SONICWALL®

2024

SONICWALL CYBER THREAT REPORT

WIE SIE SICH VOR DEM UNAUFHALTSAMEN ANSTIEG VON CYBERANGRIFFEN SCHÜTZEN KÖNNEN

sonicwall.de | @sonicwall

EINLEITUNG

ANMERKUNG VON UNSEREM CEO

Vor fast 18 Monaten haben wir bei ganz SonicWall unseren Outside-In-Ansatz eingeführt, mit dem Ziel, die Anforderungen und Probleme unserer Partner und Kunden genau zu verstehen und daraus Rückschlüsse zu ziehen, um die Bereitstellung unserer Produkte und Services zu verbessern.

2023 war ein bedeutendes Jahr, in dem dieser Ansatz begann, Früchte zu tragen. Wir haben Solutions Granted übernommen, einen führenden Managed Security Services Provider (MSSP), der mehr als tausend Managed Service Provider (MSPs) in ganz Nordamerika betreut. Des Weiteren haben wir unsere Cloud-Sicherheitsplattform für moderne, dezentrale Belegschaften durch die Übernahme von Banyan Security ausgebaut und das wachsende Portfolio von SonicWall so um SSE-Lösungen, einschließlich Zero-Trust-Network-Access (ZTNA), erweitert.

Dank dieser strategischen Entscheidungen können unsere MSP-Partner ihre Kunden rund um die Uhr mit einem Team aus Bedrohungsanalysten und Experten schützen, ohne für ein internes SOC aufkommen zu müssen. Außerdem haben wir unser Portfolio weiter in Richtung Cloud entwickelt. Partner und Kunden profitieren von mehr Flexibilität – ein entscheidender Aspekt für die kontinuierliche Entwicklung der Cybersicherheitsplattform von SonicWall.

Für unsere Kunden bedeutet die Erweiterung der SonicWall-Plattform ein größeres Portfolio an verwalteten Sicherheitslösungen, angefangen bei Firewalls bis hin zur Cloud-Sicherheit. Wie der SonicWall 2024 Cyber Threat Report jedoch zeigt, ruhen Bedrohungsakteure nicht. Sie eignen sich immer neue Taktiken an und nutzen jeden aufkommenden Angriffsvektor aus.

Mit einem Anstieg von 6 % bei böswilligen Eindringversuchen, 11 % bei Malware und 659 % bei Cryptojacking steigt die Wahrscheinlichkeit, ins Visier zu geraten, dramatisch an.

In diesem volatilen Umfeld reichen die bisherigen Schutzmechanismen nicht mehr aus: Unabhängig von ihrer Größe benötigen Unternehmen bewährte Lösungen sowie proaktive Strategien auf Grundlage neuester Bedrohungsdaten.

Genau deshalb veröffentlicht SonicWall den SonicWall Cyber Threat Report: um Bedrohungsdaten zu liefern, die nicht nur verwertbare Erkenntnisse enthalten, sondern uns auch dabei helfen, für die Zukunft zu planen und effektive Lösungen für unsere Partner zu entwickeln. Im Namen unseres erstklassigen Partnernetzwerks und des gesamten SonicWall-Teams, einschließlich der Bedrohungsexperten von Capture Labs, freuen wir uns, diesen exklusiven Einblick in die überaus dynamische Cybersicherheitslandschaft zu geben.

Bob VanKirk
President und CEO
SonicWall

Kleine Lücken, große Schäden

Cyberangriffe schlagen Wellen. Berichte über Angriffe auf große, bekannte Unternehmen oder lokale Behörden machen augenscheinlich laufend Schlagzeilen. Bei genauerer Betrachtung zeigt sich ein sehr ähnliches Bild. Die Berichterstattung der Fachpresse über die größten Sicherheitsvorfälle ist von bekannten Namen wie Mailchimp, MGM, Activision und 23andMe geprägt.

Angesichts dieser Meldung liegt die Vermutung nahe, Cybercrime beträfe Großkonzerne weitaus stärker als kleinere Unternehmen. Leider entspricht dies nicht ansatzweise der Wahrheit. Laut einem Blog-Beitrag der CISA aus dem Jahr 2023 **werden kleine Unternehmen dreimal häufiger zum Ziel von Bedrohungsakteuren** als größere Organisationen. Diese Angriffe auf KMU verursachen jährlich mehrere Milliarden Dollar an Verlusten.

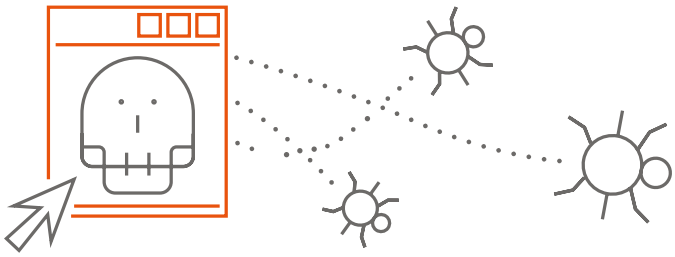
Das ist einer der Gründe für den engagierten Einsatz von SonicWall bei der Ermittlung und Veröffentlichung der neuesten Bedrohungsdaten. Da KMU 80 % unserer Endanwender ausmachen, bieten unsere Daten einen unerreichten Überblick über die Bedrohungslage, in dessen Mittelpunkt nicht große, multinationale Konzerne, sondern Unternehmen wie Ihres stehen.

Die wichtigsten Trends 2023

Der wahrscheinlich deutlichste Trend im Jahr 2023 war die Beschleunigung. Die Bedrohungsforscher von SonicWall Capture Labs verzeichneten nahezu flächendeckend ein ansteigendes Angriffsvolumen. **Malware-Angriffe nahmen im Vergleich zum Vorjahr um 11 % zu, verschlüsselte Bedrohungen um 117 % und Cryptojacking um 659 %.** Dieser Trend zeigte sich auch auf regionaler Ebene, wobei der Anstieg des Angriffsvolumens im Verhältnis 3:1 zum Rückgang stand.

Anstelle des unablässig von außen einwirkenden Kräftespiels der letzten Jahre setzten Bedrohungsakteure 2023 auf altbewährte Methoden. Dabei ließe sich vermuten, dass ein steigendes Malware-Angriffsvolumen und dauerhaft hohe Phishing-Quoten mit großen Mengen neuer Malware einhergehen würden. Es kam jedoch genau anders: Im Vergleich zum Vorjahr wurde sogar 38 % *weniger* wirklich neue Malware erkannt.

Das bedeutet jedoch nicht, dass Bedrohungsakteure ihre Methoden nicht verfeinert haben. SonicWall-Experten beobachteten das Aufkommen von Microsoft OneNote-Dateien als ersten Angriffsvektor sowie massive Kampagnen, die auf Schwachstellen in WinRAR und MOVEit abzielten.



