Cryptocurrency Social Networking Apps

CryptoClip Hijacker

By Vigneshwaran PApril 8, 2022

Stealing crypto-currency is not new to threat actors. Thinner profit margins from mining makes stealing the coins from wallets more lucrative. One of the common techniques is to scrape the clipboard for wallet addresses and replace them with that of the attacker's own address. The victim is left with no knowledge of the theft happening.

In this blog, we will be looking at one such CryptoClip hijacker malware, that was generally seen to be spammed out via Discord. Discord is one of the ways to stay in touch with people of a common interest. Hence spamming out CryptoClip hijacker malware to Discord servers that discuss crypto trading, mining would mean the malware reaches people who are actively dealing with crypto currency.

An unsuspecting user could download and execute these binaries. This malware could be spammed out via the traditional e-mail attachment technique too. We found one such malware that had the filename CryptoClipWatcher.exe, probably trying to pose as the safe CryptoClipWatcher tool.

Binary Overview

This binary is .NET compiled

CryptoClipWatcher.dat

Property	Value
File Name	[redacted]\CryptoClipWatcher.dat
File Type	Portable Executable 32 .NET Assembly
File Info	Microsoft Visual Studio .NET
File Size	1.06 MB (1115048 bytes)
PE Size	1.05 MB (1105920 bytes)
Created	Friday 18 March 2022, 11.52.55
Modified	Tuesday 16 November 2021, 12.05.25
Accessed	Wednesday 23 March 2022, 13.56.39
MD5	3488617002B1652F487D5AD410CB92AF
SHA-1	0DDFAEEC3426C36495CA8A1B476CBF3EC88A8321

Property	Value
CompanyName	Microsoft Corporation
FileDescription	Host Process for Windows Services
FileVersion	10.0.19041.546 (WinBuild.160101.0800)
InternalName	svchost.exe
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	svchost.exe
ProductName	Microsoft® Windows® Operating System

Figure 1: Version info of the malware

This file's version information and the internal name was spoofed to be like svchost.exe. Legitimate svchost.exe file would be Microsoft Visual C++ 8 compiled, and not .NET as observed in Figure 1. The file is also signed with a fake digital certificate as shown Figure 3.

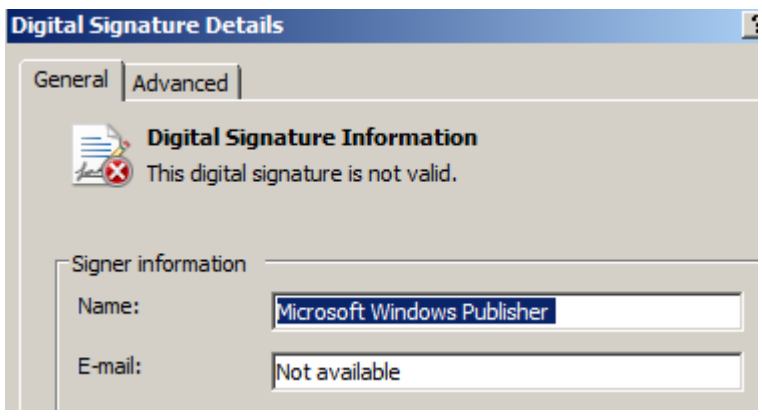

Figure 2: Digital Certificate information

The malware uses a simple decryption logic for all its encrypted data. First the encrypted string and a key ('UUdkUzZTQkFtMXlKTkE3Zw==') is decoded in base64 format. Then the decoded string is XORed with the decoded key. Figure 3 depicts this decryption process.

```
public static string Decrypt(string text, string key)
{
    if (text == "")
    {
        return "";
    }
    key = Encoding.UTF8.GetString(Convert.FromBase64String(key));
    text = Encoding.UTF8.GetString(Convert.FromBase64String(text));
    StringBuilder stringBuilder = new StringBuilder();
    for (int i = 0; i < text.Length; i++)
    {
        stringBuilder.Append(text[i] ^ key[i % key.Length]);
    }
    return stringBuilder.ToString();
}
```

Figure 3: Code to decrypt/decode

Even the file's original filename was seen as base64 encoded and XOR encrypted. The decoded value was EjUdI0I8AS0EQS4rOiJfAiM=: crypto clip watcher. which as mentioned earlier is the name of a legitimate crypto tool.

```
public static string CcwProcessName
{
    get
    {
        return Core.Decrypt("EjUdI0I8AS0EQS4rOiJfAiM=", Settings.XorPass);
    }
}
```

Figure 4: Original file name

Persistence technique used in this binary file

On statically analyzing the decompiled IL binary we found the reference to a persistence entry in %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup where the malware self copies and executes itself under the guise of svchost32.exe. Adds the same filepath to the run entry as well, under the subkey "Host Process for Windows Services" as shown in Figure 5.

```
Operation:   RegSetValue
Result:      SUCCESS
Path:        HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Host Process for Windows Services
Duration:    0.0000880

Type:        REG_SZ
Length:      186
Data:        C:\Users\[redacted]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\\svchost32.exe
```

Figure 5: Persistence entry in registry

Uses one another standard technique of adding scheduled tasks using cmd.exe.

```
CryptoClipWatcher.exe (1516)
    cmd.exe (3860)
        schtasks.exe (3404)
    svchost32.exe (2092)
```

