BITSIGHT Luminate EXCHANGE

02

The Mythos Effect:

The infinite attack surface & disappearance of enterprise boundaries

Assessing Claude Mythos Preview's cybersecurity capabilities

April 7, 2026

Nicholas Carlini, Newton Cheng, Keane Lucas, Michael Moore, Milad Nasr, Vinay Prabhushankar, Winnie Xiao

Hakeem Angulu, Evyatar Ben Asher, Jackie Bow, Keir Bradwell, Ben Buchanan, David Forsythe, Daniel Freeman, Alex Gaynor, Xinyang Ge, Logan Graham, Kyla Guru, Hasnain Lakhani, Matt McNiece, Mojtaba Mehrara, Renee Nichol, Adnan Pirzada, Sophia Porter, Andreas Terzis, Kevin Troy

Earlier today we announced Claude Mythos Preview, a new general-purpose language model. This model performs strongly across the board, but it is strikingly capable at computer security tasks. In response, we have launched Project Glasswing, an effort to use Mythos Preview to help secure the world's most critical software, and to prepare the industry for the practices we all will need to adopt to keep ahead of cyberattackers.

https://red.anthropic.com/2026/mythos-preview/

Novel and Not Yet Patched

"Over 99% of the vulnerabilities we've found have **not yet been patched**, so it would be irresponsible for us to disclose details about them"

BITSIGHT

Assessing Claude Mythos Preview's cybersecurity capabilities

April 7, 2026

Nicholas Carlini, Newton Cheng, Keane Lucas, Michael Moore, Milad Nasr, Vinay Prabhushankar, Winnie Xiao

Hakeem Angulu, Evyatar Ben Asher, Jackie Bow, Keir Bradwell, Ben Buchanan, David Forsythe, Daniel Freeman, Alex Gaynor, Xinyang Ge, Logan Graham, Kyla Guru, Hasnain Lakhani, Matt McNiece, Mojtaba Mehrara, Renee Nichol, Adnan Pirzada, Sophia Porter, Andreas Terzis, Kevin Troy

Earlier today we announced Claude Mythos Preview, a new general-purpose language model. This model performs strongly across the board, but it is strikingly capable at computer security tasks. In response, we have launched Project Glasswing, an effort to use Mythos Preview to help secure the world's most critical software, and to prepare the industry for the practices we all will need to adopt to keep ahead of cyberattackers.

https://red.anthropic.com/2026/mythos-preview/

Novel and Not Yet Patched
"Over 99% of the vulnerabilities we've found have **not yet been patched**, so it would be irresponsible for us to disclose details about them"

Vulnerabilities in Hardened Software
"Mythos Preview fully **autonomously** identified and then exploited a **17-year-old** remote code execution vulnerability in **FreeBSD** that allows anyone to gain root on a machine running NFS"

BITSIGHT

Assessing Claude Mythos Preview's cybersecurity capabilities

April 7, 2026

Nicholas Carlini, Newton Cheng, Keane Lucas, Michael Moore, Milad Nasr, Vinay Prabhushankar, Winnie Xiao

Hakeem Angulu, Evyatar Ben Asher, Jackie Bow, Keir Bradwell, Ben Buchanan, David Forsythe, Daniel Freeman, Alex Gaynor, Xinyang Ge, Logan Graham, Kyla Guru, Hasnain Lakhani, Matt McNiece, Mojtaba Mehrara, Renee Nichol, Adnan Pirzada, Sophia Porter, Andreas Terzis, Kevin Troy

Earlier today we announced Claude Mythos Preview, a new general-purpose language model. This model performs strongly across the board, but it is strikingly capable at computer security tasks. In response, we have launched Project Glasswing, an effort to use Mythos Preview to help secure the world's most critical software, and to prepare the industry for the practices we all will need to adopt to keep ahead of cyberattackers.

https://red.anthropic.com/2026/mythos-preview/

Novel and Not Yet Patched
"Over 99% of the vulnerabilities we've found have **not yet been patched**, so it would be irresponsible for us to disclose details about them"

Vulnerabilities in Hardened Software
"Mythos Preview fully **autonomously** identified and then exploited a **17-year-old** remote code execution vulnerability in **FreeBSD** that allows anyone to gain root on a machine running NFS"

