SONICWALL

IHRE DATEN IN DEN HÄNDEN VON ERPRESSERN

Warum Ransomware die bevorzugte Exploit-Methode für Cyberkriminelle ist

STOPPEN SIE RANSOMWARE EIN FÜR ALLE MAL

Cyberkriminelle und Hacker waren schon immer gut darin, in Netzwerke einzudringen und Daten zu stehlen. Oft war es allerdings ziemlich schwierig und zeitaufwendig, diese Daten gewinnbringend zu nutzen.

Bis die Ära der Ransomware begann: Mit diesem Erpressungstrojaner ist es nämlich nicht mehr nötig, Daten herauszuschleusen und über dunkle Kanäle weiterzuverkaufen.

Heute ist es einfacher, ein Netzwerk zu hacken, die Daten zu verschlüsseln und zu sperren, bis der Besitzer ein Lösegeld bezahlt. Ohne eine proaktive Echtzeit-Cybersicherheitsstrategie haben Organisationen schlechte Karten.

Lesen Sie diesen Leitfaden, um ein besseres Verständnis von Ransomware zu gewinnen. Erfahren Sie auch, wie Cloud-basiertes Sandboxing Hacker stoppen kann, bevor sie in Ihre Systeme eindringen, Ihre Daten sperren und Ihr Unternehmen erpressen.

Überblick

SONICWALL®

Ransomware: Sind Sie vor dem nächsten Ausbruch geschützt?

Besteht das Risiko, dass auch Sie einer Ransomware-Attacke zum Opfer fallen? Können Angreifer Ihre Daten verschlüsseln und sperren, bis Sie ein Lösegeld bezahlen?

Egal wie groß oder klein ein Unternehmen ist, aus welcher Branche es stammt oder in welcher Weltregion es tätig ist: Ransomware-Angriffe können heute jede Organisation treffen. In den Medien erfährt man meistens von Angriffen auf große Institutionen, wie zum Beispiel auf das Hollywood Hospital, das 2016 über eine Woche offline war, nachdem Cyberkriminelle Dateien mithilfe von Ransomware verschlüsselten und ein Lösegeld für die Entschlüsselung forderten.

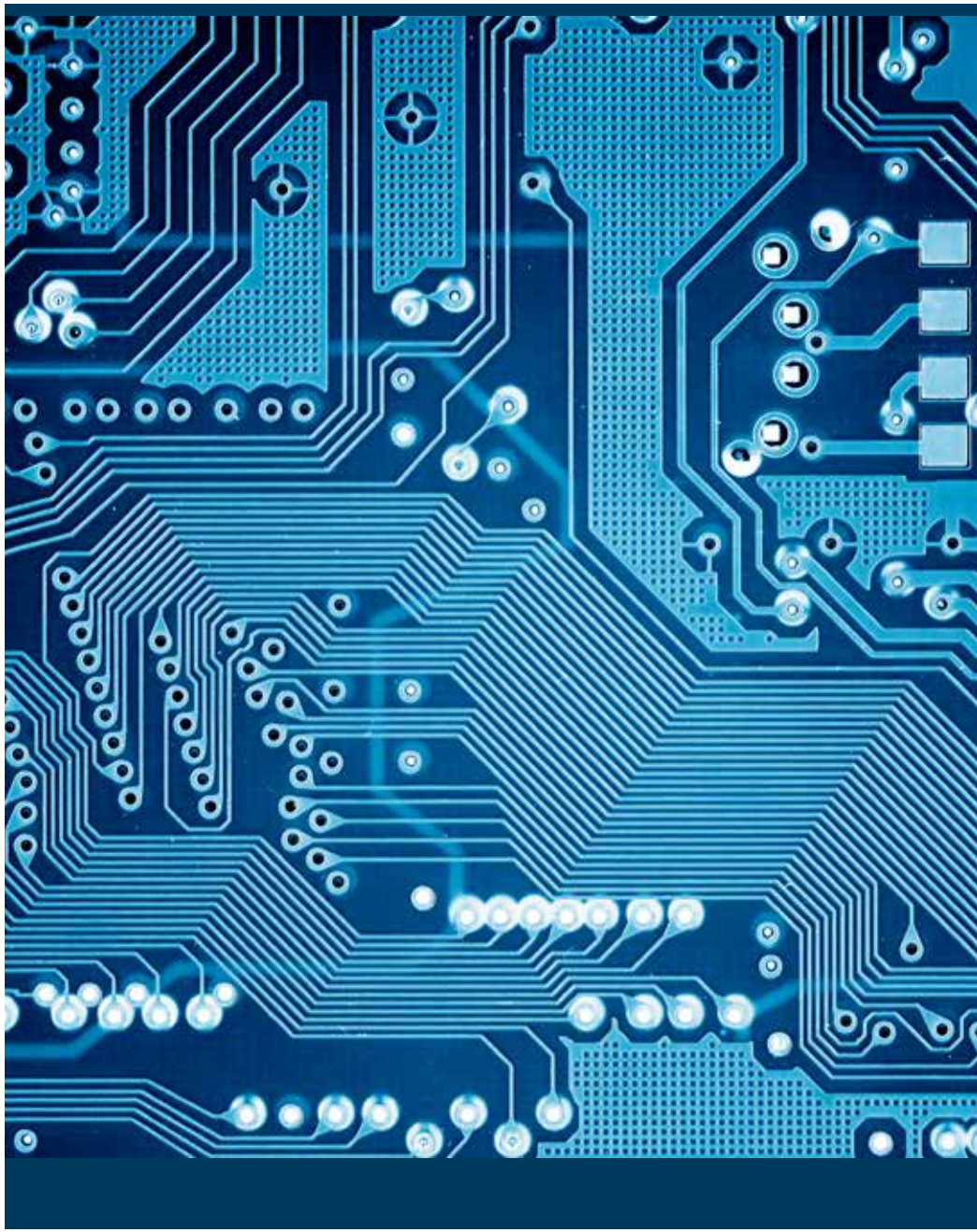
Doch auch kleine Unternehmen haben mit dieser Art von Bedrohung zu kämpfen. Laut einer Untersuchung von Kaspersky sind kleine und mittlere Unternehmen sogar am schlimmsten betroffen: In einem Zeitraum von zwölf Monaten fielen 42 Prozent von ihnen Ransomware-Angriffen zum Opfer.

