Incident Response Case Study

Case ID: SOC338

Threat: Lumma Stealer – DLL Side Loading via Click Fix Phishing

Platform: LetsDefend.io

Analyst: Chris Bekoe

Date: 14/06/25

Alert

An alert was generated after a suspicious link was detected in the email of Dylan from the email address 'update@windows-update.site' with the SMTP IP address of 132.232.40.201 and was sent to Dylan on Mar,13 2025, 09:44AM. Email security tools did not flag the message; the action showed was 'Allowed'.

Detection

The sender address of the email looked suspicious and the subject of the email contained shouting. A countdown was included in the mail trying to get the user to act quickly in addition to the many 'UPDATE NOW' buttons all over the mail.

Also, at the footer some of the footer elements were just typed there and not links.

Analysis

The presence of multiple embedded URLs further raised suspicion. To further analyse the suspicious URLs, it was passed into VirusTotal. Results showed that it was flagged as malicious and classified as phishing indicating that the URL poses a significant threat to the system of the recipient.

The next step was to check whether Dylan, the recipient fell victim to the phishing mail. Checking the log management, filtering with the Dylan's phone IP address, it was established that he happened to click on the suspicious URL. The log management showed communication from Dylan's phone to the SMTP IP address of the mail.

Lastly, the terminal history of Dylan's device also showed that 'mshta.exe' – which is used by attackers to run malicious scripts, was ran about the same time the suspicious URL was visited and in the process a URL 'https://overcoatpassably[.]shop/Z8UZbPyVpGfdRS/maloy.mp4' was also visited.

Impact

Dylan's device was immediately considered as highly compromised. Also it was safe to assume that all personally identifiable information was compromised as well and if not dealt with may spread and infect all devices on the same network as Dylan's

Response

- The device was isolated from the network immediately.
- The email containing the suspicious URL was deleted.

Recommendations

- All passwords should be reset.
- End user training on phishing awareness should be conducted.
- Implementation of sandboxing and other stricter spam filtering policies.
- Enable EDR (Endpoint Detection and Response) across all devices.