



MAPPING THE FUTURE

Dealing With Pervasive and Persistent Threats

TREND MICRO
SECURITY
PREDICTIONS
FOR 2019



TREND
MICRO™

research 

테크놀로지 트렌드, 2019 and Beyond

- 클라우드 컴퓨팅의 도입
- 더 큰 데이터를 사용하는 ML 및 AI
- 2020년 5G의 출시
- 가정 및 공장에서의 스마트 기기 사용 증가 (IoT and IIoT)

데이터, 지식 및 새로운 기능은 훨씬 더 빠른 속도로 이동하며 전문가 뿐만 아니라 개인의 생활에도 다양한 측면으로 스며들 수 있습니다.



사용자 행위 및 사회 정치적 측면, 2019 and Beyond

- 온라인 커뮤니케이션을 위한 채팅 및 비디오의 활용
- WFH (Working From Home)의 증가 예: 스마트 홈에서의 자택근무
- 여러 국가에서 시행될 예정인 중요한 선거

*다양한 측면의 개발에 따라 보안 분야 또한
각기 다른 영향을 받게될 것입니다.*



CONTENTS



CONSUMERS



ENTERPRISES



GOVERNMENTS



SECURITY
INDUSTRY



INDUSTRIAL
CONTROL
SYSTEMS



CLOUD
INFRASTRUCTURE



SMART
HOMES



Getting Ready
for the Year
Ahead

A man and a woman are standing in a server room, looking at a tablet together. The room is filled with rows of server racks, and the lighting is dim with some blue and green highlights from the equipment. The woman is on the left, wearing a light blue shirt and dark pants. The man is on the right, wearing a dark sweater over a collared shirt and dark pants. They are both looking at a tablet held by the man. The background shows the perspective of the server aisle, with racks receding into the distance.

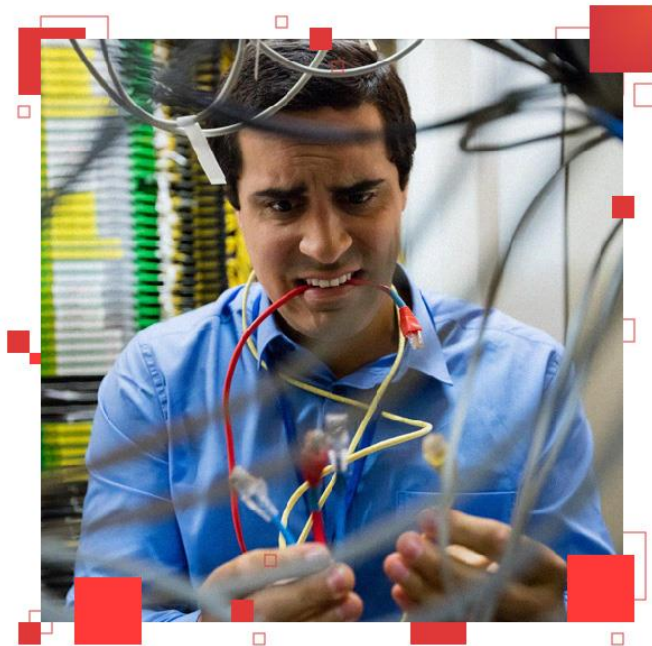
CLOUD INFRASTRUCTURE

하이브리드 클라우드 사용자는 마이그레이션 중 잘못된 구성, 클라우드 크립토잭킹, 클라우드 배포 소프트웨어 취약점 등과 같은 더 많은 보안 문제에 직면하게 될 것입니다.



▶ 마이그레이션 중 잘못된 구성된 보안 설정으로 더 많은 보안 유출을 초래

- 마이그레이션 도중 잘못된 구성으로 인해 더 많은 주요 데이터 침해 사례가 발생할 수 있습니다.
- 특히 많은 수의 버킷과 이동식 부품의 경우 보안을 위해 설정을 수정하는 것이 어려운 경우가 많습니다.
- 클라우드 마이그레이션은 범위 및 속도 측면에서 각기 고유합니다.



