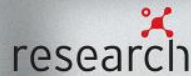


Caught in the Net: Unraveling the Tangle of Old and New Threats

트렌드마이크로 2018 위협 리뷰 보고서

2018: New, familiar, and game-changing threats

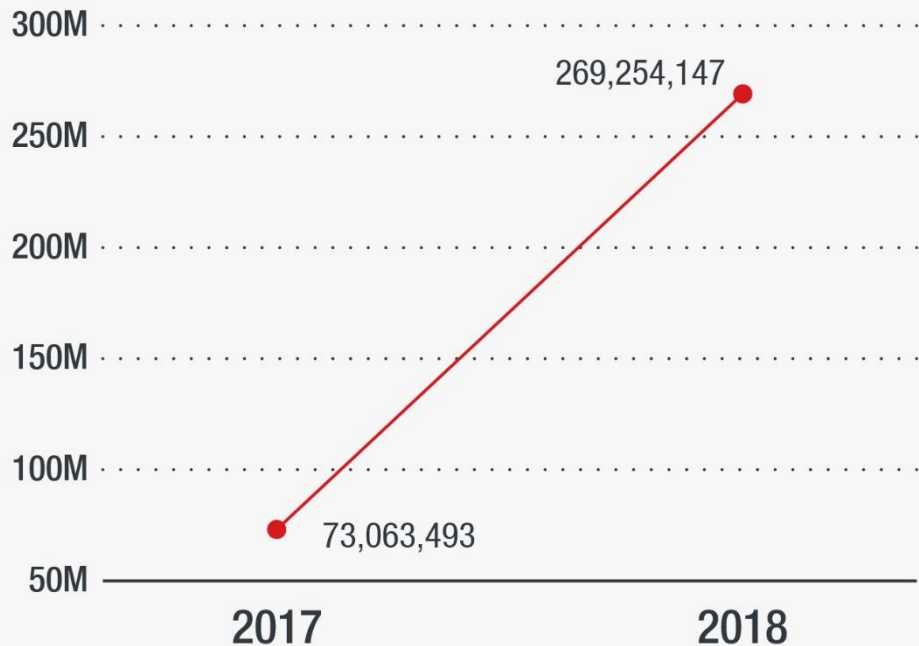
- 다양한 형태의 메시징 위협 증가
- 공격 감소에도 불구하고 여전히 강한 영향력을 가진 랜섬웨어
- 하드웨어와 클라우드에서 계속해서 발견되는 취약점과 증가하는 ICS 버그
- IoT 보안 사고에 따른 스마트홈에 대한 불안감 증가
- 나날이 증가하는 개인 정보 보호 탈취 및 대형 정보 유출 사고에 대한 우려
- 머신러닝 솔루션, 다부문 연구 및 관련 법 제정의 발전



다양한 형태의 메시징 위협 증가

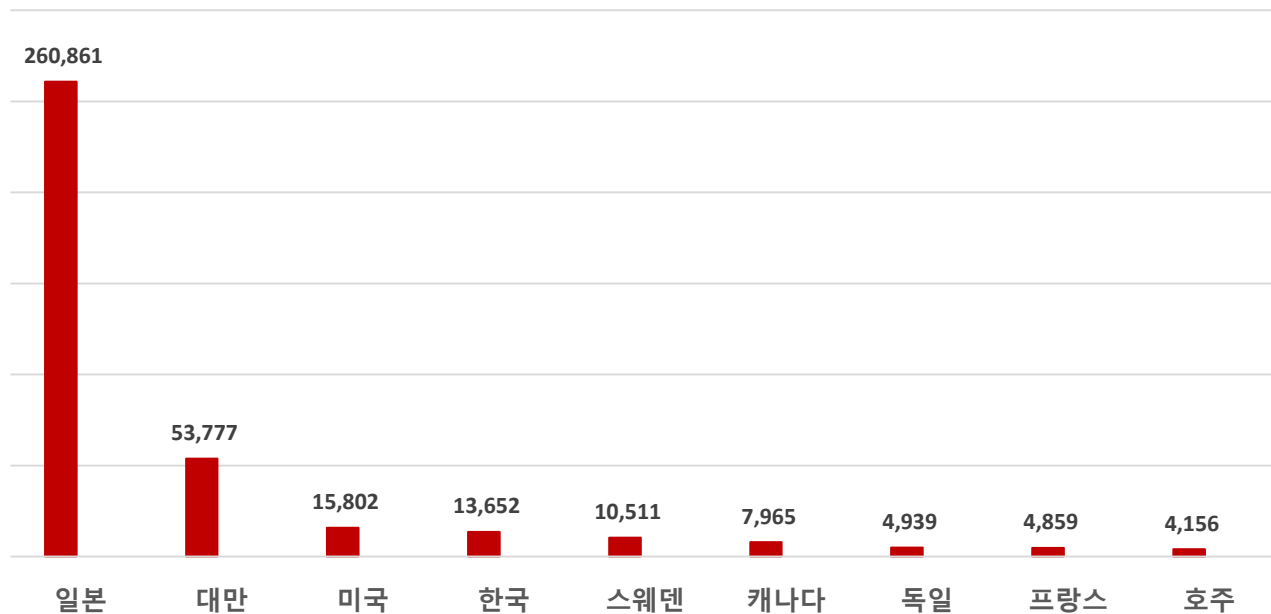
Trend Micro 2018 Annual Security Roundup

