Article Information

Authors: Michael Bacina, Steven Pettigrove, Jake Huang
Service: Blockchain
Sector: Financial Services, FinTech, IT & Telecommunications

SEAL team deploys to thwart DeFi domain exploit

Michael Bacina, Steven Pettigrove & Jake Huang of the Piper Alderman Blockchain Group bring you the latest legal, regulatory and project updates in Blockchain and Digital Law.

Last week, an unknown threat actor exploited an alleged vulnerability in Squarespace to take over accounts which controlled domains that had been recently migrated as part of the Squarespace acquisition of Google Domains. The exploit affected a number of DeFi protocols, including Compound.Finance a leading decentralised money market and lending protocol on Ethereum.

The forced migration of Google Domains appears to have allowed the threat actor to gain access to Squarespace accounts of over a hundred front-end web domains for crypto protocols. The threat actor was able to redirect users to phishing sites, intercept emails, and hijack control of Google Workspace (formerly GSuite) tenants to read email and add devices. The phishing sites are designed to steal visitors' cryptocurrency (known as drainers).

SEAL 911 first responders and SEAL (Security Alliance) security researchers worked alongside affected companies to coordinate the incident response, assist in recovering access to affected domains, and advise the broader cryptocurrency ecosystem on how to protect themselves. According to Coininfomania, no loss of funds has been reported to date.

The Security Alliance is the coalition behind several other Web3 security initiatives, including the Whitehat Safe Harbor, SEAL Wargames, which allows developer teams to simulate security incident scenarios, and the SEAL 911 Emergency Hotline, which enables users, developers and security researches who need access to urgent security advice, help with disclosing a critical vulnerability, or to connect with a team of carefully vetted expert volunteers. SEAL 911 has helped disrupt, intercept, and remediate several hacks, recovering over USD 50 million in crypto-assets. SEAL has also built the world's first crypto ISAC or information sharing and analysis centre to enhance real time sharing of threat intelligence, and combat cyber hacks and financial crime in Web3.

Piper Alderman is an advisor to the Security Alliance and was pleased to collaborate with SEAL on the Whitehat Safe Harbor Agreement alongside leading blockchain and cyber security lawyers including Gabriel Shapiro, the Lexpunk coalition, Debevoise & Plimpton LPP, and the policy teams at Paradigm and A16Z Crypto, among many others.