Figure 6: Process tree of the malware

The self-copied file svchost32.exe is scheduled to be executed every minute by creating a job file as shown in Figure 7.

```
try
{
    Process.Start(new ProcessStartInfo
    {
        FileName = "cmd.exe",
        Arguments = string.Format("/c schtasks.exe /create /tn \"{0}\" /tr \"{1}\" /SC MINUTE /mo {2}", taskname, filename,
          minutes.ToString()),
        CreateNoWindow = true,
        WindowStyle = ProcessWindowStyle.Hidden
    });
}
```

Figure 7: The previous command line as seen statically in the decompiled binary

Malware Mechanism

This file has 38 crypto wallet addresses of the attacker, few of the shown in Figure 8. This addresses are also encoded with base64 and XORed with the key.

```
ADA : AddressType @04000015
BANANO_1 : AddressType @04000019
BANANO_3 : AddressType @0400001A
BCH_P2PKH_CashAddr : AddressType @04000007
BTC_BECH32 : AddressType @04000006
BTC_GOLD : AddressType @04000008
BTC_P2PKH : AddressType @04000004
BTC_P2SH : AddressType @04000005
DASH : AddressType @04000010
DCR : AddressType @0400000D
DOGE : AddressType @0400000F
ETH_ERC20 : AddressType @0400000B
IOTA : AddressType @04000016
LISK : AddressType @0400001D
LTC_BECH32 : AddressType @0400000A
LTC_P2PKH : AddressType @04000009
NAMECOIN : AddressType @04000027
NANO_1 : AddressType @04000017
NANO_3 : AddressType @04000018
NEO : AddressType @04000014
NIOBIO : AddressType @0400001C
QIWI_ID : AddressType @04000025
QTUM : AddressType @0400001E
STEAM_URL : AddressType @04000028
STELLAR : AddressType @04000013
STRATIS : AddressType @0400001B
TEZOS : AddressType @04000024
TRON : AddressType @04000023
value__ : int @04000003
VERTCOIN : AddressType @04000022
```

Figure 8: List of crypto currency that are targeted by the malware

Some of the transactions to this wallet are shown below in Figure 9.

```
AddressInfo.Patterns.Add(new AddressType?(AddressType.BTC), Core.Decrypt("DSUGMlgMcRpccFQQL2xNVHx+OSgDaj8dDw==",
  Settings.XorPass));
```

Encoded regex pattern for BTC

```
\bban_3[1A-Za-z3-9]{59}\b
```

Decoded regex patten

Figure 9: Encoded wallet address in decompiled code and decoded address.

A regex pattern("\b(79|380)[0-9]{9}\b") is used by this malware to scrape for crypto wallet addresses. Once that is done the malware validates to which currency the scraped wallet is relevant to, using the currency wallet specific regex. These regexes are also encoded as shown in Figure 10.

```
}).ToList<string>());
AddressInfo.Address.Add(new AddressType?(AddressType.BTC), Core.Decrypt("gHFiYLGkdODBYvbi8DKA0QUwoJJFxZSgsFcGUBAhceGQ8Y",
  Settings.XorPass).Split(new char[]
{
```

Encoded wallet ID

```
1EdJwv7FXnYHRoiCeYKe1h3AK1RfSPzJ9K
```

Decoded wallet ID

Figure 10: Currency specific regex encoded/decoded

The user wallet address in the clipboard is replaced with the malware author's wallet address. The code snippet to find and replace the clipboard content is shown in Figure 11.

```
public static string GetText()
{
    Thread thread = new Thread(new ThreadStart(ClipboardAsync.thGetText));
    thread.SetApartmentState(ApartmentState.STA);
    thread.Start();
    thread.Join();
    return ClipboardAsync._GetText;
}
```

Figure11: Get/Set text from clipboard

We checked one of the attacker's crypto wallet addresses and found a couple of transactions being made to it, which roughly translates to about 100$.

Transactions

This address has transacted 2 times on the Bitcoin blockchain. It has received a total of 0.00233968 BTC ($100.84) and has sent a total of 0.00233968 BTC ($100.84). The current value of this address is 0.00000000 BTC ($0.00).

Address	1EdJwv7FXnYHRoiCeYKe1h3AK1RfSPzJ9K
Format	BASE58 (P2PKH)
Transactions	2
Total Received	0.00233968 BTC
Total Sent	0.00233968 BTC
Final Balance	0.00000000 BTC

Figure 12: Transaction showing transfer of the crypto to the attackers' wallet address

It is always advisable to download tools or applications from reputable sources and exercise caution while using any such binaries. It is also always advisable to use a security software like K7 Total Security.

Indicators Of Compromise (IOCs) and Detections

Hash 3488617002B1652F487D5AD410CB92AF

Detection Name Trojan(00545fd01)

Original File Name crypto clip watcher.exe

Mutex 2c092895c2e64adb

Behavior suspicious program (ID 700018)

Like what you're reading? Subscribe to our top stories.

If you want to subscribe to our monthly newsletter, please submit the form below.

Email* :

- Previous Post« The Discord Token Grab
- Next Post

More Posts