CryptoCore Group – ClearSky Cyber Security

Published: 2020-06-24 · Archived: 2026-04-10 02:54:17 UTC

A Threat Actor Targeting Cryptocurrency Exchanges

In this research, we present a hidden and persistent group, that has been targeting crypto-exchanges, mainly in the US and Japan since as early as 2018. The actor has successfully stolen millions' worth of cryptocoins. We named it as "CryptoCore" (or "Crypto-gang"), aka "Dangerous Password", "Leery Turtle". The CryptoCore report mainly focuses on the group's profile, modus operandi, and digital infrastructure.

Read the full report: CryptoCore Group

CryptoCore operations timeline

Introducing CryptoCore

CryptoCore is a group that targets almost exclusively cryptocurrency exchanges and companies working with them via supply-chain attack. The CryptoCore group is known for having accumulated a sum of approximately 70 million USD from its heists on exchanges. We estimate that the group managed to rake in **more than 200 million USD in two years**.

This group is not extremely technically advanced, yet it seems to be swift, persistent, and effective, nevertheless. We assess it to be active at least since May 2018, judging from the timestamp of the first known relevant sample, and it maintained steady activity since then. Its activity has receded in the first half of 2020, one possible reason being the limitations induced by the COVID-19 pandemic, but it didn't stop completely.

Attribution

We have been tracking CryptoCore group campaigns for almost two years, with no conclusive understanding of the operators' origin; however, we assess with medium level of certainty that the threat actor has links to the East European region, Ukraine, Russia or Romania in particular.

Modus Operandi

The key goal of CryptoCore's heists is to gain access to cryptocurrency exchanges' wallets, be it general corporate wallets or wallets belonging to the exchange's employees. For this kind of operation, the group begins with an extensive reconnaissance phase against the company, its executives, officers and IT personnel. While the group's key infiltration vector to the exchange is usually through spear-phishing against the corporate network, the executives' personal email accounts are the first to be targeted. Infiltrating the personal email accounts is an optional phase; however, it's a matter of hours to weeks until the spear-phishing email is sent to a corporate email account of an exchange's executive.

The spear-phishing is typically carried out by impersonating a high-ranking employee either from the target organization or from another organization (e.g. advisory board) with connections to the targeted employee. After gaining an initial foothold, the group's primary objective is obtaining access to the victim's password manager account. This is where the keys of crypto-wallets and other valuable assets – which will come handy in lateral movement stages – are stored. The group will remain undetected and maintain persistence until the multi-factor authentication of the exchange wallets will be removed, and then act immediately and responsively.

CryptoCore Digital Infrastructure – Graph

The following Maltego graph visualizes CryptoCore digital infrastructure, mainly dedicated IP addresses linked to C&C domains via passive DNS. The long, chain-like structure of the graph demonstrates a strong connection between network indicators, which in turn corroborates our findings. (click to enlarge)

Contact Us

To all future targeted cryptocurrency exchanges, we encourage your IR team to validate malicious activity with our findings to fingerprint and mitigate additional CryptoCore operations. For further help, please reach us out at **info@clearskysec.com**.

Read the full report: CryptoCore Report

Source: https://www.clearskysec.com/cryptocore-group/