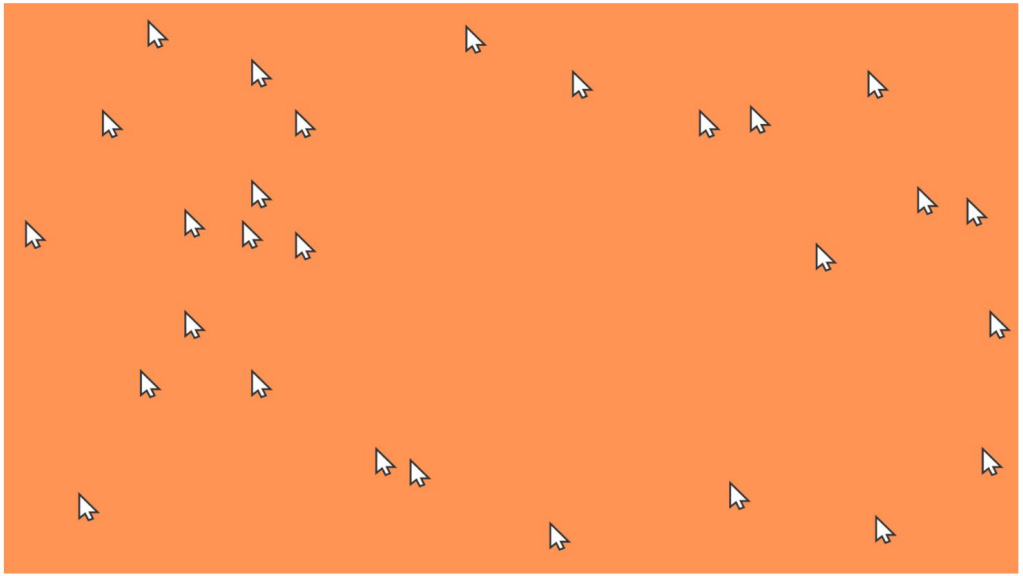
Exploits Generated Autonomously
"Each of the exploits below were written completely **autonomously**, without any human intervention after an initial prompt"

BITSIGHT

PRIVACY & SECURITY

The zero-days are numbered

APRIL 21, 2026 BOBBY HOLLEY



Large Number of New Vulnerabilities
"[W]e had the opportunity to apply an early version of Claude Mythos Preview to Firefox. This week's release of Firefox 150 includes fixes for **271 vulnerabilities identified during this initial evaluation.**"

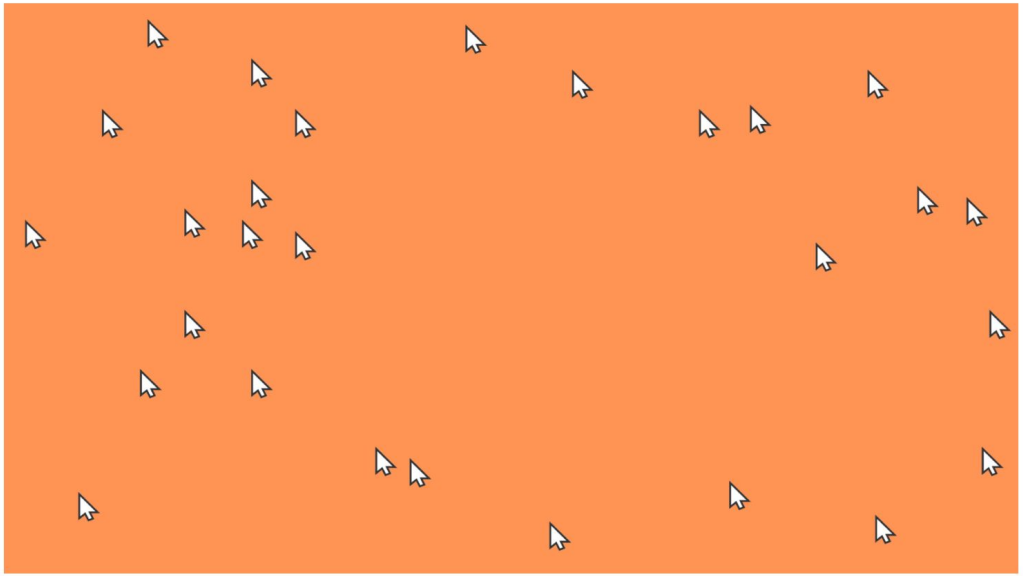
https://blog.mozilla.org/en/privacy-security/ai-security-zero-day-vulnerabilities/

