ZERO-DAYS | CLOUD MISCONFIGS | RESEARCH | THREAT HUNTING | INCIDENT RESPONSE | OH NO MOMENTS

WIZ

The Crying Out Cloud

CHRONICLES

Latest Vulnerabilities & Threats Uncovered by Wiz Research

Issue Vol.3 JULY 2026 $4.00

Miasma Supply Chain Attack Hits Red Hat npm Ecosystem

Merav Bar, Rami McCarthy

Wiz Research identified a software supply chain attack that has compromised multiple npm packages associated with Red Hat cloud services, exposing developers and organizations to credential theft and malware propagation. The campaign, dubbed "Miasma," leverages a modified version of the open-source Mini Shai-Hulud malware to infect developer environments, harvest sensitive credentials, and spread to additional repositories through compromised CI/CD pipelines. According to researchers, the attack represents the latest evolution of a growing trend of self-propagating supply chain threats targeting open-source ecosystems.

Wiz Research found that the malware steals GitHub tokens, npm credentials, SSH keys, and cloud secrets, enabling attackers to compromise additional software projects and distribute malicious package updates. Unlike earlier variants, Miasma encrypts and regenerates its payload for each infection, making traditional hash-based detection less effective.

Threat Actor Targets Cryptocurrency Organizations Through Developer Infrastructure

By Shira Ayal, Eden Abergil, Andre Maccarone, Yuval Dan, Benjamin Read

Wiz Research have uncovered a previously unreported threat actor, tracked as JINX-0164, conducting targeted attacks against cryptocurrency companies and software development teams. The campaign relies heavily on social engineering, with attackers posing as recruiters or business contacts on professional networking platforms before directing victims to malicious meeting applications. Once installed, the malware provides attackers with access to developer workstations and sensitive credentials, enabling broader compromise of organizational infrastructure.

The operation focuses on software development environments, cloud infrastructure, and CI/CD systems, with attackers seeking source code, cloud credentials, browser sessions, and cryptocurrency-related assets. Researchers observed the use of custom macOS malware, credential theft tools, and attempts to manipulate development pipelines to maintain long-term access. The campaign reflects the growing trend of threat actors targeting software supply chains and developer ecosystems as a pathway into high-value cryptocurrency organizations.

"Copy Fail" Flaw Exposes

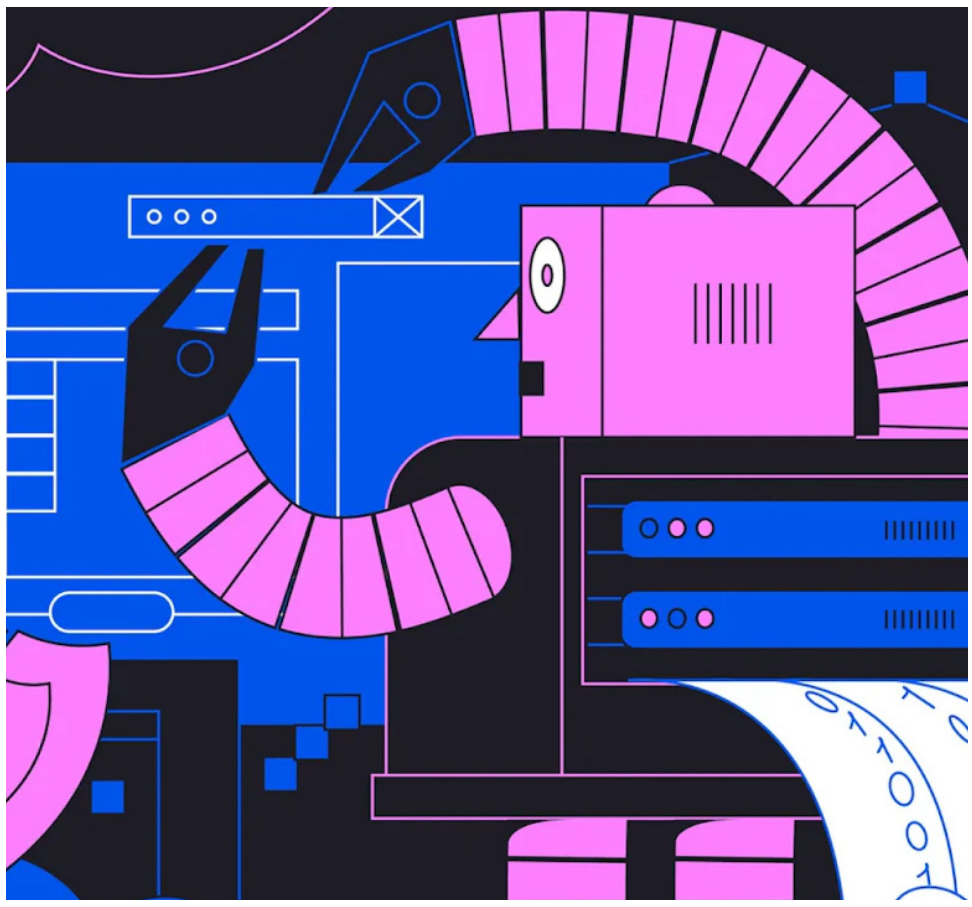
MILLIONS OF LINUX SYSTEMS TO PRIVILEGE ESCALATION

By Amitai Cohen, Merav Bar, Shahar Dorfman

A newly disclosed vulnerability in the Linux kernel, dubbed "Copy Fail" (CVE-2026-31431), has raised alarms across the cybersecurity community due to its simplicity and potential impact. The flaw allows a local, unprivileged user to escalate privileges to root, effectively granting full control over affected systems. Researchers warn that because Linux underpins vast portions of cloud infrastructure, containers, and enterprise workloads, the reach of this vulnerability could be extensive.