Unseren Daten zufolge sind Schwachstellen nach wie vor der häufigste Angriffsvektor – was sich angesichts ihrer steigenden Zahl auch kaum ändern wird. **Im Jahr 2023 wurden 28.834 CVEs veröffentlicht**. Ein Rekord, der einem Anstieg von 15 % gegenüber 2022 entspricht. Im Dezember haben Bedrohungsforscher von SonicWall **CVE-2023-51467 entdeckt und ordnungsgemäß offengelegt**. Die Schwachstelle betraf ApacheOFBiz. Seitdem wurde eine große Anzahl an Exploit-Attacken beobachtet.

Andere Kampagnen zeigten sich ähnlich innovativ. Neuartige Phishing-Kampagnen lotsten Opfer zu überzeugenden Anmeldeseiten für Microsoft Outlook und American Express oder nutzten QR-Codes, um Dateiscans zu umgehen. Cyberkriminelle nutzten die Inflation und die unsichere wirtschaftliche Lage aus, um betrügerische Darlehens-Apps voller Spyware und Funktionen für den Diebstahl von Anmeldedaten in Umlauf zu bringen. Auch wurden in PDFs eingebettete Google-Skripts zum Diebstahl von Kryptowährung missbraucht. Eine deutliche Mahnung, auch in scheinbar vertrauenswürdigen Umgebungen wachsam zu bleiben.

Von KMU bis Großkonzern, heute und in Zukunft

Die künftige Bedrohungslage wird sich stark von der heutigen Situation unterscheiden. Bedrohungsakteure nutzen ChatGPT und andere generative KI, um Phishing-Versuche zu verfeinern, überaus überzeugende BEC-Angriffe (Business Email Compromise) auszuführen und schnell Schadcode zu erzeugen.

Dennoch birgt KI auch großes Potenzial für die Cybersicherheit. SonicWall setzte als einer der ersten Anbieter auf KI und maschinelles Lernen. Capture ATP und RTDMI erkennen bereits viele dieser Arten von Angriffen. Das wahre Potenzial von KI als Mittel zur Bedrohungsabwehr wird sich jedoch erst in den kommenden Jahren offenbaren.

Höchststand seit 2019

2023 verzeichneten Bedrohungsforscher von SonicWall Capture Labs 6,06 Milliarden Malware-Angriffe – 11 % mehr als im Vorjahr. Dies ist das höchste globale Angriffsvolumen seit 2019, was darauf hindeutet, dass Malware-Aktivitäten wieder das Niveau vor der Pandemie erreicht haben. Dabei werden Bedrohungsakteure immer zahlreicher, einfallsreicher und aktiver.

Der globale Anstieg an Malware ergab sich jedoch aus zwei gegenläufigen Trends. Malware in Asien und Europa verzeichnete einen *Rückgang* um 2 %, der angesichts eines größeren Anstiegs in Nordamerika (+15 %) und LATAM (+30 %) jedoch verblasste.

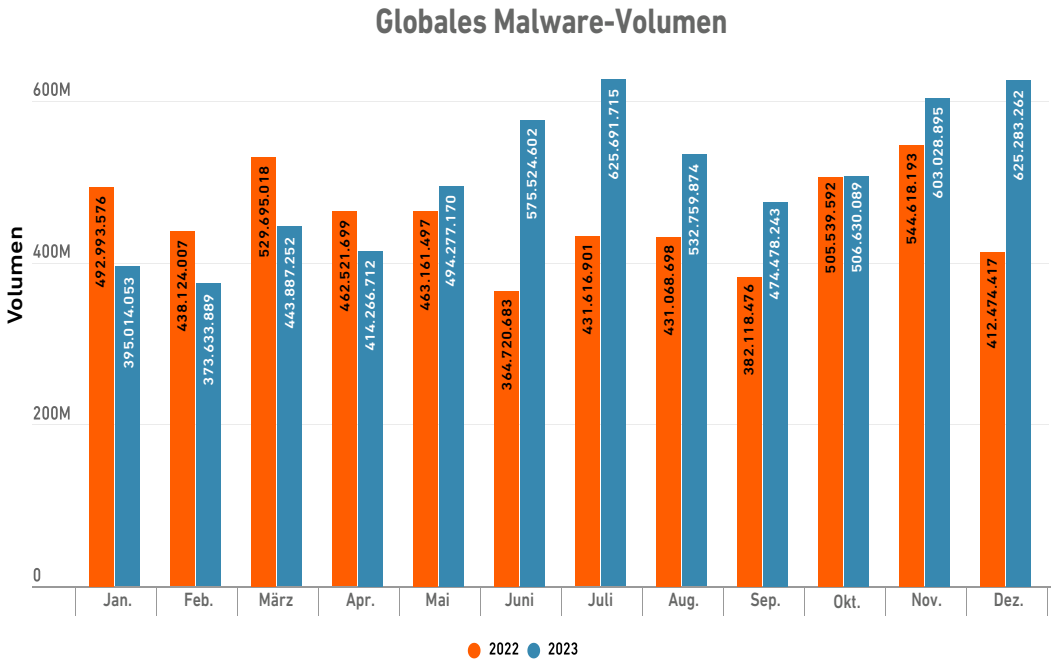
Diese Diskrepanz schlug sich auch in unseren branchenspezifischen Daten nieder. Entfielen 2022 auf den Bildungssektor noch die mit Abstand meisten Malware-Angriffe, gingen diese 2023 um 3 % zurück. Im Gegenzug gerieten Gesundheitswesen und Einzelhandel um 20 % und Behörden um 38 % häufiger ins Visier. Am härtesten traf es jedoch Kunden in der Finanzbranche – hier haben sich Malware-Angriffe *verdoppelt*. Dadurch wurde sie zum am schwersten betroffenen Bereich aller in 2023 untersuchten Branchen. 2021 und 2022 lag sie noch auf dem letzten Platz der Liste bzw. in der Mitte.

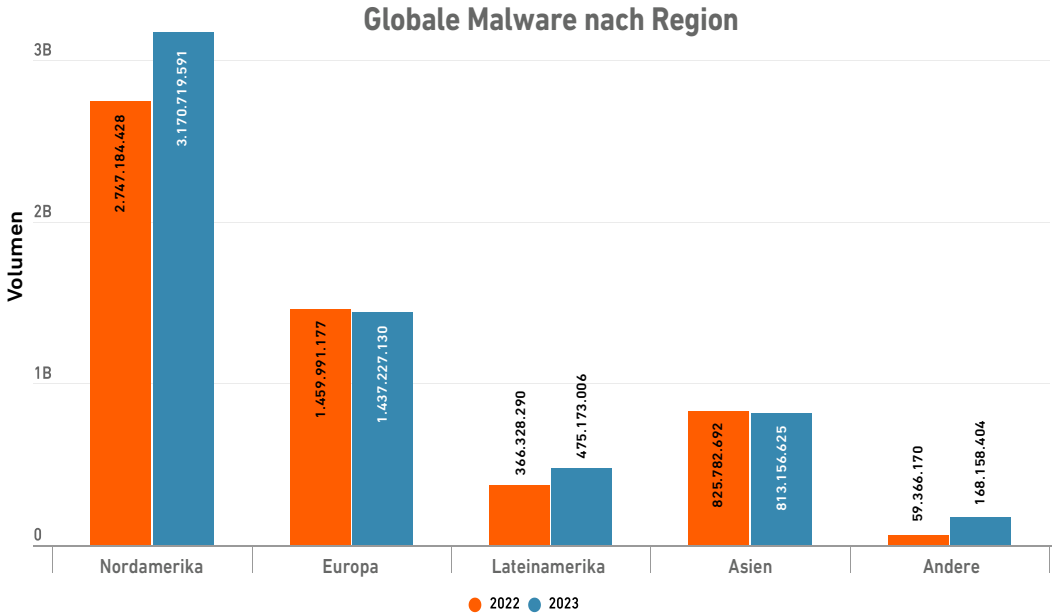
Brennpunkt Notizzettel: Schädliche OneNote-Dateien

