

## **USB Drop Attack Risk Assessment Report**

Mohammed Alabdaljabbar - Roberto Martinez - Lauren De Leon - Nicholas Marini - Jonathan

Ruiz

Florida International University

CIS 4951 - Capstone II

Syedmasoud Sadjadi

June 30, 2025

### **Abstract**

This project focuses on USB Drop Attacks. It is one of the many types of social engineering, specifically baiting. It involves putting malicious usb drives in public places and sometimes offices secretly. The attackers would put a sticker that would definitely attract some people, like “free bitcoin” as an example. The bait would then insert the usb and then would get malware. In offices, attackers would mostly disguise themselves in order to attack a certain company to gain information. Our team did a simulation of the project, we chose to use a digispark, which is a microcontroller. It will be used to simulate the usb attack in a harmless way, and once inserted, a message should pop up telling us it is an awareness. Our goal is to raise awareness, and not to use real malware.

The report showcases mitigation strategies evaluation, the impact of attacks caused by USB, and gives examples that happened in the real world. For organizations that have potential vulnerabilities by the user behavior and physical security, we put a recovery and response plan on the report. As a team, we learned that even cheap hardware like the digispark, can show us how real attacks happen. As a result, endpoint protection and training employees is important. Awareness in cybersecurity should always remain a priority, and defending from social engineering attacks is the same, our research and findings reinforced that value.

This project explores USB drop attacks, a form of baiting in which attackers leave infected USB devices with enticing messages, such as “Free Bitcoin,” to trick users into plugging them in. To address this issue, our team simulated this type of attack using a Digispark microcontroller, aiming to highlight and raise awareness about real-world attacks and the importance of employee training and endpoint security. Key risks include data theft, malware infection, reputation

damage, etc, and what they have in common is that it's driven by human curiosity, and our team's goal is to help. After all, awareness is the first line of defense.

## **Introduction**

Nowadays, hackers continue to attack many people in many ways. They take advantage of people's curiosity and mistakes done by some people that leads to a security vulnerability. They use many types of social engineering. There is one specific type of social engineering and its called baiting. Baiting is basically tricking people into thinking that they will get a prize, but they get attacked instead. One of the most known baiting attacks are USB drop attacks. It is an attack where the attacker puts a malicious usb in public and puts a sticker like, "free food code", with the expectation that people will insert the USB. They would then get malware, without the person inserting the USB realizing it.

In order to raise awareness from these attacks, this capstone project focused on doing a simulation of these attacks. A digispark microcontroller was used for this project as the main part of the simulation. When inserted, an awareness message will pop up, which will show people what happens in a usb attack. No real malware was used for this project as the intention is to raise awareness.

A risk assessment report was also done by our team. The report should point out potential threats. Mitigation strategies proposals and an analyzation of these threats impacts is also in the report. A recovery and response plan is also included, as it is very important to help organizations or companies that has vulnerabilities of these attacks. It should help them on what to do when they get attacked. The project aims to showcase how cheap parts like the digispark

are a prime example of USB drop attacks. It is a helpful way to educate people how these attacks happen. Using documentation, simulation, and awareness, it shows us how it is effective.

### **Threat Description**

A USB drop attack is a type of social engineering that can be described as baiting where unsuspecting users are tricked into using a USB that was intentionally dropped in a public or semi-public accessible location. Attackers drop USB devices intending to hook a person into plugging the USB in to utilize the system. Once the unsuspecting person plugs-in the USB we may be running malicious code, malware, or utilizing a backdoor for the attacker. In short, the attacks prey upon human curiosity and exploit a natural human hand movement that bypasses traditional cybersecurity.

In some instances it is not uncommon for attackers to impersonate employees or service people and leave infected USB devices in conference rooms, break rooms, parking lots or wherever unmonitored access is established. A notable attack was reported where USB sticks were infected and dropped in proximity of government facilities or critical infrastructure agencies, and led to numerous breaches of security.

Our simulation emulates this behavior, but rather than installing malware, the Digispark simply runs a harmless script to produce a security awareness message once plugged into a computer. This example helps illustrate the low-cost possibilities of weaponizing inexpensive hardware, and the need for the intent nature of employees to be vigilant in their own security posture, as well as in securing physical devices.

