CryptoCore – Cryptocurrency Exchanges Under Attack

atlas-cybersecurity.com/cyber-threats/cryptocore-cryptocurrency-exchanges-under-attack/

June 26, 2020

Friday, June 26th, 2020 | Cyber Threats

CryptoCore has established itself as a hidden and persistent hacker group that has been targeting cryptocurrency exchanges, mainly in the US and Japan, since 2018, effectively stealing millions' worth of cryptocurrencies. Their main targets have been almost exclusively exchanges and companies working with them via supply-chain attacks and have netted around 70-million US dollars from its attacks. ClearSky Cyber Security has been tracking the group for nearly two years and notes that the group has maintained steady activity ranging as far back as May 2018, while their activity has seemingly slowed down in the first half of 2020, ClearSky attributes this to the COVID-19 pandemic rather than the group's disbandment. While there doesn't exist much evidence to the group's origins, ClearSky is relatively confident that the threat actor has links to the East European region, specifically Ukraine, Russia, or Romania.

The main motivation behind their attacks is to gain access to the cryptocurrency exchanges' wallets, whether it be general corporate wallets or wallets belonging to the exchanges' employees. They begin their attacks with an extensive reconnaissance phase against the company and its employees, ranging from executives to IT personnel. Their main avenue for infiltration is through spear-phishing, typically targeting the executives' personal email accounts first, but this is sometimes an optional phase and they will instead simply target corporate email accounts instead of personal. These phishing emails are typically crafted to appear from a high-ranking supervisor within the target's own organization or from another organization, such as an advisory board, with connections to the target organization.

After gaining initial foothold, CryptoCore then attempts to access the victim's password manager account as this is where the keys of crypto-wallets and other valuable assets – to be used during the lateral movement stages – are stored. The threat actor will remain undetected and maintain persistence until the multi-factor authentication of the exchange wallets will be removed, ClearSky suspects that the group utilizes Mimikatz for credential harvesting. Once that is achieved, the group will act immediately in stealing the cryptocurrency within the wallets.

Some of the CryptoCore's main characteristics are:

- Persistence and adherence to same general TTPs and targets
  The group maintains the same general infection avenue, reconnaissance, and post-exploitation behaviors, while also changing the format of their bait document, spoofed webpages, and specific tools used; their naming convention for their documents and even some payloads also remain consistent between campaigns. They group also seems to be reluctant to “give up” on a target, attacking the same exchange until they are successful.
- Use of Cloud services such as Google Drive
  Google Drive is often used by the group to store their files, specifically their bait documents, with some phishing emails containing links directly to Google Drive or to a spoofed version. They do not limit themselves specifically to Google Drive, but it is their most utilized hosting service.
- Use of malicious cryptocurrency-themed domains
  Such as btcprime[.]tk, krypitalvc[.]com, blockchaintransparency[.]institute, etc.
- Use of bit.ly URL shortening service
  Having two main advantages for the CryptoCore group: the ability to mask suspiciously looking links behind a neutral bit.ly link and providing the attacker with click statistics to track the number of potential infections; bit.ly is widely used by the threat actor for its communications and the deployment of scripts and files for further infection.
- Use of LNK shortcuts as downloads
  The attacker is known to hide LNK shortcuts behind icons and titles of other file types, mostly text files. Whether it be a password file needed to access the main document or the main document itself that is the shortcut, but LNK files are widely utilized by the group. These files are used to connect to the command and control (C2) server and download next-stage files.
- Use of Visual Basic Script (VBS) files
  VBS files are utilized quite heavily by CryptoCore as both downloaders and backdoors. The group’s seemingly main backdoor, named by Proofpoint Emerging Threats as ‘CageyChameleon,’ is also a VBS file rather than an executable or an in-memory payload. The group has been known to utilize the Mimikatz password-dumping tool as well, so VBS files are not the group’s only post-exploitation tool.
- Swiftness and responsiveness
  While the group has been known to reuse the same infrastructures (domains, IPs, etc.) they are also quick to register and employ new domains and links. In one case, ClearSky was able to ascertain that a domain being utilized in an attack was only registered for use thirty-minutes prior to the attack.

While not much is known about CryptoCore besides their attacks, targets, and MO, there does exist some information about their internal infrastructure. This evidence includes:

- Use of Dedicated IP Addresses

  CryptoCore operators use dedicated IP addresses where they host their C2 domains and these IPs are associated with autonomous systems (AS) located in multiple countries, but located mainly within the US, Taiwan, Brazil, Egypt, Mongolia, and Thailand (in descending order according to their usage.)
- C2 TLD to Registrar and Nameserver Distribution

  The threat actor mostly registers their C2 domains using the .xyz TLD via NameCheap registrar services. Also, the group also registers all dedicated C2 domains that are associated with the .info TLD via NameSilo registrar services. These domains typically contain keywords that resemble names of cloud services, possibly with the intention of typo-squatting. The group also frequently uses the TLD .com, alongside gTLDs containing relevant words to mislead their victims, such as .email, .services, etc. CryptoCore apparently prefers PublicDomainRegistry and NameSilo registrar services but by no means limits themselves to only these two services.
- Anomalous Registration of Multiple C2 Domains in 3 Days

  To this day, the CryptoCore group typically tends to register a new C2 domain once or twice a month, while also not registering multiple C2 domains on the same day, except for one time. Two months after targeting a specific company in July 2018, CryptoCore registered ten domains within three days, pointing to the possibility that the group's digital infrastructure had been compromised and that they needed to quickly set up a new system in a few days.
- Re-Registering Expired C2 Domains

  This behavior may suggest the attacker's intent to reuse the same infrastructure for different ongoing campaigns, as well as future ones. There also exists evidence that year-old domains are still being utilized by the group and should thus remain blocked for long periods.
- Use of DDNS Services Until 2019

  In 2018 and 2019, CryptoCore operators had heavily relied on DDNS services such as dynu (dynu.com, kozow.com, theworkpc.com), ChangeIP (onmypc.org, itemdb.com, itsaol.com) and DNSExit/Netdorm (linkpc.net, publicvm.com). In 2020, however, ClearSky observed an uptick in registering new domains and pointing C2 domains to dedicated servers.

For a detailed analysis of CryptoCore's indicators of compromise (IOCs) please reference the attached document 'CryptoCore IOCs.'

Sources:

- ClearSky

- CyberStruggle
  It's important to note that CyberStruggle has dubbed this threat actor as 'Leery Turtle'
- Safety Internal Reference
  Translated from Chinese

Attachments

CryptoCore IOCs (535 kB)

Previous
Next