Symantec

요약

2018 인터넷 보안 위협 보고서(ISTR)

ISTR

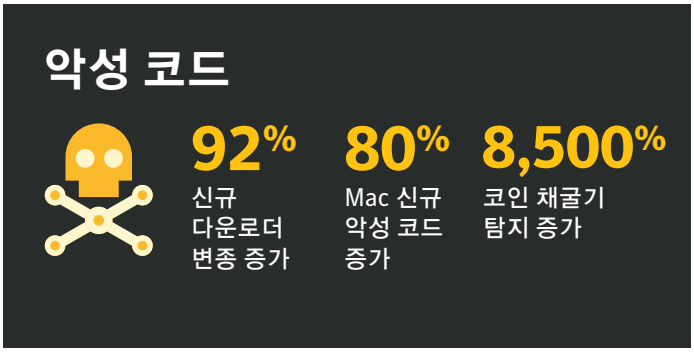
제23호

요약

WannaCry 및 Petya/NotPetya가 갑작스럽게 확산되고 코인 채굴기가 빠른 속도로 증가하는 등 2017년은 디지털 보안 위협이 예상치 못한 새로운 출처로부터 발생할 수 있다는 사실을 다시 상기시켜준 해였습니다. 해가 바뀌면서 공격자들이 새로운 공격 경로를 개발하는 동시에 흔적을 숨기는 데 주력하면서 보안 위협이 양적으로 증가했을 뿐 아니라 보안 위협 환경의 다양성 역시 확대되었습니다.

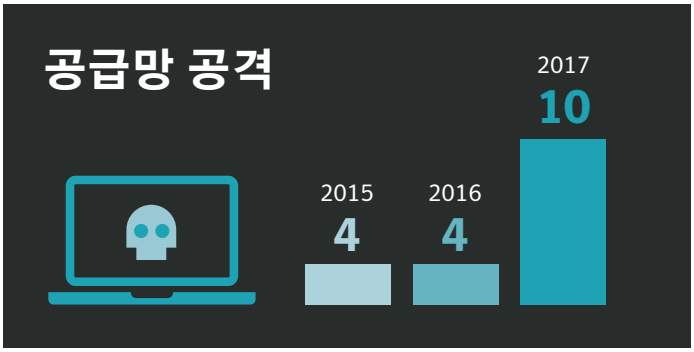
코인 채굴 공격 급증

수익 창출을 위해 랜섬웨어에 집중했던 사이버 범죄자들이 다른 기회도 모색하기 시작했습니다. 지난해 암호 화폐의 가치가 천문학적으로 상승하자 코인 채굴을 대체 수익원으로 인식하는 사이버 범죄자들이 많아졌습니다. 이러한 코인 채굴 열풍으로 인해 2017년에는 엔드포인트 시스템에서 코인 채굴기가 탐지되는 경우가 8,500% 증가했습니다.



몇 줄의 코드만 있으면 작업이 가능할 만큼 진입 장벽이 낮기 때문에 사이버 범죄자들이 코인 채굴기를 이용하여 개인 사용자와 기업으로부터 컴퓨터 처리 능력 및 클라우드 CPU 사용 권한을 훔쳐 암호 화폐 채굴에 사용하고 있습니다. 코인 채굴은 디바이스의 속도가 줄어들고 배터리가 과열되며 경우에 따라 디바이스가 사용 불가 상태가 되는 등 당장 성능과 관련된 문제를 야기하지만 그 영향은 훨씬 광범위하며 특히 기업의 경우 더욱 그렇습니다. 기업의 환경 전반에서 코인 채굴기가 급증하면 기업 네트워크가 중단될 수 있습니다. 또한 코인 채굴기가 사용한 클라우드 CPU에 대해 부과되는 사용 요금 때문에 해당 기업이 재정적 타격을 받을 수도 있습니다.

