Supervisory control and data acquisition) HMI (Human-machine interface) 소프트웨어 공급업체인 Advantech였습니다. 가정 및 사무실 소프트웨어 공급업체의 경우 가장 많은 취약점 권고를 받은 곳은 Adobe였으며, 여러 Adobe 제품 중에서 Adobe Acrobat Pro DC는 ImageConversion 프로세스용으로 가장 많은 수의 권고를 받았습니다. 또한 또 다른 PDF 리더로 널리 알려진 Foxit은 자체적인 취약점을 가지고 있었습니다. 마이크로소프트의 경우 약 3분의 1의 취약점이 Internet Explorer 및 Edge 브라우저와 관련이 있는 반면 나머지는 대부분 Windows에 있었습니다.

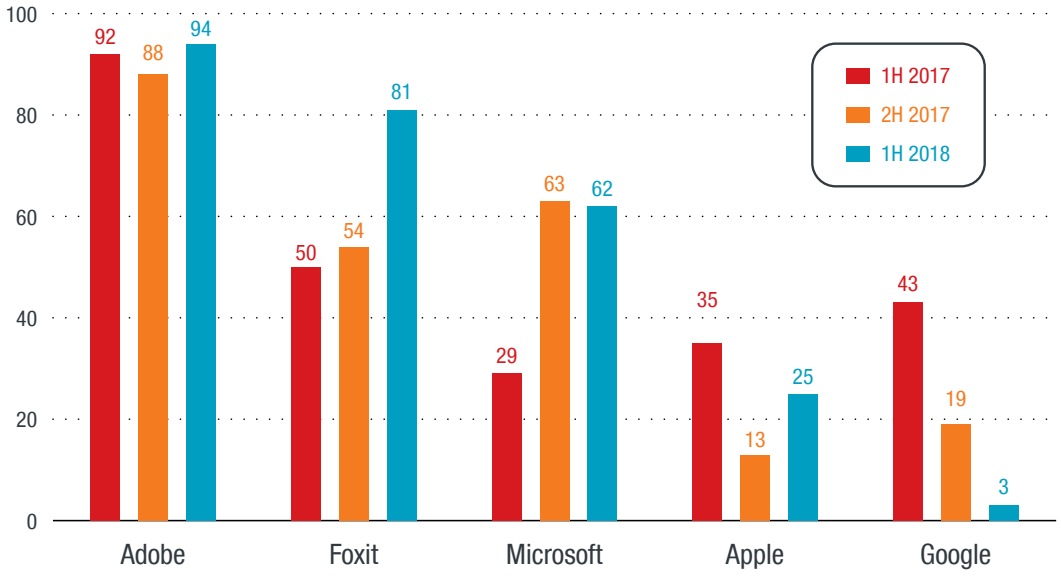


그림 2. 2018 상반기 동안 발견된 취약점 수에 대한 공급업체 별 (non-SCADA) 비교: 가정 및 사무실 소프트웨어 공급업체 중에서 가장 많은 취약점 자문을 받은 Adobe

기업의 취약점은 계속해서 존재하겠지만, 이러한 사실이 습관처럼 변해 안주감에 빠져서는 안됩니다. 지난 5월, Rig 익스플로잇 키트는 Microsoft Office 및 Internet Explorer에 양향을 미치는 Windows VBScript 엔진의 원격 코드 실행 버그를 사용하였습니다.[9,10] 해당 취약점이 공개된 지 35일 후와 Microsoft의 정식 패치가 이루어 진지 17일 후에 일어난 일입니다.[11] 또한 Rig는 Adobe Flash[12]에서 Use-after-free 버그를 사용하였고, 나중에는 Magnitude 및 Grandsoft와 같은 다른 익스플로잇 키트도 CVE-2018-8174를 사용하기 시작했습니다.[13]

이렇듯 새롭게 발견된 취약점에 대한 공격자들의 맹렬한 공격으로 기업은 보안 업데이트로 따라잡기 훨씬 어려워졌습니다. 종종 취약점의 개수와 네트워크를 이용 가능한 상태로 유지해야 함에 따라 기업은 특정 취약점에 더 집중하고 다른 취약점에 대한 개방 패치를 남기는 실질적인 절충안을 따를 수밖에 없습니다. 따라서 기업은 공격이 알려지거나 발견된 시점과 패치가 발행되는 날 바로 패치를 해야 할 만큼 취약점이 심각한지의 중요도에 크게 의존할 수밖에 없는 각각의 개별적인 노출창을 가지고 있습니다. 사이버 범죄자들은 항상 익스플로잇 공격을 행하기 쉽고 광범위한 취약점을 노리고 있기 때문에 기업은 항상 올바른 보안 정책을 유지하여야 합니다.

30% 증가한 SCADA 취약점 권고

취약점 연구원들은 2018년 지금까지 상당히 많은 수의 SCADA 관련 취약점을 발견하였으며, 이는 지난해의 반년 동안 발견된 것보다 30%나 증가한 수치입니다. 다행히도 공급업체의 조정 기간이 초과된 경우 발표된 취약점 권고의 수가 크게 감소하였고, 이는 공급업체가 해당 문제에 대한 패치 또는 트렌드마이크로 ZDI의 권고와 함께 해당 취약점 문제를 완화하였기 때문입니다.

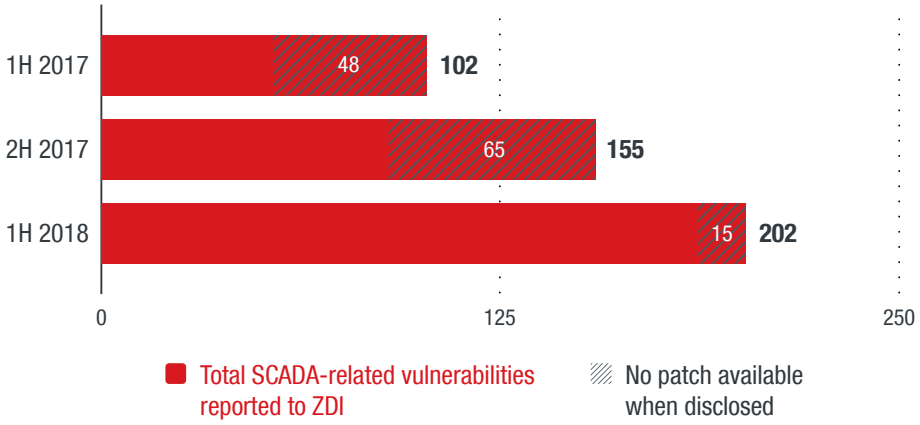


그림 3. 공개된 SCADA 취약점 비교:
2018년 상반기 더 많은 SCADA 취약점이 공개됨

특히 SCADA 관련 취약점 중 65%가 웹 기반의 HMI 소프트웨어 Advantech WebAccess에서 발견되었습니다. SCADA HMI는 중요한 인프라를 관리하고 서로 다른 제어 시스템의 상태를 감시하는 주요 디지털 허브로, 발전소 운영을 직접 제어합니다. 일반적으로 개별 프로세스에 대한 접근은 제한적이지만, 생산 목표 또는 가치 목표를 보내고 특정 운영에 대한 진단 데이터를 수집할 수 있습니다. 이런 점에서 HMI에 나타난 데이터는 공격자가 정찰할 만한 가치를 지니고 있다고 볼 수 있습니다. 다른 극단적인 경우 공격자가 중요한 설정을 변경할 수 있으며, 가능성은 적지만 장비 및 속성 또한 손상시킬 수 있습니다.

SCADA 시장은 전 세계 14개 대형 및 소규모 공급업체에 매우 활성화되어 있으며,[14] 이러한 공급업체의 중점은 종종 실제 산업 장비인 비즈니스의 더 수익성이 높은 측면에 맞추어져 있습니다. 트렌드마이크로의 연구에 따르면, 이로 인해 발견된 SCADA 관련 취약점의 해결은 평균적으로 약 150일이 걸릴 수 있습니다.[15] 또한 해당 기간은 소프트웨어 패치 적용의 문제가 될 수 있습니다.

네트워크 및 정보 시스템 보안 (NIS Directive)에 대한 새로운 지침에 따라, 유럽연합 지역의 중요 인프라 IT 관리자에게 있어 SCADA의 보안 취약점을 해결하는 것은 특히 중요해질 것입니다.[16] 해당 지침은 사고 대응 팀과 협력 그룹을 설립하고 보안 문화를 정착시켜 꾸준한 운영을 보장하도록 요구하고 있으며, 이는 EU 회원국 내 서비스를 운영하는 모든 기업에 적용됩니다. 지침을 준수하지 않을 경우 GDPR (General Data Protection Regulations)과 같은 무거운 벌금이 부과될 수 있습니다.[17] (GDPR 벌금: 최대 2000만 유로 또는 회사의 전세계 연간 매출액의 4% 중 더 높은 금액)[18]

랜섬웨어의 위협이 아직 남아 있는 현시점에 가상화폐 악성 채굴 탐지 건은 두배 이상 올랐습니다

최고조에 달한 가상화폐 채굴 탐지

2017년 하이엔드 그래픽카드의 가격이 대폭 인상한 것으로 미루어 보아[19], 많은 이들이 비싼 채굴 리그 설치 및 채굴 풀에 참여하여 Bitcoin, Ether, Monero와 같은 가상화폐를 취득하기 시작한 것을 짐작할 수 있습니다. 현물의 대체품이자 이론적으로는 더 안전한 교환 수단인 가상화폐를 채굴하는 것은 매우 단순한 일처럼 보입니다. 그러나 직면한 기술적 문제는 채굴기가 어떻게 지속 가능한 방식으로 충분한 컴퓨팅 자원을 만들어 내면서 수익을 낼 수 있느냐는 것입니다. 즉, 24시간 내내 채굴을 할 때 1,000달러 이상의 그래픽카드가 과열되거나 손상되는 것을 방지하면서 전기세 또한 채굴하는 코인보다 적게 낼 수 있는 방법입니다.

이러한 현상이 사이버 범죄 영역으로 스며드는 것은 놀라운 일이 아닙니다. 사이버 범죄자들은 의심스럽지 않은 사용자의 컴퓨터를 통해 채굴 활동을 할 수 있다는 것을 이미 알아차렸습니다. 지난해 말 사용자 또는 디바이스 소유자의 동의 없이 채굴 활동을 하거나 채굴 활동에 기여하는 소프트웨어 조각들을 발견하기 시작했을 때쯤 이러한 트렌드를 파악하였습니다. 어떤 경우에는 합법적인 채굴 도구가 남용되기도 하지만 무단으로 채굴기가 설치되는 경우 (예: 암호화폐에 관련 없는 기업 네트워크)에는 설치된 채굴 도구가 원치 않는 소프트웨어로 간주됩니다. 트렌드마이크로는 연구를 위해 이러한 종류의 소프트웨어를 "암호화폐 채굴 탐지"로 분류했습니다.

암호화폐 채굴 탐지를 분석해본 결과 2017년 상반기에 약 75,000건에서 하반기에는 약 326,000건으로 증가했습니다.[20] 2018년 상반기에는 전년도 하반기에 비해 가상화폐 채굴 탐지가 약 141% 증가하였습니다.

