WHITEPAPER

Ransomware – die rasante Zunahme einer Cyberbedrohung

Was Sie über Erpressungssoftware wissen müssen

Zusammenfassung

Wenn eine Cyberbedrohung in einem Jahr um das 35-Fache zunimmt und im nächsten Jahr noch häufiger wird, sollte jedes Unternehmen alarmiert sein. Genau das ist bei Ransomware passiert. Cyber-Kriminelle haben Firmen aus vielen verschiedenen Branchen sowie Unternehmen praktisch jeder Größe ins Visier genommen.

Ransomware-as-a-Service (RaaS) und andere „Hacker-Toolkits" haben den Einstieg für Cyber-Kriminelle erleichtert. Damit können selbst unerfahrene Bedrohungsakteure zerklüftete Security-Infrastrukturen erfolgreich angreifen. Und monetäre Technologien wie Bitcoin machen es Strafverfolgungsbehörden praktisch unmöglich, Lösegeldzahlungen zu verfolgen. Wegen der exponentiellen Zunahme von Lösegeldzahlungen an Ransomware-Gruppen ist die Wahrscheinlichkeit groß, dass solche Angriffe in Zukunft noch häufiger auftreten werden. Banken haben die Gefahr bereits erkannt und decken sich mit Bitcoins ein, damit ihre Kunden Cyber-Kriminelle ggf. schnell für das Entsperren gehackter Daten bezahlen können.

Bedrohung durch Runaway Ransomware

Die Analyse weltweiter Daten der FortiGuard Labs ergab einen erheblichen Anstieg der Ransomware-Gesamtaktivität im 2. Halbjahr 2020 gegenüber der ersten Jahreshälfte. Analysiert wurde die Aktivität aller als Ransomware klassifizierten Signaturen. Das Ergebnis: Im Dezember 2020 war die Ransomware-Aktivität im Vergleich zum Juli 2020 um das 7-Fache angestiegen (Abbildung 1).

„Im Vorjahr haben wir eine wahre Explosion von Ransomware erlebt und gesehen, dass die Lösegeldforderungen von fünfstelligen Beträgen im Jahr 2015 auf sechsstellige Summen gestiegen sind und mittlerweile Millionen von Dollar betragen."[1]