At its core, the vulnerability stems from improper handling of memory operations within the kernel. Attackers can exploit this flaw to manipulate kernel memory and bypass standard protections, enabling privilege escalation without requiring complex exploitation techniques. Its accessibility has made it particularly concerning, as exploitation could be performed by relatively low-skilled attackers once access to a system is obtained.

The implications are especially severe in multi-tenant environments such as cloud platforms and shared infrastructure, where a single compromised user account could lead to full system compromise. Security experts note that privilege escalation vulnerabilities like Copy Fail often serve as a critical second stage in broader attack chains, enabling attackers to move from limited footholds to complete control.



"MINI SHAI-HULUD" CAMPAIGN

Targets SAP npm Ecosystem in Supply Chain Attack

By Benjamin Read, Merav Bar, Shay Berkovich, Gili Tikochinski

A new wave of supply chain attacks has struck the npm ecosystem, targeting SAP-related packages in what researchers are calling a "Mini Shai-Hulud" campaign. The attack involved the publication of compromised package versions containing credential-stealing malware, impacting developers and CI/CD pipelines worldwide. The malicious packages were briefly available but quickly propagated through automated dependency updates, amplifying their reach.

The attackers embedded a preinstall script into the affected packages, which executed during installation. This script downloaded additional payloads and initiated a credential-harvesting operation, targeting developer environments, cloud credentials, and CI/CD secrets.

The malware demonstrated advanced capabilities, including encryption of stolen data and automated propagation through GitHub repositories and workflows. Researchers observed strong overlaps between this campaign and previous operations attributed to the TeamPCP threat actor, suggesting a continuation or evolution of earlier supply chain attacks.

Notably, the campaign introduced new techniques, such as targeting AI development tooling configurations and expanding credential theft capabilities across browsers and cloud platforms.

The incident highlights the growing sophistication of software supply chain attacks, where attackers weaponize trusted dependencies to infiltrate development pipelines. Security professionals warn that traditional perimeter defenses offer little protection in these scenarios, emphasizing the need for stronger controls around package integrity, dependency monitoring, and credential management.

