Cryptojacking – oder wenn der Computer fremdgeht

Durch den letztjährigen Boom bei den Kryptowährungen ist das Interesse an Bitcoin, Monero, Ethereum und Ripple, um nur einige zu nennen, massiv gestiegen. Oftmals fehlt jedoch ein grundlegendes Verständnis über die Kryptowährungen und den damit verbundenen Risiken. Dieses mangelnde Risikobewusstsein macht den Markt auch für Kriminelle attraktiv, sodass immer mehr Einzelpersonen und Unternehmen Opfer von illegalem Cryptomining werden.

Zuerst eine kurze Begriffserklärung. Unter «Cryptomining» versteht man das Schürfen von Krypto-währungen auf einem Computer. Dies ist völlig legal, solange dafür die eigene Hardware verwendet wird. «Cryptojacking» steht für die kriminelle Seite des Booms. Da das Schürfen von den Kryptowährungen grosse Rechenleistung erfordert und somit hohe Energie- sowie Hardware-Kosten nach sich ziehen, gehen Kriminelle zur Gewinnmaximierung immer mehr dazu über, diese Arbeit von anderen ohne deren Wissen erledigen zu lassen. «Jacking» steht somit für Entführung von fremder Rechnerleistung, heimlich bzw. gegen den Willen des Besitzers.

Die Angreifer gehen dabei sehr geschickt vor, um ihre Malware zu tarnen. Hacker nutzen dabei aktiv Schwachstellen aus und platzieren Cryptomining-Software auf Server/PCs, Smartphones, IoT, Tablets, Netzwerke-Devices, und Websites. Da das Schürfen immer mehr Energie und Rechnerkapazität benötigt, werden immer mehr auch Unternehmensressourcen dafür gekapert, um so eine stabile, zuverlässige und kontinuierliche Einnahmequelle zu erzeugen.

Die häufigsten Infektionswege

Die hohen Gewinnaussichten motivieren die Angreifer, immer wieder neue Infektionsmethoden und -techniken zu entwickeln, sodass wir uns in Zukunft vermehrt auf Angriffe durch Cryptojacking einstellen müssen. Dazu gehören unter anderem:

- Websites die «JavaScript (WebAssembly)» einbetten, damit wird Cryptomining im Webbrowser ermöglicht.
- E-Mails mit bösartigen Anhängen oder schadhaften Links.
- Kompromittierte Websites, die Code durch Ausnutzung von Browser-Plugin-Schwachstellen injizieren.
- Kompromittierte vertrauenswürdige Systemprozesse mit modifiziertem Code.
- Cryptomining Anwendungen mit verschlüsselter Kommunikation.
- Aktive Ausnutzung von Schwachstellen in serverbasierten Anwendungen.
- Ausnutzung von Schwachstellen in Technologien wie Adobe Flash (o.ä.), um damit die Malware via Exploit-Kits zu verteilen.

Von Bitcoin zu Monero

Auch der Global Threat Index von Check Point zeigt einen rasanten Anstieg bei Cryptomining-Malware auf. Unter den 10 häufigsten auftretenden Malware-Arten befinden sich drei verschiedene Varianten von Cryptomining-Malware, wobei Coinhive mit 23 Prozent aller Infektionen für die meisten Infektionen verantwortlich ist.

Coinhive sieht sich eigentlich als legales Angebot für Websitebetreiber. Die können ihre Besucher und Besucherinnen auch darüber informieren und das Einverständnis zum Schürfen einholen. Doch auf vielen Seiten, unter anderem auf vielen illegalen Streamingdiensten, werden die Skripte vor allem heimlich

eingesetzt. So wurden schon Cloud-Services von renommierten Unternehmen wie Tesla oder bekannte Persönlichkeiten der Webseite von wie der Fussballer Cristiano Ronaldo, davon betroffen.

