Fake-Romantik braucht es nicht mehr: Kryptowährungsbetrüger bieten ihr Pig Butchering-Modell weltweit als Serviceleistung an

Sophos X-Ops untersuchte zwei Jahre lang die Machenschaften von Sha-Zhu-Pan-Betrügern und deckt eine zunehmend professionelle Betrugsmasche auf, die Opfer zu falschen Investitionen verleiten soll. Die Entwicklung zeigt dabei einen ähnlichen Verlauf wie bei anderen Angriffsarten: vom Einzelfall hin zu einem lukrativen Geschäftsmodell für verschiedenste Cyberbanden.

Wiesbaden, 5. Februar 2024 – Sophos hat aufgedeckt, wie Sha-Zhu-Pan-Betrüger für ihre vermeintlich auf Romantik zielenden so genannten Pig-Butchering-Betrügereien inzwischen ein Geschäftsmodell nutzen, das dem „Cybercrime-as-a-Service" ähnelt. Dabei verkaufen die Betrüger Sha-Zhu-Pan-Kits im Dark Web auf der ganzen Welt und expandieren so in neue Märkte. Sophos beschreibt diese Operationen (auch bekannt als Pig Buchtering) in dem Artikel „Cryptocurrency Scams Metastasize into New Forms". Die neuen Sets stammen von Banden des organisierten Verbrechens in China und stellen die technischen Komponenten bereit, die für die Umsetzung eines speziellen Pig-Butchering-Programms namens „DeFi savings" benötigt werden. Die Kriminellen stellen DeFi-savings als passive Anlagemöglichkeiten dar, die Geldmarktkonten ähneln. Die Opfer müssen lediglich ihre Krypto-Wallets mit einem Maklerkonto verbinden, in der Erwartung, dass sie mit ihrer Investition beträchtliche Zinsen verdienen werden. In Wirklichkeit fügen die Opfer ihren Krypto-Wallets einem betrügerischen Handelspool für Kryptowährung hinzu, wo sie von Kriminellen geleert werden.

Das Betrugsmodell professionalisiert sich ähnlich wie andere Angriffsarten

„Als das Pig Butchering zum ersten Mal während der COVID-Pandemie auftrat, waren die technischen Aspekte der Betrügereien noch relativ primitiv und es erforderte großen Aufwand, um die Opfer erfolgreich zu täuschen", erläutert Sean Gallagher, Principal Threat Researcher bei Sophos. „Doch die Gauner haben ihre Techniken verfeinert und wir sehen eine ähnliche Entwicklung wie bei Ransomware und anderen Arten von Cyberkriminalität in der Vergangenheit: die Entwicklung eines As-a-Service-Modells. Pig-Butchering-Banden erstellen fertige DeFi-App-Kits, die andere Cyberkriminelle im Dark Web kaufen können. Infolgedessen tauchen in Gebieten wie Thailand, Westafrika und sogar in den USA neue Verbrecherringe auf, die nicht mit chinesischen Gruppen in Verbindung stehen. Wie bei anderen Arten von kommerzieller Cyberkriminalität senken diese Kits die Einstiegshürden für Cyberkriminelle und vergrößern den potentiellen Opferpool erheblich. Im vergangenen Jahr stellte diese Methode bereits ein milliardenschweres Betrugsphänomen dar und wird voraussichtlich in diesem Jahr exponentiell wachsen."

Pig Butchering hat eine steile Karriere genommen

Sophos X-Ops verfolgt seit zwei Jahren die Entwicklung des Pig Butcherings. Bei den ersten Varianten – von Sophos als „CryptoRom" bezeichnet – wurden potenzielle Opfer über Dating-Apps kontaktiert und anschließend dazu gebracht, betrügerische Krypto-Handelsanwendungen von Drittanbietern herunterzuladen.

Im Jahr 2022 fanden die Betrüger Wege, die App-Store-Prüfverfahren zu umgehen, um ihre betrügerischen Apps in den legitimen App Store und Google Play Store zu schleusen. Im selben Jahr tauchte auch ein neues Betrugsmuster auf: gefälschte Kryptowährungshandelspools (Liquidity Mining).

Zwei riesige Pig-Butchering-Ringe mit Sitz in Hongkong und in Kambodscha deckte Sophos X-Ops im Jahr 2023 auf. Diese Banden nutzten legitime Krypto-Handels-Apps und erstellten

Fake-Personen, um Opfer anzulocken. Weitere Untersuchungen ergaben, dass die Gauner ihr Arsenal auch um KI erweiterten.
Ende 2023 spürten Sophos X-Ops eine umfangreiche Liquiditätssuche auf, an der drei verschiedene chinesische organisierte Verbrecherringe beteiligt waren, die es auf fast 100 Opfer abgesehen hatten. Hierbei konnten Sophos X-Ops auch zum ersten Mal die Verfügbarkeit von Betrugskits für das Pig Butchering nachweisen.