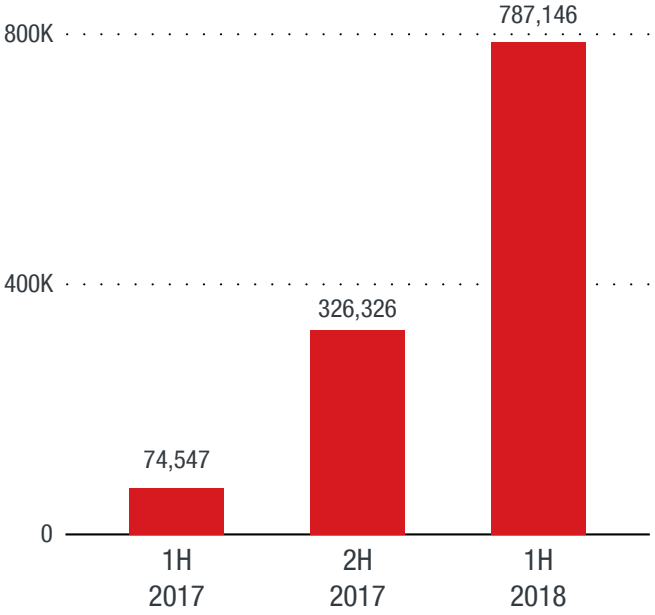


그림 4. 암호화폐 채굴 탐지 수 비교: 암호화폐 채굴의 지속적인 증가

2018년에는 노골적으로 악성 행위를 하는 암호화폐 채굴기 패밀리만 탐지되기 시작했습니다. 더불어 47개의 새로운 암호화폐 멀웨어 패밀리가 발견되었습니다. 이는 많은 투자 집단이 암호화폐를 채굴하기 위한 은밀한 방법에 동원되고 있음을 나타냅니다.

2018년 상반기 내내 해커들은 채굴기 설치를 목적으로 서버 익스플로잇 공격, PHP 취약점, 악성 광고, 다른 형태의 멀웨어 공격과 심지어 금융 사기 사이트까지 다양한 벡터를 사용했습니다. 이러한 패턴은 2017년부터 보였던 양상의 연장선상으로써, 사이버 범죄자들이 어떠한 방법이 가장 많은 이득을 낼 수 있는지 알아내기 위해 가능한 모든 방법을 시도하는 것으로 보입니다.

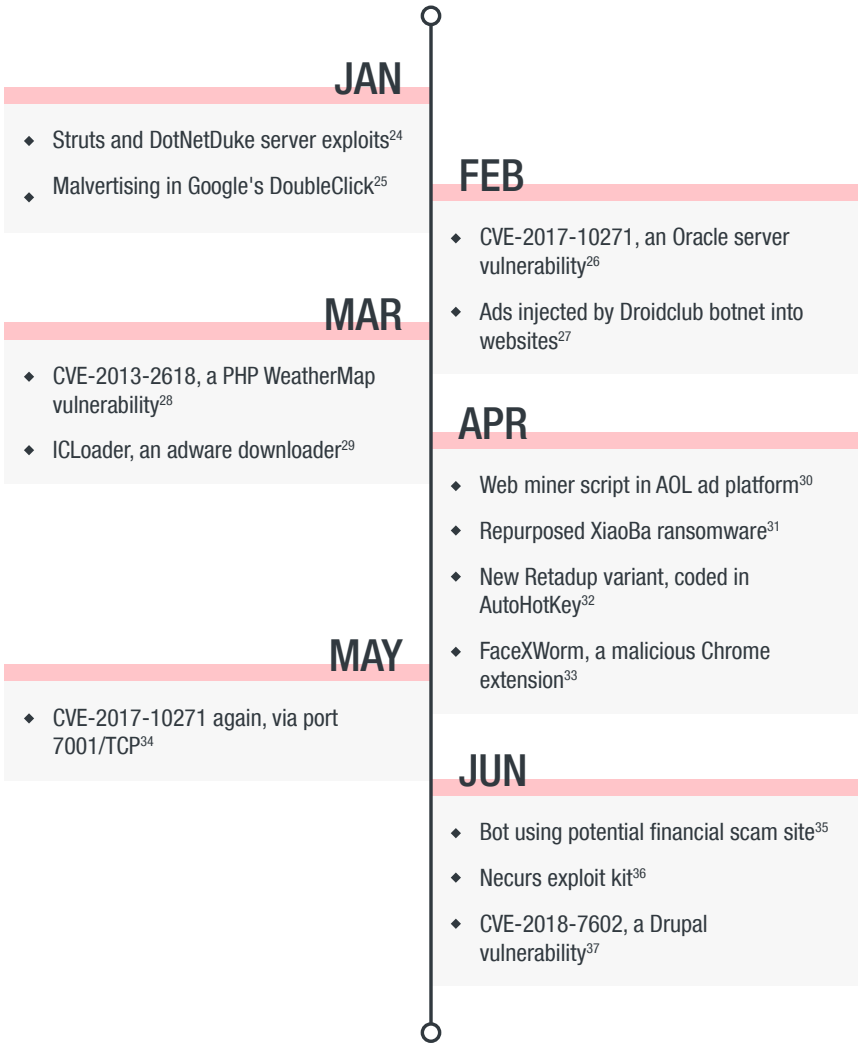


그림 5. 2018년 상반기 사이버 범죄자들이 가상화폐 채굴기를 퍼트리기 위해 사용한 다양한 방법

일부 해커들은 단순한 암호화폐 채굴에서 더 나아가 가상 화폐에 거래소를 해킹하는 공격을 행하기도 했습니다. 해커들은 지난 1월 암호화폐 거래소를 해킹하여 5억 달러 상당의 NEM 코인을 탈취하였고[21], 인도의 해커들은 지난 4월 330만 달러 가치의 비트코인을 훔쳤습니다.[22] 이러한 해커들의 경향은 올 상반기 암호화폐의 가치가 하락했음에도 불구하고 지속되었습니다.[23]

기업의 관점에서, 네트워크에 존재하는 무단 암호화폐 채굴기의 존재는 개별 사용자의 디바이스뿐만 아니라 전체적인 네트워크의 보안에도 위협적인 일입니다. 가상화폐 채굴기로 인한 피해는 (특히 악성 가상화폐 채굴기의 경우) 랜섬웨어로 인한 피해만큼 직접적이지는 않지만, 기업들이 입는 피해가 하나도 없는 것은 아닙니다. 가상화폐 채굴기는 채굴 과정에서 최대한 활용할 수 있는 컴퓨터의 리소스를 빼앗아 갑니다. 따라서 네트워크 성능에 영향을 미칠 수 있으며 하드웨어 마모 및 고장을 야기할 수 있고, 이는 곧 하드웨어의 수명 감소와 에너지 소비의 증가로 이어집니다. 현재 기업이 직면한 새로운 위험은 가상화폐 채굴기가 잘 눈에 띄지 않고 일반적인 위협 보다 조용하기 때문에 이로 인해 잘못된 보안 인식을 심어줄 수 있는 가능성이 있다는 점입니다.

숫자는 줄어들고 있지만 계속해서 진화하는 랜섬웨어

2018년 상반기에 랜섬웨어 탐지 수는 단 3%로 증가하여 전년 대비 현저히 증가 수가 느려진 것을 확인할 수 있었습니다. 암호화폐 채굴기 탐지 수가 랜섬웨어 탐지 수를 대신하여 1위를 차지하였지만, 공격자들이 랜섬웨어 공격에 흥미가 떨어진 것은 결코 아닙니다.

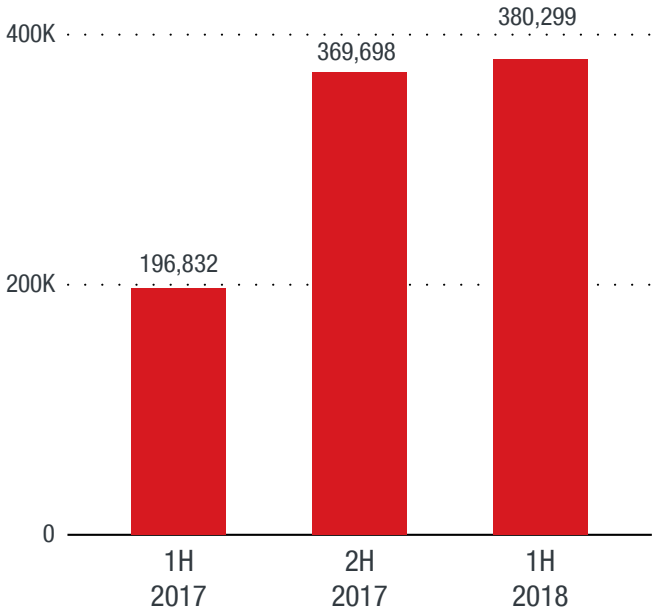


그림 6. 랜섬웨어 탐지 수 비교 그래프:
전반기 동안 탐지 증가률이 3%에 그친 랜섬웨어 탐지 수

랜섬웨어에 대한 대중의 관심이 높아지면서 네트워크 단에서 수행되는 랜섬웨어 완화 정책 및 개선된 백업 방법이 수행됨에 따라 올해 들어 랜섬웨어가 느리게 증가한 현상은 이미 예측되었던 결과라고 볼 수 있습니다.

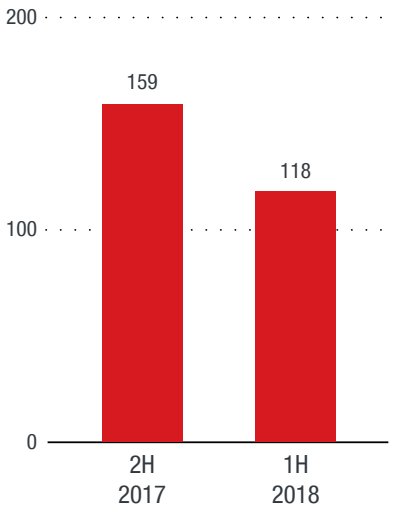


그림 7. 탐지된 새로운 랜섬웨어 패밀리 수 비교 그래프:
랜섬웨어 패밀리의 출현 감소

사이버 범죄자들은 2018년 상반기 동안 갠드크랩 (GandCrab), 블랙하트 (BlackHeart), 사이낵 (SynAck), 블랙루비 (Black Ruby)와 같이 주목할 만한 새로운 랜섬웨어 패밀리를 출현시킴으로써 랜섬웨어 유지와 배포에 대한 접근 방식을 계속 발전시키는 모습을 보여주었습니다. 갠드크랩은 2018년 1분기에 등장하여 암호화와 난독화 절차뿐만 아니라 시스템 내에서의 지속성이 향상된 것으로 유명했는데[38], 이는 개발자들이 랜섬웨어의 성공과 실패에 빠르게 적응할 수 있다는 점을 보여줍니다. 블랙하트는 합법적이지만 오래된 AnyDesk 버전과 함께 악성 페이로드는 패키지도 포장하는데, 이는 백그라운드에서 랜섬웨어가 활동하는 것을 숨기기 위한 행위로 보입니다[39]. 사이낵은 2017년에만 도입된 도플갱잉 (doppelgänging) 프로세스를 처음 사용함으로써 연구원들의 탐지와 분석을 더욱 어렵게 하였습니다[40]. 블랙 루비의 경우[41] 랜섬웨어로서의 기능을 할 뿐만 아니라 Monero 채굴기 또한 설치하였고, 이는 공격자들이 랜섬웨어와 가상화폐 채굴기 모두로부터 수익을 보고 있다는 증거가 되었습니다.

랜섬웨어는 다양한 진입점과 기술을 사용하므로, 모든 경우의 수를 따졌을 때 하나의 보안으로 탐지와 차단을 기대할 수 없습니다. 따라서 기업은 보안에 대한 다계층적인 접근 방식뿐만 아니라 적절한 기술을 적시에 사용하기 위해 다양한 위협 방어 기술을 지능적으로 혼합한 보안 솔루션을 사용해야 합니다.

