Blog: Stay Ahead of Cyber Threats

By Intel 471

Published: 2026-04-01 · Archived: 2026-04-05 19:48:55 UTC

Emerging Threats//Apr 1, 2026

TeamPCP Supply Chain Attacks

TeamPCP is exploiting trusted npm and PyPI packages to compromise developer environments, steal credentials, and extend attacks across software supply chains.

Mar 31, 2026

Turning Geopolitical Tension into Actionable Intelligence

Intel 471's updated Geopolitical Intelligence solution is designed to translate volatile global dynamics into timely, actionable insights.

Mar 24, 2026

CVE-2025-68613: Zerobot botnet exploits critical vulnerability impacting n8n AI orchestration platform

Zerobot, a Mirai-based botnet known for targeting Internet of Things (IoT) devices, has leveraged a critical vulnerability tracked as CVE-2025-68613 to compromise instances of the n8n workflow automation platform.

Mar 17, 2026

Introducing Cyber Threat Exposure Bundle: A Unified Approach to External Risk

To empower organizations against the growing complexity of their attack surface, Intel 471 is introducing the Cyber Threat Exposure Bundle.

Mar 13, 2026

CVE-2026-20127: Critical Cisco SD-WAN vulnerability exploited in wild

CVE-2026-20127 is an improper authentication vulnerability impacting Cisco Catalyst SD-WAN Controller, formerly vSmart, and SD-WAN Manager, formerly vManage, components.

Emerging Threats//Mar 13, 2026

Handala Threat Group

An Iranian aligned threat group conducting destructive and espionage focused cyber operations against organizations in Israel and Western countries.

Mar 12, 2026

OpenClaw: A viral AI assistant and a magnet for infostealer malware and ClickFix trickery

Since early 2026, interest in OpenClaw — the open source autonomous AI agent developed by Peter Steinberger — has surged.

Mar 9, 2026

Israeli, US strikes against Iran triggers a surge in hacktivist activity

On Feb. 28, 2026, the U.S. and Israel launched coordinated strikes against Iran, marking the start of open conflict after months of escalating tensions.

Mar 5, 2026

CVE-2026-1731: Finding a critical RCE in an age of AI-driven vulnerability research

CVE-2026-1731 is an operating system (OS) command injection vulnerability impacting BeyondTrust Remote Support (RS) and Privileged Remote Access (PRA) software

Mar 4, 2026

Born to bypass MFA: Taking down Tycoon 2FA

Intel 471 has worked with law enforcement and private industry in action coordinated by Europol's European Cybercrime Centre (EC3), culminating in today's takedown of Tycoon 2FA's operations and infrastructure.