악성 코인 채굴 기술이 발전하면서 앞으로도 IoT 디바이스가 익스플로잇의 표적으로 주목받을 것입니다. 시만텍 연구 조사에 따르면, 2017년에 전체 IoT 공격이 600% 증가했습니다. 즉 사이버 범죄자는 네트워크에 연결된 이러한 디바이스의 특성을 악용하여 대규모의 채굴을 시도할 수 있습니다.



소프트웨어 공급망 공격 급증

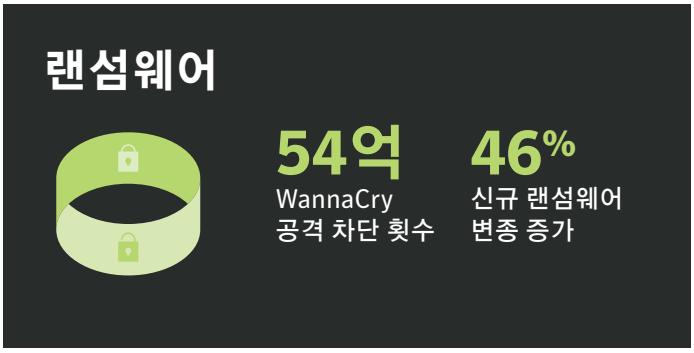
EternalBlue 익스플로잇이 2017년에 엄청난 피해를 일으켰지만, 사실 공격자가 취약점을 찾아내 악용하는 것이 더욱 힘들어지고 있습니다. 그에 대한 반작용으로, 공급망에 악성 코드를 심어두고 의심하지 않은 기업을 감염시키는 공격자가 늘고 있습니다. 2017년에는 이러한 공격이 매달 1회씩 발생했는데, 그 전해에는 연 4회 발생했으므로 200% 증가한 것입니다.

공격자의 입장에서 소프트웨어 업데이트 하이재킹은 강력하게 보호받는 표적에 침투하여 감염시키거나 특정 지역이나 업종을 공략하는 진입 지점 역할을 수행합니다. Petya/NotPetya (Ransom.Petya)가 가장 잘 알려진 예입니다. Petya/NotPetya는 우크라이나의 회계 소프트웨어를 진입 지점으로 삼고 다양한 방법으로 기업 네트워크 전반에 확산되면서 공격자의 악성 페이로드를 배포했습니다.

시장 조정 단계에 진입한 랜섬웨어 비즈니스

비즈니스 관점에서 보면, 2016년 랜섬웨어 수익성에 자극을 받아 누구나 시장에 뛰어들면서 몸값 요구액도 지나치게 올랐습니다. 2017년에는 랜섬웨어 제품군이 줄어들고 몸값 요구액도 낮아지면서 '시장 조정'이 이루어졌습니다. 랜섬웨어가 일종의 상용품이 된 것입니다. 상당수의 사이버 범죄자가 높은 가치를 보유한 암호 화폐를 수익 실현의 대안으로 간주하고 코인 채굴 쪽으로 방향을 돌린 듯합니다. 기존의 랜섬웨어 집단이 다각화를 시도하면서 일부 온라인 뱅킹 보안 위협도 부흥기를 맞이했습니다.

지난해 평균 몸값 요구액은 522달러로 그 전해 평균의 절반도 되지 않습니다. 랜섬웨어 변종 수는 46% 증가하여 기존 범죄 집단이 아직도 왕성하게 활동 중임을 보여주지만, 랜섬웨어 제품군의 수는 감소했습니다. 즉 예전만큼 혁신적이지 않고 더 가치가 높은 새로운 표적으로 관심을 옮겼을 수도 있습니다.



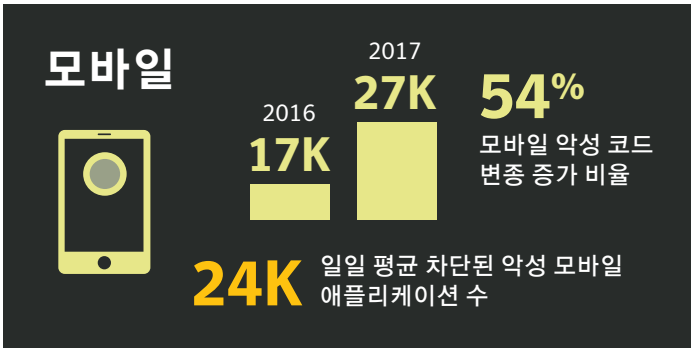
제로데이는 줄었으나 여전히 증가세인 표적 공격

시만텍 연구 조사에 따르면, 전체적으로 표적 공격 활동이 2017년에 10% 증가했는데, 정보 수집(90%)이 주 동기였습니다. 그러나 비중이 크지 않은 10%의 공격 집단은 어떤 형태로든 파괴적인 활동을 벌이고 있습니다.

