Security Incident Report

Incident Report #: IR-83631

Reported Date and Time: April 5, 2025

Technician: Eric Guzman

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

Identification (Type and how detected):

James from the Sales Department contacted the IT Help Desk reporting unusual behavior on his laptop. He stated the system was running unusually slow, and that internal reports had been modified and emails appeared as read, despite him being on vacation during that time. The IT technician determined this to be a potential security incident. A full antivirus scan using AVG Business Edition was conducted, which detected malicious threats, including a keylogger and the Avalanche malware (achtung.exe).

Triage (Impact):

The infection was isolated to James's laptop. There is no indication that the malware spread to the rest of the corporate network or compromised any shared resources. The impact was limited to a single endpoint.

Containment (Steps taken):

1. The laptop was disconnected from the network by disabling wireless connectivity.
2. A full deep scan was performed using AVG, which identified the malicious files and quarantined them.
3. A screenshot of the scan summary and detection list was captured for documentation.
4. The Quarantine (Virus Vault) was reviewed and then emptied to remove the threats permanently.

Investigation (Cause):

James admitted to disabling the antivirus software because it slowed down his system. He had received an email from a trusted contact containing vacation photos and later installed third

party antivirus software promoted in a follow up message. This social engineering attack likely served as the entry point for the malware infection.

Threat Research (achtung.exe):

Upon researching achtung.exe using security threat intelligence sources, it was found to be part of the Avalanche botnet infrastructure, often associated with Trojan droppers and keyloggers. This malware typically masquerades as a legitimate executable and is distributed through phishing emails and malicious downloads. It creates a backdoor to exfiltrate credentials, capture keystrokes, and allow remote access.

Eradication steps involve:

1. Isolating the infected host (air-gapping).
2. Running a full AV scan to detect and quarantine the file.
3. Deleting it from quarantine or restoring the system from a known-good backup.
4. Reviewing startup entries and registry for persistence mechanisms.
5. Re-enabling real-time AV protection and ensuring definitions are current.

Recovery and Repair (Resolution):

The threats were quarantined and removed using AVG Business Edition. After confirming that the system was clean, the laptop was returned to service. Additionally, corporate email scanning policies were updated to include more aggressive filtering for spam and malware ridden attachments.

Lessons Learned (Debriefing and Feedback):

1. Endpoint antivirus must remain enabled and up to date at all times.
2. Users should be prohibited from installing unauthorized software, including third party antivirus tools.
3. Employees must be educated on how to identify phishing attempts and suspicious attachments.
4. Regular antivirus scans and centralized AV management should be enforced.
5. IT should implement a policy based approach to ensure endpoint security settings are not modified by users.