MORPHISEC

Executive Briefing

Emerging Threat: PyStoreRAT – A Modular, Fileless JavaScript RAT Delivered Through Weaponized GitHub Repositories

How a New Multi-Stage RAT Exploits Developer Trust, Bypasses Modern EDR and Enables Stealthy Credential Theft, Payload Delivery & Ransomware Staging

Overview: A New Class of Developer-Focused Supply Chain Attacks

Morphisec Threat Labs has identified PyStoreRAT, a previously undocumented, multi-stage, JavaScript-based Remote Access Trojan (RAT) delivered through weaponized GitHub repositories disguised as developer utilities and OSINT tools. These repositories contain lightweight Python or JavaScript loader stubs that silently download and execute a remote HTA file, launching the full RAT via mshta.exe.

PyStoreRAT is far more than a simple backdoor. It is:

- Modular
- Multi-stage
- Fileless at launch
- Designed for evasion
- Architected to deploy highly dangerous follow-on payloads (including Rhadamanthys stealer)

It supports execution of EXE, DLL, MSI, Python, PowerShell, JavaScript, and HTA payloads, making it one of the most versatile RATs observed in recent campaigns.

Read the Complete Analysis

This campaign deliberately exploits the trust developers place in open-source ecosystems, particularly GitHub, an attack vector rapidly becoming a preferred distribution channel for threat actors.

Business-Level Implications

Business Risk	What It Means for Your Organization
Developer Workflow Exploitation	Compromise of engineering workstations leads directly to source code theft, CI/CD contamination and supply chain impact.
GitHub & Open-Source Ecosystem Abuse	Attackers now use community-trusted platforms to deliver malware, bypassing email gateways and traditional threat filters.
Highly Modular Payload Delivery	PyStoreRAT can deploy multiple malware families (stealers, worms, ransomware loaders) within minutes.
Advanced Evasion of Leading EDR Vendors	Built-in checks specifically evade CrowdStrike Falcon and others, undermining confidence in detection-first tools.
Credential Theft & Lateral Movement	The RAT gathers privileged system data, enumerates AV tools, targets crypto wallets and enables further compromise.

This represents a shift toward multi-language, script-based implants designed for stealth, automation, and long-term persistence, which is particularly effective against developer ecosystems.

Key Takeaways for CEOs, CIOs & CISOs

1. **Developer Environments Are Now High-Value Targets**
   Attackers increasingly target engineers, researchers and OSINT practitioners—roles often under protected compared to traditional IT.

2. **GitHub & Open-Source Trust Is Actively Exploited**
   Organizations relying on public repositories face a growing vector for dependency poisoning, RAT delivery and supply chain compromise.

3. **Credential Theft Is the New First Stage of Ransomware**
   PyStoreRAT deploys info-stealers like Rhadamanthys and gathers sensitive authentication data for use in persistence and extortion operations.

4. **Fileless, Script-Based Implants Evade Traditional EDR**
   The RAT uses:
   - HTA execution
   - Obfuscated JScript
   - Manual JSON parsing to evade EDR hooks
   - mshta.exe reflective loading
   - Falcon-specific anti-analysis logic

   These techniques bypass signature-based, behavior-based, and ML-based detection strategies.

How Morphisec Stops These Attacks Before They Execute

Morphisec's Automated Moving Target Defense (AMTD) technology prevents PyStoreRAT at the earliest possible stage by denying malware the ability to execute within memory.

Morphisec Advantage	What It Prevents
Pre-Execution Blocking	Stops mshta.exe-initiated RATs before they assemble payloads in memory.
Deception-Based Credential Protection	Prevents credential theft used to escalate attacks.
Memory-Based Obfuscation Disruption	Disarms reflective loaders, bypassing the RAT's stealth chain.
Deterministic Prevention	Eliminates reliance on signatures, heuristics, or behavioral detection.
Zero Impact on Developer Productivity	No sandboxing delays, scanning latency, or workflow disruption.

Morphisec halted PyStoreRAT before it could deploy Rhadamanthys or establish long-term persistence, preventing full compromise of the target systems.

Why Business Leaders Should Care

PyStoreRAT demonstrates a clear evolution toward stealth-first, developer-focused malware. The risks extend across:

- Intellectual property and source code theft
- Compromise of product and software supply chains
- Engineering workflow disruption
- Cloud access and MFA bypass
- Compliance exposure (SOX, SOC2, NIST, GDPR)
- Cyber insurance implications
- High-impact extortion operations

Developer workstations are the “new crown jewels.” Losing control of them threatens the entire business.

Strategic Actions for Security Leadership

Priority	Leadership Action
Expand risk lens	Include developers, OSINT teams, automation engineers and contractors in cyber risk assessments.
Harden open-source workflows	Validate repository trust, enforce dependency scanning, and monitor GitHub interactions.
Assume stealers precede ransomware	Build controls around credential protection and pre-execution prevention.
Move past detection-first strategies	Adopt prevention-first security capable of stopping fileless, modular implants.
Validate EDR limitations	Test existing tools against mshta.exe, JScript, HTA loaders, and Python stagers.

See Morphisec Stop PyStoreRAT in Real-Time

Experience how Morphisec blocks fileless, developer-targeted attacks like PyStoreRAT before execution, before payload assembly and before credential theft begins.

Request a demo and learn how AMTD stop credential theft, data exfiltration, and ransomware cold.

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