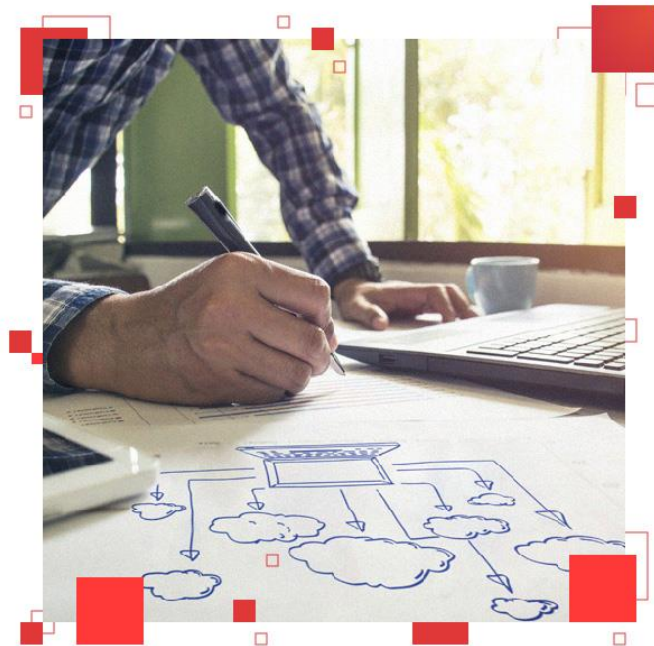
▶ 암호화에 사용되는 클라우드 인스턴스 채굴

- 클라우드를 통한 가상화폐 채굴은 시작 및 사후 관리가 용이합니다.
- 따라서 더 많은 사이버 범죄자들이 클라우드 계정을 탈취하여 가상화폐를 채굴하거나 대체 계정을 통제할 것입니다.
- 클라우드 버킷 스캐너 툴 또한 사용이 가능합니다.
- 크립토재킹 멀웨어는 사용량을 조절하여 탐지를 최소화 합니다.



▶ 클라우드 관련 소프트웨어 취약점 발견

- 클라우드 인프라 취약점 연구가 시작될 것입니다.
- Kubernetes의 취약점은 이미 발견된 바 있으며, 최근에는 심각한 취약점 또한 발견되었습니다.
- 12개 이상의 악성 도커 이미지가 최소 500만 회 이상 다운로드 되었습니다.



Getting Ready for the Year Ahead



지속적이고 자동화된 보안으로 컨테이너 이미지를 보호하는 것은 클라우드를 안전하게 유지하기 위해 매우 중요합니다. 트렌드마이크로의 클라우드 보안 솔루션은 클라우드의 속도 및 효율성에 영향을 주지 않으면서 이미지를 스캔하고 버그를 탐지하여 안전한 컨테이너 구축을 도와드립니다:

- Hybrid Cloud Security Solution
- Trend Micro Network Defense
- Trend Micro Deep Security™
- Trend Micro™ Deep Security™ Smart Check

ENTERPRISES

자택근무의 증가, GDPR 준수의 어려움, 소셜엔지니어링 공격, 기업 이메일 공격, 자동화 및 사이버 탈취와 관련된 위험이 증가할 것입니다.



▶ 첫 GDPR 위반 사례에 부과될 4%의 벌금

- 규제당국은 첫 GDPR 위반 기업에게 연간 매출액의 4%를 벌금으로 부과하여 GDPR 위반의 본보기로 삼을 것 입니다.
- 2020년까지 최대 75%의 새로운 비즈니스 애플리케이션은 규정준수와 보안 사이에서 어려운 결정을 내려야 할 것입니다.



▶ 소셜엔지니어링 공격에 악용될 실제 이벤트

- 2020 도쿄 올림픽, 브렉시트, 이탈리아 예산 문제 등 많은 사회적 이슈들이 소셜엔지니어링 공격에 악용될 것입니다.



Photo by [Gentrit Sylejmani](#) on [Unsplash](#)

▶ 변화된 BEC 대상

- 사이버 범죄자들은 CxO의 비서나 집행 보좌관, 재무부 고위 책임자 또는 매니저 등을 사칭할 대상으로 삼을 것입니다.



