Iranian Threat Actor Nimbus Manticore Expands Campaigns into Europe with Advanced Malware and Fake Job Lures

By rohann@checkpoint.com

Published: 2025-09-22 · Archived: 2026-04-13 02:00:47 UTC

Key Highlights

- Check Point Research is actively tracking Iranian threat actor Nimbus Manticore. Our latest findings show it is expanding operations into Europe and now targeting the defense, telecom, and aerospace sectors.
- The group uses fake job portals and spear-phishing to lure victims, delivering malicious files disguised as part of hiring processes, all while impersonating major local and global aerospace companies.
- Evolving malware such as MiniJunk and MiniBrowse help attackers stay hidden, steal data, and maintain long-term access.
- Campaigns align with IRGC strategic priorities, focusing on intelligence collection on sensitive defense vendors during periods of heightened geopolitical tension.

Introduction

Since early 2025, Check Point Research has tracked successive waves of activity from Nimbus Manticore, a mature Iran-nexus advanced persistent threat (APT) group. Sometimes referred to as UNC1549 or Smoke Sandstorm, and previously associated with the Iranian Dream Job campaign, Nimbus Manticore primarily targets aerospace and defense organizations in the Middle East and Europe.

The group is best known for its targeted spear-phishing campaigns that deliver custom implants, including Minibike, also known as SlugResin. First reported in 2022, Minibike has evolved steadily, adopting obfuscation techniques, modular architecture, and redundant C2 infrastructure.

Recent activity shows a significant leap in sophistication: the use of a previously undocumented technique to load DLLs from alternate paths by modifying process execution parameters. This variant, dubbed MiniJunk, demonstrates how Nimbus Manticore continuously advances its malware to evade detection.

In this blog, we highlight the evolution of Minibike into a new variant dubbed MiniJunk, the use of fake recruiting portals for malware delivery, victimology across the Middle East and Western Europe, and the broader implications for defense, telecom, and aviation sectors.

For more details, read the comprehensive technical analysis published by Check Point Research:

https://research.checkpoint.com/2025/nimbus-manticore-deploys-new-malware-targeting-europe

Malware Delivery Websites

The infection chain begins with phishing links that lure victims to fake job-related login pages. These sites share several notable traits:

- **Brand Impersonation**: Sites mimic companies such as Boeing, Airbus, Rheinmetall, and flydubai, built using a React template that adapts to the brand being impersonated.
- **Domain Strategy**: Domains typically follow a “career” theme, are registered behind Cloudflare, and conceal the true hosting infrastructure.
- **Controlled Access**: Each victim is given a unique set of login details in advance. Only when the correct credentials are entered does the site deliver a malicious archive containing the malware, allowing attackers to track individuals and block unwanted visitors.

This controlled, per-victim access demonstrates strong operational security and credible pretexting consistent with state-sponsored tradecraft.

Figure 1 – Websites used to deliver malicious archives after successful login.

Evolving Toolset: MiniJunk and MiniBrowse

Nimbus Manticore’s newer tools focus on two main outcomes. MiniJunk allows the attackers to quietly maintain access to a victim’s systems over long periods of time, while MiniBrowse is used to steal sensitive information without drawing attention. These tools are constantly updated so they can avoid security scans, remain functional for longer, and give attackers reliable ways to spy on targeted organizations.

Figure 2 – The infection chain.

Separate Cluster of Activity

Alongside MiniJunk operations, Check Point Research observed a parallel activity cluster, previously reported by PRODAFT. While this cluster uses smaller payloads and simpler techniques without the heavy obfuscation seen in MiniJunk, it still relies on the same spear-phishing and fake recruiting strategies. In other words, the attackers are applying similar methods with less technical complexity but the same goal: tricking victims into handing over access.

Here, too, attackers pose as HR recruiters, but in this case, they likely reach out on LinkedIn or other professional platforms. After making contact, they move the conversation to email and send Outlook messages that direct victims to tailored recruiting portals. As in the MiniJunk campaigns, each portal is customized with unique login details for the target, giving attackers close control and visibility.

Check Point Harmony Email & Collaboration blocked one such attempt against an Israeli telecommunications provider, underscoring how both activity clusters share the same deceptive tactics and wide-ranging targets.

Victimology and Target Sectors

Expansion to Europe:

- While Nimbus Manticore consistently targets the Middle East, especially Israel and the UAE, recent operations show increased interest in western Europe, specifically Denmark, Sweden, and Portugal.

Focused targeting of specific sectors:

- We found a correlation between the malware delivery websites and the targeted sectors. For example, a fake hiring portal of a telecommunication company will target employees and organizations in this sector.
- Our findings point to similar targets in several key sectors: telecommunications, especially satellite providers**,** defense contractors, aerospace and airlines. These sectors align with the IRGC's strategic intelligence collection efforts.

Protecting Against Nimbus Manticore

Over the past year, Nimbus Manticore has advanced its malware arsenal, delivery methods, and targeting strategy. By evolving Minibike into MiniJunk, deploying MiniBrowse, and refining its spear-phishing techniques, the actor has demonstrated resilience and stealth even during high-intensity geopolitical conflict.

The group's expanded focus on Western Europe, particularly in defense, telecom, and aviation, signals a growing Iranian cyber espionage campaign aligned with IRGC strategic priorities.

To counter these threats, organizations need protection that blocks attacks before they reach employees. Check Point Harmony Email & Collaboration provides exactly that by detecting and preventing spear-phishing attempts, fake job portals, and malicious attachments like those used in Nimbus Manticore campaigns. By stopping these lures at the email and collaboration level, Harmony helps organizations avoid compromise and ensures their people remain the strongest line of defense.

To counter these threats, organizations need protection that blocks attacks before they reach employees and endpoints.

▪ **Check Point Harmony Email & Collaboration:** To detect and prevent spear-phishing, fake job portals, and malicious attachments at the email and collaboration level, stopping initial lures.

▪ **Harmony Endpoint:** To secure devices against advanced malware *once it lands*, providing protection even if the initial email defense is bypassed.

▪ **Quantum Network Security:** To stop malicious traffic at the network perimeter, creating a barrier against download of malicious files, C2 communications and data exfiltration.

Check Point Research will continue to track Nimbus Manticore's operations and share insights that strengthen customer resilience against nation-state campaigns.

For more details, read the comprehensive technical analysis published by Check Point Research:

https://research.checkpoint.com/2025/nimbus-manticore-deploys-new-malware-targeting-europe

---