Der Weg der Krypto-Ransomware: Erkennung, Reaktion und Prävention

Was ist Krypto-Ransomware?

Krypto-Ransomware ist eine Art von Malware, die auf einem Server, Computer oder Mobilgerät gespeicherte Dateien verschlüsselt, um Geld zu erpressen. Bei der Verschlüsselung werden Dateien so „codiert“, dass sie nicht mehr lesbar sind. Für den Entschlüsselungscode, der zur Wiederherstellung der Dateien benötigt wird, wird ein Lösegeld verlangt.[1]

Die Angreifer nutzen eine Mischung aus ausgefeilten technologischen Kenntnissen und psychologischer Manipulation (Social Engineering) als Auslöser für Krypto-Ransomware-Angriffe.

Übliche Übertragungswege

- Bösartige Dateien oder Links, die per E-Mail, SMS oder Sofortnachricht übermittelt werden
- Trojaner-Downloader, Exploit-Kits oder Toolkits, die von Angreifern auf Websites eingeschleust werden
- Sicherheitslücken in anfälliger Software
- Internetverkehr, der auf bösartige Websites umgeleitet wird
- Legitime Websites, in deren Webseiten bösartiger Code eingeschleust wurde
- Malvertising-Kampagnen
- Selbstverbreitungsfähigkeiten (Ausbreitung von einem infizierten Computer auf einen anderen)[1,2]

Wie erfolgt die Infizierung?

95 % der Verstöße gegen die Cybersicherheit werden durch menschliches Versagen verursacht.[6]

Remote-Mitarbeiter haben eine Sicherheitsverletzung in **20 % der Organisationen verursacht.**[8]

Phishing, der betrügerische Versuch, an sensible Informationen oder Daten wie Nutzernamen oder Kreditkartendaten zu gelangen, in dem sich eine Person als vertrauenswürdige Marke ausgibt, ist mit Abstand eine der häufigsten Ursachen für die Verbreitung.

Nach einem Rückgang im Jahr 2019 **hat das Phishing 2020 wieder zugenommen und betrifft nun 1 von 4200 E-Mails.**[6]

Wie hoch ist das Risiko?

Mehr als **4.000 Ransomware-Angriffe** sind seit 2016 täglich aufgetreten.[3]

Ransomware-Angriffe gegen Unternehmen erfolgen **alle 11 Sekunden.**[4]

50 % der Unternehmen geben an, dass sie nicht das Gefühl haben, ausreichend auf die Bedrohung vorbereitet zu sein.[4]

Top 5 Branchen, die am anfälligsten für Ransomware sind:

- 59 % Gesundheitswesen
- 50 % Finanzen/Versicherung
- 45 % Regierung
- 41 % Professional Services
- 37 % Bildungswesen

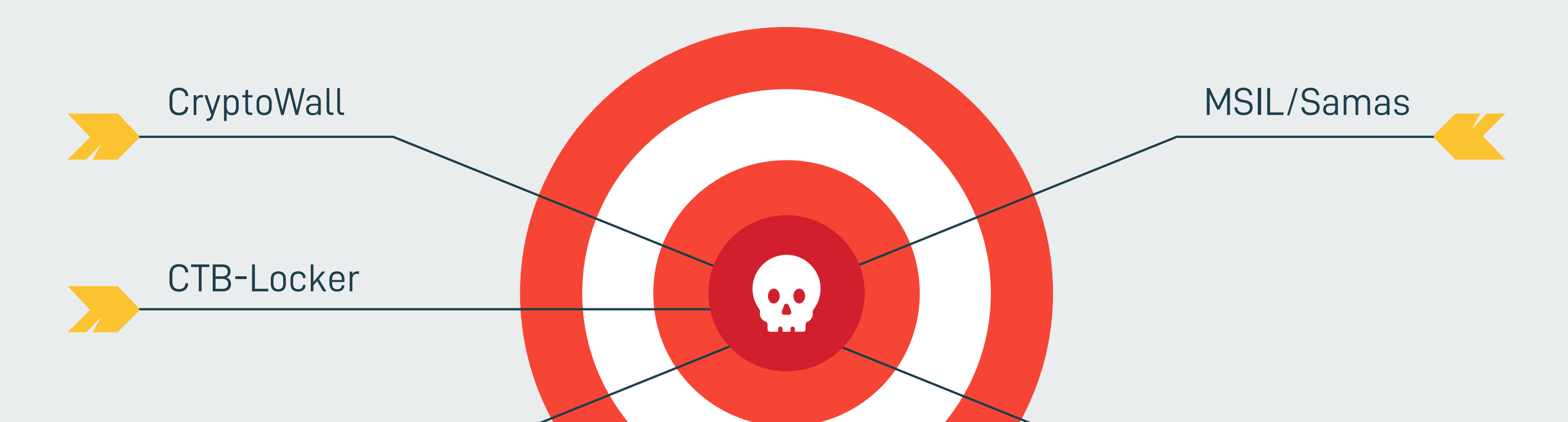
Ransomware-Varianten

Ransomware-Varianten sind immer ausgefeilter und zerstörerischer geworden.

Einige Varianten verschlüsseln nicht nur die Dateien auf dem infizierten Gerät, sondern auch den Inhalt von freigegebenen oder vernetzten Laufwerken, extern angeschlossenen Speichermedien und Cloud-Speicherdiensten, die den infizierten Computern zugeordnet sind.

Diese Varianten gelten als besonders zerstörerisch, da sie die Dateien von Benutzern und Unternehmen verschlüsseln und diese Dateien unbrauchbar machen, bis ein Lösegeld gezahlt wird.

