패러다임의 변화

2018년 트렌드마이크로 보안 예측 보고서

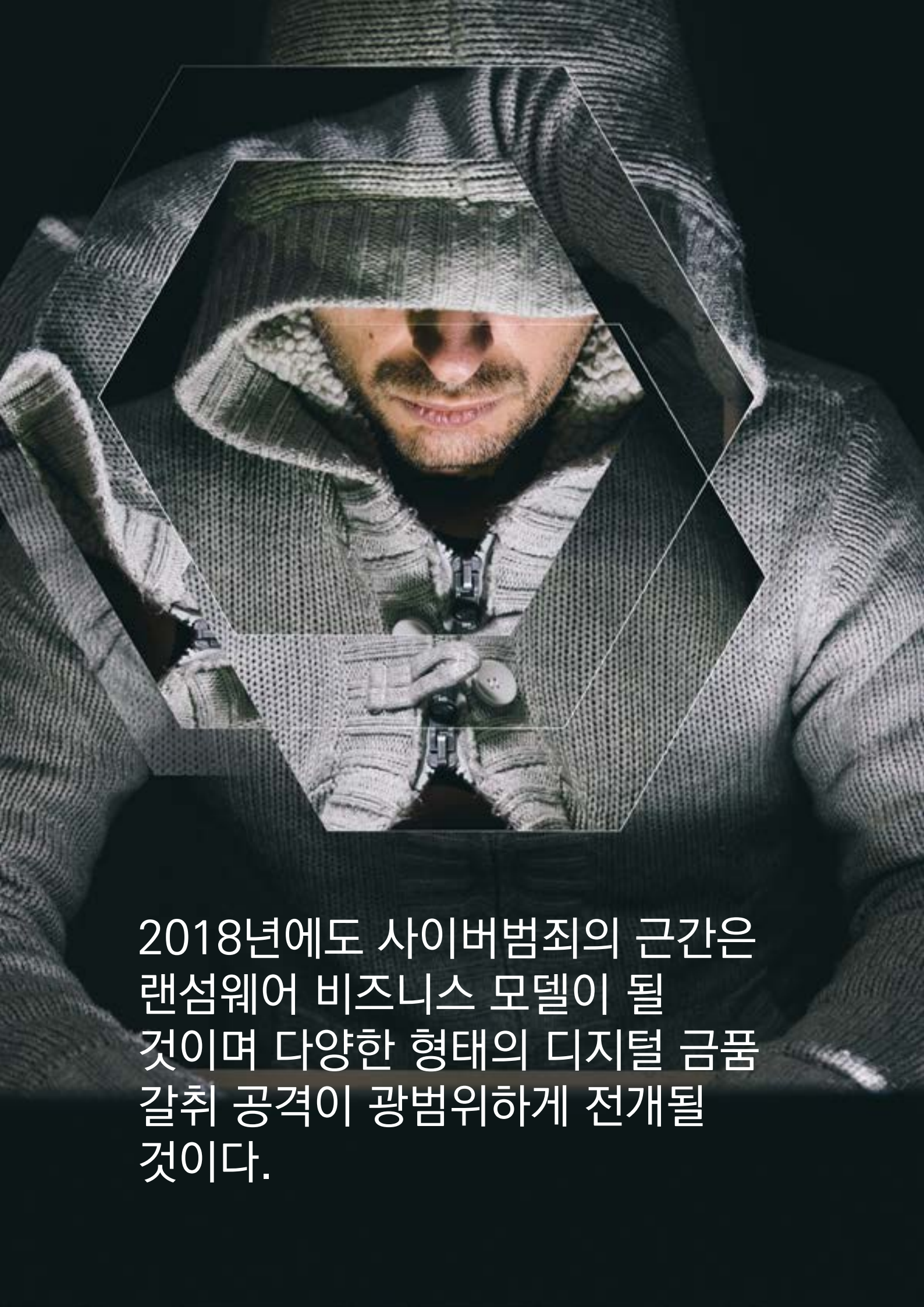
공격 수단의 기반이 되는 두 가지 요소는 기술과 리소스이지만 시스템의 취약점을 제대로 파악하지 못하는 공격자들은 보안을 침해하거나 효과적인 공격을 시도할 수 없습니다. 대규모 멀웨어 공격, 이메일을 이용한 금품 갈취, 기기 해킹 및 서비스 방해와 같은 위협들은 모두 기술적 취약점이나 사람의 취약점과 같은 네트워크 상의 취약점을 이용합니다.

보안 수준이 낮은 네트워크를 통한 연결과 상호 작용이 계속 증가하는 추세이지만 안타깝게도 발생되는 위협에 대처할 수 있는 기술 구현은 매우 열악한 상황입니다. 오늘날과 같이 위협들이 끊임없이 진화하는 환경에서는 적기 적소에 보안을 구현하는 것이 매우 중요합니다.

2018년은 디지털 금품 갈취형 공격이 사이버범죄자들의 비즈니스 모델의 근간이 될 것이며 이를 통해 엄청난 수익을 낼 수 있는 다양한 공격 전술들이 전개될 것입니다. IoT 기기들이 점차 스마트 환경과 접목되면서 이러한 IoT 기기들의 취약점들이 사이버범죄자들의 공격 기회를 확대시킬 것입니다. 그리고 비즈니스 이메일 사기 행위를 통해 금전적 피해를 입게 될 조직들이 증가할 것이며 가짜 뉴스와 사이버선전이 활개치는 시대에도 고전적 사이버범죄 기술이 계속 사용될 것입니다. 머신 러닝과 블록체인 어플리케이션은 기대와 함정을 모두 가지고 있습니다. 내년에는 EU의 개인정보보호규정(GDPR)이 시행됨에 따라 기업들은 해당 지침을 수용해야 하는 난제를 해결해야 합니다. 기업들은 취약점 문제에 시달릴 뿐 아니라 내부 프로세스 상의 허점이 악용되어 상당한 업무 방해 피해를 입게 될 수도 있습니다.

