2020 SONICWALL CYBER THREAT REPORT

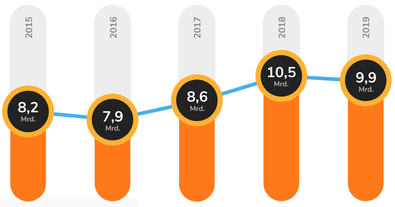
Die Grenzen Ihres digitalen Imperiums sind unabsehbar. Was einst ein abgegrenzter und verteidigbarer Raum war, ist heute ein grenzenloses Territorium – ein riesiger, weit verstreuter Bestand an Geräten, Apps, Appliances, Servern, Netzwerken, Clouds und Benutzern.

Machen Sie sich mit den exklusiven Bedrohungsinformationen von SonicWall vertraut, um besser zu verstehen, wie Cyberkriminelle denken – und um auf die nächsten Bedrohungen vorbereitet zu sein.

MALWARE WIRD WENIGER, ABER GEZIELTER UND RAFFINIERTER

9,9 Mrd.

Malware-Angriffe wurden von SonicWall im Jahr 2019 protokolliert*, was einem Rückgang von 6 % gegenüber dem Rekordvolumen von 10,52 Milliarden im Jahr 2018 entspricht.



EIN NEUES ZIEL FÜR RANSOMWARE

187,9 Mio

Ransomware-Angriffe richteten sich jetzt auf solche Opfer, die aufgrund ihrer hochsensiblen Daten oder ausreichender verfügbaren Finanzen (oder beides) mit höherer Wahrscheinlichkeit bezahlen werden.

Das bedeutet, dass sich 2019 ein Großteil der 187,9 Millionen Ransomware-Angriffe gegen staatliche, provinziale und lokale Regierungen sowie Bildungssysteme richtete.

KRYPTOJACKING AM AUSSTERBEN

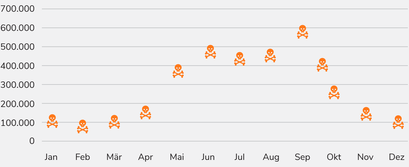
Der Preis von Bitcoins und komplementären Kryptowährungen sorgte für eine unkontrollierbare Situation zwischen Coinhive-basierter Kryptojacking-Malware und dem legitimen Coinhive-Mining-Service.

78 % Nach der Schließung von Coinhive sank das Volumen der Kryptojacking-Hits in der zweiten Jahreshälfte 2019 um 78 %.

DATEILOSE MALWARE-ANGRIFFE ERREICHEN IHREN HÖCHSTSTAND IM 3. QUARTAL

Dateilose Malware existiert ausschließlich als Artefakt im Arbeitsspeicher. Da kein Teil der schädlichen Aktivität auf die Festplatte des Computers geschrieben wird, sind die im Computer eingesetzten forensischen Strategien ziemlich wirkungslos. Mit mehr als 570.000 Angriffen, die SonicWall allein im September 2019 verzeichnete, erreichte das Volumen im dritten Quartal seinen Höhepunkt.

Volumen an dateiloser Malware 2019



KONSTANTER ANSTIEG BEI VERSCHLÜSSELTEN BEDROHUNGEN

Erfahrene Cyberkriminelle verwenden weiterhin die TLS/SSL-Verschlüsselung, um ihre Angriffe vor den Inspektionen durch herkömmliche Sicherheitskontrollen zu verbergen. 2019 verzeichneten die Bedrohungsforscher von SonicWall Capture Labs bei der im TLS/SSL-Datenverkehr eingeschleusten Malware einen Anstieg von 27,3 % gegenüber dem Vorjahr.

27 % Zunahme der im TLS/SSL-Verkehr eingeschleusten Malware 2019.

IOT-ANGRIFFSVOLUMEN IM STEIGEN

2019 stellten die Bedrohungsforscher von SonicWall Capture Labs einen Anstieg der IoT-Malware um 5 % und ein Gesamtvolumen von 34,3 Millionen Angriffen fest.

Angesichts der Flut von neuen IoT-Geräten, die sich jeden Tag miteinander verbinden, ist ein Anstieg von IoT-Malware-Angriffe nicht nur zu erwarten, sondern Unternehmen sollten sich gezielt darauf vorbereiten.

34,3 Mio

BEREITEN SIE SICH VOR

Besuchen Sie SonicWall.com/ThreatReport um den vollständigen **SonicWall Cyber Threat Report 2020** herunterzuladen. In diesem Bericht erhalten Sie wichtige Bedrohungsinformationen, die Ihnen helfen besser zu verstehen, wie Cyberkriminelle denken – und die Sie auf die nächsten Bedrohungen vorbereiten.

BERICHT ABRUFEN

SONICWALL

SonicWall.com

* Im Rahmen seiner Best-Practice-Vorgaben optimiert SonicWall auf regelmäßiger Basis seine für Erfassung, Analyse und Reporting eingesetzte Methodik. Dazu gehören u. a. Optimierungen der Datenbereinigung, Änderung der Datenquellen und Konsolidierung der Threat-Feeds. Die in früheren Reports veröffentlichten Zahlen wurden eventuell für verschiedene Zeitspannen, Regionen oder Branchen angepasst.