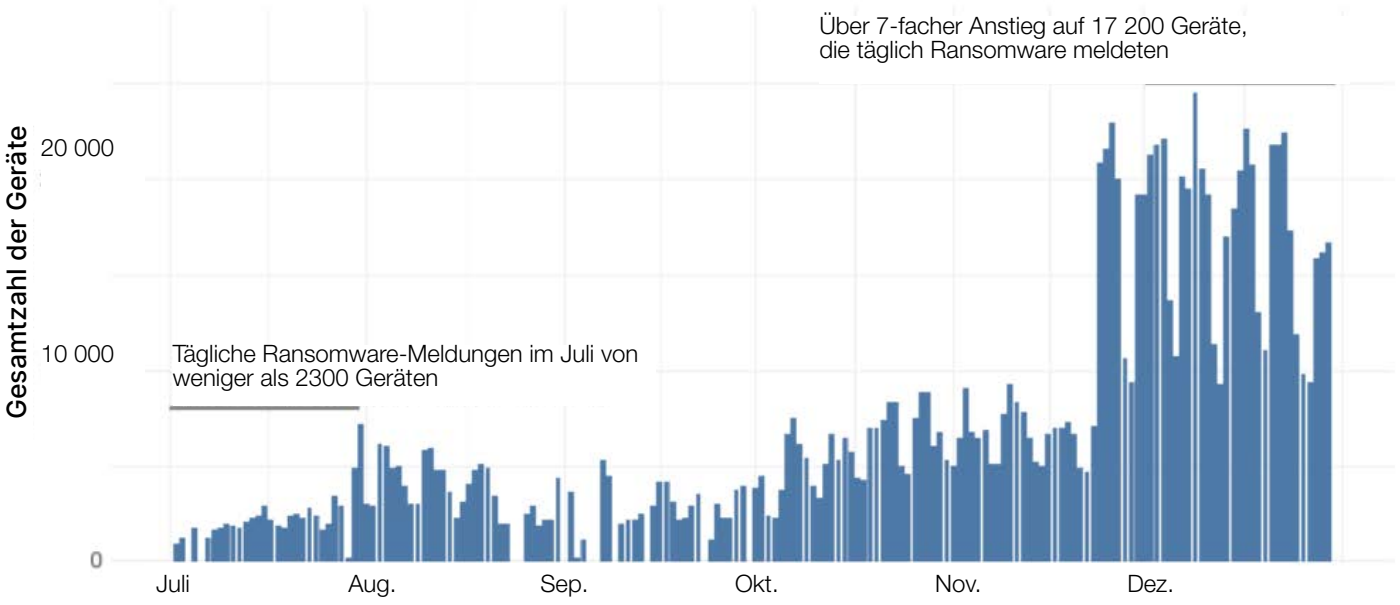


Abbildung 1: Anzahl der Geräte, die im 2. Halbjahr 2020 täglich Ransomware erkannten

Zu den aktivsten Ransomware-Stämmen im 2. Halbjahr 2020 gehörten Egregor, Ryuk, Conti, Thanos, Ragnar, WastedLocker, Phobos/EKING und BazarLoader. Trotz der unterschiedlichen Verbreitung dieser Ransomware zeigte die allgemeine Entwicklung eine steigende Aktivität in diesem Zeitraum (Abbildung 2).

Bedrohungsakteure haben herausgefunden, dass die Verschlüsselung kritischer Systeme und Lösegeldforderungen für die Entschlüsselung eine relativ einfache Möglichkeit ist, Geld von Unternehmen jeder Größe und Branche zu erpressen. Es handelt sich dabei um eine gezieltere, bedrohlichere Form des Ransomware-Schemas, auch als „Großwildjagd" bekannt. Dieser Boom bei Ransomware-Banden 2020 sowie die hohen Summen, die sich damit erbeuten lassen, dürften praktisch eine Garantie für dafür sein, dass der Trend zur „Massen-Abzocke" so bald nicht vorbei ist.

Viele Angreifer nutzten durch die Corona-Pandemie verursachte Störungen aus, um speziell gegen Unternehmen und Einrichtungen im Gesundheitswesen Ransomware-Angriffe zu fahren. Im Oktober veröffentlichten die US-Behörde für Cybersecurity und Infrastruktursicherheit (CISA), das US-Gesundheitsministerium und das FBI eine gemeinsame Warnung, um Krankenhäuser und Gesundheitsdienstleister in den USA auf steigende Ransomware-Aktivitäten mit Malware wie TrickBot und BazarLoader hinzuweisen. Andere Branchen, die im 2. Halbjahr 2020 stark unter Ransomware-Angriffen litten, waren Dienstleistungsunternehmen, Anbieter von Verbraucherdiensten, öffentliche Einrichtungen und Finanzdienstleister.