이러한 위협들이 2018년에 주류를 이루게 될 것으로 전망되며 이는 곧 기존의 보안 솔루션만으로 위협들을 해결할 수 없다는 것을 의미합니다. 환경이 점차 상호 연결되고 복잡해짐에 따라 위협도 진화하므로 보안에 대한 우리의 태세를 재정립해야 합니다.

트렌드마이크로는 기존 및 신생 위협들뿐 아니라 위협 상황에 맞는 맞춤 보안 솔루션도 조사하고 있습니다. 본 보고서를 통해 2018년에 중요성이 더욱 높아질 보안 영역에 대해 올바른 정보를 기반으로 의사 결정을 내릴 수 있는 방법을 확인해보십시오.



2018년에도 사이버범죄의 근간은 랜섬웨어 비즈니스 모델이 될 것이며 다양한 형태의 디지털 금품 갈취 공격이 광범위하게 전개될 것이다.

2017년 예측 보고서에서는 사이버범죄자들이 랜섬웨어를 다양하게 활용한 공격 수법을 전개할 것으로 예측했었는데 실제로 WannaCry나 Petya처럼 빠르게 전파되는 네트워크 공격, Locky와 FakeGlobe의 광범위한 스팸 전파, 그리고 동유럽 국가를 대상으로 한 BadRabbit의 워터링 홀 공격이 활개를 친 한 해였습니다.

당분간은 랜섬웨어가 쇠퇴할 것으로 기대되진 않습니다. 다양한 형태의 디지털 금품 갈취가 만연해짐에 따라 2018년에는 랜섬웨어가 더 큰 활약을 할 것으로 예상됩니다. 사이버범죄자들은 피해자들로 하여금 금품을 지불하도록 유도하는 도구로써 데이터를 활용하고 있습니다. 지하경제 포럼이 여전히 서비스 형태의 랜섬웨어(RaaS)를 제공하고 있고 랜섬을 받기 위한 안전한 방법으로 비트코인을 사용할 수 있기 때문에 사이버범죄자들은 이러한 비즈니스 모델에 더욱 주력할 것입니다.

디지털 금품 갈취를 위한 효과적인 수단인 랜섬웨어

여러 해에 걸쳐 이루어진 사이버범죄 전술의 진화 과정을 살펴보면 사이버범죄자들은 사용자들을 속여 자격 증명을 수집하는 방법 대신 직접적으로 금품을 갈취하는 방법을 채택하고 있습니다. 초기 온라인 위협들은 개인 정보를 훔치기 위해 뱅킹 거래를 하이재킹하는 멀웨어와 인포스틸러에 주로 의존하였습니다. 이는 안티멀웨어 솔루션(FAKEAV)으로 가장하여 사용자들이 가짜 소프트웨어를 다운로드받도록 하여 멀웨어를 전파하고 사용자가 감염된 컴퓨터에 액세스하려면 돈을 내야 하는 방식입니다. 랜섬웨어는 이러한 FAKEAV를 모방하여 한 단계 더 진화하였습니다.

최근 랜섬웨어 공격을 통한 금품 갈취의 효과가 입증되면서 사이버범죄자들은 고수익 창출 가능성이 높은 피해자들로부터 더 많은 금품을 갈취할 방법을 모색할 것입니다. 공격자들은 피해자의 범위를 확대하기 위해 랜섬웨어 페이로드가 포함된 이메일을 대량 발송하는 피싱 공격을 지속적으로 전개할 것으로 예상됩니다. 또한 IIoT(산업용 사물 인터넷) 환경의 단일 조직을 표적으로 하여 운영을 방해하고 생산라인에 영향을 미치는 랜섬웨어 공격으로 더 큰 규모의 수익 창출을 도모할 것입니다. 우리는 이미 대규모 WannaCry 및 Petya 사건을 통해 이를 확인한 바 있으며 이러한 수익 창출이 위협의 궁극적인 목표가 될 것입니다.

사이버범죄자들의 주요 비즈니스 모델

2018	랜섬웨어와 디지털 금품 갈취가 사이버범죄자들의 핵심 공격 수단이 될 것이다.
2017	WANNACRY와 PETYA의 예기치 못한 랜섬웨어 공격
2016	신종 랜섬웨어 패밀리가 752%나 증가하였고 서비스형태의 랜섬웨어(RaaS)가 출현하였다.
2015	랜섬웨어가 지속적으로 증가하고 시스템을 암호화하여 비트코인을 통한 지불을 요구하는 공격이 계속되었다.
2014	랜섬웨어 BITCRYPT가 파일들을 암호화하고 비트코인을 통한 지불을 요구하였다.
2013	랜섬웨어 CRYPTOLOCKER가 파일을 암호화하고, 시스템을 잠근 후 300달러를 요구하였다.
2011	데이터 침해 공격을 통해 훔친 개인 정보와 금융 정보가 사이버범죄자들의 지하 경제에서 거래되었다.뱅킹 트로얀 SPYEYE가 금융 정보와 수백만 달러의 금품을 탈취하였다.
2010	안드로이드 트로얀 DROIDSMS가 출현하였고 무단으로 할증 요금이 지불되는 SMS를 전송하였다.
2009	STUXNET이 패치되지 않은 취약점을 통해 주요 인프라에 침투하였다.
2008	KOOBFACE이 페이스북을 통해 전파되었고 페이스북, 트위터 및 기타 소셜 미디어 네트워크에서 사용자 정보를 무단 수집하였다. FAKEAV가 가짜 안티바이러스 경고 메시지를 이용하여 신용카드 정보를 무단 수집하였다.
2007	인포스틸러 ZEUS가 발견되었다.
2004	키 입력을 기록하거나 뱅킹 인터페이스를 변경시키는 온라인 뱅킹 멀웨어가 널리 퍼졌다.