Von diesen Opfern zahlte einer von drei das geforderte Lösegeld – wobei einer von fünf trotz Bezahlung seine Dateien nicht mehr zurückerhielt. Sie sehen: Ganz egal, ob Sie in einer großen Organisation oder in einem kleinen Unternehmen arbeiten, das Risiko ist allgegenwärtig.

ZU ENDE LESEN >

SONICWALL®

Sieben Eigenschaften, die erfolgreiche Ransomware-Angriffe gemeinsam haben



2016 registrierte SonicWall ein 600-prozentiges Wachstum der Ransomware-Familien. Im Annual Threat Report 2017 berichtete SonicWall über eine große Bandbreite an Ransomware-Formen und Angriffsvektoren – einige davon erfolgreich, andere weniger.

Was also macht einen erfolgreichen Angriff aus? Wenn Sie die sieben Komponenten einer Ransomware-Strategie verstehen, können Sie sich besser vor einer der bösartigsten Malware-Formen der Geschichte schützen.

1. Intelligente Zielgruppenforschung

Ein guter Betrüger weiß, wie er die richtigen Mitarbeiter in einer Organisation findet, um sie mit einer passenden Nachricht in die Irre zu führen. Hacker wissen, dass sie bei städtischen Einrichtungen und Healthcare-Unternehmen gute Karten haben.

Obwohl Organisationen ihre Mitarbeiter für dieses Thema sensibilisieren, fallen immer noch sehr viele auf clever konzipierte Social-Media-Posts und E-Mails herein. Außerdem können Hacker auf jede beliebige öffentliche Datenbank für Leadgenerierung zugreifen, um passende Opfer für ihre Phishing-Kampagnen zu finden.

2. Effektive Umsetzung

Da 65 Prozent der Ransomware-Angriffe per E-Mail erfolgen, können Betrüger infizierte Anhänge ganz einfach an Mitarbeiter aus der Kreditorenbuchhaltung senden und behaupten, dass es sich um eine unbezahlte Rechnung handelt. Ein solcher Angriff legte das Versorgungsunternehmen Lansing Board of Water & Light in Michigan (USA) zwei Wochen lahm und verursachte obendrein noch Kosten in Höhe von rund 2,4 Millionen USD.

ZUR VOLLSTÄNDIGEN LISTE >

SONICWALL®

Ransomware as a Service (RaaS) gehört mittlerweile zum Standard

Die richtige Vertriebsmethode spielt bei jedem Geschäftsmodell eine wesentliche Rolle: direkter Verkauf, Distributionskanäle oder eine Kombination von beiden? Dasselbe gilt für Ransomware-Entwickler.

