SONICWALL

Cyber Threat Report 2019

KURZFASSUNG | EUROPÄISCHE AUSGABE

SonicWall.com

SONICWALL®

CAPTURE LABS

EINFÜHRUNG: EUROPÄISCHE AUSGABE

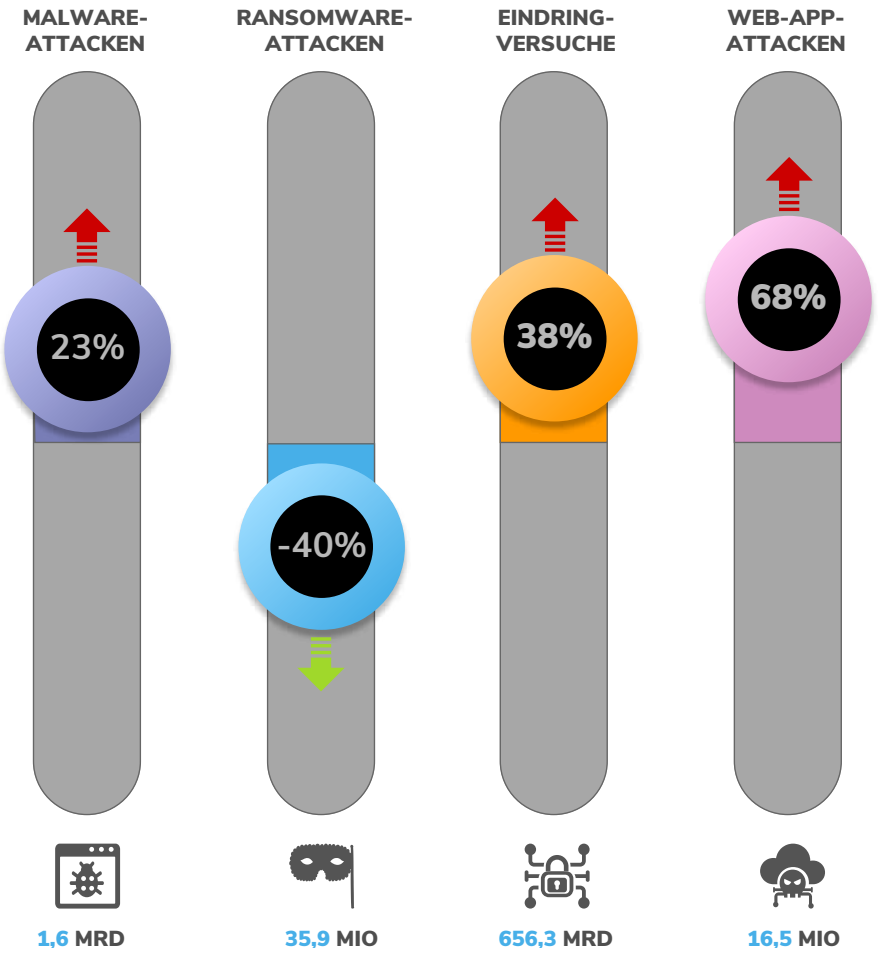
In der Welt der Cyberbedrohungen wird nicht diskriminiert oder differenziert. Netzwerke, Identitäten, Geräte oder Daten von Wert — insbesondere geistiges Eigentum, Finanzdaten, sensible Dateien, kritische Infrastruktur oder politisch nutzbare Informationen — werden von Cyberkriminellen identifiziert, ins Visier genommen und skrupellos angegriffen.

SonicWall steht fest zu seiner Verpflichtung zur Erforschung, Analyse und Bereitstellung von Informationen zu Cyberbedrohungen und veröffentlicht die gewonnenen Erkenntnisse in seinem SonicWall Cyber Threat Report 2019. Diese Kurzfassung wird ergänzend zu dem detaillierten Report herausgegeben und liefert einen Überblick über die von SonicWall Capture Labs gewonnenen Erkenntnisse.

SONICWALL®

WICHTIGE ERKENNTNISSE 2018

CYBERATTACKEN-TRENDS 2018 IN EUROPA



- Albanien
- Andorra
- Belgien
- Bosnien und Herzegowina
- Bulgarien
- Dänemark
- Deutschland
- Estland
- Finnland
- Frankreich
- Gibraltar
- Griechenland
- Großbritannien/ Nordirland
- Guernsey
- Irland
- Island
- Isle of Man
- Italien
- Jersey
- Kroatien
- Lettland
- Liechtenstein
- Litauen
- Luxemburg
- Malta
- Mazedonien
- Niederlande
- Norwegen
- Österreich
- Polen
- Portugal
- Rumänien
- Russland
- San Marino
- Schweden
- Schweiz
- Serbien
- Slowakei
- Slowenien
- Spanien
- Tschechien
- Ukraine
- Ungarn
- Weißrussland
- Zypern

