CryptoRom-Betrüger erweitern ihren Werkzeugkasten um KI-Chat-Tools wie ChatGPT und erfundene Hacks auf Kryptokonten

Sophos veröffentlich neuen Bericht zu „pig butchering" Betrugsmaschen. Demnach setzen Cybekriminelle nun auf KI-Unterstützung für romantische Chats und erfinden Hackerangriffe auf Kryptokonten, um nochmals mehr Geld zu ergaunern. Zusätzlich ist es gelungen sieben neue Fake Apps für Krypto-Investitionen in die offiziellen Stores einzuschleusen.

Wiesbaden, 2. August 2023 – Sophos hat heute neue Erkenntnisse über CryptoRom-Betrügereien veröffentlicht. Hierbei handelt es sich um eine Untergruppe der so genannten "pig butchering" (shā zhū pán) Betrugsmaschen, die darauf abzielen, Nutzer von Dating-Apps dazu zu bringen, in gefälschte Kryptowährungs-Fonds zu investieren.
Der heute veröffentlichte Bericht "Sha Zhu Pan Scam Uses ChatGPT to Target iPhone and Android Users" beschreibt die Einzelheiten neuen Vorgehens. Seit Mai hat Sophos X-Ops hierfür beobachtet, wie die Betrüger ihre Techniken verfeinern, indem sie ein KI-Chat-Tool wie beispielsweise ChatGPT in ihre Werkzeugsammlung aufnehmen. Auch die kriminellen Einschüchterungstaktiken sind erweitert worden: den Opfern wird mitgeteilt, dass ihre Kryptokonten gehackt wurden und nun noch mehr Geld benötigt wird. Zusätzlich hat Sophos X-Ops entdeckt, dass die Betrüger sieben neue gefälschte Kryptowährungs-Investitions-Apps in den offiziellen Apple App Store und in Google Play Store eingeschleust haben, was die Zahl der potenziellen Opfer abermals erhöht.

Im Jahr 2022 verursachte Anlagebetrug die höchsten Verluste unter allen von der Öffentlichkeit an das Internet Crime Complaint Center (IC3) des FBI gemeldeten Betrugsfällen und belief sich auf insgesamt 3,31 Milliarden US-Dollar. Betrügereien im Zusammenhang mit Kryptowährungen, einschließlich des sogenannten "pig butchering", machten den Großteil dieser Betrugsfälle aus und führten zu einem Anstieg von 183 % gegenüber 2021 auf 2,57 Milliarden US-Dollar an gemeldeten Verlusten im letzten Jahr.

Sophos X-Ops erfuhr erstmals von CryptoRom-Betrügern, die das KI-Chat-Tool, höchstwahrscheinlich ChatGPT einsetzen, als ein betroffenes Opfer sich an das Team wandte. Nachdem der Betrüger den Kontakt zum Opfer über die App "Tandem" aufgenommen hatte – eine App die Sprachlernende mit Muttersprachlern verbindet, die auch als Dating-App genutzt wird – überzeugte er das Opfer, das Gespräch auf WhatsApp fortzusetzen. Das Opfer wurde misstrauisch, als es eine ausführliche Nachricht erhielt, die offensichtlich teilweise von einem KI-Chat-Tool mit einem großen Sprachmodell (LLM) geschrieben wurde.

ChatGPT für den romantischen Chat in fremden Sprachen
"Seit OpenAI die Veröffentlichung von ChatGPT angekündigt hat, gab es breite Spekulationen, dass Cyberkriminelle das Programm für ihre eigenen bösartigen Aktivitäten nutzen könnten. Wir können jetzt sagen, dass dies zumindest im Fall von 'pig butchering' Betrügereien tatsächlich geschieht. Eine der Hauptherausforderungen für Betrüger bei CryptoRom-Betrügereien besteht darin, überzeugende und anhaltende romantische Gespräche mit ihren Zielpersonen zu führen. Diese Gespräche werden hauptsächlich von 'Keyboardern' geführt, die vornehmlich in Asien ansässig sind und eine Sprachbarriere haben. Die Verwendung von einem Tool wie ChatGPT kann eine effizientere und effektivere Methode sein, um diese Gespräche aufrechtzuerhalten und die Betrügereien weniger arbeitsintensiv und authentischer zu gestalten. Es ermöglicht den 'Keyboardern' auch, gleichzeitig mit mehreren Opfern zu interagieren", sagt Sean Gallagher, Principal Threat Researcher bei Sophos.

Erfundene Hacks auf Krypokonten
Sophos X-Ops hat zudem eine neue Betrugstaktik der Betrüger entdeckt, bei der zusätzliches Geld erpresst wird. Traditionell werden Opfer von CryptoRom-Betrügereien, wenn sie versuchen, ihre "Gewinne" einzufordern, von den Betrügern informiert, dass sie 20 % Steuern auf ihre Gelder zahlen müssen, bevor die Auszahlungen vorgenommen werden können. Kürzlich enthüllte ein Opfer jedoch, dass die Betrüger nach Zahlung der "Steuern" für die Auszahlung des Geldes nunmehr behaupteten, dass die Gelder "gehackt" worden seien und dass für eine Ausschüttung eine weitere Einzahlung von 20 % der Summe notwendig sei.