Anfang 2023 fiel Forschern von SonicWall auf, dass Bedrohungsakteure einen neuen Einfallsvektor zur Infektion von Systemen nutzten: Microsoft OneNote-Dateien. Diese manipulierten Anhänge wurden per E-Mail versendet und gingen mit diversen Social-Engineering-Techniken einher. Dadurch stiegen die Chancen, dass das Ziel auf eine der im Anhang verborgenen Schaddateien klickte und so die Payload ausführte.

Doch die Sicherheitsanbieter wurden schnell hellhörig und begannen, Erkennungen auf Basis dieser angehängten Payload-Dateien auszulösen. Dann stiegen die Bedrohungsakteure auf URLs um, die auf die Payload verwiesen. Gleichzeitig begannen die Angreifer, ihren Code mit wiederholten Null-Bytes am Ende der OneNote-Dateien aufzublähen, um die Dateigröße auf über 500 MB zu erhöhen und so viele AV-Scans zu umgehen.

Im März ging die Nutzung dieser Dateien jedoch schon drastisch zurück, wahrscheinlich weil Microsoft ein Office-Update veröffentlichte, nachdem sich eingebettete Dateien mit gefährlichen Erweiterungen nicht mehr in OneNote öffnen ließen. Trotz seiner Kurzlebigkeit hatte sich dieser Trend weit genug verbreitet, um manipulierte OneNote-Dateien zu den beliebtesten Office-Schaddateien von ganz 2023 zu machen. So verwendeten unter anderem Qakbot, AsyncRat und AgentTesla OneNote-Anhänge als Einfallspforte.





Manipulierte PDFs auf dem Vormarsch

Manipulierte PDFs gehören seit Langem zum Standardrepertoire von Bedrohungsakteuren. Im Jahr 2023 stieg ihre Verwendung jedoch drastisch an, und zwar von etwa einem Fünftel aller neu erkannten Schaddateitypen auf fast ein Drittel – ein klares Zeichen dafür, dass diese Taktik weiterhin erfolgreich ist.

Dieser Zuwachs beflügelte den Einfallsreichtum und damit die Entwicklung vieler nennenswerter Varianten. SonicWall beobachtete 2023 mehrere Fälle von PDFs, die QR-Codes enthielten. In einem Fall wurde dem Benutzer mit dem Ablauf eines Microsoft-Passworts gedroht, wenn dieser den Code nicht scannte.

Eine weitere PDF enthielt eine schädliche URL, die zur Tarnung per Google Script erstellt wurde. Ebenfalls Teil dieses komplexen Betrugs waren gefälschte Bitcoin-Transaktionsprotokolle und eine gefälschte „Mining-Fortschrittsanzeige“, die Opfer zur Eingabe von Finanzdaten verleitete, um fiktive Zahlungen zu erhalten.

Wie schon in der Vergangenheit haben Bedrohungsakteure auch 2023 mit großem Aufwand versucht, sich als bekannte Marken auszugeben. Darin werden sie immer besser. Unter anderem fanden wir manipulierte PDFs, die als iTunes-Belege, Warnungen über mehrere Anmeldeversuche bei einem Wells Fargo-Konto und sogar als Anmeldeseite der Kollaborationsplattform RingCentral getarnt waren.

Die wichtigsten Taktiken von Bedrohungsakteuren

Portable Executable (PE)-Dateien sind allgegenwärtig

PE-Dateien sind nach wie vor die gängigste finale Payload, da sie sich einfach übertragen, mit allgemeinen Tools nutzen und einfach ausführen lassen. 2023 erkannten wir jedoch einen Anstieg an PE-Malware, die in .NET verfasst war. Mittlerweile wird der Großteil an PE-Malware in .NET verfasst, vermutlich aufgrund seiner Zugänglichkeit und seines großen Funktionsumfangs. Das trifft auch auf berüchtigte Malware-Familien wie RedLine, AgentTesla und AsyncRAT zu.

Glücklicherweise sind PE-Dateien hinreichend als Malware-Träger bekannt und werden folglich gründlich untersucht. Und obwohl einige Malware-Autoren Skriptdateien als Einfallsvektoren für andere Malware verwenden oder Schadcode komplett in JavaScript, VBScript, PowerShell usw. verfassen, sind SonicWall-Kunden geschützt: Die erstklassige Skriptemulation von RTDMI bietet eine ausgezeichnete Erkennung schädlicher Skripte.

WinRAR – leichtes Spiel für Angreifer

Anfang 2023 begannen Bedrohungsakteure, eine neue Schwachstelle in WinRAR, dem beliebten Dateiarchivierungstool von Windows, auszunutzen. In der zweiten Jahreshälfte waren bereits mehrere Stealer-Malware-Familien wie AgentTesla, Remcos, Rhadamanthys und Guloader an diversen Kampagnen beteiligt, bei der CVE-2023-38831 ausgenutzt wurde. Diese Schwachstelle ermöglicht Hackern die Ausführung von beliebigem Code in ZIP-Archiven. Da WinRAR in Unternehmen weitläufig genutzt wird, konnten sich diese Kampagnen schnell weltweit auf die USA, den nahen Osten und Asien ausbreiten. Mittlerweile werden sie mit im Regierungsauftrag handelnden Hackern aus Russland und China in Verbindung gebracht, darunter Sandworm, APT28 und APT 30.

