The Growing Danger of Blind Eagle: One of Latin America's Most Dangerous Cyber Criminal Groups Targe ...

By rohann@checkpoint.com

Published: 2025-03-10 · Archived: 2026-04-21 02:13:13 UTC

Executive Summary

- Check Point Research (CPR) has uncovered a series of ongoing, targeted cyber campaigns by Blind Eagle (APT-C-36)—one of Latin America's most dangerous threat actors
- Days after Microsoft released a fix for CVE-2024-43451, the group began employing a comparable technique involving harmful .url files, showing how attackers can turn security updates into weapons against their victims
- CPR found over **9,000 infections** in just one week
- Attacks leverage trusted platforms like Google Drive, Dropbox, GitHub, and Bitbucket to distribute payloads, bypassing traditional security defenses
- The final malware, Remcos RAT, enables data theft, remote execution, and persistent access

Blind Eagle's Cyber Espionage Tactics Are Evolving—Fast

Cyber criminals move quickly, but Blind Eagle (APT-C-36) is proving just how fast. The notorious advanced persistent threat (APT) group, known for targeting Colombia's justice system, government institutions, and private organizations, has launched a new campaign that demonstrates how attackers can weaponize security patches against their targets.

Just six days after Microsoft patched CVE-2024-43451, Blind Eagle incorporated a similar method into their attack arsenal, using malicious .url files to track victims and execute malware. This technique allows them to identify potential targets without any interaction from the victim, making their approach stealthier than traditional phishing campaigns.

CPR uncovered more than **1,600 infections** from a single campaign—a staggering number given the targeted nature of APT attacks. What's particularly alarming is the group's ability to bypass security measures by using legitimate cloud platforms like Google Drive, Dropbox, GitHub, and Bitbucket to deliver their malware.

This campaign underscores the growing sophistication of cyber threats and the need for proactive defenses to counter them.

Weaponizing a Microsoft Patch: How Blind Eagle is Using .URL Files to Target Victims

On November 12, 2024, Microsoft patched CVE-2024-43451, a vulnerability that exposed NTLMv2 hashes, allowing attackers to hijack user credentials. In response, Blind Eagle developed a technique using .url files, not to exploit the vulnerability directly, but to track victims and trigger malware downloads.

This attack method is particularly dangerous because it requires minimal user interaction. Simply right-clicking, deleting, or dragging the file can trigger a WebDAV request, which notifies the attackers that the file has been accessed. If the victim then clicks on the file, the next-stage payload is downloaded and executed, leading to a full-blown compromise.

The stealth of this method makes detection difficult. Unlike traditional malware that requires a user to open an attachment or enable macros, these .url files act passively, reporting back to attackers even before they are executed. This can allow Blind Eagle to identify and prioritize potential victims before deploying the full malware payload, as their malicious .url files notify attackers when accessed.

Trusted Cloud Platforms: The New Malware Delivery Mechanism

Blind Eagle has previously leveraged legitimate cloud-based services and continues to do so, making it more difficult for security tools to detect and flag their malicious activity compared to suspicious domains.

CPR identified Blind Eagle leveraging:

- **Google Drive**
- **Dropbox**
- **GitHub**
- **Bitbucket**

By disguising malware as harmless-looking files hosted on trusted services, Blind Eagle can evade traditional security filters. When a victim interacts with the malicious file, the malware downloads and executes a remote access trojan (RAT), giving attackers complete control over the compromised system.

This method also enables Blind Eagle to quickly update their malware payloads without needing to reconfigure their attack infrastructure. If one hosting account is taken down, they can simply upload their malware to a new cloud storage account and continue operations.

What Happens After Infection? The Full Attack Chain

Once executed, the malware deployed by Blind Eagle is designed for stealth, persistence, and data exfiltration. The final payload used in this campaign is Remcos RAT, a widely used remote access trojan that grants attackers complete control over an infected machine.

After infection, the malware can:

- Capture user credentials by logging keystrokes and stealing stored passwords.
- Modify and delete files, allowing attackers to sabotage systems or encrypt data for ransom.
- Establish persistence by creating scheduled tasks and registry modifications, ensuring it survives reboots.
- Exfiltrate sensitive information, sending it back to command-and-control (C2) servers operated by Blind Eagle.

CPR found that one campaign alone led to over **9,000 victims** in just one week, indicating that these tactics are proving highly effective.

Blind Eagle's Rapid Adaptation: A New Trend in Cyber Attacks?

The speed at which Blind Eagle weaponized a newly patched vulnerability raises a critical concern: Are cyber criminals adapting faster than defenders?

This case highlights a worrying trend in modern cyber warfare—threat actors are no longer waiting for zero-day vulnerabilities to be disclosed. Instead, they are closely monitoring security patches, analyzing them, and finding ways to mimic or repurpose the behavior of the exploit before organizations have fully implemented defenses.

Blind Eagle's ability to quickly integrate a patched exploit into their campaigns suggests that cyber criminals are becoming more agile, innovative, and prepared. Security teams must respond by accelerating their patch management strategies and implementing AI-driven threat prevention solutions to detect emerging threats before they can take hold.

How Organizations Can Defend Against Blind Eagle's Attacks

With APT groups evolving their tactics rapidly, organizations must move beyond traditional security models and adopt a proactive defense strategy.

Key steps to mitigate these threats include:

- **Strengthening email security** – Blind Eagle primarily relies on phishing emails to deliver its payloads. A robust email security solution can detect and block malicious attachments before they reach users.
- **Implementing real-time endpoint protection** – Behavioral-based detection with Harmony Endpoint can recognize suspicious file interactions and block malware execution before damage occurs.

- **Monitoring web traffic and DNS activity** – Since Blind Eagle leverages cloud storage services, security teams must analyze outbound network connections and flag unusual requests to trusted platforms.
- **Enhancing security awareness training** – Employees remain the weakest link in cyber security. Regular training on identifying phishing attempts and suspicious file behavior can prevent successful attacks.
- **Leveraging advanced threat prevention solutions**—Traditional signature-based security tools struggle against rapidly evolving threats. Check Point Threat Emulation, together with Harmony Endpoint, provides comprehensive protection across attack tactics, file types, and operating systems, defending against the exact threats described in this report.

To learn more about Blind Eagle, read Check Point Research's comprehensive report here.

Protection Names:

- Exploit.Wins.CVE-2024-43451.ta.A
- Infostealer.Win.Generic.F
- Injector.Win.RunPE.A
- Infostealer.Win.PasswordStealer.A
- Trojan.Win.Unpacme.gl.I
- Exploit.Win.UnDefender.A
- Packer.Win.VBNetCrypter.H
- Packer.Win.VBNetCrypter.E
- Packer.Win.DotNetCrypter.G
- Trojan.Win.Benjaminbo_test.gl.A
- behavioral.win.suspautorun.a
- behavioral.win.imagemodification.g