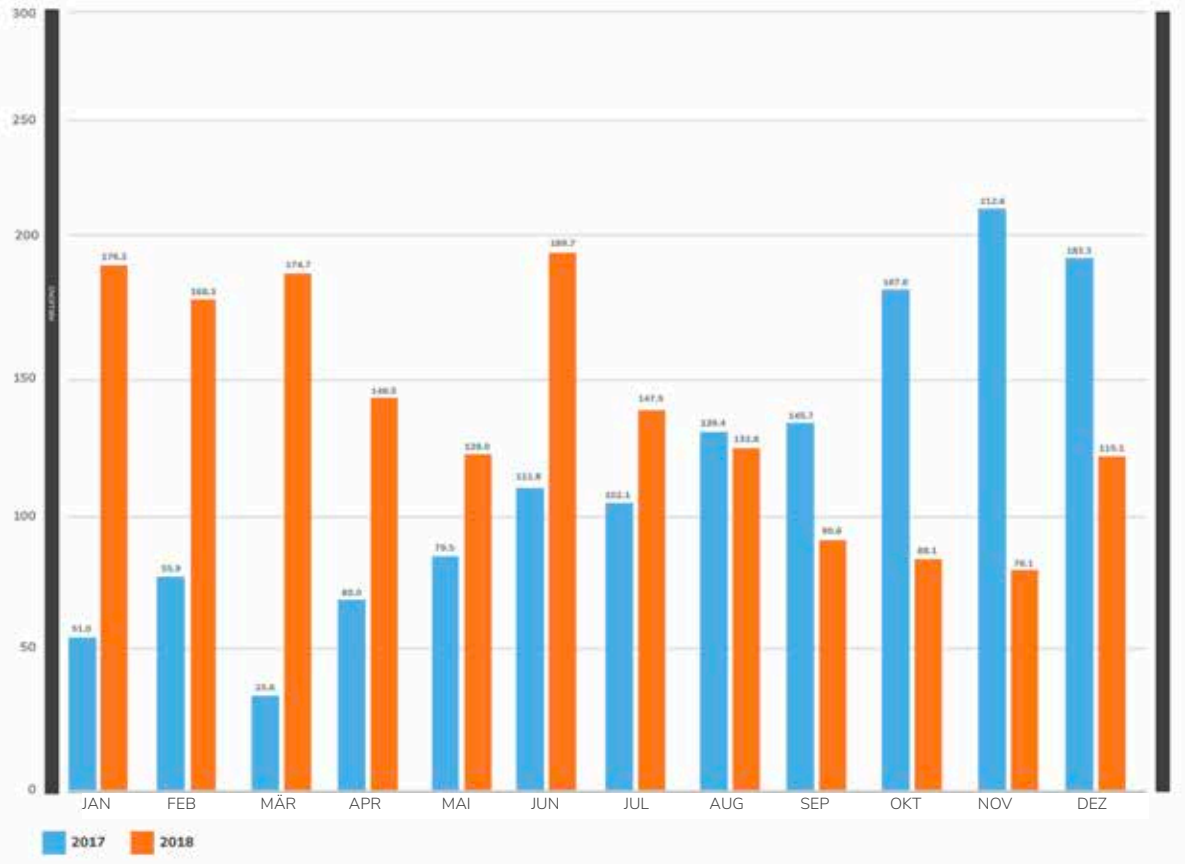
SONICWALL®

DAS MALWARE-VOLUMEN STEIGT WEITER

Mit dem Rückgang des Malware-Volumens im Jahr 2016 tauchten schnell Spekulationen auf, dass die Cyberkriminalität insgesamt im Abklingen begriffen sei. Doch leider ist das Aufkommen von **Malware-Attacken seitdem um 33,4 % gestiegen**.

SonicWall hat 2018 weltweit 10,52 Milliarden* Malware-Attacken protokolliert, die höchste Zahl seit Beginn dieser Erfassungen. Allein in Europa verzeichnete SonicWall 1,64 Milliarden Malware-Attacken — ein Anstieg von 23 % gegenüber 2017. Interessant ist, dass sich trotz des Volumenanstiegs im Jahr 2018 im Juni desselben Jahres ein Abwärtstrend abzeichnete.