BITSIGHT

PRIVACY & SECURITY

The zero-days are numbered

APRIL 21, 2026 BOBBY HOLLEY



https://blog.mozilla.org/en/privacy-security/ai-security-zero-day-vulnerabilities/

Large Number of New Vulnerabilities
"[W]e had the opportunity to apply an early version of Claude Mythos Preview to Firefox. This week's release of Firefox 150 includes fixes for **271 vulnerabilities identified during this initial evaluation.**"

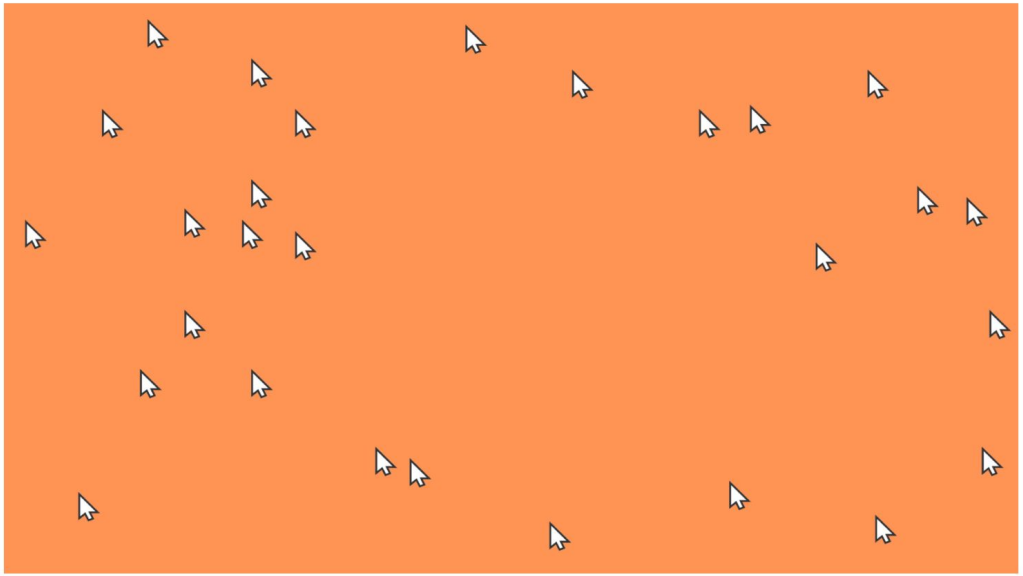
Dizzying Number to Deal With
"As these capabilities reach the hands of more defenders, many other teams are now experiencing the **same vertigo** we did when the findings first came into focus"

BITSIGHT

PRIVACY & SECURITY

The zero-days are numbered

APRIL 21, 2026 BOBBY HOLLEY



https://blog.mozilla.org/en/privacy-security/ai-security-zero-day-vulnerabilities/

Large Number of New Vulnerabilities
"[W]e had the opportunity to apply an early version of Claude Mythos Preview to Firefox. This week's release of Firefox 150 includes fixes for **271 vulnerabilities identified during this initial evaluation.**"

Dizzying Number to Deal With
"As these capabilities reach the hands of more defenders, many other teams are now experiencing the **same vertigo** we did when the findings first came into focus"

Changing the Game?
"Defenders finally have a chance to win, decisively"