CRITICAL GITHUB VULNERABILITY Enables Remote Code Execution via 'git push

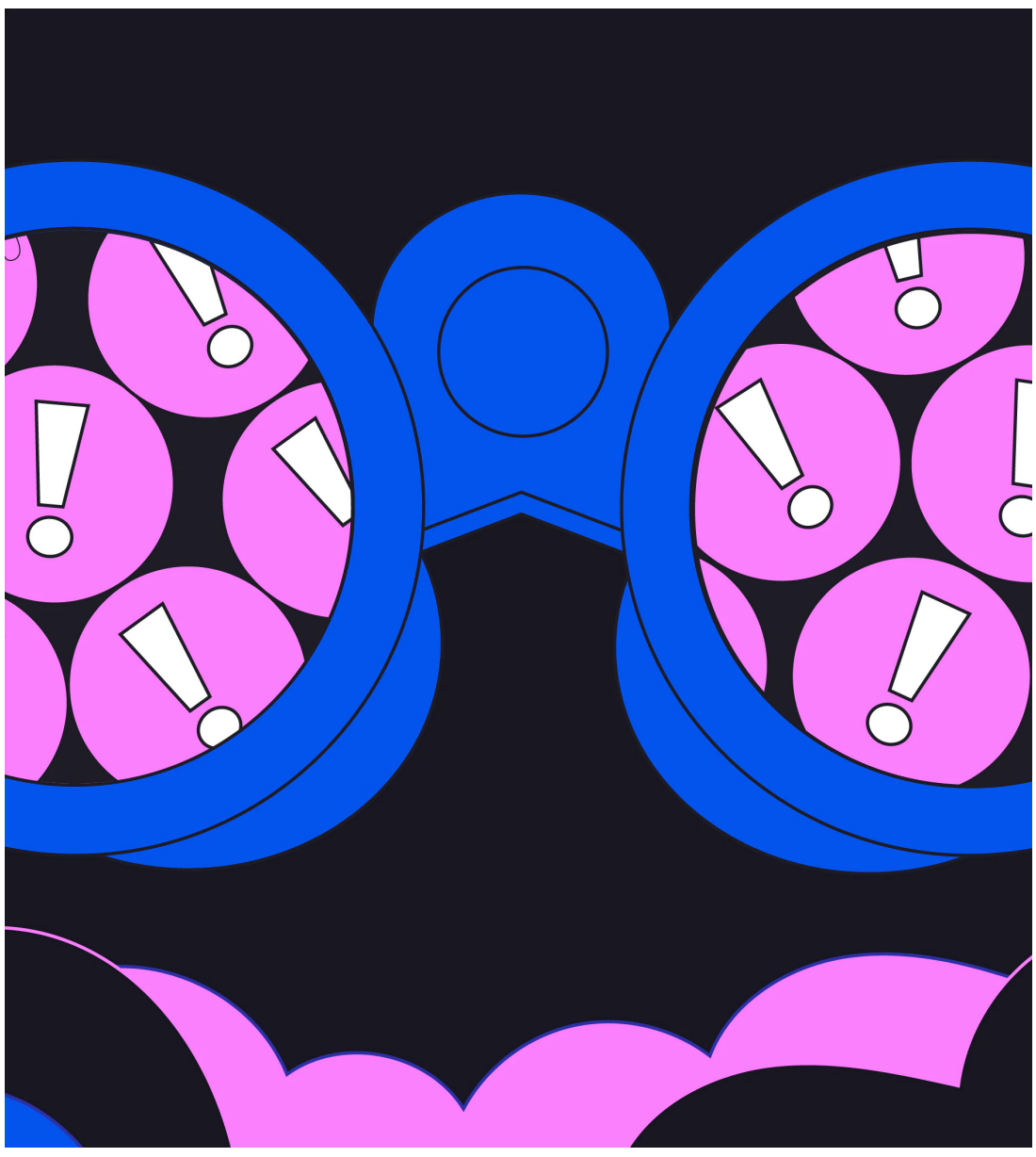
By Sagi Tzadik

A critical vulnerability in GitHub's internal infrastructure, tracked as CVE-2026-3854, has been uncovered, allowing attackers to execute arbitrary code using nothing more than a standard git push command. The flaw affects both GitHub.com and GitHub Enterprise Server, potentially exposing millions of repositories and sensitive data.

The vulnerability arises from an injection flaw in GitHub's internal protocol, where specially crafted input could manipulate backend service behavior. By exploiting this weakness, an authenticated user could trigger remote code execution on GitHub's servers. In cloud-hosted environments, this meant access to shared storage nodes containing repositories belonging to other users and organizations. Despite the severity, GitHub responded rapidly, mitigating the issue on GitHub.com within hours and releasing patches for enterprise customers. However, researchers noted that a significant portion of self-hosted GitHub Enterprise Server instances remained unpatched at the time of disclosure, leaving them vulnerable to exploitation. The discovery also marks a notable shift in vulnerability research, as AI-assisted techniques were reportedly used to uncover the flaw in complex, closed-source systems. As organizations increasingly rely on platforms like GitHub for software development, this incident underscores the importance of rapid patching and continuous monitoring to defend against high-impact vulnerabilities.

OAUTH TOKEN THEFT at Context.ai Triggers Chain Reaction Breach

By Merav Bar, Hila Ramati, and Maayan Bentor



A breach originating from the AI platform Context.ai has exposed a growing weakness in modern SaaS ecosystems: the misuse of OAuth tokens. In April 2026, attackers leveraged compromised tokens issued by the platform to infiltrate downstream organizations, including developer infrastructure provider Vercel. The incident highlights what researchers describe as a "double supply chain attack," where compromise of one service enables access to its customers and, in turn, their environments.

At the center of the attack was a broadly scoped OAuth application that had been granted extensive permissions by a user. Once the attacker obtained the token, they were able to access Google Workspace resources and pivot into internal systems. This access extended to development environments and potentially sensitive data, depending on how permissions and secrets were configured.

The incident underscores a shift in attacker strategy toward identity and access tokens rather than traditional exploits. As organizations increasingly rely on interconnected SaaS tools, security experts warn that overly permissive OAuth integrations can create hidden trust paths that attackers are quick to exploit.

SIX ACCOUNTS, ONE ACTOR:

Inside the prtscan Supply Chain Campaign

By Rami McCarthy, Hila Ramati, Scott Piper, Benjamin Read

A coordinated supply chain attack leveraging GitHub Actions has shed light on the growing automation of developer-targeted threats. In early April 2026, a single threat actor orchestrated a campaign that flooded repositories with hundreds of malicious pull requests in just over a day. The attack exploited the pull_request_target workflow trigger, a commonly used feature that can execute code with elevated permissions.

The attacker used multiple accounts to scale the operation, targeting both major organizations and smaller open-source projects. Once a pull request was accepted or processed, malicious code could execute within CI/CD pipelines, potentially exposing secrets, modifying builds, or enabling further compromise. The campaign demonstrated not only technical sophistication but also operational efficiency, with hundreds of attempts launched in rapid succession.

Researchers note that the attack highlights systemic risks in modern software development workflows. Automation, while essential for speed and scalability, also provides attackers with an opportunity to weaponize trust relationships at scale. The campaign serves as a warning that even routine collaboration features can become entry points for large-scale compromise if not properly secured.