꾸준히 증가하는 피싱



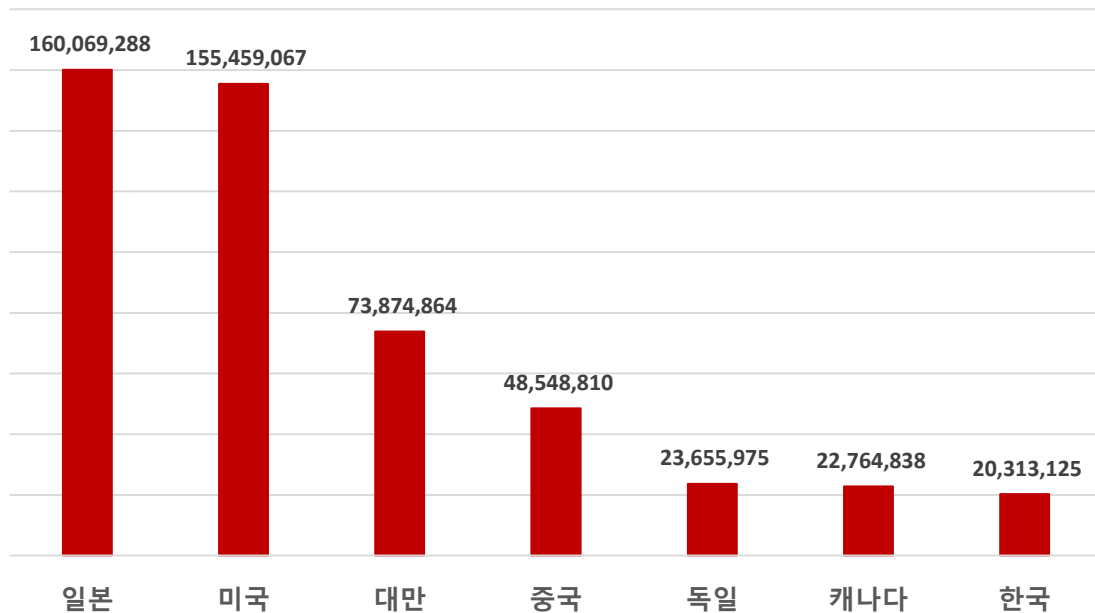
- 269% 증가한 피싱 관련 URL 차단 횟수
- 고유 클라이언트 IP 주소에 의한 피싱 관련 URL 접속 차단 82% 증가
- OS 플랫폼의 다양성에 따른 피싱 증가
- 익스플로잇 키트 활동 감소

익스플로잇 키트 공격



2018년 한 해 일어난 익스플로잇 키트 공격 횟수를 나라별로 나타낸 그래프입니다. 한국은 전세계 4번째에 기록되었습니다.

악성 URL 접근 방지



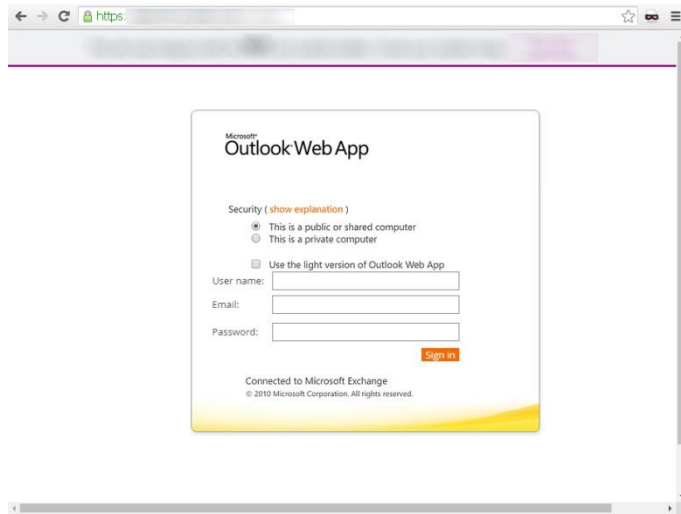
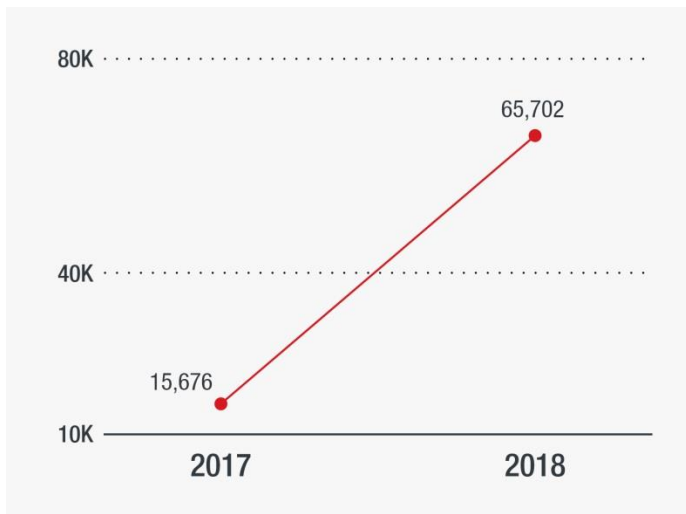
2018년 한 해 트렌드마이크로 제품이 사용자가 악성 URL을 접근하는 것을 차단한 수를 나타낸 그래프입니다. 한국은 전세계 7번째에 기록되었습니다.