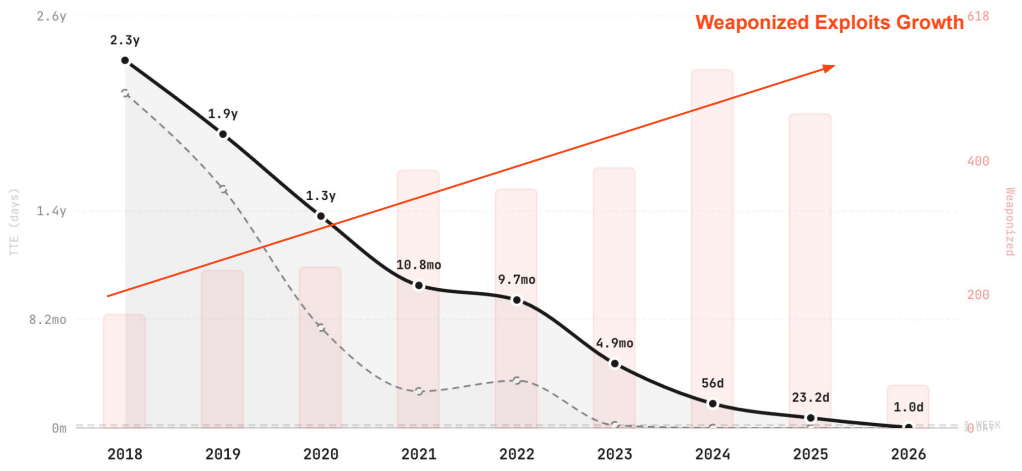
BITSIGHT

Zero Day Clock: Weaponized Exploits Growing

BITSIGHT Luminate EXCHANGE

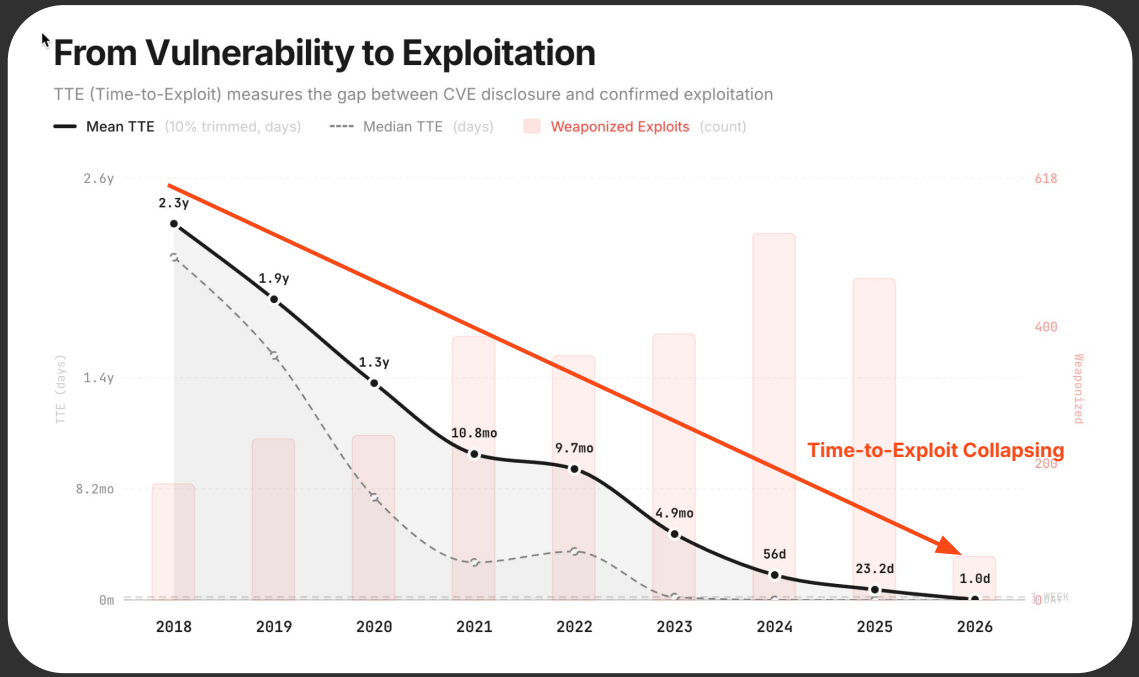
From Vulnerability to Exploitation

TTE (Time-to-Exploit) measures the gap between CVE disclosure and confirmed exploitation



Zero Day Clock: Time-to-Exploit Collapsing

BITSIGHT Luminate EXCHANGE



Moody's Report: AI Uncovering Software Bugs

BITSIGHT Luminate EXCHANGE

MOODY'S RATINGS

Cross-Sector

SECTOR IN-DEPTH
18 March 2026

Send Your Feedback

TABLE OF CONTENTS

Cybersecurity – Global

AI is uncovering software bugs faster than firms can patch them

Summary

New artificial intelligence (AI) tools are becoming powerful assistants in identifying weaknesses in software coding that hackers can exploit for unauthorized network access. While this is a positive development for software security, in practice it has meant that some corporate cybersecurity teams are struggling to keep up. At a time when criminals a accelerating their attacks on identified software vulnerabilities, an inability to patch them quickly enough leaves enterprises increasingly exposed to cyber breaches and the operati damage and disruption they can cause.