공격 집단이 표적으로 삼은 기업에 침투할 때 이미 검증되어 믿을 수 있는 방법을 사용하는 이른바 '자급자족' 추세가 계속되고 있습니다. 2017년에는 스피어피싱이 감염 경로 1위를 차지했는데, 조직화된 공격 집단의 71%가 사용했습니다. 제로데이의 인기는 계속 하락세입니다. 시만텍이 추적하는 140개 표적 공격 집단 중에서 과거에 제로 데이 취약점을 이용했던 것으로 알려진 곳은 27%에 불과했습니다.

계속 급증하는 모바일 악성 코드

모바일 환경의 보안 위협은 이번에도 전년 대비 증가했습니다. 2017년 새로운 모바일 악성 코드 변종의 수는 2016년 대비 54% 증가했습니다. 또한 지난해 매일 평균 24,000개의 악성 모바일 애플리케이션이 차단되었습니다.



보안 위협이 증가하는 추세이지만, 문제가 더 심각해진 것은 오래된 운영 체제가 계속 사용되고 있기 때문입니다. 특히 Android™에서 최신 주요 버전을 실행 중인 디바이스가 20%, 최신 부수적 릴리스를 설치한 디바이스는 2.3%에 불과합니다.

모바일 사용자는 그레이웨어, 즉 100% 악성은 아니지만 문제를 일으킬 수 있는 앱으로 인해 개인 정보가 유출될 위험도 있습니다. 시만텍은 그레이웨어 앱의 63%에서 디바이스의 전화 번호가 유출되고 있음을 확인했습니다. 그레이웨어가 2017년에 20% 증가한 만큼 당분간 이 문제가 계속될 것으로 보입니다.

자세한 내용은
시만텍 2018 인터넷 보안 위협 보고서(ISTR)
(https://go.symantec.com/kr/istr)에서 확인하십시오.

시만텍 소개

글로벌 사이버 보안 분야를 선도하는 시만텍은 기업, 정부 기관 및 개인의 중요한 데이터가 어디에 있든 안전하게 보호될 수 있도록 지원한다. 시만텍은 엔드포인트, 클라우드, 인프라 전반을 정교한 공격으로부터 방어할 수 있는 전략적인 통합 솔루션을 전 세계 기업과 기관에 제공하고 있다.

또한, 전 세계 5천만 이상의 개인사용자와 가정에서 시만텍 노턴 제품과 라이프록(LifeLock) 제품을 이용해 가정과 다양한 기기에서 디지털 라이프를 보호하고 있다. 시만텍은 세계 최대 규모의 민간 사이버 인텔리전스 네트워크를 통해 고도화된 지능형 위협을 탐지하고 고객들을 보호한다. 보다 자세한 정보는 시만텍 웹사이트(www.symantec.com/ko/kr)와 페이스북, 트위터, 링크드인을 통해 확인할 수 있다.

시만텍코리아
서울시 강남구 테헤란로 152
강남파이낸스센터 28층

TEL: 02-3468-2000
FAX: 02-3468-2001

www.symantec.com/ko/kr

ISTR
(인터넷 보안 위협 보고서)

Copyright © 2018 Symantec Corporation. All rights reserved. Symantec, Symantec 로고, Checkmark 로고는 미국 및 기타 국가에서 Symantec Corporation 또는 그 자회사의 상표 또는 등록 상표입니다. 다른 이름은 해당 회사의 상표일 수 있습니다. 03/18