MORPHISEC

Threat Analysis

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

Author: Shmuel Uzan

Introduction

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.

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.

What is Blender and Why is it a Target?

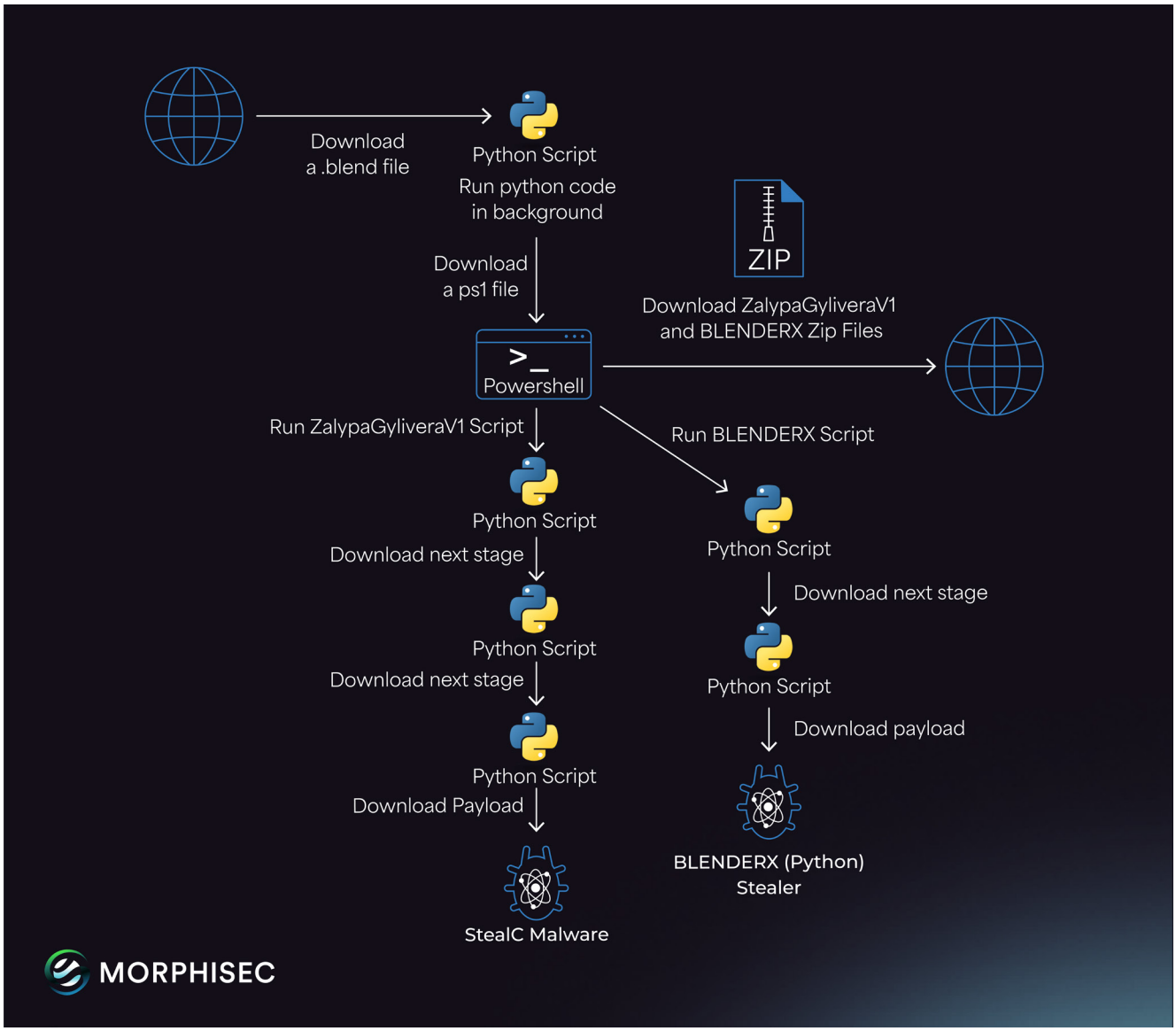
Blender is a powerful, free, and open-source 3D creation suite that supports modeling, animation, rendering, and more across Windows, macOS, and Linux. Its popularity stems from a vibrant community, extensive add-ons, and zero cost—making it ideal for hobbyists, professionals, and educators.

