Neuer Sophos-Report:
Weit verbreiteter Raccoon-Stealer nutzt auch Telegram für Crypto-Mining und Crypto-Diebstahl

Erstmals auch Chat-Dienst Telegram für die Befehls- und Kontrollkommunikation eingespannt.

Der Raccoon-Stealer wird über Spam und gecrackte Dropper-Installer verbreitet und zudem mit Ransomware und anderer bösartigen Malware kombiniert.

Wiesbaden, 5. August 2021 – Sophos hat die neue Studie "Trash Panda as a Service" Raccoon-Stealer Steals Cookies, Cryptocoins and More" veröffentlicht. Thema ist ein Stealer, der als Raubkopie getarnt Kryptowährungen und Informationen erbeutet und gleichzeitig schädliche Inhalte wie Kryptominer auf das Zielsystemen einschleust.

„Da ein Großteil des täglichen und beruflichen Lebens heute von web-basierten Diensten abhängt, haben es Cyberkriminelle mit ihrer Malware zunehmend auf gespeicherte Web-Zugangsdaten abgesehen, denn diese bieten ihnen Zugriff auf viel mehr im Vergleich zu gestohlenen Passwort-Hashes", sagt Sean Gallagher, Senior Threat Researcher bei Sophos.

Raccoon-Stealer nimmt jetzt auch Krypto-Wallets ins Visier

„Die von uns beobachtete Cybercrime-Kampagne zeigt, dass der Raccoon-Stealer sowohl Kennwörter und Cookies als auch Autofill-Texte von Websites stiehlt – einschließlich Kreditkartendaten und andere persönliche Informationen, die von einem Browser gespeichert werden können. Dank eines kürzlichen Updates der sogenannten Clipper-Malware, die Daten in der Zwischenablage oder die Zielinformationen für eine Kryptowährungstransaktion ändert, zielt Raccoon-Stealer jetzt auch auf Krypto-Wallets ab. Durch das Update lassen sich Systeme mit zusätzlicher Malware infizieren oder Dateien abrufen und laden. Das sind eine Menge Optionen, die Cyberkriminelle leicht zu Geld machen können – mit einem Dienst, der der sie lediglich 75 Dollar pro Woche an Miete kostet", so Gallagher weiter.

Telegram als neue und zusätzliche Taktik

Raccoon-Stealer wird normalerweise über Spam-E-Mails verbreitet. In der von Sophos untersuchten Angriffsserie wird er jedoch über Dropper verbreitet, den die Betreiber als gecrackte Software-Installationsprogramme getarnt haben. Dropper kombinieren den Raccoon-Stealer mit zusätzlichen Angriffswerkzeugen, darunter schädliche Browser-Erweiterungen, YouTube-Klickbetrug-Bots und Djvu/Stop, eine Ransomware, die vor allem Privatanwender im Visier hat. Die Kriminellen hinter der Raccoon-Stealer-Kampagne nutzten den Sophos-Forschungsergebnissen zufolge erstmals auch den Chat-Dienst Telegram für die Befehls- und Kontrollkommunikation.

„Informationsdiebe spielen eine wichtige Rolle im Ökosystem der Cyberkriminalität. Sie bieten einen schnellen Return on Investment und ermöglichen einen einfachen und billigen Einstiegspunkt für größere Angriffe", sagt Gallagher. „Cyberkriminelle verkaufen gestohlene Identitätsdaten auf Darknet-Plattformen, so dass andere Angreifer, darunter Ransomware-Betreiber oder Initial Access Broker, sie für ihre eigenen kriminellen Absichten nutzen können. Alternativ nutzen die Angreifer die Anmeldedaten für weitere Angriffe auf andere Benutzer auf derselben Plattform. Es besteht eine ständige Nachfrage nach gestohlenen Benutzer- und Anmeldedaten für den Zugang zu legitimen Diensten, um ohne großen Aufwand weitere Malware zu verbreiten. Datendiebe mögen als eine vergleichsweise geringere Bedrohung erscheinen, sie sind es aber nicht."

Schutz für Unternehmen und Privatpersonen
Für Unternehmen empfiehlt Sophos, alle Konten von Online-Diensten für die Kommunikation und Zusammenarbeit am Arbeitsplatz durch Multi-Faktor-Authentifizierung (MFA) zu schützen. Zudem sollte sichergestellt sein, dass die Computer aller Mitarbeiter über einen aktuellen Malware-Schutz verfügen. Sophos Intercept X schützt Endpoints durch die Erkennung von Aktionen und Verhaltensweisen von Malware wie Raccoon-Stealer. Zudem überprüft die Security-Lösung den Speicher auf verdächtige Aktivitäten und schützt vor dateiloser Malware.

Privatpersonen rät Sophos zu einer Sicherheitslösung auf allen Geräten, die sie und ihre Familien für Online-Kommunikation und Spiele nutzen. Sophos Home schützt private Computer (Windows und Mac) mit einem mehrschichtigen Ansatz und auf Basis der Technologie der Unternehmensprodukte zuverlässig vor Malware und Cyberbedrohungen. Es ist zudem empfehlenswert, das Herunterladen und Installieren von nicht lizenzierter Software von jeder Quelle zu vermeiden.

Weitere Informationen über Raccoon-Stealer und andere Cyber-Bedrohungen finden Sie im Blog SophosLabs Uncut.

Weiterführende Informationen:
- Taktiken, Techniken und Verfahren (TTPs) der unterschiedlichen Arten von Ransomware, finden Sie im SophosLab Uncut
- Informationen über das Verhalten von Angreifern, Incident Reports sowie Tipps für Security-Profis finden Sie auf Sophos News SecOps
- Um Ransomware-Angriffe zu stoppen, lesen Sie die fünf Frühindikatoren für einen Angreifer
- Erfahren Sie mehr über den Sophos Rapid Response Service, der Angriffe rund um die Uhr eindämmt, neutralisiert und untersucht
- Die vier besten Tipps zur Reaktion auf einen Sicherheitsvorfall von Sophos Rapid Response und dem Managed Threat Response Team

Neu: 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 Verbrauchern 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 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