GDPR의 패널티 정책에도 불구하고 대형 정보 유출 사고는 증가합니다

2016년 4월 유럽연합이 시행하기로 결정한 정보 보호 규정 (General Data Protection Regulation, GDPR)은 EU 시민의 정보를 부적절하게 취급한 사실이 드러나면 유럽에 있지 않은 기업도 포함한 모든 기업에게 벌금이 부과되는 획기적인 규제이며, 해당 규제의 등장으로 보안 업계에 큰 파장을 일으켰습니다.[42] 영향을 받는 모든 기업들은 약 2년 동안 컴플라이언스에 대비하였고, GDPR은 2018년 5월 25일 본격적으로 시행되었습니다.[43]

GDPR의 시행으로 정보 유출 보고 건수가 줄어든다면, 이는 기업들이 정보 보안 전략에 큰 노력을 기울이고 있다는 증거일 것입니다. 그러나 정보 유출 건수는 줄어들지 않았습니다. 미국의 정부기관 및 언론 매체의 정보 유출을 감시하는 기관인 Privacy Rights Clearinghouse에 따르면, 2018년 상반기에만 보고된 정보 유출 건수는 259건에 달하며 이는 작년 하반기에 비해 높은 숫자입니다.

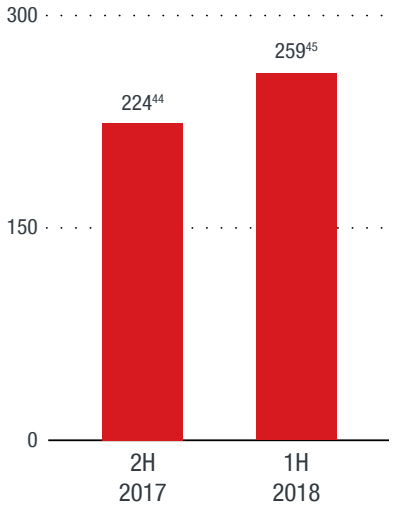


그림 8. 미국에서 보고된 정보 유출 6개월 단위 비교 그래프:
정보 유출 건수의 증가

트렌드마이크로는 동일한 데이터 세트를 사용하여 분석한 결과, 2018년 상반기에 발생된 15개의 정보 유출 사례에서 100만 건 이상의 데이터가 노출되었음을 확인하였습니다. "대형 정보 유출"이라 불리는 이러한 사건의 대부분이 소매상이나 온라인 상인들에게 악영향을 미쳤습니다. 이러한 위반 사례의 수는 전년도 대비 6건 밖에 증가하지 않았지만 적어도 6백만 건 이상의 기록이 노출된 것으로 볼 때, 이는 무시할 수 없는 수치입니다.

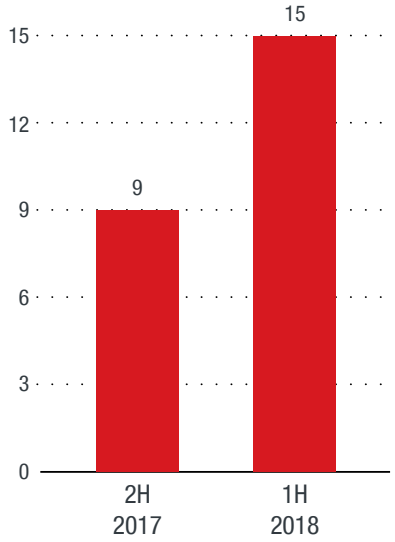


그림 9. 미국에서 보고된 6개월 단위의 정보 유출 건의 비교 그래프:
대형 정보 유출 사건의 증가

정보 유출은 꽤 오랫동안 위협 환경의 일반적인 특징이었습니다. 그리고 최근 정보 유출의 증가는 실제 사고 발생의 증가와 정보 관련 컴플라이언스에 대한 공격의 증가로 볼 수 있습니다. 또한 같은 데이터 시트의 분석 결과 42%의 사고가 의도하지 않은 공개를 통해 발생한 것으로 보이는 반면 41%는 해킹으로 인한 것으로 나타났습니다. 더불어 보고된 정보 유출에 대한 정보에 따르면 해커의 활동으로 인한 것보다 더 많은 기록이 노출된 것이 밝혀졌습니다. 즉, 기업이 정보 유출의 위험을 알고 있더라도 여전히 포괄적인 방식으로 적절한 정보 보호 매커니즘을 시행하지 못하고 있다는 것입니다.

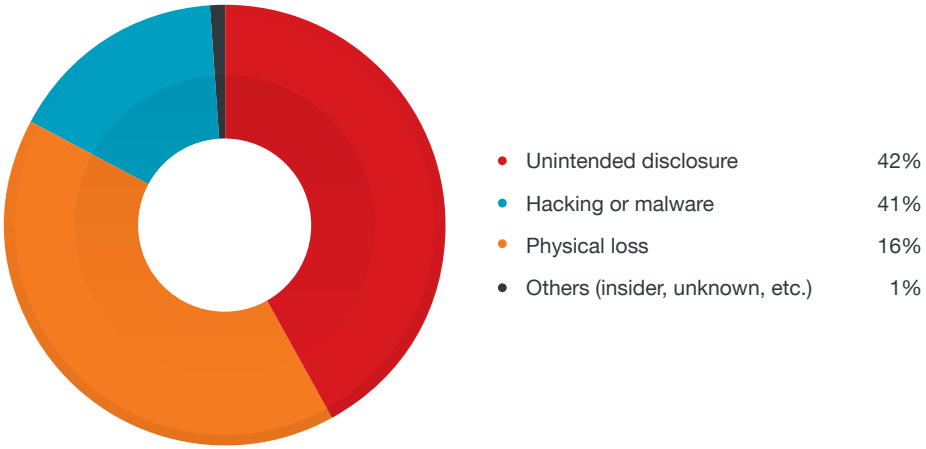


그림 10. 2018년 상반기 정보 유출 원인:
정보 유출의 가장 많은 원인은 의도되지 않은 공개였습니다.

다수의 대규모 정보 유출은 클라우드와 관련이 있습니다. 한 마케팅 회사가 관리하는 최대 3억 4천만 개의 기록으로 구성된 약 2 테라바이트의 데이터베이스가 보안 연구자에 의해 공개적으로 액세스할 수 있는 서버에 노출된 것으로 밝혀졌습니다. [46] 이동 통신사의 웹사이트 버그는 누구나 휴대폰 번호만을 사용하여 고객의 개인 정보에 접근할 수 있도록 허용하였지만, 실제 버그는 메인 사이트가 아닌 고객 관리 포털에 있었습니다.[47] 한 데이터 기술 회사가 다른 소셜네트워크에서 스크랩된 개별 프로필이 담긴 100만 테라바이트 이상의 레코드가 포함된 파일을 암호가 없는 퍼블릭 클라우드에 보관하였습니다.[48] 그리고 한 프랜차이즈 카페 업체는 고객 등록 정보를 웹사이트에 일반 텍스트로 남겨두어 수백만 개의 고객 이름, 이메일 주소 및 기타 고객 기록을 유출하였습니다.[49] 지난 몇 년간 비슷한 사고가 여러 번 있었음에도 불구하고 아직까지 이러한 일련의 사건들이 나타난다는 것은 사고 이후 고객 데이터를 보관하는 방법과 장소에 어떠한 확실한 대책이 수립되지 않았다는 것을 나타냅니다.

의료 서비스 분야의 경우 사고 횟수로 따졌을 때 가장 많이 정보 유출을 겪은 산업 분야입니다. 유출된 의료 시스템에 관한 트렌드마이크로의 연구에 따르면[50] 의료 서비스 업종이 네트워크 보안 개선에 어려움을 겪는 데에는 몇 가지 이유가 있습니다. 이러한 이유에는 환자 관리의 최우선을 두고 대부분의 리소스를 사용 점, 많은 내부 사용자가 여러 시스템에 대한 액세스 권한이 있는 점, 그리고 전용 사이버 보안 대응 팀의 부족한 점이 있습니다.

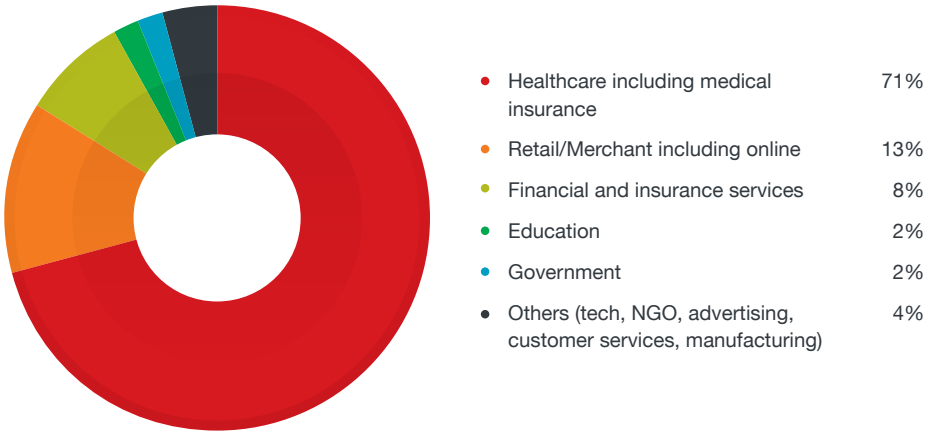


그림 11. 2018년 상반기 산업별 정보 유출 사고:
의료 분야가 가장 많이 정보 유출 사고를 당한 산업이었습니다.

트렌드마이크로는 또한 더 폭넓게 현상을 이해하기 위해 전 세계의 정보 유출 자료와 공개된 자료를 검토하였습니다. (미국 이외의 지역에서 공개된 정보 유출에 대한 요약은 이 보고서의 Threat Landscape in Review 부분에서 확인하실 수 있습니다.) 검토 결과, 최소 10만 개의 레코드가 유출되어 18개 이상의 정보 유출 사건이 발생하였으며, 그중 적어도 9개는 대형 유출 사고로 간주될 수 있었습니다.

미국 이외의 지역에서 발생한 대규모 정보 유출 사례에는 사용자 ID, 닉네임, 암호 등 천만 개에 가까운 정보가 유출된 중국 동영상 공유 및 스트리밍 사이트 사고가 있습니다.[51] 또한 노르웨이에서는 한 의료 서비스 업체가 해킹을 당하여 약 3백만 명의 환자 기록이 유출되었습니다.[52] 이스라엘에서는 취학 전 교사와 부모를 연결해 주는 애플리케이션에 저장된 600만 장의 아이들의 얼굴과 신상정보, 사진을 유출시키는 취약점이 발견되었습니다.[53] 그리고 두바이에서는 해커가 차량 이용 서비스 (ride-hailing service) 스토리지 시스템에 액세스하여 1400만 고객의 개인 정보가 공개되었습니다.[54]

기업들이 심각한 정보 유출 사고를 겪고 나서도 다시 비슷한 사건이 생기는 점을 볼 때, 그만큼 오늘날의 정보 유출의 영향이 얼마나 큰지 알 수 있습니다.[55] 하지만 정보 유출이 기업의 수익에 미치는 영향은 너무나 현실적입니다. 정보 유출의 여러 측면을 살펴본 한 글로벌 연구에 따르면, 대형 정보 유출 사고의 비용은 4천만 달러에서 3억 5천만 달러에 이를 수 있다고 합니다.[56] 기업은 타격을 입은 비즈니스와 잃어버린 고객, 떨어진 평판, 문제 해결을 위한 리소스 비용 등 정보 유출이 초래할 수 있는 위험을 계속해서 감수해야 합니다.

기업은 특히 GDPR의 시행을 고려하여 개인 정보 보호에 대한 보안을 강화해야 합니다.[57] 이 규정에 따라 EU 시민들의 데이터를 수집, 보관, 처리하는 회사들은 개인 정보 보호 정책을 더 강화하여 시행해야 합니다. 정보 유출 사고가 일어났을 시, 해당 기업은 이를 인지하고 난 후 72시간 이내에 고객과 당국에 사고의 발생을 알려야 합니다. GDPR을 준수하면 보관하는 정보가 EU 시민의 것이 아니더라도 데이터를 보호하기 위한 태세를 강화할 수 있으며, 지금까지 언급된 여러 가지 사고를 방지할 수 있습니다.