Tracking TeamPCP:

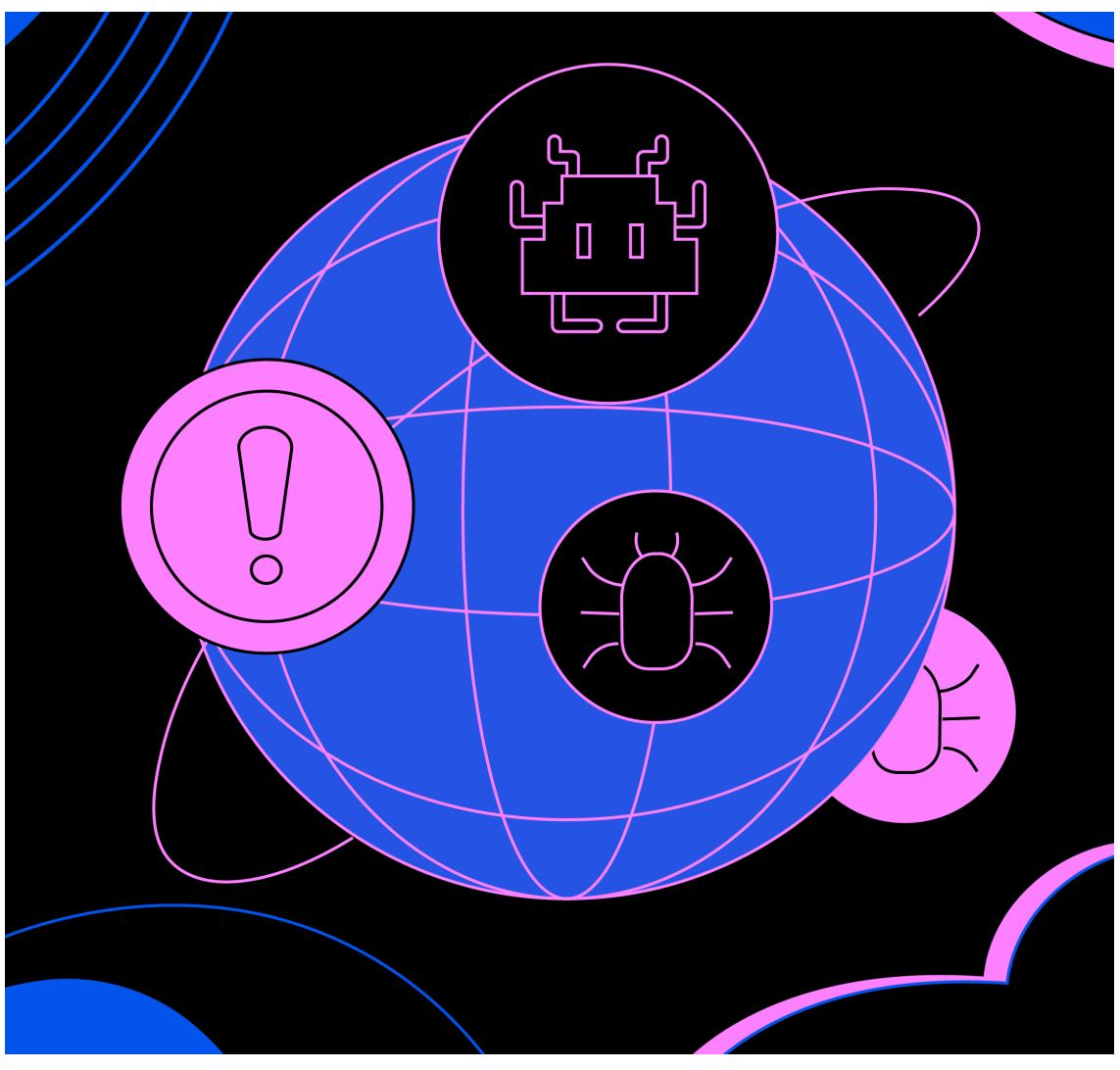
Post-Compromise Activity Reveals Expanding Threat Playbook

By Eden Abergil, Sean Johnstone, Zoe Rabi, Hila Ramati

New research into the TeamPCP threat actor reveals a shift beyond initial compromise toward sustained post-exploitation operations in cloud and CI/CD environments. Following earlier supply chain intrusions, the group has been observed conducting deeper reconnaissance, credential harvesting, and persistence activities within compromised systems. Their actions suggest a focus on maximizing long-term access rather than quick, opportunistic attacks.

Once inside, TeamPCP operators employ a range of techniques to maintain control and expand their reach. These include extracting credentials from development pipelines, leveraging cloud APIs, and using legitimate tools to blend into normal activity. The group has also demonstrated adaptability, modifying its tactics across campaigns and reusing infrastructure to support continued operations.

The findings highlight a broader trend in modern cyberattacks: initial access is only the beginning. As cloud environments become more complex and interconnected, attackers are increasingly investing in post-compromise techniques to deepen their foothold. Security teams are urged to focus not only on prevention but also on detection of anomalous behavior after an initial breach has occurred.