꾸준히 증가하는 피싱

- 2018년 피싱 공격의 직접적 원인이된 데이터 침해 사고
- 사이버 범죄자들의 애플 아이디 추적을 위한 AES 암호화 사이트 사용
- SMS를 사용한 피싱 (스미싱)에 사용되는 펑키코드 기법
- 메일 계정을 도용한 후 기존의 주고 받던 이메일을 사용한 피싱 출현

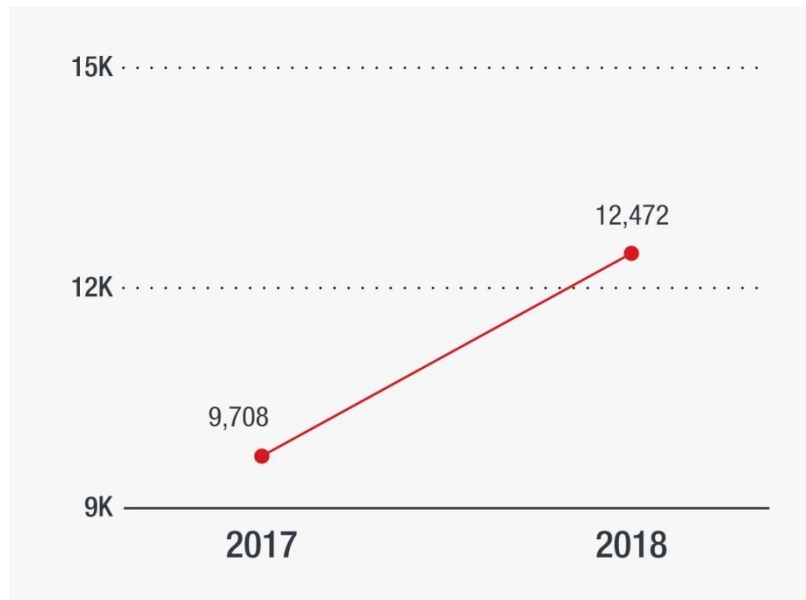
꾸준히 증가하는 피싱

엔터프라이즈 고객사의 Office 365 환경으로의 많은 이전으로 계정정보 탈취를 목적으로 하는 피싱이 증가하고 있습니다.

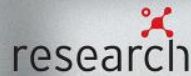


Office 365와 Exchange Online을 가장한 피싱 URL 차단이 3배 이상 증가하였습니다.

BEC 시도의 증가



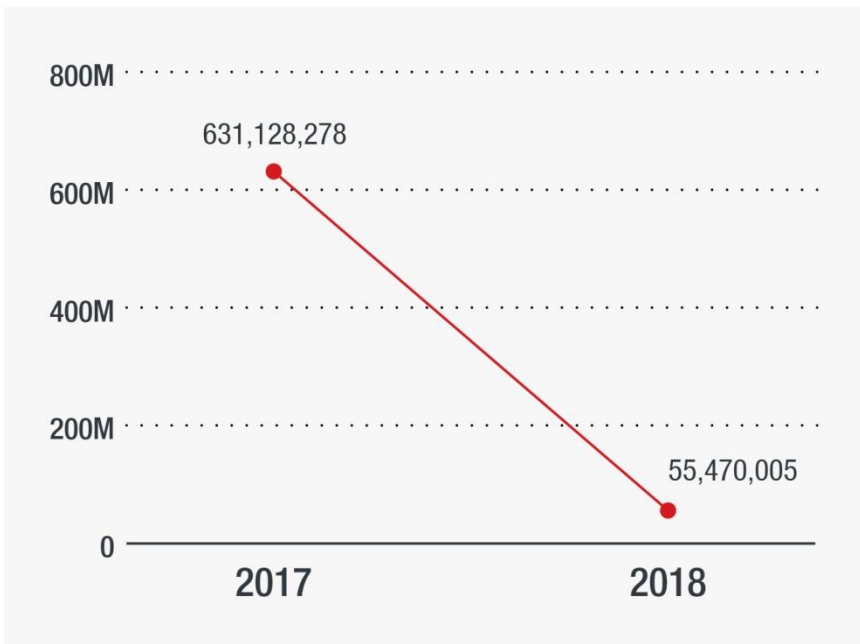
BEC 공격은 2017년에 비해 28% 증가하였으며, 실제 공격 수가 적어도 단 한번의 시도 마다 공격 성공 가능성이 훨씬 높습니다.