그러나 단순히 규정을 준수하는 것을 넘어, 기업은 다계층의 보안 기술을 구현하고 보안 사고 발생 시 포괄적으로 데이터를 보호하기 위한 전략을 수립하기 위해 노력해야 합니다. 또한 클라우드 기반 서비스 사용과 관련하여 의도하지 않은 정보 유출은 최근 정보 유출 사고의 큰 발생 요인 중 하나이므로, 기업은 보안의 방식을 클라우드 및 데이터를 저장하는 타사 파트너까지 확대해야 합니다.

Mirai 경고에도 불구하고 라우터 보안은 여전히 취약합니다

트렌드마이크로는 사물인터넷 (IoT)에 대한 심각한 위협이 출현할 수 도있는 위협 상황을 오랫동안 주시해 왔습니다. 그러나 스마트 기기의 수가 계속해서 증가하면서 관련된 소프트웨어의 표준화에는 여전히 많은 일들이 필요합니다. 따라서 공격자가 특정 디바이스 유형 또는 소프트웨어를 성공적으로 공격할 만한 포인트를 찾지 못했을 가능성이 높으며, 스마트 기기만을 대상으로 하는 대규모 공격은 아직 보지 못했습니다. 한편, 인터넷 통신에서 간과되고 있는 구성요소는 가정과 사무실의 오픈된 네트워크이며, 이는 일반 컴퓨터, 스마트 커피 머신 등을 포함한 온갖 종류의 디바이스를 해킹에 노출시킬 수 있습니다.

3월 말, 트렌드마이크로는 브라질 기반의 디바이스를 목표로 하는 스캐닝 활동을 발견하였으며 해당 활동은 중국의 감염된 라우터로 인해 생겼던 Mirai 사건을 연상시켰습니다.[58] 2016년 처음 발견된 Mirai는 감염에 취약한 디바이스에서 발생한 DDoS 공격을 말합니다.[59] 당시 사용되었던 소스 코드는 현재 공개된 상태로 있으며,[60] 따라서 사이버 범죄자들이 해당 소스 코드를 수정 및 사용하여 또 다른 공격 캠페인을 시작할 수 있습니다. 이전 사례에서와 같이 기본 자격 증명 사용은 해커들이 연결 장치를 해킹하기 위해 이용해왔으며, 그중 상당 부분은 홈 라우터와 IP 카메라였습니다.[61]

트렌드마이크로는 또한 비슷한 시기에 유사한 캠페인이 브라질에서 진행되고 있는 것을 보여주는 코드를 발견하였습니다.[62] 그리고 지난 5월, 멕시코에서 Mirai와 유사한 또 다른 스캐닝 활동을 감지하였고, Mirai와의 차이점은 가정이나 사무실 네트워크에 광섬유 연결을 제공하기 위해 사용되는 GPON (Gigabite Passive Optical Network)[63]의 취약점을 이용한다는 점이었습니다.

그러나 2018년 상반기에 발생한 가장 큰 네트워킹 장치 기반의 공격은 멀티스테이지 VPNFilter 공격이었습니다. 2017년 100만 개 이상의 기업에 영향을 미친 Mirai 및 Reaper와 같은 이전의 유사한 악성 프로그램 조각은 비교적 단순한 구조와 페이로드였습니다.[64] 그러나 VPNFilter의 경우 매우 다릅니다. VPNFilter는 지속적인 구성요소, 데이터 하베스터 (Data harvester) 및 스니퍼 플러그인 (Sniffer plugin)으로 구성되며, 라우터를 사용할 수 없게 만드는 가상의 킬 스위치도 있습니다. 2016년 초부터 활동량이 최고조에 달하면서 최소 54개국에서 50만 대 이상의 네트워크나 네트워크 디바이스를 감염시켰습니다.[65]

Mirai[66] (first variant in 2016)	Reaper[67] (October 2017)	VPNFilter[68]
• 넓은 범위의 IP 주소를 스캔 • 미리 정의된 기본 자격 증명 목록을 통해 자격 증명이 약한 디바이스를 공격 • 수십만 명이 사용하는 CCTV, DVR 및 라우터에 관련된 DDoS 공격에 사용됨 • 몇몇 유명 웹사이트에 접속하지 못하게 함 *이후 소스 코드가 공개되어 다른 사이버 범죄자들이 새로운 버전의 악성 코드를 생성함.[69]	• IoT 디바이스에 익스플로잇 공격 실행 • 라우터와 IP 카메라, NAS 디바이스 공격 • 100만 개 이상의 조직을 공격함 • 운영자가 DDoS, 트래픽 프록시 및 기타 활동에 대한 코드를 전달할 수 있도록 실행 환경을 통합	• 이중화 및 지속성을 보장하기 위해 세 개의 구성요소로 제작됨 • 데이터 수집을 위한 정찰 기능이 있음 • 라우터를 복구할 수 없는 상태로 만들기 위한 자체 파괴 기능이 포함됨 • 최소 54개국에서 50만개의 라우터에 영향을 미침 • 기능 향상을 위한 여러개의 플러그인 보유

표 1. Mirai, Reaper, VPNFilter 비교 표: VPNFilter 필터는
이전의 대규모 라우터 기반 공격보다 훨씬 많은 구성 요소를 가지고 있습니다.

미연방 수사국 (FBI)에서 공개적으로 사용자의 라우터 전원 사이클에 대한 발표까지 하면서 해당 공격에 대한 인식이 높아졌음에도 불구하고[70], 소규모 기업 및 가정에서 쓰이는 네트워크에는 여전히 VPNFilter 공격에 취약할 뿐만 아니라 다른 취약점을 가지고 있습니다. 잠재적으로 VPNFilter의 영향을 받을 수 있는 라우터를 대상으로 한 트렌드마이크로의 스캔 데이터에 따르면, 총 19개의 버그를 식별할 수 있었으며 이는 곧 디바이스가 취약하다는 것으로 판단됩니다. 이 취약성은 CVE-2011-4723과 같은 오래된 취약점과 여러 가지 암호 및 인증 관련 문제를 포함한 비교적 새로운 취약점이 혼합된 것입니다.[71]

사용자들이 기본 사용자 이름 및 비밀번호 조합, 기본값 설정 변환, 펌웨어의 정기적인 체크 및 업데이트 등의 아주 기초적인 보안 방법을 수행하지 않았을 때 이전 공격들의 영향과 함께 VPNFilter의 공격 결과가 어떤지는 매우 생생하게 보입니다.

파일리스, 매크로 및 소규모 멀웨어로 인해 파일을 기반으로 한 보안 기술이 위협받고 있습니다

기존의 안티 멀웨어 솔루션은 새로운 멀웨어 모델과 직접적인 관련이 있었습니다. 공급업체는 특정 멀웨어 또는 그 변종을 감지할 수 있는 다양한 패턴 유형을 생성할 수 있습니다. 2018년에는 획기적인 회피 기법이 따로 발견되지는 않았지만, 트렌드마이크로는 사이버 범죄자들이 파일 기반의 탐지 기술을 우회할 수 있는 가능성을 높이기 위해 어떻게 멀웨어 캠페인을 지속하고 있는지 관찰해 왔습니다. 실제로 2018년 상반기 사이버 범죄자들은 파일리스 위협, 매크로 및 소규모의 멀웨어를 사용하였습니다.

파일리스 위협은 일반적으로 시스템의 로컬 스토리지에 기록된 바이너리 파일 또는 실행 파일을 사용하는 대신 시스템 레지스트리에서 실행됩니다. 악성코드는 실행 중인 애플리케이션 메모리에 삽입되거나 파워셸과 같은 합법적 툴을 통해 스크립트를 실행하여 주입될 수도 있습니다. 트렌드마이크로는 특정 실행 이벤트 또는 이벤트와 같은 논-파일 (Non-file) 기반의 지표를 추적하여 파일리스 위협의 활동을 탐지할 수 있었습니다.

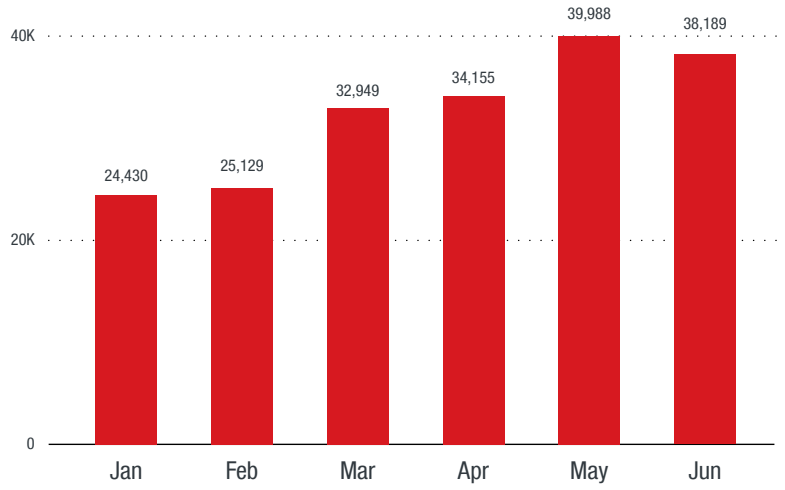


그림 12. 2018년 상반기 매월 차단된 파일리스 이벤트 그래프: 지속적으로 발견되는 파일리스 위협

매크로 또한 계속해서 위협 환경의 일부로 자리 잡고 있지만, 5월은 악성 스팸을 통해 배포된 Powload가 가장 많이 나타났습니다.[72] 스팸은 일반적으로 Ursnif나 Bebloh와 같은 악성 프로그램으로 이어지지만, 먼저 첨부되거나 연결된 매크로를 사용하여 최종 페이로드의 다운로드를 실행합니다. 하지만 스팸이 아닌 타깃 공격 캠페인에도 사용되는 악성 매크로를 발견하였습니다. 2017년 사용된 MuddyWater 캠페인 전략과 마찬가지로, 5월에 발견되 타깃 공격의 구성 요소에는 악성 매크로가 포함된 악성 Word 문서가 포함되어 있었습니다. 매크로과 화성화되면 코드가 조작된 파워셸 스크립트를 실행하여 궁극적으로 주 정찰 구성 요소인 백도어를 다운로드합니다.[73]

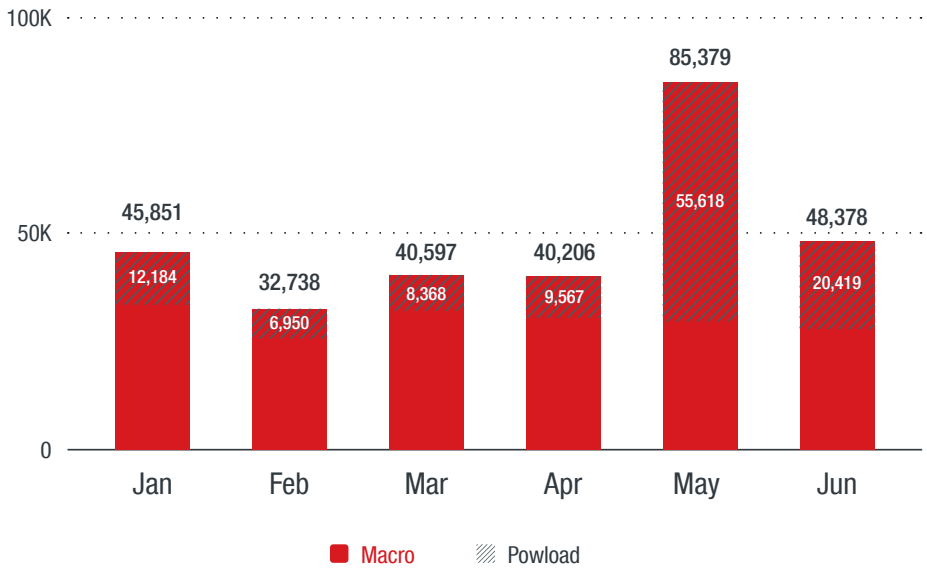


그림 13. 월별 매크로 멀웨어 및 Powload 탐지 그래프:
매크로 멀웨어 탐지 중 가장 많은 원인은 Powload 였습니다.