### **Risk Identification**

USB drop attacks pose a number of threats to organizations, and to individuals. The first risk is unauthorized access to your data. When a malicious USB flash drive is plugged into a device, it may collect or steal information, like passwords or confidential files without the user knowing it is happening.

The user may not be aware that the USB device is attacking their device and network and they are actively deploying malware to their device. When the compromised flash drive is plugged into a device, it can deploy spyware, ransomware, and/or keystroke loggers that will do harm to the system or freeware that is corrupting and spreading to other devices on the network. Malicious USB flash drives can lead to a serious affect on the company's operations. Some organizations may lose seeing their employees financially compensated for time worked, as the standard work day whether in a hybrid or full time environment may stall, on a single device.

A second risk is reputational risk. If a security breach received media attention, or constituents and customers received emails or notifications of a potential data breach, and the organization did have safeguards in place could be trust and damage attached for a long time. Organizations may also incur sanctions from regulators, or be sued privately, if the attack resulted in an incidental loss of personal data or an organization failed to meet the privacy terms when conducting business.

Ultimately all these risks are a demonstration of why strong endpoint protection along with regular staff training, utilization police around using USB flash drives and devices of an unknown origin.

### Risk Analysis

Risk Matrix Table

| Risk Matrix |               | Severity   |       |                           |             |              |
|-------------|---------------|------------|-------|---------------------------|-------------|--------------|
|             |               | Negligible | Minor | Moderate                  | Major       | Catastrophic |
| Probability | Frequent      |            |       |                           |             |              |
|             | Likely        |            | R16   | R6, R8, R10, R17          | R1, R3, R13 | R2           |
|             | Moderate      |            |       | R5, R7, R9, R11, R14, R15 |             |              |
|             | Unlikely      |            |       | R12,                      | R4, R15     |              |
|             | Very Unlikely |            |       |                           |             |              |

| ID | Date Raised | Description                                                                                                                           | Probability<br>1 – 5 | Impact<br>1 – 5 | Severity | Mitigation                                                                                              |
|----|-------------|---------------------------------------------------------------------------------------------------------------------------------------|----------------------|-----------------|----------|---------------------------------------------------------------------------------------------------------|
| R1 | 06/16/25    | The device has limited RAM and flash memory. There is a risk of memory overflow.                                                      | 4                    | 4               | 16       | Monitor memory usage, optimize code, avoid heavy libraries                                              |
| R2 | 06/16/25    | Anyone with access to the device can reprogram the device for malicious purposes. Examples include USB Rubber Ducky and HID keyboard. | 4                    | 5               | 20       | Monitor physical device access, disable USB bootloader, enclose hardware                                |
| R3 | 6/16/25     | Lacks encryption, secure boot, and tamper resistance.                                                                                 | 4                    | 4               | 16       | Isolate device physically, restrict use to sensitive purposes                                           |
| R4 | 6/16/25     | Vulnerable to temperature, voltage, or EMI issues.                                                                                    | 2                    | 4               | 8        | Power regulation, shielding, create housing for device                                                  |
| R5 | 6/17/25     | Fluctuation in power may cause damage to or reset the device.                                                                         | 3                    | 3               | 9        | Test power draw beforehand, add capacitors, evaluate USB port beforehand                                |
| R6 | 6/17/25     | Device can become unprogrammable if bootloader fails.                                                                                 | 4                    | 3               | 12       | Regular backups, use verified bootloaders                                                               |
| R7 | 6/18/25     | Depending on the system OS, device may not work reliably. May not work if OS was recently updated.                                    | 3                    | 3               | 9        | Test device for target systems, frequent backups, keep system versions that are known to be compatible. |
| R8 | 6/18/25     | Lacks an onboard debugger, making it hard to troubleshoot.                                                                            | 3                    | 4               | 12       | Use external debuggers that are compatible with device.                                                 |
| R9 | 6/19/25     | Unstable uploads can lead to firmware failure.                                                                                        | 3                    | 3               | 9        | Review upload settings, verify power stability                                                          |