Coinhive macht Cryptojacking einfach, indem es einen einbettungsfähigen «JavaScript (WebAssembly)»-Code anbietet, der die CPU des Website-Besuchers für die Generierung von Monero verwendet. Monero benötigt dazu keine Hallen voller Rechner, sie kann auf normalen Hardware-Plattformen generiert werden, was lediglich eine normale CPUs voraussetzt. Smartphones und normale PCs reichen dafür völlig aus. Monero legt zudem einen hohen Wert auf die Privatsphäre. Während bei Bitcoin jeder jede Transaktion verfolgen kann, werden sie mit Monero verschlüsselt und können nicht öffentlich nachvollzogen werden - wer damit handelt, bleibt anonym.

Kleiner Parasit, grosse Wirkung

Die Folgen von Cryptojacking sind nicht zu unterschätzen! Der Schaden kann sich unmittelbar finanziell auswirken, wenn die Cryptomining-Software z.B. die Cloud-Infrastrukturen infiziert. Für Unternehmen besteht dabei im besten Fall die Gefahr, dass die übermässige Nutzung der Cloud-Ressourcen dabei die Stromrechnung in die Höhe treibt, im schlimmsten Fall wird die Produktivität und Leistung der Rechenzentren erheblich beeinträchtigt oder dieses komplett stillgelegt – was einen immensen Schaden bedeutet würde. Meistens konsumiert die Malware bis zu 100 % CPU Leistung auf den Systemen. Batterien können unter Umständen überhitzen und entsprechende Geräte im schlimmsten Fall unbrauchbar machen. Systeme können so komplett ausbrennen bzw. in kürzester Zeit erheblich altern.

Cryptojacking auf die Spur kommen und abwehren

Ähnlich wie Ransomware kann Cryptojacking auch Unternehmen treffen, deren IT-Systeme in gut abgesichert sind. Das Aufspüren eines Cryptojackings kann sehr diffizil sein, insbesondere wenn nur wenige Systeme kompromittiert wurden. Ein ganzheitlicher Ansatz der auf Prävention und Erkennung ausgerichtet ist, ist nötig um den Schutz von Endpunkten, Netzwerk, Servern und Clouds zu verbessern.

Was kann man tun?

Trainieren Sie Ihren Help Desk auf Cryptojacking-Warnzeichen. Ein Anstieg von Reklamationen über mangelnde Performance kann ein erster Hinweis sein.

Rollen Sie eine Network-Monitoring-Lösung aus: Was alle Cryptomining Malware gemeinsam haben, ist der Fakt, dass sie permanent nach aussen kommunizieren und so neue Hashwerte erhalten um diese berechnen zu können. Sie kommunizieren mit den Control Servern der Angreifer, was an den DNS Requests erkennbar ist. Allerdings haben nur wenige Unternehmen mit Netzwerk-Monitoring-Tools auch die nötigen Fähigkeiten, um die richtigen und wichtigen Infos aus der Datenanalyse ziehen zu können.

Verwenden Sie einen entsprechenden Endpoint-Schutz, welcher nicht nur auf bekannte Muster prüft, sondern via Machine Learning und AI Technologien verhaltensbasiert reagieren kann. Cisco Umbrella stellt einen zusätzlichen Schutz dar, welcher innerhalb von Minuten etabliert werden kann.

Weitere empfohlene Massnahmen:

- Integrieren Sie die Bedrohung durch Cryptojacking in Ihr Security Awareness Training.
- Blockieren Sie Skripte, die über Webseiten ausgeliefert werden.
- Aktualisieren Sie Ihre Browser-Erweiterungen.
- Statten Sie Webbrowser mit Adblockern oder Anti-Cryptomining-Erweiterungen aus.
- Halten Sie Ihre Webfilter Tools auf dem neuesten Stand.
- Halten sie Ihre Server/Clients durch Patche auf dem neuesten Stand.

ISPIN Cyber Defense Service

Die Fachspezialisten der ISPIN stehen Ihnen gerne mit Rat und ausgefeilten Cyber Defense Services zur Verfügung.

Kontaktieren Sie uns für ein persönliches Gespräch.