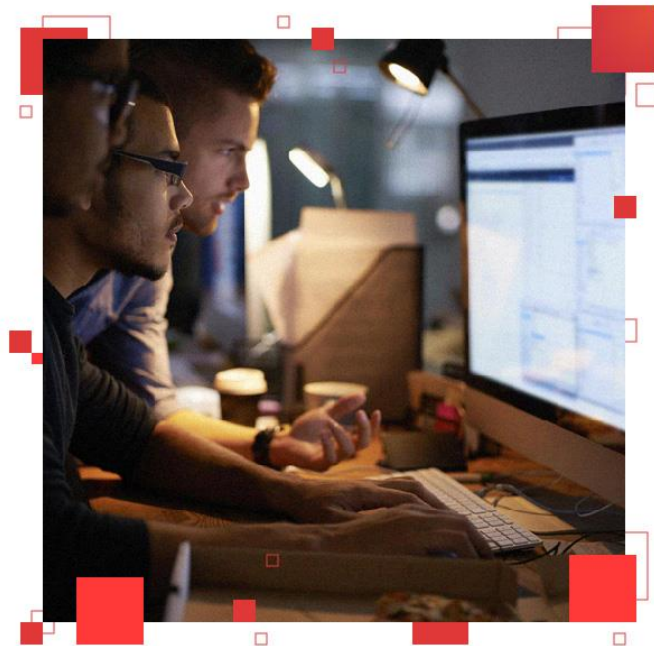
▶ 비즈니스 프로세스 침해의 새로운 공격 벡터가 될 “자동화”

- 모니터링 및 기능의 더 많은 측면은 소프트웨어 또는 온라인 애플리케이션을 통해 수행됩니다.
- 이는 공급망 공격 (Supply Chain Attack)에도 사용될 것입니다.



▶ 더 광범위해질 디지털 탈취 대상

- 온라인 스미어 캠페인 (Smear Campaigns)
- GDPR 벌금이 오히려 사이버 범죄자들의 몸값 요구에 있어 기준이 될 수 있습니다.



Getting Ready for the Year Ahead



알려지지 않은 위협에 맞서기 위해서는 더욱 지능적인 다계층의 보안이 필요합니다. 이에 따라 IT 보안 기술 부족 현상이 더욱 뚜렷해지고 전문 지식의 습득이 더욱 중요해질 전망입니다.

기업은 다음과 같은 엔드포인트, 네트워크 및 게이트웨이 솔루션을 사용하여 환경을 보호해야 합니다:

- Trend Micro™ Security, Apex One™, and Worry-Free™ Business Security
- Trend Micro™ Smart Protection Suites
- Trend Micro Worry-Free™ Business Security
- Trend Micro™ Hosted Email Security
- Trend Micro™ Deep Security™
- Trend Micro Deep Discovery™

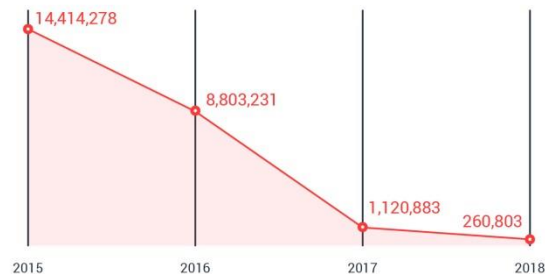
CONSUMERS

단일 플랫폼 컴퓨팅의 시대는 지났습니다. 채팅, 비디오,
온라인 거래를 통해 세상이 점점 더 다양해지고
사회화됨에 따라 소셜엔지니어링 기법을 이용한 사이버
범죄가 더욱 증가할 것 입니다.

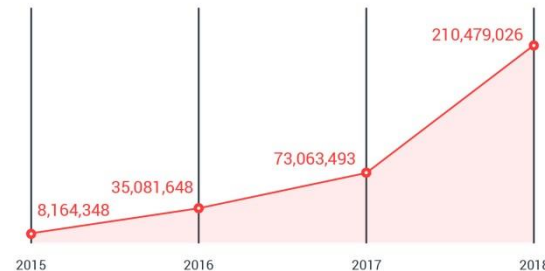


▶ 익스플로잇 킷 공격을 대체할 피싱을 사용한 소셜엔지니어링 기법 공격

- 익스플로잇 공격 또한 줄어들텐 것이며, 소셜 엔지니어링 공격은 더욱 증각할 것입니다.
- 이메일 뿐 아니라 SMS 및 채팅을 통한 피싱이 발생 할 수 있습니다.
- 스포츠 경기, 다가올 선거, 사회 정치적 사항은 소셜엔지니어링 수법으로 사용될 것입니다.



