FortiGuard Incident Response Team Detects Intrusion into Middle East Critical National Infrastructure | FortiGuard Labs

Published: 2025-05-01 · Archived: 2026-04-05 16:42:17 UTC

Introduction

The FortiGuard Incident Response (FGIR) team recently investigated a long-term cyber intrusion targeting critical national infrastructure (CNI) in the Middle East, attributed to an Iranian state-sponsored threat group. The attack involved extensive espionage operations and suspected network prepositioning—a tactic often used to maintain persistent access for future strategic advantage.

Full Report Available: The following article provides key findings, but a full report of this activity is available here. The report includes an analysis of novel malware deployed throughout the intrusion, a detailed breakdown of adversary TTPs across different attack stages, Indicators of Compromise (IOCs) to assist defenders, and attribution considerations for deeper insight.

Key Findings

The intrusion persisted from at least May 2023 to February 2025, with signs of compromise dating back as far as May 2021. Attackers initially gained access via stolen VPN credentials and established persistence through multiple web shells and backdoors, including Havoc, HanifNet, HXLibrary, and NeoExpressRAT. They bypassed network segmentation using open-source proxying tools like plink, Ngrok, glider proxy, and ReverseSocks5.

Key insights from the investigation include:

- The attack unfolded in waves, with the adversary deploying new malware and infrastructure over time. They used custom loaders to execute Havoc and SystemBC in memory.
- In addition to publicly available tools, the adversary deployed novel backdoors such as HanifNet, HXLibrary, and NeoExpressRAT, enabling command execution, file operations, and system discovery.
- The adversary avoided U.S.-based infrastructure, instead relying on non-U.S. VPS providers.
- Persistence was maintained through scheduled tasks designed to blend in with legitimate Windows processes.
- Virtualization infrastructure was actively targeted, with the adversary conducting reconnaissance to understand network configurations.
- After containment efforts, the adversary attempted to regain access by exploiting ZKTeco ZKBioTime software vulnerabilities, which had not been previously reported in the wild. They also launched targeted phishing attacks, using compromised third-party emails to steal administrator credentials.

Intrusion Stages

The attack unfolded in four distinct phases:

1. Establishing a Foothold and Initial Operations (May 2023 – April 2024)
The adversary used stolen credentials to access the victim's SSL VPN, deploying web shells on public-facing servers and installing Havoc, HanifNet, and HXLibrary backdoors. They then stole credentials and moved laterally using RDP and PsExec.

2. Consolidating the Foothold (April 2024 – November 2024)
Additional persistence mechanisms were introduced, including NeoExpressRAT. The adversary chained proxies (plink, Ngrok) to bypass segmentation, exfiltrated targeted email data, and began interacting with virtualization infrastructure.

3. Initial Remediation and Adversary Response (November 2024 – December 2024)
The victim implemented initial containment steps, prompting a surge in adversary activity. To maintain access, additional web shells, SystemBC, and MeshCentral were deployed, with a focus on targeting deeper CNI network segments.

4. Intrusion Containment and Final Adversary Response (December 2024 – Present)
The victim successfully removed adversary access. In response, attackers attempted to re-enter via vulnerabilities in web applications and launched targeted phishing campaigns to steal credentials. Multiple failed access attempts were detected.

Victim's Network and Attack Path

The victim organization had a highly segmented network, including a restricted Operational Technology (OT) environment. While no confirmed disruption to OT systems was found, FGIR observed targeted reconnaissance and credential harvesting, indicating strong adversary interest in these systems. The attackers moved from IT to restricted segments by chaining proxy tools and implants to bypass segmentation.

Adversary Tooling and Infrastructure

The attacker relied on VPS-hosted infrastructure, avoiding U.S.-based providers. Notable malware variants used include:

- **HanifNet** – .NET-based backdoor for persistent access
- **HXLibrary** – Malicious IIS module enabling deep system control
- **NeoExpressRAT** – Golang-based backdoor with hardcoded C2 communication
- **RemoteInjector** – Loader for executing Havoc backdoors via scheduled tasks

Lessons Learned and Defensive Recommendations

State-sponsored cyber adversaries continue to target and compromise critical infrastructure networks, seeking to maintain persistent access. Organizations should prioritize the following defensive measures:

- **Enhance credential security** by enforcing multi-factor authentication (MFA) for VPN and privileged accounts and implementing strict password policies with regular credential rotation.

- **Strengthen network segmentation and monitoring** to restrict lateral movement and implement zero-trust architecture with layered access controls.
- **Improve endpoint and web security** by conducting routine integrity checks on web-facing services and implementing application allowlisting to prevent unauthorized execution.
- **Deploy behavioral analytics and EDR solutions** to detect anomalies in real-time and conduct regular penetration testing and third-party security reviews.
- **Ensure incident response preparedness** by developing and testing cybersecurity playbooks for state-sponsored threats and deploying rapid detection and containment capabilities.

Final Insights and Strategic Implications

This investigation highlights the persistent and evolving nature of state-backed cyber threats targeting Middle Eastern CNIs. The adversary demonstrated advanced tactics to deeply embed themselves, evade detection, and sustain long-term access.

Despite containment efforts, the adversary has continued efforts to regain access, indicating a long-term strategic interest in this environment. Organizations must remain vigilant, continuously refining their detection and response strategies to defend against sophisticated, state-sponsored cyber campaigns.

*For a **detailed breakdown of adversary TTPs, novel malware, and IOCs**, access the full report here.*