MALWARE-VOLUMEN 2018 IN EUROPA



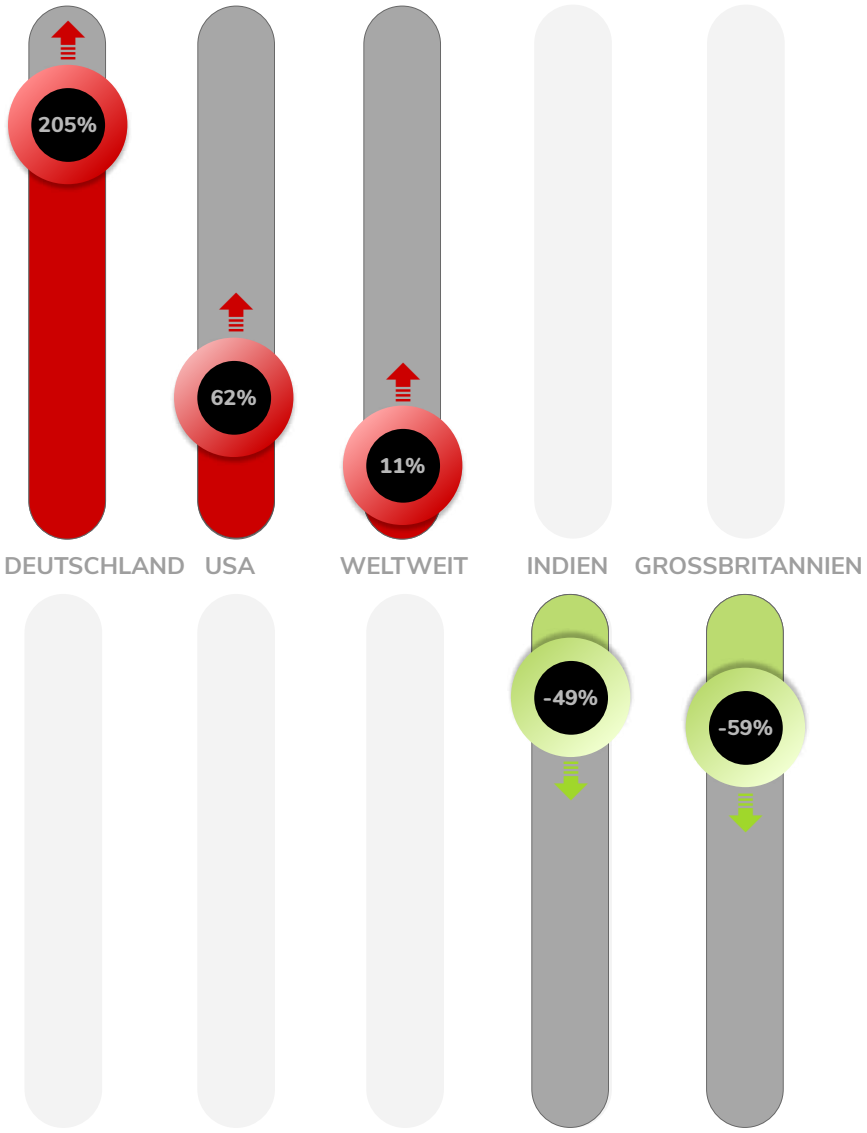
* Im Rahmen seiner Best-Practice-Vorgaben optimiert SonicWall auf regelmäßiger Basis seine für Erfassung, Analyse und Reporting eingesetzte Methodik. Dazu gehören u. a. Verbesserung der Datenbereinigung, Änderung der Datenquellen und Konsolidierung der Threat-Feeds. Die in früheren Reports veröffentlichten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

GROSSBRITANNIEN UND INDIEN WAPPNEN SICH GEGEN RANSOMWARE

Eine Analyse der Threat-Daten des gesamten Jahres 2018 durch die Bedrohungsforscher von SonicWall Capture Lab brachte ein schockierendes Resultat. Das Ransomware-Volumen ist in allen geografischen Regionen gestiegen, außer in zwei Ländern: Großbritannien/Nordirland und Indien.

Während alle größeren Länder in Nordamerika, Europa und Asien einen Anstieg der Ransomware-Attacken verzeichneten, reduzierte sich das Ransomware-Volumen in **Großbritannien und Indien um jeweils 59 % und 49 %**.

Anteilmäßig waren die folgenden Länder am stärksten betroffen: **Auf Deutschland entfielen 27,6 % des europäischen Ransomware-Volumens**, auf Italien 23 %, Großbritannien 13,2 %, die Niederlande 10,7 % und Frankreich 9,9 %.



GEFÄHRLICHE ARBEITSSPEICHER-BEDROHUNGEN, SEITENKANALATTACKEN FRÜHZEITIG ERKANNT

Mit einer zum Patent angemeldeten Technologie entschärft SonicWall Real-Time Deep Memory Inspection (RTDMI™) gefährliche Seitenkanalangriffe. Seitenkanäle sind das fundamentale Transportmittel für die zur Ausnutzung und Exfiltration der Daten von Prozessorschwachstellen verwendeten Techniken, wie Foreshadow, PortSmash, Meltdown und Spectre.