매크로가 강력한 영향력을 나타내면서 악성 의도를 숨길 수 있는 또 다른 방법을 제공하기 때문에 매크로는 사이버 범죄자들이 선호하는 배포 매커니즘입니다. 매크로 멀웨어는 사용자가 파일의 매크로를 사용하도록 설정한 후에만 코드를 실행하므로 멀웨어 실행 파일보다 탐지하기 어렵습니다.

2018년 상반기 트렌드마이크로가 파악한 또 다른 중요한 상승은 매우 작은 규모의 POS (Point-of-Sales) 악성 프로그램의 확산입니다. 매우 작은 규모의 POS 악성 프로그램은 짧은 시간 동안 널리 퍼져 총 POS 멀웨어 탐지량의 약 3/4을 차지했습니다.

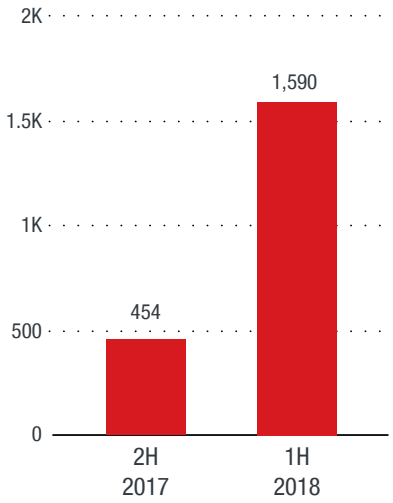


그림 14. 작년 하반기와 올 상반기 POS 멀웨어 탐지 비교:
POS 멀웨어 증가

이러한 증가는 2014년[74] 초부터 발견된 POS 멀웨어 패밀리인 TreasureHunter의 소스 코드가 지난 5월 공개되었기 때문일 수도 있습니다. 멀웨어 소스 코드 누출의 경우 유사하거나 관련된 멀웨어 감염이 발생하는 것은 매우 흔한 일입니다. 또한 트렌드마이크로는 PinkKite라고 불리는 새로운 POS 멀웨어 제품군,[75]을 발견하였습니다 (트렌드마이크로 탐지명 TinyPOS).

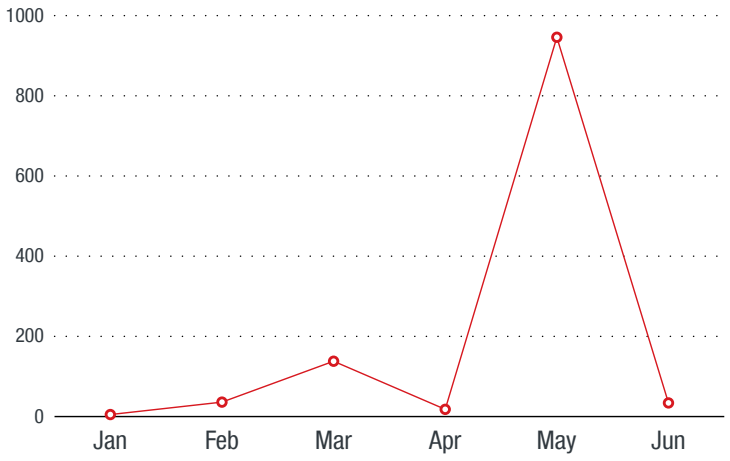


그림 15. TinyPOS의 2018년 상반기 탐지 수:
5월에 갑자기 증가한 TinyPOS

이러한 POS 멀웨어는 파일 크기가 작기 때문에 일반적으로 사이버 범죄자들에게는 명령 측면에 있어 몇 가지 옵션을 선택할 수 있습니다. 이러한 구조는 일반 파일로 쉽게 오인될 수 있으므로 탐지가 더 어렵습니다.

POS 터미널을 많이 사용하는 대형 소매점의 IT 관리자에게는 다계층의 보호 수단을 설정하는 것이 중요합니다. 엔드포인트 애플리케이션 제어는 소프트웨어의 실행을 화이트리스트에 기반하여 제한함으로써 네트워크를 POS 멀웨어로부터 보호할 수 있으며, 네트워크 기반의 솔루션은 인바운드 통신 검사 외에도 아웃바운드 통신을 플래그 할 수 있습니다.

파일리스 위협과 이와 유사한 위협의 일반적인 추세는 사이버 범죄자들이 안티 멀웨어 기술에만 의존하는 기업의 고질적인 보안 전략에 잘 알고 있다는 뜻입니다. 다행히도 대부분의 위협 요소는 기본적으로 여러 구성으로 되어있어서 이메일 또는 링크를 전송 메커니즘으로 사용하거나, 서버를 통해 다른 구성 요소 또는 최종 페이로드를 전달하거나, 네트워크 또는 시스템 로그에 행동적 단서를 남깁니다. 따라서 기업은 여러 계층에 걸친 보안 접근 방식을 취하고 네트워크 전반에 걸쳐 통합된 추가 보호 계층을 사용함으로써 파일리스 매크로 위협을 방지할 수 있습니다.

BEC가 지속적으로 증가함에 따라 BEC 손실액이 예상을 뛰어넘었습니다

기업은 계속해서 BEC (Business Email Compromise, 비즈니스 이메일 침해)와 관련된 문제를 겪고 있습니다. 특히 소셜엔지니어링 기법은 BEC에서 쓰이는 가장 전형적인 수법입니다. 이는 C-level 임원, 공식 공급업체 직원, 변호사 등을 가장하여 이메일을 보내, 지불을 요청하여 기업의 자금을 빼돌립니다. 어떤 경우에는 궁극적으로 기업의 자금을 빼돌리기 위해 임원의 신상 정보를 먼저 훔치기도 합니다.

실제 공격 내용은 사건마다 다를 수 있지만, BEC는 공격자가 이용할 수 있는 단서나 약점을 식별하기 위해 공격 대상 회사에 대한 충분한 정찰을 합니다. 그런 다음 보통 C-level 임원으로 가장하여 회사의 W-2 레코드와 같은[76] 중요한 정보를 요구하거나 자금의 이체 등을 지시합니다. BEC는 오픈소스 인텔리전스와 소셜엔지니어링 기법을 사용하는 로우테크 (Low-tech)이지만, 매우 높은 수익률을 내고 있습니다. 이러한 이유로 2018년에도 BEC로 인한 손실이 계속 증가할 것으로 예측됩니다.[77]

2013년 10월부터 BEC를 모니터링해온 FBI에 따르면 최근 BEC 및 EAC (Email Account Compormise, 이메일 계정 사기) 사고에 발생한 총 손실액은 지난 5월과 비교해 136% 증가한 125억 달러입니다.[78] 이 수치는 또한 트렌드마이크로가 예측한 BEC 공격으로에 대한 예상 손실액 보다 39%나 높은 것으로, 정기적인 조언과 상당한 언론 보도에도 불구하고 정상적인 이메일과 사기 이메일을 분별하는 능력이 악화하고 있음을 보여줍니다.

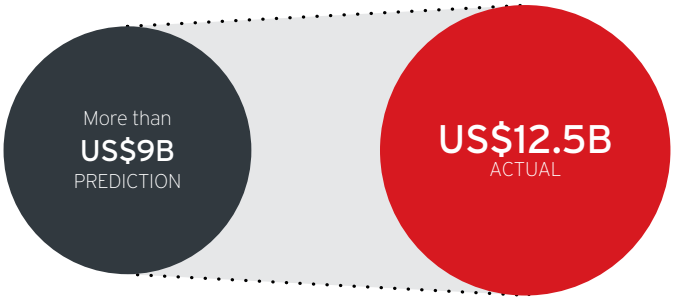


그림 16. FBI가 발표한 BEC 및 EAC 누적 손실액:
예상치를 초과한 BEC 및 EAC 손실액

또한 2018년 상반기 동안의 BEC 시도는 지난해 하반기 보다 5% 증가했습니다.

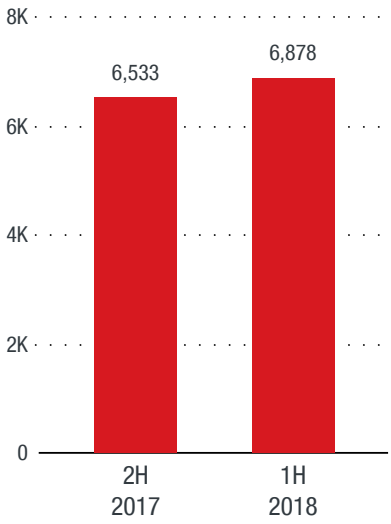


그림 17. 기록된 BEC 시도 횟수에 대한 반기별 비교 그래프: BEC 시도 횟수 증가

참고: 데이터는 BEC 시도 횟수만을 나타내며, 공격이 성공했는지의 여부를 나타내지 않습니다.

BEC 샘플은 주로 CEO를 가장한 사기 메일로 구성됩니다.

BEC 문제는 국제적인 이슈가 되어 FBI와 법무부를 포함한 미국의 연방 당국이 Operation WireWire라고 명명한 작전을 수행하였습니다. 이와 같은 노력으로 미국과 다른 국가 (나이지리아, 캐나다, 모리셔스, 폴란드 등)에서 74명의 체포가 이루어졌고 미화 1400만 달러의 송금이 취소되었습니다.[79] 이런 식의 노력은 BEC 감소에 영향을 줄 수 있지만, BEC 실행이 다른 공격보다 용이함에 따라 또다시 개인 및 집단의 BEC 공격이 단계적으로 증가할 수 있습니다.

네트워크 레벨에서 기업은 이메일 기반 위협에 대처하기 위한 더 나은 전략을 모색해야 합니다. BEC 공격은 소셜 엔지니어링 기법을 사용하기 때문에 파일 기반의 탐지 기능은 소용이 없지만, 이메일 평판 기술은 어느 정도의 예방에 도움이 될 수 있습니다. 또한 전문 규칙을 사용하는 인공지능 기반 솔루션과 특정 이메일이 사기성 이메일인지의 여부를 조사하기 위해 발송자의 이메일 작성 방식을 분석하는 머신러닝 기술과 같은 BEC 관련 솔루션[80]도 있습니다.

Threat Landscape in Review

2018년 상반기 동안 Trend Micro™ Smart Protection Network™ 인프라는 다양한 사이버 범죄 운영에 사용되는 이메일, 파일 및 URL 구성 요소인 200억 개 이상의 위협으로부터 사용자를 보호하였습니다.

20,488,399,209

2018년 상반기 차단된 위협의 수

올 상반기 차단된 위협의 수는 지난해 하반기보다 아주 근소하게 적은 수입니다.

그림 18. 차단된 이메일, 파일 및 URL 위협 요소의 분기별 비교 그래프:
차단된 이메일 및 URL 위협의 수가 소폭 증가하였습니다.

또한 가능한 한 많은 사용자 디바이스를 감염시킨 후 가상화폐를 채굴하는 활동에 대한 사이버 범죄자들의 관심이 높아짐에 따라 새로운 암호화폐 채굴기 패밀리의 수도 급증하였습니다.