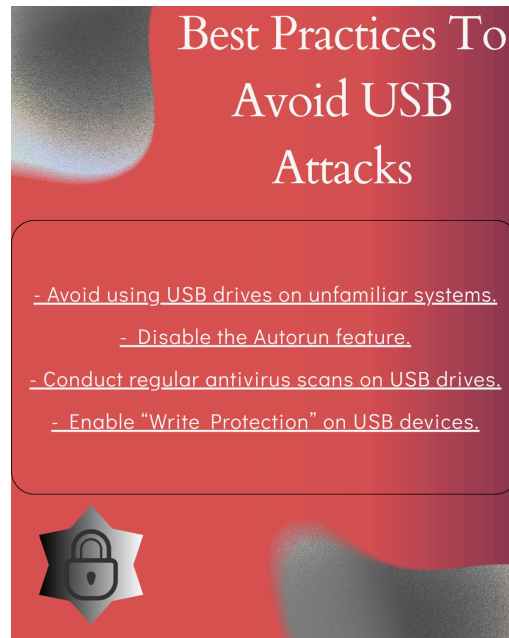
|     |         |                                                                                             |   |   |    |                                                                                    |
|-----|---------|---------------------------------------------------------------------------------------------|---|---|----|------------------------------------------------------------------------------------|
|     |         |                                                                                             |   |   |    | before uploading.                                                                  |
| R10 | 6/20/25 | The device may fail to enumerate or be recognized intermittently.                           | 3 | 4 | 12 | Implement retry logic and use good-quality USB connectors from trusted sources.    |
| R11 | 6/23/25 | Flash has limited write cycles which can wear out with frequent uploads on device.          | 3 | 3 | 9  | Minimize reprogramming. Use EEPROM where possible                                  |
| R12 | 6/24/25 | The pins on the device share multiple functions, which can cause overlap.                   | 3 | 2 | 6  | Pin mapping and planning.                                                          |
| R13 | 6/25/25 | There is no authentication mechanism. Anyone can interact with the device once plugged in.  | 4 | 4 | 16 | Avoid deploying device in untrusted environments.                                  |
| R14 | 6/26/25 | There is no encryption or authentication over USB.                                          | 3 | 3 | 9  | Physically isolate device and data diodes.                                         |
| R15 | 6/27/25 | The device is not fully compliant with USB standards and may act unpredictably as a result. | 3 | 3 | 9  | Test the device thoroughly with any device that is planned to be used with device. |
| R16 | 6/28/25 | Device can overheat over high current and/or poor ventilation.                              | 3 | 2 | 8  | Manage device draw. If necessary, use heat sinks.                                  |
| R17 | 6/28/25 | The device can become unresponsive if code is incorrect or unfinished.                      | 4 | 3 | 12 | Review and test all code. Implement code review practices.                         |



## Mitigation Strategies

### AWARENESS POSTERS





### **The Digispark Awareness Messages**

For our project, the device known as the Digispark included an awareness message that kindly allowed the opportunity for users to learn from the mistake that they committed. Our objective for this message is to effectively show users that, when carelessly connecting external devices into their workstations or personal devices, they run a huge risk of not only causing harm to their own device but also to an organization that they may be a part of. The DigiSpark message that is presented, "You have just been hacked; please don't plug in random USBs," is an effective scare tactic to allow users one last opportunity to learn. Users should not have to reach this extremity if they carefully listen to companies' cybersecurity training and protocols to best avoid these problems.

### **Security Policy Improvements**

The security policy improvements that would allow for any company to best mitigate this kind of attack would be to actively require all employees to have autoplay disabled on all devices, which would play a crucial part in mitigating the initial stages of contact with malware if a device gets infected by a USB baiting attack. An up-to-date firewall and antivirus are also essential for any company, as these services allow for the devices and files to be scanned prior to their use and add an additional layer of protection for the devices. And in the strange case that a USB drive is found floating around the workplace, employees must be proactive and take the devices to the appropriate departments to have them checked through security software in order to find out if someone actually left their drive behind or if it was an attempt at an attack.

### **Recommendations For Employee Training**

Cybersecurity employee training is crucial to any organization since it allows for non-technical users to learn how to protect the data they work with on a daily basis and advises them how to not make any silly mistakes in their day-to-day procedures. Big corporations follow different compliance frameworks; however, a very common framework used amongst all sizes of industries is the NIST framework. This structure has proven to be effective amongst many companies and works for any size company. With this in mind, companies should be mindful of how fast the cybersecurity industry changes, and for this reason, two comprehensive learning sessions should be held throughout the year to allow for employees to retain the guidelines and guidance on how to avoid these kinds of attacks. Companies will have the freedom to place the awareness posters all around the office to ensure that employees are well informed year-round, and if any employees were to be involved in an incident involving data security, it is required for that individual to take additional training. This is an effective method for employees to stay

focused on their work and ensure they follow guidelines to stay safe and not insert any foreign drives into their workstations.

