REPORT
USB Security Risk Assessment

v1.2.1

Author:

Eldon Gabriel

July 9, 2025

Cybersecurity Professional | IT Security Consultant

Table of Contents

Revision History

Version	Date	Author	Description of Changes
v1.0.0	02/15/2025	Eldon G.	Initial draft.
v1.0.1	02/16/2025	Eldon G.	Fixed typos and improved sentence clarity
v1.1.0	02/16/2025	Eldon G.	Revised the cover page and Risk Mitigation Recommendations sections.
v1.1.1	02/16/2025	Eldon G.	Enhanced Incident Overview section for clarity and technical depth.
v1.1.2	02/16/2025	Eldon G.	Enhanced approach Analysis section for clarity and technical depth.
v1.2.0	07/09/2025	Eldon G.	Added full section structure, numbering, and conclusion.

1.0 USB Security Risk Assessment

1.1 Project Description

A USB drive was found at the Rhetorical Hospital, raising concerns about a possible USB-baiting attack. A forensic team was called in to check for malware risks, review the files on the device, and test how well the hospital's USB security rules hold up.

1.2 Incident Overview

When I arrived at work, I found an unclaimed USB drive with the hospital's logo. Knowing that it could pose a security risk, I picked it up and conducted a secure, controlled assessment. Inside, I found many files, both personal and work-related, including sensitive data and personal details.

2.0 Approach & Analysis

2.1 Investigation Methodology

A USB drive was examined in a sandboxed virtual environment to eliminate the risk to the hospital network. The investigation included:

- Physical inspection for tampering
- Mounting in read-only mode
- Scanning for malware, autorun scripts, and hidden files
- System monitoring for suspicious behavior

2.2 Sandboxed Investigation

Various files were recovered, including personal documents, images, and work-related materials. One folder included HR-related information, shift schedules, and employee contact details, heightening data security concerns. The presence of both personal and work files violated secure data handling practices.

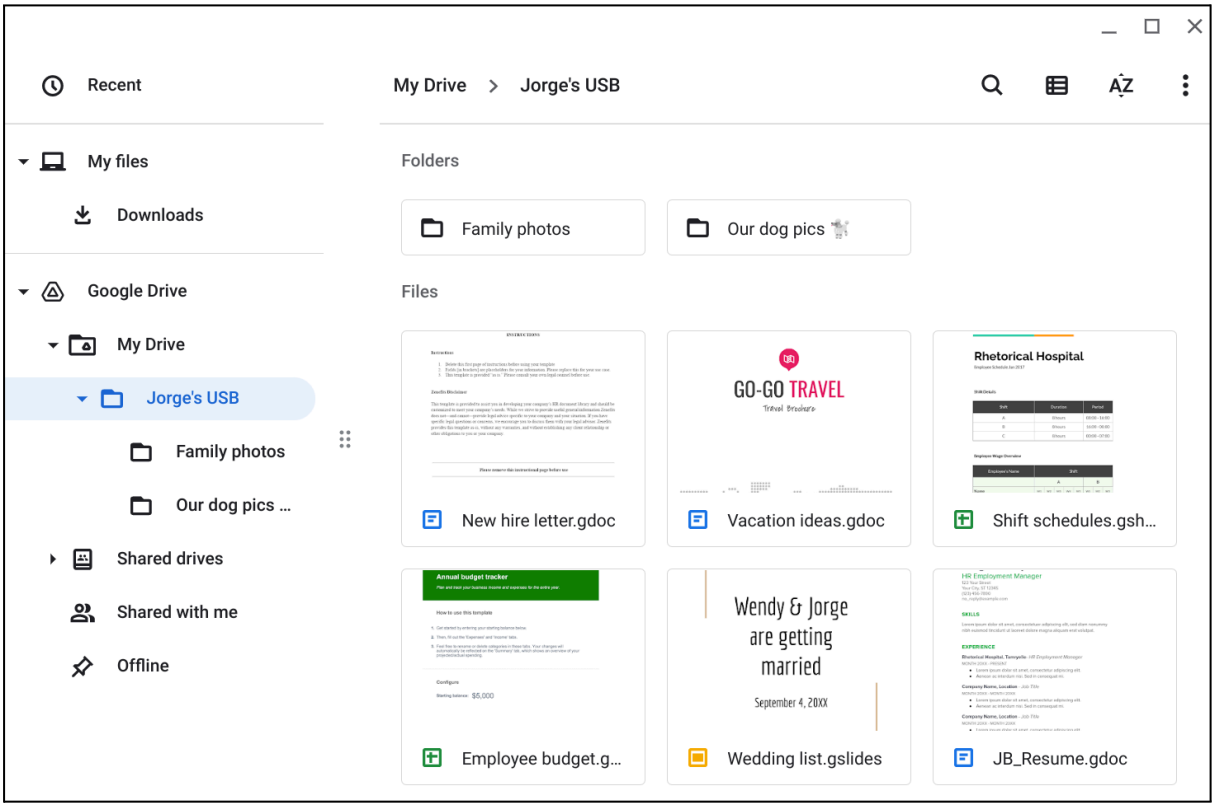

Figure 1: Screenshot of Jorge's USB file. *Image source*: Google, n. d., www.coursera.com

3.0 Threat Analysis

3.1 USB Contents

Notable files included:

- HR documents (e.g., new hire letters, resumes)
- Shift schedules
- PII and internal hospital documents
- Family and personal photos

3.2 Potential Attack Scenarios

The USB could have been used for

- Deploying malware (keyloggers, RATs, ransomware)
- Gathering credentials for internal access
- Launching phishing campaigns using data on the drive

These files may have been intentionally planted as decoys. If connected to a trusted workstation, this could have triggered malware installation or a persistent backdoor.

3.3 Risk Summary

Threat	Impact
Malicious USB Infection	*Malware execution across the hospital network*
Data Exposure	*Unauthorized access to hospital PII*
Social Engineering Attack	Phishing based on leaked personal data

4.0 USB Baiting

4.1 USB Baiting Threats

USB baiting remains a common tactic used by attackers. This scenario illustrates its risk when a device is discovered and unknowingly plugged into a corporate environment. Key concerns include:

- **Hidden malware** inside benign-looking files
- **Ransomware payloads** disguised as documents
- **Social engineering hooks** via embedded personal data

5.0 Risk Mitigation Recommendations

5.1 Technical Controls

- **Encrypt sensitive data** at rest and in transit
- **Enforce access controls** using RBAC
- **Deploy endpoint protection** to scan USB devices
- **Replace outdated protocols** (e.g., disable autorun)

5.2 Policy and Awareness

- **Restrict USB usage** unless explicitly authorized
- **Implement a clear USB device policy** across departments
- **Train employees** on phishing, baiting, and suspicious device handling
- **Develop an incident response plan** for physical device threats

6.0 Conclusion

6.1 Key Takeaways

- The USB contained both sensitive and personal data, thus violating secure data storage practices.
- Attackers may leverage such drives to infiltrate networks or harvest data.
- An isolated and secure analysis prevented possible compromise.

6.2 Security Implications and Recommendations

- Implement strict USB access policies and encryption standards.
- Increase awareness and provide training on USB-related threats.
- Establish a formal process for reporting and investigating the found devices.

Rhetorical Hospital must take proactive steps to mitigate the risks associated with physical USB threats. This incident highlights the importance of secure device handling and continuous staff education in maintaining a robust cybersecurity posture.