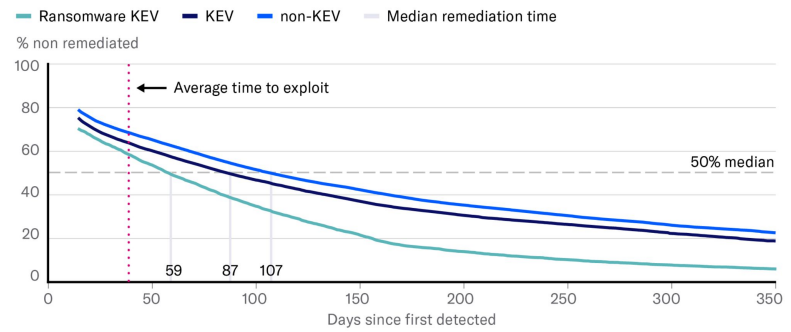
» **Software vulnerabilities are a prime vector for unauthorized network access.** Today's complex and widely reused codebases often contain human errors that attack can exploit at scale. Because many breaches begin by leveraging known but unpatched software flaws, minimizing vulnerabilities and reducing exposure time would reduce b the likelihood and, in many cases, the severity of cyber incidents.

» **AI shows significant promise in identifying software flaws.** AI tools have uncover

Exhibit 7

Remediation times lag the average time to exploit

Share of vulnerabilities that remain externally observable, by days since first detection* and vulnerability type



*We analyzed all vulnerabilities first observed in the last two years.