공격 감소에도 불구하고 여전히 강한 영향력을 가진 랜섬웨어

Trend Micro 2018 Annual Security Roundup

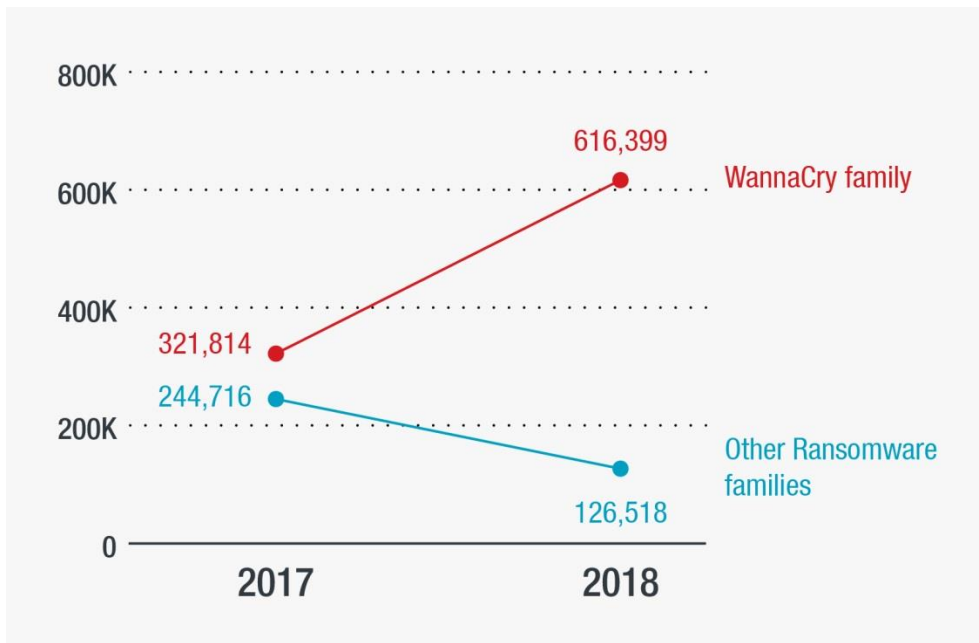
랜섬웨어 공격의 감소



개선된 랜섬웨어 솔루션, 랜섬웨어에 대한 인식의 변화 및 탈취된 파일을 위해 돈을 지불하는 것에 대한 회의적인 태도 등의 이유로 랜섬웨어의 공격이 감소하였습니다.

랜섬웨어 관련 위협 요소(files, emails, URLs)가 감소했습니다.

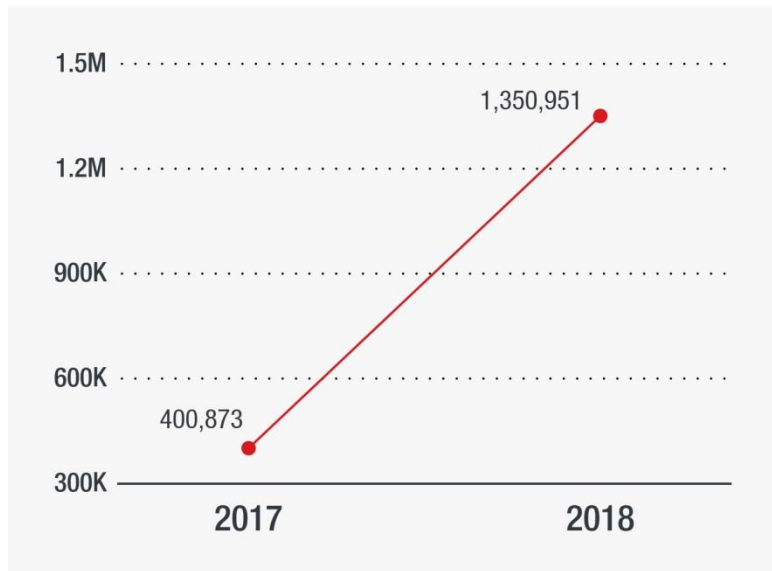
여전히 악명높은 WannaCry



WannaCry는 EternalBlue 익스플로잇 (Shadow Brokers 해커 그룹에 의해 유출됨)을 통한 SMB 취약점을 통해 시스템에 접근합니다. 시스템 접근 후 Worm을 통해 네트워크 전체에 퍼져나갑니다.

최근 2년 동안 랜섬웨어 탐지의 절반 이상을 WannaCry가 차지하였습니다.