익스플로잇 킷 활동 수



차단된 피싱 관련 URL 수

▶ 챗봇의 악용

- 이전의 전화 공격과 유사한 사전 녹음 메시지 (IVR)를 사용한 공격
- 예: 주문 조작, RAT 설치, 사이버 탈취



▶ 워터링 홀 공격에 악용될 인터넷 유명인의 계정

- 수백만 명의 팔로워를 보유한 유명한 유튜버 및 온라인 유명인의 계정을 이용한 공격
- 예: 팔로워들이 다양한 악성 소프트웨어 및 DDoS 공격, 정보 탈취 등의 공격 대상이 될 수 있습니다.



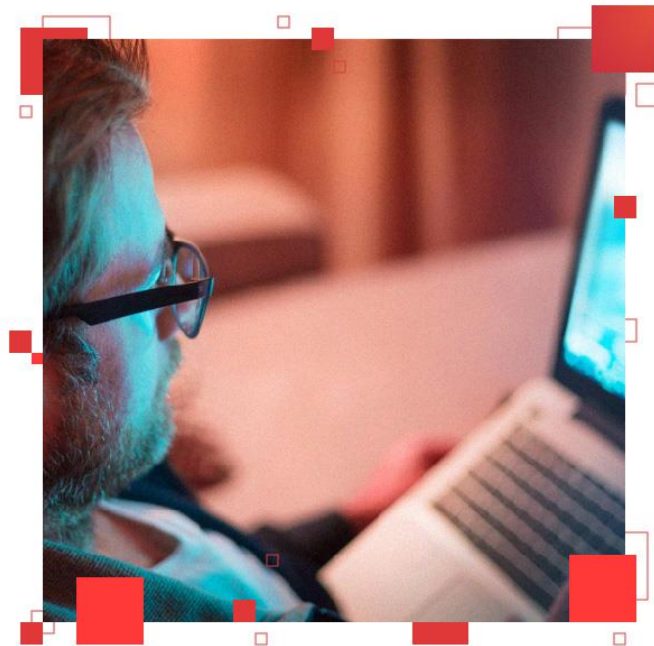
▶ 유출된 자격 증명의 대량 사용

- 자격 증명 탈취 (Credential Stuffing) 현상이 계속해서 증가합니다.
- 사용자들이 같은 패스워드를 여러 웹사이트에서 동일하게 사용 혹은 재사용하는 것 또한 문제의 원인이 됩니다.



▶ 몸캠피싱의 증가

- 사용자 개개인에 맞춘 공격은 성인 뿐만 아니라 십대들도 대상으로 하고 있습니다.
- 이러한 공격으로 인해 더 많은 피해자가 생겨날 것입니다.



Getting Ready for the Year Ahead



- 사용자들은 새로운 소셜엔지니어링 공격에 넘어가지 않도록 Trend Micro™ 인텔리전스와 같은 블로그를 통해 최신 위협 뉴스에 귀기울여야 합니다.
- Trend Micro™ Security를 통해 악성 이메일 및 URL로부터 모든 기기와 정보를 보호하십시오.
- Trend Micro™ Password Manager를 통해 더 강력하게 암호를 유지 관리하십시오.
- 항상 거래 내역을 확인하고 의심스러운 내역을 보고하십시오.

A person wearing a black leather jacket is shown from the chest down, holding a small white envelope and a key. The background is dark with a grid of small white dots. On the right side, there is a teal-colored rectangular area containing a white icon of a classical building with columns.

GOVERNMENTS

앞으로 있을 주요 선거에서는 소셜 미디어를 통해 퍼져 나가는 가짜 뉴스가 넘칠 것이며, WannaCry와 NotPetya와 같은 공격에 많은 피해자가 생겨날 것입니다. 이에 따라 정부는 IoT와 IIoT의 위험을 앞서 나가기 위해 노력할 것입니다.

