Aemilianum College Inc.
Rizal St. Piot, West District, Sorsogon City
Sorsogon, Philippines 4700
Contact No.: (056) 211 – 6012
Email Address: aemilianumcollege@gmail.com
www.aemilanum.edu.ph

SECURITY INCIDENT REPORT FORM

Reported By

Name: Shane H. Habla

Jomer T. Malcontento

Michele Ynna Marie G. Futol

Ralph Lauren John D. Albero

Date of Report: April 29, 2025

Incident Details

Date of Incident: March 20, 2025

Location of Incident: Computer Laboratories 1, 2, and 5 at Aemilianum College Inc.

Type of Incident: Malware Infection via USB Drive

Description:

While attending class at Aemilianum College Inc., a student plugged in an unknown USB flash drive into the computer in Computer Laboratory 1. The student was not aware that the USB contained malware, and it will automatically execute once plugged in. The malicious software spread pretty quickly over the local network and affected the computers in Labs 1, 2 and 5. It could disable anti-virus software, install keyloggers and create backdoor access points. This allowed remote hackers to monitor activities and obtain sensitive info on students and faculty stored locally.

The IT department detected suspicious activities, with spikes of traffic and unauthorized access which was checked. The infection was found three days after first exposure, and by then the system was already compromised.

Impact Assessment

Possible Risks and Damages:

1. Data Theft – A breach may have taken place, resulting in the leak of student projects, faculty documents, and stored passwords.
2. Malware likely caused damage to the academic resources and software tools used in labs.
3. Cybersecurity trust breach affecting reputations of students, faculty, and other stakeholders.
4. System cleaning and restoration disrupted class and laboratory session – Operational Downtime.

Affected Areas:

- Computer Labs 1, 2, 5, Local Lab Networks, Shared Drives and Faculty/Student Accounts from the computers in the lab.

Response Actions Taken

Immediate Containment:

1. Isolated all affected laboratory networks immediately.
2. Shutdown and physically disconnected infected computers. take snaps, and secure backups.
3. Involved hard drive forensic imaging for investigation purpose.
4. Disabled shared drive access across laboratories.
5. Set up some nifty tools to catch any suspicious connections leaving our system.

Mitigation Steps:

1. All computers in the lab will receive full malware scans and reinstallation of a clean operating system.
2. Turned off all USB ports temporarily to avoid further infections.
3. Restricted autorun on all lab systems via Group Policy.
4. Conducted emergency cybersecurity awareness sessions for students and teachers.

5. Tightened endpoint monitoring tools and scheduled automatic security updates for every computers' operating systems.
6. Stricter policies regarding the use of external devices (USB drives).

Evidence Collected:

Time	Action
2 hours	Isolate infected computers from labs 1, 2, and, 5 and gather system logs.
5 hours	Disconnect shared drives and keep malware samples.
8 hours	Forensic imaging of hard drives initiation.
12 hours	Network scans implementation for secondary infections.
24 hours	Clean-up operations and restoration of systems.

Root Cause Analysis

Identified Cause:

- An unauthorized USB drive misused contained malware that exploited autorun vulnerabilities and targeted security weaknesses.

Vulnerabilities Exploited:

- Lack of device control policies (no USB blocking).
- Disabled or outdated antivirus protections.
- Weak local network segmentation between labs.

Recommendations & Preventive Measures

Short-term fixes:

- Full forensic investigation to ensure full clearance.
- Alert impacted users and provide help with passwords and account security.

Long-term Solutions:

- Establish strict rules for the use of external storage devices (whitelisting, encryption).
- Make sure to enforce and update your anti-virus regularly.
- Implement endpoint protection and USB control software.
- Make the network segmentation and firewall rules between the laboratories stronger.
- Online training sessions for faculty, staff, and students.
- Schedule regular security audits of laboratory systems.
- Develop and deploy a centralized USB threat prevention and management system tailored to the institution's IT environment.

Conclusion

The case of Computer Labs 1, 2 and 5 shows the serious risks associated with the use of removable media (USB/flash drives) without regulation. Schools and colleges have a lot of data that can be exploited.

They also tend to have sloppy management of digital devices. These days, human errors such as inserting an unknown USB device remain a major risk factor.

The breach was able to be contained by isolating the problem at hand and responding to it quickly. Moving forward, technical controls and security policies along with user awareness are essential to limiting the risk of this ramification.