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

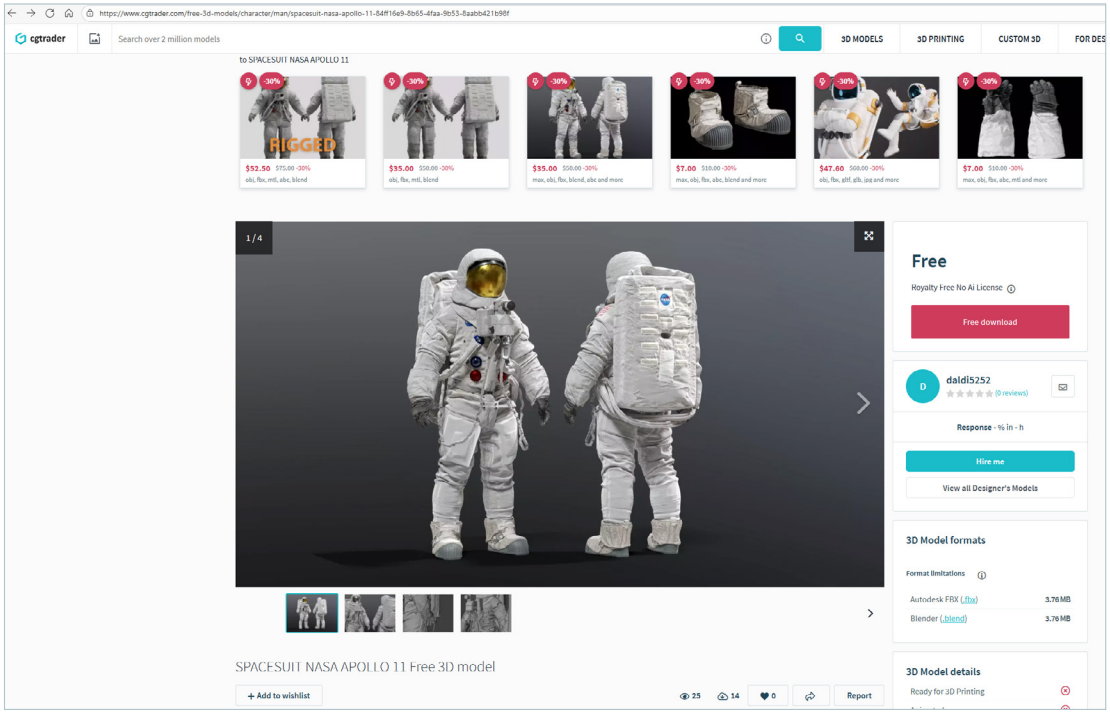
The infection follows this sequence:



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)



The sample file (SHA256: c62e094cf89f9a2d3b5018fdd5ce30e664d40023b2ace19acc1fd7c6b2347143) contains a weaponized Rig_Ui.py. Upon opening with Auto Run enabled:

- **Embedded Python Execution:** The script fetches a loader from hxxps://blenderxnew.tohocaper1979.workers[.]dev/get-link
- **PowerShell Stage:** Downloads a PS1 script (SHA256: B95F39B3C110D5F-C7E89E50209C560FE7077B9B66A5FC31065F0C17C7F06EE83)
- **ZIP Downloads:** The PS1 fetches two archives from domains like:
    - hxxp://178.16.53[.]64/documents/files/zip/
    - hxxp://91.92.243[.]91/documents/files/
    - ZalypaGyliveraV1.zip: Contains a Python environment with StealC
    - BLENDERX.zip: Deploys an auxiliary Python stealer (fetches from hxxps://zalukina.avisregde1988.workers[.]dev/get-link).
- **Extraction and Persistence:** Archives unzip to %TEMP%. LNK files (e.g., ZalypaGyliveraV1.lnk, SHA256: 7B4FC95BE7CA3BDE156FD53D10D05BF8C1A11D36155DC6179C9D4AFD D5E6862F) are executed hidden and copied to %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\ for persistence.
- **Pyramid C2 Module:** Python scripts download encrypted payloads (ChaCha20) via Pyramid cradle from URLs like hxxp://91.92.243[.]87:443/login/3keXipGb5Rr+gpGO9CjsSfdz+of