가상화폐 채굴기 탐지 100만건 돌파

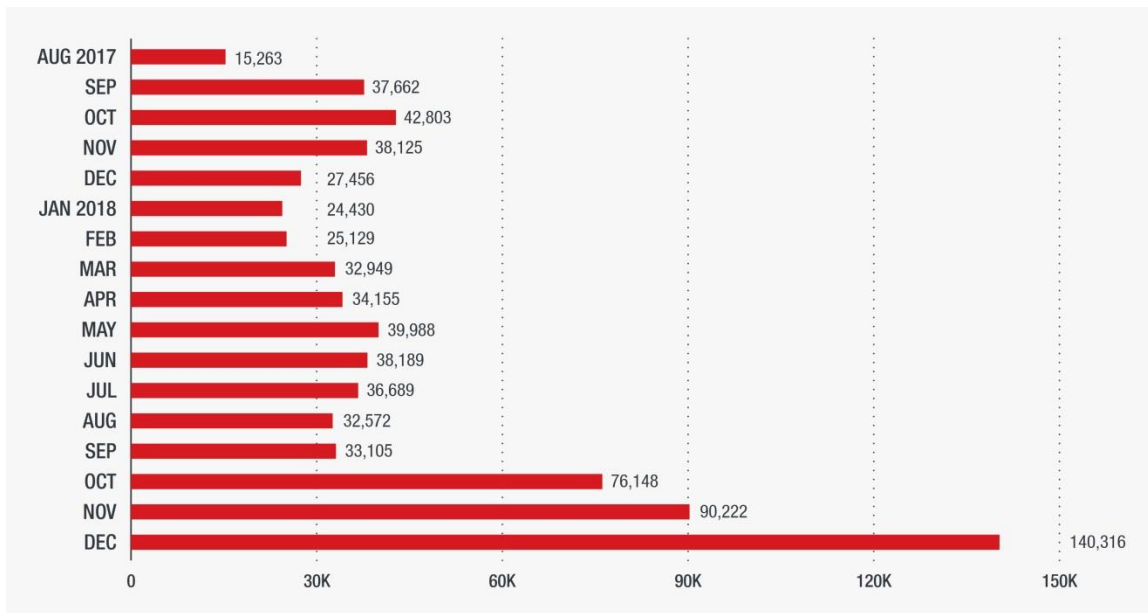


아래와 같은 공격으로 가상화폐 채굴기가 설치됩니다.

- 광고 플랫폼 남용
- 팝업 광고 남용
- 서버 익스플로잇
- 악성 브라우저 확장
- 플러그인
- 봇넷
- 합법 소프트웨어에 편승
- 익스플로잇 키트
- Repurposed ransomware

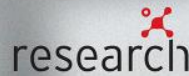
가상화폐 채굴기 탐지는 2018년에 100만건 이상 탐지되면서 그 정점을 찍었습니다. 이는 전년도 대비 237%나 상승한 수치입니다.

파일리스 위협의 증가



파일리스 위협은 별개의 바이너리를 사용하지 않습니다. 대신 메모리에 바로 주입되거나 스크립트 실행, 레지스트리 변경 등으로 실행됩니다.

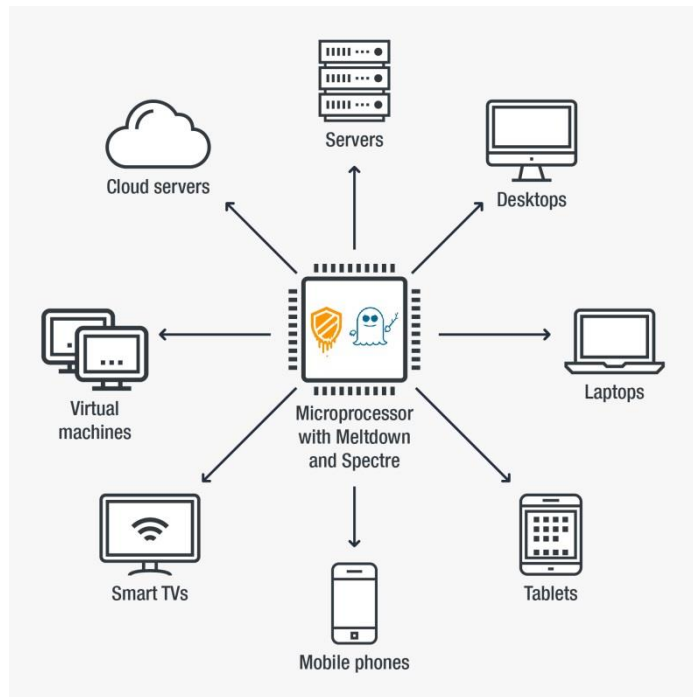
파일리스 위협이 계속해서 나타나고 있습니다.



하드웨어와 클라우드에서 계속해서 발견되는 취약점과 증가하는 ICS 버그

Trend Micro 2018 Annual Security Roundup

멜트다운 (Meltdown) & 스펙터 (Spectre)



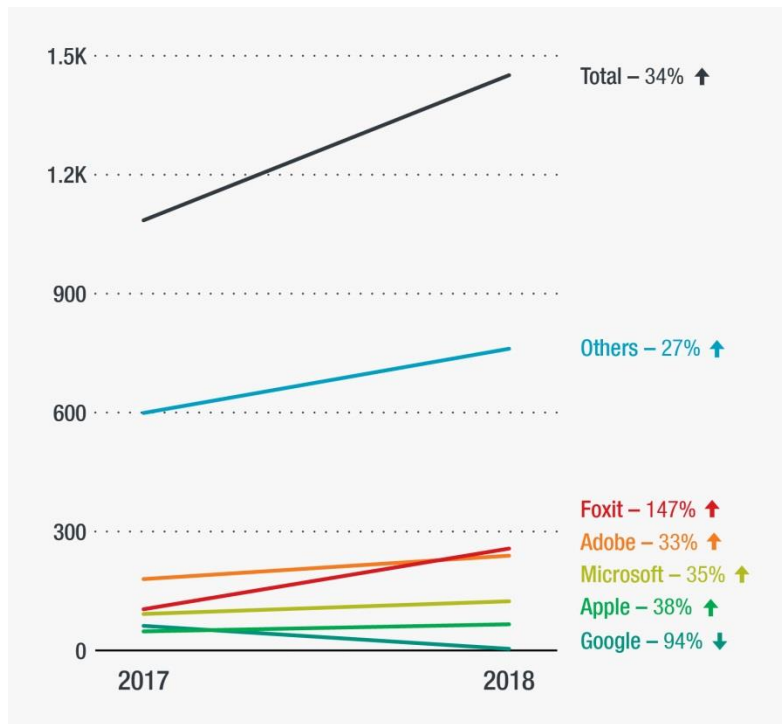
- 2개의 프로세서 수준의 취약점
- 패치 적용 후 디바이스 크래쉬, BSOD 그리고 성능 이슈가 계속해서 발생했습니다.
- 현재까지도 완벽한 해결 방법이 나오지 않고 있습니다.

