MORPHISEC

Executive Report

Emerging Threat: Russian-Linked StealC V2 Campaign Using Trusted Creative Platforms to Evade Detection

How a New Malware Campaign Targets Creative Teams, Bypasses Traditional Security, and Reveals the Future of Innovation-Aware Cyber Threats

Overview: A New Class of Supply Chain & Creative Workflow Attacks

Recently, Morphisec Threat Labs research uncovered and prevented a sophisticated malware campaign that weaponizes Blender .blend files, a format widely used by 3D designers, engineering teams, gaming studios, creative agencies, and product innovators.

Threat actors embedded malicious scripts inside downloadable 3D model files hosted on trusted platforms like CGTrader, using Blender's Auto Run Python Scripts functionality to deploy StealC V2, an advanced infostealer that targets credentials, VPNs, browsers, crypto wallets, cloud services, and enterprise data.

Read the Complete Analysis

This marks a significant shift: attackers are moving beyond traditional IT systems to target creative workflows, design tools, and innovation ecosystems, all areas that are historically overlooked by cybersecurity controls.

Business-Level Implications

Business Risk	What It Means for Your Organization
Expansion of Attack Surface	Design, engineering, R&D, marketing, product development, and creative assets now represent meaningful cyber risk.
Exploitation of "Trusted Tools"	Emerging attacks are leveraging widely used platforms (Blender, Unreal, GitHub, Figma), where users implicitly trust downloaded files.
AI-Assisted Attack Evolution	StealC V2 demonstrates rapid mutation, modular payload delivery, and use of Pyramid C2 infrastructure, evading traditional tools.
Credential Theft as Ransomware Fuel	These campaigns start not with encryption, but with credential harvesting, leading to data theft, persistence, and supply chain compromise.
EDR/MDR Limitations	These fileless, script-based malware strains have extremely low detection rates across AV and EDR platforms.

Key Takeaways for CEOs, CIOs & CISOs

1. Cyber Risk Is Moving Beyond Traditional IT

   Attackers are targeting creative organizations, game development, digital content providers, higher education, film/media, and manufacturing, exploiting legitimate tools used in design, animation, and 3D rendering.

2. Blender, CAD, Unity, Unreal Engine, and Adobe may now be part of your cyber risk surface

   These platforms allow embedded scripting, automation, or plugin execution; an attractive entry point for attackers.

3. The First Stage of Ransomware Is No Longer Encryption – It's Theft

   StealC V2 is designed to extract credentials, establish persistence, and enable silent access for weeks or months, creating a launchpad for ransomware or extortion. StealC V2 quickly enables full account takeover, MFA bypass, and cloud/system exploitation, without triggering alerts.

4. Traditional EDR, AV, and Sandbox tech struggle to detect these threats

   Malware runs in-memory, uses legitimate tools (PowerShell, Python), and executes without dropping files, bypassing signature-based and behavioral security tools.

How Morphisec Stops These Attacks Before They Execute

Morphisec's prevention-first platform uses Automated Moving Target Defense (AMTD) to block fileless, memory-based attacks before execution, stopping StealC and similar malware at the earliest stage without signatures, alerts, or performance impact.

Morphisec Advantage	What It Prevents
Decoy credentials injected into memory	Detects credential theft attempts instantly
Memory-based deception	Stops fileless and reflective loaders
Deterministic pre-execution prevention	Blocks malware before it runs, not after
No alert fatigue	No dwelling, triage, or manual investigation required
Zero impact on productivity or workflows	No sandboxing, no isolation, no scanning delays

Why Business Leaders Should Care

This emerging class of attacks represents more than a cybersecurity issue. It's a business risk, affecting:

- Intellectual property protection
- Secure product development (film, gaming, CAD, manufacturing)
- Cloud and supply chain integrity
- Digital brand trust
- M&A due diligence and risk assessment
- Compliance (SOX, GDPR, SOC2, NIST, HIPAA)

Strategic Actions for Security Leadership

Priority	Leadership Action
Expand risk lens	Include creative tools, 3D/modeling environments, design studios, and remote contractors in cyber risk analysis.
Assume stealers precede ransomware	Credential theft and data exfiltration are now Stage 1 of modern ransomware/ intrusion campaigns.
Move past detection-first strategies	Adopt prevention-first capabilities that stop attacks before execution, not after alerting.
Protect high-risk roles	Secure R&D, product design, media/marketing, and game/content development environments.
Test EDR & MDR limitations with trials	Detect the blind spots in existing detection-based tech, especially fileless attacks.

See Morphisec Stop StealC V2 in Real-Time

Zero signatures. No dwell time. Real prevention, not detection.

Request a demo and learn how AMTD prevents credential theft, data exfiltration, and ransomware before they begin.

Get a Demo

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. Shrink your attack surface faster to prevent ransomware entry. Eliminate blind spots across complex environments that attackers exploit for ransomware campaigns.

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.

To learn more, visit morphisec.com