Minerva Labs Blog

News & Reports

A new BluStealer Loader Uses Direct Syscalls to Evade EDRs

May 03, 2022 | Natalie Zargarov

BluStealer malware was first detected in May 2021 by James_inthe_box. Back then, it was delivered through a phishing mail, either as an attachment or a Discord link leading to the malware download URL. According to Avast 2021 analysis, it “consists of a core written in Visual Basic and the C# .NET inner payload(s). The VB core reuses a large amount of code from a 2004 SpyEx project. Its capabilities to steal crypto wallet data, swap crypto addresses present in the clipboard, find and upload document files, exfiltrate data through SMTP and the Telegram Bot API, as well as anti-analysis/anti-VM tactics”

BluStealer authors are not staying behind, and in their latest version, they implement what was one of 2021’s biggest trends - the use of direct syscalls to bypass EDRs.

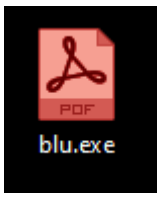
The latest version seems to have a pdf icon inserted to it, which would indicate that the delivery is via email, with the intention of tricking the user into executing the .exe loader while thinking it's a pdf. 

Figure 1 - First Stage Icon

The first stage loader is created with NSIS (Nullsoft Scriptable Install System), a professional open-source system used to create Windows installers, which drops three files to the user’s temp folder:

1. rwzhmby.exe - second stage loader file
1. mhxbnyunxz — third stage loader file
1. 3amz20m5vs — BluStealer malware

It then executes the rwzhmby.exe with C:\Users\username\AppData\Local\Temp\mhxbnyunxz.

```
text "UTF-16LE", 'C:\Users\     \AppData\Local\Temp\rwzhmby.exe C:\Us'
text "UTF-16LE", 'ers\     \AppData\Local\Temp\mhxbnyunxz',0
```

Figure 2 — Second Stage execution Command Line

The second stage loader reads the mhxbnyunxz and then allocates new memory, decrypts every byte read from mhxbnyunxz and continues to the decrypted code.

```
push    edi
push    esi
push    eax
call    ds:GetCommandLineW
mov     ecx, esp
push    ecx             ; pNumArgs
push    eax             ; lpCmdLine
call    ds:CommandLineToArgvW
push    offset Mode     ; "rb"
push    dword ptr [eax+4] ; flAllocationType
call    ds:_wfopen
add     esp, 8
mov     edi, eax
sub     esp, 10h
movdqa  xmm0, ds:lpAddress
movdqu  xmmword ptr [esp+1Ch+lpAddress], xmm0 ; lpAddress
call    ds:VirtualAlloc
mov     esi, eax
push    edi             ; Stream
push    1               ; ElementCount
push    1C41h           ; ElementSize
push    eax             ; Buffer
call    ds:fread
add     esp, 10h
```

Figure 3 - Read and Allocate Memory for Third Stage

The decrypted code (third stage) from mhxbnyunxz is the most interesting part. It is the main BluStealer loader and is responsible for gaining persistency, creating the necessary environment, and finally executing the malware itself.

BluStealer Environment:

The loader checks if the C:\Users\username\AppData\Roaming\rmfyvviyify folder exists. If it doesn't, it creates it and then creates a copy of the second stage rwzhmby.exe file to the folder under the name juvhkpig.exe.

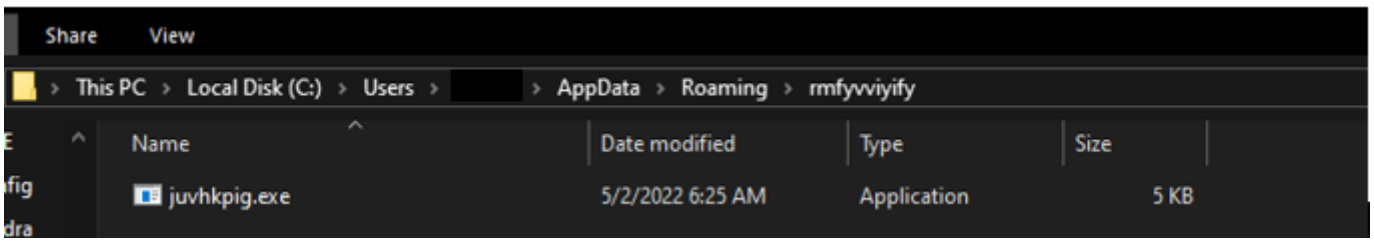


Figure 4 - Copied file to newly created folder

Persistency:

After creating a folder and copying rwzhmby.exe to it, the loader creates a new HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\wnyutmbcgovbty registry key, which will run the malware every time the user logs on.

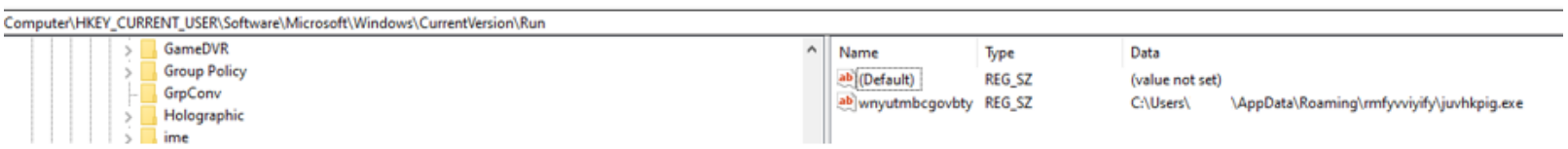


Figure 5 — Registry Persistency

Main Payload Execution:

The main payload seems to arrive in the 3amz20m5vs file. The loader first reads the file into allocated memory and then decrypts it. The only thing left is then to execute it. The malware uses a Process Hallowing Technique with a twist to execute the main payload a malware . Some of the API calls used for Process Hollowing were switched to direct syscalls.

```
debug050:000303F3
debug050:000303F3
debug050:000303F3
debug050:000303F3 sub_303F3 proc near
debug050:000303F3 mov     edx, esp
debug050:000303F5 sysenter
debug050:000303F7 retn
debug050:000303F7 sub_303F3 endp
debug050:000303F7
```

Figure 6 - Direct Syscall Function

The List of Standard API calls used in the Process Hollowing technique:

1. CreateProcessA — the loader runs ---first file ---- in suspended mode.
2. NtQueryInformationProcess
3. ReadProcessMemory
4. NtUnmapViewOfSection — called by direct syscall (0x002a)
5. VirtualAllocEx
6. WriteProcessMemory - called by direct syscall (0x003a)
7. GetThreadContext
8. SetThreadContext
9. ResumeThread - - called by direct syscall (0x0052)

Implementing an evasion technique like Process Hollowing while partly changing API calls to direct syscall is likely to confuse and bypass security products that rely on a specific set of API calls for detection.

The injected file is the final stage. Its original file name is firebed.exe and it is BluStealer itself. It seems to have been compiled on Apr 7th 2022, which might indicate that the author is constantly working on the stealer's capabilities. As a first step it creates a C:\Users\Public\30464142464246463030303330364632424642464630303033 30 folder which will contain the stolen data before the exfiltration. The injected file, firebed.exe, is also copied to this folder under the name misguise.exe.

Persistence capabilities have been changed since the previous version was released in September 2021. Our sample creates a HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\boos registry key which executes C:\Users\Public\30464142464246463030303330364632424642464630303033 30\misguise.exe

The new version of BluStealer is able to steal credentials from the following browsers:

- Iridium
- 7Star
- Cent Browser
- Chedot
- Vivaldi

- Kometa
- Elements Browser
- Epic Privacy Browser
- Sleipnir5
- Citrio

- Coowon
- liebao
- QIP Surf
- Orbitum
- Amigo

- Torch
- Yandex Browser
- Comodo Dragon
- 360Browser
- Maxthon3

- K-Melon
- Sputnik
- Nichrome
- CocCoc
- Uran

- Chromodo

- Atom
- Brave Browser
- Microsoft Edge
- Chromium

- Google Chrome
- Opera
- Mozilla Firefox

Many people store different credentials in their browsers so stealing this type of data might endanger both private and corporate users.

