Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

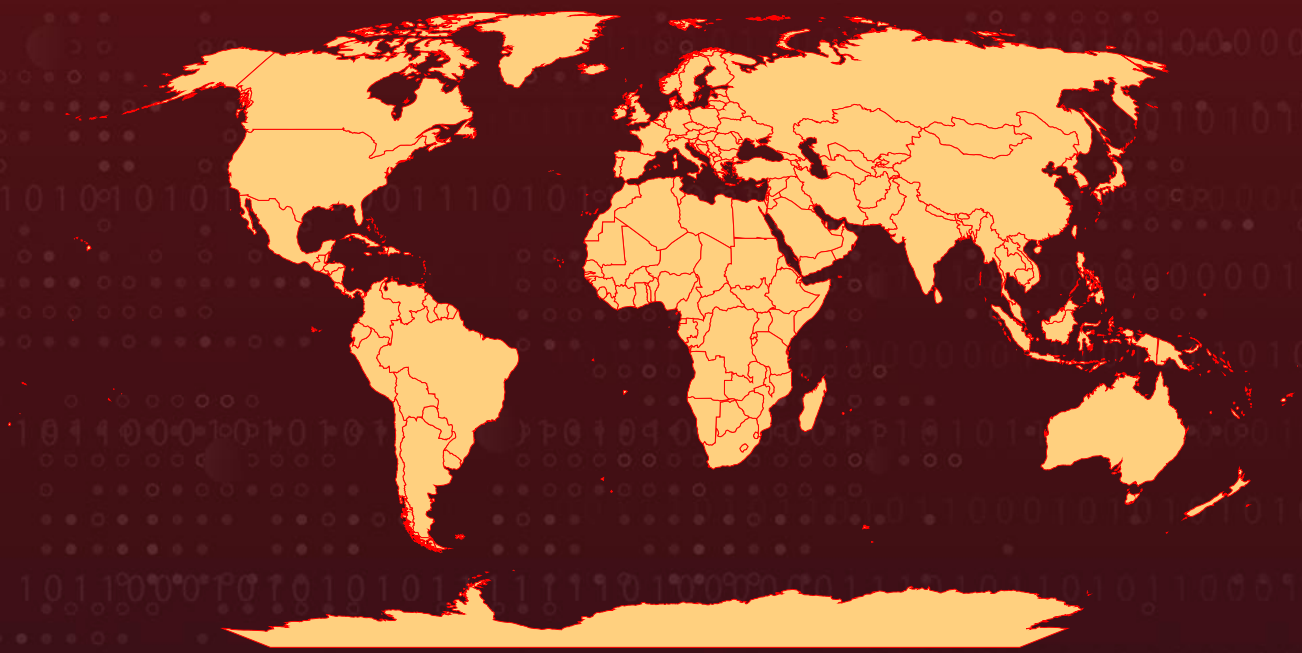
StealC V2 Spreads via Malicious Blender Files

Date of Publication	Admiralty Code	TA Number
November 27, 2025	A1	TA2025361

Summary

Attack Discovered: 2025
Targeted Region: Worldwide
Malware: StealC V2
Affected Platforms: Windows, macOS, and Linux
Attack: Attackers have found a clever new way to push the StealC V2 infostealer by hiding malicious Python scripts inside Blender 3D model files shared on popular asset sites. What looks like a harmless 3D project instantly turns into an infection chain the moment it's opened, quietly pulling in loaders, PowerShell scripts, ZIP bundles, and a full Pyramid C2 setup in the background. Recent evidence ties this activity to Russian-speaking operators. By abusing Blender's script-execution capabilities, the attackers slip StealC V2 onto victims' systems, where its powerful features harvest data from browsers, wallets, VPNs, messaging apps, and more, turning creative workflows into an unexpected path for cyber intrusion.

Attack Regions



Attack Details

#1 In recent months, researchers have uncovered a crafty malware campaign that misuses Blender Foundation files to deliver the rapidly evolving StealC V2 infostealer. For at least six months, attackers have been quietly uploading malicious .blend files to platforms like CGTrader. These files look like ordinary 3D assets, but once opened in Blender, they trigger concealed Python scripts that run automatically, turning a trusted creative tool into a silent delivery mechanism for malware.