출처:
http://blog.trendmicro.com/trendlabs-security-intelligence/threat-morphosis/
https://www.trendmicro.com/vinfo/us/security/definition/ransomware
https://documents.trendmicro.com/assets/rpt/rpt-setting-the-stage.pdf

개인정보보호규정이 시행되면 금품 갈취 공격도 활동을 개시할 것입니다. 사이버범죄자들은 개인정보보호규정에 포함된 개인 정보를 표적으로 하여 기업들에게 연간 총매출의 최대 4퍼센트에 달하는 엄청난 규정 위반 벌금 대신 그들에게 금품을 지불하도록 요구할 것입니다. 기업들은 사이버범죄자들이 금융 정보를 공개하고 이로 인해 기업에게 부과될 엄청난 개인정보보호규정 위반 벌금 규모에 따라 사이버범죄자들이 책정한 랜섬 비용을 지불하게 될 것이며 이로 인해 정보 유출 시도와 랜섬 요구가 증가할 것입니다. 이 외에도 우리는 과거 저작권 침해 및 경찰 경고문이 FAKEAV 및 랜섬웨어 공격에 이용되었던 것과 유사한 방식으로 개인정보보호규정 역시 소셜 엔지니어링 전술로 사용될 것으로 예상하고 있습니다.

사용자와 기업들은 효과적인 웹 및 이메일 게이트웨이 솔루션을 최전방 방어 수단으로 구현함으로써 이러한 디지털 금품 갈취 공격에 대처할 수 있습니다. 하이파이 머신 러닝, 활동 모니터링 및 취약점 방어 기능을 갖춘 솔루션은 위협들이 표적 시스템에 침투하지 못하도록 차단합니다. 이 기능들은 기존 솔루션들에 의해 쉽게 탐지되었던 악성 페이로드나 바이너리를 이용하지 않고 파일리스(fileless) 전달 방식을 이용하는 랜섬웨어 변종을 차단하는데 특히 효과적입니다.

사이버범죄자들이 IOT 기기를
악용하기 위한 새로운 방법을
모색할 것이다.

디지털 비디오 리코더(DVR), IP 카메라 및 라우터와 같은 IoT 기기들을 하이재킹한 대규모 Mirai 및 Persirai DDoS 공격을 통해 상호 연결된 기기들이 얼마나 취약하고 쉽게 붕괴될 수 있는 지에 대한 논의가 제기되고 있습니다. 최근 Mirai 코드를 기반으로 한 IoT 봇넷, Reaper가 발견되었는데 이는 상호 연결된 다양한 기기들을 감염시키는 수단으로 널리 이용되고 있었습니다.

사이버범죄자들은 DDoS 공격 외에도 사법부가 범죄수사와 감염 후 범죄과학을 위해 주로 IP 주소와 로그를 참조한다는 점을 고려하여 자신의 위치와 웹 트래픽에 혼선을 야기시키는 프록시를 생성하기 위해 IoT 기기에 관심을 돌릴 것으로 예상됩니다. 익명 기기들로 이루어진 대규모 네트워크(기본 설정된 자격 증명으로 실행되고 로그가 없는)는 감염된 네트워크 내에서 사이버범죄자들이 자유롭게 악의적 활동을 할 수 있는 발판이 될 수 있습니다.

제조사들이 안전하게 설계되지 않은 기기들을 시장에 출시하게 된다면 그만큼 더 많은 IoT 취약점들이 발견될 것이며 IoT 기기의 패칭은 PC 패칭처럼 간단하지 않기 때문에 위험이 더욱 가중될 것입니다. 픽스가 발표되지 않았거나 최신 버전으로 업데이트되지 않은 안전하지 않은 한 대의 기기가 중앙 네트워크로 침투하는 진입점이 될 수 있습니다. KRACK 공격은 무선 연결 자체만으로도 보안 문제를 가중시킬 수 있다는 것을 보여준 사례입니다. 이 취약점이 WPA2 프로토콜에 연결하는 거의 모든 기기를 감염시키면서 연결된 환경에서 보편적으로 사용될 5세대 기술에 대한 의구심을 불러일으키고 있습니다.

사이버범죄의 표적이 될 수 있는 기기들

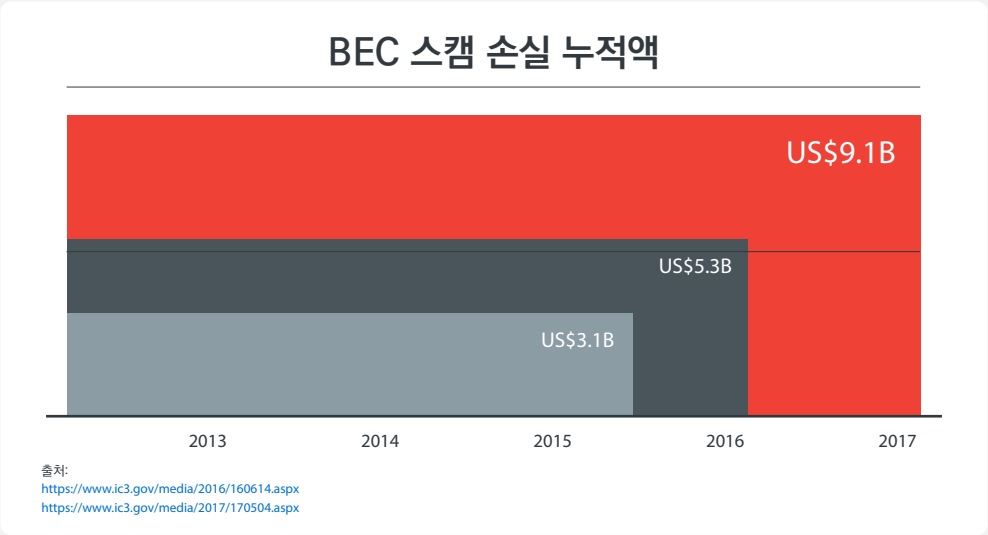
수십만 개의 드론들이 미국 영공에서 활개를 치기 시작했지만 드론 기기에 대한 관리 감독은 쉽지 않을 전망입니다. 최근 드론 관련 사고나 충돌 사고에 대한 기사를 종종 접하게 되는데 이는 시작에 불과하며 해커들은 이미 컴퓨터에 액세스하여 기밀 정보를 입수한 후 드론으로 배달되는 물품을 하이재킹하고 있습니다. 마찬가지로 무선 스피커나 음성 인식 기기와 같이 가정에서 널리 이용되는 기기들을 통해서도 해커들은 집의 위치를 파악하고 침입을 시도할 수 있게 될 것입니다.