Date Closed:
April 14, 2025

Prepared By:

Shane H. Habla
Jomer T. Malcontento
Michele Ynna Marie G. Futol
Ralph Lauren John D. Albero

Reviewed By:

Ms. Laila L. Delito
Supervisor

USBGUARD+: A PROPOSED SYSTEM FOR SECURING ACADEMIC NETWORKS AGAINST USB MALWARE THREATS

A Project Proposal

Presented to the

Faculty of the Graduate School

AEMILIANUM COLLEGE INC

Sorsogon City

In Partial Fulfillment

of the

Requirements for the Subject

Information Assurance and Security

(ITPC11)

SHANE H. HABLA

JOMER T. MALCONTENTO

MICHELE YNNA MARIE G. FUTOL

RALPH LAUREN JOHN D. ALBERO

LAILA L. DELITO

College Instructor

ABSTRACT

This document is a project proposal that includes the design of a Centralized Security Solution – USBGuard+ which aims to prevent the detection and neutralization of USB malware threats in an educational setting. The system incorporates access control, malware scanning, encryption enforcement, user activity logging, and real-time alerts. The system is proposed after the outbreak of a USB malware incident at Aemilianum College Inc. which infected a number of computer laboratories. The project will mitigate the risk of malware intrusion on sensitive data and enable a more secure IT environment.

INTRODUCTION

1. OVERVIEW OF THE CURRENT STATE OF TECHNOLOGY

A. Use Case Scan: Due to the flexibility USB flash drives offer, they continue to be one of the most popular types of portable storage devices among students in academic institutions. Unfortunately, they are also one of the most prolific carriers of malware.

B. Current Situation: In Aemilianum College Inc. and many other USB equipped institutions, USB port usage is often unrestricted. There is little to no endpoint security, accompanied by stagnant antivirus solutions, and many systems seem to operate on obsolete antivirus software. Plugging in unverified drives tends to be a common reality.

C. Problem Details:

- Absence of device control policies
- Antivirus programs are not regularly updated
- Absence of centralized monitoring for USB ports usage
- Systems that have autorun enabled are still considered vulnerable
- Insufficient training on cyber security practices concerning the internet

2. MAIN OBJECTIVE

Create an automated threat management system tasked with handling detection, prevention, and logging of security events associated with USB connections, USBGuard+, a malware USB security measure device.

3. SPECIFIC OBJECTIVES

- Formulate a controller that restricts access to USB devices to whitelisted users only
- Conduct malware checks through the application programming interfaces of antivirus software
- Implement measures to ensure that data stored on USB drives can only be accessed through encrypted channels
- Allow for instant notification and automated locking for acts perceived as suspicious
- Develop an advanced interface for administrators to formulate, track, and monitor set policies on USBGuard+.

4. PURPOSE

USBGuard+ will address the problems encountered in the current system by:

- Restricting access to USB ports.
- Blocking suspicious activities upon device insertion.
- Auditing all relevant actions taken on the device.
- User training via alerts.

5. SIGNIFICANCE

- IT Department: Enhanced insight and oversight regarding device usage.
- Students & Faculty: Augmented uptime of systems and the accuracy of data.
- Administration: Enhanced reputation regarding security as well as compliance adherence.

6. SCOPE

- Control of USB device software for classroom Wintel-based laboratories.
- Detection and logging of malware in real time.
- Administrative panel for confinement and reporting.

7. LIMITATION

- Windows based computers only.
- Malware without AV updates undetectable.
- Offline systems are not included unless connected to the monitoring server.

REVIEW OF RELATED LITERATURE

USB-based attacks are becoming more complex, with successful exploits increasingly employing various techniques, such as social engineering and signal injection. Although there are incomplete defenses such as USB firewalls (e.g., USBFilter and USBGuard), reported attacks exploiting malevolent USB devices ("BadUSB") have the potential for causing real harm (e.g., high Volume service crashes, or data theft). The latest investigations underway are making progress on implementing a security framework, called USBIPS, on operating system (OS) vulnerabilities, with the goal of providing defense-in-depth protection based on behaviours around and methods of allowlisting access to USBs, and using endpoint detection and response as part of a centralized threat analysis framework. (Wang & Hsu, 2024)

This subject matter is incredibly relevant in the context of the malware incident identified within Aemilianum College Inc's Computer Laboratories. In this scenario, the infection that occurred using an unauthorized USB device was a reflection of the concerns regarding how malicious USB devices could easily bypass protection offered up by most protocols. It highlights the need to develop stronger security frameworks, that integrate all USB access controls in the risk analysis, which was also the theme of the recommendations in the incident report for long-term solutions to prevent a repeat of this incident and reinforce the defender's risk profile.