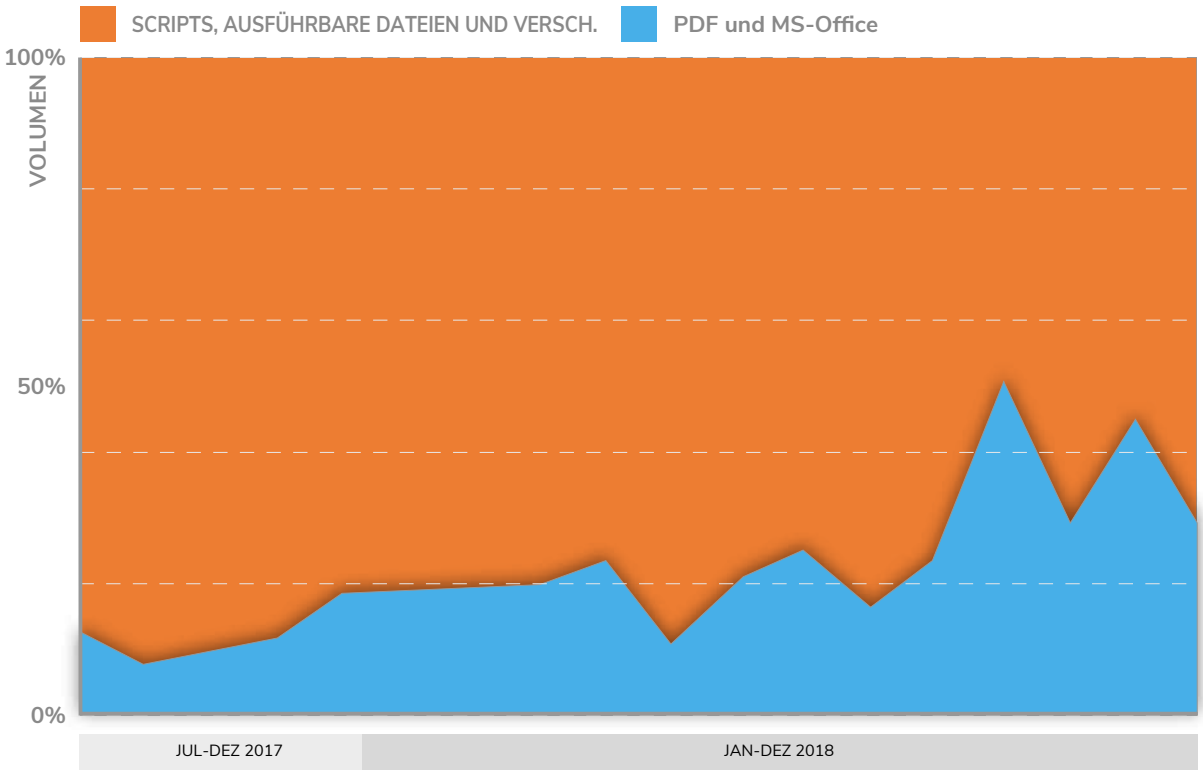
Eine kürzlich unter dem Titel **„Spectre is here to stay“** veröffentlichte Forschungsarbeit bestätigt, dass verschiedene Schwachstellen in den heutigen Prozessoren weder software- noch hardwareseitig behoben werden können, was schwere Sicherheitsbedenken aufbringt. Da Seitenkanalattacken weiterhin ein großes Risiko im Computing-Umfeld darstellen, wird eine Technologie zur Minimierung solcher Attacken zur grundlegenden Voraussetzung.

SONICWALL®

SCHÄDLICHE PDF- UND MS-OFFICE-DATEIEN ÜBERWINDEN BISHERIGE SICHERHEITSKONTROLLEN

Cyberkriminelle machen sich PDF- und Office-Dateien zunutze, um herkömmliche Firewalls und sogar Single-Engine-Sandboxen zu umgehen.

IMMER MEHR SCHÄDLICHE PDF- UND MICROSOFT-OFFICE-DATEIEN



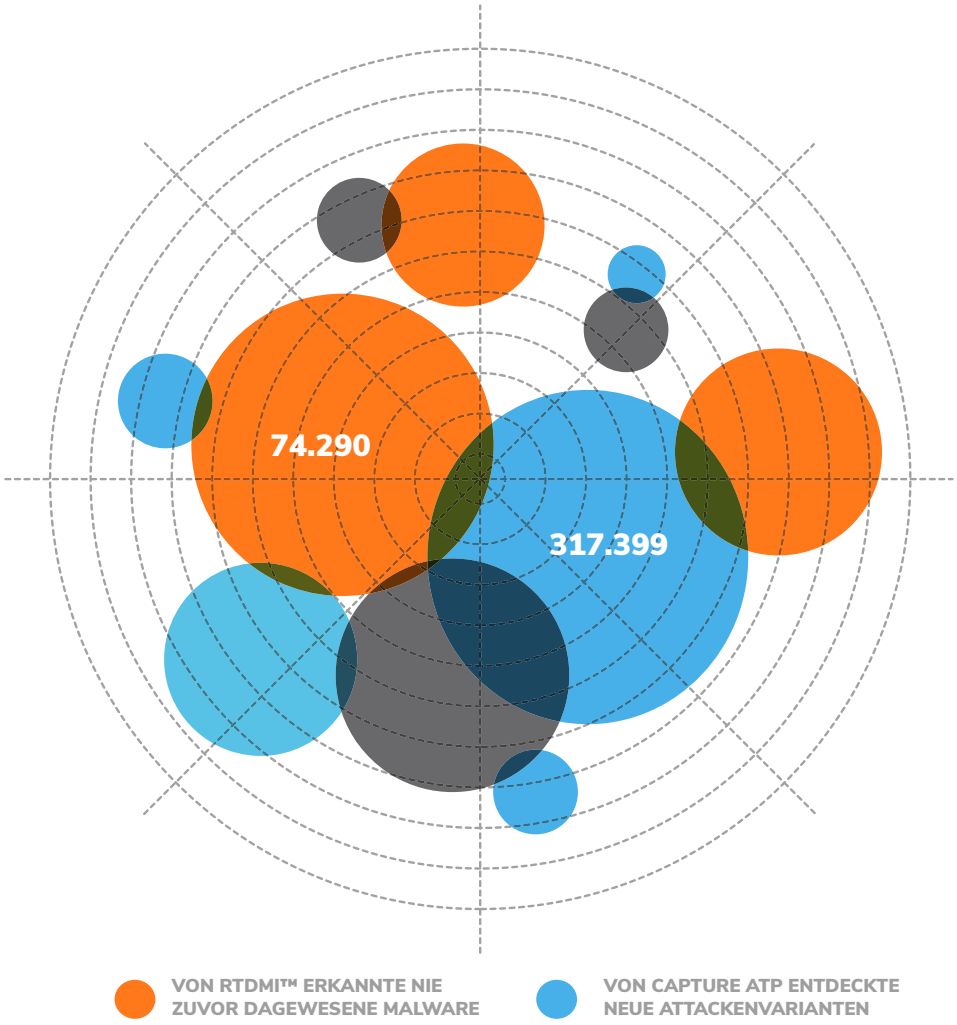
2018 wurden mit dem SonicWall Capture ATP **Multi-Engine Sandbox Service 47.073 PDFs und 50.817 Office-Dateien mit versteckter Malware** identifiziert. Da die meisten Sicherheitskontrollen die in diesen Dateien versteckte Malware nicht erkennen und abwehren können, erhöht sich der Erfolg dieser bösartigen Nutzlast weit über das auf den ersten Blick gering scheinende Volumen hinaus.

