ADVISORY ON SPEAR-PHISHING CAMPAIGN TARGETING AVIATION COMPANIES

Overview

A spear-phishing campaign is targeting aviation companies, using malicious documents that deliver information-stealing malware. The campaign involves attackers spoofing emails of legitimate organizations with lures relevant to aviation, travel, or cargo. The emails sent distribute an actively developed loader, which then delivers a remote access Trojan RevengeRAT, aka AsyncRAT that is designed to remotely monitor and control other computers.

The malware is equipped with a keylogger, screen viewer and command execution capabilities.

Effect

The document attached to the email (usually in PDF format) contains a link to a VBScript file hosted on Google Drive, that drop the Trojan payloads on the victims machine, This ultimately leads to delivery of the Remote Access Trojans (RATs), leaving the organization vulnerable to an array of security risks.

and an attached .PDF file included an embedded link, containing a malicious VBScript which would then drop Trojan payloads on a target machine.

The Trojans continuously re-run components until they are able to inject into other processes. Consequently, they exfiltrate data including credentials, screenshots and webcam data, browser and clipboard data, system and network information, often via SMTP Port 587.

Preventive Measures

- Avoid opening and delete suspicious looking emails without opening them.
- Upgrade secure email gateways and controls.
- Don’t click on links within emails.
- Verify emails before opening them or downloading.
- Regular cyber security training.

For further enquiries, please contact CERRT.NG through the following channels:

E-mail: support@cerrt.ng
Phone:+2348178774580
Web: www.cerrt.ng
Twitter: https://twitter.com/cerrt_ng