#2 Blender's popularity plays a major role here. As a free, open-source 3D creation suite, it supports modelling, animation, rendering, and a thriving ecosystem of add-ons across all major operating systems. Its flexibility and community-driven growth make it ideal for professionals and hobbyists alike. But this same flexibility introduces risk. Blender allows Python scripts to be embedded directly into .blend files, and when Auto Run is enabled, those scripts can execute instantly upon opening, creating opportunities for attackers to weaponize the platform.

#3 Although the community had sounded general warnings about malicious Blender files before, none of those discussions connected the activity to StealC or any recognized threat actor. New evidence now suggests ties to Russian-speaking operators whose tactics resemble earlier campaigns, including those impersonating the Electronic Frontier Foundation (EFF) to target Albion Online players. Both sets of operations share familiar patterns: deceptive lure files, background execution chains, and the use of Pyramid C2 infrastructure to manage their attacks.

#4 The attack begins when a user opens a malicious .blend file containing weaponized Python scripts. If script auto-execution is turned on, the script retrieves a loader from a remote server, which then downloads a PowerShell script responsible for pulling down two ZIP archives. One archive contains a Python environment housing StealC, while the other delivers an auxiliary Python-based stealer. These components unpack into the %TEMP% directory, where hidden LNK files are executed and made persistent via the Startup folder. The infection chain culminates in the deployment of a Pyramid C2 module, where ChaCha20-encrypted Python scripts fetch additional payloads.

#5 This ultimately delivers StealC V2, an infostealer that has rapidly evolved since its introduction in April 2025, supporting more than 23 browsers, over 100 plugins and extensions, numerous cryptocurrency wallets, messaging apps, VPN clients, email clients, and featuring an upgraded UAC bypass. Overall, this campaign serves as a reminder of how even trusted creative tools can be weaponized, underscoring the growing need for cautious file handling and stronger security awareness.

Recommendations

- **Be Cautious when Downloading 3D Assets:** Only download Blender models from trusted creators or verified marketplaces. If something looks unusual, has very few downloads, or comes from an unknown uploader, avoid opening it.
- **Disable Auto Run for Python Scripts in Blender:** Blender allows embedded Python scripts to run automatically, which attackers are abusing. Go to Edit → Preferences → File Paths and make sure Auto Run is turned off unless you absolutely need it.
- **Scan Downloaded Files Before Opening:** Even if the file looks harmless, like a 3D model, run it through your antivirus or endpoint security tool before opening it in Blender.
- **Review Your Startup Folder Regularly:** Malware often hides malicious shortcuts (LNK files) in the Startup folder to run every time your system boots. Removing suspicious entries can break persistence.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0010** Exfiltration	**TA0011** Command and Control
T1059 Command and Scripting Interpreter	**T1059.006** Python	**T1190** Exploit Public-Facing Application	**T1566** Phishing

T1547 Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1204** User Execution	**T1548** Abuse Elevation Control Mechanism
T1548.002 Bypass User Account Control	**T1027** Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information	**T1036** Masquerading
T1555 Credentials from Password Stores	**T1555.003** Credentials from Web Browsers	**T1071** Application Layer Protocol	**T1041** Exfiltration Over C2 Channel
T1059.001 PowerShell			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	178[.]16[.]53[.]64, 104[.]245[.]241[.]157, 178[.]16[.]54[.]69, 178[.]16[.]54[.]78, 91[.]92[.]241[.]143, 192[.]168[.]178[.]60, 91[.]92[.]242[.]85, 91[.]92[.]242[.]88, 91[.]92[.]243[.]87
URLs	hxxps[:]//www[.]cgtrader[.]com/free-3d-models/character/man/spacesuit-nasa-apollo-11-84ff16e9-8b65-4faa-9b53-8aabb421b98f, hxxps[:]//zalukina[.]avisregde1988[.]workers[.]dev/get-link, hxxp[:]//91[.]92[.]243[.]91/documents/files/64CC37828HHKDeQ/[.]zip, hxxps[:]//serikalikl[.]spoticualpe1970[.]workers[.]dev/get-link, hxxp[:]//91[.]92[.]243[.]87[:]443/login/3keXipGb5Rr+gpGO9CjsSfdz+of, hxxp[:]//213[.]209[.]150[.]224[:]443/login/3keXipGb5Rr+gpGO9CjsSfdz+of5, hxxp[:]//212[.]87[.]222[.]84[:]443/login/3keXipGb5Rr+gpGO9CjsSfdz+of5, hxxps[:]//zalypagylivera[.]nzalupadons1912[.]workers[.]dev/get-link,

