Erst mästen, dann schlachten: Pig-Butchering-Betrüger ergaunern mit gefälschtem Kryptowährungs-Handelspool mehr als 1 Million Dollar

Kryptobetrug hat sich in den letzten drei Jahren als dominante Form der internetgestützten Betrugsmaschen herauskristallisiert. Anzahl der gefälschten Liquiditätspools steigt sprunghaft von wenigen Dutzend auf über 500 Portale an

Sophos hat Details zu einer aktuellen Sha-Zhu-Pan-Operation – auch „Pig Butchering" genannt – veröffentlicht: erst mästen, dann schlachten, so lässt sich die millionenschwere betrügerische Masche beschreiben, die gefälschte Handelspools für Kryptowährungen nutzte, um mehr als 1 Million US-Dollar zu ergaunern. Der Report Latest Evolution of 'Pig Butchering' Scam Lures Victim in Fake Mining Scheme beleuchtet sehr detailliert die Geschichte des Opfers „Frank" und wie er 22.000 US-Dollar in nur einer Woche verlor. Die Betrüger hatten sich als Date auf der Plattform MeetMe ausgegeben und ihn zur Tätigung der hohen Investition auf eine gefälschte Webseite gelockt.

Nachdem die Entwickler bei Sophos X-Ops Franks Geschichte untersucht hatten, deckte das Team insgesamt 14 Domains auf, die mit dem Betrug verknüpft waren, gemeinsam mit Dutzenden nahezu identischer Betrugsseiten, die zusammengenommen innerhalb von drei Monaten mehr als 1 Million US-Dollar ergaunerten.

Liquiditätspools – Fälschungen sind fast nicht mehr zu erkennen
Diese Masche nutzt die weitestgehend unregulierte Welt von Handelsanwendungen für dezentralisierte Finanz-Kryptowährungen (DeFI). Derartige Apps ermöglichen das Erstellen sogenannter „Liquiditätspools" für verschiedene Arten von Kryptowährungen, zu denen Nutzer Zugang haben, um Geschäfte von einer Kryptowährung zur anderen zu machen. Teilnehmer erhalten einen Prozentsatz von jeder Gebühr, die jeweils für den Abschluss eines Geschäfts gezahlt wird – ein verlockendes Return on Investment. Um die Plattform zu nutzen, müssen Interessierte zunächst einen Online-Smartvertrag unterzeichnen. Dieser gewährt einem anderen Account (normalerweise der Betreiber der Plattform) Zugang zu den Brieftaschen (Wallets) der Teilnehmer, um den Handel zu erleichtern. Gefälschte Plattformen, wie sie Pig-Butchering-Betrüger zunehmend nutzen, um Geld von den Opfern abzuschöpfen, arbeiten fast genauso. Aber anders als bei legalen Pools räumen die Betrüger das Geld aus dem gesamten Liquiditätspool in ihre eigene Tasche.

Opfer wandte sich direkt an Sean Gallagher von Sophos
Sean Gallagher, Principal Threat Researcher bei Sophos, hat den Fall nicht nur in der Theorie analysiert: Frank hatte ihn persönlich angesprochen und um Hilfe gebeten.
„Als wir das erste Mal die gefälschten Liquiditätspools entdeckten, war das eher primitiv und noch in der Entwicklung. Jetzt aber sehen wir Sha-Zhu-Pan-Betrüger, die diese spezielle Masche des Kryptowährungsbetrugs nahtlos in ihr bestehendes Set an Taktiken (wie z.B. die Opfersuche via Dating-Apps) integrieren. Nur sehr wenige der Opfer verstehen, wie legale Kryptowährungsgeschäfte funktionieren, daher haben die Betrüger ein leichtes Spiel. Es gibt mittlerweile sogar Bausätze für diese Art von Betrug. Während Sophos im letzten Jahr ein paar Dutzend dieser gefälschten Liquiditätspools-Seiten verfolgte, sehen wir nun mehr als 500."

