Symantec

INTERNET SECURITY THREAT REPORT

요약

인터넷 보안 위협 보고서

2019년 인터넷 보안 위협 보고서

ISTR

제24호

요약

폼재킹, 표적 공격, 자력형 공격이 비즈니스 위협

수많은 범죄자들이 최소한의 노력으로 손쉽게 돈을 벌 수 있는 최신 익스플로잇에 집중하고 있습니다. 한때 랜섬웨어와 크립토재킹이 유행했으며, 이제 폼재킹(Formjacking)의 시대가 도래했습니다.

시만텍은 인터넷 보안 위협 보고서(ISTR) 제 24호에서 글로벌 보안 위협 활동, 사이버 범죄자 동향, 공격자 동기에 관해 통찰력 있는 정보를 공유합니다.

이 보고서는 전 세계 1억 2,300만 개 공격 센서에서 이벤트를 기록하고, 일일 1억 4,200만 개의 보안 위협을 차단하며, 157개국 이상의 보안 위협 활동을 모니터링하는 세계 최대 규모의 보안 위협 인텔리전스 네트워크인 Symantec Global Intelligence Network에서 수집한 데이터를 분석합니다.

{FORMJACKING}

폼재킹

폼재킹으로 손쉽게 수익을 올리는 사이버 범죄자들

폼재킹 공격은 간단하며 수익성이 높습니다. 사이버 범죄자는 소매업체의 웹 사이트에 악성 코드를 로드하여 구매자의 신용 카드 정보를 훔쳐내며, 매월 평균 4,800개 이상의 웹 사이트가 감염됩니다.

실제로 티켓마스터 및 영국항공과 같이 잘 알려진 기업이나 중견기업 모두 공격을 받았으며, 공격자들은 지난 한 해 수천만 달러 이상의 수입을 거두었습니다.

감염된 웹 사이트당 도용된 10개의 신용 카드로 매월 220만 달러의 수익을 거두고, 지하시장에서는 신용 카드 한 장당 최대 45달러를 벌어들입니다. 영국항공에 대한 공격 한 건으로 380,000개의 신용 카드가 도용되고 범죄자들의 순수익이 1,700만 달러를 상회합니다.

RANSOMWARE

랜섬웨어

CRYPTOJACKING

크립토재킹

하락세에도 공격은 지속

랜섬웨어와 크립토재킹(Cryptojacking) 역시 사이버 범죄자들의 지속적인 수익원입니다. 하지만 2018년에는 수익이 줄어들면서 활동 역시 적어졌습니다.

랜섬웨어는 2013년에 처음 등장한 이래 전체적으로 20% 하락했지만 기업을 대상으로는 12% 증가한 수치를 기록했습니다.

크립토재킹은 암호 화폐 가치가 90% 급감하면서 2018년에 52% 하락했습니다. 그럼에도 낮은 진입 장벽과 최소한의 간접비로 여전히 인기 있는 악성 코드입니다. 실제로 시만텍은 2018년에 전년 대비 4배 많은 크립토재킹을 차단했습니다.

TARGETED ATTACKS

표적 공격

파괴적인 활동을 선호하는 표적 공격자들

SW 공급망 및 자력형 공격(Living-off-the-Land, LotL)은 사이버 범죄자들의 주 활동 무대가 되었으며, 2018년에 공급망 공격은 78%까지 급증했습니다.

공격자는 자력형 공격 기법을 통해 합법적인 프로세스에 악성 코드를 숨길 수 있습니다. 예를 들어, 악성 파워쉘 (PowerShell) 스크립트는 작년 한 해 최대 1,000% 증가했습니다.

시만텍은 매월 115,000개의 악성 파워쉘 스크립트를 차단했지만, 이 수치는 전체 파워쉘 사용의 1% 미만에 해당할 뿐입니다. 하지만 무작정 전체 파워쉘 활동을 차단하는 방식을 사용하면 비즈니스 활동을 저해하게 되므로 대다수 표적 공격 그룹이 자력형 기법을 선호 전술로 활용하여 감시망을 피해 은밀히 활동합니다.

