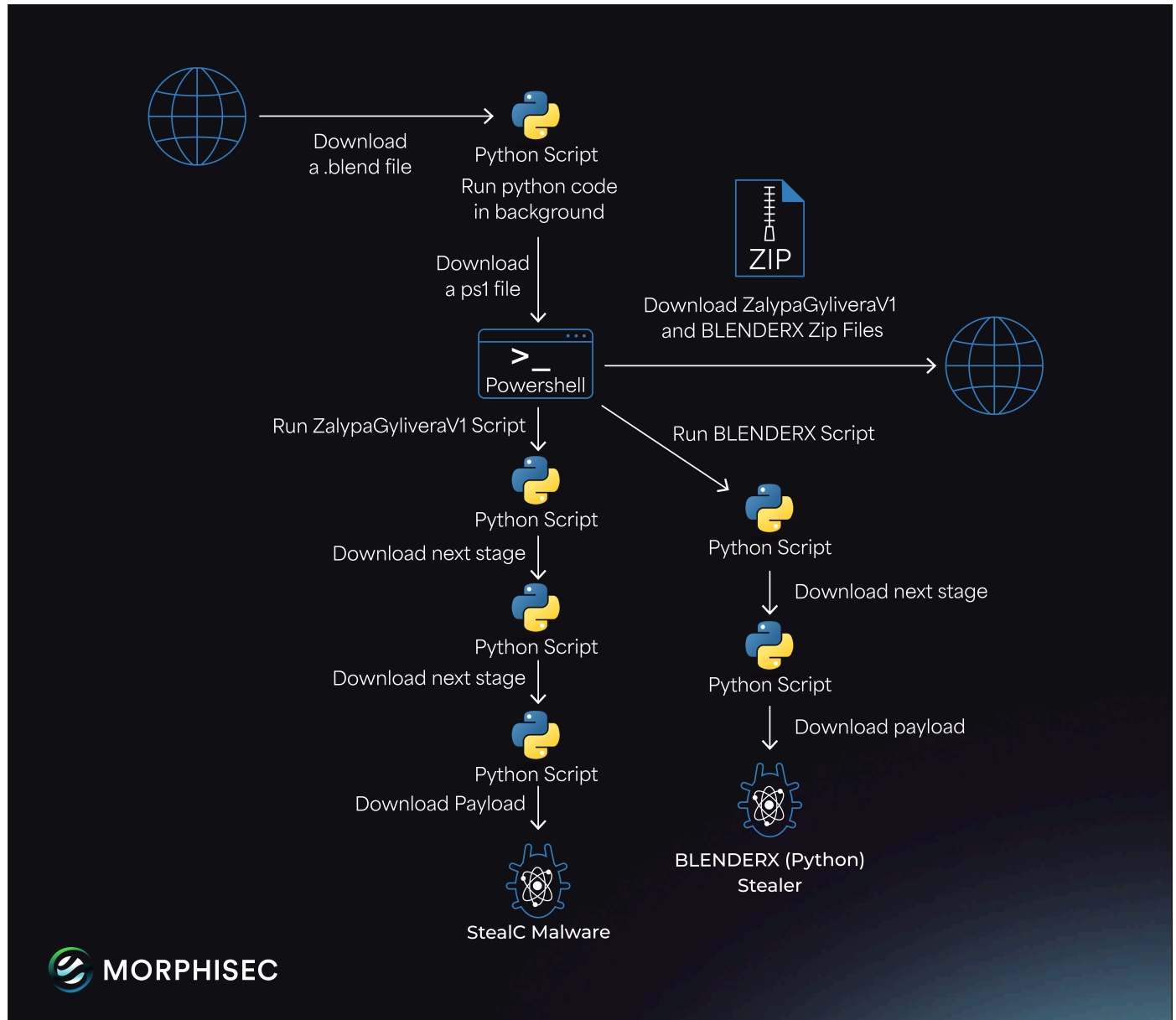


Morphisec Thwarts Russian-Linked StealC V2 Campaign Targeting Blender Users via Malicious .blend Files

 morphisec.com/blog/morphisec-thwarts-russian-linked-stealc-v2-campaign-targeting-blender-users-via-malicious-blend-files

November 24, 2025



In recent months, Morphisec has successfully prevented multiple sophisticated malware campaigns leveraging Blender Foundation files to deliver the notorious StealC V2 infostealer.

This ongoing operation, active for at least six months, involves implanting malicious .blend files on platforms like CGTrader. Users unknowingly download these 3D model files, which are designed to execute embedded Python scripts upon opening in Blender—a free, open-source 3D creation suite.

Introduction

Previous warnings about malicious .blend files have circulated on Reddit and other forums (e.g., [Reddit thread](#) and [Medium](#) article), but none linked them to StealC or Russian-speaking threat actors.

However new evidence now connects this Blender campaign to patterns previously observed in [Russian operations](#), including the impersonation of the Electronic Frontier Foundation (EFF) to target Albion Online players with StealC v2 and Pyramid C2 infrastructure. Both campaigns employ decoy documents, evasive techniques, and background execution of malware.

In this post, we dissect the technical attack path, reveal the full infrastructure of domains and files uncovered during our investigation, and highlight how Morphisec's ransomware prevention platform blocked these threats early.

[To download the full PDF analysis, click here.](#)

What is Blender and Why is it a Target?