The advent of portable electronic devices such as smartphones, small appliances, and IoT devices has led to an increase in the reliance on the Universal Serial Bus (USB) standard for both communication and power supply. While the convenience of USB has been extensively welcomed, the forbearance on the default trust model has been exploited by attackers who have leveraged it to gain access to sensitive user data. While security experts and device manufacturers battle these attacks, the focus within the threat landscape continues to move to new attacks that are stealthy in nature, such as side-channel attacks, which exploit the electromagnetic emissions and power consumed to infer information about user privacy (Liu, Spolaor, Turrin, Bonafede, & Conti, 2021).

The development within this literature is connected to the recent malware incident that occurred in Aemilianum College Inc.'s Computer Laboratories. The attackers in this incident exploited the trust created through USB devices, and demonstrated the sheer ease by which a device that appears to be innocuous can lead to the compromise of an entire network.

Comprehension of the vulnerabilities within USB technology reinforces the need for stricter device policy and technical controls recommended in the mitigation strategies on the incident report.

USB peripherals have become a means of cyber-attacks because, generally, users trust these devices - they [users] view these devices as benign. A survey of 29 USB-based attacks, found that they can be classified into 4 groups - which demonstrates the potential for common USB devices (e.g., flash drives, keyboards, smartphones, etc.) to deliver malicious payloads. USB attacks leverage hardware vulnerabilities, while also cashing in on user trust; the environments for USB cyber attacks range from individuals to organizations (Nissim, Yahalom, & Elovici, 2017).

This related literature makes so much sense when considered in the context of the recent incident at Aemilianum College Inc‘s Computer Laboratories. The malware infection caused by an unapproved USB device, is indicative of a growing threat of USB-based attacks, and the need to improve device control policies and user awareness and training, that were identified as necessary actions in both the survey and the recommendations in the incident report.

The USB standard is so widely established that it works across the entire spectrum of devices, from large computer systems to small embedded systems. However, the openness of USB also presents tremendous vulnerabilities, as demonstrated in attacks such as BadUSB, due to the unrestricted functionality of USB devices. In this paper, FirmUSB, a framework for analyzing firmware, has provided the opportunity to utilize knowledge of USB protocol to discover malicious activity concealed under the layers of device firmware. FirmUSB provides substantial value in utilizing microcontrollers and maximizing analysis speed in addition to eliminating efforts to obtain source code. FirmUSB has offered an opportunity to emphasize some of the issues and possible ways to address securing embedded USB devices (Hernandez, Fowze, Tian, Yavuz, & Butler, 2017)

This body of literature is closely related to the malware event that occurred at Aemilianum College Inc.’s Computer Laboratories. The obvious infection associated to a USB device demonstrates the ease of implicit restrictions for compromised peripherals to obtained write permission on endpoints and to slip past their basic security norms. This incident demonstrates a need for more thorough device validation and higher endpoint factors, validating the incident

report's recommendations of enforcing stricter control of USB interfaces and enhancing security protocols on systems.

Industrial Control Systems (ICS) are known mostly to be attractive targets for more Advanced Cyber Threats, and the common USB thumb drive has been shown to be a spreading vector. USB drives like these are commonly utilized in ICS environments to transfer information between isolated systems, presenting a significant problem, especially when traveled by half by critical files and the rest non-critical files. The threats include malware embedded in files and firmware-based attacks such as BadUSB, which writes to a devices firmware and impersonates a keyboard when connected to the host, issuing commands automatically with malicious content (Griscioli & Pizzonia, 2018).

The literature is relevant to incidents of malware in the Computer Laboratories at Aemilianum College Inc. in the beginning of October 2023 where a USB device acted as the compromise. It demonstrates the risks of USB use in a promiscuous manner and allows to also lean into a defence in-depth approach with intermediary protection systems like USBCaptchaIn. This study backs up Item #51 from the report as an incentive for a way to increased USB access control and with automated contingencies in place to reduce human error and as a reminder of consequences in both educational institutions or industrial organizations.