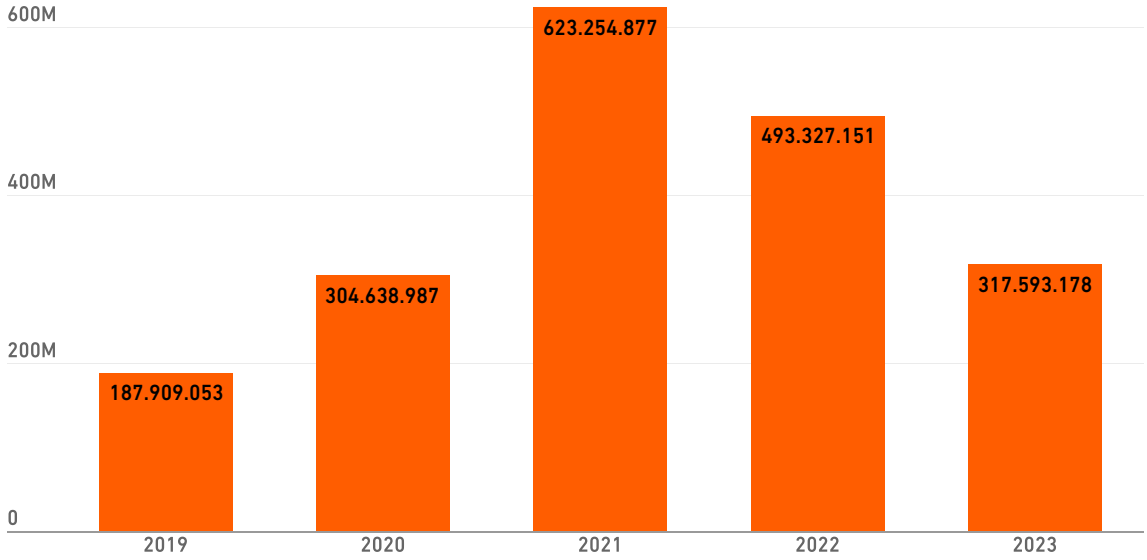
Nach wie vor nicht zu unterschätzen

Die Ransomware-Bedrohungslage entwickelte sich 2023 im Laufe des Jahres weiter. Bedrohungsexperten von SonicWall Capture Labs zeichneten 317,6 Millionen Ransomware-Angriffe auf – 36 % weniger als im Vorjahr, aber die bis dato dritthöchste Gesamtsumme. Dieser Trend zeigte sich in mehreren Regionen: In Nordamerika und Europa gingen Ransomware-Angriffe je um ein Drittel zurück, in LATAM sogar um 52 %.

Eine bemerkenswerte Ausnahme bildete Asien. Das Ransomware-Volumen stieg 2023 dort auf einen neuen Rekord von 17,5 Millionen – also 1.627 % mehr als 2019.

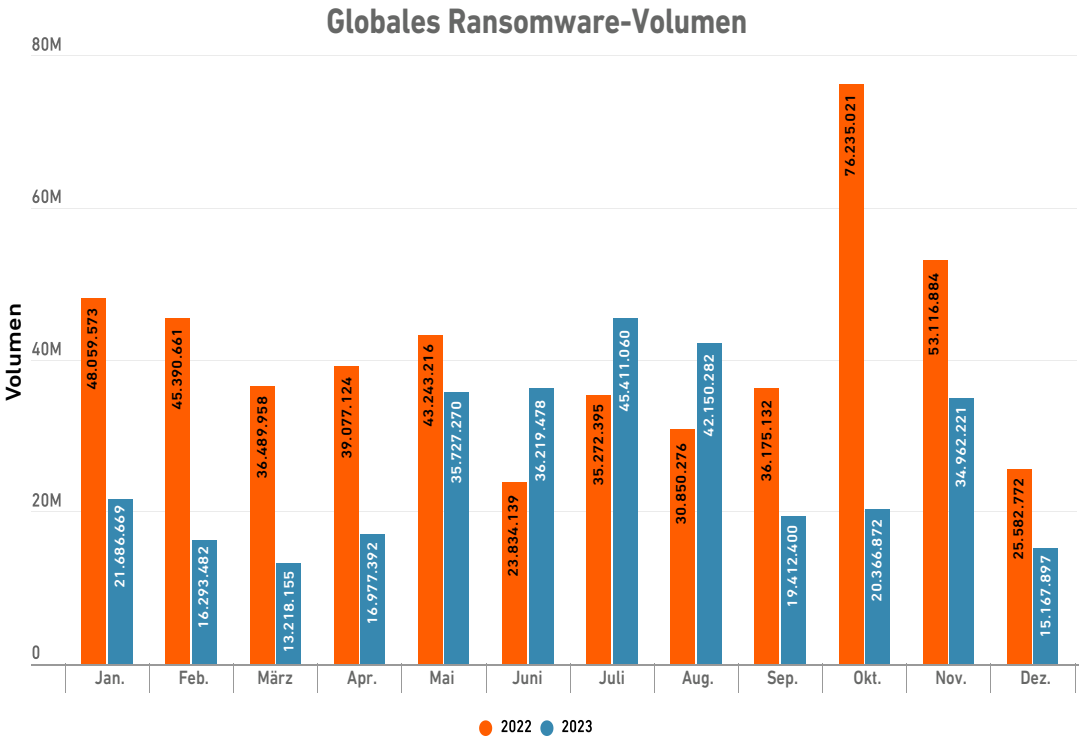
Ausschlaggebend für diesen Anstieg waren vor allem Angriffe auf die Finanzbranche. Im Mai stahl die Ransomware-Gruppe LockBit 15 Millionen Kundendatensätze und 1,5 Terabyte an internen Daten der Bank Syariah Indonesia. Im November griff LockBit auch die Industrial and Commercial Bank of China (ICBC) an, die weltweit größte Bank gemessen an ihren Assets. Außerdem gerieten laut einem IDC-Bericht aus dem September 2023 ungefähr dreiviertel aller indischen Unternehmen im Jahr 2022 ins Visier von Ransomware. Diese Zahl dürfte seitdem weiter gestiegen sein.

Globales Ransomware-Volumen nach Jahr



Die berüchtigtste Ransomware 2023: LockBit

Die Verhaftung zweier Beteiligten konnte LockBit kaum etwas anhaben: Die Gruppe blieb 2023 der führende Ransomware-Angreifer. Dies dürfte an regelmäßigen Innovationen wie Bug-Bounty-Programmen zur Steigerung der „Produktqualität", Marketingmaßnahmen und der regelmäßigen Veröffentlichung aktualisierter Toolkits mit verbesserten Funktionen liegen. Nach dem Leak von LockBit 3.0/„Black" kontaktierte SonicWall die Bedrohungsakteure, die eine enorme Lösegeldforderung stellten (Näheres dazu erfahren Sie hier).



Unverändert wichtig: Die Bedeutung von Ransomware heute

Wie besorgt sollten Sie über Ransomware sein, wenn Sie nicht gerade in einem der zunehmenden Hotspots leben?

In unserer SonicWall Threat Mindset Survey 2023 haben wir Kunden gefragt, welche Arten von Cyberangriffen sie am meisten besorgt. Mit 83 % stand Ransomware einmal mehr an der Spitze, noch vor Phishing, verschlüsselten Bedrohungen, dateiloser Malware, IoT-Angriffen und mehr.

Trotz des Rückgangs an Ransomware-Angriffen bei unseren KMU-Kunden glauben wir, dass die Befragten auf dem richtigen Kurs sind.

Hierzu ein paar Daten zur Entwicklung der letzten Jahre. Ein Rückgang von 36 % klingt zunächst dramatisch – bis man den Zuwachs zwischen 2020 und 2022 bedenkt. Selbst nach diesem Rückgang war 2023 das Jahr mit den drittmeisten Ransomware-Angriffe bis dato. **Und mit 27 % mehr Ransomware-Angriffen in der zweiten Jahreshälfte 2023 als in der ersten Jahreshälfte geht der Trend in die falsche Richtung, um die gravierenden Anstiege der Jahre 2021 und 2022 auszugleichen**.

