Global iPhone crypto scam escalates to new heights, research finds

Sophos has released new insight on an international cryptocurrency trading scam targeting iPhone users through popular dating apps, such as Bumble and Tinder. A report detailing the latest findings, *CryptoRom Fake iOS Cryptocurrency Apps Hit US, European Victims For At Least $1.4 Million*, shows that the operation has escalated. The attackers have expanded from targeting people in Asia to include people in the U.S. and Europe. Sophos has uncovered a Bitcoin wallet controlled by the attackers that contain nearly $1.4m in cryptocurrency, allegedly collected from victims. Sophos researchers have code-named the threat 'CryptoRom'.

Source: Unsplash

“The CryptoRom scam relies heavily on social engineering at almost every stage,” said Jagadeesh Chandraiah, senior threat researcher at Sophos.

“First, the attackers post convincing fake profiles on legitimate dating sites. Once they’ve made contact with a target, the attackers suggest continuing the conversation on a messaging platform. They then try to persuade the target to install and invest in a fake cryptocurrency trading app. At first, the returns look very good but if the victim asks for their money back or tries to access the funds, they are refused and the money is lost. Our research shows that the attackers are making millions of dollars with this scam.”

Double trouble

In addition to stealing money, the attackers can also gain access to victims’ iPhones, according to Sophos’ research. In this version of the attack, cybercriminals leverage “Enterprise Signature,” a system for software developers that helps organisations to pre-test new iOS applications with selected iPhone users before they submit them to the official Apple App Store for review and approval.

With the functionality of the Enterprise Signature system, attackers can target larger groups of iPhone users with their fake crypto-trading apps and gain remote management control over their devices. This means the attackers could potentially do more than just steal cryptocurrency investments from victims. They could also, for instance, collect personal data, add and remove accounts, and install and manage apps for other malicious purposes.

“Until recently, the criminal operators mainly distributed the fake crypto apps through fake websites that resemble a trusted bank or the Apple App Store,” said Chandraiah. “The addition of the iOS enterprise developer system introduces further risk for victims because they could be handing the attackers the rights to their device and the ability to steal their personal data. To avoid falling victim to these types of scams, iPhone users should only install apps from Apple’s App Store. The golden rule is that if something seems risky or too good to be true – such as someone you barely know telling you about some ‘great’ online investment scheme that will deliver a big profit – then sadly, it probably is.”

Sophos recommends that users install a security solution on their mobile devices, such as Intercept X for Mobile, to protect iOS and Android devices from cyber threats. It is also worth securing all home and personal computers with additional protection such as Sophos Home.