Viele von ihnen entscheiden sich dafür, ihren erfolgreichen Code als Kit zu verkaufen. Auf diese Weise fallen viele Risiken und der enorme Distributionsaufwand weg – und sie bekommen trotzdem ein Stück vom Kuchen ab.

Im Laufe des letzten Jahres und sogar noch vor den massiven WannaCry-Attacken gab es inmitten der raffinierten und viel beachteten Angriffe auch eine große Anzahl kleiner gezielter Überfälle mit angepassten Exploit-Kits. Wie SonicWall herausfand, handelte es sich dabei um einen bunten Mix aus Hobby-Malware, böswilligem Chaos-Code, angepasster Ransomware und neu zusammengestellter RaaS-Ransomware.

- Trumplocker
- AlmaLocker
- Jigsaw
- Lambda
- Derialock
- Shade
- Popcorn
- Jaff

Vor kurzem zeigte ein Autor, wie einfach es ist, innerhalb von einer Stunde einen Ransomware-Angriff zu starten … **und zwar ohne jegliche Hacker-Fähigkeiten**.

Was bedeutet das für eine Organisation wie Ihre? Sollte Sie das beunruhigen? Einfach gesagt: Je größer die Anzahl an Quellen, desto mehr Angriffe. Doch keine Sorge – wir sind auf Ihrer Seite.

WEITERLESEN >

SONICWALL®

Warum Netzwerk-Sandboxing im Kampf gegen Ransomware entscheidend ist

Next-Generation-Firewalls setzen Signaturen und heuristische Analysen mit großem Erfolg ein. Gegen die hoch entwickelten Angriffe heutiger Hacker können sie allerdings nur wenig ausrichten. Um Zero-Day-Bedrohungen und gezielte Attacken effektiv zu bekämpfen, sind Sicherheitskonzepte mit robusten Sandboxing-Funktionen wichtiger denn je.

Das schnelle Wachstum externer Bedrohungen übertrifft heute die schlimmsten Befürchtungen. Cyberkriminelle nutzen perfide Automatisierungstechniken und versetzen sich in die Denkweise von Softwareanbietern, um ständig neue Angriffsvarianten zu kreieren – immer mit dem Ziel, einen möglichst großflächigen Schaden anzurichten, ohne dabei erkannt zu werden.

Führt man sich die Folgen eines Datenlecks oder einer Ransomware-Attacke vor Augen, ist klar: Die Erkennung und Bekämpfung von bösartigem Code – noch bevor er das Netzwerk erreichen kann – sollte für jede IT-Abteilung zu den Top-Prioritäten gehören.

Die wahre Herausforderung ist nicht die Ransomware, die sich bereits im Internet breitgemacht hat, sondern gezielte Angriffe und Zero-Day-Bedrohungen.

Bei gezielten Angriffen entwickeln Hacker für jede Organisation, die sie ins Visier nehmen, einen eigenen neuen Code. Zero-Day-Bedrohungen hingegen nutzen neu entdeckte Schwachstellen aus, für die es noch keine Patches gibt.

Es ist vor allem diese Art von Angriffen, um die sich Organisationen am meisten Gedanken machen müssen, da sie in der Regel – aus Sicht der Hacker – wesentlich erfolgreicher als ältere Angriffsvarianten sind. Wie also können Sie am besten verhindern, dass eine Bedrohung sich in Ihrem Netzwerk einnistet und sich von dort ausbreitet?

Laden Sie den kostenlosen IDC-Bericht herunter und erfahren Sie, wie Sie mittels Sandboxing hoch entwickelte Bedrohungen abwehren können.


IDC

IDC ANALYST CONNECTION

Robert Ayoub

Addressing Advanced Threats Through Multiple Sandbox Options

November 2016

Kostenloser IDC-Bericht

Addressing Advanced Threats Through Multiple Sandbox Options (So wappnen Sie sich mit mehreren Sandbox-Optionen gegen hoch entwickelte Bedrohungen)

BERICHT HERUNTERLADEN >

SONICWALL®

Stoppen Sie Ransomware mit Capture ATP

Beim SonicWall Capture Advanced Threat Protection (ATP)-Service handelt es sich um eine Cloud-basierte Multi-Engine-Sandbox mit automatisierter Problembehebung. Damit lassen sich unbekannte Angriffe und Zero-Day-Attacken (wie etwa Ransomware) am Gateway identifizieren und stoppen.

Dieser Service ist die einzige Lösung gegen raffinierte Bedrohungen, die mehrschichtiges Sandboxing – inklusive umfassender Systemsimulation und Virtualisierungstechniken – einschließt, um verdächtige Codeaktivitäten zu analysieren.

