Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

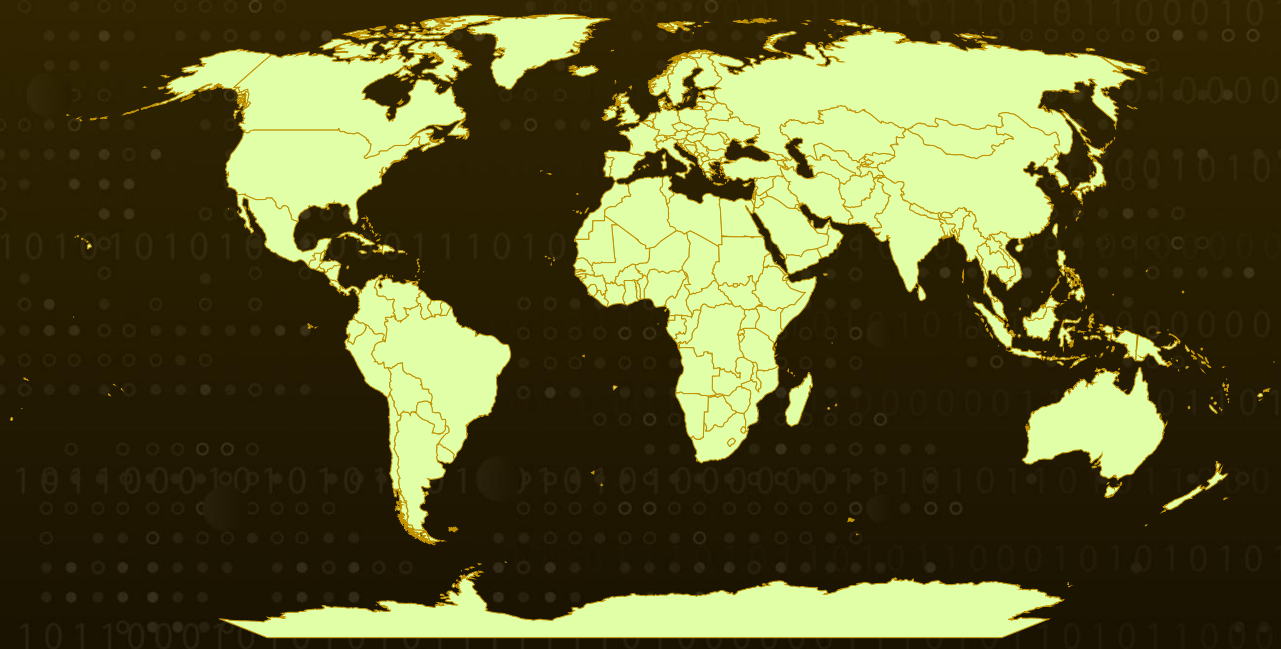
SilentSync RAT Hides in Plain Sight on PyPI

Date of Publication	Admiralty Code	TA Number
September 19, 2025	A1	TA2025289

Summary

Attack Discovered: August 4, 2025
Targeted Countries: Worldwide
Affected Platforms: Windows, Linux, macOS
Malware: SilentSync
Attack: Two seemingly harmless Python packages on PyPI, sisaws and secmeasure, were uncovered as delivery vehicles for a cross-platform RAT known as SilentSync. Disguised as utilities for government API integration and text processing, they concealed hidden backdoors that quietly pulled down SilentSync, granting attackers persistence, remote control, and the ability to steal browser data, files, and even screenshots. This case highlights how a routine pip install can turn into a serious supply-chain threat if dependencies aren't closely scrutinized.

Attack Regions



Attack Details

#1 On August 4, 2025, two malicious Python packages were flagged on PyPI: sisaws and secmeasure. At first glance, they appeared to be legitimate utility libraries, but both act as delivery mechanisms for a Remote Access Trojan dubbed SilentSync. The attackers used subtle impersonation techniques to get these packages noticed and imported by developers, turning everyday dependency installs into an infection vector.

#2 The sisaws package was crafted to mimic legitimate wrappers around public government APIs. It reproduces expected behaviors, input validation, dictionary-wrapped responses, timestamps, and role fields, so casual inspection looks normal. Hidden behind that façade is a backdoor-style function in the package initialization that only triggers when supplied with a specific token. When called correctly, it returns a forged API-like payload that masks its true intent.

#3 Beyond the initialization backdoor, sisaws' search() routine enforces use of a secondary token and reaches out to a hardcoded external endpoint. The code processes the server response unusually, trimming the first four characters and feeding the remainder into ast.literal_eval(), which tightly couples expected behavior to the actor's custom-made server-side output format. If a developer invokes the malicious initializer, the package decodes a hex string that reveals a curl command; that command pulls down an additional Python script. Although the current distribution focuses on Windows targets, the SilentSync RAT itself contains capabilities for Linux and macOS as well.

#4 The second package, secmeasure, was uploaded by the same author and similarly camouflages its true purpose. It provides a suite of innocuous string-manipulation helpers (things like whitespace stripping, HTML-escaping, Unicode normalization, and simple hex/ASCII helpers), but it also hides a malicious routine that runs the same hex-encoded curl chain used by sisaws to fetch and install SilentSync. Metadata and release activity overlap between the two packages, identical or related author emails, package names, and a burst of four releases across two days, which links them to the same campaign.