Bei Ransomware und anderen Bedrohungen können Cybersicherheitsanbieter wie SonicWall nur messen, was in ihrem eigenen Ökosystem geschieht. Zwar verzeichneten SonicWall (mit seinem großen Partnernetz und MSP-Kundenstamm) im Laufe von 2023 einen Rückgang an Ransomware. Andere Anbieter stellten im gleichen Zeitraum jedoch einen Anstieg fest. Da eine verstärkte Strafverfolgung jeden Angriff risikoreicher macht und KMU nicht mehr als „leichte Beute“ für ungezielte, flächendeckende Angriffe gelten, scheinen Bedrohungsakteure auf weniger zahlreiche und dafür deutlich differenziertere Angriffe mit potenziell größerer Ausbeute umzuschwenken.

Das bedeutet jedoch nicht, dass es überhaupt keine leichte Beute mehr gibt. Unternehmen migrieren Daten und Workflows vermehrt in die Cloud, achten dabei jedoch oft weniger auf Sicherheit als in ihren lokalen Umgebungen. Da Ransomware-Angriffe auf SaaS immer ausgefeilter werden, kann ein Mangel an Sicherheit in der Cloud katastrophale Folgen nach sich ziehen.

Außerdem laufen nach wie vor zahlreiche groß angelegte Ransomware-Kampagnen. Ende Mai beobachtete SonicWall einen SQL-Injection-Angriff auf eine als kritisch eingestufte Zero-Day-Schwachstelle in MOVEit Transfer. Die große Beliebtheit und damit weite Verbreitung dieses Tools zur Dateiübertragung in Unternehmen machte es zum Ziel der Ransomware-Bande Cl0p. Sie nutzte CVE-2023-34362 zur Durchführung einer Supply-Chain-Attacke, von der ca. 2.000 Finanz-, Versicherungs- und Gesundheitsdienstleister, Bildungseinrichtungen sowie Behörden betroffen waren. Dabei wurden die Daten von über 62 Millionen Bürgern gestohlen.

Hierzu ist festzuhalten, dass Schwachstellen wie diese der häufigste Ransomware-Vektor waren, den SonicWall 2023 beobachten konnte – und diese Kampagnen trugen dazu bei, dass Ransomware-Zahlungen 2023 erstmals die Marke von 1 Milliarde USD sprengten.

EINDRINGVERSUCHE

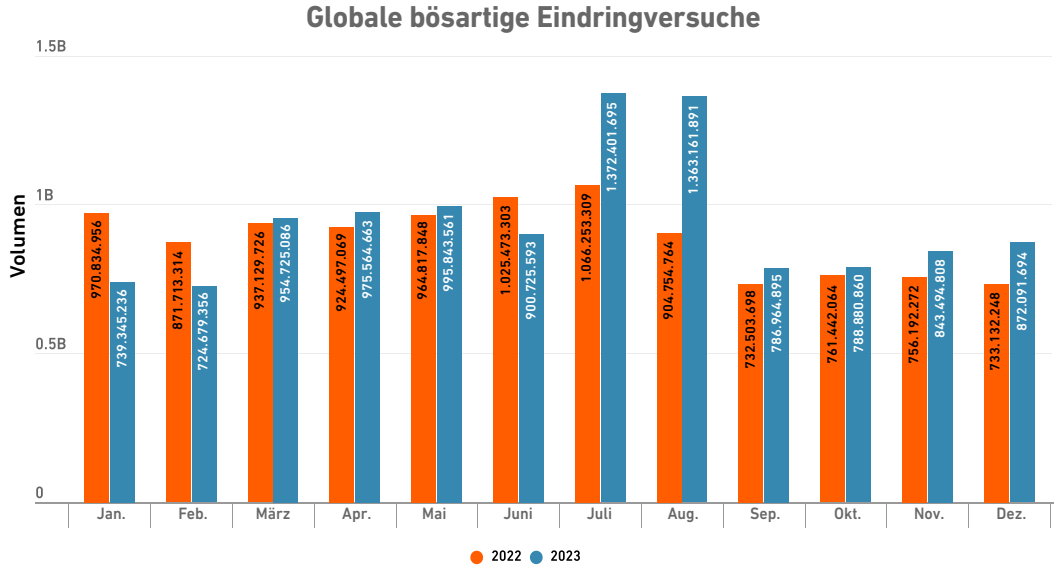
Um 20 % gestiegen

Die Gesamtzahl der Eindringversuche stieg 2023 weiter auf 7,6 Milliarden an, 20 % mehr als 2022 insgesamt. Seit dem Beginn dieser Aufzeichnungen durch SonicWall im Jahr 2013 ist die Zahl der Eindringversuche jedes Jahr gestiegen. Für das letzte Jahrzehnt ergibt sich damit ein Anstieg von 613 %.

Ein Teil dieses Anstiegs ist auf Vorfälle mit niedrigem Schweregrad im Zusammenhang mit Pings und anderen meist harmlosen Aktionen zurückzuführen. Allerdings kam es auch vermehrt zu Treffern mit mittlerem bis hohem Schweregrad – sogenannten „böswilligen Eindringversuchen". Die Zahl dieser Eindringversuche wuchs 2023 auf 11,3 Milliarden an, 6 % mehr als im Vorjahr.

Das Volumen böswilliger Eindringversuche stieg zudem in jeder der von uns analysierten Branchen. Für den Anstieg der Vorfälle mit mittlerem bis hohem Schweregrad ergab sich folgendes Bild: 19 % im Bildungswesen, 34 % im Einzelhandel, 36 % im Gesundheitswesen, 46 % bei Behörden und 47 % im Finanzwesen.

Diese Versuche lösen Alarme aus, die von SOC-Analysten oder MSPs mit SOC-Analysten überprüft werden müssen, was zu Alert-Fatigue beiträgt und wertvolle Zeit von anderen wichtigen Initiativen abzieht. Hat ein Eindringversuch Erfolg, können Bedrohungsakteure unter anderem nach Belieben Daten stehlen, Schadcode ausführen, Systeme verschlüsseln und den Betrieb so zum Erliegen bringen. Die Kosten zur Behebung sowie Compliance-Strafzahlungen können in die Tausende oder gar Millionen gehen.



Was ist ein Eindringversuch?

Ein böswilliger Eindringversuch ist ein Sicherheitsvorfall, bei dem Bedrohungsakteure versuchen, sich unter Ausnutzung einer Schwachstelle unbefugten Zugriff auf Systeme oder Ressourcen zu verschaffen. Während in den Schlagzeilen meist von der Ausnutzung unveröffentlichter „Zero-Day"-Schwachstellen zu lesen ist, sind die am häufigsten ausgenutzten Schwachstellen in der Regel bekannt und als CVEs veröffentlicht. Da Patches jedoch nicht überall zeitgleich aufgespielt werden, haben Angreifer die Möglichkeit, ungepatchte Software oder Appliances als Einfallstor in ein Netzwerk zu missbrauchen.

Einmal eingedrungen nutzen Angreifer Schwachstellen weiter aus, um sich dauerhaft im Netzwerk festzusetzen und frei bewegen zu können, indem sie sich weitere Schwachstellen in ungepatchten Systemen innerhalb des Netzwerks zunutze machen.