## **Incident Response Plan**

### **1. Purpose and Scope**

This Incident Response Plan (IRP) provides guidance for effectively responding and recovering from a USB drop attack. This plan covers the steps to detect, contain, eradicate, and recover from a malicious USB drop attack. Below contains the incident response lifecycle, which details the procedures for identification, containment, eradication, recovery, and lessons learned, in accordance with the SANS Incident Handler's Handbook and Palo Alto Network's Incident Response Plan Framework.

### **2. Incident Response Lifecycle**

#### **5.1 Identification**

##### **a. Identifiers of potentially malicious USB device**

- i. The USB device contains an unknown serial number and/or is from an unauthorized vendor.
- ii. Abnormal network traffic.
- iii. Execution of suspicious binaries or scripts post USB insertion.
- iv. Alerts triggered by intrusion monitoring tools.

#### **5.2 Containment**

##### **a. Short-term containment**

- i. Isolate potentially affected devices from the network.
- ii. Secure the device(s) in an anti-static bag, if possible.
- iii. Disable USB ports via centralized device control policies.

**b. Long-term containment**

- i. Disable and monitor USB ports through endpoint management tools.
- ii. Block related IP addresses and domains via the firewall and/or any intrusion monitoring tools.
- iii. Monitor the environment for lateral movement.
- iv. Implement device control policies to restrict USB access.

### **5.3 Eradication**

- a. Run comprehensive malware scans on any devices that could have been affected.
- b. Identify and remove any malicious payloads or scripts.

### **5.4 Recovery**

- a. Validate system integrity
- b. Restore affected devices from a known safe back-up.
- c. Reconnect previously disconnected devices to the network.

### **5.5 Lessons Learned**

- a. Update threat detection rules to include USB attack signatures from findings.
- b. Update Standard Operating Procedures based on findings.
- c. Create documentation based on the incident.

## Findings and Conclusions

### Key Risks Identified:

- Data theft and malware infections from unknown USB devices
- Reputational harm and legal consequences
- Operational Disruption

The Digispark simulation provided a safe visual demonstration of how easily these attacks can happen. As seen in the demo, there were many individuals unaware of the risks associated with unknown USB devices until they saw the awareness message. The USB drop simulation helped highlight the power of hands-on learning in changing user behaviors.

This project calls attention to the urgent need for ongoing security awareness training focused on social engineering and actual physical security threats. Also, it shows that prevention does not need expensive tools. Something as cheap as this demo in low cost hardware can illustrate high impact risks, without having to employ ultra sophisticated security measures that will heavily impact functioning and the company's financial situation. Organizations must combine employee alertness, and clear policies to defend against threats effectively.

## References

- Cimpanu, C. (2023, July 21). *China-linked hackers infect systems via malicious USB drives in Africa*. Wired. <https://www.wired.com/story/china-usb-sogu-malware/>
- Abrams, L. (2023, July 24). *USB drive malware attacks spiking again in first half of 2023*. BleepingComputer.

<https://www.bleepingcomputer.com/news/security/usb-drive-malware-attacks-spiking-again-in-first-half-of-2023/>

The Hacker News. (2023, July 20). *Malicious USB drives targeting organizations in Africa and Asia*. <https://thehackernews.com/2023/07/malicious-usb-drives-targeting.html>

Finkle, J., & Bing, C. (2023, November 10). *Ransomware attack on ICBC U.S. unit triggers global market concerns*. Reuters.

<https://www.reuters.com/technology/cybersecurity/icbc-ransomware-attack-triggers-global-regulator-trader-scrutiny-2023-11-10/>

Palo Alto Networks. (2025). *What is an incident response plan and how to get started*. Palo Alto Networks. <https://www.paloaltonetworks.com/cyberpedia/incident-response-plan>

*Incident Handler's Handbook* | SANS Institute. (n.d.). [Www.sans.org](http://www.sans.org).

<https://www.sans.org/white-papers/33901>