BATMINE	DLDRETN	MALKARBO	MINERBOT	POWXMR	TOOLXMR
BLOUIROET	HELAMINE	MALLTC	MMBTC	RETADUP	TOOLZEC
BTCTOOL	LINDMINE	MALREP	MMETH	SHAOSMINE	WEBJSE
COFFEE	MALBTC	MALXCN	MMXMR	SILVERSPACEETN	XENOM
CRYPTOLOOT	MALDCR	MALXMR	MNRGRIMEX	TOOLBTC	XMRMINE
CRYPTONIGHT	MALELI	MALXMRIG	OPMINE	TOOLDBL	XMRTOOL
DASH	MALETH	MALXR	OTOTI	TOOLETN	ZCAMINE
DLDRETH	MALETN	MALZEC	POOLVAULT	TOOLRVN	

표 2. 2018년 상반기동안 탐지된 새로운 암호화폐 채굴기 멀웨어 패밀리:
47개의 새로운 암호화폐 채굴기 패밀리가 탐지되었습니다.

그러나 암호화폐 채굴기 수의 급증으로 랜섬웨어의 수가 감소한 것은 아닙니다. 랜섬웨어를 이용한 피해자 탈취는 사이버 범죄자들의 오랜 수단으로 남을 것입니다. 하지만 새로운 랜섬웨어 패밀리의 수는 전체적으로 감소하였습니다.

ACKNYS	CRYPTOR	EXOCRYPT	INSTALADOR	PAIN	STINGER
ADAMLOCKER	CRYPWALKER	FAKEKILLBOT	KASITOO	PEDCOT	SURESOME
ANIMUS	CSGO	FBLOCKER	KINGBOROS	PESOJ	TALINSLOCKER
AURORA	CYPEN	FILECODER	KRAKATOWIS	RANCIDLOCKER	TBLOCKER
AUSIV	CYSEARCHER	FILECRYPTOR	LADON	RANDOMLOCKER	TEARDROP
AUTISMLOCKER	DATAKEEPER	FOREIGN	LAZAGNECRYPT	RAPID	TEERAC
AVCRYPT	DEATHNOTEBATCH	FURY	LEBANA	REDEYE	THANATOS
BANACRYPT	DEDWARE	GANDCRAB	LILFINGER	RONT	TK
BLACKHEART	DEFENDER	GEGLOCKER	LIME	RSAUTIL	TRON
BLACKRUBY	DEUSCRYPT	GLOBIM	MAGICIAN	RUSSENGER	USELESS
BLANK	DGER	GOODRABBIT	MEINE	SATURN	VBRSCARE
BOSLOKI	DIRCRYPT	HAKNATA	MINDCRYPT	SATWANCRYPT	VERTUN
BYTELOCKER	DISKDOC	HARROS	MINDLOST	SATYR	WADHRAMA
CARDSOME	DONUT	HAXLOCKER	MONEROPAY	SEPSIS	WANNAPEACE
CCP	DOTZERO	HEARTBLEED	NECNE	SEQUR	WHITEROSE
CESLOCKER	DWORRY	HERMES	NIKSEAD	SIGMA	WYVERN
CRUSIS	DYAR	HOLA	NMCRYPT	SIGRUN	ZENIS
CRYBRZ	ELGOSCARE	HONOR	NOWORI	SKIDDY	ZLOCKER
CRYPT	EMBRACE	HORSUKE	PABGEE	SKYFILE	
CRYPTOLOOT	EVERBE	INSANECRYPT	PACTELUNG	STACUS	

표 3. 2018년 상반기 새로운 랜섬웨어 패밀리: 118개의 새로운 랜섬웨어 패밀리가 발견되었습니다.

익스플로잇 키트는 위협 환경 속에서 조용히 지속해서 남아 있었습니다. 앞서 설명한 바와 같이, 사이버 범죄자들은 계속해서 익스플로잇 키트를 업데이트하였지만, 전체적인 익스플로잇 키트 공격의 수는 줄어들었습니다.

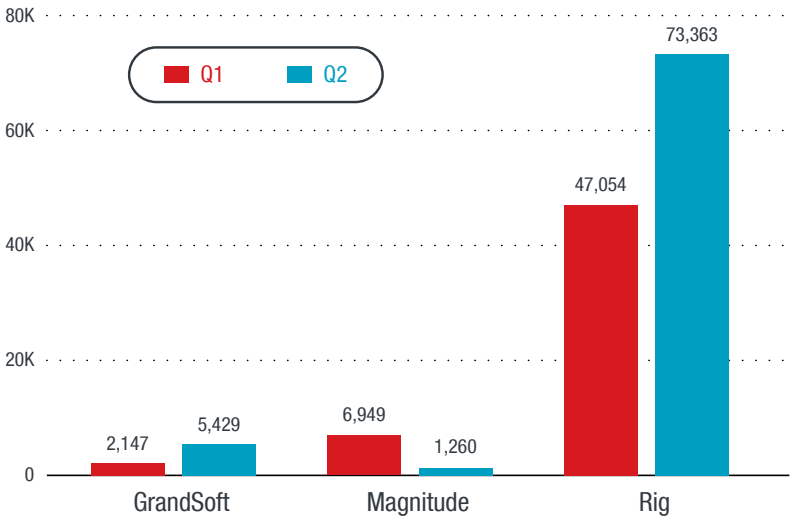


그림 19. 분기별 익스플로잇 키트 활동 그래프:
2분기에 익스플로잇 키트 활동이 증가하였으며, Rig 익스플로잇이 가장 활발하게 활동하였습니다.

랜섬웨어의 감소는 랜섬웨어 기능을 갖춘 악성 모바일 앱의 감소로 이어졌습니다. 그러나 완전히 사라진 것이 아니므로 스마트폰 사용자들은 계속해서 주의를 기울여야 합니다.

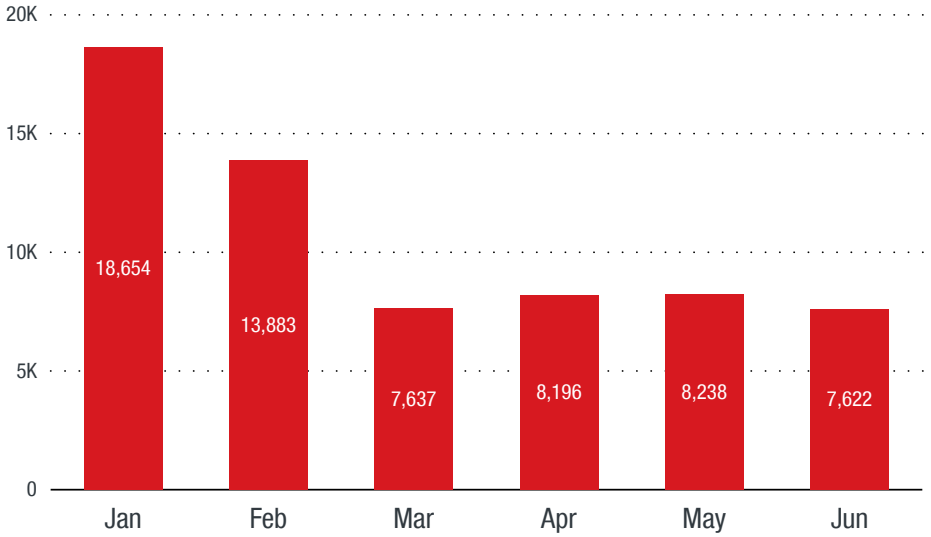


그림 20. 2018년 상반기 탐지된 모바일 랜섬웨어의 수

정보 유출은 최근 몇 년 동안 점점 더 많은 기업이 온라인 리소스 및 클라우드 서비스에 의존하게 되면서 발생하는 고질적인 문제입니다. 현재까지 언론의 관심은 주로 미국에서 일어나는 정보 유출 사건에 치우쳐 있었습니다. 하지만 정보 유출은 미국 외의 다른 나라에서도 큰 이슈가 되고 있습니다.

Company description	Date made public	Country/ Territory	Total records
Ride-hailing service	Apr 23	U.A.E.	14,000,000[81]
Bank	May 2	Australia	12,000,000[82]
State-franchised lottery group	Mar 16	U.K.	10,500,000[83]
Online school exam analysis system	Jun 10	Malaysia	10,300,000[84]
Video streaming and sharing site	Jun 13	China	10,000,000[85]
Consumer electronic retailer	Jun 13	U.K.	10,000,000[86]
Child-centric communication app	Mar 11	Israel	8,500,000[87]
Government ministry	Mar 24	India	5,000,000[88]
Healthcare facility	Jan 18	Norway	3,000,000[89]
Telecommunications provider	Feb 7	Switzerland	800,000[90]
News magazine organization	Mar 1	France	693,000[91]
IT-oriented online portal	Feb 20	Singapore	685,000[92]
Payroll system	Feb 17	India	550,000[93]
Parcel delivery company	Feb 7	Ukraine	500,000[94]
Broadband provider	Apr 18	Hong Kong	380,000[95]
Wireless telecommunications provider	Feb 12	Canada	350,000[96]
Hotel	Jun 26	Japan	124,963[97]
Telecommunications provider	Jan 24	Canada	100,000[98]

표 4. 2018년 상반기 미국 이외 국가의 정보 유출 사고:
최소 10만 개의 기록이 미국이 아닌 18개국에서 정보 유출 사고로 노출되었습니다.

References

1. Jann Horn. (3 January 2018). *Google Project Zero*. "Reading Privileged Memory with a Side-Channel." Last accessed on 31 July 2018 at https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html.

2. Vit Sembera. (5 January 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "When Speculation Is Risky: Understanding Meltdown and Spectre." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/speculation-risky-understanding-meltdown-spectre/.

3. Graz University of Technology. (2018). *Graz University of Technology*. "Meltdown and Spectre." Last accessed on 31 July 2018 at https://meltdownattack.com/.

4. Vit Sembera. (5 January 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "When Speculation Is Risky: Understanding Meltdown and Spectre." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/speculation-risky-understanding-meltdown-spectre/.

5. Tom Warren. (21 May 2018). *The Verge*. "Google and Microsoft disclose new CPU flaw, and the fix can slow machines down." Last accessed on 1 August 2018 at https://www.theverge.com/2018/5/21/17377994/google-microsoft-cpu-vulnerability-speculative-store-bypass-variant-4.

6. Liam Tung. (1 February 2018). *ZDNet*. "Meltdown-Spectre: Malware is already being tested by attackers." Last accessed on 1 August 2018 at https://www.zdnet.com/article/meltdown-spectre-malware-is-already-being-tested-by-attackers/.

7. Tom Warren. (9 January 2018). *The Verge*. "Microsoft reveals how Spectre updates can slow your PC down." Last accessed on 1 August 2018 at https://www.theverge.com/2018/1/9/16868290/microsoft-meltdown-spectre-firmware-updates-pc-slowdown.

8. Microsoft. (3 January 2018). *Microsoft*. "January 3, 2018—KB4056892 (OS Build 16299.192)." Last accessed on 31 July 2018 at https://support.microsoft.com/en-us/help/4056892/windows-10-update-kb4056892?ranMID=24542&ranEAID=nOD%2FrLJHOac&ranSiteID=nOD_rLJHOac-D9iMSKjIaU4uYO.RnHdkpA&tduid=(ec86be2bfc16e6f8ec4721531d601e74)(256380)(2459594)(nOD_rLJHOac-D9iMSKjIaU4uYO.RnHdkpA)().

9. Kafeine. (25 May 2018). *MDNC | Malware don't need coffee*. "CVE-2018-8174 (VBScript Engine) and Exploit Kits." Last accessed on 14 August 2018 at https://malware.dontneedcoffee.com/2018/05/CVE-2018-8174.html.

10. Security Tech Center. (8 May 2018). *Microsoft*. "CVE-2018-8174 | Windows VBScript Engine Remote Code Execution Vulnerability." Last accessed on 31 July 2018 at https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8174.