SonicWall trackt die Erkennung und Prävention von Exploits aus externen und internen Quellen. Ein Eindringversuch wird gezählt, wenn ein als Schwachstelle geltender Codeabschnitt eine Firewall mit aktivierter Intrusion Prevention passiert und von dieser erkannt sowie neutralisiert wird.

VERSCHLÜSSELTE BEDROHUNGEN

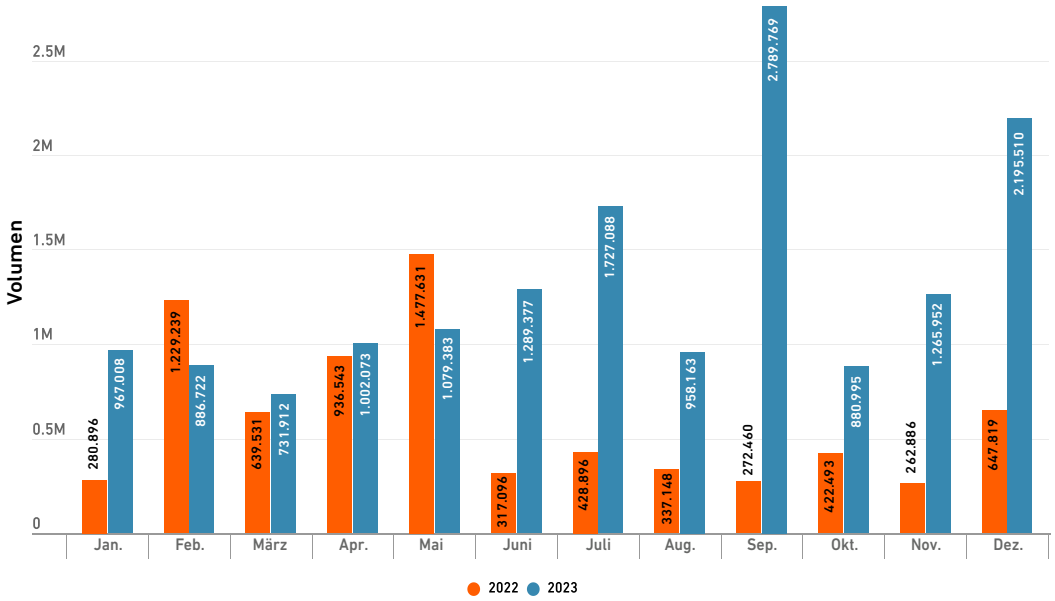
Mehr als doppelt so viele verschlüsselte Angriffe

2023 registrierten Bedrohungsforscher von SonicWall Capture Labs 15,7 Millionen verschlüsselte Angriffe weltweit. Das ist der Höchststand seit Beginn unserer Aufzeichnungen und stellt im Vergleich zum Vorjahr einen Anstieg um 117 % dar.

Während sich in Nordamerika der Anstieg noch auf 30 % belief, verzeichneten wir dreistellige Zahlen in Europa, Asien und LATAM mit je 182 %, 462 % und 527 % mehr verschlüsselten Angriffen.

In einigen der von uns analysierten Branchen kam es sogar zu noch dramatischeren Ausschlägen, alle davon im dreistelligen Bereich. In der Finanzbranche verlief der Anstieg am glimpflichsten: Die Zahl der Angriffe hat sich „nur" verdoppelt. Einen noch drastischeren Anstieg an verschlüsselten Bedrohungen verzeichneten 2023 jedoch das Gesundheitswesen (252 %), Bildungseinrichtungen (429 %), Behörden (629 %) und der Einzelhandel (680 %).

Globales Volumen verschlüsselter Angriffe



Was sind verschlüsselte Bedrohungen?

Die meisten Branchenanalysten schlussfolgern, dass mittlerweile 80–90 % des Netzwerkverkehrs verschlüsselt sind und es erforderlich machen, verschlüsselten Datenverkehr zu scannen. Zwar bietet das Verschlüsselungsprotokoll TLS (Transport Layer Security) zusätzliche Sicherheit für Web-Sitzungen und Internetkommunikation. Es wird aber von Angreifern vermehrt missbraucht, um Malware, Ransomware, Zero-Day-Angriffe und mehr zu verschleiern.

Ältere Firewalls und andere herkömmliche Sicherheitskontrollen haben nicht die nötigen Funktionen oder zu wenig Rechenleistung, per HTTPs-Verkehr gesendete Bedrohungen zu erkennen, zu untersuchen und zu neutralisieren. Bedrohungsakteuren bietet sich so ein äußerst lukrativer Angriffsvektor.

SONICWALL

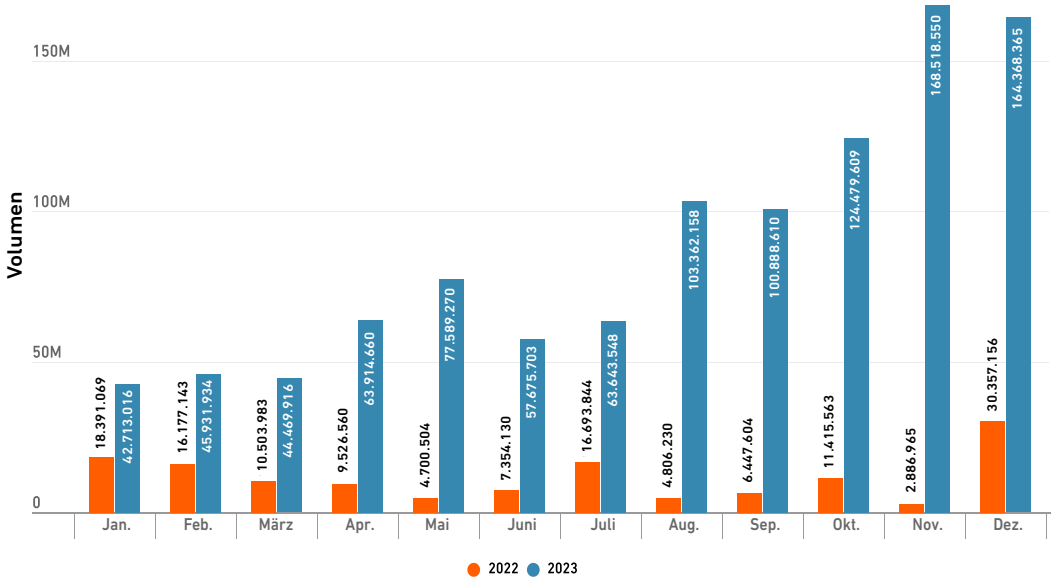
Gefahren (und Gründe für den Anstieg)

Im letztjährigen Threat Report wurde ein besorgniserregender Meilenstein erreicht: Die Anzahl der Cryptojacking-Vorfälle, die seit Beginn der Aufzeichnungen 2018 relativ gering geblieben war, überschritt zum ersten Mal 100.000.

