Dear ORNA Customer,

We are sending you this advisory to provide situational awareness about the new malware deployed by Iranian state hackers.

Summary

A new campaign by the suspected Iranian state hacking group MuddyWater, also known as Mercury and Static Kitten, has been identified targeting organizations in Israel and across the Middle East with a previously unseen custom backdoor malware called BugSleep. This campaign, discovered in May 2024, has been analyzed by researchers at Check Point and Sekoia, highlighting significant advancements in MuddyWater's TTPs.

The campaign specifically targets Israeli towns, airlines, journalists, and other organizations. There is evidence suggesting that other countries, including Azerbaijan, Turkey, and Portugal, have also been targeted.

MuddyWater is affiliated with Iran's Ministry of Intelligence and Security and has been active since at least 2017. The group has previously targeted government entities, municipalities, media outlets, and travel agencies in various countries.

The increased monitoring of legitimate remote management tools by security vendors has likely influenced MuddyWater to develop and deploy BugSleep, reducing their reliance on remote management tools. The persistent nature of these threat actors and their evolving techniques underscore the need for robust cybersecurity measures and continuous vigilance.

Malware Details

- **BugSleep:** The new malware variant is designed to remotely execute commands on compromised systems and transfer files between infected devices and the attacker's servers. Despite containing several bugs and poorly written code, it is continuously being improved by the threat actors.

- **Evasion Capabilities:** BugSleep has advanced evasion capabilities. In one variant, it prevented endpoint detection and response by blocking processes from loading images not signed by Microsoft and from generating or modifying executable code.

- **Deployment Method:** Initially delivered through phishing emails containing customized links to the Egnyte file-sharing application, which then downloaded a PDF file. Opening the PDF resulted in a ZIP file that unpacked BugSleep onto the victim's device.

- **Phishing Lures:** Transitioned from tailored malicious emails to more generic-themed, well-crafted phishing lures such as invitations to online courses. This shift allows reuse of the same lure across different targets and regions.

- **Malicious Links:** Recent campaigns embedded malicious links in PDF files instead of emails, which previously included links to online storage services hosting malicious ZIP archives.

- **Activity Increase:** There has been a notable increase in MuddyWater's activities in Israel and other countries since the beginning of the Israel-Hamas war in October 2023. Over 50 spear phishing emails linked to MuddyWater were identified targeting more than 10 sectors since February 2024.

Recommendations

Recommendation #1: Enhance Email Security

Implement advanced email filtering solutions to detect and block phishing attempts.

Recommendation #2: Endpoint Protection

Deploy and regularly update EDR solutions to detect and mitigate advanced evasion techniques.

Recommendation #3: Users Awareness

Conduct simulated attack scenarios to make sure that the employees are well aware of phishing and other risks, and also to make sure that they report the incident to the internal cybersecurity team.

Recommendation #4: Prepare for the Worst

ORNA strongly recommends that organizations ensure that all critical systems are backed up appropriately and that incident response plans are rehearsed regularly so that all participants understand their role.

References

1. The Record: https://therecord.media/iran-muddywater-hackers-target-israel-new-malware

2. BankInfoSecurity: https://www.bankinfosecurity.com/iranian-state-hackers-deploying-new-malware-backdoor-a-25778

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.

Sincerely,
ORNA Team