Cato Networks

17.08.2021 – 14:31 Uhr

Der SASE-Bericht von Cato Networks stellt fest, dass die Risikobewertung von Unternehmen durch Amazon Sidewalk beeinträchtigt wird; Geräte-ID durch neuartige Verwendung von Houdini-Malware gefährdet

Tel Aviv, Israel (ots/PRNewswire) -

Dark-Web-Cloud-Dienste erleichtern das Fälschen von Geräteidentitäten und helfen Angreifern, in Unternehmen einzudringen, die durch ZTNA-Richtlinien (Zero-Trust Network Access) geschützt sind. Der Bericht stellt außerdem fest, dass die Risikobewertung durch Amazon Sidewalk und andere Verbraucheranwendungen beeinträchtigt wird

Cato Networks, der Anbieter der weltweit ersten SASE-Plattform, gab heute die Ergebnisse seiner vierteljährlichen Analyse globaler Unternehmensnetzwerke bekannt. *Der* Cato Networks SASE Threat Research Report Q2, 2021analysierte 263 Milliarden Netzwerkflüsse in Unternehmen zwischen April und Juni 2021. Cato-Forscher zeigten eine neuartige Verwendung von Houdini-Malware, um das Spoofing eines Geräts zu fördern. Der Bericht dokumentiert auch, wie Amazon Sidewalk und andere Verbraucheranwendungen in vielen Unternehmensnetzwerken betrieben werden, wodurch eine effektive Risikobewertung untergraben wird.

"Die Bewertung von Cybersecurity-Risiken basiert sowohl auf der Sichtbarkeit von Bedrohungen als auch auf der Sichtbarkeit dessen, was im Netzwerk des Unternehmens geschieht", sagt Etay Maor, Senior Director of Security Strategy bei Cato Networks. "Die Grenzen zwischen dem Heimbüro und dem Unternehmensnetzwerk verschwimmen - immer mehr Geräte und Anwendungen finden ihren Weg in das Unternehmensnetzwerk, aber nicht unbedingt in die Risikobewertung des Unternehmens."

Houdini nutzt die Netzwerkebene aus, um Informationen zur Gerätekonfiguration zu exfiltrieren

Jahrelang haben sich Unternehmen bei der Authentifizierung von Benutzern auf die Geräteidentität verlassen. In jüngerer Zeit wurde bei der Entwicklung von ZTNA- und SASE-Architekturen gefordert, die Geräte-ID (zusätzlich zur Benutzeridentität und zum Standort) zu verwenden, um über die Zugriffsrechte der Benutzer auf Unternehmensressourcen zu entscheiden. Das Spoofing von Geräte-IDs hat für Angreifer oberste Priorität, wobei sie sich von einfachen Punktlösungen zu Cloud-basierten Diensten entwickelt haben. Daher ist die Überprüfung der Geräteidentifikation für eine starke Benutzerauthentifizierung von entscheidender Bedeutung.

Unsere Untersuchungen deuten darauf hin, dass das Spoofing von Geräteidentitäten in Zukunft noch viel häufiger vorkommen wird. Houdini ist ein bekannter Remote-Access-Trojaner (RAT), aber unsere Untersuchungen zeigen, dass diese spezielle Anwendung neu ist. Houdini exfiltrierte Daten innerhalb des User-Agent-Feldes, eine Vorgehensweise, die von älteren Sicherheitssystemen oft nicht erkannt wird. Die Cato Research Labs konnten solche Bedrohungen nur durch eine Kreuzkorrelation von Sicherheits- und Netzwerkinformationen identifizieren.

Spoofing-as-a-Service-Angebote, bei denen Cybercrime-Foren virtuelle oder physische Maschinen auf der Grundlage bestimmter Anforderungen für Angreifer bereitstellen, um einen Angriff zu starten. "Mit dem Angebot von Cyberkriminellen ist eine schwer zugängliche Lösung nun weit verbreitet", sagt Maor. "Die Hürde für Angriffe auf Unternehmen ist niedriger - das ermöglicht und motiviert Neueinsteiger im Bereich der Cyberkriminalität." Weitere Informationen über Spoofing-as-a-Service und seine Auswirkungen finden Sie in diesem Blog

Amazon Sidewalk, Verbraucheranwendungen untergraben die Risikobewertung von Unternehmen

Darüber hinaus wurde in dem Bericht festgestellt, dass die rasche Umstellung auf die Arbeit von zu Hause aus und die Einführung von Bring-your-own-device die Grenzen zwischen beruflichen und privaten Netzwerken verwischt haben. Cato Research Labs fand Hunderttausende von Sidewalk-Flows, wobei einige Unternehmen Hunderte solcher Geräte besitzen. "Wie kann man das Unternehmensrisiko einschätzen, wenn man nicht weiß, welche Geräte und Anwendungen sich tatsächlich im Netzwerk befinden?", fragt Maor.

Den vollständigen Bericht finden Sie unterhttps://go.catonetworks.com/Q221-SASE-Threat-Research-Report.html

Informationen zu Cato Networks

Cato ist die weltweit erste SASE-Plattform, die SD-WAN und Netzwerksicherheit in einem globalen, Cloud-nativen Service zusammenführt. Cato optimiert und sichert den Anwendungszugang für alle Benutzer und Standorte. Mit Cato können Kunden problemlos von MPLS auf SD-WAN migrieren, die Konnektivität zu On-Premises- und Cloud-Anwendungen optimieren, überall einen sicheren Internetzugang für Zweigstellen ermöglichen und Cloud-Rechenzentren und mobile Benutzer nahtlos in das Netzwerk mit einer Zero-Trust-Architektur integrieren. Mit Cato sind das Netzwerk und Ihr Unternehmen auf alles vorbereitet, was als nächstes kommt.