Security Incident Report

**Incident Report #:** IR-83637

**Reported Date and Time**: March 26, 2020. 8:05 PM

**Technician:** Natnael Kebede

**Site Location:** HR Department workstation (Windows 2016) that is connected to the network and belonging to John Smith.

**Identification (Type and how detected):** A trouble thicket was generated by an automated nightly system check from the Windows workstation itself.

**Virus scan detected** Keylogger and Entangle Worm (achtung.exe)

**Triage (Impact):** Fortunately, it only affected the user’s workstation and did not spread to the company network.

**Containment (Steps taken):**

1) Disconnected the contaminated workstation from the network (unplugged Ethernet cable or disabled wireless) connection to leave the machine isolated from the organization’s network, as well as the internet.

2) Ran a manual virus scan, which identified the malware, and placed it in quarantine.

**Investigation (Cause):** The Anti-Virus (AV) software installed on the machine was not fully configured and updated, and protection was disabled. The suspicious occurrence highlights a possibility for malware infection.

**Recovery and Repair (Resolution):**

Restarted the antivirus solution and updated its signatures.

Used AVG Antivirus software to quarantine and eradicate the malware.

Used AVG Antivirus software to delete the malicious files found in the quarantine area.

**Lessons Learned (Debriefing and Feedback):**

Antivirus software on systems should be configured to scan all hard drives regularly to identify any file system infections. It should also be configured to optionally scan other storage media. Additionally, users should be able to launch a scan manually as needed.

Furthermore, they should be educated on protecting themselves from viruses by running company authorized software only. Plus, they shouldn’t open any suspicious e-mail attachments, and should prevent themselves from responding to suspicious or unwanted e-mails.