Der Feind in meinem Chat – Boomende Kommunikationsplattform Discord lockt Cyberkriminelle in Scharen an

- *Malware nicht nur für PCs, sondern auch für Android-Geräte gefunden*
- *SophosLabs-Untersuchung zeigt, dass das Volumen bösartiger Inhalte auf Discord im Jahresvergleich um 140 % angestiegen ist*
- *Nutzer werden mit prominenten Spielen wie Minecraft, Fortnite, oder Grand Theft Auto geködert*

Erfolg macht sexy – das sehen augenscheinlich auch Cyberkriminelle so. In einer neuen Untersuchung haben die SophosLabs herausgefunden, dass Discord, ein momentan sehr erfolgreicher Dienst für Sprach-, Video- und Textkommunikation mit weltweit nach eigenen Angaben über 150 Millionen Nutzern, zunehmend als Malware-Verbreitungsplattform genutzt wird. So belegen die Sophos-Telemetriedaten, dass die Anzahl der URLs, die Malware im Content Management Network (CDN) von Discord hosten, in den letzten zwei Monaten im Vergleich zum Vorjahreszeitraum um 140 % gestiegen ist. Die Studi „Malware increasingly targets Disord for abuse“ basiert auf einer detaillierten Analyse von mehr als 1.800 bösartigen Dateien, die auf dem Discord-CDN erkannt wurden und zeigt auf, wie Cyberkriminelle die beliebte Plattform nutzen, um persönliche Informationen zu stehlen und andere Malware verbreiten, einschließlich eigentlich ausrangierter Ransomware, die für Sabotage- und Denial-of-Service-Attacken genutzt wird.

„Discord bietet ein dauerhaftes, hochverfügbares und globales Verteilungsnetzwerk für Malware-Betreiber, sowie ein Messaging-System, das die Kriminellen ohne großen Aufwand in Befehls- und Kontrollkanäle für ihre illegalen Aktivitäten umwandeln können“, so Sean Gallagher, Senior Threat Researcher bei Sophos. „Die riesige Benutzerbasis von Discord bietet eine ideale Umgebung für den Diebstahl persönlicher und Anmeldeinformationen durch Social Engineering.“

„Diese Betrügereien sind nicht harmlos“, so Gallagher weiter. „Wir haben eine Malware gefunden, die private Bilder von der Kamera eines infizierten Geräts stehlen kann, sowie Ransomware aus dem Jahr 2006, die die Angreifer wiederbelebt haben, um sie als ‚Mischiefware‘ zu verwenden. Diese Malware-Gattung verweigert Opfern den Zugriff auf ihre Daten, aber es gibt keine Lösegeldforderung und keinen Entschlüsselungsschlüssel wie bei Ransomware.“

Dabei sind nicht nur Privatnutzer im Fokus. Der Sophos-Report legt nahe, dass den Cyberkriminellen durchaus bewusst ist, dass Unternehmen die Discord-Plattform zunehmend für interne oder Community-Chats nutzen. Diese Entwicklung bietet Angreifern eine neue und potenziell lukrative Zielgruppe, insbesondere wenn Sicherheitsteams nicht immer den mit Transport Layer Security verschlüsselten TLS-Verkehr von und zu Discord überprüfen und damit potenziell gefährliche Aktivitäten nicht frühzeitig erkennen können.

Die wichtigsten Ergebnisse des Sophos-Labs-Reports im Überblick:

1. Die Malware wird oft als spielbezogene Tools und Cheats getarnt – häufig für beliebte Online-Spiele wie Minecraft, Fortnite, Roblox oder Grand Theft Auto. Die Forscher fanden auch einen Köder, der Spielern die Möglichkeit bot, ein Spiel in der Entwicklung zu testen.
2. Informationsdiebstahl ist die häufigste Bedrohung und macht mehr als 35% der aufgedeckten Malware aus. Die Sophos-Forscher fanden mehrere Malwaretypen, die Passwörter hacken oder exfiltrieren. So z.B. die modifizierte Version eines Minecraft-Installers, der zusätzlich zur Bereitstellung des Spiels einen „Erweiterung“ namens „Saint“ installiert. Dabei handelt es sich allerdings um sogenannte Spyware, die Tastenanschläge und Screenshots sowie Bilder direkt von der Kamera erfassen kann.

3. Die SophosLabs fanden auch Android-Malware-Pakete, die Backdoors oder Dropper (eigenständig ausführbare Programm-Dateien, die z.B. eine Malware aktivieren) auf dem Smartphone installieren sowie Finanz-Malware, die den Zugriff auf Online-Bankkonten und Kryptowährungen stehlen soll.

Auf Discord sicher bleiben

„Discord-Benutzer, egal ob privat oder geschäftlich und wofür sie die Plattform verwenden, sollten ähnlich wie beim Email-Postfach wachsam gegenüber der Bedrohung durch bösartige Inhalte bleiben, und es nicht einfach dem Anbieter überlassen, verdächtige Dateien zu identifizieren und zu entfernen“, so Gallagher. „Wir empfehlen außerdem, eine Sicherheitslösung wie beispielsweise Sophos Home auf Privatgeräten zu installieren, um sich vor Malware- und anderen Cyberbedrohungen zu schützen.“

Für Unternehmen, die Discord für Chat und Zusammenarbeit am Arbeitsplatz verwenden, empfiehlt sich die Verwendung von Multi-Faktor-Authentifizierung (MFA). Außerdem sollte sichergestellt sein, dass alle Mitarbeiter über einen aktuellen Malware-Schutz auf ihren Geräten verfügen – vor allem jene, die sie für den Zugriff auf Remote-Kollaborationsplattformen während der Arbeit verwenden. Darüber hinaus sollten IT-Sicherheitsteams den Datenverkehr von einem Online-Cloud-Dienst aufgrund der vertrauenswürdigen Natur oder Legitimität des Dienstes selbst niemals als von Natur aus als „sicher“ betrachten. Cyberkriminelle könnten sich überall verstecken.

Alle technischen Details und eine weitere Auflistung der verbreiteten Malware-Typen stehen im kompletten Report „Malware increasingly targets Disord for abuse“ zur Verfügung.

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

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