Cybersecurity Advisory

Dear ORNA Customer,

We are sending you this advisory to provide situational awareness about an attack on ESET Israel and the consequences of that breach.

Summary

It has recently come to light that an Iran-aligned threat group impersonating the cybersecurity firm ESET in a phishing campaign aimed at Israeli organizations, distributed wiper malware through emails that seemed to originate from ESET.

The email subjects used urgent language in order to distract the reader from taking a cautious approach at verifying the information within. These included links to a ZIP file that, once downloaded, deployed malicious software disguised as a legitimate ESET tool.

The campaign targeted Israeli cybersecurity personnel and reportedly took advantage of ESET's Israeli distributor's systems. While ESET confirmed the incident, they clarified that their global systems were not compromised. ESET has since implemented a detection signature designed to flag any malicious files related to this attack.

The attacks are linked to Iran-aligned threat groups like Handala, CyberToufan and TA402, known for targeting Israeli entities with politically motivated cyber activities, though no specific group has been identified as responsible for the attack.

Recommendations

Recommendation #1: Create/Follow Proper Update Policy

ORNA **strongly recommends** that organizations have proper policies in place for installing and updating their software packages that come from trusted channels of communication with the supplier.

Recommendation #2: Create and Maintain Incident Response Playbooks

ORNA recommends that organizations have incident response playbooks in place for handling rogue software on their systems. These playbooks should be regularly practiced in order to minimize the response time and potential damage.

Recommendation #3: Stay Up-to-date on Threats

ORNA recommends that organizations remain vigilant of news and advisories related to their sector and technology stack in order to be aware of any ongoing threats and to take appropriate measures to mitigate any potential attack.

References

1. https://doublepulsar.com/eiw-eset-israel-wiper-used-in-active-attacks-targeting-israeli-orgs-b1210aed7021
2. https://therecord.media/hackers-impersonate-eset-wiper-malware

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

Sincerely,
ORNA Team