▶ 다가오는 선거가 직면한 가짜 뉴스

- 2016년 이후 가짜 뉴스와 싸우기 위해 생겨난 소셜미디어의 많은 개선점은 2019년에 치뤄질 선거에서 쇠도할 사이버 프로파간다를 막기에는 역부족 일 것입니다.



▶ 국가의 사이버 공간 확대에 따라 증가할 무고한 피해자

- 사이버 능력을 강화하기 위해 국가들은 더욱 국내의 해커들을 지원할 것입니다.
- 이에 따라 WannaCry 및 NotPetya에서 발생한 것과 같은 사이버 대응과 전혀 무관한 무고한 피해자들이 생겨날 것입니다.



▶ 규제 감독 강화

- 선례: 캘리포니아주는 제조업체에서 사용하는 스마트 기기에 강력한 암호를 사용하도록 요구하였습니다.
- 지방자치단체는 안전하지 않은 소비자 및 산업용 IoT 기기 사용을 금지합니다.



Getting Ready for the Year Ahead



정부는 다음과 같은 엔드포인트, 네트워크 및 게이트웨이 솔루션을 사용하여 환경을 보호해야 합니다:

- Trend Micro™ Security, Apex One™, and Worry-Free™ Business Security
- Trend Micro™ Smart Protection Suites
- Trend Micro Worry-Free™ Business Security
- Trend Micro™ Hosted Email Security
- Trend Micro™ Deep Security™
- Trend Micro Deep Discovery™

또한 학교와 같은 곳에서 일반 대중을 대상으로 사이버 보안 인식 교육을 진행하여야 합니다.



SECURITY INDUSTRY

InfoSec과 IT팀은 사이버 범죄자들이 네트워크에
침입하기 위해 “정상” 개체를 사용하는 사례에 대응하고,
사이버 보안을 위해 AI에 투자해야 합니다.

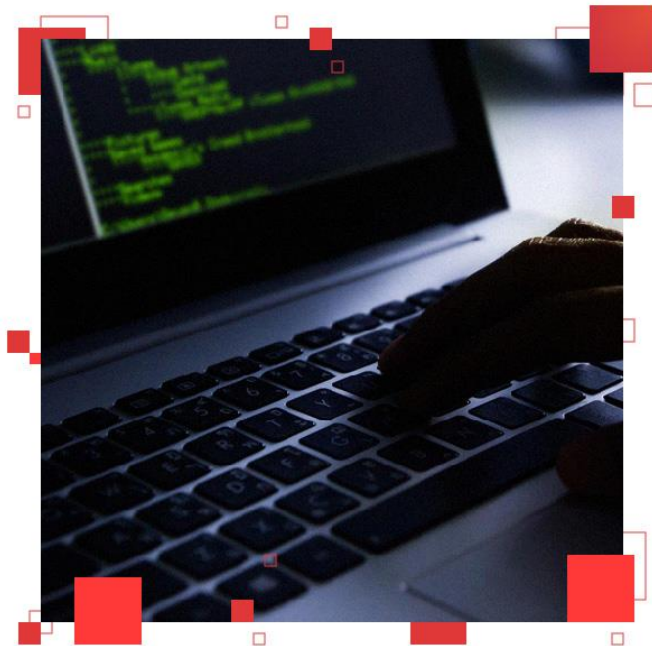


▶ 네트워크 침입을 위한 더 많은 기법 사용

- 원래의 용도나 설계 이외의 목적으로 일반적인 컴퓨팅 개체를 사용하는 새로운 공격 방법은 계속해서 검색, 문서화 및 공유 될 것입니다:
 - 일반적이지 않은 파일 확장자
 - 파일리스 구성요소, Powershell, 스크립트 및 매크로 사용 시 실제 실행 파일에 대한 의존도 감소
 - 디지털 서명된 멀웨어
 - 새로운 활성화 기법
 - 이메일 계정 또는 온라인 스토리지 서비스 앱의 남용
 - 합법적인 시스템 파일을 감염

▶ 99.99%의 익스플로잇 공격은 패치되지 않은 취약점이 원인

- 익스플로잇 기반의 공격이 성공하는 경우는 대부분 패치가 이미 몇주 혹은 몇달 전부터 존재했으나 패치가 적용이 안된 경우입니다.



