SOC TIPS

INCIDENT REPORT

BY KATE AMARACHUKWU IGWILO

SCENARIO

Incident Overview:

Your organization's SIEM tool flagged unusual outbound traffic from a corporate workstation to an IP address associated with a known malicious domain.
You investigated and discovered that an employee opened a phishing email, clicked a malicious link, and downloaded a Remote Access Trojan (RAT).
The attacker attempted to exfiltrate sensitive data, but the firewall blocked the outbound traffic.

01

INTRODUCTION

This report details a security incident flagged by the SIEM tool and promptly mitigated.

02

DESCRIPTION

At 2:15 AM on Monday, January 25, 2025, the SIEM tool flagged unusual outbound traffic originating from a corporate workstation with IP address 110.24.54.23 to a known malicious domain (hxxp://www[.]mailcioussite[.]com).

03

ANALYSIS

Upon investigating the logs, the SOC team identified that an employee had opened a phishing email, clicked on a malicious link, and downloaded a file. Further analysis revealed the file to be a Remote Access Trojan (RAT). The attacker attempted to exfiltrate sensitive data, but the attempt was unsuccessful as the outbound traffic was flagged and blocked on time.

04 RECOMMENDATIONS

- Conduct regular social engineering awareness training and phishing tabletop simulations to help employees recognize and respond to threats.
- Educate employees on limiting personal information shared on social media to reduce exposure to targeted attacks.
- Block the identified malicious IP address and domain to prevent further access.
- Stay updated on the latest attack trends and enhance threat intelligence capabilities.

05

CONCLUSION

This incident highlights the importance of swift response and continuous security awareness training. Proactive measures, such as employee education and robust monitoring systems, are crucial for effectively identifying and mitigating security threats.

SOC TIPS

NOW TRY IT!

GOODLUCK