11. Weibo. (20 April 2018). *Weibo*. "新型Office攻击使用浏览器"双杀"漏洞." Last accessed on 31 July 2018 at https://www.weibo.com/ttarticle/p/show?id=2309404230886689265523.

12. Miguel Ang, Martin Co, and Michael Villanueva. (31 May 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Rig Exploit Kit Now Using CVE-2018-8174 to Deliver Monero Miner." Last accessed on 31 July 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/rig-exploit-kit-now-using-cve-2018-8174-to-deliver-monero-miner/.

13. Martin Co and Joseph C. Chen. (2 July 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Down but Not Out: A Look into Recent Exploit Kit Activities." Last accessed on 31 July 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/a-look-into-recent-exploit-kit-activities/.

14. Trend Micro Zero Day Initiative Team. (23 May 2017). *Trend Micro Security News*. "Hacker Machine Interface." Last accessed on 31 July 2018 at https://documents.trendmicro.com/assets/wp/wp-hacker-machine-interface.pdf.

15. Ibid.

16. European Commission. (5 July 2016). *European Commission*. "The Directive on Security of Network and Information Systems (NIS Directive)." Last accessed on 1 August 2018 at https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

17. UK Government. (8 August 2017). *UK Government*. "New Fines for Essential Service Operators with Poor Cyber Security." Last accessed on 31 July 2018 at https://www.gov.uk/government/news/new-fines-for-essential-service-operators-with-poor-cyber-security.

18. EUGDPR.org. *EU GDPR Portal*. "GDPR Key Changes." Last accessed on 31 July 2018 at https://www.eugdpr.org/key-changes.html.

19. Justin Wetherill. (21 March 2018). *Forbes*. "Cryptocurrency Gold Rush And The Unforeseen Effect On PC Gamers." Last accessed on 1 August 2018 at https://www.forbes.com/sites/forbestechcouncil/2018/03/21/cryptocurrency-gold-rush-and-the-unforeseen-effect-on-pc-gamers/#5f4ca1f36286.

20. Menard Oseña. (28 February 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Cryptocurrency-Mining Malware: 2018's New Menace?" Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-malware-2018-new-menace/.

21. Bloomberg. (31 January 2018). *Fortune.com*. "How to Steal $500 Million in Cryptocurrency." Last accessed on 1 August 2018 at http://fortune.com/2018/01/31/coincheck-hack-how/.

22. Charlie Osborne. (13 April 2018). *ZDNet*. "Coinsecure, not so Secure: Millions in Cryptocurrency Stolen, CSO Blamed." Last accessed on 1 August 2018 at https://www.zdnet.com/article/coinsecure-not-so-secure-millions-in-cryptocurrency-stolen-cso-branded-as-thief/.

23. Bitcoin Price News. (22 June 2018). *CCN*. "Cryptocurrency Market Suffers Ongoing Decline, Analysts Weigh Causes." Last accessed on 1 August 2018 at https://www.ccn.com/cryptocurrency-market-suffers-ongoing-decline-analysts-weigh-causes/.

24. Hubert Lin. (19 January 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Struts and DotNetNuke Server Exploits Used For Cryptocurrency Mining." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/struts-dotnetnuke-server-exploits-used-cryptocurrency-mining/.

25. Chaoying Liu and Joseph C. Chen. (26 January 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Malvertising Campaign Abuses Google's DoubleClick to Deliver Cyrptocurrency Miners." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/malvertising-campaign-abuses-googles-doubleclick-to-deliver-cryptocurrency-miners/.

26. Johnlery Triunfante and Mark Vicente. (26 February 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Oracle Server Vulnerability Exploited to Deliver Double Monero Miner Payloads." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/oracle-server-vulnerability-exploited-deliver-double-monero-miner-payloads/.

27. Joseph C. Chen. (1 February 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Malicious Chrome Extensions Found in Chrome Web Store, Form Droidclub Botnet." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/malicious-chrome-extensions-found-chrome-web-store-form-droidclub-botnet/.

28. Trend Micro Cyber Safety Solutions Team. (21 March 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Cryptocurrency Miner Distributed via PHP Weathermap Vulnerability, Targets Linux Servers." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-miner-distributed-via-php-weathermap-vulnerability-targets-linux-servers/.

29. Joseph C. Chen. (22 March 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Pop-up Ads and Over a Hundred Sites are Helping Distribute Botnets, Cryptocurrency Miners and Ransomware." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/pop-up-ads-and-over-a-hundred-sites-are-helping-distribute-botnets-cryptocurrency-miners-and-ransomware/.

30. Chaoying Liu and Joseph C. Chen. (4 April 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Cryptocurrency Web Miner Script Injected into AOL Advertising Platform." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-web-miner-script-injected-into-aol-advertising-platform/.

31. Don Ladores and Angelo Deveraturda. (17 April 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Ransomware XIAOBA Repurposed as File Infector and Cryptocurrency Miner." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-xiaoba-repurposed-as-file-infector-and-cryptocurrency-miner/.

32. Lenart Bermejo and Ronnie Giagone. (21 April 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Monero-Mining RETADUP Worm Goes Polymorphic, Gets an AutoHotKey Variant." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/monero-mining-retadup-worm-goes-polymorphic-gets-an-autohotkey-variant/.

33. Joseph C. Chen. (30 April 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "FacexWorm Targets Cryptocurrency Trading Platforms, Abuses Facebook Messenger for Propagation." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/facexworm-targets-cryptocurrency-trading-platforms-abuses-facebook-messenger-for-propagation/.

34. Hubert Lin. (11 May 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Malicious Traffic in Port 7001 Surges as Cryptominers Target Patched 2017 Oracle WebLogic Vulnerability." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/malicious-traffic-in-port-7001-surges-as-cryptominers-target-patched-2017-oracle-weblogic-vulnerability/.

35. Jindrich Karasek and Loseway Lu. (26 June 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Cryptocurrency-Mining Bot Targets Devices With Running SSH Service via Potential Scam Site." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/cryptocurrency-mining-bot-targets-devices-with-running-ssh-service-via-potential-scam-site/.

36. Anita Hsieh, Rubio Wu, and Kawabata Kohei. (28 June 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "The New Face of Necurs: Noteworthy Changes to Necurs' Behaviors." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/the-new-face-of-necurs-noteworthy-changes-to-necurs-behaviors/.

37. Trend Micro Smart Home Network and IoT Reputation Service Teams. (21 June 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Drupal Vulnerability (CVE-2018-7602) Exploited to Deliver Monero-Mining Malware." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/drupal-vulnerability-cve-2018-7602-exploited-to-deliver-monero-mining-malware/.

38. Curtis Franklin, Jr. (21 March 2018). *Dark Reading*. "GandCrab Ransomware Goes 'Agile'." Last accessed on 1 August 2018 at https://www.darkreading.com/attacks-breaches/gandcrab-ransomware-goes-agile/d/d-id/1331336?ngAction=register&ngAsset=389473.

39. Raphael Centeno. (1 May 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Legitimate Application AnyDesk Bundled with New Ransomware Variant." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/legitimate-application-anydesk-bundled-with-new-ransomware-variant/.

40. Trend Micro. (11 May 2018). *Trend Micro Security News*. "SynAck Ransomware Leverages Process Doppelgänging for Evasion and Infection." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/synack-ransomware-leverages-process-doppelg-nging-for-evasion-and-infection.

41. Trend Micro. (20 February 2018). *Trend Micro Security News*. "Black Ruby Ransomware Targets Non-Iranian Users, Adds Coinminer." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/black-ruby-ransomware-targets-non-iranian-users-adds-coinminer.

42. Trend Micro. (2016). *TrendLabs Primer*. "Securing Data Through Network Segmentation in Modern Enterprises." Last accessed on 1 August 2018 at https://documents.trendmicro.com/assets/primers/securing-data-through-network-segmentation.pdf.

43. Ibid.

44. Privacy Rights Clearinghouse. (2017). *Privacy Rights Clearinghouse*. "Data Breaches." Last accessed on 2 February 2018 at https://www.privacyrights.org/data-breaches?title=&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&orsg_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&org_type%5B%5D=2437&taxonomy_vocabulary_11_tid%5B%5D=2434.

45. Privacy Rights Clearinghouse. (2018). *Privacy Rights Clearinghouse*. "Data Breaches." Last accessed on 11 July 2018 at https://www.privacyrights.org/data-breaches?title=&breach_type%5B%5D=285&breach_type%5B%5D=268&breach_type%5B%5D=267&breach_type%5B%5D=264&breach_type%5B%5D=265&breach_type%5B%5D=266&breach_type%5B%5D=269&breach_type%5B%5D=270&org_type%5B%5D=260&org_type%5B%5D=262&org_type%5B%5D=261&org_type%5B%5D=259&org_type%5B%5D=257&org_type%5B%5D=258&org_type%5B%5D=263&org_type%5B%5D=2437&taxonomy_vocabulary_11_tid%5B%5D=2436.

46. Andy Greenberg. (27 June 2018). *Wired*. "Marketing Firm Exactis Leaked a Personal Info Database with 340 Million Records." Last accessed on 1 August 2018 at https://www.wired.com/story/exactis-database-leak-340-million-records/.

47. Zack Whittaker. (24 May 2018). *ZDNet*. "T-Mobile Bug Let Anyone See Any Customer's Account Details." Last accessed on 31 July 2018 at https://www.zdnet.com/article/tmobile-bug-let-anyone-see-any-customers-account-details/.

48. Robert Abel. (19 April 2018). *SC Magazine*. "Social Media Aggregator LocalBlox Leaves 48M Records Exposed." Last accessed on 1 August 2018 at https://www.scmagazine.com/in-the-wake-of-the-facebook-cambridge-analytica-scandal-social-media-data-aggregation-firm-localblox-left-an-aws-bucket-misconfigured/article/759886/.

49. Brian Krebs. (2 April 2018). *Krebs on Security*. "Panerabread.com Leaks Millions of Customer Records." Last accessed on 31 July 2018 at https://krebsonsecurity.com/2018/04/panerabread-com-leaks-millions-of-customer-records/.

50. Mayra Rosario Fuentes and Numaan Huq. (5 April 2018). *Trend Micro*. "Securing Connected Hospitals." Last accessed on 1 August 2018 at https://documents.trendmicro.com/assets/rpt/rpt-securing-connected-hospitals.pdf.

51. ACFun. (13 June 2018). *ACFun*. "【公告】关于AcFun受黑客攻击致用户数据外泄的公." Last accessed on 1 August 2018 at http://www.acfun.cn/a/ac4405547.

52. Sooraj Shah. (18 January 2018). *The Inquirer*. "'Professional' hack on Norwegian health authority compromises data of three million patients." Last accessed on 1 August 2018 at https://www.theinquirer.net/inquirer/news/3024692/norway-health-south-east-rhf-hacked.

53. Amitai Ziv. (11 March 2018). *Haaretz*. "Data Breach Left Millions of Israeli Kids' Pictures Vulnerable to Hacking." Last accessed on 1 August 2018 at https://www.haaretz.com/israel-news/data-breach-left-millions-of-israeli-kids-pics-vulnerable-to-hacking-1.5889251.

54. Khaleej Times. (24 April 2018). *Khaleej Times*. "Dubai's Careem Admits to Data Breach of 14 Million Users." Last accessed on 1 August 2018 at https://www.khaleejtimes.com/nation/dubai//dubais-careem-admits-to-data-breach-of-14-million-users.

55. Natalie Gagliordi. (27 November 2015). *ZDNet*. "The Target Breach, Two Years Later." Last accessed on 1 August 2018 at https://www.zdnet.com/article/the-target-breach-two-years-later/.

56. Dean Takahashi. (10 July 2018). *VentureBeat*. "IBM Security Study: Mega Data Breaches Cost $40 Million to $350 Million." Last accessed on 1 August 2018 at https://venturebeat.com/2018/07/10/ibm-security-study-mega-data-breaches-cost-40-million-to-350-million/.