이 외에도 2018년에는 웨어러블 기기와 의료 기기를 통한 바이오해킹 사례도 발생될 것으로 예측됩니다. 심박수 측정기와 피트니스 밴드와 같은 생체 활동 측정기 역시 해커들이 사용자에 대한 정보를 수집하는 데에 악용될 수 있습니다. 생명유지용 심장 심박기에서도 취약점이 발견되었고 이는 치명적 공격에 악용될 수 있습니다.

신기술 사용자와 규제자들이 반드시 숙지해야 할 것은 IoT 기기들이 보안 강화는 고사하고 기본적인 보안도 갖추고 있지 않는 경우가 많다는 것입니다. 제조업체가 정기적으로 위험 평가와 보안 감사를 실시하지 않을 경우 기기들은 공격에 무방비상태가 될 것입니다. 사용자들 역시 기기의 보안 설정에 대한 책임이 있는데 이는 기본 설정된 암호를 변경하고 정기적으로 펌웨어 업데이트를 설치하는 정도로 간단한 작업입니다.

2018년에는 비즈니스 이메일
사기로 인한 손실액이 미화
90억을 초과할 것이다.

FBI에 따르면 2015년 1월부터 2016년 12월까지 전 세계 백여 국가에서 BEC 스캠(업무 송금 유도 이메일 사기)이 보고되었고 이로 인해 발생된 손실액도 2,370%나 급증하였습니다. 사이버범죄자들의 BEC 스캠은 현실 세계에서의 강도 행위와 같은 것이기 때문에 놀랄만한 결과는 아닙니다. BEC 스캠은 신속하게 진행되고 최소한의 정찰활동만 요구되며 손실액이 미화 50억 달러에 달한 사례에서도 알 수 있듯이 표적에 따라 엄청난 수익을 창출할 수 있습니다.



2018년에는 BEC 스캠 사고가 크게 증가하여 전 세계적으로 미화 90억 달러*의 손실이 야기될 것으로 예측됩니다. 이와 같은 예상 손실액의 증가는 BEC 스캠과 이들의 전술이 널리 알려지면서 스캠을 발견하여 신고하는 사례가 증가하기 때문일 수도 있습니다. 하지만 주된 이유는 피싱 방식을 이용한 BEC 스캠이 매우 효과적인 것으로 입증되었기 때문에 더욱 빈번하게 사용될 것이기 때문입니다. 특히 기업 경영진으로 가장하여 송금을 유도하는 BEC 스캠은 계속 증가할 것으로 전망됩니다. 흥미로운 점은 BEC 스캐머들이 키로거(keylogger)를 설치하지 않고 피싱 PDC와 사이트를 이용한다는 것인데 크리핑(crypting) 서비스를 이용하는 키로거보다 저렴하기 때문입니다. 하지만 피싱을 이용하여도 저비용으로 계정을 해킹할 수 있습니다.

소셜 미디어나 기업 웹사이트를 통해 표적 조직의 계층을 쉽게 파악할 수 있다는 점과 이메일의 간결성 때문에 BEC 스캠은 수익을 창출할 수 있는 매우 효과적인 수법으로 자리잡았습니다. 장기전도 개의치 않는 사이버범죄자들이 지속적으로 사용할 것으로 예측되는 또 다른 기업 대상 금품 갈취 위협은 바로 Business Process Compromise(BPC)입니다. BPC 공격을 이용하는 사이버범죄자들은 (기업 공급 체인의 취약점을 악용하여)내부 프로세스를 변경하여 거액의 갈취하기 위해 조직의 내부(특히 재무부서)의 업무를 조사합니다. 하지만 BPC 공격은 장기적 계획과 많은 작업이 요구되기 때문에 공격이 용이하고 간편한 BEC에 비해 2018년에는 뉴스 헤드라인을 장식할 일이 훨씬 적을 것입니다.

BEC는 소셜 엔지니어링에 의존하기 때문에 적절한 직원 교육을 통해 충분히 막을 수 있습니다. 기업들은 내부 프로세스, 특히 거래 업무 시 엄격한 업무 규정을 적용해야 합니다. 대기업뿐 아니라 중소기업들도 전화통화와 같은 다른 통신 채널을 이용하는 중복 확인 방식을 도입해야 합니다. 이 외에도 소셜 엔지니어링 기법와 조작된 행위(forged behaviors)를 정확하게 탐지하는 웹 및 게이트웨이 솔루션을 통해서도 BEC 위협을 차단할 수 있습니다.

