The Unraveling of an Iranian Cyber Attack Against the Iraqi Government

By gmcdouga

Published: 2024-09-11 · Archived: 2026-04-06 00:57:37 UTC

- Check Point Research discovered an elaborate cyber-attack against Iraqi governmental networks
- The installer used to deploy the malware bore the logo of the Iraqi General Secretariat of the Council of Ministers, while the domains of compromised servers were related to the Iraqi Prime Minister's Office and the Ministry of Foreign Affairs
- The new malware used in the attack has striking similarities to other malware families used in attacks against the governments of Jordan, Pakistan, and Lebanon, which were identified as connected to the Iranian Ministry of Intelligence and Security (MOIS)

Recently, Check Point Research uncovered a cyber attack targeting the Iraqi government, revealing a troubling pattern that underscores the sophistication and persistence of state-linked cyber threats. After investigating files uploaded to Virus Total, Check Point Research found that the malware in the attack bears significant similarities to malware in other regional attacks by Iranian-linked groups. In the ever-evolving landscape of cyber security threats, understanding the patterns and actors behind attacks is essential for building better tailored defense and proactively detect the threats.

The following blog unravels the attack, the malware involved, and connections to other malware families and malicious cyber groups.

The Attack Overview

Check Point Research has closely monitored a cyber-attack against the Iraqi government over the past several months. Upon investigation by Check Point Research, we uncovered that the affected files contained sophisticated malware and targeted Iraqi organizations such as the Prime Minister's Office and the Ministry of Foreign Affairs. We discovered that the attack is linked to APT34, an Iranian cyber group associated with the Iranian Ministry of Intelligence and Security (MOIS). This group has previously used similar tactics against the governments of Jordan and Lebanon. Findings from a Pakistani source also indicate the presence of related malware families, suggesting the same group is behind these attacks in the region.

The Malware

Two new malware families, Veaty and Spearal, were used in the attack, demonstrating advanced and evasive capabilities. These malware strains were disseminated through deceptive files masquerading as benign documents, such as the Setup Wizard below. With social engineering, these files were opened deceptively, and the malware was installed on the systems upon activation, embedding itself to ensure persistence across reboots.

The installer used to deploy the Spearal malware using the logo of the Iraqi General Secretariat of the Council of Ministers.

Veaty: An Evasive Communicator

Veaty malware employed a sophisticated communication strategy designed to evade detection. It establishes a connection with command-and-control (C2) email servers using several methods, including:

- Connecting without credentials
- Utilizing hardcoded credentials
- Employing external credentials
- Leveraging trusted network credentials

Veaty methodically attempts each of these approaches until a connection is successfully established. It used specific mailboxes for command and control, organizing and concealing its communications through carefully structured email rules. Here, the rules search for emails containing the subject “Prime Minister’s Office.” The malware transmits “Alive” messages to indicate its ongoing activity and “Command” messages to execute instructions. These messages are meticulously formatted and encrypted to minimize the risk of detection.

In a similar attack, a malware called Karkoff, communicated through compromised email addresses belonging to Lebanese government entities, identical to Veaty, which used compromised mail accounts of Iraqi government entities.

Spearal: A Tactical Complement

Spearal, the malware used in the attack, shares numerous tactics linked to malware families affiliated with the Iranian Ministry of Intelligence and Security such as the malware, Saitama. Notable similarities include using DNS tunneling for command communication

The malware families utilize DNS tunneling to transmit commands, which helps them evade conventional detection mechanisms. This method was also observed in attacks against Jordanian government entities, showing a consistent pattern in the group's regional focus and operational techniques.

The infection chain of Spearal Backdoor

Emerging Threat: CacheHttp.dll

The investigation has also revealed a new malware variant, CacheHttp.dll, which appears to target the same entities within Iraq. This malware represents an evolution of previous threats, designed to monitor and respond to specific web server activities. CacheHttp.dll examines incoming web requests for particular headers and executes commands based on predefined parameters.

Threat Prevention and Detection

Old, updated, and new malware continues to pose threats to governments, organizations, and businesses alike. The Iranian attack against Iraq demonstrates that malware is only becoming more sophisticated and challenging to detect. Check Point's security solutions offer a robust defense against advanced malware. Check Point Harmony Endpoint secures devices by detecting and mitigating advanced threats, while Check Point Threat Emulation adds

an extra layer by sandboxing suspicious files to identify malicious behavior before impacting the system. The Check Point Intrusion Prevention System (IPS) monitors network traffic in real-time, blocking potential threats. Anti-Bot technology prevents malware from communicating with command-and-control servers. Together, these solutions create a multi-layered defense that effectively prevents malware attacks.

Please view Check Point Research's full report for a comprehensive review of the attack.

Check Point Protections:

- Harmony Endpoint
  - Win.OilRig.F
  - Win.OilRig.WA.G
  - Win.OilRig.H
- Threat Emulation
  - Wins.Oilrig.ta.B/C/D/E
- Anti Bot
  - WIN32.CacheHttp.A/B/C
  - WIN32.Spearal.A/B/C/D/E/F
