CIRT.GY Guyana National Computer Incident Response Team

# AL2024_41 Hackers Exploit Godot Game Engine to Deploy GodLoader Malware (29th November 2024)

## Description

Cybercriminals have leveraged the popular open-source Godot game engine to distribute malware through a new tool called GodLoader. This malware, active since mid-2024, exploits Godot's GDScript scripting language to bypass traditional antivirus systems and infect over 17,000 systems across multiple platforms, including Windows, macOS, and Linux. The attacks have primarily targeted gamers and developers by embedding malicious code in game asset files.

## Attack Details

Hackers have weaponized Godot's .pck files to embed malicious scripts, enabling the execution of harmful code upon unpacking. This exploit was facilitated through the Stargazers Ghost Network, a malware Distribution-as-a-Service (DaaS) platform. Leveraging over 3,000 GitHub ghost accounts, the attackers created a vast network of repositories to host and distribute the malware, misleading users into downloading compromised tools and games. Between September and October 2024, the GodLoader malware campaign targeted thousands globally through over 200 fake repositories, exploiting trust in open-source platforms.

Once deployed, the malware enabled attackers to steal sensitive credentials and deliver additional payloads, such as the XMRig cryptocurrency miner. These configurations were hosted on Pastebin, where they garnered over 200,000 visits during the campaign. The Stargazer Goblin group, active since 2022, is behind this operation, earning over $100,000 by promoting GodLoader through their DaaS services. Their actions highlight the growing sophistication and monetization of cybercrime using trusted development platforms.

## Indicators of Compromise (IOCs)

- **Malicious Files:** .pck files paired with the Godot runtime containing GDScript with malicious payloads.
- **Malware Activity:** Indicators of crypto mining activity, including the deployment of XMRig and related command-and-control (C2) configurations sourced from Pastebin.

## Remediation

### User Education:

- Only download software from trusted and verified sources.
- Avoid installing executables bundled with unknown .pck files unless verified by the original developer.

### System Protections:

- Implement updated antivirus software capable of detecting anomalies in GDScript files.
- Use endpoint protection tools to identify unusual script behavior.

**Network Monitoring:**

- Monitor Pastebin and other similar platforms for malicious configurations targeting your systems.
- Deploy network-level defenses to detect and block unauthorized connections to crypto mining C2 servers.

**Community Awareness:**

- The Godot team advises that users scrutinize any game or tool built with Godot, ensuring it comes from a legitimate source.

The Godot Engine security team has clarified that the vulnerability is not inherent to Godot but rather the misuse of its open-source capabilities. As a programming tool, malicious use is similar to exploits seen in other scripting platforms like Python or Ruby. Proper vigilance and adherence to best practices can mitigate the risks associated with this attack.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

**References**

- Gatlan, S. (2024, November 27). Hackers abuse popular Godot game engine to infect thousands of PCs. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/new-godloader-malware-infects-thousands-of-gamers-using-godot-scripts/
- No one is an island: How Caribbean states are working together to tackle cybercrime. (2022, October 17). Retrieved from PublicTechnology. https://www.publictechnology.net/2022/10/17/public-order-justice-and-rights/no-one-island-how-caribbean-states-are-working-together-tackle-cybercrime/