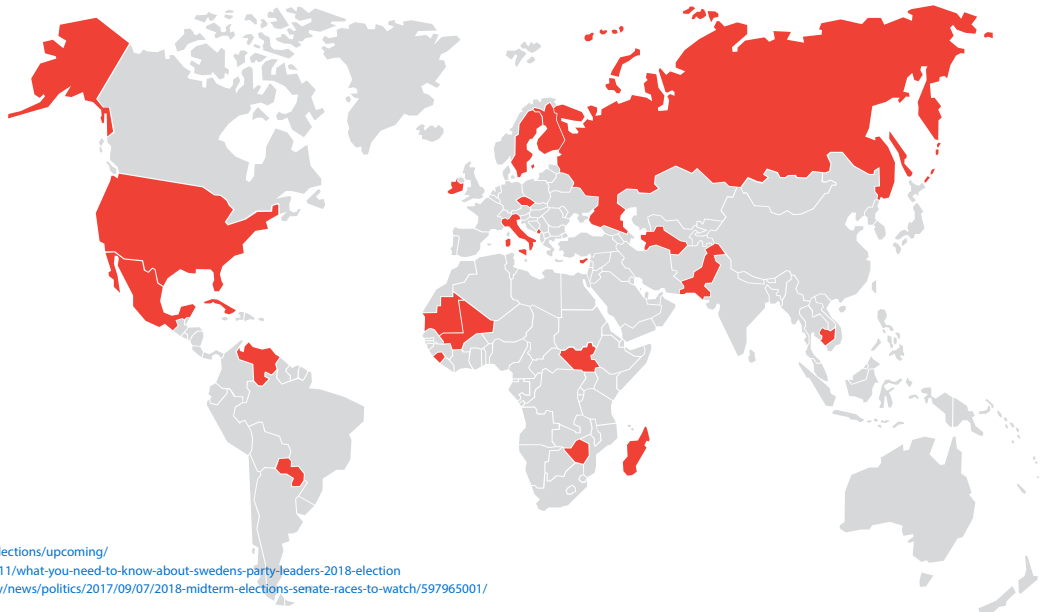
* 미화 90만 달러는 2016년 6월부터 12월까지의 월평균 손실액을 계산한 후 12를 곱해서 산출한 금액이며 BEC 사고 및 피해자의 수가 증가하지 않은 것으로 가정하였습니다.

사이버선전 공격은 기존 스팸 공격에 사용되었던 효과적인 기법을 도입하여 더욱 강력해질 것이다.

가짜 뉴스의 세 가지 구성요소는 선전의 근간이 되는 동기, 가짜 뉴스의 플랫폼으로 사용될 소셜 네트워크 그리고 이러한 뉴스를 전달하는데 사용될 도구와 서비스입니다. 2018년에는 이메일과 웹을 통해 스팸이 전파된 것처럼 사이버선전 역시 친숙한 기술을 통해 전파될 것으로 예측됩니다.

일례로, 소프트웨어 형태의 Do-it-yourself (DIY) 키트를 통해 소셜 미디어 스팸 작업을 자동화할 수 있습니다. 블랙햇 검색엔진최적화(SEO)도 소셜 미디어 최적화(SMO)에 도입되어 다른 플랫폼으로 트래픽과 방문 횟수를 제공하는 수십만 명의 사용자 기반을 확보하게 되었습니다. 외무부에 전송되는 스피어피싱 이메일에서부터 정부 당국의 권위를 떨어뜨리는 문서를 퍼뜨리는 등 불확실한 내용을 무분별하게 전파하여 자극적인 의견을 공론화하거나 실제로 시위를 일으킬 수도 있습니다.

2018년 총선거나 의원선거 또는 대통령선거가 예정되어 있는 국가들



출처:
http://www.electionguide.org/elections/upcoming/
https://www.thelocal.se/20170911/what-you-need-to-know-about-swedens-party-leaders-2018-election
https://www.usatoday.com/story/news/politics/2017/09/07/2018-midterm-elections-senate-races-to-watch/597965001/

날조된 정보는 기업들의 상황을 악화시킬 수도 있고 그들의 성과와 명성을 훼손시킬 수도 있습니다. 연구원들은 원본과 가짜를 구별하기 어렵게 만들기 위해 원본처럼 보이는 푸티지(footage)를 삽입할 수 있도록 허용하는 오디오 및 비디오 조작 도구들도 조사하고 있습니다. 지하 경제 시장에서 제공되는 도구와 서비스를 이용한 조작된 정치 캠페인은 흠집내기 전술을 통해 대중들의 인식을 좌지우지할 수도 있습니다.

다가오는 스웨덴 총선거에서도 가짜 뉴스를 이용해 선거 결과에 영향을 미치려는 시도가 이루어질 것입니다. 지난 미국 대통령 선거에서의 불법적 개입과 트위터 영향력자에 의한 "댓글농장"처럼 사회적 분열을 조장하는 메시지를 증폭시킬 수 있는 소셜 미디어의 영향력은 미국 중간 선거에서도 이어질 전망입니다.

가짜 뉴스가 게시되고 전파될 때마다 동일한 내용을 지속적으로 접하게 되는 독자들은 그러한 내용에 익숙해지고 결국엔 진실로 받아들일 수 있습니다. 뉴스 전파자들이 효과성이 입증된 기법을 이용하기 때문에 가짜 뉴스와 진짜 뉴스를 구별할 수 있는 안목을 갖추기가 매우 어려울 것입니다.

조작된 내용을 탐지하거나 차단할 수 있는 신뢰할 수 있는 방법이 아직까지는 없기 때문에 가짜 뉴스와 사이버선전이 계속 활개를 칠 것입니다. 구글이나 페이스북과 같은 유명한 소셜 미디어 사이트는 그룹에 전파되는 가짜 정보와 피드에 대한 엄중한 단속을 약속하였지만 지금까지는 그러한 단속의 영향력이 미비한 수준입니다. 상황이 이렇기 때문에 진짜와 가짜를 구별하는 최종 심사는 여전히 사용자들의 몫이 될 것입니다. 사용자들이 가짜 뉴스에 대해 제대로 인식하지 못하는 한 이러한 내용들은 온라인에서 지속적으로 퍼져나가 분별력이 부족한 독자들에게 전달될 것입니다.

위협 행위자들은 머신 러닝과
블록체인 기술을 이용하여
회피 기법을 강화할 것이다.

알려지지 않은 것을 알아내는 것이 바로 러닝 머신의 핵심 기능들 중 하나이며 러닝 머신은 의도적으로 프로그래밍하지 않고 컴퓨터가 스스로 학습할 수 있도록 하는 프로세스입니다. 상대적으로 신생 기술이긴 하지만 머신러닝은 엄청난 잠재성을 가지고 있습니다. 머신러닝의 역할은 데이터 분석과 통찰력 확보를 위한 것만은 아닙니다. 머신러닝은 입력되는 방대한 데이터를 통해 컴퓨터가 스스로 학습을 하도록 합니다. 즉 머신러닝은 소스로부터 수집하는 상황 정보에 따라 정확도가 결정될 수 있습니다.

