INCD
Israel National
Cyber Directorate

Overview of Recent Phishing Campaigns in Israel

MuddyWater

TLP: CLEAR

December 2025

Table of Contents

Executive Summary

Recently, several phishing campaigns were identified across the Israeli cyber domain, attributed to the Iranian threat group MuddyWater.

As part of one of the major activity waves, the attacker compromised multiple organizational email accounts and used them to distribute phishing emails to extensive distribution lists.
The objective of the campaign is to establish initial access on endpoint devices through the deployment of a customized backdoor tool developed by the attacker (such as *BlackBeard*), perform lateral movement within the corporate network, and continue propagating the campaign using the compromised email accounts.

The observed activity aligns with MuddyWater's known operational patterns in the region and demonstrates localized tactical adaptation, including the use of Hebrew-language messages, customization of phishing content to match the profile of the compromised organization, and inclusion of legitimate-looking documents and attachments.

A technical analysis of the phishing activity, as well as the *BlackBeard* backdoor observed in several of the campaigns, is provided later in this report.

Background - MuddyWater

MuddyWater is an Iranian threat group operating under the authority of the Iranian Ministry of Intelligence and Security (MOIS). The group is known by several additional aliases in the cybersecurity domain, including Static Kitten, Zagros, and Mango Sandstorm.

Active since 2017, MuddyWater focuses primarily on cyber espionage (CNE) operations. The group routinely leverages social engineering techniques to obtain initial access to organizational networks and maintains long-term persistence within target environments for intelligence collection.

MuddyWater operates across multiple countries, including Israel, Turkey, Afghanistan, Pakistan, the United Arab Emirates, Iraq, the United Kingdom, Azerbaijan, the United States, Egypt, and Nigeria.

Its targeting spans a wide range of sectors, including government, telecommunications, healthcare, academia, IT services, and SMBs.

In the Israeli cyberspace, MuddyWater maintains persistent and continuous activity, characterized by the distribution of phishing campaigns, the deployment of custom-developed tools, and the use of decentralized command-and-control infrastructure.

Phishing Characteristics

Impersonation:

- Use of compromised organizational email accounts to distribute highly credible phishing messages.
- Registration of lookalike domains resembling Israeli organizations.
- Tailoring email content to match the business profile of the compromised organization.
- Use of generic and deceptive file names, such as *Webinar* or *Invoice*.
- Inclusion of logos, organizational signatures, and official branding elements of the targeted entity.
- Use of Hebrew phrasing that appears mostly correct, often with minor linguistic errors typical of non-native speakers.

Tools:

- Deployment of custom-developed malware or misuse of legitimate Remote Monitoring and Management (RMM) tools repurposed for malicious activity.
- In some campaigns, the phishing email includes an Office file containing VBA macros intended to install the malicious payload on the victim's machine.

Command and Control (C2) Infrastructure:

- Operation of malicious tools via dedicated domains designed to mimic legitimate organizational naming conventions.
- Use of encrypted communication over standard protocols (HTTPS) to blend into normal network traffic.

Phishing Activity – Nov 2025

During November 2025, several phishing campaigns with similar characteristics were identified in the Israeli cyber domain.

These campaigns were distributed through corporate email accounts that had been compromised in advance by the attacker. In most cases, the phishing email contained a short and concise message, serving as a simple yet effective lure that encouraged the potential victim to download attached files onto their endpoint.

The attachment included a malicious Word (DOC) file containing embedded macro commands. Once opened, after the user clicked *Enable Content*, the macro executed and installed the Backdoor the targeted endpoint.

Following the initial infection, the attacker leveraged the victim's compromised email account to propagate the campaign further to additional recipients, including internal recipients within the organization, enabling rapid lateral spread across the corporate environment.

BlackBeard – Technical analysis

BlackBeard is a Rust-based backdoor and downloader malware family.
The malware is used during the initial access phase, enabling the attacker to gain a foothold within the organizational network.
BlackBeard is capable of performing system reconnaissance, evading security products, and downloading additional payloads to establish a deeper and more persistent presence inside the environment.

The infection chain relies on social engineering and is carried out through several clear and structured stages:

1. Delivery of the Malware:

   The victim receives a phishing email sent from a compromised organizational mailbox or from an impersonated domain.
   The email includes a seemingly legitimate Word document as an attachment.

2. Execution of Malicious Code via VBA Macros:

   The attached document contains embedded VBA macro commands.
   Upon opening the file, the user is prompted with the *"Enable Content"* button.
   Once clicked, the macro is executed, extracting, installing, and launching the BlackBeard malware on the endpoint.

3. Initial Execution:

   In its initial execution phase, BlackBeard performs the following actions:

   - Scans active processes
   - Detects installed EDR/AV products
   - Dynamically adjusts its behavior to evade detection, including the option to fully halt execution

4. Capabilities:

BlackBeard possesses extensive interaction capabilities within the compromised system, including:

- Creating, deleting, and modifying files and directories
- Uploading files from the victim machine to the attacker's server
- Downloading additional files and modules from the attacker's server
- Executing further system-level operations based on commands received from the Command-and-Control (C2) server

In practice, the malware functions both as a Downloader and as a fully operational Backdoor.

5. Command and Control (C2) Communication:

   The malware communicates and performs beaconing to a C2 server whose address is hard-coded within the binary. Communication characteristics include:

   - Use of HTTPS POST requests
   - Exfiltrated data transmitted in encrypted form within the request body
   - Use of a Cookie header containing an encrypted victim identifier, system details, and metadata related to the compromised endpoint

The use of HTTPS and Cookie headers is intended to blend malicious traffic seamlessly into normal organizational network traffic.

6. Persistence Mechanism:

To ensure its persistence even after the system is rebooted, the malware implements a File Association Hijack technique.

BlackBeard creates a file within the Startup directory using a unique file extension (.klp1).

It then modifies specific Windows Registry keys to associate this custom extension with the malicious executable.

As a result, any attempt to open a file with this extension — including those generated by the malware itself — will automatically trigger the execution of the Backdoor.

This method is stealthy and is designed to bypass detection mechanisms that rely on identifying modifications to Run Keys or Scheduled Tasks.

TTPs – MITRE ATT&CK

Attack Phase	MITRE ATT&CK ID	Technique Name
Reconnaissance	T1589	Gather Victim Identity Information
Reconnaissance	T1598	Phishing for Information
Initial Access	T1566.001	Phishing: Attachment
Initial Access	T1566.002	Phishing: Link
Execution	T1204	User Execution
Execution	T1059	Command and Scripting Interpreter
Defense Evasion	T1027	Obfuscated/Encrypted File or Information
Defense Evasion	T1036	Masquerading
Persistence	T1546.003	Event Triggered Execution: Windows File Association
Discovery	T1082	System Information Discovery
Discovery	T1057	Process Discovery
Command and Control (C2)	T1071.001	Application Layer Protocol: Web Protocols
Command and Control (C2)	T1105	Ingress Tool Transfer
Collection	T1005	Data from Local System
Exfiltration	T1041	Exfiltration Over C2 Channel