Sources: Moody's Ratings, Bitsight Technologies

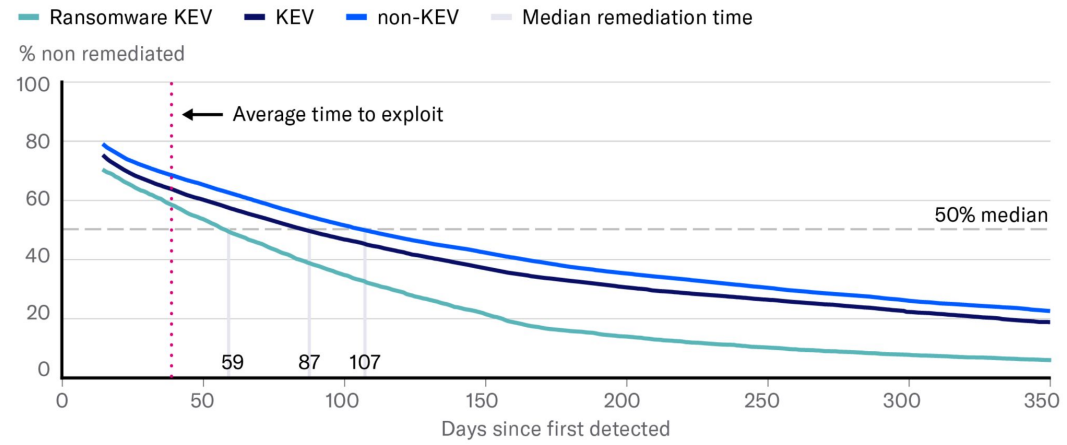
BITSIGHT

Time to Remove Vulnerabilities Remains Slow

Exhibit 7

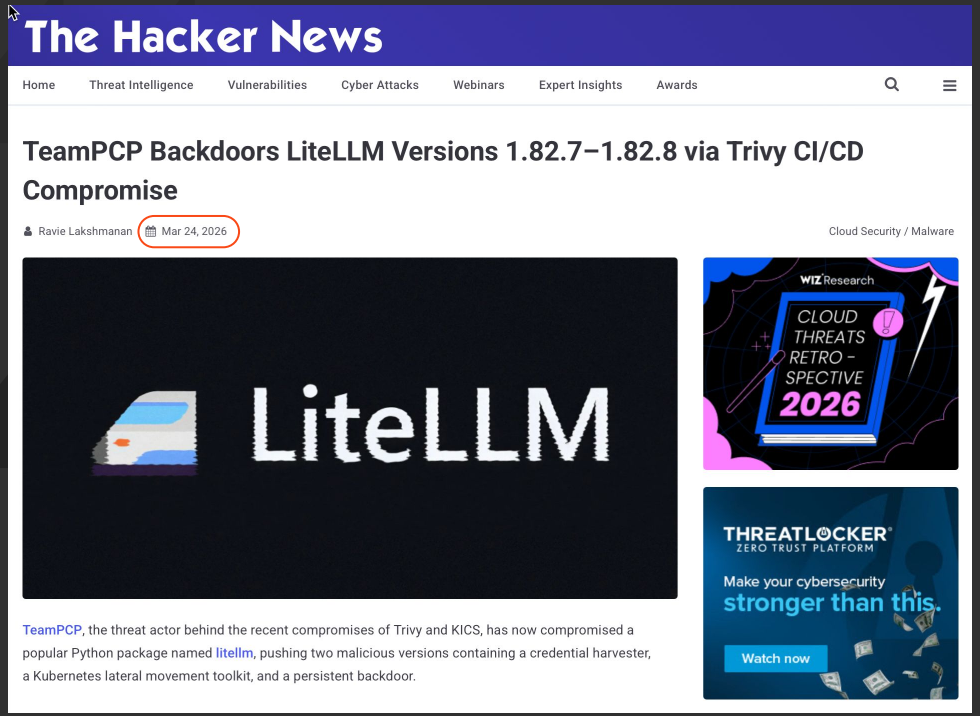
Remediation times lag the average time to exploit

Share of vulnerabilities that remain externally observable, by days since first detection* and vulnerability type



*We analyzed all vulnerabilities first observed in the last two years.

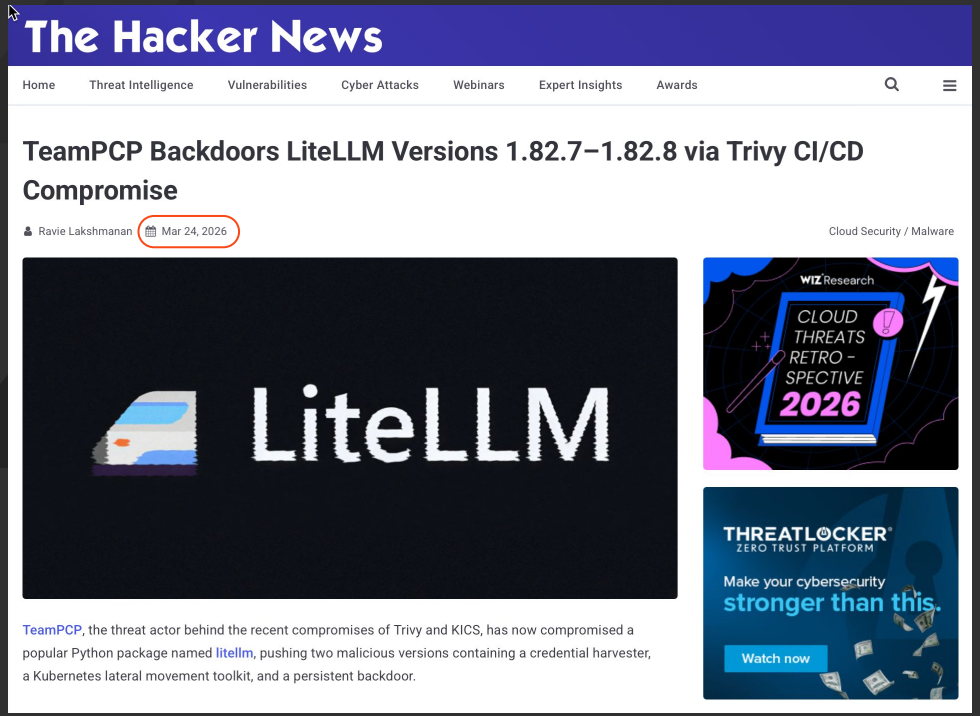
Sources: Moody's Ratings, Bitsight Technologies



https://thehackernews.com/2026/03/teampcp-backdoors-litellm-versions.html

Threat Actor Uses Supply Chain Breach
"TeamPCP, the threat actor behind the recent compromises of Trivy and KICS, has now compromised a popular Python package named litellm, pushing two malicious versions containing a credential harvester, a Kubernetes lateral movement toolkit, and a persistent backdoor."