AUSGEREIFTES MACHINE LEARNING STOPPT NOCH NIE ZUVOR DAGEWESENE MALWARE-VARIANTEN

SonicWall Capture Advanced Threat Protection (ATP) erkannte 391.689 neue Angriffsvarianten im Jahr 2018. Das bedeutet, dass im Durchschnitt **jeden Tag 1.072 neue Attacken entdeckt und blockiert werden**.

Capture ATP nutzt eine Cloud-basierte Multi-Engine-Sandbox, die parallel mit der zum Patent angemeldeten RTDMI™ Technologie von SonicWall eingesetzt wird. Beide Kapazitäten wurden im Verlauf des Jahres 2018 durch konstantes dynamisches Selbstlernen und Selbstverbessern ausgereifter.

Im Jahr 2018 erkannte **RTDMI™ 74.290 noch nie zuvor dagewesene Attacken**. Dabei handelt es sich um Malware-Varianten, die so neu, einzigartig oder komplex sind, dass zum Zeitpunkt ihrer Entdeckung durch SonicWall kein anderer Anbieter weltweit fähig war, deren Signaturen zu verfolgen oder zu erstellen.

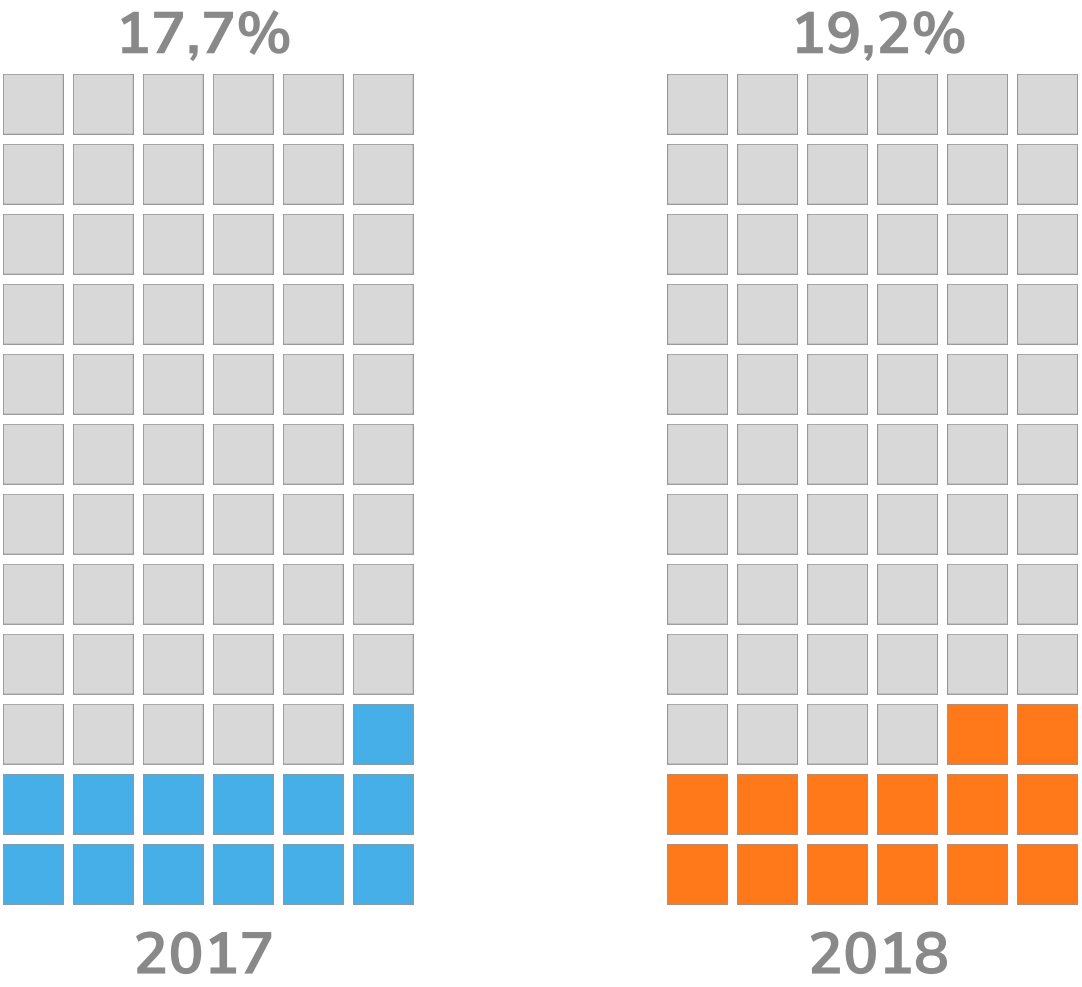


SONICWALL®

NICHT-STANDARD-PORTS REIF FÜR DEN MISSBRAUCH

Port 80 und Port 443 sind Standard-Ports für den Webverkehr und deshalb im Fokus der meisten Firewalls. Deshalb richten Cyberkriminelle ihre Aufmerksamkeit den Nicht-Standard-Ports zu, um so Ihre „Nutzlasten“ unerkannt in das jeweilige Zielumfeld einschleusen zu können.

ÜBER NICHT-STANDARD-PORTS EINGEHENDE MALWARE-ATTACKEN 2018



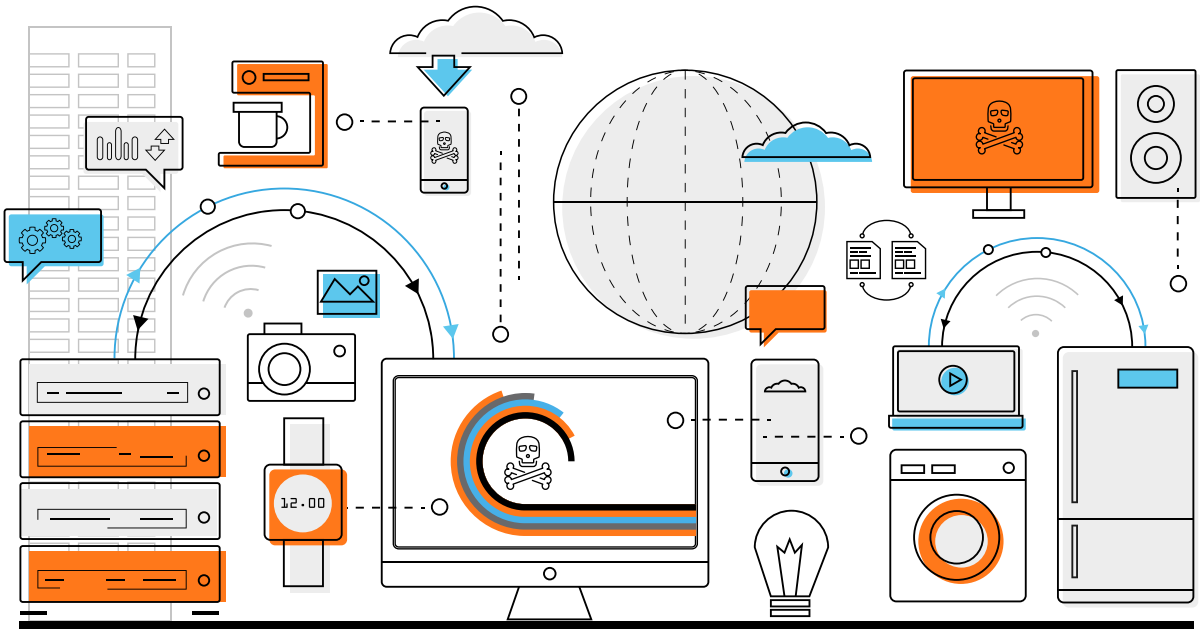
Bei einer Stichprobe von mehr als 700 Millionen Malware-Attacken im Jahr 2018 hat SonicWall entdeckt, dass **19,2 % aller Malware-Attacken über Nicht-Standard-Ports eingeschleust werden**. Aufgrund der großen Anzahl können herkömmliche proxybasierte Firewalls keine über Nicht-Standard-Ports eingehende Attacken abwehren (weder bei verschlüsseltem noch bei unverschlüsseltem Verkehr).