▶ AI기반 기술을 사용한 고도의 타겟팅 공격

- 기업의 임원이나 기타 관계자의 행동을 예측하는 AI의 사용이 나타납니다. (호텔, 노선, 항공편, 기타 선호도 등)



Getting Ready for the Year Ahead



파일리스 멀웨어는 보안 솔루션의 감지가 더욱 어렵도록 설계되었습니다. 따라서 기업은 게이트웨이, 네트워크, 서버 및 엔드포인트에서 위협을 탐지하기 위해 다음과 같은 다계층의 솔루션을 구현해야 합니다:

- Trend Micro™ Security, Apex One™, and Worry-Free™ Business Security
- Trend Micro™ Smart Protection Suites
- Trend Micro Worry-Free™ Business Security

마찬가지로 보안에 대한 사전 예방적이고 다계층의 접근법은 취약점을 이용하는 위협을 방지하는데 효과적입니다. 여기에는 다음과 같은 네트워크 트래픽 솔루션 및 취약점 보호 솔루션이 포함됩니다:

- TippingPoint® Next-Generation Intrusion Prevention System (NGIPS)
- Trend Micro™ Deep Discovery™ Inspector
- TippingPoint® Advanced Threat Protection
- Trend Micro™ Deep Security™
- Trend Micro™ Apex One™

An orange industrial robot arm is positioned on the left side of the frame. In the center, a person's hands are holding a tablet displaying a complex industrial control system (ICS) interface. The background is a blurred industrial setting with warm lighting. On the right side, there is a green and blue geometric design element consisting of several squares and rectangles. A dark blue square contains a yellow line-art icon of a factory with three chimneys.

INDUSTRIAL CONTROL SYSTEMS

주요 인프라에 대한 공격과 더 많은 HMI 취약점은 ICS
보유 기업에게 큰 문제가 될 것입니다.

▶ ICS를 타깃으로 하는 실제 공격의 출현

- 국가들간의 중요 기반 시설에 대한 공격이 일어날 가능성이 있습니다.
- 영향: 운영 중단, 장비 손상, 간접적인 재무 손실, 최악의 경우 안전 위험 초래



▶ ICS 취약점의 주요 소스가 될 HMI 버그

- 이러한 종류의 소프트웨어는 취약점 연구자들이 더 쉽게 이용할 수 있습니다.
- HMI 소프트웨어는 공격에 취약합니다.
- 이러한 종류의 소프트웨어는 격리된 환경에서만 실행된다는 생각은 잘못된 가정입니다.



Getting Ready for the Year Ahead



ICS는 SCADA 시스템, DCS, PLC 및 공장과 공장을 운영하는 기타 구성요소를 포함합니다. 이러한 구성요소들은 전문화된 시스템이기 때문에 다른 방어 전략이 필요합니다. 따라서 다음과 같은 솔루션을 사용하여 네트워크 보안 및 기기 보안을 확립해야 합니다:

- TippingPoint® Next-Generation Intrusion Prevention System (NGIPS)
- Trend Micro™ Deep Discovery™ Inspector
- TippingPoint® Advanced Threat Protection
- Trend Micro™ Deep Security™
- Trend Micro™ Apex One™



TREND MICRO™ RESEARCH

트렌드마이크로는 사이버 보안의 글로벌 리더로 안전한 디지털 정보 교환의 세계를 만들기 위해 최선의 노력을 다하고 있습니다.

Trend Micro Research는 새로운 위협 발견, 핵심 인사이트 공유, 사이버 범죄 예방에 대해 노력하는 열정적인 전문가들에 의해 운영되고 있습니다. 트렌드마이크로의 글로벌 팀은 매일 수백만 건의 위협을 파악하고 취약점 공개에서 업계를 선도하며 새로운 위협 기술에 대한 혁신적인 연구를 발표하고 있습니다. 트렌드마이크로는 새로운 위협을 예측하고 연구 결과를 제공하기 위해 끊임없는 노력을 기울이고 있습니다.

www.trendmicro.com

©2018 by Trend Micro, Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and Trend Micro Smart Protection Network are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.