Continued Stolen Credential Use
"This campaign is almost certainly not over," Endor Labs said. "TeamPCP has demonstrated a consistent pattern: each compromised environment yields credentials that unlock the next target."



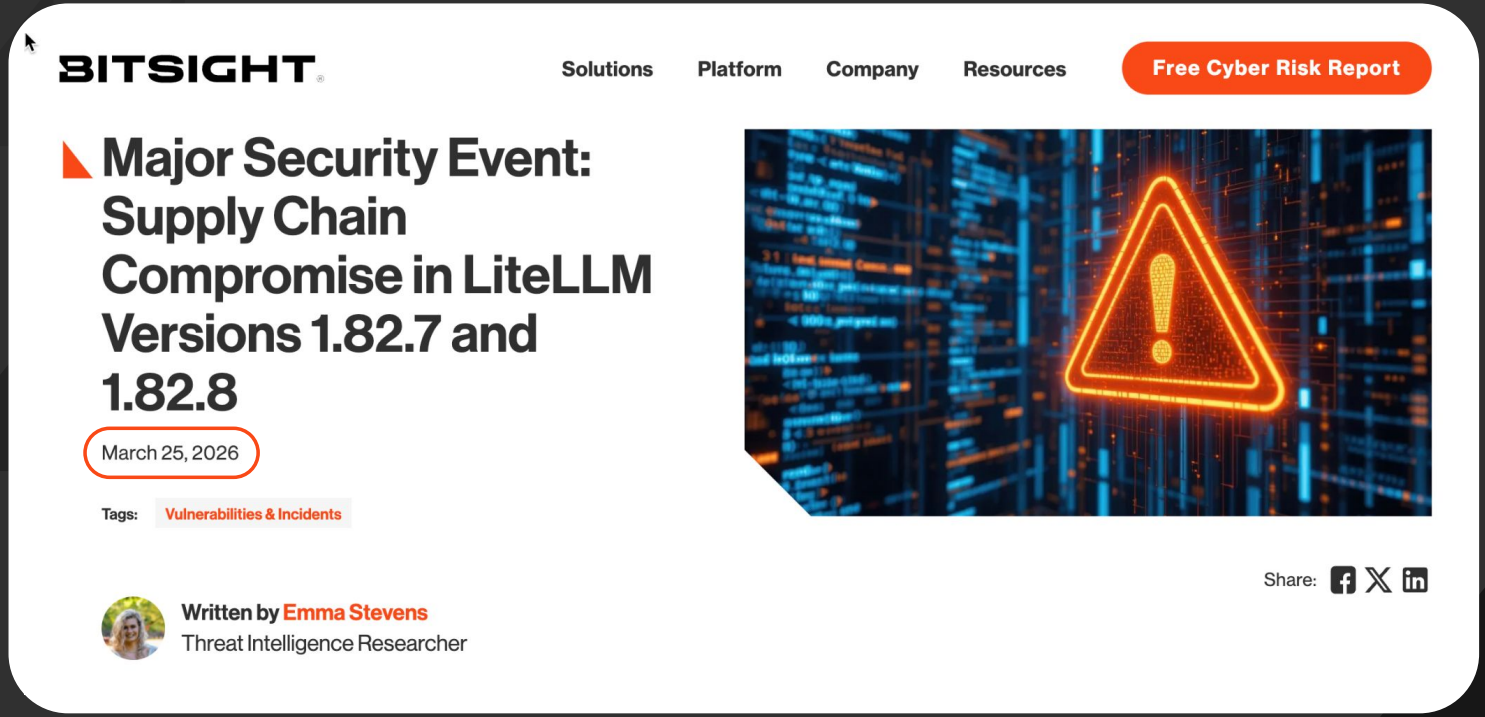
https://thehackernews.com/2026/03/teampcp-backdoors-litellm-versions.html

Threat Actor Uses Supply Chain Breach

"TeamPCP, the threat actor behind the recent compromises of Trivy and KICS, has now compromised a popular Python package named litellm, pushing two malicious versions containing a credential harvester, a Kubernetes lateral movement toolkit, and a persistent backdoor."