It also steals doc files (.txt, .xls, .xlsx,.doc, .docx, .pdf, .utc, .rtf) and personal data from email applications such as “MailMaster” and “ThunderBird” .

Zcash crypto wallet was added to last year's list and the current list of wallet keys that can be stolen is:

1. Zcash
2. Armory
3. Bytecoin
4. Jaxx Liberty
5. Exodus
6. Electrum
7. Atomic
8. Guarda
9. Coinomi

The last step is exfiltrating the collected data through SMTP.

It is worth mentioning, that Loader implementing such evasive injection technique can allow it to will bypass most security products, Including AVs &EDRs. By changing the main payload file, the loader can potentially one might execute different types of malwares, including ransomware.

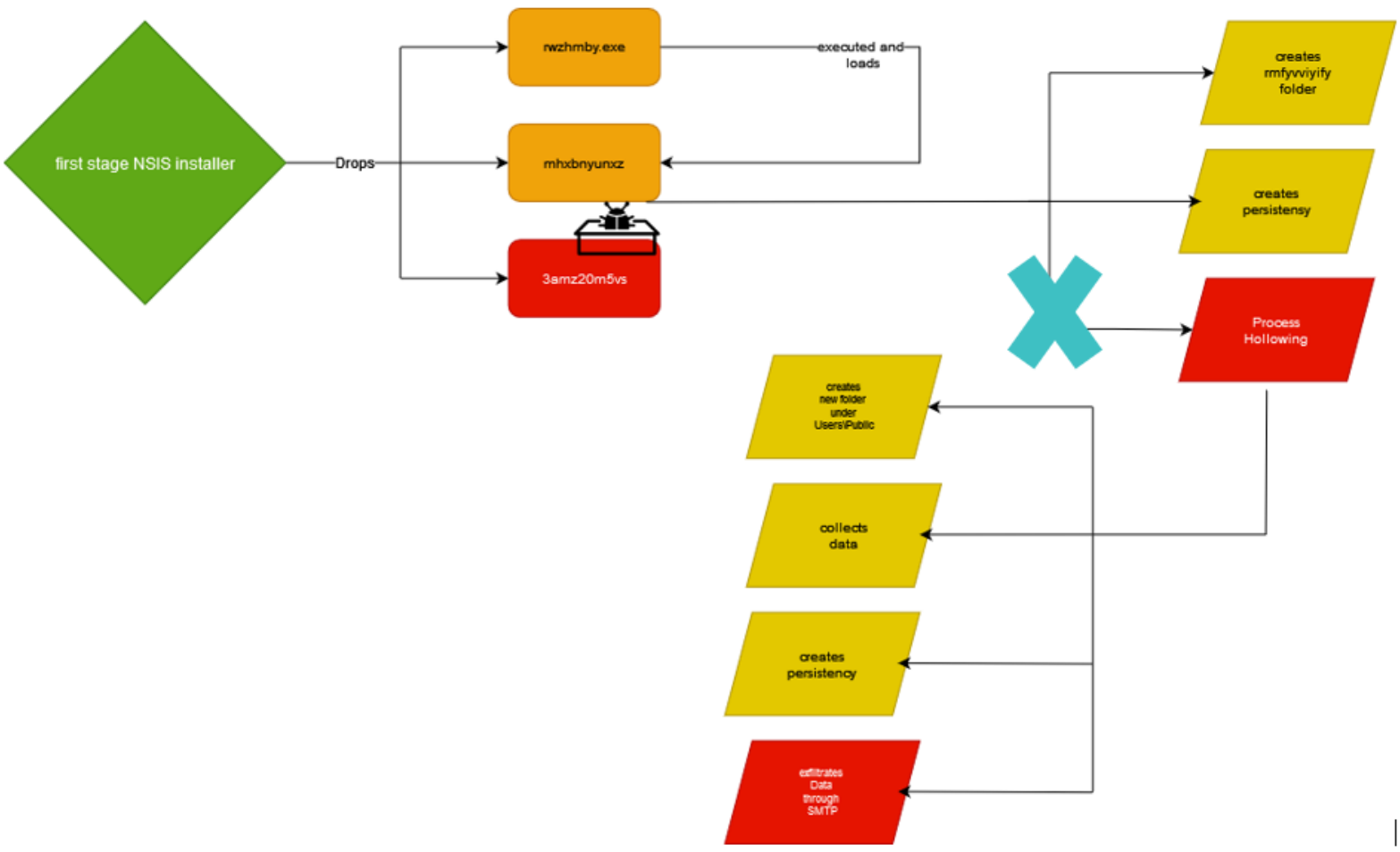


Figure 7 - BluStealer Execution Flow

Minerva Labs prevents the main payload from being executed by preventing the use of direct syscalls execution:

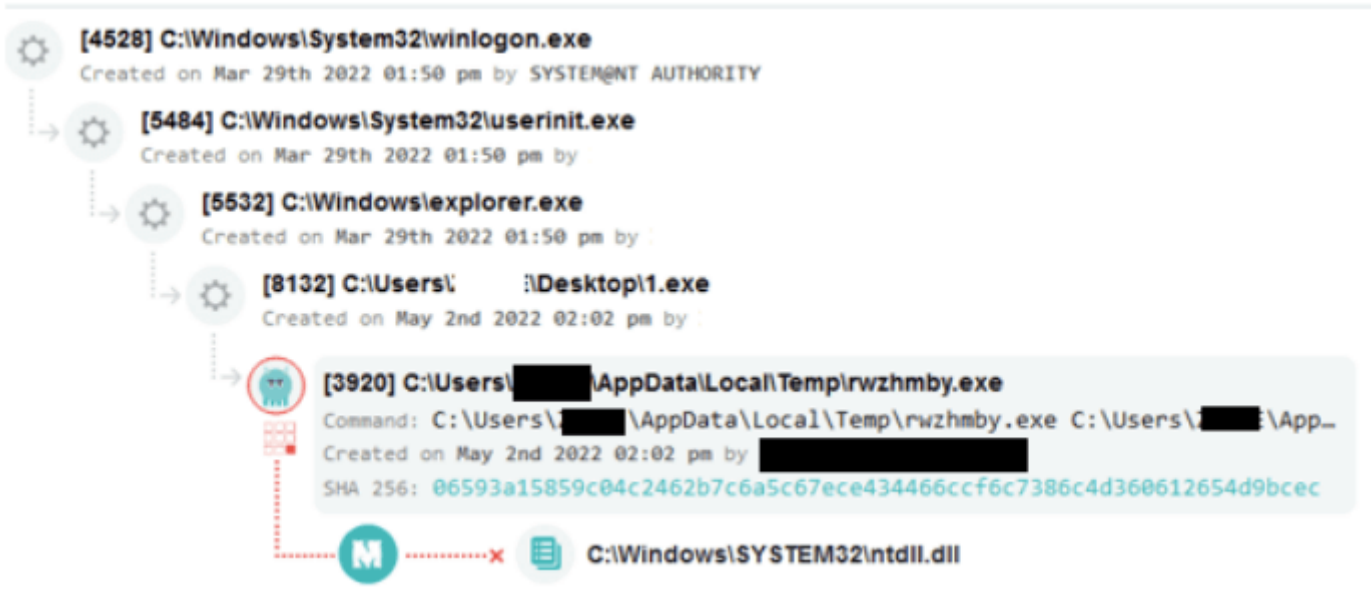


Figure 8 - Minerva Labs Prevention

IOC’s

1. 790F4DA318B3A9592F4B35B73528DE2C - rwzhmby.exe

1. 122C0AA6F0362E3F6F11FF83E3A608C4 - mhxbnyunxz

1. 43E7B7F7D9E59C3256CF7E5CE114FC53 - 3amz20m5vs

1. 953B2013A8B0D4BE5368A65FC74C93F4 - firebed.exe/ misguise.exe

« Previous Post