미래에는 머신러닝이 보안 솔루션의 핵심 요소가 될 것입니다. 머신러닝은 보다 정확하고 타게팅된 의사 결정을 내리는 데에 있어선 엄청난 잠재력을 발휘하겠지만 멀웨어를 앞설 수 있을 것인가라는 질문을 생각해보게 됩니다.

CERBER 랜섬웨어는 멀웨어가 악의적으로 보이지 않게 패키징되어 있어서 특정 머신러닝 솔루션들이 탐지하지 못하는 로더(loader)를 사용하였습니다. 이는 실행 또는 에뮬레이션 없이 파일을 분석하는 사전 실행(pre-execution) 방식의 머신 러닝을 이용하는 소프트웨어에게 있어선 상당히 문제가 될 수 있는데 WannaCry를 모방한 UIWIX 랜섬웨어의 경우 사전 실행(pre-execution) 머신 러닝이 탐지하여 차단해야 할 파일이 아예 존재하지 않기 때문입니다.

머신 러닝은 강력한 도구이지만 완벽한 도구는 아닙니다. 연구원들이 러닝머신의 트래픽 검사와 제로데이 익스플로잇 탐지 능력을 조사하고 있지만 사이버범죄자들 역시 제로 데이 탐지 기능보다 한 발 앞서 나가기 위해 이 기능을 이용할 것입니다. 도로표지판을 살짝 조작해 놓을 경우 자율운행 차량들이 이를 다르게 인식하듯이 기기의 머신 러닝 엔진도 그럴 가능성이 있습니다. 연구원들은 머신러닝 모델 내에 적들에게 노출되어 악용될 수 있는 사각지대가 어느 정도 존재하는지 이미 조사하였습니다.

머신러닝이 보안 개선에 도움이 되는 것은 확실하지만 보안 메커니즘에 대한 완벽한 대안책이 될 수는 없을 것으로 생각됩니다. 이는 만병 통치약이 아닌 심층 방어 전략에 도입할 수 있는 부가적인 보안 계층으로 간주해야 합니다. 게이트웨이에서부터 엔드포인트까지, 엔드투엔드 보안을 보장하는 다계층 방어 체제를 갖추어야 알려진 또는 알려지지 않은 보안 위협들에 대처할 수 있을 것입니다.

비즈니스 구조에 획기적인 변화를 가져오고 현재 가장 널리 도입되고 있는 신기술은 블록체인입니다. 블록체인 기술은 디지털 가상 화폐 분야에서 가장 널리 사용되고 있으며 이러한 분산 장부 기술은 향후 5-10년 내에 광범위하게 도입될 것으로 예상됩니다. 현재, 기술 업계에서부터 신생 금융 업계와 대기업 및 정부 부처 전체에 이르기까지 많은 이니셔티브가 비즈니스 모델 혁신을 위해 블록체인을 기반으로 하고 있습니다.

블록체인은 참가자들 간 합의를 통해 이루어지고 무단 변경이나 의도적 개입이 불가능하며 거래량이 많아질수록 블록체인 시리즈가 더 복잡하고 난해해집니다. 이러한 난해함은 공격 매개체를 강화하려는 사이버범죄자들에게 새로운 기회가 될 수도 있습니다. 이들은 이미 Ethereum DAO 해킹에서 블록체인을 표적으로 삼았으며 미화 5천만 달러의 가상 화폐를 빼돌렸습니다.

한때 안전하다고 생각되었던 대부분의 우수한 기술들과 마찬가지로 머신 러닝과 블록체인도 세심한 주의가 요구됩니다.

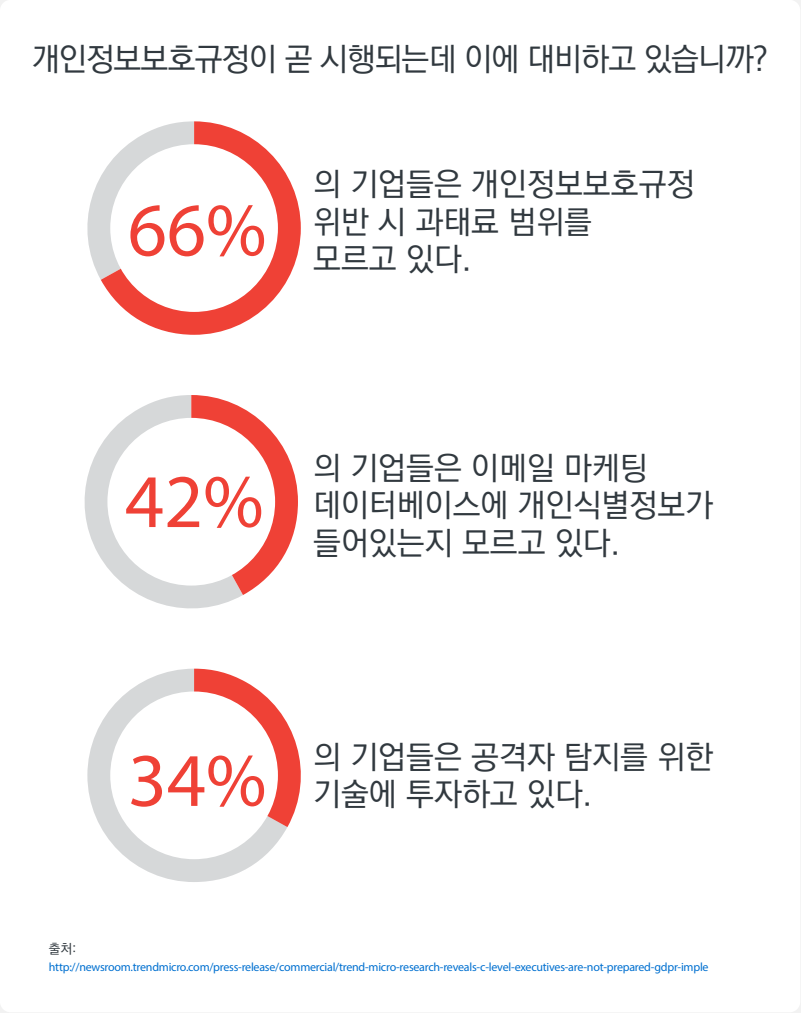
많은 기업들이 세간의 화제가 될 법정소송 사건이 발생해야 개인정보보호규정을 위한 확실한 조치를 취할 것이다.

