Report – EventID 59 “I hacked your computer”

Platform: LetsDefend
Role: Junior SOC Analyst
Alert Type: Phishing Mail Detected
System: Microsoft Exchange
Severity: Low

1. Alert Metadata

- **EventID:** 59
- **Event Time:** Feb 14, 2021, 03:00 AM
- **Rule:** SOC101 - Phishing Mail Detected
- **SMTP Address:** 27.128.173.81
- **Source Email:** hahaha@ihackedyourcomputer.com
- **Destination Email:** mark@letsdefend.io
- **Email Subject:** I hacked your computer
- **Device Action:** Blocked

2. Investigation Steps

1. Reviewed alert metadata and rule details.
2. Verified sender and recipient email addresses.
3. Checked subject for social engineering indicators.
4. Validated SMTP IP reputation.
5. Observed device action (Blocked → confirmed protection).
6. Documented findings and captured screenshots for evidence.

3. Analysis

- The email is a **phishing and social engineering attempt** designed to intimidate the recipient.
- The sender domain is suspicious and not affiliated with the organization.
- Subject line “I hacked your computer” indicates an attempt to trigger fear and prompt the user to act without thinking.
- The Exchange system successfully **blocked** the email, preventing delivery.

4. Findings

- Real phishing attempt targeting users.
- Attackers rely on fear and urgency (social engineering).
- Automated security controls correctly blocked the threat.

5. Conclusion

- This alert is a **True Positive**.
- No further compromise occurred due to effective blocking.
- Recommend continued monitoring of similar SMTPs and phishing patterns.