REVIEW OF RELATED SYSTEMS

Smadav is a USB safeguard antivirus created in Indonesia. It uncovers malware disguised as shortcuts, autorun viruses, and even files hidden by harmful software on flash drives. Rather than replacing other antivirus programs, Smadav is an additional portable solution that cleans and scans USB devices. It is highly valued in regions where viruses spread through USB drives, especially in public computers and laboratory terminals. Smadav also does not offer features like management from a single control point, system-wide surveillance, or monitoring in real time (Smadav Antivirus, n.d.).

In contrast, USBGuard+ is envisioned as a more comprehensive, network-backed solution for institutional settings like computer labs. While every PC runs Smadav, USBGuard+ would provide centralized monitoring and enforcement of set policies across all lab computers. USBGuard+ is also unlike Smadav in that it adopts a proactive stance, offering preventive

measures such as whitelisting, enforcing file encryption, system-level logging, and block-listing all unauthorized devices. This makes USBGuard+ a superior enterprise solution.

SafeConsole Anti-Malware is a powerful solution tailored for encrypted USB drives. Protects against malware inline on the USB stick, which means files are protected from threats no matter what computer they are used on. This tool also offers SafeConsole management platform integration which enables administrative control, consolidated reporting, and automated updates of malware definitions. This helps corporations with strict data governance policies regarding sensitive information and secure file transport (DataLocker, n.d.).

The major difference between SafeConsole and USBGuard+ regarding USB security is hardware dependence and flexibility of the institutions. SafeConsole is tailored for use with SafeConsoleReady™ devices which might make it difficult for underfunded schools or organizations due to its limited scope of use. Inversely, USBGuard+ is designed to enable protection on all USB devices connected at institutional endpoints and uses software enforcement instead of hardware dependence. This makes USBGuard+ a better alternative for schools like Aemilianum College Inc. due to the increased flexibility and reduced costs.

Kanguru Defender provides encrypted USB drives with pre-copy file scanning antivirus software. Its first line of defense is to block malicious content from entering the drive. These drives are certified FIPS compliant and are suited for the government and healthcare industries containing sensitive or confidential information. The software scans data as it is being deposited onto the drive which serves a “clean on entry” model (Kanguru, n.d.).

USBGuard+ has different scope and accessibility. Kanguru’s solution is based on specific USB drives, while USBGuard+ would track all USB interactions on any standard computer making it much more cost-efficient and scalable for schools. Beyond Paw-tect, USBGuard+ has lab-wide threat detection, audit trails, and permissions which Kanguru only offers on a per-device basis. This allows USBGuard+ to defend institutional settings individually and organizationally without being restricted by proprietary hardware.

Endpoint Protector stands out as an advanced tool for Data Loss Prevention (DLP) due to its robust device control capabilities. It enables administrators to finely adjust access to USB ports and other peripherals so that removable media data leakage does not occur. It helps corporations

that deal with proprietary or regulated data since the system supports policy-driven enforcement and monitoring of the endpoints in real time. Additionally, the system is capable of generating alerts or blocking data transfers during suspected activities (CoSoSys, n.d.).

