ORNA™
Cybersecurity Advisory

Dear ORNA Customer,

We are sending you this advisory to provide situational awareness of a recently disclosed attack on several academic organizations in Israel.

Summary

According to a report from cybersecurity researchers, the Iranian hacktivist group **LORD NEMESIS** executed a successful supply chain attack targeting Rashim Software Ltd., a leading provider of academic administration solutions in Israel, and subsequently infiltrated several academic institutes relying on Rashim's services.

The attackers compromised Rashim's admin account, exploited multi-factor authentication weaknesses, and utilized the VPN infrastructure for data exfiltration, demonstrating a calculated and prolonged presence within the systems. The attack, attributed to Iran's geopolitical motivations, highlights the evolving threat landscape where hacktivist groups leverage cyber operations for ideological and political purposes rather than monetary gain.

Research suggests that **LORD NEMESIS'** TTPs overlap with the previously identified threat group that is named and tracked as Nemesis Kitten. In 2022 the U.S government announced sanctions and legal actions against Tehran-backed operations, including groups Cobalt Mirage, APT35 and Charming Kitten, who were all connected to the Iranian Islamic Revolutionary Guard Corp (IRGC).

The impact of the attack is profound, emphasizing the significant risks associated with third-party vendors and the broader implications of supply chain compromises. The successful breach of these academic institutes allowed LORD NEMESIS access to potentially compromising sensitive student information, whilst strategically releasing their findings to the global web to maximize psychological impact.

The incident underscores the urgent need for organizations to bolster cybersecurity defenses, implement robust vendor risk management practices, and stay vigilant against evolving cyber threats, particularly those driven by geopolitical motives.

Recommendations

Recommendation #1: Limit Vendor Access Privileges

ORNA strongly recommends organizations to restrict and carefully manage access privileges granted to third-party vendors in order to minimize the risk of compromise through supply chain attacks.

Recommendation #2: Thorough Due Diligence on Vendors

ORNA strongly recommends organizations to conduct thorough due diligence on third-party vendors, including assessing their security practices and ensuring they adhere to robust cybersecurity standards.

Recommendation #3: Multi Factor Authentication

ORNA strongly recommends organizations to implement strong authentication mechanisms, including MFA, to enhance security.

Indicators of Attack/Compromise

Malicious IP addresses:

- 45.150.108.242
- 195.20.17.128
- 195.20.17.171

References

Op C Net: https://op-c.net/blog/lord-nemesis-strikes-supply-chain-attack-on-the-israeli-academic-sector/
Recorded Future: https://therecord.media/iran-linked-lord-nemesis-hacktivists-target-israel

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

Sincerely,
ORNA Team