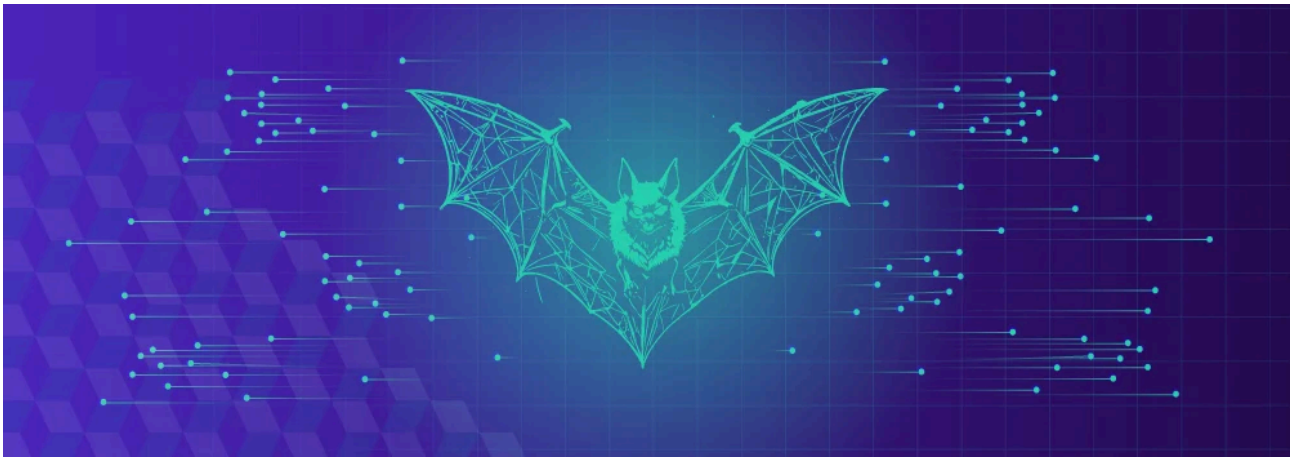
BatShade: Vietnamese Threat Actor Evolves With Vampire Bot And Social Engineering Malware | Aryaka Threat Research Blog

By Aditya K Sood

Published: 2025-10-07 · Archived: 2026-04-05 16:32:11 UTC



Get the new Batshadow Threat Report or Explore Interactive Report

Aryaka Threat Research Labs has identified a new campaign by the Vietnamese threat actor BatShadow, which continues to rely on social engineering to compromise job seekers and digital marketing professionals. The attackers pose as recruiters, distributing malicious files disguised as job descriptions and corporate documents. When opened, these lures trigger the infection chain of a Go-based malware we refer to as Vampire Bot.

This campaign demonstrates how threat actors exploit trust in professional workflows to achieve persistence, conduct system surveillance, and exfiltrate sensitive information, all while blending their activity into normal-looking traffic.

The infection typically begins with ZIP archives containing lure PDFs alongside malicious shortcut or executable files, which are masked with misleading extensions. In this case, the malicious files execute hidden PowerShell commands that display a decoy PDF to the victim while silently downloading and installing the malware in the background. The attackers also employ browser-based tricks, instructing victims to switch to specific browsers to bypass built-in protections and ensure the successful delivery of the payload.