EU가 드디어 2018년 5월부터 개인정보보호규정을 시행하게 되며 유럽 외의 국가들을 포함하여 EU 국민의 데이터를 다루는 기업들의 데이터 관리 방식에 엄청난 파장이 예상됩니다. 우리가 조사한 자료에 의하면 C레벨 경영자들의 대부분(57퍼센트)이 개인정보보호규정에 대한 준비를 하지 않았고 일부는 어떤 정보가 개인식별정보인지도 모르거나 위반 벌금에 대해 개의치 않는 것으로 나타났습니다.

지각수용자(Laggards)들은 규제기관이 규정 위반에 대한 제재를 가해야만 개인정보보호규정에 주의를 기울일 것입니다. 데이터 개인정보보호 감시자들이 기업들로 하여금 특정 데이터를 처리하지 못하도록 금지시켜 비즈니스 운영을 방해할 수도 있고 정부 당국이나 시민들에 의한 소송도 제기될 수 있습니다.

일례로 미국 회사인 Equifax의 경우 영국 소비자도 피해를 입은 것으로 알려져 있어서 개인정보보호규정이 시행된 후에 정보 유출 사건이 발생했었다면 엄청난 벌금이 부과되었을 것입니다. 정보 유출 사고가 발생한 1년 뒤에 이를 발표한 국제적인 택시 예약 서비스 업체인 Uber 역시 엄청난 벌금이 부과되었을 것입니다. 정보유출 공지 규정을 위반할 경우 규제기관은 최대 2천만 유로 또는 전년도 기준 기업의 총 연간매출액의 4퍼센트를 벌금으로 부과할 것입니다.

개인정보보호규정 시행을 인식하고 있는 기업들은 데이터 프로세싱과 모니터링을 전두 지휘할 전담 데이터 보호 책임자(DPO)의 중요성을 깨닫게 될 것입니다. 특히 기밀 데이터를 다루는 대기업이나 업종의 경우 데이터보호책임자(DPO)를 반드시 갖추어야 할 것입니다. 기업들은 데이터를 특성별로 분류하고 다른 국가들과 EU 국가의 데이터를 구분하는 등 데이터 보안 전략을 재검토해야 할 것입니다.



다른 지역이나 국가들도 규정 불이행에 대한 더 엄중한 처벌과 광범위한 체계를 구축하여 적절한 데이터 규정을 시행해야 할 것입니다. 미국식품의약국(FDA)은 검사 체계를 개선하기 위해 유럽의 여러 제약 규제 기관들을 조사하고 있습니다. 호주는 개인정보보호법(정보유출고지법) 2017을 기반으로 독자적인 정보 유출 고지법 시행을 준비하고 있으며 영국의 데이터 보호법(Data Protection Bill)은 브렉시트 이후 EU의 법안에 맞춰 업데이트되고 있습니다. EU의 우려에도 불구하고 체결된 EU-미국간 프라이버시 쉴드 협약은 얼마나 구속력 있게 시행될 것인지가 관건입니다.

기업 어플리케이션과
플랫폼은 조작 및 취약점
문제에 직면하게 될 것이다.

4차 산업혁명을 통해 가상물리 시스템(cyber-physical system)과 생산 프로세스가 상호 연결되고 소프트웨어를 기반으로 최적화되고 있는 오늘날의 환경에서는 다양한 부문에서 위험이 야기될 수 있습니다. 실제 생산 환경 또는 프로세스의 가상 복제품이나 시뮬레이션을 구축하는 디지털 트윈을 도입함으로써 기업들은 실제 물리적 자산에서 야기되는 성능 문제를 해결할 수 있습니다. 이를 통해 기업 운영 방식을 획기적으로 전환시킬 수 있지만 시스템을 조작하여 운영을 방해하거나 피해를 입히려는 의도를 가진 악의적 행위자들이 생산 네트워크에 침입할 수 있는 위험이 발생할 수 있을 것으로 예상됩니다. 이러한 악의적 행위자들은 디지털 트윈 자체를 조작한 후 조작된 생산 프로세스를 정상적인 상태로 보이게 만들 수 있습니다.

이 외에도, 생산관리시스템(MES)을 통해 SAP이나 그 밖의 기업자원관리(ERP) 시스템으로 직접 전송되는 생산 데이터가 해킹될 수 있습니다. 데이터 일부가 조작되었거나 잘못된 명령이 ERP 시스템에 전달될 경우 기기들은 공급물품의 수량을 잘못 전달하거나 의도치 않은 송금을 하는 등의 잘못된 업무를 진행하여 프로세스를 붕괴시킬 수도 있고 시스템 과부하를 야기시킬 수도 있습니다.

2018년도 공격의 대상은 기업 시스템들만이 아닐 것이며 어도비와 마이크로소프트 플랫폼의 보안 결함도 계속 문제가 될 것으로 예측됩니다. 주목할 만한 점은 브라우저 기반 및 서버 측 취약점에 대한 관심이 높아질 것이라는 전망입니다.

여러 해 동안 어도비 플래시 플레이어, 마이크로소프트 자바 및 실버라이트와 같은 널리 알려진 브라우저 플러그 인의 취약점들이 표적이 되어왔습니다. 2018년에는 자바스크립트 엔진의 취약점들로 인해 최신 브라우저들에 문제가 야기될 것으로 예측됩니다. 웹 상에서 스크립트의 사용이 광범위해지면서, 구글 크롬 V8 충돌문제, 오픈 소스화되고 있는 Microsoft Edge의 차크라, 자바스크립트 기반 브라우저 취약점들이 2018년에는 더욱 두드러질 것으로 전망됩니다.