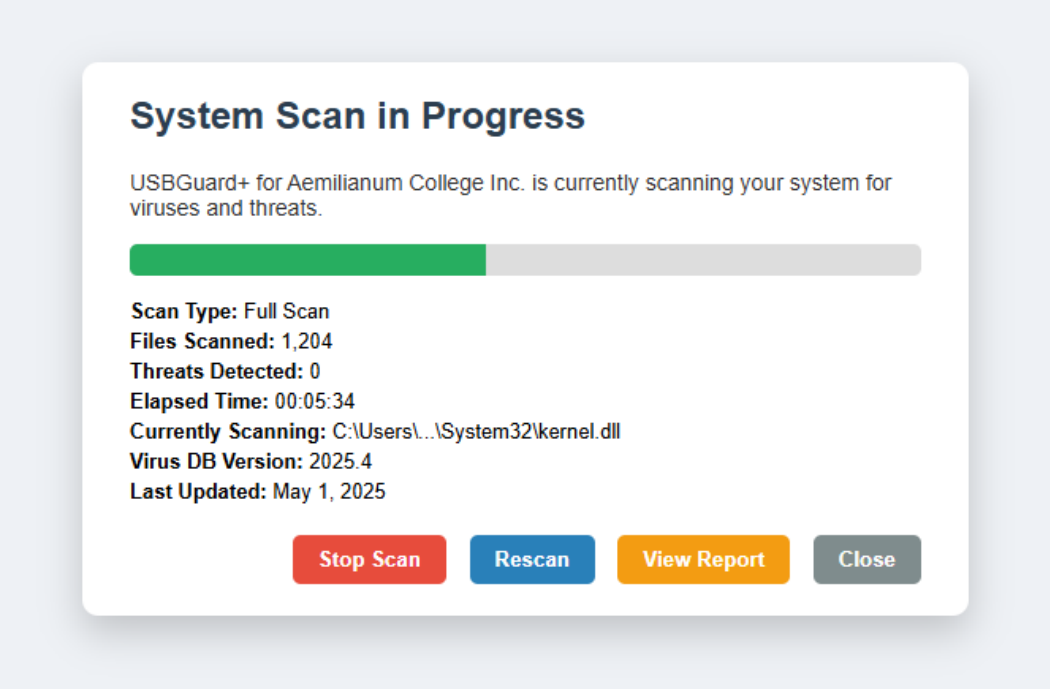
On the other hand, USBGuard+ does not concentrate on data leakage prevention as much as Endpoint Protector does, but focuses on malware containment and prevention in academic or learning environments. As both systems control USB ports and policies access, USBGuard+ attempts to contain the spread of the infections through external devices by scanning content, blocking autorun.inf scripts, and sequestering infected endpoints into a lab network. The focus on education rather than DLP and concentrating on malware on the periphery shifts from Endpoint Protector's enterprise-focused model.

CrowdStrike Falcon® Device Control is part of a broader endpoint protection platform beneficial for larger organizations and enterprises. It provides granular control of USB device usage, centralized logging and device whitelisting and policy automated management. In addition, since it is integrated with Falcon's threat intelligence and detection engine, it is good at working in environments where the use of USB devices must be tightly controlled. It also presents additional visibility into how USB devices interact with systems, which may help an organization meet its auditing or compliance obligations (CrowdStrike, n.d.).

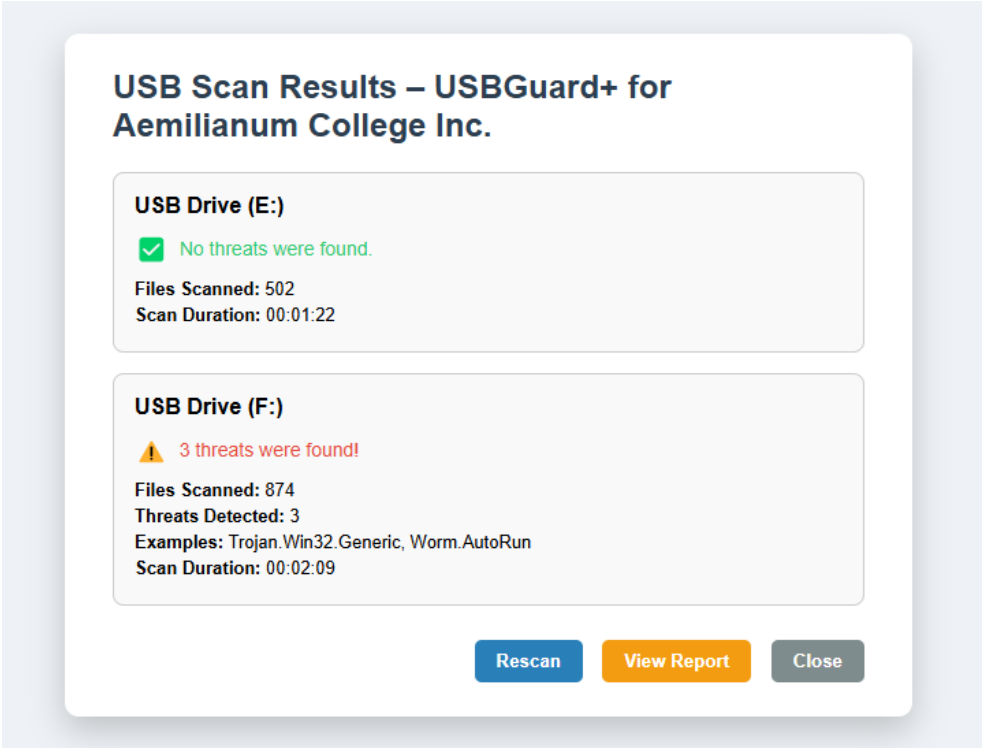
USBGuard+, on the other hand, was made only for educational institutions. It has a much simpler interface and implementation than Falcon and is designed for ease of deployment in a laboratory computer environment. Falcon provides enterprise grade protection with high-end integrations and cloud-based controls. USBGuard+ would be adequate for localized control on a budget. Offline capability would be important for control in school laboratories. USBGuard+ would have modules for training awareness designed to fit in to the educational mandate of educational institutions as compared to compliance-based environments.