클라우드 취약점으로 인한 백엔드 서버 액세스 허용



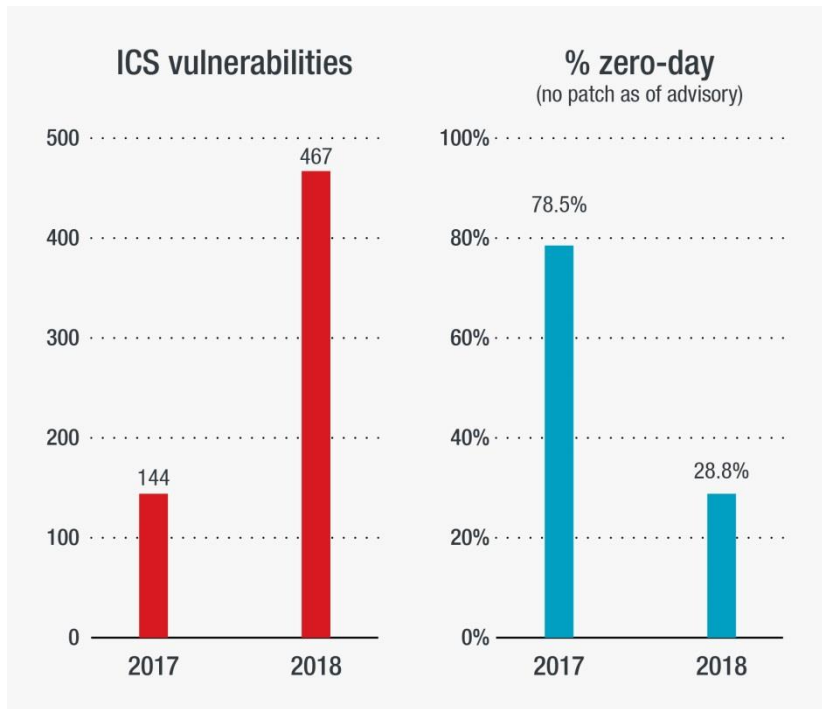
- 오픈소스 클라우드 오케스트레이션 소프트웨어인 Kubernetes의 심각한 취약점이 발견되었습니다.
- 해당 취약점은 특수 조작된 네트워크 요청을 사용하는 공격자가 Kubernetes API 서버를 통해 백엔드 서버에 접근할 수 있도록 합니다.
- 따라서 새로운 플랫폼과 기술이 DevOps에 사용될 때 보안이 매우 중요하다는 점을 알 수 있습니다.

PDF 리더 버그의 증가

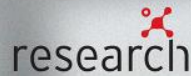


- Foxit 은 가장 많은 취약점을 가진 벤더이며 (257개), Adobe가 239개로 그 뒤를 이었습니다.
- Adobe와 Foxit 모두 PDF 제작, 수정, 관리 하기 위한 툴 제작사입니다.
- Microsoft, Apple, and Google은 각각 124개, 66개, 4개의 취약점을 가지고 있습니다.

여전히 문제가 되는 ICS에 대한 HMI 버그



- ICS에 이용된 소프트웨어에서 이미 보고된 몇 가지의 취약점이 발견되었습니다.
- Advantech과 Wecon은 각각 100개 이상의 취약점이 있습니다.
- 취약점은 주로 ICS 및 SCADA 환경으로 위한 HMI 소프트웨어에서 발견되었습니다.
- 다행히 패치없이 공개된 ICS 취약점의 비율은 줄었지만 ICS 벤더는 전반적으로 다른 소프트웨어 벤더에 비해 여전히 많은 취약점을 보유하고 있습니다.



