Blind Eagle Hacks Colombian Institutions Using NTLM Flaw, RATs and GitHub-Based Attacks

thehackernews.com/2025/03/blind-eagle-hacks-colombian.html

March 11, 2025

The threat actor known as **Blind Eagle** has been linked to a series of ongoing campaigns targeting Colombian institutions and government entities since November 2024.

"The monitored campaigns targeted Colombian judicial institutions and other government or private organizations, with high infection rates," Check Point said in a new analysis.

"More than 1,600 victims were affected during one of these campaigns which took place around December 19, 2024. This infection rate is significant considering Blind Eagle's targeted APT approach."

Blind Eagle, active since at least 2018, is also tracked as AguilaCiega, APT-C-36, and APT-Q-98. It's known for its hyper-specific targeting of entities in South America, specifically Colombia and Ecuador.

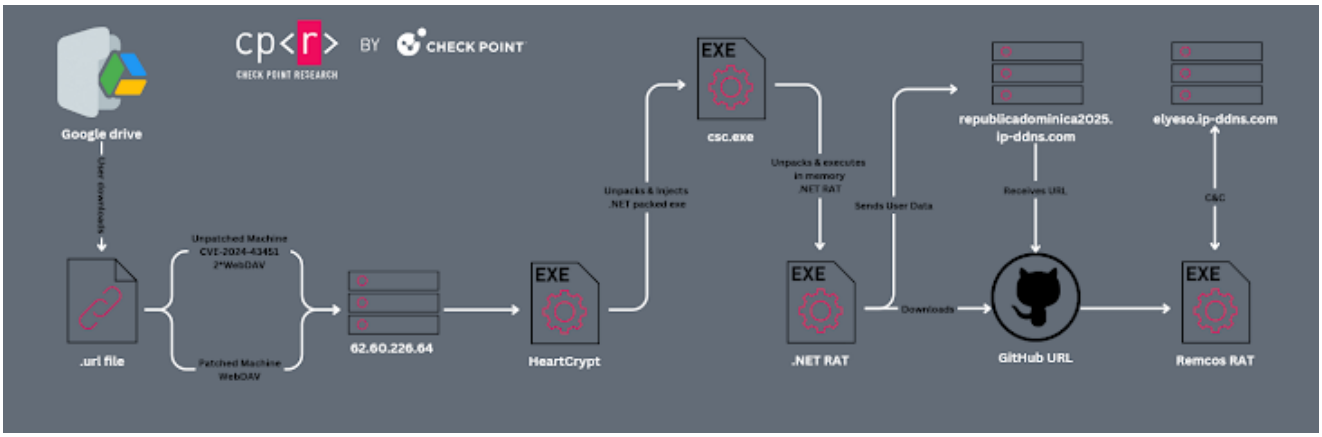
Attack chains orchestrated by the threat actor entail the use of social engineering tactics, often in the form of spear-phishing emails, to gain initial access to target systems and ultimately drop readily available remote access trojans like AsyncRAT, NjRAT, Quasar RAT,

and Remcos RAT.

The latest set of intrusions are notable for three reasons: The use of a variant of an exploit for a now-patched Microsoft Windows flaw (CVE-2024-43451), the adoption of a nascent packer-as-a-service (PaaS) called HeartCrypt, and the distribution of payloads via Bitbucket and GitHub, going beyond Google Drive and Dropbox.

Specifically, HeartCrypt is used to protect the malicious executable, a variant of PureCrypter that's then responsible for launching the Remcos RAT malware hosted on a now-removed Bitbucket or GitHub repository.

CVE-2024-43451 refers to an NTLMv2 hash disclosure vulnerability that was fixed by Microsoft in November 2024. Blind Eagle, per Check Point, incorporated a variant of this exploit into its attack arsenal a mere six days after the release of the patch, causing unsuspecting victims to advance the infection when a malicious .URL distributed via a phishing email is manually clicked.

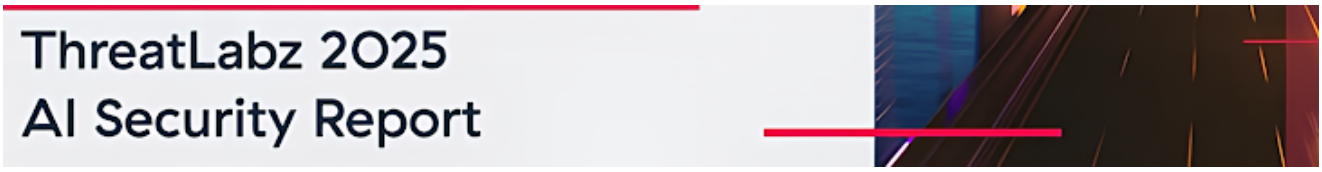


"While this variant does not actually expose the NTLMv2 hash, it notifies the threat actors that the file was downloaded by the same unusual user-file interactions," the cybersecurity company said.

"On devices vulnerable to CVE-2024-43451, a WebDAV request is triggered even before the user manually interacts with the file with the same unusual behavior. Meanwhile, on both patched and unpatched systems, manually clicking the malicious .URL file initiates the download and execution of the next-stage payload."

Check Point pointed out that the "rapid response" serves to highlight the group's technical expertise and its ability to adapt and pursue new attack methods in the face of evolving security defenses.

Serving as a smoking gun for the threat actor's origins is the GitHub repository, which has revealed that the threat actor operates in the UTC-5 timezone, aligning with several South American countries.



That's not all. In what appears to be an operational error, an analysis of the repository commit history has uncovered a file containing account-password pairs with 1,634 unique email addresses.

While the HTML file, named "Ver Datos del Formulario.html," was deleted from the repository on February 25, 2025, it has been found to contain details such as usernames, passwords, email, email passwords, and ATM PINs associated with individuals, government agencies, educational institutions, and businesses operating in Colombia.

"A key factor in its success is its ability to exploit legitimate file-sharing platforms, including Google Drive, Dropbox, Bitbucket, and GitHub, allowing it to bypass traditional security measures and distribute malware stealthily," Check Point said.

"Additionally, its use of underground crimeware tools such as Remcos RAT, HeartCrypt, and PureCrypter reinforces its deep ties to the cybercriminal ecosystem, granting access to sophisticated evasion techniques and persistent access methods."

Found this article interesting? Follow us on Twitter and LinkedIn to read more exclusive content we post.