Die fünf wichtigsten Ransomware-Varianten, die auf US-amerikanische Unternehmen und Einzelpersonen abzielen:[5]



Anzeichen eines Angriffs

- Ungewöhnliche Änderungen von Dateinamen
- Sperren von Bildschirmen
- Hintergrundbild mit einer Lösegeldforderung

Einmal infiziert, sind die möglichen Folgen eines Ransomware-Angriffs:

- Verlust der Geschäftsproduktivität
- Geschäftskritischer Ausfall
- Datenverlust und/oder Gerät

Wie sollten Sie reagieren?

Wenn ein Angriff vermutet wird, zählt jede Sekunde.

- Scannen Sie Netzwerke zur Bestätigung, dass ein Angriff stattfindet.
- Isolieren Sie den/die infizierten Computer sofort.
- Sichern Sie sofort Backup-Daten oder -Systeme, indem Sie sie offline nehmen.
- Stellen Sie sicher, dass die Backups frei von Malware sind.
- Sammeln und sichern Sie, falls vorhanden, Teilbereiche der erbeuteten Daten.
- Ändern Sie alle Passwörter von Online-Konten und Netzwerken, nachdem Sie das System aus dem Netzwerk entfernt haben.
- Aktualisieren Sie alle Systempasswörter, sobald die Malware vom System entfernt ist.
- Löschen Sie Registry-Werte und Dateien, um das Laden des Programms zu verhindern.[5]
- Kontaktieren Sie die Strafverfolgungsbehörden.

Verhindern zukünftiger Angriffe

- Verwenden Sie einen Multi-Layer Ansatz zur Überwachung der Netzwerkaktivitäten und scannen Sie aktiv nach Malware und bösartigen Bedrohungen.
- Sichern Sie Dateien/Daten regelmäßig mit einer Business Continuity-Lösung.
- Patch-Management
- Beschränken/begrenzen Sie Konten.
- Multi-Faktor-Authentifizierung auf Endgeräten
- Anti-Malware-Dienste
- Ransomware-Erkennung
- Mitarbeiterschulung und -training[2]

Langfristige präventive Schutzoptionen

Angesichts der Tatsache, dass die**durchschnittlichen Kosten für Ausfallzeiten (274.200 US-Dollar) im Jahr 2020 um 94 % gestiegen sind**[7], kann kein Unternehmen – ob groß oder klein – den Schaden übersehen, den ein Angriff verursachen kann. Der beste Weg, diesen Bedrohungen einen Schritt voraus zu sein, sind Lösungen zur Erkennung von Ransomware und zur Verhinderung ihrer Ausbreitung sowie im Falle einer Infektion zur schnellen Wiederherstellung und Wiederbeschaffung von Daten.

Die Ransomware-Erkennung von Datto RMM

Eine Funktion, die Antiviren-Programme ergänzt, um eine zusätzliche Sicherheitsebene zu bieten

Die zum Patent angemeldete Technologie überwacht Krypto-Ransomware in Echtzeit und alarmiert MSPs in dem Moment, in dem Ransomware beginnt, Dateien zu verschlüsseln, anstatt darauf zu warten, dass ein Benutzer das Problem erkennt und meldet.

RMM-Ransomware-Erkennung kann das infizierte Gerät automatisch vom Netzwerk isolieren, während die Verbindung zu Datto RMM aufrechterhalten wird, um eine Ausbreitung zu verhindern und eine schnellere Reaktion und effektive Maßnahmen zu ermöglichen, einschließlich der Wiederherstellung eines früheren Zustands mit Datto Continuity-Lösungen.

Datto SIRIS

Eine All-in-One-Lösung für Business Continuity und Disaster Recovery (BCDR), die lokale Backups und Wiederherstellungen mit einem sicheren, cloudbasierten Repository und einer vollständigen Disaster Recovery in der unveränderlichen Datto Cloud verbindet.

Im Falle eines Angriffs kann ein Techniker mit Datto SIRIS Dateien und Server **wiederherstellen und in einen früheren Zustand versetzen.**

Als Teil des Backup-Prozesses erkennt die **patentierte Ransomware-Scan-Technologie** in SIRIS, ob die gesicherten Daten mit Ransomware infiziert sind.

Die patentierte **Screenshot-Verifizierung** überprüft dann, ob das Backup wiederhergestellt werden kann.

Lokale und cloudbasierte Backup-Snapshots, die von SIRIS erstellt wurden, können nicht durch Ransomware infiziert werden.

Sie können die Zeit einfach **auf einen Zeitpunkt** (Snapshot) vor dem Angriff „zurückdrehen“.

Wenn Sie mehr darüber erfahren möchten, wie Sie Ihre Kunden vor Ransomware schützen und effektiv reagieren können, wenn sie betroffen sind, sprechen Sie mit einem Solutions Engineer und erfahren Sie, wie Datto helfen kann.

Quellen:

[1]https://www.f-secure.com/v-descs/articles/crypto-ransomware.shtml#:~:text=

[2]https://heimdalsecurity.com/blog/why-ransomware-attacks-still-work/

[3]https://safeatlast.co/blog/ransomware-statistics/#gref

[4]https://phoenixnap.com/blog/ransomware-statistics-facts

[5]https://www.justice.gov/criminal-ccips/file/872771/download

[6]https://www.varonis.com/blog/cybersecurity-statistics/

[7]Der State of the Channel Ransomware Report 2020 von Datto

[8]https://blog.malwarebytes.com/reports/2020/08/20-percent-of-organizations-experienced-breach-due-to-remote-worker-labs-report-reveals/

datto