공격자들은 서버 측 취약점을 이용하여 악의적 페이로드를 전달하는 방식에 주력할 것으로 보입니다. 그리고 2018년에는 서버 메시지 블록(SMB)과 Samba 익스플로잇을 통해 랜섬웨어를 전파하는 방식도 빈번하게 사용될 것으로 예상됩니다. 특히 SMB 취약점은 사용자의 직접적인 개입 없이도 악용될 수 있습니다. SMB 취약점은 WannaCry와 Petya 랜섬웨어 공격 및 최근 EternalRomance를 악용한 BadRabbit 공격을 받았을 때 Windows에서 실행되던 많은 네트워크를 마비시켰던 EternalBlue 익스플로잇과 같은 취약점입니다. 리눅스에서 실행되는 오픈 소스 Samba도 SMB 프로토콜의 취약점을 악용할 수 있습니다.

SAP과 ERP를 통한 생산 프로세스의 공격이 예상되므로 기업들은 관련 어플리케이션들에 대한 보안을 최우선으로 해야 하며 어플리케이션 사용을 철저히 관리 및 감독하여 무단으로 사용되는 일이 없도록 해야 합니다.

사용자와 기업들은 정기적으로 소프트웨어 업데이트를 확인하고 패치가 출시되는 즉시 적용시켜야 합니다. 하지만 관리자들이 업데이트를 즉각적으로 설치하지 못하는 경우도 있으므로 시스템에 취약점 방어 기능을 적용시켜 패치되지 않은 취약점과 제로데이로부터 플랫폼을 보호할 것을 권장합니다. 네트워크 솔루션은 가상 패칭과 웹 트래픽에 대한 사전 모니터링을 통해 잠재적 공격으로부터 연결된 기기들을 보호할 수 있어야 합니다.

2018년 보안 문제 해결 방안

취약점, 랜섬웨어, 스팸 및 표적 공격 등을 포함하여 현재 및 2018년에 예상되는 다양한 위협들을 고려해 볼 때 기업과 사용자들이 취해야 할 최선의 방책은 모든 계층에서 위험을 최소화하는 것입니다.

기업을 위한 우수한 가시성 및 다계층 보안 방어책

광범위한 위협들을 차단하고 발생된 위협들에 대한 방어를 강화하기 위해선 모든 네트워크에 대한 가시성을 제공하고 취약점과 공격에 대한 실시간 탐지 및 보안을 제공하는 보안 솔루션을 도입해야 합니다. 다양한 위협에 대비하여 세대를 초월한(cross-generational) 기술을 채택하는 능동적인 보안 전략을 세워 잠재적 공격과 자산 손실을 막아야 합니다. 다음은 이러한 보안 기술들입니다:

- **실시간 검사.** 능동적인 자동 검사를 통해 효과적으로 멀웨어를 탐지하고 시스템 성능을 향상시킵니다.

- **웹 및 파일 레퓨테이션.** 웹 레퓨테이션, 안티스팸 기술, 어플리케이션 제어를 통한 멀웨어 탐지 및 방어 기능이 사용자들을 랜섬웨어 공격과 익스플로잇으로부터 보호합니다.

- **행동 분석.** 기존의 방어 기술을 회피하는 지능형 멀웨어와 기법들도 사전에 탐지하여 차단합니다.

- **하이파이 머신 러닝.** 위협 인텔리전스 데이터로 인해 인력 투입도 개선되어 알려진 또는 알려지지 않은 위협들을 신속하고 정확하게 탐지하고 방어할 수 있습니다.

- **엔드포인트 보안.** 샌드박싱, 정보유출 탐지 및 엔드포인트 센서 기능이 포함된 보안 솔루션은 의심스러운 활동들을 탐지하고 네트워크 내에서 이루어지는 공격과 감염 확산움직임(lateral movement)을 차단합니다.

사용자들을 위한 모범 사례와 지속적인 보안책

모든 기기들이 상호 연결되고 있는 현대의 환경에서는 다양한 기기와 어플리케이션을 통해 정보에 액세스하는 활동이 너무도 자연스러운 현상이 되었습니다. 어떤 기기, 어플리케이션, 네트워크를 사용하건 상관없이 사용자들은 적절한 설정을 통해 보안 격차 문제를 해결할 수 있게 될 것입니다:

- **기본 설정된 암호 변경.** 스마트 기기 특히 라우터에 사용하는 암호를 독창적이고 복잡하게 설정하면 공격자가 기기를 해킹할 가능성이 대폭 줄어듭니다.

- **기기 보안 설정.** 기기의 기본 설정을 변경하여 개인정보를 지속적으로 보호하고 암호화를 구현하여 데이터가 무단으로 조회 및 사용되지 못하도록 방지합니다.

- **즉각적인 패치 설치.** 펌웨어를 최신 버전으로 유지하여(또는 자동 업데이트 기능을 활성화하여) 패치되지 않은 취약점을 방지합니다.

- **소셜 엔지니어링 전술 회피.** 수신하는 이메일과 방문하는 사이트들이 스팸, 피싱, 멀웨어 및 표적 공격에 노출될 수도 있다는 사실을 항상 염두에 둡니다.

보안이 적절하게 구현되어 있다면 다양한 보안 계층으로 전체 위협 주기에 따른 문제들을 해결할 수 있으므로 기업 및 사용자들은 유리한 보안 입지를 갖추게 됩니다. 이메일과 웹 게이트웨이에서부터 엔드포인트에 이르기까지 상호 연결된 위협 방어를 통해 끊임없이 진화하는 위협들에 대한 보안을 극대화할 수 있습니다.

For Raimund Genes (1963 - 2017)

Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver topranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe.

트렌드마이크로

(우 06181) 서울특별시 강남구 테헤란로 522 6층 (대치동 홍우빌딩)
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™ | 트렌드마이크로