TYPE	VALUE
URLs	hxxps[:]//zalypagylivera[.]disppomeverp1976[.]workers[.]dev/get-link, hxxp[:]//178[.]16[.]54[.]69[:]443/login/3keXipGb5Rr+gpGO9CjsSfdz+of5, hxxp[:]//178[.]16[.]54[.]69[:]443/login/w1GHz5ydpg/q, hxxp[:]//91[.]92[.]241[.]143[:]443/login/w1GHz5ydpg/q, hxxps[:]//zalukina[.]avisregde1988[.]workers[.]dev/get-link, hxxps[:]//serikalikl[.]spoticualpe1970[.]workers[.]dev/get-link, hxxp[:]//91[.]92[.]243[.]87[:]443/login/3keXipGb5Rr+gpGO9CjsSfdz+of, hxxp[:]//91[.]92[.]243[.]87[:]443/login/3keXipGb5Rr+gpGO9CjsSfdz+dqtXp32//B8qVKFSbc=, hxxps[:]//new[.]tohocaper1979[.]workers[.]dev/get-link, hxxps[:]//addons1[.]12cloudaddons198756[.]workers[.]dev/get-link, hxxps[:]//addons1[.]poupathockm2ist10012[.]workers[.]dev/get-link, hxxps[:]//[.]mouthrunnbeva1986[.]workers[.]dev/get-link, hxxps[:]//[.]osloyverjua1977[.]workers[.]dev/get-link, hxxps[:]//zovwowgyl[.]simzqlupasdali1976[.]workers[.]dev/get-link, hxxp[:]//zovwowgyl[.]spoticualpe1970[.]workers[.]dev/get-link, hxxp[:]//91[.]92[.]242[.]88[:]443/login/3keXipGb5Rr+gpGO9CjsSfdz+of5, hxxp[:]//91[.]92[.]242[.]88[:]443/login/3keXipGb5Rr+gpGO9CjsSfdz+dqtXp32//B8qVKFSbc=, hxxps[:]//zalypagylivera[.]opkerrira1972[.]workers[.]dev/get-link, hxxps[:]//zalypagylivera[.]disppomeverp1976[.]workers[.]dev/get-link
SHA256	FC16AB400800B3D6A05B6FB3884D5BA52ED097B8F50A2BEAB25442961B8FB8D0, AD278E48574CB10FE84B9B46C8B7BEF4F71C25B29F3EDAC93829B675B736BD69, 44a18a7431199cec3cd46b6c76ce8dbcb9201f181fd6f9906ed9ca742c5b87d, 4c4fcb13e70c438799ffd7263b050b807f4416952955f3c65801cc63b92985d8, 5681c26dae72c7a6f6b6e2f85fd3a3487888a6032c7a876bfbc4bf2c3a18ab97, 8924df94890216c5b32142662e2131e0190163a2e96fa0183e5759a1dad89663, 984cddf10b9aeda26d31de10bf6a020f8da61d15826fea7d90257ddf7e135368, a7ee45c1f72872e61f219d561f16710947f3d18441fc730c4a8896ddb98583ea, c3ab6d4bd8ee655fb8e5255a7acbcb39eb3fff013b9bd5893fd28e5d568fd0a5, c62e094cf89f9a2d3b5018fdd5ce30e664d40023b2ace19acc1fd7c6b2347143,