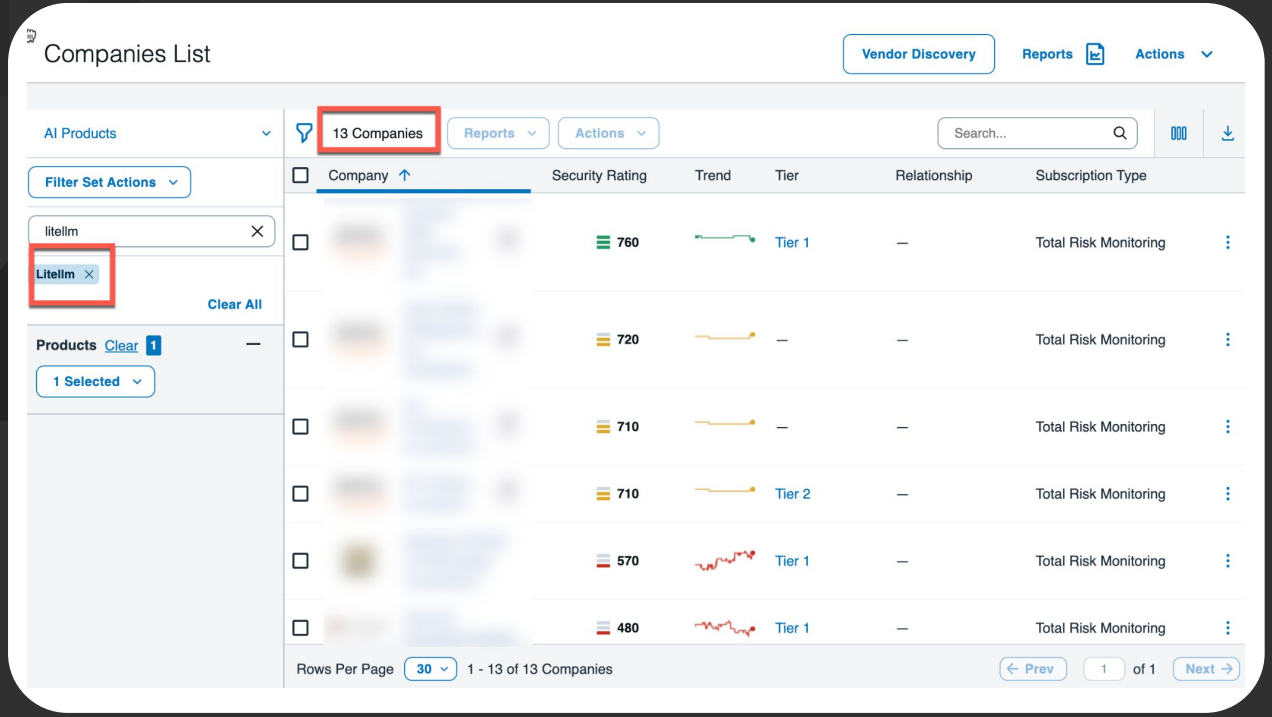
Continued Stolen Credential Use

"This campaign is almost certainly not over," Endor Labs said. "TeamPCP has demonstrated a consistent pattern: each compromised environment yields credentials that unlock the next target."



https://www.bitsight.com/blog/litellm-versions-1-82-7-1-82-8-supply-chain-compromise

Visibility Within Hours



How Bitsight is Responding

BITSIGHT Luminate EXCHANGE

Speed

Increased Frequency of Scanning
Pre-indexed for instant visibility and
Rapid Response

Coverage

Massive Expansion of Fingerprints
and Vulnerabilities

BITSIGHT

Speakers

BITSIGHT Luminate EXCHANGE

Stephen Boyer

Co-Founder & Chief Innovation Officer, Bitsight

Ian Brown

Group CISO, Spectris

Will Davies

Group Deputy CISO, Endava

BITSIGHT

BITSIGHT

BITSIGHT Luminate EXCHANGE

Networking Break

30 Minutes

BITSIGHT