Alles Wissenswerte zu Ransomware

Sie sind vielbeschäftigt. Sie sind müde. Sie möchten einfach nur Pokémon Go spielen oder auf das Intranet Ihres Unternehmens zugreifen. Was auch immer der Grund ist: Wenn Sie bei einem Software-Update auf „Später erinnern“ klicken, machen Sie Ihr Gerät anfällig für Ransomware.

Das ist nur eine der vielen Möglichkeiten, die Ransomware für den Zugang zu Ihrem System nutzt. Malvertising, Phishing-E-Mails und sogar komplex modifizierte USB-Sticks sind bekannte Taktiken, die Angreifer zur Kompromittierung Ihres Systems nutzen. Schauen wir uns eine übliche Methode etwas genauer an.

Sie klicken auf „Später erinnern“

Keine Software ist perfekt. Entwickler ermitteln regelmäßig Bugs in ihren Programmen und veröffentlichen Patches, um diese Fehler zu beseitigen. Wenn Sie die Aktualisierung von Plug-ins oder Anwendungen hinauszögern, können Angreifer diese bekannten Schwachstellen leicht ausnutzen. Bei einem weit verbreiteten Exploit-Kit verliefen 80 Prozent aller erfolgreichen Versuche über Flash. Sei es Flash, Silverlight oder auch Google Chrome – Sie sollten regelmäßig Updates und Patches installieren.

Ihr System wurde infiziert

Ransomware hat jetzt die Kontrolle über infizierte Systeme auf Ihrem Gerät. Die Malware verwendet dann einen asymmetrischen Schlüssel, um Dateien zu verschlüsseln. Im Allgemeinen ist sie in der Lage, die Daten ohne Ihre Zustimmung zu verschlüsseln. Nur der Entwickler der Ransomware hat den Schlüssel, um diese wieder freizugeben. Einige Arten von Ransomware verbreiten sich auch über das Netzwerk. Sicherheitsexperten sagen voraus, dass diese Selbstverbreitung weiter zunehmen wird.

Eine Lösegeldforderung erscheint

Sobald die Infizierung abgeschlossen ist, erscheint eine Nachricht auf dem Bildschirm, in der ein Lösegeld in Bitcoins gefordert wird. Ein typisches Lösegeld kann zwischen 200 und 10.000 US-Dollar betragen. Einige Einrichtungen haben einen weitaus höheren Preis bezahlt. Ein Krankenhaus in Kalifornien zahlte 17.000 US-Dollar für seine Daten. Dies geschah, nachdem sie täglich 100.000 US-Dollar verloren hatten, da der Standardbetrieb nicht aufrechterhalten werden konnte.

Sicherheitsexperten raten davon ab, das Lösegeld zu zahlen. Einige Arten von Ransomware können die Dateien entweder gar nicht entsperren oder vernichten sie automatisch. Sicherheitsforscher von Talos haben festgestellt, dass der Einsatz dieser schädlichen, zerstörenden Ransomware zunimmt. Laut dem Cisco Midyear Security Report 2016 warnen Sicherheitsforscher davor, dass die Datenintegrität ein neues Problem bei Ransomware wird. Sie können nicht darauf vertrauen, dass die Angreifer die Integrität der verschlüsselten Daten sicherstellen. Die potenziellen Auswirkungen von beispielsweise manipulierten Patientenakten oder Konstruktionsplänen können verheerend sein.

Darüber hinaus unterstützen Sie durch Ihre Lösegeldzahlung diesen kriminelle Geschäftszweig. Solange die Angreifer Geld mit Ihren Aktionen verdienen, werden sie auch immer ausgereiftere Ransomware entwickeln.

So können Sie Ransomware bekämpfen

Die beste Möglichkeit, sich gegen Ransomware zu wappnen, ist die Einrichtung mehrerer Sicherheitsebenen.

Vor einem Angriff

Sie können Ihre Verteidigungsstrategie auf einfache Weise stärken. Sie sollten mit einem Disaster Recovery-Partner als Backup-Plan zusammenarbeiten, um einen reibungslosen Betrieb Ihres Unternehmens auch im schlimmsten Fall zu gewährleisten. Aber Sie können auch noch einfachere Maßnahmen ergreifen. Erstellen Sie regelmäßige Backups, um wichtige Daten zu schützen. Installieren Sie Anzeigenblocker, und aktualisieren Sie immer Ihre Software, wenn Sie dazu aufgefordert werden.

Die Anzeigenblocker alleine können jedoch nicht alle Malvertising-Vorfälle erkennen und blockieren oder schädliche Hyperlinks identifizieren. Dafür wird eine Lösung wie Cisco® Umbrella benötigt. Sie kann in weniger als 5 Minuten installiert werden, erkennt schädliche Websites und blockiert Anfragen auf Host-Ebene.

Während eines Angriffs

Mit Umbrella werden die meisten Ransomware-Dateien auf der DNS-Layer gestoppt, bevor sie das Gerät eines Endbenutzers erreichen. Aber auch die besten Sicherheitsmaßnahmen bieten keinen garantierten Schutz vor Ransomware.

Sie müssen sehen können, was im Netzwerk vor sich geht, und in der Lage sein, Angriffe zu identifizieren, sobald diese auftreten. Die Bedrohungserkennung von Cisco Stealthwatch™ überwacht den Netzwerkverkehr und identifiziert Anomalien wie eine Ransomware-Infektion. Die Lösung sendet dann eine Warnung, dass das System kompromittiert wurde.

Cisco verfügt über leistungsstarke Tools, um die Ausführung der Datei zu verhindern:

Alles Wissenswerte zu Ransomware

- Umbrella schützt Ihr System, indem die von der Datei gesendete Anfrage an die Verschlüsselungsinfrastruktur blockiert wird. Das bedeutet, dass die Ransomware nicht mehr kommunizieren kann und daher auch nicht die zur Verschlüsselung Ihrer Daten erforderlichen Informationen erhält.
- Umbrella blockiert die Anfrage, und die Next-Generation Firewall von Cisco blockiert die Verbindung, sodass Ihr System doppelt geschützt ist.
- Wenn eine Datei sowohl die DNS-Layer als auch die Firewall umgangen hat, kann Cisco Advanced Malware Protection (AMP) für Endpunkte die Datei an der Ausführung hindern und dann noch einen Schritt weitergehen. Die Lösung analysiert kontinuierlich alle Dateiaktivitäten im System, sodass Sie alle schädlichen Dateien finden und löschen können.

Nach einem Angriff

Wenn Sie bereits durch Ransomware kompromittiert wurden, müssen Sie das Ausmaß des Schadens ermitteln und die Verbreitung der Ransomware verhindern. AMP kann die Ausführung bekannter Malware-Dateien verhindern und die Datei vom Endpunkt entfernen.

Um die Verbreitung von Ransomware im Netzwerk zu stoppen, sollten Sie die dynamische Segmentierung mit Cisco TrustSec® Technologie nutzen. Diese kann die infizierten Teile des Netzwerks ermitteln und die Verbreitung der Ransomware verhindern.

Sie möchten mehr erfahren? Besuchen Sie cisco.com/go/ransomware.

C11-737870-00 09/16