2020

SONICWALL 사이버 위협 보고서

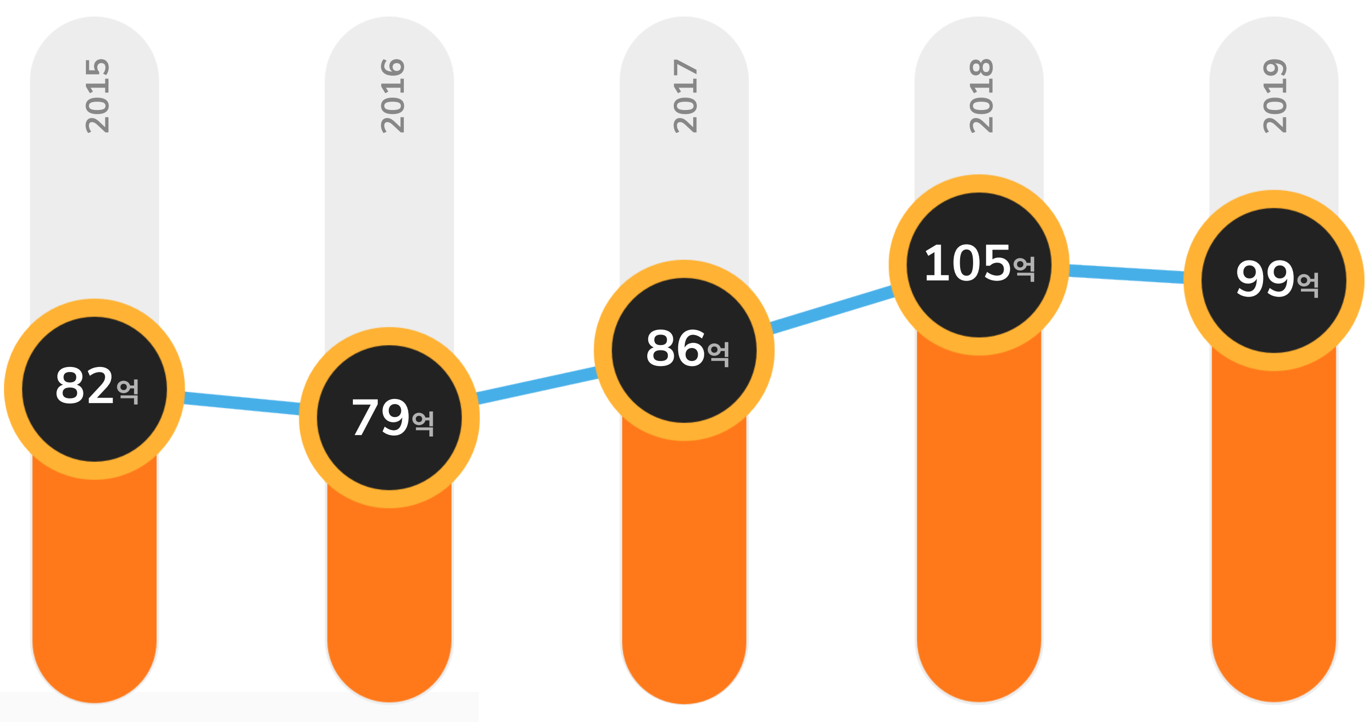
디지털 세상에는 국경이 없습니다. 수많은 장치, 앱, 어플라이언스, 서버, 네트워크, 클라우드, 사용자 규모는 한때는 유한하고 보호가 가능했던 수준이었으나 이제는 기하급수적으로 증가하게 되었습니다.

SonicWall의 독점적 위협 인텔리전스를 확인하고 사이버 범죄자들의 사고 방식을 이해하여 그들의 범죄 행위에 충분히 대비하시기 바랍니다.

발생 건수는 줄었지만 보다 고도화되고 집중화된 맬웨어 공격

99억

건의 맬웨어 공격이 2019년에 SonicWall에 의해 기록되었는데* 이러한 수치는 최고 기록을 달성했던 2018년의 105.2억건보다 6% 하락한 수준입니다.



새로운 표적을 찾은 랜섬웨어

1억 8790만

민감한 데이터를 보유하고 있거나 필요한 대로 자금 지출을 할 수 있어(또는 둘 다) 더 많은 돈을 지불할 것 같은 피해자들을 예리하게 표적 대상으로 공격하기 위해 랜섬웨어가 사용되고 있습니다.

2019년에 주 정부, 지방 정부, 지역 정부와 교육 기관을 상대로 1억 8790건의 랜섬웨어 공격이 발생했었습니다.

흔들리는 크립토재킹

비트코인과 상호보완적 암호화폐의 가격으로 인해 코인하이브(Coinhive) 기반의 크립토재킹 맬웨어와 합법적인 코인하이브 채굴 서비스 사이에 불안정한 상황이 생겼습니다.

78%

코인하이브의 폐쇄로 크립토재킹 공격의 건수가 2019년 하반기에 78% 하락했습니다.

파일리스 맬웨어, 3분기에 최고치

파일리스 맬웨어는 메모리 기반 요소로 존재하며 컴퓨터의 하드 드라이버에 그 활동을 전혀 기록하지 않으므로 기존의 컴퓨터 포렌식 방식에 매우 강합니다. 발생 건수가 3분기에 최고점을 찍었고 SonicWall은 2019년 9월에만 570,000건 이상을 확인했습니다.

2019년 파일리스 맬웨어 발생 건수

암호화된 위협이 지속적으로 상승

노련한 사이버 범죄자들은 TLS/SSL 암호화를 계속 사용하여 기존 보안 통제 수단에 의한 검사에서 공격의 정체를 감추고 있습니다. 2019년에 SonicWall Capture Labs 위협 연구원들은 TLS/SSL 트래픽을 통해 맬웨어 공격이 작년 대비 27.3%가 증가했음을 확인했습니다.

27%

2019년에 TLS/SSL 트래픽을 통해 맬웨어 공격 증가.

증가하는 IOT 공격 규모

2019년에 SonicWall은 IoT 맬웨어 공격이 5%가 증가한 것으로 파악했으며 총 사례 수는 3430만 건이었습니다.

그러나 매일 연결되는 많은 수의 새로운 IoT 장치로 IoT 맬웨어 공격의 증가는 확실하게 예견되고 있습니다.

3430만

다음 할 일을 대비하세요

웹사이트 SonicWall.com/ThreatReport를 방문하여 전체 내용의 **2020 SonicWall 사이버 위협 보고서**를 다운로드하십시오. 위협 인텔리전스를 확인하고 사이버 범죄자들의 사고 방식을 이해하여 그들의 범죄 행위에 충분히 대비하시기 바랍니다.

전체 보고서를 확인하세요

SONICWALL®

| SonicWall.com

* SonicWall은 모범적 방식으로서 정기적으로 데이터의 수집, 분석, 보고 방법을 최적화하고 있습니다. 여기에는 데이터 정화 조정사항, 데이터 출처의 변경, 위협 피드의 통합 등이 포함됩니다. 이전 보고서에서 공개된 수치는 다양한 시기, 지역 또는 업계에 맞게 조정되었을 수 있습니다.