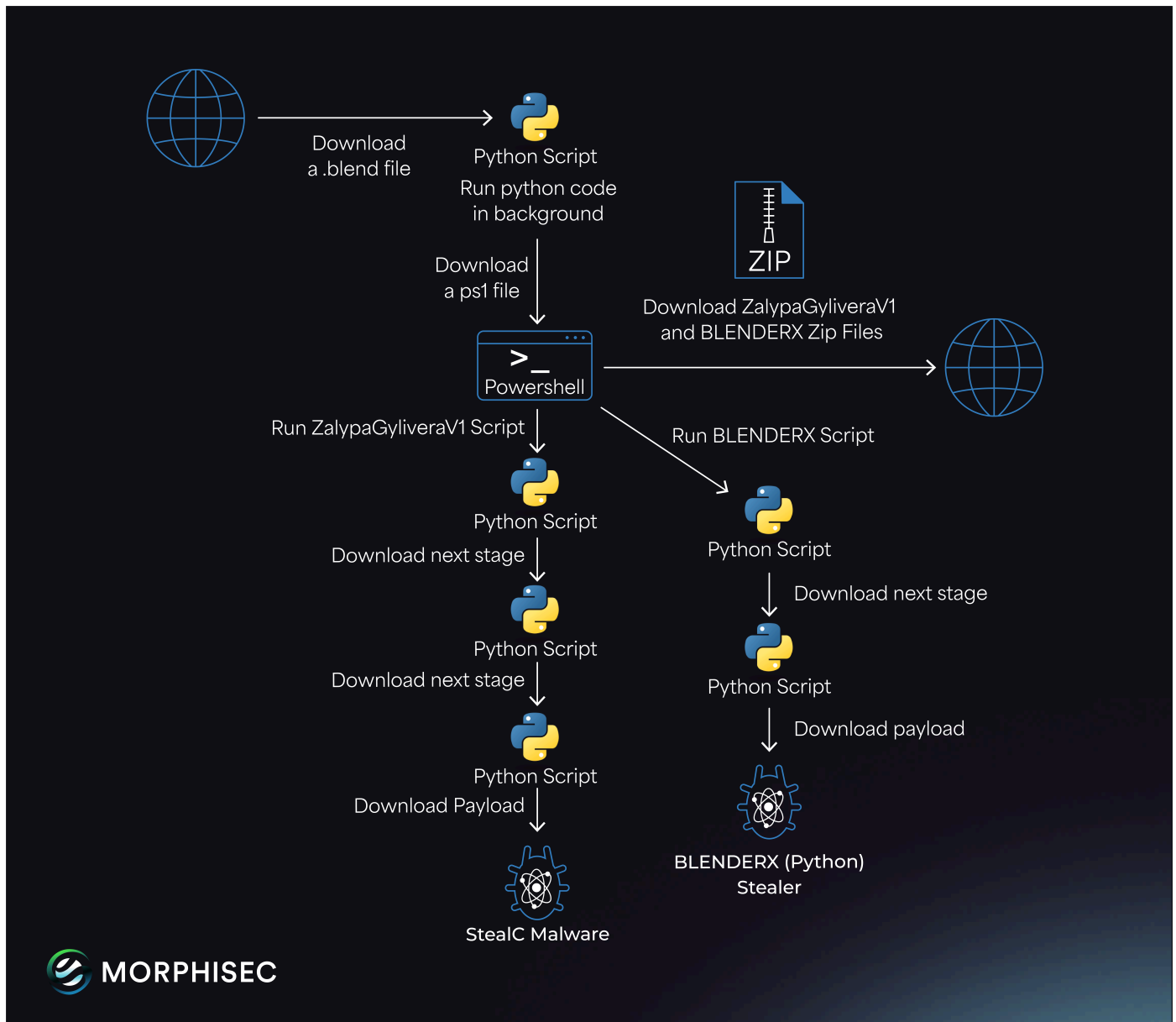
Blender is a powerful, free, and open-source 3D creation suite that supports modeling, animation, rendering, and more across Windows, macOS, and Linux. Its popularity stems from a vibrant community, extensive add-ons, and zero cost—making it ideal for hobbyists, professionals, and educators.

A key feature enabling abuse is the ability to embed Python scripts in .blend file in bpy.data.texts field. Scripts like [Rig_Ui.py](#) generate user interfaces for character rigs (e.g., facial controls or clothing systems). When Blender's Preferences → File Paths → Auto Run Python Scripts is enabled, these scripts execute automatically upon file open.

Security Note: Keep Auto Run disabled unless the file source is trusted. Attackers exploit Blender that typically runs on physical machines with GPUs, bypassing sandboxes and virtual environments.

The Attack Chain: From .blend to StealC V2

The infection follows this sequence:



Initial Access

Threat actors upload malicious .blend files to free 3D asset sites, such as:

- <https://www.cgtrader.com/3d-models> (hxxps://www.cgtrader[.]com/free-3d-models/character/sci-fi-character/acs-orange-spacesuit)
- <https://www.cgtrader.com/3d-models> (https://www.cgtrader[.]com/free-3d-models/character/man/spacesuit-nasa-apollo-11-84ff16e9-8b65-4faa-9b53-8aabb421b98f)



SPACESUIT NASA APOLLO 11 Free 3D model

+ Add to wishlist

25

14

0



Report

Free

Royalty Free No AI License

Free download



dald15252

5 reviews



Response - % in - h

Hire me

View all Designer's Models

3D Model formats

Format limitations

Autodesk FBX (.fbx) 3.76 MB

Blender (.blend) 3.76 MB

3D Model details

Ready for 3D Printing

Animated