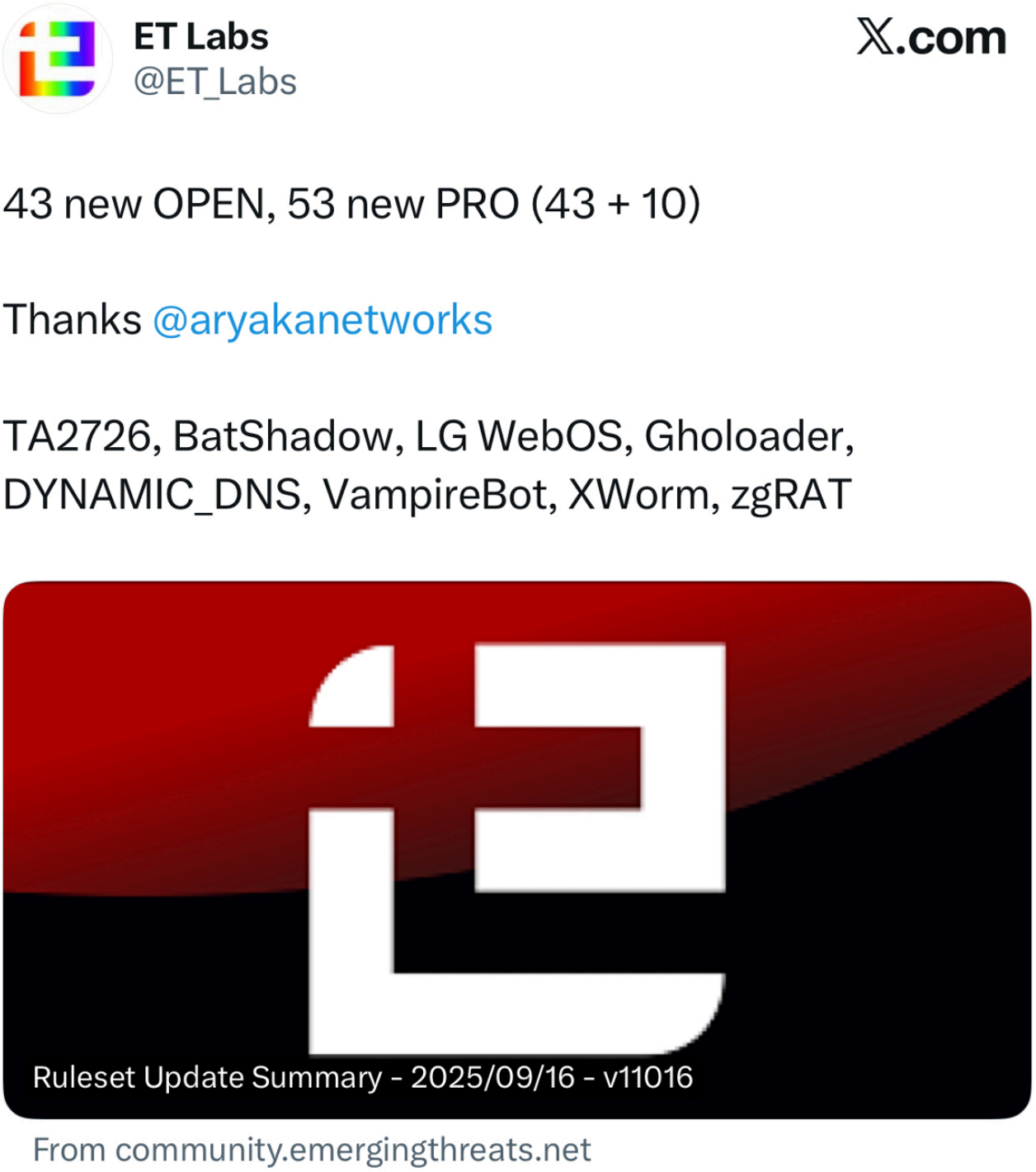
Once executed, Vampire Bot performs detailed host profiling, collecting usernames, hardware identifiers, operating system details, privilege levels, and information on installed security products. This data is encrypted before being transmitted to the attacker’s infrastructure. To maintain persistence, the malware hides itself in system folders, applies attributes to remain concealed, and creates a mutex to prevent multiple instances from running.

A central feature of Vampire Bot is its continuous desktop surveillance. The malware captures screenshots at configurable intervals, compresses them into WEBP format, and exfiltrates them over encrypted channels. It also

maintains a persistent C2 polling loop to receive instructions, which may include executing commands or downloading additional payloads. Task results are transmitted back to the operators, granting them complete remote control of the compromised system.

This evolution of BatShadow's tactics reflects a shift from the group's earlier reliance on commodity malware toward more customized tools designed for stronger persistence and stealth. By embedding malicious code into familiar job-application workflows, the actors increase the likelihood of successful compromise while reducing the chances of detection. This shift underscores the urgent need for continuous vigilance in the cybersecurity field.

Lastly, Aryaka threat research labs work closely with community partners to ensure detection capabilities are enhanced with threat intelligence. We responsibly disclosed the research with Proofpoint Emerging Threats research team to update the rulesets. This collaborative effort, including the mention from Emerging Threats, highlights the strength of the cybersecurity community in addressing evolving cyber challenges.



Read the report here or Explore Interactive Report

Source: https://www.aryaka.com/blog/batshade-vampire-bot-social-engineering-malware/