Mit derselben Technik wie zu Beginn des Jahres: Sieben neue Fake Apps in den offiziellen Stores
Bei weiteren Untersuchungen entdeckte Sophos X-Ops sieben gefälschte Kryptowährungs-Investitions-Apps im offiziellen Google Play Store und Apple App Store. Diese Apps haben scheinbar harmlose Beschreibungen in den App-Stores (zum Beispiel behauptet BerryX, dass es etwas mit Lesen zu tun habe). Sobald die Benutzer die App jedoch öffnen, werden sie mit einer gefälschten Krypto-Trading-Oberfläche konfrontiert.
Um den Überprüfungsprozess im Apple App Store zu umgehen, verwenden die App-Entwickler dieselbe Technik, über die Sophos erstmals im Februar 2023 berichtet hat. Sie reichen die App zur Genehmigung unter Verwendung von legitimen, alltäglichen Webinhalten ein. Sobald die App genehmigt und veröffentlicht wurde, ändern sie den Server, auf dem die App gehostet wird, mit Code für die betrügerische Oberfläche.
Viele dieser sieben neuen Apps verwenden identische Vorlagen und Beschreibungen, was darauf hindeutet, dass dieselben ein oder zwei Betrügerringe die Masche entwickelt haben.

Appell an Nutzer: Seien Sie misstrauisch
"Bevor die CryptoRom-Betrüger in der Lage waren, ihre Apps in den Apple Store zu bringen, mussten sie eine umständliche technische Lösung verwenden, um iOS-Benutzer anzugreifen, was ihre Opfer aufmerksam machen könnte. Jetzt ist es für sie viel einfacher, iPhone-Benutzer ins Visier zu nehmen, was ihre Opfergruppe erweitert. Diese Apps sind auch einfach zu recyceln und wiederzuverwenden. Tatsächlich scheint die BerryX-App in Verbindung mit den gefälschten Apps zu stehen, die wir zu Beginn dieses Jahres entdeckt und blockiert haben. Obwohl wir Google und Apple über diese neuesten Apps informiert haben, ist es wahrscheinlich, dass weitere auftauchen werden. Diese Betrüger sind rücksichtslos. Heute behaupten sie gegenüber den Opfern, dass ihre Konten gehackt wurden, um mehr Geld zu erpressen, aber in Zukunft werden sie wahrscheinlich neue Methoden der Erpressung entwickeln. Die beste Verteidigung gegen 'pig butchering' ist das Bewusstsein für diese Betrugskampagnen. Wir ermutigen Benutzer, die misstrauisch sind oder glauben, Opfer geworden zu sein, uns zu kontaktieren", sagte Gallagher.

Mehr über die neusten Taktiken der CryptoRom-Kriminellen erfahren Sie in dem Bericht "Sha Zhu Pan Scam Uses ChatGPT to Target iPhone and Android Users" auf Sophos.com.

Über Sophos
Sophos ist ein weltweit führender und innovativer Anbieter von fortschrittlichen Cybersecurity-Lösungen, darunter Managed Detection and Response (MDR)- und Incident-Response-Dienste. Das Unternehmen bietet ein breites Portfolio an Endpoint-, Netzwerk-, E-Mail- und Cloud-Sicherheitstechnologien, das bei der Abwehr von Cyberangriffen unterstützt. Als einer der größten auf Cybersecurity spezialisierten Anbieter schützt Sophos mehr als 500.000 Unternehmen und mehr als 100 Millionen Anwender weltweit vor aktiven Angriffen, Ransomware, Phishing, Malware und vielem mehr.
Die Dienste und Produkte von Sophos werden über die cloudbasierte Management-Konsole Sophos Central verbunden und vom bereichsübergreifenden Threat-Intelligence-Expertenteam Sophos X-Ops unterstützt. Die Erkenntnisse von Sophos X-Ops erweitern das gesamte Sophos Adaptive Cybersecurity Ecosystem. Dazu gehört auch ein zentraler Datenspeicher, der eine Vielzahl offener APIs nutzt, die Kunden, Partnern, Entwicklern und anderen Anbietern von Cybersecurity und Informationstechnologie zur Verfügung stehen. Sophos bietet Cybersecurity-as-a-Service für Unternehmen an, die vollständig verwaltete, schlüsselfertige Sicherheitslösungen benötigen. Kunden können ihre Cybersecurity auch direkt mit der Security Operations Platform von Sophos verwalten oder einen hybriden Ansatz verfolgen, indem sie ihre internen Teams mit Sophos Services ergänzen, einschließlich Threat Hunting und Systemwiederherstellung.
Sophos vertreibt seine Produkte über Reseller und Managed Service Provider (MSPs) weltweit. Der Hauptsitz von Sophos befindet sich 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