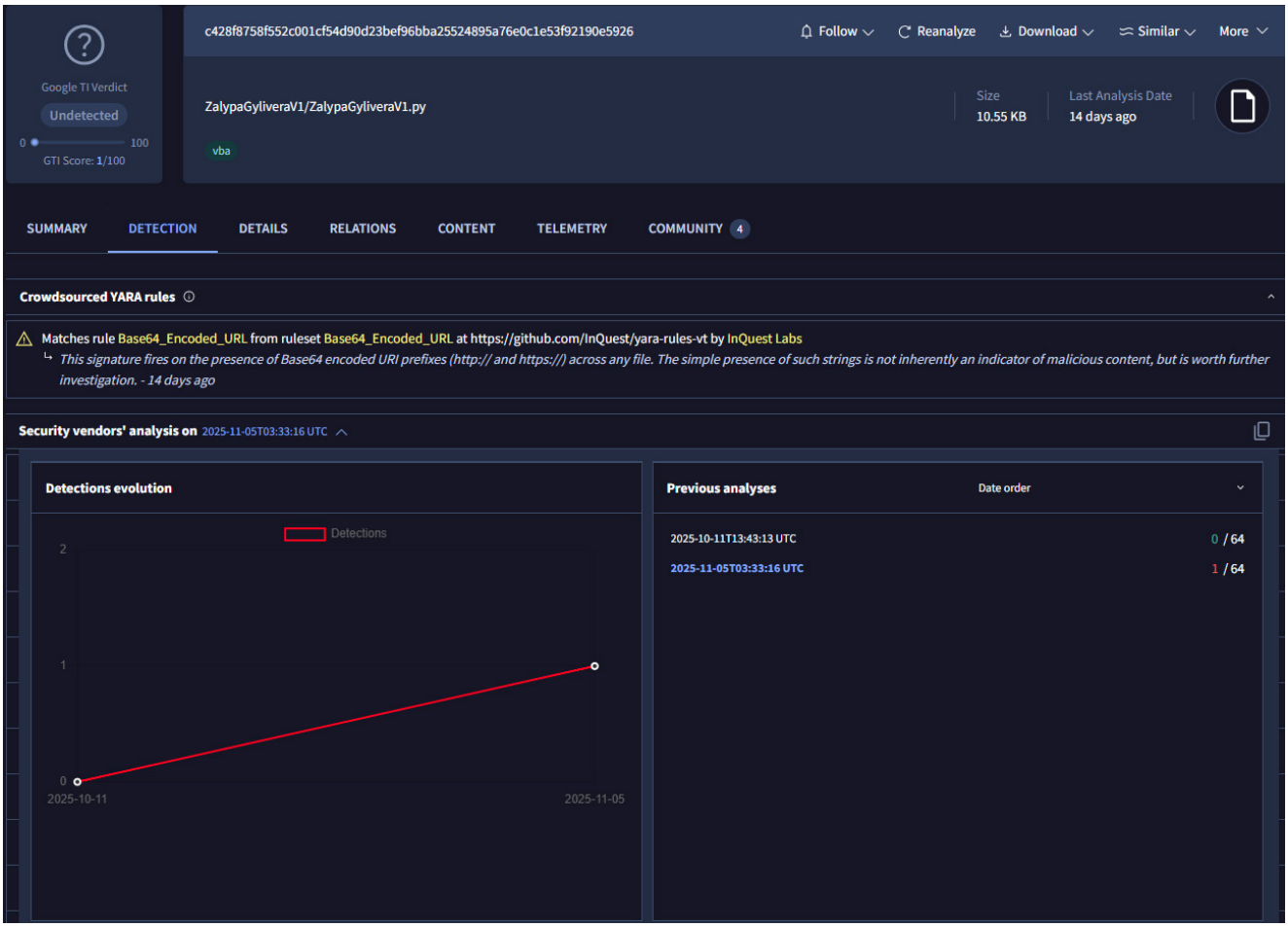
The Evolution of StealC V2

Intelligence from underground marketplaces shows StealC V2 (first announced on April 28, 2025), via an edit to the original StealC sales thread, evolved rapidly to attract low-tier cybercriminals. Until May 31, 2025, pricing remained: $200/month, $550/3 months, or $800/6 months. The latest known update on July 11, 2025, upgraded both the malware build and the admin dashboard. StealC V2's expanded feature set makes it a versatile infostealer, targeting:

- Support for more than 23 browsers (e.g. Chromium, Firefox, Opera, Brave, ...) - Server-side decryption of credentials for most browsers. Including support for Chrome 132+.
- More than 100 web plugins and extensions.
- More than 15 desktop wallets.
- Messaging apps: Telegram, Discord, Tox, Pidgin.
- VPN clients: ProtonVPN, OpenVPN.
- Mail clients: Thunderbird.
- Updated UAC bypass.