Der Höhepunkt: Die Zeiten des aufwendigen Opfer-Umschmeichelns sind passé
Bei den jüngsten von Sophos X-Ops untersuchten Pig-Butchering-Fällen haben die Betrüger alle früheren technologischen Hindernisse beseitigt und den Aufwand für Social Engineering deutlich verringert. Bei dem DeFi-saving-Betrug beteiligen sich die Opfer nun am betrügerischen Krypto-Handel über legitime, bekannte Kryptowährungs-Apps und gewähren den Betrügern (wenn auch unwissentlich) direkten Zugriff auf ihre Geldbörsen. Darüber hinaus können die Betrüger das Wallet-Netzwerk verbergen, das die gestohlenen Kryptowährungen wäscht, was es den Strafverfolgungsbehörden erschwert, den Betrug zu verfolgen.

„Der DeFi-saving-Betrug ist der Höhepunkt der vergangenen zwei Jahre, in denen die Pig-Butchering-Betrüger ihr Vorgehen verfeinert haben. Vorbei sind die Zeiten, in denen die Betrüger ihre Opfer überzeugen mussten, eine App herunterzuladen oder die Kryptowährung selbst in eine gestohlene digitale Geldbörse zu transferieren“, so Gallagher. „Die Gangster haben auch gelernt, wie sie ihre Machenschaften besser vermarkten können. Sie nutzen die Funktionsweise von Liquiditäts-Mining-Pools, um Gelder zu stehlen, indem sie den Opfern erzählen, es handele sich um ein einfaches Anlagekonto. Die Opfer sind so einfacher zur Investition zu bewegen, da die meisten den Handel mit Kryptowährungen nicht verstehen und obendrein alles unter dem Deckmantel vertrauenswürdiger Marken geschieht. Mit anderen Worten: Noch nie war es so einfach, Opfer eines Pig-Butchering-Betrugs zu werden, und noch nie war es so wichtig, sich der Existenz dieser Betrügereien bewusst zu sein und zu wissen, worauf man achten muss.“

Pig-Butchering-Betrug verhindern
Um zu verhindern, Opfer eines Pig-Butchering-Betrugs zu werden, empfiehlt Sophos folgende Maßnahmen:

- Skeptisch gegenüber Fremden sein, die sich über soziale Netzwerke wie Facebook oder per SMS melden. Vor allem dann, wenn sie das Gespräch schnell in einen privaten Messenger wie WhatsApp verlegen wollen.
    - Dies gilt auch für neue Matches auf Dating-Apps und insbesondere dann, wenn der Fremde beginnt, über den Handel mit Kryptowährungen zu sprechen.
- Misstrauisch sein gegenüber allen „Schnell-reich-werden“-Angeboten oder Kryptowährungs-Investitionsmöglichkeiten, die große Gewinne in kurzer Zeit versprechen.
- Sich mit den Verlockungen und Taktiken von Romantik- und Anlagebetrügereien vertraut machen. Non-Profit-Organisationen wie das Cybercrime Support Network bieten hierfür viele Informationen.
- Mögliche Pig-Butchering-Opfer sollten sofort alle Gelder aus den betroffenen Geldbörsen abheben und die Strafverfolgungsbehörden kontaktieren.

Historie der zweijährigen Pig-Butchering-Untersuchung von Sophos

2021

- Sophos X-Ops entdeckt die ersten gefälschten „CryptoRom“-Handelsapps, die auf Nutzer in Asien abzielen
- Kurz darauf entdeckt Sophos X-Ops, dass diese Betrüger ihre Aktivitäten ausweiten und Opfer auch in den USA und Europa ins Visier nehmen

2022

- Sophos X-Ops entdeckt weitere gefälschte Apps von CryptoRom-Betrügern sowie eine neue Methode, damit Opfer die gefälschten Apps erfolgreich auf ihre iOS-Geräte herunterladen
- Eine neue Art des Pig Butchering entsteht: Liquidity Mining

2023

- Sophos X-Ops entdeckt die ersten gefälschten Apps für CryptoRom-Systeme im Apple App Store, da Betrüger Wege finden, den App-Store-Prüfprozess zu umgehen
- Sophos X-Ops deckt zwei riesige Big-Butchering-Ringe auf, die von Hongkong und Kambodscha aus operieren. Anstatt gefälschte Apps zu verwenden, nutzen diese Betrüger nun legitime Krypto-Handelsanwendungen und erstellen ausgeklügelte Personas, um ihre Opfer zu ködern
- Sophos X-Ops findet weitere gefälschte Apps - und erfährt, dass Pig-Butchering-Betrüger jetzt auch generative KI in ihr Toolkit aufnehmen
- Ein Opfer von Pig Butchering verliert innerhalb einer Woche 22.000 Dollar. Dies führt Sophos X-Ops zu einem riesigen Liquiditätsbetrug, der von drei verschiedenen chinesischen organisierten Verbrecherringen betrieben wird

2024

- Sophos X-Ops deckt das technisch ausgefeilteste Pig Butchering auf, das es bisher gab: „DeFi savings"-Betrug. Diese und andere kryptobasierte Betrügereien werden als Kits zum Verkauf angeboten, was dazu führt, dass Pig-Butcher-Ringer in neuen Regionen der Welt auftauchen.

Mehr über die aktuellen DeFi-Sparpläne und die Entwicklung des Pig Butchering in „Cryptocurrency Scams Metastasize into New Forms“ finden Sie 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/
X/Twitter: @sophos_info

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