#5 SilentSync, the payload delivered by both packages, is a cross-platform Python RAT that achieves persistence via platform-specific mechanisms and speaks to its command-and-control over plain. Its capabilities include harvesting browser-stored credentials and cookies, executing arbitrary shell commands, taking screenshots, and exfiltrating files or entire directories; it also removes artifacts after operations to impede detection. This incident underscores the supply-chain risk posed by malicious packages in public repositories: dependencies require careful vetting, pinned versions, and automated scanning, because a single import can quietly turn a benign application into a foothold for data theft.

Recommendations

- **Double-check what you install:** Before adding a Python package from PyPI, take a moment to verify the name, author, and version. Typosquatted packages like sisaws can look almost identical to legitimate ones; a single extra letter can mean downloading malware instead of a real library.
- **Use trusted sources and reviews:** Stick to well-known, established packages with active communities and good documentation. Check download numbers, project pages, and whether the code is maintained. Unknown packages with little history or activity are riskier.
- **Scan dependencies automatically:** Set up automated tools in your development environment or CI/CD pipeline to scan for malicious or vulnerable packages. This ensures you don't rely only on manual checks and can catch hidden threats earlier.
- **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	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0010** Exfiltration
TA0011 Command and Control	**T1547** Boot or Logon Autostart Execution	**T1555** Credentials from Password Stores	**T1071** Application Layer Protocol
T1140 Deobfuscate/Decode Files or Information	**T1082** System Information Discovery	**T1195** Supply Chain Compromise	**T1059** Command and Scripting Interpreter

T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers	T1113 Screen Capture	T1027 Obfuscated Files or Information
T1036 Masquerading	T1106 Native API	T1547.001 Registry Run Keys / Startup Folder	T1539 Steal Web Session Cookie

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	327233d73236ca4d7c18ffd8f9924127, 9a092bbfc5325cbfca2f9807d074616a, 3918cace55342909c8309ec37d0207fd
URL	hxxps[:]//pastebin[.]com/raw/jaH2uRE1
IPv4	200[.]58[.]107[.]25
SHA256	bbe8f3e78ca09b8deb0d476d45bedc2aa1401916e5de20819d9e745e2b7d3ab0

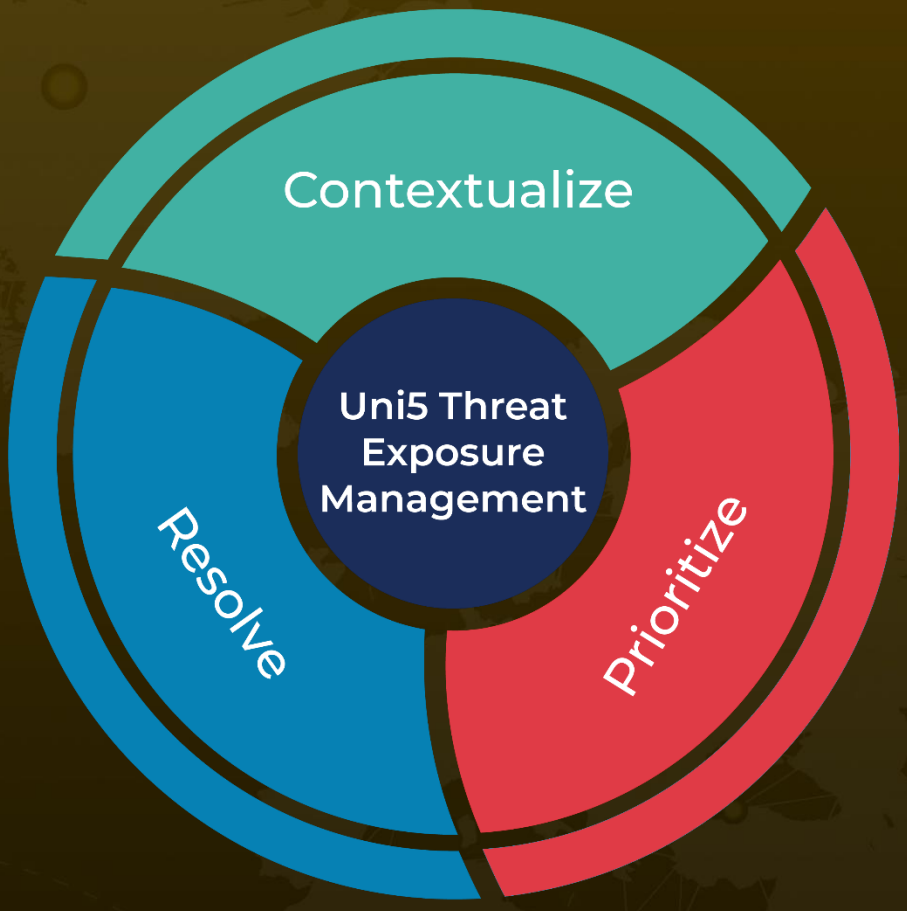
References

https://www.zscaler.com/blogs/security-research/malicious-pypi-packages-deliver-silentsync-rat#indicators-of-compromise--iocs-

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

September 19, 2025 • 5:50 AM

More at www.hivepro.com