U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0403

KNIGHT RANSOMWARE SPREADS VIA FAKE EMAILS

DATE ISSUED: 16th August 2023

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

A new spam campaign was identified by Sophos researcher Felix, where the Knight ransomware is distributed under the guise of TripAdvisor complaints. This ransomware was formerly known as Cyclop and was rebranded in July 2023.

BREAKDOWN

Knight ransomware is a recent rebrand of the Cyclop Ransomware-as-a-Service, which switched its name at the end of July 2023. A new spam email campaign is using pray-and-spray mass distribution techniques to target a large number of users. The spam email includes ZIP file attachments named “TripAdvisorComplaint.zip” which contains an executable file named 'TripAdvisor Complaint - Possible Suspension.exe'. A newer version of this campaign spotted and analyzed by Bleeping Computer includes an HTML attachment named 'TripAdvisor-Complaint-[random].PDF.htm'. The HTML file is opened in a fake browser window to TripAdvisor which pretends to be a complaint asking the user to review it. However, clicking the 'Read Complaint' button will download an Excel XLL file named 'TripAdvisor_Complaint-Possible-Suspension.xll' which executes the malware when opened. But if Excel detects the Mark of the Web (MoTW) it will not enable the .NET add-in built into the Excel document, nullifying the attack unless a user unblocks the file. Enabling the add-in will cause the Knight Lite ransomware encryptor to be injected into a new explorer.exe process and begin to encrypt the files on your computer.

REMEDIATION STEPS

- Educate employees about phishing and social engineering tactics. Encourage them to be cautious when opening email attachments or clicking on links.
- Maintain frequent backups of critical data on separate systems or offline storage. This ensures you can recover your data without paying a ransom if attacked.
- Keep all operating systems, software, and applications up to date with the latest security patches to prevent exploitation of known vulnerabilities.
- Use email filtering and authentication protocols to prevent phishing emails from reaching your inbox.
- Check out our Ransomware Defence Strategy Guide for more tips on how to secure your environment.

REFERENCES & RESOURCES

Bleeping Computer	https://www.bleepingcomputer.com/news/security/knight-ransomware-distributed-in-fake-tripadvisor-complaint-emails/