SONICWALL®

RASCHER ANSTIEG VON IoT-ATTACKEN

Der Bedarf an verbundenen Geräten steigt seit einiger Zeit in Riesenschritten an. Dies führte dazu, dass eine Flut von Internet of Things (IOT)-Geräten rasch und ohne ausreichende Sicherheitskontrollen auf den Markt gebracht wurde. In vielen Fällen sind die IoT-Geräte mit vorgegebenen Sicherheitseinstellungen konfigriert, die sich leicht durch bekannte Anmeldedaten oder leistungsstarke Botnets kompromittieren lassen.

Im Jahr 2018 hat SonicWall **32,7 Millionen IoT-Attacken** aufgezeichnet, das ist ein Anstieg von 217,5 % im Vergleich zu den von SonicWall 2017 verzeichneten 10,3 Millionen IoT-Attacken.



VERSCHLÜSSELTE ATTACKEN IM KONSTANTEN WACHSTUM BEGRIFFEN

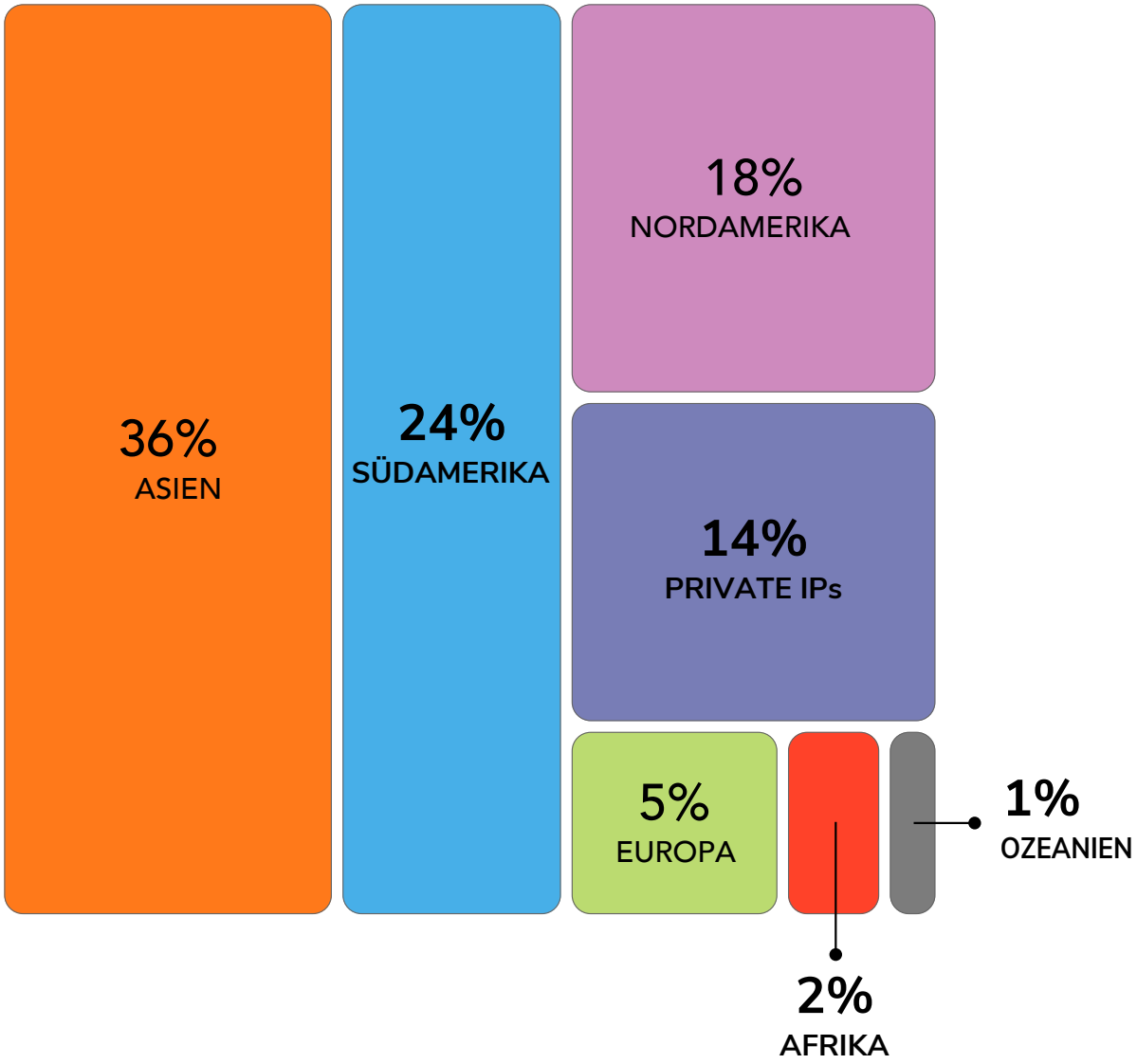
Das konstant wachsende verschlüsselte Verkehrsvolumen geht mit mehr unter der TLS/SSL-Verschlüsselung verhüllten Attacken einher. 2018 wurden mehr als **2,8 Millionen Attacken verschlüsselt**, was einem Anstieg von 27 % gegenüber 2017 entspricht.