Dies sollte jedoch nur der Anfang des Aufschwungs von Cryptojacking sein. Anfang April 2023 übertraf die Zahl der Cryptojacking-Vorfälle bereits die Gesamtsumme des Jahres 2022 und nahm von da an weiter zu. Bis zum Jahresende hatten Bedrohungsforscher von SonicWall Capture Labs *1,06 Milliarden* Cryptojacking-Vorfälle registriert – 659 % mehr als 2022. Grund für diese Gesamtsumme war ein nie dagewesenes Angriffsvolumen im November und Dezember. Dabei kam es in beiden Monaten jeweils zu mehr Cryptojacking-Treffern als im gesamten Jahr 2022.

Auch in jeder Region zeigte sich ein starker Zuwachs. In APAC und LATAM stiegen Cryptojacking-Treffer um 87 % bzw. 116 % an. Zu einem massiven Anstieg kam es in NOAM (+596 %) und Europa (+1.046 %).

Globales Cryptojacking-Volumen



Was ist Cryptojacking?

Cryptojacking ist ein Cyberangriff, bei dem Bedrohungsakteure die Rechenressourcen ihrer Opfer kapern, um ohne deren Zustimmung und Wissen Kryptowährungen zu minen. Dazu installieren sie Malware, die oft über Phishing-E-Mails oder kompromittierte Websites versendet wird und unerkannt im Hintergrund auf den Rechnern, Smartphones oder Servern der Opfer läuft. Diese Malware nutzt die Rechenleistung und Energiezufuhr der gekaperten Geräte, um komplexe mathematische Probleme zu lösen („Proof of Work“) und so Kryptowährung für den Angreifer zu generieren.

Der aktuelle Cryptojacking-Trend

Auch 2023 war bei den meisten Cryptojacking-Angriffen XMRig involviert. Bei dieser Open-Source-Software handelt es sich um ein legitimes Tool, das über das Internet frei verfügbar ist. Durch seine hohe Benutzerfreundlichkeit wird es jedoch auch oft missbraucht. Es ist selbst für unerfahrene Bedrohungsakteure zugänglich, bietet jedoch auch fortgeschrittenen Benutzern Möglichkeiten zur Abänderung von Code, um sich der Erkennung zu entziehen und Profit zu erzeugen.

XMRig wird oft als Trojaner missbraucht oder in anderen Software- oder Adware-Bundles versteckt. Es wird unter anderem über Phishing, Malvertising, Schwachstellen, schädliche Dropper und gecrackte Software verbreitet. Das Tool ist effizient und eignet sich zum Minen der Kryptowährung Monero (auch bekannt als XMR und aufgrund ihrer Anonymitätsmerkmale bei Cyberkriminellen äußerst beliebt) mit relativ hoher Geschwindigkeit, ohne übermäßig viele Systemressourcen zu belegen. Dennoch beansprucht es beim Minen im Hintergrund *konstant* viel CPU-Leistung.

Das ist letztendlich kostspielig, sowohl hinsichtlich der Produktivität, da Cryptojacking Aktivitäten abseits des Minings deutlich verlangsamen kann, als auch konkret im finanziellen Sinn: Opfer müssen nicht nur für den erhöhten Stromverbrauch aufkommen, sondern auch Geräte ersetzen, die überhitzen oder deren Lebensdauer aufgrund der hohen Auslastung sinkt.

Auch die Umwelt leidet darunter: Alleine von 2020–2021 verursachte Bitcoin-Mining denselben CO^2-Ausstoß wie 190 Gaskraftwerke oder die Verbrennung von ca. 38,1 Millionen Tonnen Kohle. Der gesamte Stromverbrauch dieser Mining-Vorgänge übersteigt den Stromverbrauch vieler Industrienationen.

Crypto-Mining wird als eine der umweltschädlichsten Branchen eingestuft. Laut einer Studie in Scientific Reports verursachte von 2016 bis 2021 jeder US-Dollar an gemintem Bitcoin 35 Cent an Klimaschäden.

Trotz der hohen Kosten ist Cryptomining nicht illegal und Cryptojacking wird nur selten strafrechtlich verfolgt. Dies könnte sich jedoch ändern. 2024 gab es bereits eine aufsehenerregende Verhaftung im Zusammenhang mit Cryptojacking: Europol, ukrainische Strafverfolgungsbehörden und ein Cloud-Provider konnten zusammen einen Verdächtigen stellen, der durch illegales Mining mehr als 2 Millionen USD an Kryptowährung erlangt haben soll.

Laut Daten von SonicWall machte Cryptojacking ein Sechstel aller Malware-Vorfälle im Jahr 2023 aus. Angesichts der zunehmenden Beliebtheit von unerlaubtem Mining ist es möglich, dass es zu denselben gemeinsamen Reaktionen des öffentlichen und privaten Sektors kommt, die auf den Ransomware-Boom in den frühen 2020ern folgten.

RTDMI erkennt mehr als 1,5 Millionen Bedrohungen

Trotz des Anstiegs bei den meisten Bedrohungsarten verzeichnete SonicWall Capture Advanced Threat Protection (ATP) mit Real-Time Deep Memory Inspection (RTDMI) im Jahr 2023 deutlich weniger neue Malware-Varianten: 387.000, 38 % mehr als im Vorjahr.

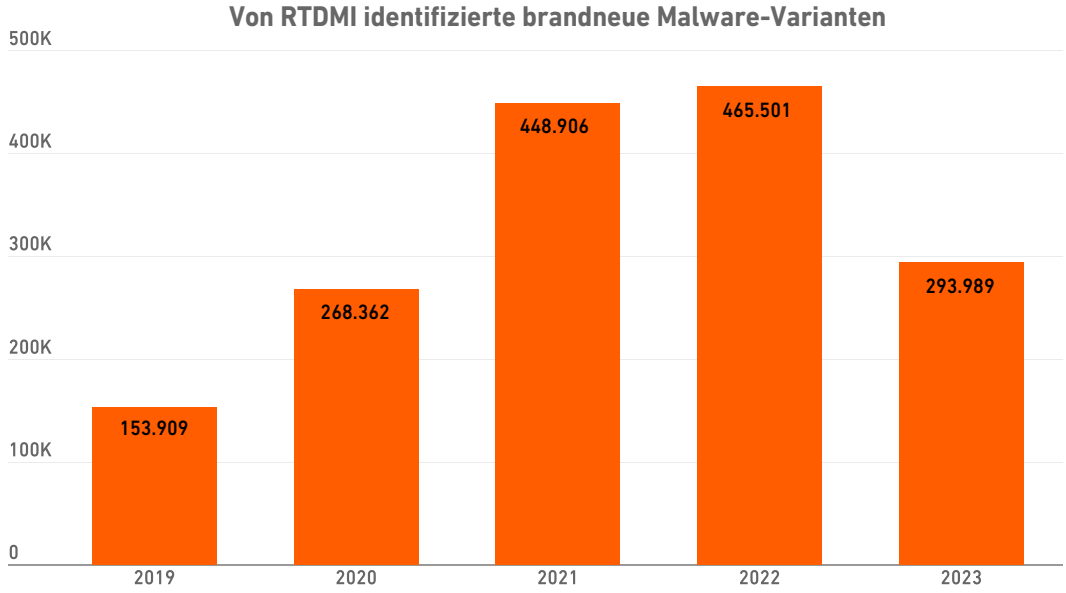
Zusammen mit der Zunahme von Malware und dem anhaltend hohen Phishing-Niveau gewährt dies Aufschluss über die Bedrohungslage 2023: Bedrohungsakteure lassen nicht locker, aber im Augenblick suchen sie nach funktionierenden Varianten, die sie wiederholt nutzen können. Vor allem im Dezember gab es deutlich weniger neue Varianten als üblich – sie erreichten den Tiefststand seit August 2020.