TYPE	VALUE
SHA256	0C2BEDEA744686EBA1BFE116A0702F144FAD0B6020A8E91F12574398683A9DE5, 7B4FC95BE7CA3BDE156FD53D10D05BF8C1A11D36155DC6179C9D4AFDD5E6862F, 0DBF2EFBFFC23831A571BEFB1D830C2D5FD855061259C93D6E5DE35FAD9D5BC1, 5DA95DE05A961989A4A67187E19A27143298E520B974D7F7C35A4BFCCB7F0BA4, F2F8846D55221682124E1030AB8DB45A2AEE39400AF9D2410F8339294ECA8FA0, FD4498A7F9BC714466A86F59AA4565A2B5F4C4EEE7C1A36E71FAC43D7C876ABD, 158ABE39FF73E2EC950F4BC783020EB1F41BE0DC89C0A6B8032A3438EDDE9DFD, 11FA573238720A06562476CD2BFCABEDBFF5661D5BC83AA0325521643C903BA1, 7E59E79F48FD2279F9E8BFEFA91D79FEB4AFEF5720F7A338E46D2A6D1A607872, A7E617783D7F1B0079C605126FBA074EE7EE431077CD97D391E41F364A0AFE1B, 1AB530CDCE98295D0566E237E8E577CE4D77B73586EA7E7200D963831391E64B, EA270CF9DB1F861FD59FF142444D32BBACC00003E9BB821A84E7F2B8F5277211, DB799377A0FEDE856C12D3C7EB30ECDC30EC09B6C021C22D7C5D68E7A6F66109

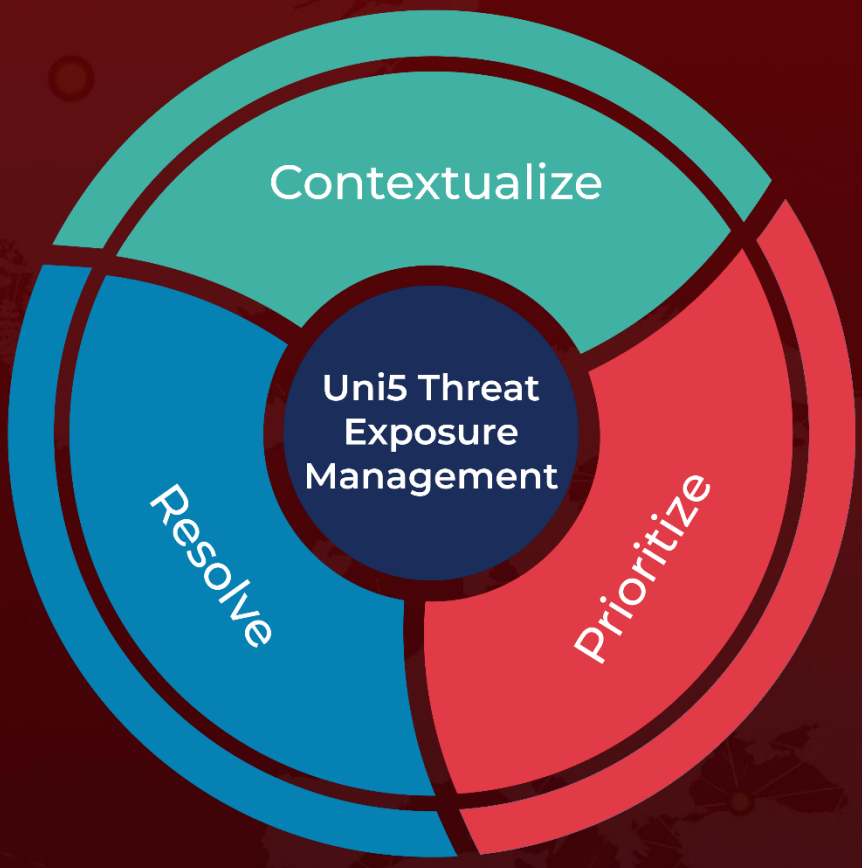
References

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

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 27, 2025 • 8:00 AM

More at www.hivepro.com