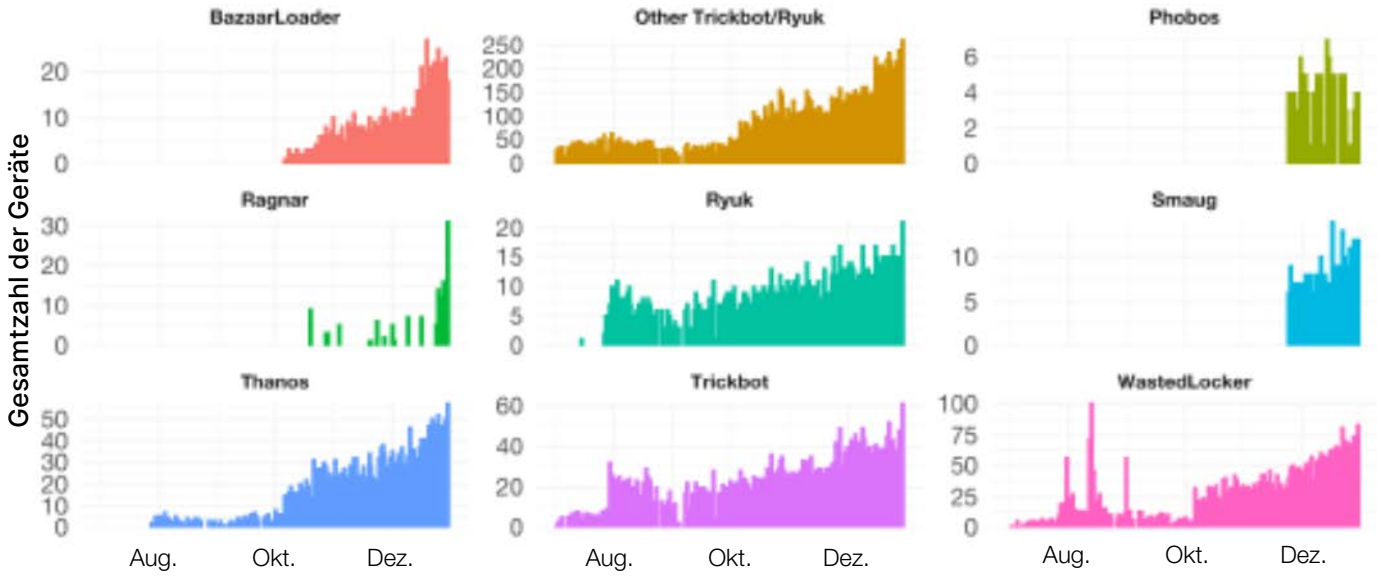


Abbildung 2: Tägliche Erkennungen von ausgewählten Ransomware-Stämmen im 2. Halbjahr 2020

Die von den FortiGuard Labs und anderen beobachteten Ransomware-Aktivitäten in der zweiten Jahreshälfte 2020 wurden durch mehrere Entwicklungen geprägt. Eine der Besorgniserregendsten war die stetige Zunahme von Ransomware-Angriffen, bei denen Daten abgezogen und bei ausbleibendem Lösegeld verkauft oder veröffentlicht wurden. Datendiebstahl als „Zusatznutzen" bei Ransomware-Kampagnen kam erstmals Anfang 2020 vor, machte jedoch am Jahresende den Großteil der Angriffe aus.

Bei Angriffen mit den meisten großen Ransomware-Stämmen (wie Sodinokibi, Ryuk, Egregor, Conti) wurden im Vorjahr standardmäßig Daten abgegriffen. Bei einigen gemeldeten Vorfällen führten die Angreifer die Opfer mit (manchmal falschen) Zusagen hinters Licht, um sie zum Zahlen von Lösegeld zu bewegen. So gab es viele Fälle, in denen die Opfer das Lösegeld zahlten unter der Bedingung, dass die Angreifer die gestohlenen Daten löschten – die dann aber trotzdem von den Cyber-Kriminellen veröffentlicht oder verkauft wurden. Unternehmen sollten sich deshalb bewusst sein, dass zuverlässige Daten-Backups allein keinen Schutz vor Ransomware-Forderungen darstellen.[2]

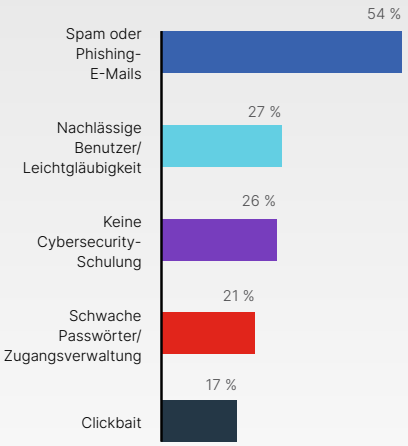
Wie Ransomware in Ihr Unternehmen gelangt

Verbreitung von Ransomware

Wie gelangt Ransomware in Ihr Unternehmen? Zur Beantwortung dieser Frage muss zuerst untersucht werden, wie Ransomware verbreitet wird. Hierfür können alle digitalen Wege genutzt werden: E-Mail, Website-Anhänge, Geschäftsanwendungen, soziale Netzwerke und USB-Laufwerke sowie weitere digitale Übertragungswege. E-Mails sind nach wie vor der „Ransomware-Einschleuser Nr. 1". Am häufigsten verwenden Cyber-Kriminelle dabei Links in E-Mails, gefolgt von E-Mail-Anhängen.