DER AUFSTIEG UND FALL VON CRYPTOJACKING

Cryptojacking verschwand 2018 fast genauso schnell wie es aufgetaucht ist. SonicWall verzeichnete weltweit zwischen April und Dezember **57,5 Millionen Cryptojacking-Attacken**. Im September erreichte das Cryptojacking mit 13,1 Millionen aufgezeichneten Attacken seinen Höhepunkt und befindet sich seitdem in einem konstanten Fall.

Laut den Daten von SonicWall wurden 2018 in Europa nur 5 % aller weltweiten Cryptojacking-Attacken verzeichnet. Trotz fallender Preise sind Cryptowährungen aufgrund der damit verbundenen Anonymität weiterhin eine wertvolle Ware für Cyberkriminelle.

CRYPTOJACKING 2018 NACH REGION



PHISHING-VOLUMEN SINKT WELTWEIT, ATTACKEN SIND GEZIELTER

26 MILLIONEN **PHISHING-ATTACKEN** WELTWEIT

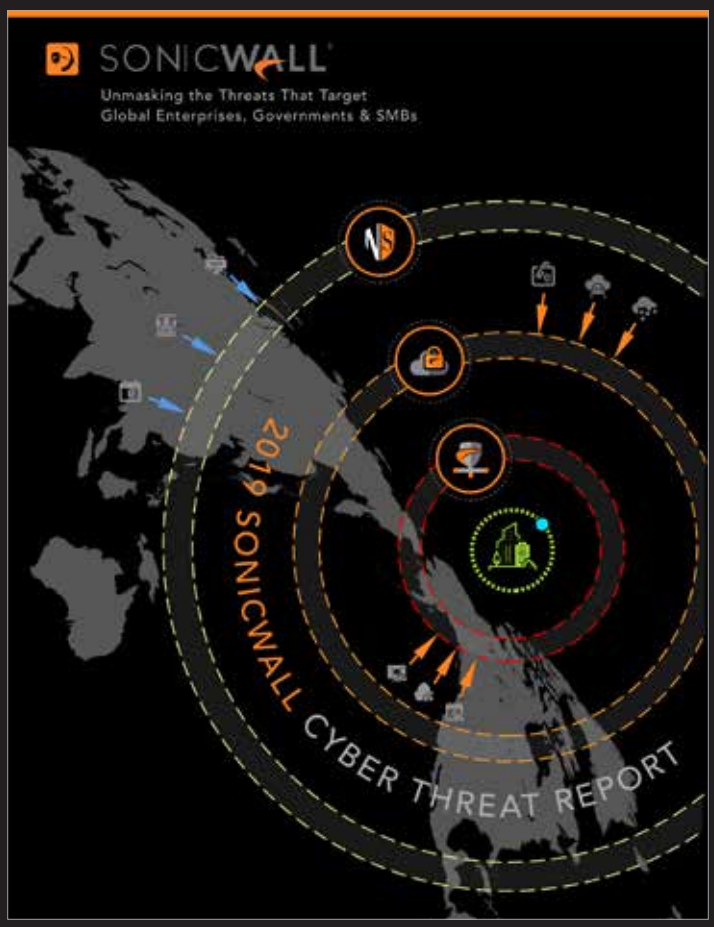
Da Unternehmen weitaus versierter im Blockieren von E-Mail-Attacken sind und ihre Mitarbeiter geschult haben, verdächtige E-Mails zu erkennen und zu löschen, wenden sich Angreifer neuen Taktiken zu. Somit hat sich das Gesamtvolumen dieser Attacken reduziert, doch die Phishing-Attacken sind heute weitaus gezielter (z. B. Kompromittierung der Unternehmens-E-Mail, Konten-Übernahme, Whaling usw.).

2018 verzeichnete SonicWall **weltweit 26 Millionen Phishing-Attacken**, das entspricht einer Reduzierung von 4,1 % gegenüber 2017. SonicWall-Kunden waren 2018 im Durchschnitt 5.488 Phishing-Attacken ausgesetzt.

SONICWALL®

Exklusive Cyber Threat-Informationen und Analysen von SonicWall Capture Labs.

ERFAHREN SIE MEHR



Besuchen Sie SonicWall.com/ThreatReport und laden Sie sich den kompletten Sonic Wall Cyber Threat Report 2019 herunter. Der Bericht liefert neue Einblicke in die Strategien von Cyberkriminellen und erklärt, wie Sie Ihre Organisation bzw. Ihr Unternehmen auch vor den ausgefeiltesten Cyberattacken schützen können.

* Im Rahmen seiner Best-Practice-Vorgaben optimiert SonicWall auf regelmäßiger Basis seine für Erfassung, Analyse und Reporting eingesetzte Methodik. Dazu gehören u. a. Verbesserung 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.

SONICWALL