„Zunächst erstellen die Angreifer:innen überzeugende Fake-Profile auf Dating-Seiten. Sobald sie mit einer Zielperson in Kontakt getreten sind, schlagen sie vor, das Gespräch auf einer Messaging-Plattform fortzusetzen." (Jagadeesh Chandraiah, Senior Threat Researcher, Sophos)

Geld weg statt Liebe: iPhone-Krypto-Betrug eskaliert auch in Europa

*1,2 Millionen Euro-Beute in nur einem Wallet entdeckt***.**
Cyberganster nehmen vermehrt europäische und amerikanische Nutzer von Apps wie Tinder und Bumble auf Korn, um deren iPhones für ihre Machenschaften zu kapern.
Sophos gibt der Bedrohung den Codenamen CryptoRom.

Wiesbaden, 13. Oktober 2021 – Neue Erkenntnisse von Sophos deuten darauf hin, dass der internationale Cyber-Betrug mit Kryptowährung eskaliert. Cyberkriminelle nutzen beliebte Dating-Apps wie Tinder und Bumble, um iPhones von arglosen Nutzern:innen für ihre betrügerischen Machenschaften zu missbrauchen. Während es die Angreifer:innen in der Vergangenheit hauptsächlich auf asiatische Regionen abgesehen hatten, verlagern sich die Angriffe nun auch nach Europa und in die USA. Sophos hat ein von Cyberkriminellen kontrolliertes Bitcoin-Wallet mit fast 1,4 Millionen US-Dollar (1,2 Millionen Euro) entdeckt, die mutmaßlich von den Opfern gestohlen wurden.
Sophos hat dieser Bedrohung den Codenamen "CryptoRom" gegeben und einen detaillierten Bericht "CryptoRom Fake iOS Cryptocurrency Apps hit US, European victims for at least $1.4 million" veröffentlicht.

„Der CryptoRom-Betrug basiert in nahezu jeder Phase auf Social Engineering", sagt Jagadeesh Chandraiah, Senior Threat Researcher bei Sophos. „Zunächst erstellen die Angreifer:innen überzeugende Fake-Profile auf Dating-Seiten. Sobald sie mit einer Zielperson in Kontakt getreten sind, schlagen sie vor, das Gespräch auf einer Messaging-Plattform fortzusetzen. Dann versuchen sie, die Zielperson zu überreden, eine gefälschte Handels-App für Kryptowährung zu installieren und dort zu investieren. Auf den ersten Blick sehen die Renditen sehr gut aus. Wenn das Opfer jedoch das Geld zurückfordert oder versucht, auf die Finanzen zuzugreifen, wird es abgewiesen und das Geld ist verloren. Unsere Recherchen zeigen, dass die Betrüger:innen mit dieser Masche Millionen von Euro erbeuten."

Doppeltes Ungemach
Laut Untersuchungen können die Angreifer:innen noch weit mehr als nur Geld stehlen. Sie können auch Zugriff auf die iPhones ihrer Opfer erlangen. Bei dieser Variante des Angriffs nutzen Cyberkriminelle ein System für Software-Entwickler namens "Enterprise Signature". Normalerweise hilft diese Software Unternehmen dabei, neue iOS-Anwendungen mit ausgewählten iPhone-Nutzer:innen vorab zu testen, bevor sie diese zur Überprüfung und Genehmigung an den offiziellen Apple App Store senden. Mit der Funktionalität des Enterprise-Signature-Systems können Angreifer:innen mit ihren gefälschten Apps für den Kryptohandel größere Gruppen von iPhone-Benutzer:innen ansprechen und die Kontrolle über deren Geräte aus der Ferne erlangen. Damit sind sie potenziell in der Lage, noch mehr Schaden anzurichten, als sie es mit den Fake-Investitionen in Kryptowährung ohnehin schon tun. Sie können zum Beispiel persönliche Daten sammeln, Konten hinzufügen und entfernen und Apps für andere bösartige Zwecke installieren.

Eine Regel muss sein: Nur Apps aus dem App Store
„Bis vor kurzem verbreiteten die Krypto-Dieb:innen ihre betrügerischen Apps hauptsächlich über gefälschte Websites, die einer vertrauenswürdigen Bank oder dem Apple App Store ähneln", erklärt Chandraiah. „Mit der Nutzung des iOS-Entwicklersystems erhöht sich das Risiko für Opfer nochmals deutlich, da es den Angreifer:innen Rechte auf dem Smartphone und auch die Möglichkeit persönliche Daten zu stehlen geben kann. Um zu vermeiden, dass man Opfer dieser Betrugsmasche wird, sollten iPhone-Nutzer:innen ausschließlich Apps aus dem Apple App Store installieren. Die goldene Regel lautet: Wenn etwas riskant erscheint oder zu schön ist, um wahr zu sein, dann Finger weg – insbesondere, wenn weitgehend unbekannte Personen ein großartiges Online-Investmentprogramm mit großem Gewinn versprechen."

Sophos empfiehlt Sicherheitslösungen auch auf mobilen Geräten zu installieren. Dazu gehört beispielsweise Intercept X for Mobile, das iOS- und Android-Geräte vor Cyber-Bedrohungen schützt.

Weitere Informationen zu den gefälschten Kryptowährungs-Apps, die auf iPhones abzielen, sowie zu anderen mobilen Bedrohungen, sind auf SophosLabs Uncut zu finden.

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

Über Sophos
Sophos ist ein weltweit führender Anbieter von Next Generation Cybersecurity und schützt mehr als 500.000 Unternehmen und Millionen von Verbrauchern in mehr als 150 Ländern vor den modernsten Cyberbedrohungen. Basierend auf Threat Intelligence, KI und maschinellem Lernen aus den SophosLabs und von SophosAI bietet Sophos ein breites Portfolio an fortschrittlichen Produkten und Services, um Anwender, Netzwerke und Endpoints vor Ransomware, Malware, Exploits, Phishing und einer Vielzahl anderer Cyberattacken zu schützen. Sophos bietet mit Sophos Central eine einzige, integrierte und cloudbasierte Management-Konsole. Sie ist das Herzstück eines anpassungsfähigen Cybersecurity-Ökosystems mit einem zentralen Data Lake, der eine Vielzahl offener API-Schnittstellen bedient, die Kunden, Partnern, Entwicklern und anderen Cybersecurity-Anbietern zur Verfügung stehen. Sophos vertreibt seine Produkte und Services über Partner und Managed Service Provider (MSPs) weltweit. Der Sophos-Hauptsitz ist 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