Im Fall von E-Mails werden Phishing-E-Mails als Lieferbenachrichtigung oder fingierte Aufforderungen zu Software-Updates gesendet. Sobald der Benutzer auf den Link oder den Anhang klickt, werden häufig (in jüngerer Vergangenheit seltener) ganz offen weitere schadhafte Komponenten heruntergeladen. Diese verschlüsseln dann Dateien mit privaten 2048-RSA-Schlüsseln, wodurch es für den Benutzer nahezu unmöglich wird, die Dateien je wieder zu öffnen. In anderen Fällen wird Ransomware als Datei auf einer Website eingebettet. Wenn der Benutzer diese Datei herunterlädt und installiert, wird der Angriff aktiviert.

Häufigste Ursachen für Ransomware-Infektionen:[3]



Arten von Ransomware

Ransomware-Angriffe können auf verschiedene Weise erfolgen. Im vergangenen Jahr haben sich die Angriffsabläufe stark verändert. Herkömmliche Ransomware zielt auf Daten ab und sperrt Dateien, bis das Lösegeld bezahlt wird. Wie bereits erwähnt, hat sich durch das schnelle Wachstum des Internets der Dinge (IoT) eine neue Ransomware-Variante entwickelt. Diese sucht nicht nach den Daten eines Unternehmens, sondern zielt auf Steuerungssysteme (z. B. von Fahrzeugen, Fertigungslinien, Antriebssystemen) ab und fährt sie herunter, bis das Lösegeld gezahlt wird.

Folgende Arten von Ransomware werden aktuell am häufigsten verwendet:

- **Standard-Ransomware:** Bestimmte Ransomware gibt es als serienmäßige Software, die Cyber-Kriminelle auf Darknet-Marktplätzen kaufen und auf ihren Servern installieren können. Das Hacken und Verschlüsseln von Daten wird dann direkt von der Software gelenkt. Zu der serienmäßigen Ransomware zählen beispielsweise Stampado und Cerber.
- **Ransomware-as-a-Service:** CryptoLocker ist wahrscheinlich das bekannteste RaaS-Modell. Nachdem seine Server aus dem Verkehr genommen wurden, hat sich CTB-Locker zur häufigsten RaaS-Angriffsmethode entwickelt. Ein weiterer schnell wachsender RaaS ist Tox – ein Kit, das Cyber-Kriminelle einfach herunterladen können. Dieses Kit erstellt eine spezielle ausführbare Datei, die von den Cyber-Kriminellen installiert oder verteilt werden kann. Zur Bezahlung überlassen die Cyber-Kriminellen 20 % des Lösegelds an Tox – natürlich in Bitcoin.
- **Ransomware-Partner-Programme:** Bei diesem RaaS-Modell verbreiten „Hacker-Dienstleister“ mit einer gewissen Erfolgsbilanz die Malware.
- **Angriffe auf IoT-Geräte:** Ransomware infiltriert auch IoT-Geräte, die geschäftskritische Systeme steuern. Die Software fährt das System herunter, bis ein Lösegeld für das Entsperren des Systems gezahlt wird.

