Illegaler Zugang zu Unternehmensdaten: Cookie-Klau ist zunehmend im Trend

- *Cyberkriminelle nutzen gestohlene Cookies, um Multi-Faktor-Authentifizierungen zu umgehen und Zugriff auf Unternehmensressourcen zu erhalten*
- *Mit gestohlenen Cookies können sich Angreifer als rechtmäßige Benutzer ausgeben und frei im Unternehmens-Netzwerk bewegen.*

Wiesbaden, 23. August 2022 – Sophos beschreibt im neuesten X-Ops Report "Cookie stealing: the new perimeter bypass", dass Cyberkriminelle zunehmend gestohlene Session-Cookies nutzen, um die Multi-Faktor-Authentifizierung (MFA) zu umgehen und Zugriff auf Unternehmensressourcen zu erhalten. In einigen Fällen ist der Cookie-Diebstahl eine gezielte Attacke, bei der Cookie-Daten von kompromittierten Systemen ausgelesen werden. Dabei nutzen die Kriminellen legitime ausführbare Dateien, um ihre Aktivitäten zu verschleiern.

Sobald sie mithilfe der Cookies einen Zugang zu web- oder cloudbasierten oder Unternehmens-Ressourcen haben, können sie diese für weitere Angriffe nutzen. Dazu gehören beispielsweise die Kompromittierung von E-Mails oder Social Engineering, um zusätzliche Systemzugänge zu ergaunern oder sogar für die Änderung von Daten oder Quellcode-Repositories zu sorgen.

„Im vergangenen Jahr haben wir beobachtet, dass Cyberkriminelle vermehrt auf Cookie-Diebstahl zurückgreifen, um die zunehmende Verbreitung von MFA zu umgehen. Sie nutzen neue und verbesserte Malware – etwa Raccoon Stealer – um den Diebstahl von Authentifizierungs-Cookies, auch bekannt als Access Tokens, zu vereinfachen", sagt Sean Gallagher, Principal Threat Researcher bei Sophos. „Wenn Angreifende im Besitz von Session-Cookies sind, können sie sich frei in einem Netzwerk bewegen."

An der Authentifizierung vorbei: „Pass-the-Cookie"-Angriffe
Sitzungs- oder Authentifizierungs-Cookies sind eine bestimmte Art von Cookie, die von einem Webbrowser gespeichert werden, wenn sich ein Benutzer bei Webressourcen anmeldet. Sobald Cyberkriminelle in ihren Besitz gelangen, können sie einen "Pass-the-Cookie"-Angriff durchführen, bei dem sie das Zugriffstoken in eine neue Web-Sitzung einschleusen und dem Browser vorgaukeln, es melde sich ein authentifizierter Benutzer an. Damit ist keine weitere Authentifizierung mehr erforderlich. Da bei der Verwendung von MFA auch ein Token erstellt und in einem Webbrowser gespeichert wird, kann derselbe Angriff verwendet werden, um diese zusätzliche Authentifizierungsebene zu umgehen. Erschwerend kommt hinzu, dass viele legitime webbasierte Anwendungen langlebige Cookies anlegen, die selten oder nie ablaufen; Einige Cookies werden nur dann gelöscht, wenn sich der Benutzer ausdrücklich vom Dienst abmeldet.

Dank Malware-as-a-Service wird es selbst für eher unerfahrene Cyberkriminelle immer einfacher, in das lukrative Geschäft mit dem Diebstahl von Zugangsdaten einzusteigen. Sie müssen beispielsweise nur eine Kopie eines Trojaners wie Raccoon Stealer kaufen, um Daten wie Passwörter und Cookies in großen Mengen zu sammeln und können sie dann auf kriminellen Marktplätzen wie Genesis anbieten. Andere Kriminelle in der Angriffskette, wie z. B. Ransomware-Betreiber, können diese Daten dann kaufen und durchforsten, um alles, was sie für ihre Angriffe als nützlich erachten, zu nutzen.

Der Cookie-Diebstahl wird immer strategischer
Bei zwei der jüngsten Vorfälle, die Sophos untersuchte, verfolgten die Angreifenden hingegen einen gezielteren Ansatz. In einem Fall verbrachten sie Monate im Netzwerk des Zielunternehmens und sammelten Cookies des Microsoft Edge Browsers. Die erste Kompromittierung erfolgte über ein Exploit-Kit. Anschließend nutzten sie eine Kombination aus Cobalt-Strike- und Meterpreter-Aktivitäten, um über ein legitimes Compiler-Tool die Zugriffstoken abzugreifen. In einem anderen Fall nutzten die Angreifenden eine legitime Microsoft-Visual-Studio-Komponente, um eine bösartige Malware abzusetzen, die eine Woche lang Cookie-Dateien abfing.

„Während wir in der Vergangenheit massenhaften Cookie-Diebstahl beobachten konnten, gehen Cyberkriminelle jetzt gezielt und präzise vor, um Cookies zu stehlen. Da ein großer Teil des Arbeitsplatzes inzwischen webbasiert ist, gibt es keine Grenzen für die bösartigen Aktivitäten, die Angreifer:innen mit gestohlenen Sitzungscookies durchführen können. Sie können Cloud-Infrastrukturen manipulieren, geschäftliche E-Mails kompromittieren, andere Mitarbeitende zum Herunterladen von Malware überreden oder sogar Code für Produkte umschreiben. Die einzige Grenze ist ihre eigene Kreativität", so Gallagher. „Erschwerend kommt hinzu, dass es keine einfache Lösung gibt. Zwar können Dienste beispielsweise die Lebensdauer von Cookies verkürzen, was jedoch bedeutet, dass sich die Benutzer:innen häufiger neu authentifizieren müssen. Da Angreifer:innen legitime Anwendungen nutzen, um Cookies abzugreifen, müssen Unternehmen die Erkennung von Malware mit einer Verhaltensanalyse kombinieren."

Um mehr über den Diebstahl von Sitzungscookies zu erfahren und darüber, wie Cyberkriminelle diese Technik ausnutzen, um schädliche Aktivitäten auszuführen, lesen Sie den vollständigen Report "Cookie Stealing: the new perimeter bypass" auf Sophos.com.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Über Sophos
Sophos ist ein weltweit führender Anbieter von Next Generation Cybersecurity und schützt mehr als 500.000 Unternehmen und Millionen von Anwendern in mehr als 150 Ländern vor den modernsten Cyberbedrohungen. Basierend auf Threat Intelligence, KI und maschinellem Lernen aus den SophosLabs und von SophosAI bietet Sophos ein breites Portfolio an fortschrittlichen Produkten und Services, um Anwender, Netzwerke und Endpoints vor Ransomware, Malware, Exploits, Phishing und einer Vielzahl anderer Cyberattacken zu schützen. Sophos bietet mit Sophos Central eine einzige, integrierte und cloudbasierte Management-Konsole. Sie ist das Herzstück eines anpassungsfähigen Cybersecurity-Ökosystems mit einem zentralen Data Lake, der eine Vielzahl offener API-Schnittstellen bedient, die Kunden, Partnern, Entwicklern und anderen Cybersecurity-Anbietern zur Verfügung stehen. Sophos vertreibt seine Produkte und Services über Partner und Managed Service Provider (MSPs) weltweit. Der Sophos-Hauptsitz ist in Oxford, U.K. Weitere Informationen unter http://www.sophos.de/.

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de