Bitcoin Clipper Malware

Fundamentals of Malware Analysis Project

Muhammad Shahmir Ahmed Siddiqui 21K-3563

January 7, 2024

Abstract

Bitcoin clipper malware is a type of malicious software that specifically targets cryptocurrency transactions. It operates by silently replacing cryptocurrency wallet addresses copied to the victim's clipboard with the attacker's own address. This effectively redirects funds intended for the victim to the attacker's wallet. Bitcoin clipper malware has become increasingly prevalent in recent years, posing a significant threat to cryptocurrency users.

0.1 Introduction

The objective of this project is to understand the working mechanism of a bitcoin clipper malware. By gaining insights into the functionality and tactics employed by threat actors, we can contribute to enhancing the overall cybersecurity landscape. Our focus lies on getting a thorough understanding of how this specific malware operates, using which, we can develop effective countermeasures, patches, and recommendations.

0.2 Working

The bitcoin clipper designed by us uses a Windows application that monitors the clipboard for changes and modifies its contents if the clipboard contains a wallet address. The code uses the Windows API and the C++ filesystem library. Here is a breakdown of the main functionalities:

1)Persistence: The persistence function attempts to add the executable (btcclipper.exe) to the Windows registry in the "Run" key. This ensures that the program is executed every time the user logs in.

2)Clipboard Functions:
i.GetClipboard: Retrieves the current content of the clipboard.
ii.SetClipboard: Sets the clipboard content to a predefined Bitcoin wallet address (btc).
iii.Wallet Address Validation: The IsWallet function uses a regular expression to check whether a given string is a valid Bitcoin wallet address. It matches addresses that start with '1', '3', or 'bc1', followed by 23 to 59 alphanumeric characters.
iv.Clipboard Update Listener: The ClipboardFormatListenerProc function is a callback function that gets called when the clipboard content changes (WMCLIPBOARDUPDATE). When a clipboard update is detected, it checks if the new clipboard content is a valid Bitcoin wallet address. If it is, and it's different from the predefined address (btc), it modifies the clipboard content to the predefined wallet address using SetClipboard.

3)Main Function: It sets up the window class (WNDCLASSW) for the clipboard listener. Registers the window class. Creates a hidden window and adds it as a clipboard format listener. Enters a message loop (GetMessage) to handle messages until the program is closed. Upon closing, it removes the clipboard format listener, destroys the window, and unregisters the window class.

0.3 Tools

The following tools were utilized in this project:
*** Visual Studio Code IDE:** A network protocol analyzer used to capture and analyze network traffic, enabling the identification of malicious activity.
*** Windows API:** A debugger used to analyze and reverse engineer malicious software, providing insights into its behavior and functionality.
*** Sandboxed VM:** An application isolation tool used to safely execute suspected malware in a controlled environment, preventing potential damage to the host system.

Working Screenshot

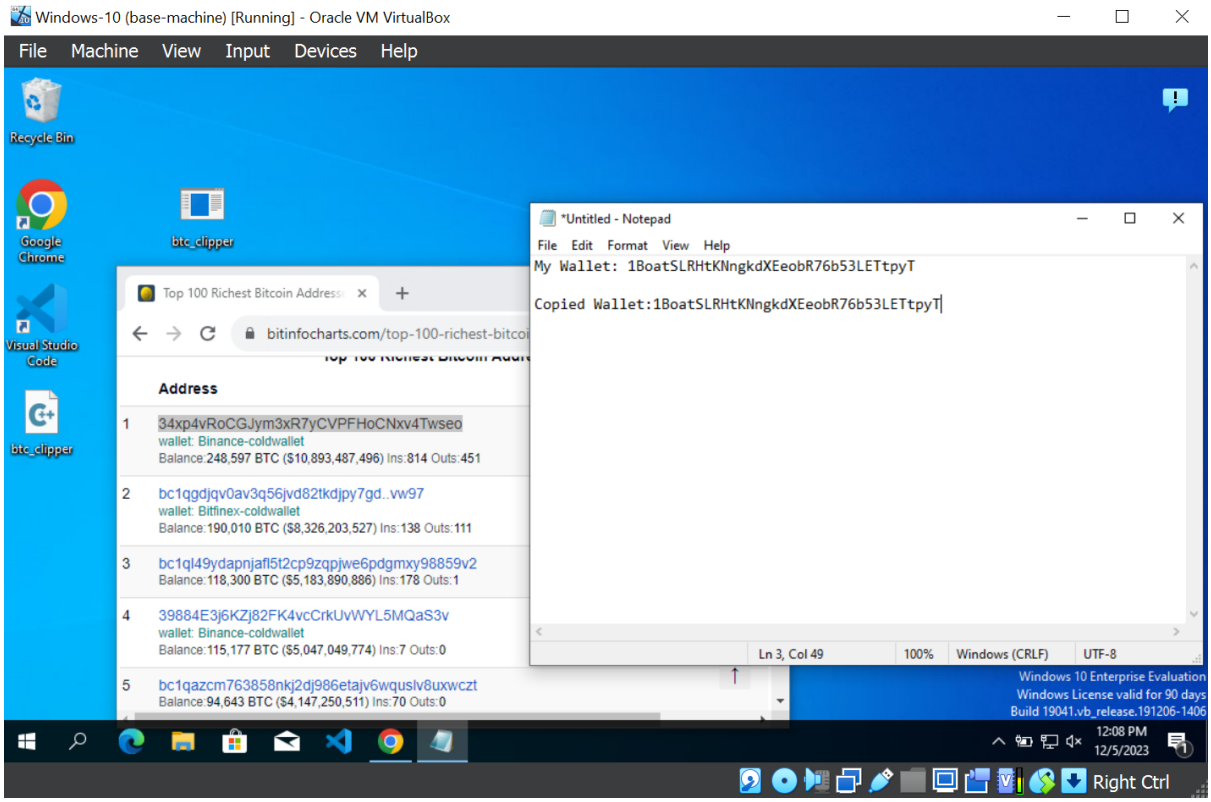

Figure 1: Working Malware Screenshot

0.4 Mitigation Techniques

- **Application Whitelisting:**Implement application whitelisting to allow only approved applications to run on the system.
- **Behavioral Analysis:**Employ behavioral analysis tools to detect abnormal behavior patterns in applications.
- **Clipboard Access Policies:** Monitor and control clipboard access within the organization. Limit the ability of applications to modify clipboard contents.
- **Logging and Monitoring:** Implement comprehensive logging to capture and analyze system activities, especially those related to registry changes, clipboard modifications, and network activity.
- **Registry Monitoring:**Implement monitoring mechanisms to detect changes to critical registry entries, especially those related to autostart locations.

Conclusion

In summary, the provided code highlights the necessity for a robust cybersecurity approach. A multi-layered strategy involving monitoring, logging, and analysis is crucial. To counter the malicious Bitcoin clipper malware, enforcing strict User Access policies related to the clipboard becomes pivotal.A proactive stance, coupled with user awareness and appopriate malware research, is essential in defending against evolving cyber threats. By combining these measures, organizations can fortify their security posture, detect potential risks, and respond effectively to incidents.