Interessanterweise verwendet Ransomware zusätzlich zu polymorphem Code häufig metamorphen Code, um ihre digitale Identität bei gleicher Vorgehensweise zu ändern. Wegen des schnellen Wachstums und der kontinuierlichen Weiterentwicklung ist es für Unternehmen, die sich auf herkömmliche signaturbasierte Antivirus-Lösungen verlassen, noch schwerer, Schritt zu halten. Wenn eine Variante identifiziert und auf die schwarze Liste gesetzt wurde, sind Cyber-Kriminelle bereits zu einer neuen Variation übergegangen. Die Ransomware-Familien Ryuk und Sodinokibi trugen z. B. beide zum Anstieg der verlangten Lösegeldbeträge im 1. Quartal 2020 bei.[4]

Ziele von Ransomware

Nahezu jedes heutige Betriebssystem ist Ziel von Ransomware. Angriffe erstrecken sich auch auf die Cloud und mobile Geräte. Von Ransomware bislang verschonte Clouds eröffnen Hackern nun eine neue „Marktchance".[5]

Cyber-Kriminelle greifen zudem fast jede Branche an. Allein 2020 warnte die US-Behörde für Cybersecurity und Infrastruktursicherheit (CISA) vor Ransomware, die auf den Pipeline-Betrieb, das Gesundheitswesen, den öffentlichen Sektor, Schulen und weitere Bereiche abzielt.

Eine weitere Strategie von Ransomware-Hacktivisten ist der Angriff und die Infektion anfälliger Geschäftsserver. „Die Ransomware DearCry, die Anfang 2021 neu entdeckte Schwachstellen bei Microsoft Exchange ausnutzte, ist ein gutes Beispiel für diese Taktik und zeigt zugleich die Agilität von Cyber-Kriminellen."[6] Durch die Kompromittierung von Servern können Hacker Hosts identifizieren und angreifen und die Anzahl von potenziell infizierten Servern und Geräten in einem Netzwerk vervielfachen. Der Zeitrahmen des Angriffs wird somit verdichtet, wodurch dieser Angriffstyp viraler ist als über Endanwender eingeschleuste Infektionen. Diese Entwicklung könnte dazu führen, dass Opfer mehr für Entschlüsselungscode zahlen und die Zeiten bis zum Wiedererlangen der verschlüsselten Daten länger werden.

Branchenwarnungen im Jahr 2020:[7]

- 10.12.2020: AA20-345A (Schulen)
- 28.10.2020: AA20-302A (Gesundheitswesen)
- 28.10.2020: AA20-302A (Öffentlicher Sektor)
- 18.12.2020: AA20-049A (Pipeline-Betrieb)

Fazit

Die finanziellen Auswirkungen von Ransomware gehen weit über das bezahlte Lösegeld hinaus. Die Ausfallzeiten führen zu Umsatz- und Produktivitätsverlusten in einer Größenordnung von sechsstelligen, wenn nicht sogar Millionenbeträgen. Unternehmen aus verschiedensten Branchen können diese Folgen bestätigen.

Mit unsystematischen Sicherheitsansätzen lassen sich keine Ransomware-Angriffe verhindern. Benötigt werden integrierte Modelle, die eine mehrstufige Security mit Next Generation Firewalls (NGFW), moderner Endpunkt-Sicherheit und weitere Schutzfunktionen schaffen. Diese Sicherheitskontrollen müssen zudem proaktive Bedrohungsinformationen verwenden, um ein erfolgreiches Verteidigungsbollwerk vor Cyber-Angriffen aufzubauen.

[1] Jonathan Holmes, et al.: „Cyber Summit 2020: Trends and Predictions in Ransomware". Federal Bureau of Investigation (FBI), 2020.

[2] „Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs". Fortinet, Februar 2021.

[3] „Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2020". Statista, 16. Februar 2021.

[4] David Bisson: „Increase in Ransomware Demand Amounts Driven by Ryuk, Sodinokibi". Tripwire, 4. Mai 2020.

[5] Corey Nachreiner: „Why Ransomware Will Soon Target the Cloud". Dark Reading, 11. Februar 2020.

[6] „New DearCry Ransomware Targets Exchange Server Vulnerabilities". FortiGuard Labs, 12. März 2021.

[7] „Ransomware Alerts and Tips". Cybersecurity and Infrastructure Security Agency, abgerufen am 28. April 2021.

1. Juli 2021, 11:53 Uhr

679688-A-1-DE