Dank dieser hoch entwickelten Funktionalität lassen sich mehr Bedrohungen aufspüren als mit umgebungsspezifischen Single-Engine-Sandbox-Lösungen, die leichter zu umgehen sind.

- **Abwehr von Ransomware in Echtzeit**
- **Analyse unterschiedlichster Dateitypen**
- **Erweiterte Multi-Engine-Bedrohungsanalyse**
- **Schnelle Implementierung von Signaturen zur Problemlösung**
- **Berichte und Warnmeldungen**
- **Blockieren der Bedrohung bis zur Klärung des Sicherheitsstatus**

Sie möchten mehr über den SonicWall Capture Advanced Threat Protection-Service erfahren? Laden Sie einfach das Datenblatt herunter oder besuchen Sie uns unter **sonicwall.com/capture**.

Wie funktioniert Capture ATP?

ZUM DATENBLATT >

SONICWALL®

Demo: SonicWall Capture ATP vs. aktuelle Malware

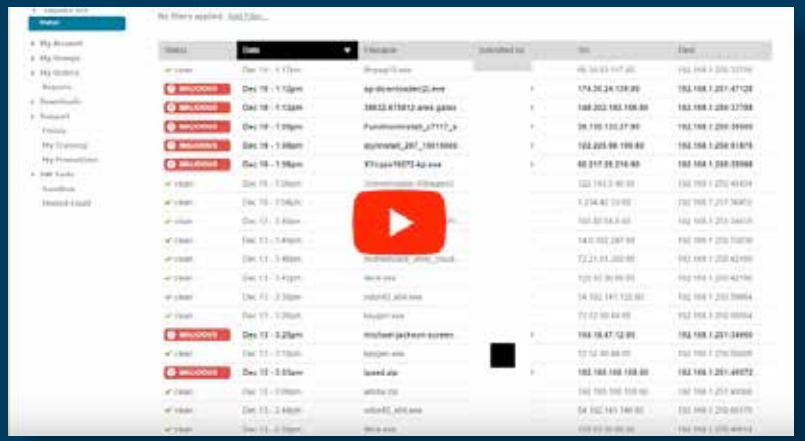
SonicWall Capture Advanced Threat Protection schützt Kunden zuverlässig vor den immer gefährlicheren Zero-Day-Bedrohungen (wie z. B. Ransomware), indem es raffinierte Angriffe am Gateway erkennt und diese blockiert, bis der Sicherheitsstatus geklärt ist. Dieser Cloud-basierte Service ist mit den SonicWall-Firewalls erhältlich.

Wie effektiv ist Capture ATP? Um Ihnen zu zeigen, wie wir hoch entwickelte Angriffe stoppen, die jeden Tag zahllose Unternehmen bedrohen, haben wir die gefährlichste und neueste Malware aus dem Internet gegen die SonicWall-Technologie antreten lassen.

Erfahren Sie, wie wir nur mithilfe von Gateway Anti-Virus (GAV) und Capture ATP diesen bösartigen Code in Echtzeit identifiziert und unschädlich gemacht haben. Capture ATP findet schnell und effizient heraus, was die Malware mit der Anwendung, dem Betriebssystem, der Software und der Hardware im Schilde führt.

Um eine weitere Verbreitung zu verhindern, stellt die Global Threat Intelligence-Infrastruktur anschließend sicher, dass die Signaturen für die neu identifizierten Bedrohungen umgehend auf allen SonicWall-Netzwerksicherheitsappliances implementiert werden.

Kunden profitieren so von hocheffizienten Sicherheitsmechanismen, schnellen Reaktionszeiten und niedrigeren Total Cost of Ownership.



VOLLSTÄNDIGE DEMO ANSEHEN >

SONICWALL®

Über uns

Seit über 25 Jahren gehört SonicWall zu den weltweit führenden Anbietern effizienter Sicherheitslösungen. Angefangen bei Access-Security über Netzwerksicherheit bis hin zu E-Mail-Security: Wir entwickeln unser Produktportfolio kontinuierlich weiter, damit unsere Kunden Innovationen realisieren, Prozesse beschleunigen und wachsen können. Mit über einer Million Sicherheitsgeräte in nahezu 200 Ländern und Regionen weltweit bietet SonicWall seinen Kunden alles, was sie brauchen, um für die Zukunft gerüstet zu sein.

Wenn Sie Fragen zur Nutzung dieser Unterlagen haben, wenden Sie sich an:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, Kalifornien 95054, USA

Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com

SONICWALL®