Sophos durchleuchtet zwei Cyberbetrugs-Ringe, die neue Crypto-Romance-Wege gehen

Betrüger nutzen einen gefälschten Goldhandelsmarktplatz und eine andere Gruppierung ergaunerte bereits 500.000 Dollar in Kryptowährung.
Betrüger gehen über Dating-Apps hinaus und zielen zunehmend auf Nutzer von Twitter- und Text-Nachrichten

Wiesbaden, 14. Februar 2023 – Sophos hat Details über zwei immer noch aktive Finanzbetrugsgruppierungen veröffentlicht, die ihre Opfer von Asien aus um Tausende von Dollar bringen. Der Sophos-Bericht Fool's Gold: Dissecting a Fake Gold Market Pig Butchering Scam beleuchtet die Vorgehensweise der sogenannten Pig Butchering- oder Sha-Zhu-Pan-Betrugsringe. Eine Gruppierung aus Hong Kong führt einen gefälschten Gold-Handelsplatz, eine weitere mit Sitz in Kambodscha und Verbindungen zum organisierten Verbrechen in China brachte den Betrügern in nur einem Monat 500.000 US-Dollar an Kryptowährung ein. Die Cyberkriminellen visierten in beiden Fällen den Sophos Principal Threat Researcher Sean Gallagher direkt via Twitter und Textnachrichten an, anstatt den Erstkontakt wie sonst üblich über Dating-Apps herzustellen.

Sean Gallagher über das Prinzip dieser Betrugsform:
„Wir verfolgen und berichten seit zwei Jahren über eine Untergruppe von Pig-Butchering-Betrügern namens CryptoRom. Bei dieser besonderen Betrugsform ködern Cyberkriminelle Dating-App-Nutzer und verleiten sie im Verlauf einer vorgetäuschten Liebesbeziehung, vermeintliche Investitionen in Kryptowährungen zu tätigen. Aber CryptoRom ist wirklich nur die Spitze des Eisbergs. Seit Beginn der Pandemie hat diese Art des Cyberbetrugs massiv zugenommen. Die Kriminellen gehen ihre Opfer mittlerweile nicht mehr nur auf allen großen Social-Media-Plattformen, sondern sogar über Direktnachrichten an. Zudem beschränken sie sich nicht mehr nur auf Kryptowährungen, sondern benutzen auch Geschäfte mit Gold oder andere Währungen und Handelsgütern als Köder."

Für die Analyse des ersten Betrugs mit einem fiktiven Goldinvestment interagierte Gallagher drei Monate mit einem der Kriminellen nach deren direkter Kontaktaufnahme via Twitter. Der Betrüger gab sich als 40-jährige Frau aus Hong Kong aus und versuchte schnell, die Konversation zu WhatsApp zu verschieben. Von hier aus versuchte er, Gallagher zu einer Investition auf einer gefälschten Goldhandels-Plattform zu überreden und warb dafür mit „Onkel Martin", angeblich ein früherer Analyst beim Wertpapierhandel- und Investmentbanking-Unternehmen Goldmann Sachs. Dafür lenkte der Kriminelle Gallagher direkt auf eine Webseite, die das Branding einer seriösen japanischen Bankgesellschaft namens Mebuki Financial imitierte, wo die Devisen- und Warenhandelsdienstleistungen erbracht werden sollten.

Technisch deutlich raffinierterer Betrug
Obwohl das Social Engineering bei diesem Betrug weniger ausgefeilt war als bei anderen von Sophos untersuchten Fällen, zeigt er eine deutliche Zunahme der technischen Raffinesse. Die Kriminellen nutzten eine aufwendige Kombination sehr effektiver Suchmaschinenoptimierung, verfeinerter Betrugsseiten zur „Registrierung" neuer Klienten auf ihrer gefälschten Mebuki-Webseite und eine raubkopierte Version einer legitimen Handels-App („MetaTrader 4") mit zugefügtem Schadcode, um den Opfern das Geld zu entwenden. Die Kriminellen haben sogar aktiv ihre Betrugs-Infrastruktur erneuert, um nicht abgeschaltet zu werden.

„Beide Betrüger-Ringe sind noch immer aktiv und es ist schwierig, sie zu stoppen. Während wir die Domains und IP-Adressen, die von den Angreifern aus dem Hong-Kong-Ring verwendet werden, als schadhaft markiert haben, richteten die Betrüger bereits eine neue Download-Infrastruktur für ihre raubkopierte Version der MetaTrader-App ein, so dass es für uns ein Kampf gegen Windmühlen ist“, kommentiert Gallagher den permanenten Kampf gegen die immer neuen Wege der Betrugsgruppen. „Die Organisationen sind immer breiter aufgestellt und wählen ihre Opfer regions- und plattformübergreifend aus. Der Wechsel von Krypto zu Gold zeigt ebenfalls, wie einfach diese Gruppierungen eine neue Nische finden können. Die beste Verteidigung ist, das öffentliche Bewusstsein für diese Art von Betrug zu schärfen. Bei den Anwendern sollten die Alarmglocken klingen, wenn sie SMS oder Direktnachrichten von Dating-Apps oder Social-Media-Kanälen von Unbekannten bekommen, die ein Gespräch anregen und dann lieber auf WhatsApp oder Telegram wechseln möchten. Besonders, wenn auch noch Behauptungen über Gewinne aus Kryptowährungen oder anderen Geschäften fallen.“

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 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