Paradies Clipper - Crypto Jacker Malware Analysis

Published: 2022-08-02 · Archived: 2026-04-05 18:22:46 UTC

This Malware Analysis video will center on Paradies clipper, this malware will replace victim's cryptocurrency addresses with the threat actors address via the clipboard, it's a perfect simple introduction to the world of malware analysis, stay tuned for more interesting malware reverse engineering videos in the future. Learn more about Paradies Clipper here: https://guidedhacking.com/threads/par... Donate on our Forum : http://bit.ly/2HkOco9 Support us on Patreon : http://bit.ly/38mnveC This crypto jacker video is brought to you by a new GH content creator named fr3dhk Follow him here here: _ / fr3dhk _ The Crypto Jacker malware is written in C++ with a C2 that the actor can use to see statistics on their malware. Within the video we take apart the malware and look at how the malware accomplishes it's functionality. The threat actor provides a demonstration video of the Paradies Clipper so that they can display functionality to potential customers. Within the video it will display exactly how the malware should function and what the inside of the malware C2 will look like. The C2 shows victims data such as their IP, OS, infection date, location and when they were last online. We use this as something to search for within the strings of the binary as the binary is not obfuscated. Then looking at the functionality of the Paradies Clipper we discuss how it carries out its persistence on the machine by first copying itself to localapp data and then using different permissions commands will make sure that the infected can not delete the malware. After doing this it will delete itself from the initial path that it was ran at and execute the newly copied malware in the localapp data directory. Once done then it will create a registry key that points to the malware so that it is run when the Windows OS is booted. After this we check out the crypto replacement functionalities by looking at the imports of the binary, Paradies Clipper imports some functions from the user32 dll to change and replace the victims keyboard. Using these functions when the victim copies something to their clipboard the malware will check it with multiple different crypto address regexes. If there is a match then it'll compare the copied address to the addresses stored within the malware so that it does not replace an already replaced address in the clipboard. Once the replacement has occurred then the malware will tell the C2 that it has replaced an address so that the threat actor can keep track of the malwares replacements. In future videos we'll take a look at how to emulate C2s to get commands from the malware and analyze network traffic. Then we'll move on to how to automate config extraction so that you extract information from multiple binaries. The video displays uses of IDA and debugging and how these can be applied to malware analysis. Same crypto jacker malware family but a different samples:E6ACCFE183328D9395022461A41C4F94 @siri_urz on Twitter 7CC522350595E854C07E3ED346067A91 @siri_urz on Twitter Associated Crypto wallets:BTC: 1C7HpJnRNaUNY8F7inQXyxmJ9aQsczZAML Ethereum: 0x301e8c4Dffaeb682b67bdfB5d340F36EFE2Cf877 Stay tuned for more malware analysis content coming soon! Follow us on Facebook : http://bit.ly/2vvHfhk Follow us on Twitter : http://bit.ly/3bC7J1i Follow us on Twitch : http://bit.ly/39ywOZ2 Follow us on Reddit : http://bit.ly/3bvOB57 Follow us on GitHub : http://bit.ly/2HoNXIS Follow us on Instagram : http://bit.ly/2SoDOlu #malwareanalysis #malware #malwares

---