IoT 보안 사고에 따른 스마트홈에 대한 불안감 증가

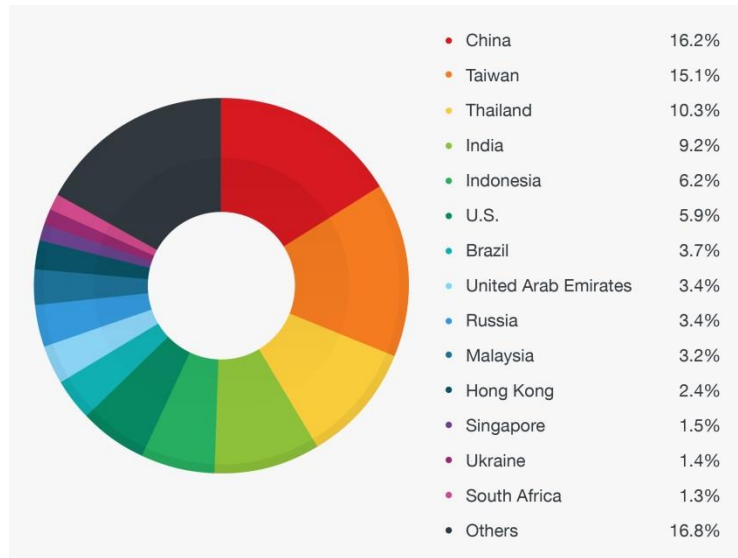
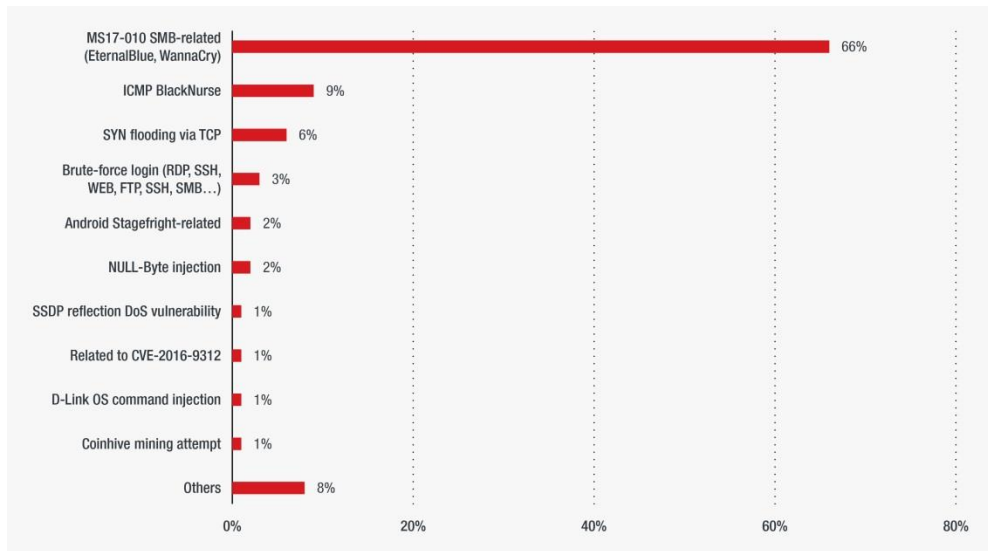
Trend Micro 2018 Annual Security Roundup

사이버 범죄자에 의해 탐색되는 라우터



- 브라질의 MikroTik 라우터는 가상화폐 채굴 공격의 대상이 되었습니다. 그 이유는 공격자가 RouterOS에서 일반적으로 포함되는 원격 관리 서비스 소프트웨어의 보안 결함을 이용했기 때문입니다.
- 또한 Novidade라는 이름의 익스플로잇 키트를 조사하였습니다. 해당 익스플로잇 키트는 CSFR (Cross-site request forgery)를 이용하여 라우터 DNS를 변경합니다. 따라서 인터넷 접속시 공격자가 제어하는 서버로 리디렉션됩니다.

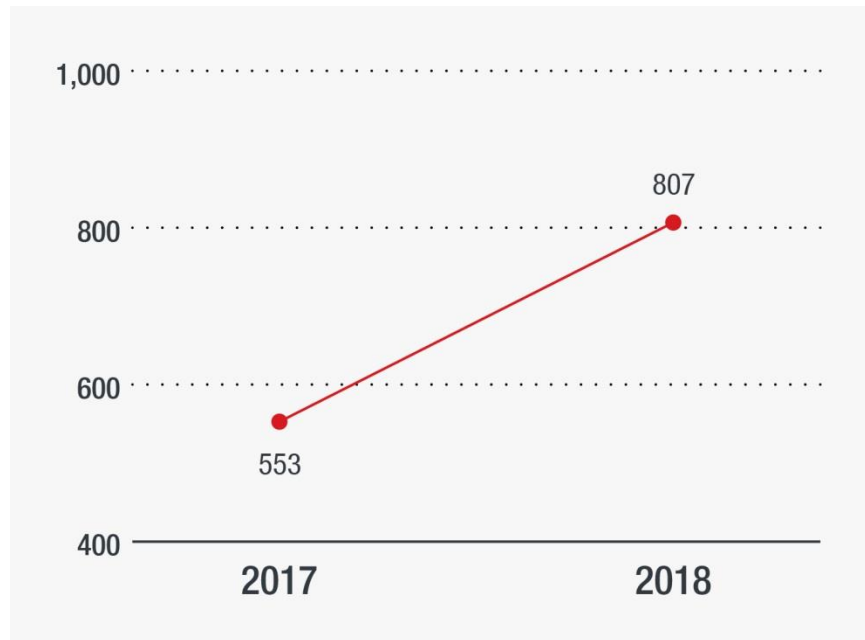
아웃바운드 라우터 연결의 대부분을 차지하는 SMB 취약점 관련 이벤트



SMB 취약점 관련 이벤트는 가장 많이 원인이 된 아웃바운드 이벤트였습니다. 해당 취약점은 WannaCry가 퍼트리기 위해 사용했던 것과 동일한 Worm이었습니다. 아웃바운드 라우터 이벤트의 국가별 분포를 보면 대부분이 아시아의 여러 나라에서 비롯되었음을 알 수 있습니다.

나날이 증가하는 개인 정보 보호 탈취 및 대형 정보 유출 사고에 대한 우려

새로운 정점에 도달한 데이터 침해



- 미국에서 보고된 데이터 침해 위반 행위는 전년 대비 46% 증가하였습니다. 이는 규제 강화에 대응하여 위반 사항에 대한 보고가 증가했기 때문이기도 하지만, 동시에 데이터 프라이버시 및 보안에 아쉬운 점이 많다는 뜻이기도 합니다.
- 미국에서 보고된 최소 22건의 위반은 100만건 이상의 기록에 영향을 미쳤습니다.