57. Trend Micro. *Trend Micro*. "EU General Data Protection Regulation (GDPR)." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/security/definition/eu-general-data-protection-regulation-gdpr.

58. Trend Micro IoT Reputation Service Team. (11 April 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Mirai-like Scanning Activity Detected From China, With Targets in Brazil." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/mirai-like-scanning-activity-detected-from-china-targets-in-brazil/.

59. Trend Micro. (26 October 2016). *Trend Micro TrendLabs Security Intelligence Blog*. "The Internet of Things Ecosystem is Broken. How Do We Fix It?" Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/internet-things-ecosystem-broken-fix/.

60. Brian Krebs. (1 Ocotber 2016). *Krebs on Security*. "Source Code for IoT Botnet 'Mirai' Released." Last accessed on 1 August 2018 at https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/.

61. Trend Micro IoT Reputation Service Team. (11 April 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Mirai-like Scanning Activity Detected From China, With Targets in Brazil." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/mirai-like-scanning-activity-detected-from-china-targets-in-brazil/.

62. Fernando Mercês. (17 April 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Not Only Botnets: Hacking Group in Brazil Targets IoT Devices With Malware." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/not-only-botnets-hacking-group-in-brazil-targets-iot-devices-with-malware/.

63. Trend Micro IoT Reputation Service Team and Trend Micro Smart Home Network Team. (21 May 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "GPON Vulnerabilities Exploited for Mexico-based Mirai-like Scanning Activities." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/gpon-vulnerabilities-exploited-for-mexico-based-mirai-like-scanning-activities/.

64. Trend Micro. (24 October 2017). *Trend Micro Security News*. "Millions of Networks Compromised by New Reaper Botnet." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/millions-of-networks-compromised-by-new-reaper-botnet.

65. Trend Micro. (24 May 2018). *Trend Micro Security News*. "Reboot Your Routers: VPNFilter Infected Over 500,000 Routers Worldwide." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/reboot-your-routers-vpnfilter-infected-over-500-000-routers-worldwide.

66. Kevin Y. Huang, Fernando Mercês, and Lion Gu. (14 December 2016). *Trend Micro TrendLabs Security Intelligence Blog*. "Home Routers: Mitigating Attacks That Can Turn Them to Zombies." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/home-routers-mitigating-attacks-that-turn-them-to-zombies/.

67. Trend Micro. (24 October 2017). *Trend Micro Security News*. "Millions of Networks Compromised by New Reaper Botnet." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/millions-of-networks-compromised-by-new-reaper-botnet.

68. Trend Micro. (24 May 2018). *Trend Micro Security News*. "Reboot Your Routers: VPNFilter Infected Over 500,000 Routers Worldwide." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/reboot-your-routers-vpnfilter-infected-over-500-000-routers-worldwide.

69. Brian Krebs. (1 October 2016). *Krebs on Security*. "Source Code for IoT Botnet 'Mirai' Released." Last accessed on 1 August 2018 at https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/.

70. Federal Bureau of Investigation Internet Crime Commission. (25 May 2018). *FBI IC3*. "Foreign Cyber Actors Target Home and Office Routers and Networked Devices Worldwide." Last accessed on 1 August 2018 at https://www.ic3.gov/media/2018/180525.aspx.

71. Tony Yang and Peter Lee. (13 July 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "VPNFilter-affected Devices Still Riddled with 19 Vulnerabilities." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/vpnfilter-affected-devices-still-riddled-with-19-vulnerabilities/.

72. Trend Micro. (10 May 2018). *Trend Micro Virus Encyclopedia*. "X2KM_POWLOAD.AOEDT Virus Definition." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/x2km_powload.aoedt.

73. Michael Villanueva and Martin Co. (14 June 2018). *Trend Micro TrendLabs Security Intelligence Blog*. "Another Potential MuddyWater Campaign uses Powershell-based PRB-Backdoor." Last accessed on 1 August 2018 at https://blog.trendmicro.com/trendlabs-security-intelligence/another-potential-muddywater-campaign-uses-powershell-based-prb-backdoor/.

74. Jai Vijayan. (10 May 2018). *Dark Reading*. "Author of TreasureHunter PoS Malware Releases Its Source Code." Last accessed on 1 August 2018 at https://www.darkreading.com/vulnerabilities---threats/author-of-treasurehunter-pos-malware-releases-its-source-code-/d/d-id/1331778.

75. Ionut Arghire. (16 March 2018). *Security Week*. "PinkKite POS Malware Is Small But Powerful." Last accessed on 31 July 2018 at https://www.securityweek.com/pinkkite-pos-malware-small-powerful.

76. John Wilson. (29 March 2018). *Forbes*. "Tax Time is W-2 Scam Time." Last accessed on 1 August 2018 at https://www.forbes.com/sites/forbestechcouncil/2018/03/29/tax-time-is-w-2-scam-time/#41578ee652fa.

77. Trend Micro. (5 December 2017). *Trend Micro*. "Paradigm Shifts." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2018.

78. Federal Bureau of Investigation. (12 July 2018). *FBI IC3*. "Business Email Compromise: The 12 Billion Scam." Last accessed on 1 August 2018 at https://www.ic3.gov/media/2018/180712.aspx.

79. Federal Bureau of Investigation. (11 June 2018). *FBI*. "International Business E-Mail Compromise Takedown." Last accessed on 1 August 2018 at https://www.fbi.gov/news/stories/international-bec-takedown-061118.

80. Trend Micro. (16 April 2018). *Trend Micro Security News*. "Curbing the BEC Problem Using AI and Machine Learning." Last accessed on 1 August 2018 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/curbing-the-bec-problem-using-ai-and-machine-learning.

81. Careem. (23 April 2018). *Careem*. “Important Security Information.” Last accessed on 1 August 2018 at https://blog.careem.com/en/security/.

82. Paul Farrelll. (2 May 2018). *Buzzfeed News*. “Australia’s Largest Bank Lost The Personal Financial Histories Of 12 Million Customers.” Last accessed on 1 August 2018 at https://www.buzzfeed.com/paulfarrell/australias-largest-bank-lost-the-personal-financial?utm_term=.so2yyQbV8K#.qqGaakAm2X.

83. DataBreaches.net. (16 March 2018). *DataBreaches.net*. “National Lottery Hacked: 10.5M Players are Warned to Change Their Passwords.” Last accessed on 1 August 2018 at https://www.databreaches.net/national-lottery-hacked-10-5m-players-are-warned-to-change-their-passwords/.

84. Zurairi Ar. (9 June 2018). *MSN*. “Putrajaya’s Exam Portal Shut Down, After Data Breach Affecting Millions.” Last accessed on 1 August 2018 at https://www.msn.com/en-us/news/national/putrajaya%E2%80%99s-exam-portal-shut-down-after-data-breach-affecting-millions/ar-AAyrb5c?li=AAaD1A0.

85. Global Times. (13 June 2018). *Global Times*. “Hackers Attack Popular Video-Sharing Site, Breach Millions of Private Info.” Last accessed on 1 August 2018 at http://www.globaltimes.cn/content/1106860.shtml.

86. Rory Cellan-Jones. (31 July 2018). *BBC News*. “Dixons Carphone Says Data Breach affected 10 Million.” Last accessed on 1 August 2018 at https://www.bbc.com/news/business-45016906.

87. Amitai Ziv. (11 March 2018). *Haaretz*. “Data Breach Left Millions of Israeli Kids’ Pictures Vulnerable to Hacking.” Last accessed on 1 August 2018 at https://www.haaretz.com/israel-news/data-breach-left-millions-of-israeli-kids-pics-vulnerable-to-hacking-1.5889251.

88. JKR Staff. (24 March 2018). *Janta Ka Reporter*. “Revealed! Personal Data of 50 Lakh Ex-servicemen May Have Been Breached, Armed Forces Veteran Calls It Chilling.” Last accessed on 1 August 2018 at http://www.jantakareporter.com/india/personal-data-50-lakh-ex-servicemen-may-breached/177927/.

89. Sooraj Shah. (18 January 2018). *The Inquirer*. “‘Professional’ hack on Norwegian health authority compromises data of three million patients.” Last accessed on 1 August 2018 at https://www.theinquirer.net/inquirer/news/3024692/norway-health-south-east-rhf-hacked.

90. Jason Murdock. (7 February 2018). *International Busines Times*. “Swisscom data breach: Personal details of one in ten Swiss citizens stolen.” Last accessed on 1 August 2018 at https://www.ibtimes.co.uk/swisscom-data-breach-personal-details-one-ten-swiss-citizens-stolen-1659593.

91. Zack Whittaker. (1 March 2018). *ZDNet*. “French News Site L’Express Exposed Reader Data Online, Weeks Before GDPR Deadline.” Last accessed on 1 August 2018 at https://www.zdnet.com/article/french-magazine-lexpress-exposed-reader-data/.

92. Channel News Asia. (20 February 2018). *Channel News Asia*. “HardwareZone Forum Hit by Security Breach; 685,000 User Profiles Affected.” Last accessed on 1 August 2018 at https://www.channelnewsasia.com/news/singapore/hardwarezone-hwz-security-breach-685000-user-profiles-affected-9975156.

93. Joji Simon. (17 February 2018). *On Manorama*. “Data breach again: Salary bill of Supplyco staff leaked on WhatsApp.” Last accessed on 1 August 2018 at https://english.manoramaonline.com/news/kerala/2018/02/16/data-breach-salary-bill-of-supplyco-staff-leaked-on-whatsapp.html.

94. Kostiantyn Tsentsura. (7 February 2018). *Kyiv Post*. “Personal data of 500,000 Nova Poshta Clients Allegedly Leaked to Dark Web.” Last accessed on 1 August 2018 at https://www.kyivpost.com/technology/personal-data-500000-nova-poshta-clients-allegedly-leaked-dark-web.html.

95. Danny Mok. (18 April 2018). *South China Morning Post*. "Personal Data of Some 380,000 Hong Kong Broadband Customers Hacked, Service Provider Says." Last accessed on 1 August 2018 at https://www.scmp.com/news/hong-kong/law-crime/article/2142317/personal-data-some-380000-hong-kong-broadband-customers.

96. Rose Behar. (12 February 2018). *Mobile Syrup*. "Hacker Uncovers Freedom Mobile Customer Login Vulnerability." Last accessed on 1 August 2018 at https://mobilesyrup.com/2018/02/12/freedom-mobile-security-breach/.

97. Chisato Tanaka. (26 June 2018). *The Japan Times*. "Prince Hotels Hack Results in Loss of 124,000 Customers' Credit Card Numbers, Other Data." Last accessed on 1 August 2018 at https://www.japantimes.co.jp/news/2018/06/26/business/corporate-business/prince-hotels-hack-results-loss-124000-customers-credit-card-numbers-data/#.WzNPNadKhPY.

98. Christine Dobby. (23 January 2018). *The Globe and Mail*. "Police Probing Bell Canada Data Breach; Up to 100,000 Customers Affected." Last accessed on 1 August 2018 at https://www.theglobeandmail.com/report-on-business/police-probing-bell-canada-data-breach-up-to-100000-customers-affected/article37701579/.

TREND MICRO™ 트렌드마이크로

트렌드마이크로
서울특별시 강남구 영동대로 416 KT&G타워 3층 (우 06176)
TEL. 02-561-0990
FAX. 02-561-0660
www.trendmicro.co.kr

보고서 문의 : pr@trendmicro.co.kr
영업 문의 : sales@trendmicro.co.kr
기술 문의 : support@trendmicro.co.kr

TREND MICRO™

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and investigation, enabling better, faster protection. With over 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro secures your connected world. For more information, visit www.trendmicro.com.