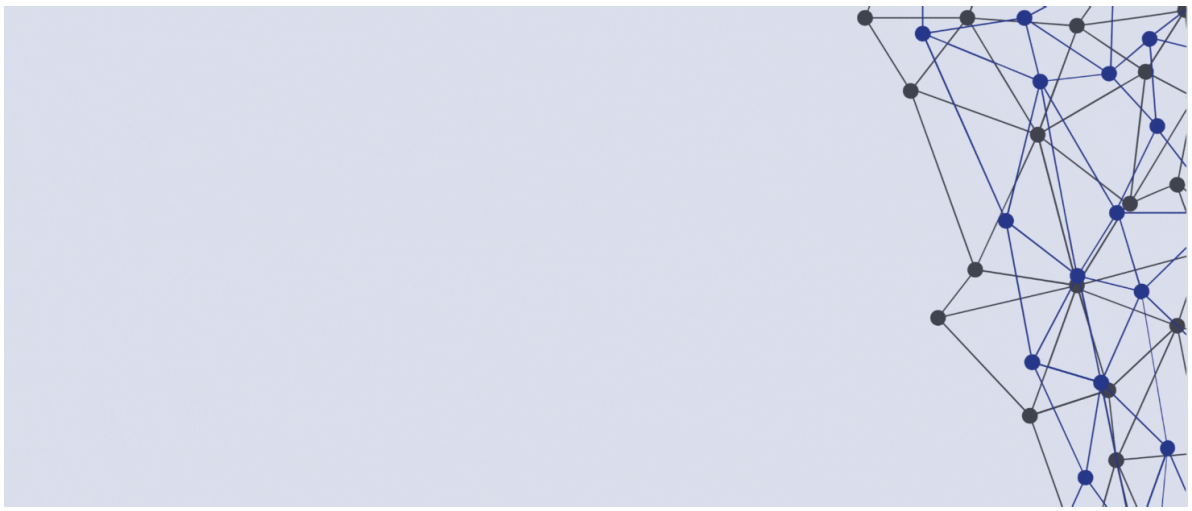
thedefensepost.com

Five Eyes Warns of Russian Hackers Targeting Cloud-Based Networks

Rojoef Manuel

3–4 Minuten



Das UK National Cyber Security Center (NCSC) und die Five Eyes Alliance haben eine Empfehlung zu "evolvierenden Taktiken" russischer Hacker veröffentlicht, um Cloud-basierte Organisationen anzugreifen.

Im Rahmen der Untersuchung wurden Cyber-Akteure, die mit dem russischen ausländischen Geheimdienst (SVR) in Verbindung stehen, gesehen, wie sie ihre Methoden anpassen, um die wachsende Verschiebung der Nutzer von physischen Infrastrukturen zu virtuellen oder Cloud-basierten Netzwerken nachzuholen.

SVR-gestützte Cyber-Akteure erlangten im Jahr 2020 Bekanntheit, weil sie die Lieferkette eines IT-Monitoring-Softwareanbieters und die Fähigkeiten von Organisationen die an der Entwicklung von sind haben.

Aktualisierungsansatz

Die Dokumentation, die von der britischen Regierung in Partnerschaft mit Kanada, Australien, Neuseeland und den USA erstellt wurde, identifizierte die APT29-Cybergruppe, die mit den Aktivitäten verbunden ist.

NCSC und seine Kollegen schrieben, dass Sektoren, die zuvor ins Visier genommen wurden, einschließlich Wissenschaft, Gesundheitswesen und Think Tanks, allmählich von "traditionellen Zugangsmitteln" in Cloud-gehostete Umgebungen übergegangen sind.

Als Reaktion darauf aktualisierte die Gruppe ihren Ansatz in den letzten 12 Monaten, indem sie von Systemen ausgegebene Token und Benutzerkonten gestohlen hat.

Auf diesen Prozess folgen die Einschreibung von nicht autorisierten Geräten unter der Cloud-Umgebung des Ziels sowie Passwortänderungen und Brute-Forceing, die aufgrund der schwachen Passwörter des Opfers und des Fehlens zusätzlicher Verifizierungsschritte oft erfolgreich sind.

Der durch diese Operation gewonnene Zugriff ermöglicht es Akteuren, andere "hochentwickelte Fähigkeiten" einzusetzen, um das Ziel weiter zu infiltrieren.

„Bewusstheit schärfen“

Das NSCS-Update besagte, dass sich Cyberangriffe des SVR bereits von den genannten Sektoren auf zusätzliche Organisationen wie Strafverfolgungsbehörden, Luftfahrt, lokale und staatliche Räte und Bundesbehörden ausgeweitet haben.

"Wir sind entschlossen in unserem Engagement, bösartige Cyberaktivitäten aufzudecken, einschließlich der Sensibilisierung für Veränderungen im Verhalten von Gruppen, die sich hartnäckig an Großbritannien richten", sagte Paul Chichester, Direktor von NCSC **Paul Chichester**statedOperations.

"Die NCSC fordert die Organisationen auf, sich mit den Informationen und der Minderungsberatung innerhalb der Beratung vertraut zu machen, um ihre Netzwerke zu verteidigen."