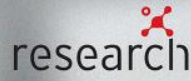
더욱 더 강화되는 데이터 프라이버시 규제

GDPR 데이터 규제 당국은 실제로 아래와 같이 벌금을 부과하였습니다:

- 오스트리아 CCTV 관련 위반: 5,280 유로
- 일반 텍스트로 비밀번호를 저장한 독일 SNS: 20,000 유로
- 포르투갈 병원 의료 자료 관련 위반: 40만 유로

다른 주 및 국가들도 개인 정보 보호 법률을 제정하거나 시행하기 시작했습니다:

- 2월 부터 시행된 호주의 Notifiable Data Breaches Scheme
- 영국은 1998년 이전의 데이터 보호법을 대체하기 위한 The Data Protection 법안에 대해 3월에 공개위원회 심의를 받았습니다.
- 캐나다는 위반 통지에 관한 보다 실용적인 규정을 발표했습니다.
- 2018년 캘리포니아 소비자 개인정보보호법은 6월에 만장일치로 통과되었습니다.
- 일본의 개인정보보호에 관한 법률과 함께 GDPR 의 적정화 선언도 7월에 확정되었습니다.



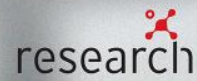
트렌드마이크로 리서치 업데이트

Trend Micro 2018 Annual Security Roundup

- [Ahead of the Curve: A Deeper Understanding of Network Threats Through Machine Learning](#)
 - 머신러닝이 어떻게 많은 양의 데이터를 정리하는 과정을 가속화할 수 있는지 보여주고 분석가들이 결론과 타임제로 프로텍션을 형성하도록 도와드립니다.
- [Adversarial Sample Generation: Making Machine Learning Systems Robust for Security](#)
 - Adversarial samples은 머신러닝의 오작동을 유발할 수 있지만, 또한 ML 시스템의 효율성을 향상시키기 위해 어떻게 사용될 수 있는지 알아볼 수 있습니다.
- [Uncovering Unknown Threats With Human-Readable Machine Learning](#)
 - 이 보고서는 소프트웨어 다운로드의 주요 측면을 탐구한 [시리즈](#)로, 다운로드한 파일의 악성 여부를 판단할 수 있는 머신러닝 기능을 어떻게 개발했는지 알려드립니다.

- Exposed and Vulnerable Critical Infrastructure: Water and Energy Industries
 - 트렌드마이크로 연구원들은 두개의 중요한 산업 분야에서 중소기업들의 산업제어시스템 (ICS)와 휴먼 머신 인터페이스 (HMI)의 보안 격차를 조사하였습니다.
- MQTT and CoAP: Security and Privacy Issues in IoT and IIoT Communication Protocols
 - 본 논문은 IoT 프로토콜 보안을 평가하기 위해 전세계 MQTT 브로커와 CoAP 서버 (사물인터넷, 사물 애플리케이션 및 시스템의 산업용 인터넷에 의해 사용되는 불필요한 통신 프로토콜)를 검토합니다.
- Securing Connected Hospitals: A Research on Exposed Medical Systems and Supply Chain Risks
 - 트렌드마이크로는 HITRUST (Health Information Trust Alliance)와 제휴하여 노출되는 의료 시스템과 장치, 공급망 사이버 위협의 문제를 탐구하였습니다.

- The Rise and Fall of {Scan4You}
 - FBI가 사이버 범죄조직의 주요 2명을 체포해 인도한 후 오프라인으로 전환한 대형 사이버 범죄 조직 Scan4You에 대한 상세 보고서입니다. 트렌드마이크로는 2012년부터 해당 케이스를 연구해 왔으며, 2014년 부터 FBI와 협력해오고 있습니다.
- Evolution of Cybercrime
 - 근 10년 이상 동안 사이버 범죄가 어떻게 변화했는지를 보여줍니다.



Threat Landscape in Review

Trend Micro 2018 Annual Security Roundup

48,387,151,118

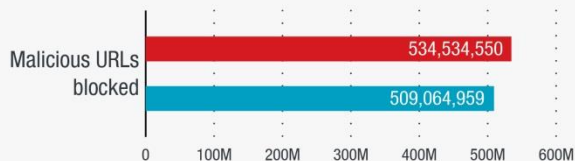
2018년 차단된 위협



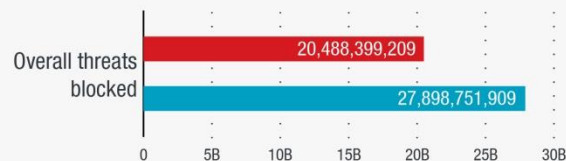
2018 Total: 41,519,659,844



2018 Total: 5,823,891,765



2018 Total: 1,043,599,509



2018 Total: 48,387,151,118

1H 2018 2H 2018



For the complete report, please visit:

[https://www.trendmicro.com/vinfo/us/security/
research-and-analysis/threat-
reports/roundup/unraveling-the-tangle-of-old-
and-new-threats](https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/unraveling-the-tangle-of-old-and-new-threats)