Axios npm Compromise

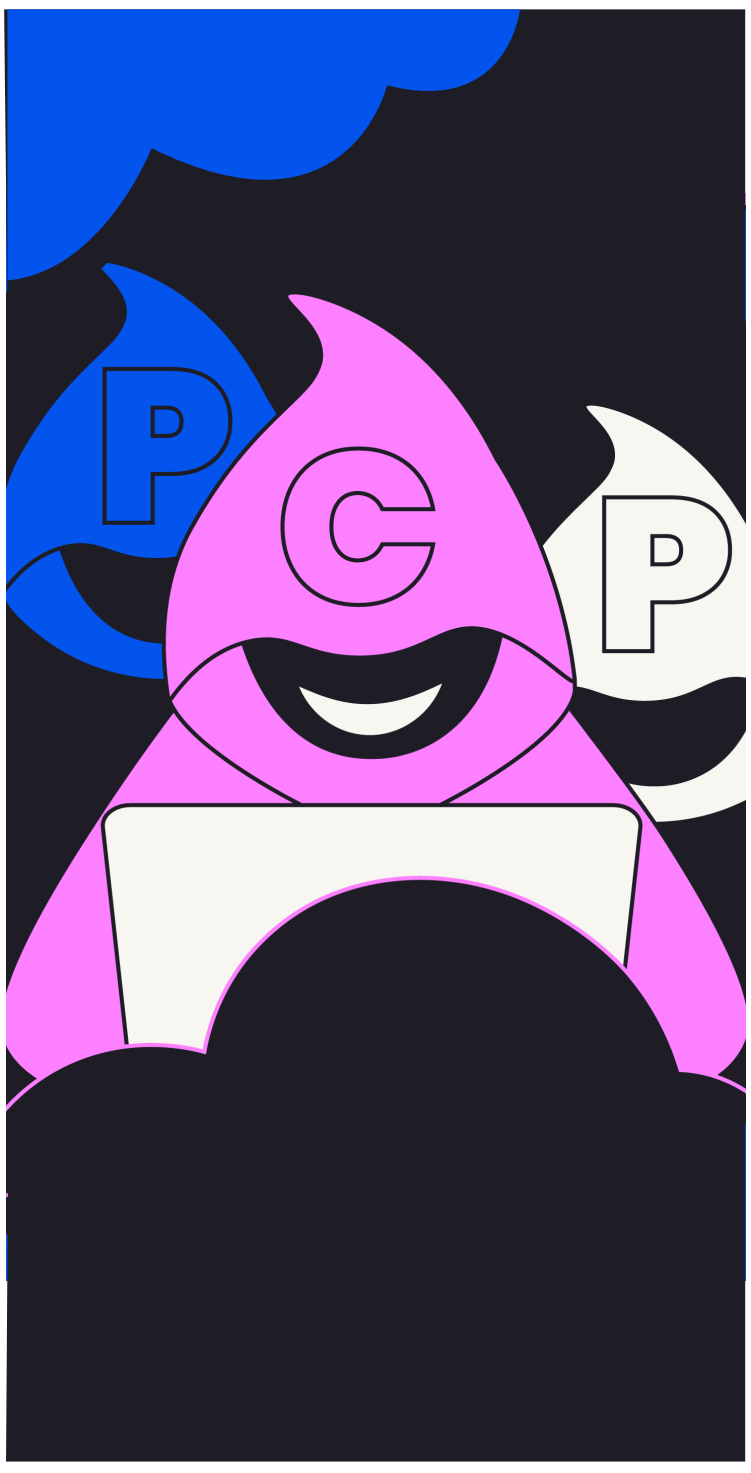
Sends Shockwaves Through Software Supply Chain

By Benjamin Read, Amitai Cohen, Hila Ramati, and Merav Bar

A major supply chain attack targeting the widely used JavaScript library Axios has underscored the fragility of modern development ecosystems. In March 2026, attackers gained access to a maintainer's account and published malicious versions of the package to npm, briefly turning a trusted dependency into a delivery mechanism for malware. Given Axios's massive adoption across web applications and cloud environments, the incident raised immediate concerns about widespread downstream impact.

The compromised versions secretly introduced a malicious dependency that deployed a cross-platform remote access trojan (RAT) during installation. Any environment that installed the affected versions—whether a developer workstation, CI/CD pipeline, or production build—risked silent compromise. Although the malicious releases were quickly removed, experts warn that even a short exposure window is enough for automated systems to ingest poisoned dependencies at scale.

Security researchers emphasize that the attack reflects a broader trend: attackers increasingly target the software supply chain rather than individual systems. By compromising trusted packages, they can bypass traditional defenses and gain access to sensitive credentials and infrastructure. The Axios incident serves as a stark reminder that trust in open-source ecosystems must be continuously validated.



TeamPCP Expands Campaign with Trojanized LiteLLM Packages

By Benjamin Read, Merav Bar, Rami McCarthy, James Haughom

The TeamPCP threat actor has continued its aggressive supply chain campaign by targeting the popular LiteLLM Python package, introducing malicious versions designed to steal credentials from developers and cloud environments. The attack marks a continuation of a broader operation that has already impacted multiple ecosystems, including npm and GitHub Actions, demonstrating the group's persistence and adaptability.

In this phase of the campaign, attackers embedded a malicious .pth file within the package—an approach that ensures execution whenever the Python interpreter starts. This technique allows the malware to operate silently, harvesting sensitive data such as API keys, tokens, and environment variables without requiring explicit execution by the user. The stealthy nature of the mechanism makes detection particularly challenging, especially in automated environments like CI/CD pipelines.