Natürlich werden immer noch viele neue Malware-Varianten erstellt – allein die mehr als 800 brandneuen Varianten, mit denen Kunden 2023 im Durchschnitt zu kämpfen hatten, reichten aus, um die Zahl der insgesamt registrierten Varianten über die 1,5-Millionen-Marke zu puschen. Aber der Fortschritt an Innovationen scheint verlangsamt, zumindest für den Augenblick.

RTDMI verbessert Sicherheit von Anmeldedaten

Während sich die Bedrohungsakteure im Jahr 2023 auf Altbewährtes verließen, hat SonicWall im gleichen Zeitraum seine Tools und Produkte optimiert. Wir haben RTDMI um ein neues Engine-Modul erweitert, um die Erkennung von Anmeldedaten-Diebstahl über HTML deutlich zu verbessern.

HTML-Phishing-Betrug ist eine der gängigsten Methoden zum Diebstahl von Anmeldedaten, wobei die Seiten oft durch iframe-Umleitung, JavaScript, dynamisches Laden und andere Methoden stark verschleiert werden, um keinen Verdacht zu erregen. Das neue Modul ermöglicht die Erkennung dieser stark verschleierten Dateien. Es rendert HTML-Inhalte sicher in einer Sandbox-Umgebung und entschleiert den endgültigen Zustand, in dem die böswilligen Aktivitäten oder Absichten eindeutig beobachtet werden können, ohne das Netzwerk zu gefährden.



„Zero-Day-“ vs. „brandneue“ Angriffe

„Zero-Day-Angriffe“ gehören zu den bekanntesten Begriffen in der Cybersicherheit, weil sie mit berüchtigten Sicherheitsvorfällen in Verbindung stehen. Dabei handelt es sich um völlig neue und unbekannte Bedrohungen, die auf Zero-Day-Schwachstellen abzielen, für die der Zielanbieter bzw. das Zielunternehmen noch keinen Schutz bereitgestellt hat (z. B. Patches oder Updates).

Umgekehrt verfolgt SonicWall die Erkennung und Abwehr von „brandneuen Angriffen“, also Aktivitäten, die von SonicWall Capture ATP zum ersten Mal als bösartig eingestuft werden. Diese decken sich oft stark mit den Mustern von Zero-Day-Angriffen, da SonicWall ein großes Volumen an Angriffen analysiert.

WIE SIE SICH SCHÜTZEN

Die in diesem Bericht beschriebene Zunahme an Bedrohungen zeigt, dass Sie unweigerlich im Visier stehen. Sie können jedoch Maßnahmen ergreifen, um Ihre Cybersicherheit im Allgemeinen zu stärken:

1. **Multifaktor-Authentifizierung (MFA) aktivieren**
   MFA erhöht die Sicherheit bei der Authentifizierung – selbst wenn sich Angreifer Zugang zu Ihren Passwörtern verschaffen, erhalten sie keinen Zugriff auf Ihre Konten, da eine zweite Authentifizierung vom Benutzer, also Ihnen, gefordert wird.
2. **Schnell patchen**
   Zero-Day-Schwachstellen gehen durch die Presse, aber die meisten Exploits zielen auf monate- oder jahrealte Schwachstellen ab.
3. **Regelmäßig Sicherheitsanalysen durchführen**
   So können Sie Schwachstellen erkennen, Risiken bewerten, Ihre Abwehr proaktiv stärken und sich so zuverlässig vor immer neuen Bedrohungen schützen.
4. **Laufend Sicherheitsschulungen abhalten**
   Mit der Technologie schreitet auch die Cybersicherheit voran. Grundlegende Schulungen und Routineverfahren – wie etwa das Vermeiden bösartiger Links und die Erkennung sowie Meldung potenzieller Sicherheitsrisiken – führen zu einer aufgeklärteren und wachsameren Belegschaft.
5. **Verschlüsselten Datenverkehr scannen**
   Schätzungen von Experten zufolge sind 80 bis 90 % des gesamten Netzwerkverkehrs heute verschlüsselt. Doch viele ältere Firewalls haben weder die nötigen Funktionen noch die Rechenleistung, um Cyberangriffe, die über den HTTPS-Datenverkehr übertragen werden, *überhaupt* – geschweige denn mittels TLS 1.3 – zu erkennen, zu prüfen und abzuwehren. Daher lässt sich Malware per Verschlüsselung einfach implementieren und ausführen. Laut SonicWall stieg die Zahl der über HTTPS übertragenen Malware von 2022 bis 2023 um ganze 117 %. Insgesamt registrierte SonicWall im Jahr 2023 15,8 Millionen verschlüsselte Angriffe – fast genauso viele wie 2021 und 2022 zusammengerechnet. Der Zuwachs an verschlüsseltem Datenverkehr und verschlüsselten Bedrohungen unterstreicht die Notwendigkeit von umfassenden Scans.
6. **Sicherheit auf die Cloud ausweiten**
   Je mehr Unternehmen ihre Daten und Workflows in die Cloud verlagern, desto bessere und flexiblere Ansätze mit Security Service Edge (SSE) und Zero-Trust-Netzwerk-Architektur (ZTNA) braucht es, um hybride Arbeitsumgebungen zu schützen.

Für aktuelle Bedrohungsdaten und Neuigkeiten aus der Branche folgen Sie dem SonicWall-Blog.

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, Kalifornien 95035, USA

www.sonicwall.com

Über SonicWall

Mit über 30 Jahren Erfahrung stellt der Cybersecurity-Pionier SonicWall seine Partner in den Mittelpunkt. Als führender Sicherheitsanbieter kann SonicWall schnell und kostengünstig maßgeschneiderte Sicherheitslösungen für jedes Unternehmen weltweit in Echtzeit bereitstellen, skalieren und verwalten – egal ob in der Cloud oder in hybriden und herkömmlichen Umgebungen. Basierend auf den Daten seines eigenen Threat-Research-Centers bietet SonicWall nahtlosen Schutz vor den ausgefeiltesten Cyberangriffen und versorgt Partner, Kunden und die Cybersicherheits-Community mit aussagekräftigen Bedrohungsdaten.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA

SONICWALL

Als Best Practice optimiert SonicWall regelmäßig seine Methoden zur Datenerfassung, Analyse und Berichterstattung. Dazu gehören Verbesserungen der Datenbereinigung, Änderungen an Datenquellen und die Konsolidierung von Bedrohungsfeeds. In früheren Berichten veröffentlichte Zahlen wurden möglicherweise für verschiedene Zeiträume, Regionen oder Branchen angepasst.