Security Incident Report

Incident Report #: IR-83631

Reported Date and Time: March 12, 2017

Technician: Trevor Dash

Site Location: Sales Department laptop belonging to James Rowenmantle. Windows 2016

Identification (Type and how detected): James in sales called the IT help desk complaining that his system is really slow. He also stated his laptop is behaving weird. Some of his internal reports have been modified and emails from last week have shown up as read. He knows he it wasn't him because he was on vacation last week and left his laptop at home.

Virus scan detected Keylogger and Avalanche (achtung.exe)

Triage (Impact): Fortunately it only affected the user's laptop and did not spread to the company network.

Containment (Steps taken):

1) Disabled wireless on the laptop to disconnect it from the company network.

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

Investigation (Cause): Jame feels that the Anti-Virus (AV) makes his system slow. So he turned it off. Several weeks ago he received an email from a good and trusted friend that contains some vacation pictures. Shortly thereafter he received an offer to try a new and improved AV software and installed it.

Recovery and Repair (Resolution):

Used Antivirus software to quarantine and eradicate the malware.

Implemented scanning of corporate email for malware and spam.

Lessons Learned (Debriefing and Feedback):

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

Users should be educated on protecting themselves from viruses by running only company authorized Antivirus software, not opening suspicious e-mail attachments, not responding suspicious or unwanted e-mails.