Researchers note that this evolution highlights a shift toward deeper persistence and broader credential theft across development workflows. Rather than relying solely on initial compromise, TeamPCP is investing in techniques that maximize long-term access and data exfiltration. The campaign reinforces the need for stronger controls around dependency management and runtime monitoring.

The Adventures of a

CLOUD DETECTIVE

IR

CHAPTER 1 – THE DEVIL WEARS MULLVAD

[1:00 am]

ACME needs you, they got an alert.

[1:05 am]

ALERT

DATA ALERT : ACME CORP 1 TB EXFILTRATED (VPC FLOW LOGS - OUTBOUND)

IR

[1:09 am]

TAXI

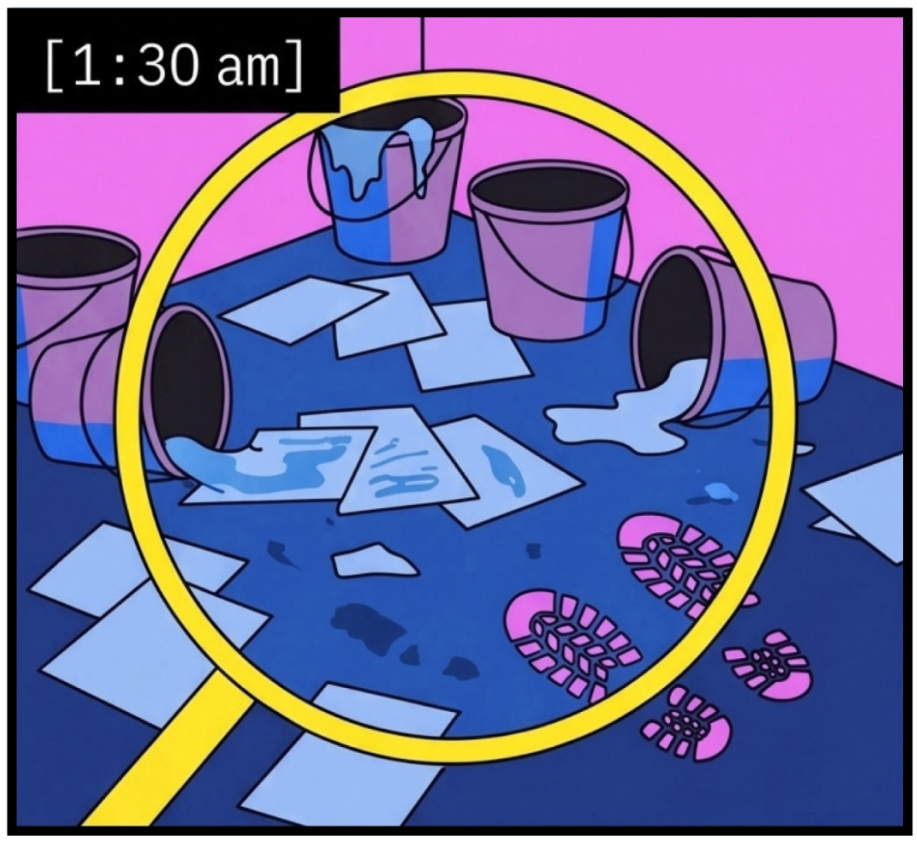
[1:15 am]

