Inside Stealth Falcon’s Espionage Campaign Using a Microsoft Zero-Day

By bferrite

Published: 2025-06-10 · Archived: 2026-04-06 02:58:43 UTC

Inside Stealth Falcon’s Espionage Campaign Using a Microsoft Zero-Day

- Check Point Research (CPR) identified a previously unknown Windows vulnerability (CVE-2025-33053) being actively exploited in the wild.
- Following CPR’s responsible disclosure, Microsoft released a patch on its June 10th Patch Tuesday
- The zero-day was used in a targeted espionage operation likely conducted by Stealth Falcon, a threat group known to target entities in the Middle East and Africa.
- The attack chain begins with a deceptive internet shortcut (.url file) that silently triggers malware hosted on an attacker-controlled WebDAV server, abusing legitimate Windows tools in the process.
- The operation deployed a sophisticated custom loader and implant designed to evade detection, hinder analysis, and selectively activate only on valuable targets.

The operation deployed a sophisticated custom loader and implant designed to evade detection, hinder analysis, and selectively activate only on valuable targets. In March 2025, Check Point Research uncovered an attempted cyber attack against a major defense organization in Turkey. The attackers used a previously unknown remote code execution vulnerability in Windows to execute files from a remote WebDAV server they controlled, exploiting a legitimate built-in Windows tool to run malicious code silently. Following responsible disclosure, Microsoft assigned the vulnerability CVE-2025-33053 and released a patch on June 10, 2025, as part of their monthly Patch Tuesday updates.

Based on the techniques used, the infrastructure behind the campaign, and the profile of the intended target, Check Point Research attributes this activity to the well-established APT group known as **Stealth Falcon**.

In this blog, we break down how the group leveraged CVE-2025-33053 to deliver a custom-built implant known as **Horus Agent**, part of a broader toolset designed for espionage. We’ll also explore the implications of this campaign for defenders, especially those protecting government, defense, and critical infrastructure organizations.

For an in-depth understanding of Sealth Falcon’s campaign, read Check Point Research’s comprehensive report here.

Who Is Stealth Falcon?

Stealth Falcon, also known by the alias *FruityArmor*, is a long-running cyber espionage group active since at least 2012, with a track record of targeting political and strategic entities across the Middle East and Africa. Over time, Stealth Falcon’s tactics have evolved, but their focus remains on high-value targets in government and defense

sectors. Today, Stealth Falcon is known for its use of zero-day exploits, custom malware, and delivery mechanisms, all hallmarks of a well-resourced APT.

How the Attack Worked

The attack began with what looked like a standard shortcut file — a .url file disguised as a PDF document related to military equipment damage. Submitted to VirusTotal by a source associated with a major Turkish defense company, the file was likely delivered via a phishing email, a tactic Stealth Falcon has used many times before.

What made this shortcut file dangerous was its ability to silently run code from a remote server controlled by the attackers. The attackers manipulated the Windows file execution search order. They tricked a built-in Windows utility into executing a malicious program hosted on their remote server.

This technique allowed Stealth Falcon to run their code without needing to drop files on the first stage of the infection chain directly onto the victim's computer. It also helped them evade detection by relying on legitimate, trusted Windows components to carry out the attack.

The infection chain.

Horus Loader: A Customized Entry Point for Espionage

Once the shortcut file was activated, it kicked off the next phase of the attack: a multi-stage loader we called **Horus Loader**, named after the Egyptian falcon god, echoing the group's codename.

Horus Loader is built to be flexible and evasive. It can:

- Clean up traces left by earlier parts of the infection chain
- Bypass basic detection mechanisms
- Drop and open a decoy document to avoid suspicion
- Deploy the final spyware payload discreetly

The Final Act: Delivering Horus Agent

While the victim is occupied with viewing the decoy document, the malware continues its work quietly in the background. What follows is one of the most **technically advanced stages** of the operation: the deployment of a **custom-built espionage tool** known as *Horus Agent*.

Custom-Built Backdoor: Horus Agent

The final payload is Horus Agent, a private implant built for Mythic, a legitimate open-source command-and-control (C2) framework commonly used in red team operations.

Unlike off-the-shelf malware, Horus is written in C++ and built from the ground up with stealth and flexibility in mind. It shares only basic traits with other known Mythic agents — enough to function on the platform, but not enough to be easily detected or attributed based on code similarities.

Once installed, the Horus Agent connects to its C2 server and begins polling for instructions using the Mythic framework. While some commands are built-in, Stealth Falcon also developed several custom ones tailored for stealth and flexibility, showing intent for gathering intelligence quietly and executing payloads with minimal detection.

Unlike earlier modified Mythic agents, Horus appears custom-built. It emphasizes stealth, anti-analysis protections, and a minimal command set, focused on fingerprinting targets and selectively deploying further payloads. This streamlined design suggests deep awareness of both target environments and defensive tools, helping the group stay under the radar while protecting their broader toolset.

Conclusion: A Zero-Day Attack with Strategic Implications

Stealth Falcon continues to evolve, combining zero-day exploitation CVE-2025-33053 and legitimate tools, multi-stage loaders, and custom-built implants in a resilient campaign. Their creative abuse of WebDAV and Windows working directory behavior highlights how even small misconfigurations or overlooked features can be weaponized.

Mitigation and Defense

This attack highlights the importance of proactive threat detection, visibility into system behavior, and real-time protection. For organizations in sectors like defense, government, or critical infrastructure, it’s a reminder that targeted threats are an ongoing concern. Given the nature of this vulnerability and its connection to core Windows API behavior, it may impact a broad range of Windows versions.

To determine if your environment has been breached, we suggest examining your logs and monitoring systems for the following:

- Emails with archive attachments including a seemingly harmless URL or LNK file.
- Unusual or unidentified connections to WebDAV servers launched by default Windows processes.

Upon discovering the vulnerability, Check Point quickly developed and deployed protections to keep customers secure well before the issue became public. Our Intrusion Prevention System, Threat Emulation, and Harmony Endpoint solutions now detect and block exploitation attempts targeting this flaw. Check Point Research continues to monitor global telemetry to track any new activity and provide timely updates as the threat landscape evolves.

For an in-depth understanding of Sealth Falcon’s campaign, read Check Point Research’s comprehensive report here.