VirusTotal Low Detection Rates

Many of the identified samples in VirusTotal have an extremely low detection ratio, e.g. c428f8758f552c001cf54d90d23bef96bba25524895a76e0c1e53f92190e5926



Morphisec's Advanced Anti-Ransomware Platform: Stopping the Stealer Before the Breach

Morphisec doesn't just detect StealC, it prevents theft by using proactive deception and behavioral interception, long before data leaves the endpoint.

Morphisec dynamically generates and injects high-fidelity decoy credentials into memory and browser storage, mimicking real user logins for high-value targets.

When StealC accesses those decoys, it triggers Morphisec prevention; processes are terminated allowing for no exfiltration or persistence.

Morphisec turns credential theft from a high-probability event into a non-event. It's technology that doesn't rely on signatures and won't impact performance. Morphisec provides deterministic prevention that stops ransomware before it starts.

To see how Morphisec stops infostealers like the StealC campaign, schedule a demo today.

About Morphisec

Morphisec is the trusted global leader in prevention-first Anti-Ransomware protection, redefining cybersecurity with our industry-leading Automated Moving Target Defense (AMTD) technology. Our solutions are trusted by over 7,000 organizations to protect more than 9 million endpoints worldwide, stopping 100% of ransomware attacks at the endpoint and safeguarding businesses against the most advanced and dangerous threats, including zero-day exploits and ransomware.

At Morphisec, we don't just fortify defenses – we proactively prevent attacks before they happen, delivering unmatched protection and peace of mind to our customers. With our Ransomware-Free Guarantee and commitment to Preemptive Cyber Defense, we set the standard for accountability and innovation in the fight against modern cybercrime.

As a rapidly growing company, we are dedicated to empowering security professionals and organizations to adapt, protect, and defend against ever-evolving threats. Join us in shaping the future of cybersecurity with prevention-first strategies and unparalleled expertise.

IOCs

Type	Value
IP	178.16.53[.]64
IP	104.245.241[.]157
IP	178.16.54[.]69
IP	178.16.54[.]78
IP	91.92.241[.]143
IP	192.168.178[.]60
IP	91.92.242[.]85
IP	91.92.242[.]88
IP	91.92.243[.]87
URL	https://www.cgtrader[.]com/free-3d-models/character/man/spacesuit-nasa-apollo-11-84ff16e9-8b65-4faa-9b53-8aabb421b98f
URL	hxxps://zalukina.avisregde1988.workers[.]dev/get-link
URL	hxxp://91.92.243[.]91/documents/files/64CC37828HHKDeQ/BLENDERX.zip
URL	hxxps://serikalikl.spoticualpe1970.workers[.]dev/get-link
URL	hxxp://91.92.243[.]87:443/login/3keXipGb5Rr+gpGO9CjsSfdz+of
URL	http://213.209.150[.]224:443/login/3keXipGb5Rr+gpGO9CjsSfdz+of5
URL	http://212.87.222[.]84:443/login/3keXipGb5Rr+gpGO9CjsSfdz+of5
URL	https://zalypagylivera[.]nzalupadons1912.workers.dev/get-link
URL	https://zalypagylivera[.]disppomeverp1976.workers.dev/get-link
URL	http://178.16.54[.]69:443/login/3keXipGb5Rr+gpGO9CjsSfdz+of5
URL	http://178.16.54[.]69:443/login/w1GHz5ydpg/q