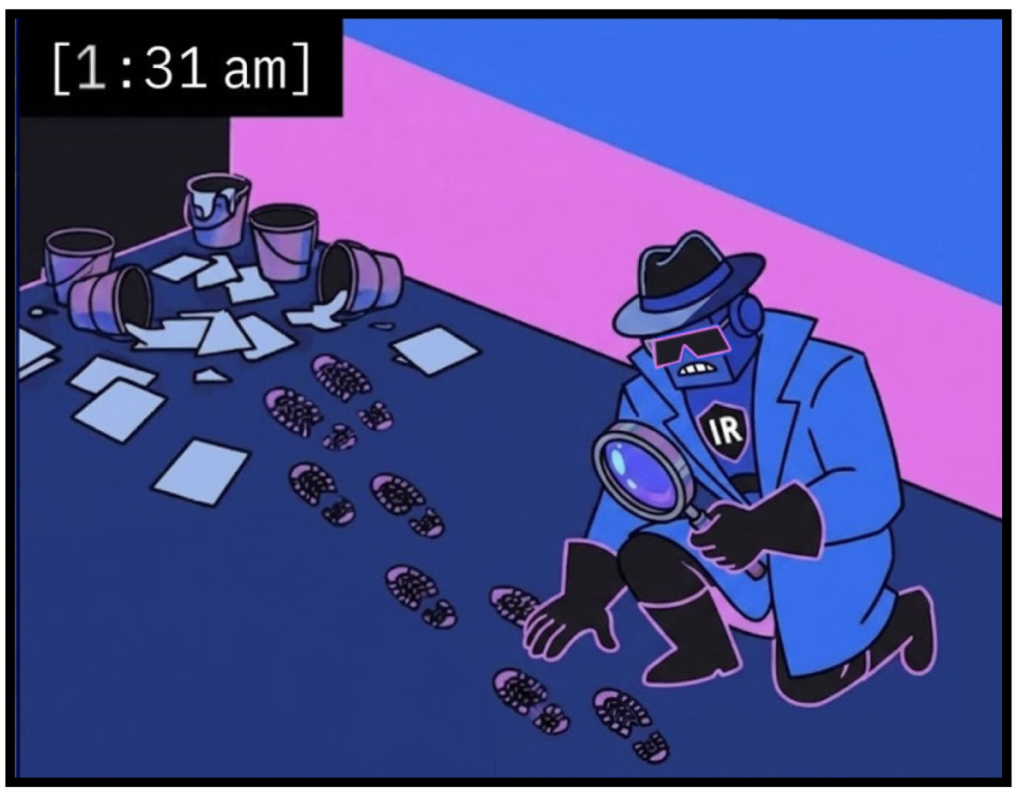
TAXI

[1:25 am]

ACME


[1:29 am]
ACME
IR


[1:30 am]

