AL2024_07 Hackers Phish Finance Orgs Using Trojanized Minesweeper Clone

Description

Hackers are leveraging a trojanized Minesweeper clone to target finance organizations. The malicious game is used to deploy malware and steal sensitive data, posing a significant security threat.

Details

The attack commences with a phishing email from "support@patient-docs-mail.com," masquerading as a medical center under the subject "Personal Web Archive of Medical Documents." Recipients are lured into downloading a 33MB .SCR file via a Dropbox link. This file deceptively blends innocuous code from a Python-based Minesweeper clone with harmful Python scripts that fetch further malicious components from anotepad.com.

The Minesweeper code includes a function, "create_license_ver," repurposed to decode and run the concealed malicious script. This script, a 28MB base64-encoded string, decodes to form a ZIP file containing an MSI installer for SuperOps RMM. This installer is then executed using a static password, granting attackers unauthorized remote access to the victim's computer.

Indicators of Compromise (IoCs)

Organizations should be vigilant for the following indicators of compromise:

- Unexpected presence of SuperOps RMM software, especially if it is not used by the organization.
- Network traffic involving calls to "superops.com" or "superops.ai."
- Emails from "support@patient-docs-mail.com" with subject lines related to medical documents.
- Downloads of .SCR files, particularly those with a size of 33MB, from Dropbox links.

Remediation

Organizations can mitigate the risk by:

- Blocking emails from suspicious domains like "patient-docs-mail.com."
- Monitoring network activity for connections to "superops.com" or "superops.ai."
- Scanning systems for the presence of SuperOps RMM and other unauthorized software.
- Implementing strict email filtering to block phishing attempts.
- Educating employees on identifying phishing emails and the risks of downloading unknown files.

References:

- Toulas, B. (2024, May 26). Hackers phish finance orgs using trojanized Minesweeper clone. Retrieved from Bleeping Cpomputer.

  https://www.bleepingcomputer.com/news/security/hackers-phish-finance-orgs-using-trojanized-minesweeper-clone/

- Jacob, S. (2024, May 30). Hackers use trojanized minesweeper clone to target finance organizations. Retrieved from Spiceworks.

  https://www.spiceworks.com/it-security/cyber-risk-management/news/hackers-use-trojanized-minesweeper-clone-to-target-finance-orgs/