Type	Value
URL	http://91.92.241[.]143:443/login/w1GHz5ydpg/q
URL	https://zalukina[.]avisregde1988.workers.dev/get-link
URL	https://serikalikl[.]spoticualpe1970.workers.dev/get-link`
URL	http://91.92.243[.]87:443/login/3keXipGb5Rr+gpGO9CjsSfdz+of
URL	http://91.92.243[.]87:443/login/3keXipGb5Rr+gpGO9CjsSf dz+dqtXp32//B8qVKFSbc=
URL	https://blenderxnew[.]tohocaper1979.workers.dev/get-link
URL	https://addons1[.]12cloudaddons198756.workers.dev/get-link
URL	https://addons1[.]poupathockm2ist10012.workers.dev/get-link
URL	https://blenderx[.]mouthrunnbeva1986.workers.dev/get-link
URL	https://blenderx[.]osloyverjua1977.workers.dev/get-link
URL	https://zovwowgyl[.]simzqlupasdali1976.workers.dev/get-link
URL	http://zovwowgyl[.]spoticualpe1970.workers[.]dev/get-link
URL	http://91.92.242[.]88:443/login/3keXipGb5Rr+gpGO9CjsS fdz+of5
URL	http://91.92.242[.]88:443/login/3keXipGb5Rr+gpGO9CjsSf dz+dqtXp32//B8qVKFSbc=
URL	https://zalypagylivera[.]opkerrira1972.workers.dev/get-link
URL	https://zalypagylivera[.]disppomeverp1976.workers.dev/get-link
StealC	FC16AB400800B3D6A05B6FB3884D5BA52ED097 B8F50A2BEAB25442961B8FB8D0
StealC	AD278E48574CB10FE84B9B46C8B7BEF4F71C25B29F3E DAC93829B675B736BD69
.Blend	44a18a7431199cec3cd46b6c76ce8dbcb9201f181fd6f9906e d9ca742c5b87d

Type	Value
Blend	4c4fcb13e70c438799ffd7263b050b807f4416952955f3c65801cc63b92985d8
Blend	5681c26dae72c7a6f6b6e2f85fd3a3487888a6032c7a876bfbc4bf2c3a18ab97
Blend	8924df94890216c5b32142662e2131e0190163a2e96fa0183e5759a1dad89663
Blend	984cddf10b9aeda26d31de10bf6a020f8da61d15826fea7d90257ddf7e135368
Blend	a7ee45c1f72872e61f219d561f16710947f3d18441fc730c4a8896ddb98583ea
Blend	c3ab6d4bd8ee655fb8e5255a7acbcb39eb3fff013b9bd5893fd28e5d568fd0a5
Blend	c62e094cf89f9a2d3b5018fdd5ce30e664d40023b2ace19acc1fd7c6b2347143
BlenderX.zip	0C2BEDEA744686EBA1BFE116A0702F144FAD0B6020A8E91F12574398683A9DE5
4CC37828 HHKDeQ.zip	7B4FC95BE7CA3BDE156FD53D10D05BF8C1A11D36155DC6179C9D4AFDD5E6862F
ZalypaGyliveraV1.zip	0DBF2EFBFFC23831A571BEFB1D830C2D5FD855061259C93D6E5DE35FAD9D5BC1
ZalypaGyliveraV1.zip	5DA95DE05A961989A4A67187E19A27143298E520B974D7F7C35A4BFCCB7F0BA4
KursorResourcesV4.zip	F2F8846D55221682124E1030AB8DB45A2AEE39400AF9D2410F8339294ECA8FA0
Zalupa.ps1	FD4498A7F9BC714466A86F59AA4565A2B5F4C4EEE7C1A36E71FAC43D7C876ABD

Type	Value
ZalypaGyliv-eraV1.zip	158ABE39FF73E2EC950F4BC783020EB1F41BE0DC 89C0A6B8032A3438EDDE9DFD
KursorRe-sources.zip	11FA573238720A06562476CD2BFCABEDBFF5661D5B C83AA0325521643C903BA1
BLENDERX.zip	7E59E79F48FD2279F9E8BFEFA91D79FEB4AFEF 5720F7A338E46D2A6D1A607872
Decoy pds	A7E617783D7F1B0079C605126FBA074EE7EE431077CD97D 391E41F364A0AFE1B
BLENDERX Stelaer	1AB530CDCE98295D0566E237E8E577CE4D77B73586E A7E7200D963831391E64B
kursor.py	EA270CF9DB1F861FD59FF142444D32BBACC00003E9B B821A84E7F2B8F5277211
Python script tools	DB799377A0FEDE856C12D3C7EB30ECDC30EC09B6C 021C22D7C5D68E7A6F66109