Ein Fake-Date wird zum Verhängnis
Sophos X-Ops lernte die im aktuellen Report untersuchte Liquidity-Mining-Operation zuerst bei einem Opfer kennen: Frank (Name wurde geändert, um die Privatsphäre des Opfers zu bewahren). Dieser war über die Dating-AppMeetMe mit „Vivian" in Kontakt gekommen, eine

angeblich deutsche Frau, wohnhaft und arbeitend in Washington. Frank chattete mit der vermeintlichen Freundin, die ihre romantischen Versprechen mit hartnäckigen Versuchen mischte, Frank zu Investitionen in Kryptowährungen zu animieren.

Schlussendlich eröffnete Frank ein Trust-Wallet-Konto (eine legitime Applikation, um US-Dollar in Kryptowährungen umzuwandeln) und verband sich mit dem Link zur Liquiditätspool-Webseite, die Vivian empfohlen hatte. In Wahrheit war die Seite eine nahezu perfekte Fälschung, die sich als Portal von Allnodes tarnte, ein etablierter dezentralisierter Finanzplattform-Provider. Zwischen dem 31. Mai und 5. Juni 2023 investierte Frank 22.000 US-Dollar. Nur drei Tage später leerten die Betrüger seine digitale Brieftasche. Er wollte sein Geld zurückholen und wandte sich an Vivian, die forderte, dass er noch mehr in den Pool investieren müsse, um sein Geld zurückzubekommen und die „Früchte“ zu ernten.

Während er auf die Autorisierung seiner Bank für einen Geldtransfer zu Coinbase wartete, fing Frank an, Nachforschungen anzustellen, was passiert sein könnte und stieß auf den Artikel über Liquidity Mining von Sophos. Dann bat er Sean Gallagher um Hilfe. Trotzdem Sean Frank geraten hatte, Vivian auf WhatsApp zu blockieren, fand diese Wege um ihr Opfer weiter via Telegram zu kontaktieren und beharrte auf seinen Investitionen. Auch ein langer emotionaler Brief sollte ihn überzeugen – ein Schreiben, das sehr wahrscheinlich von einer AI-Anwendung generiert wurde.

Keinerlei Regulierung bei Krypto-Apps – leichtes Spiel für Betrüger
„Was diese Art des Betrugs besonders schwierig aufzudecken macht, ist, dass er keine Schadsoftware braucht, die auf dem Gerät des Opfers installiert werden muss. Sie bezieht nicht einmal eine gefälschte App mit ein, wie solche, die wir in anderen CryptoRom Scams aufgedeckt haben. Dieser durch und durch falsche Liquiditätspool wurde über die rechtmäßige Trust-Wallet-Applikation betrieben. Frank hat sogar versucht, den Trust-Wallet-Support zu kontaktieren, um sein Geld wiederzubekommen, aber er landete nur bei dem Fake Support der gefälschten Webseite. Es gibt keinerlei Regulierung dieser Pools auf Krypto-Apps, ob legitim oder nicht“, gibt Gallagher zu bedenken. „Diese Betrügereien sind ausschließlich durch Social Engineering erfolgreich und die Betrüger sind hartnäckig. Der einzige Weg, sich vor diesen Übergriffen zu schützen, besteht darin, wachsam zu sein und zu wissen, dass sie existieren und wie sie funktionieren. Nutzer müssen sich vor Personen in Acht nehmen, mit denen sie nichts zu tun haben und die plötzlich über eine Dating-App oder eine Social-Media-Plattform Kontakt zu ihnen aufnehmen. Insbesondere wenn die „Person“, die Kontakt aufnimmt, das Gespräch auf eine Plattform wie WhatsApp verlagern möchte und dann über Investitionen in Kryptowährungen spricht.“

Sophos hat seine Analysen in diesem Fall mit Chainalysis und Coinbase geteilt, ebenso mit anderen Bedrohungsspezialisten im Kryptowährungsraum, die alle weiterhin Nachforschungen anstellen.

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