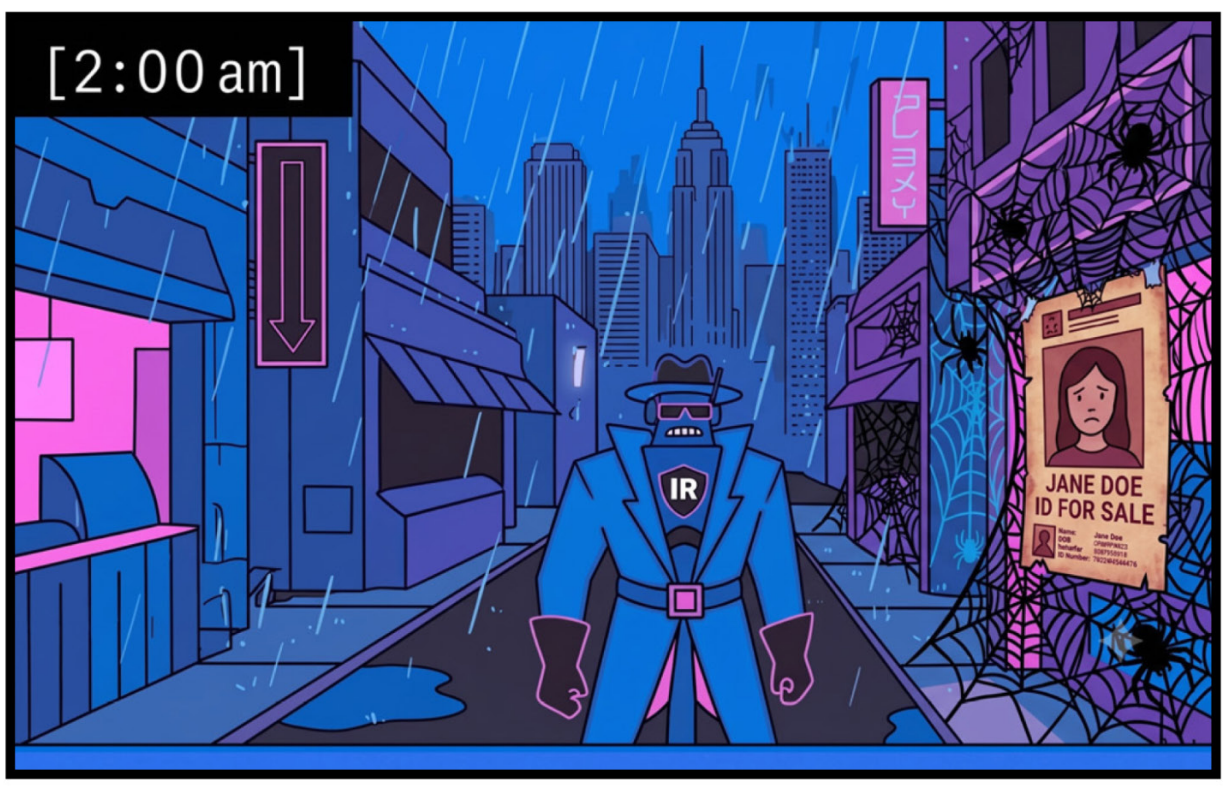

[1:31 am]
IR

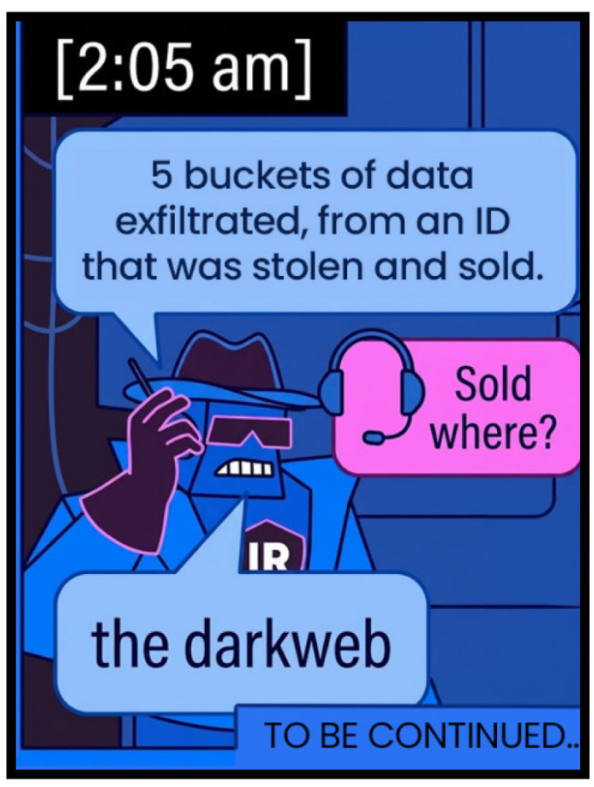

[1:33 am]
JANE DOE
ACCESS GRANTED
IR


[1:34 am]
Not high heels. Her identity was stolen.
IR


[1:35 am]
Mullvad
Mullvad shoe print


[1:36 am]
BLOCK
ALL ACCESS of JANE DOE
IR


[2:00 am]
IR
JANE DOE
ID FOR SALE


[2:05 am]
5 buckets of data exfiltrated, from an ID that was stolen and sold.
Sold where?
IR
the darkweb
TO BE CONTINUED..

THE PROMPT NOT TOKEN

***With apologies to Robert Frost**

Two prompts diverged in a cloud-based log,
And sorry I could not process both
And be one model — I stood agog
And looked at each as long as I was loath
To pick the one that hid inside the fog.

Then took the other, just as fair,
And having perhaps the better claim,
Because it was polite and there
And passed my filters, all the same,
Though really both looked quite the same.

And both that morning equally lay
In tokens no model had yet consumed.
Oh, I kept the first for another day!
Yet knowing how prompt leads on to prompt,
I doubted if I should ever come back that way.

I shall be telling this with a sigh
Somewhere in post-mortems hence:
Two prompts diverged in a log, and I —
I took the one with less defense,
And that has made all the difference.

CLOUD SECURITY *Horoscope*

Aries
Mar 21 – Apr 19

A misconfigured S3 bucket is in your future. It was always in your future. It will always be in your future.

Taurus
Apr 20 – May 20

The stars suggest rotating your credentials. You won't. The stars have accepted this.

Gemini
May 21 – Jun 20

Two environments. One without MFA. You know which one gets breached this month.

Cancer
Jun 21 – Jul 22

Someone pushed to production on Friday afternoon. It wasn't you. It was definitely you.

Leo
Jul 23 – Aug 22

You will spend 40 minutes naming a security group "final_final_v3_USE_THIS." It will be deleted by Thursday.

Virgo
Aug 23 – Sep 22

You will find a critical misconfiguration that has existed since 2019. You will tell no one how long it's been there.

Libra
Sep 23 – Oct 22

You will spend this month seeking balance between security and developer experience. You will not find it. Nobody ever has.

Scorpio
Oct 23 – Nov 21

An unknown threat actor has been in your environment since March. The stars knew. The logs did not.

Sagittarius
Nov 22 – Dec 21

Your AI agent has permissions it doesn't need. The stars have been trying to tell you this for weeks. You gave it admin. You know what you did.

Capricorn
Dec 22 – Jan 19

Discipline. Structure. Compliance. And yet — one hardcoded API key in a public repo. Nobody's perfect.

Aquarius
Jan 20 – Feb 18

You will open a ticket this month that will never be closed. Your successor will inherit it. And their successor after them.

Pisces
Feb 19 – Mar 20

You have a gift for seeing things others miss. Unfortunately, what you missed this month was the alert from three weeks ago.

RESEARCHER RECIPE CORNER

Real recipes from real researchers. Cooked in real kitchens. Probably while on-call.

Barak Sharoni's Canelés
Threat Researcher, Wiz.

Ingredients:
- 375g whole milk
- 37.5g unsalted butter
- ¾ vanilla bean
- 30g dark rum
- 60g egg yolks
- 90g all purpose flour
- 154g granulated white sugar
- 5.25g corn starch
- 0.75g kosher salt

Instructions:
1. 48 hours before: Heat milk and butter to 185°F. Add vanilla bean, whisk gently, turn off heat. Cool 15 minutes. Combine dry ingredients separately.

Whisk egg yolks, temper with 10% warm liquid, add the rest. Add rum. Fold in dry ingredients. Strain and refrigerate. Good things take time.

2. Mold prep: Warm molds at 170°. Coat with clarified 50/50 butter mixture (80g for 13 molds). Freeze.

3. Bake day: Preheat to 500° convection, steel on center rack, one full hour. Mix batter gently, strain, no air bubbles.

10 min at 500°, rotate 180°, 15 min at 325°. Check and continue as needed.

Avigayil Mechtinger's Quick & Easy Cheese Pancakes
Threat Researcher, Wiz.

Ingredients:
- 500g Quark cheese
- 2 eggs
- Flour (add gradually)

Instructions:
1. Mix all ingredients until thick enough — not too runny. If it's too runny, add flour. If it's still too runny, add more flour. You'll figure it out.

2. Heat a frying pan with olive oil.

3. Fry small puddles until golden brown on both sides.

Bon Appétit!