MORE AMBITIOUS
보다 강력하고

AND STEALTHIER
은밀한 공격

또한 기업 침투를 위해 스피어 피싱과 같이 효과가 입증된 방법이 더 많이 사용되었습니다. 분석자들은 여전히 공격자들의 일차적인 동기를 수집하지만 일부 그룹은 파괴에도 집중합니다. 실제로 10개 중 1개에 달하는 표적 공격 그룹이 악성 코드를 사용하여 업무를 방해하거나 비즈니스 운영을 중단시키고 있으며, 이는 이전 연도 대비 25% 증가한 수치입니다.

일례로 2년간 사라졌다가 다시 등장한 샤문(Shamoon)은 와이핑(wiping) 악성 코드를 배포하여 중동의 한 표적 기업에 있는 시스템에서 파일을 삭제하기도 했습니다.

CLOUD

클라우드

클라우드 관련 과제: 클라우드 데이터 관련 보안은 사용자의 몫

잘못 구성된 단일 클라우드 워크로드나 스토리지 인스턴스로 인해 기업이 수백만 달러의 비용을 지출하거나 심각한 컴플라이언스 문제에 직면하게 될 수 있습니다. 2018년에는 잘못 구성된 S3 버킷에서 7천만 개 이상의 레코드가 유출되거나 도난당하는 일이 발생했습니다. 공격자는 웹상의 사용 툴을 통해 잘못 구성된 클라우드 리소스를 식별할 수 있습니다.

침입자는 Meltdown, Spectre, Foreshadow와 같은 하드웨어 칩 취약점을 이용하여 동일한 물리적 서버에 호스팅된 클라우드 서비스의 보호받는 메모리 공간에 액세스할 수 있습니다. 익스플로잇에 성공할 경우 일반적으로 금지된 메모리 위치에 대한 액세스가 허용됩니다.

이는 클라우드 서비스에서 특히 문제가 되는데, 클라우드 인스턴스가 자체 가상 프로세스를 보유하여 메모리 풀을 공유하기 때문입니다. 즉 물리적 시스템 한 대에 대한 공격이 성공하면 여러 클라우드 인스턴스의 데이터가 유출되는 셈입니다.

IoT

선호하는 IoT 디바이스가 주요 공격 경로

라우터 및 연결된 카메라가 감염된 디바이스의 90%를 차지하지만 스마트 전구부터 음성 인식 비서에 이르는 대부분의 IoT 디바이스가 공격에 취약한 상태입니다.

점점 더 많은 표적 공격 그룹이 IoT를 진입점으로 삼아 디바이스를 지우거나 파괴하고, 인증 정보 및 데이터를 훔쳐내며, SCADA 통신을 가로채고 있습니다.

산업용 IT는 운영 및 산업 제어 시스템을 손상시키는 쓰립(Thrip) 또는 트리톤(Triton)과 같은 보안 위협 그룹의 잠재적인 사이버 전쟁터로 부상했습니다.

ELECTION INTERFERENCE 2018

2018년 선거 방해

선거 결과에 영향을 미치는 소셜 미디어 피드

이목이 집중된 2018 미국 중간 선거는 별다른 사고 없이 무사히 치러졌습니다. 하지만 소셜 미디어상의 논쟁은 여전히 치열합니다.

합법적인 정치 웹 사이트를 모방한 악성 도메인이 발견되고 중단되었으며, 러시아 연결 계정에서 제 3자를 통해 소셜 미디어 광고를 구입했습니다.

소셜 미디어 회사는 선거 방해 공작에서 보다 적극적인 역할을 담당하고 있습니다. 페이스북은 작전실을 구축하여 선거 방해 작업을 방지하고, 트위터는 투표 만류 메시지를 게시하는 10,000개 이상의 봇을 제거했습니다.

선거 보안

민주주의를 실현하려면 올바른 사이버 보안이 필요합니다.

자세히 보기 ▸

자세히 알아보십시오. 시만텍 2019 인터넷 보안 위협 보고서(ISTR)를 다운로드하십시오.
https://symc.ly/APISTR

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