MOCK SCREENS

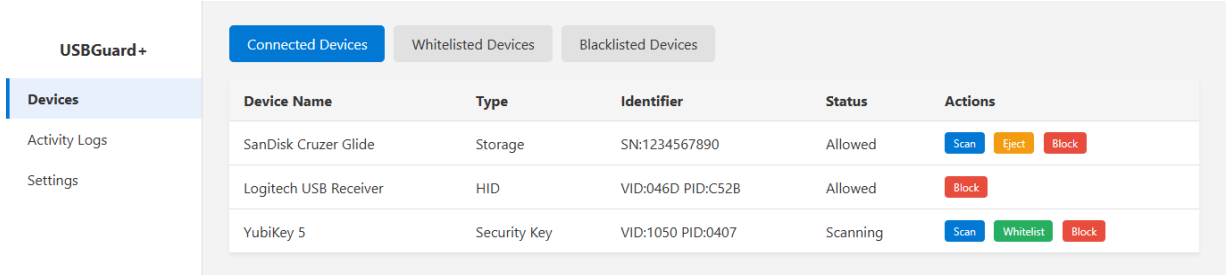
A. Scanning in progress



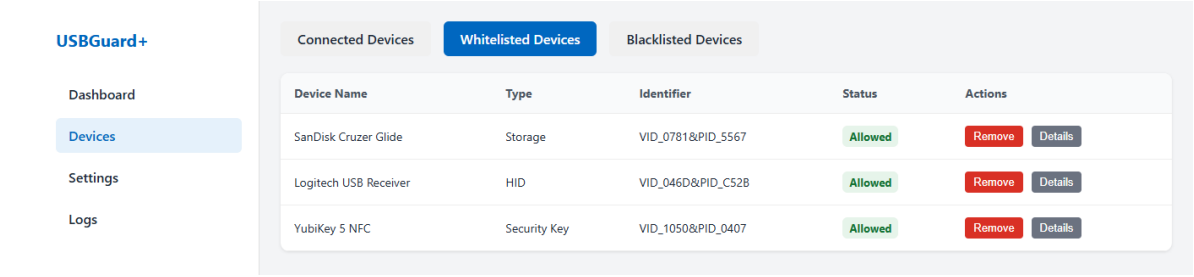
B. Scanning Complete



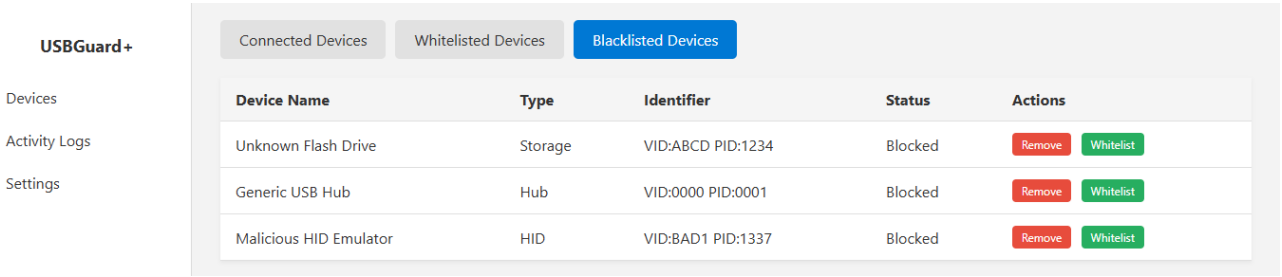
C. MAIN DASHBOARD (Connected Devices)



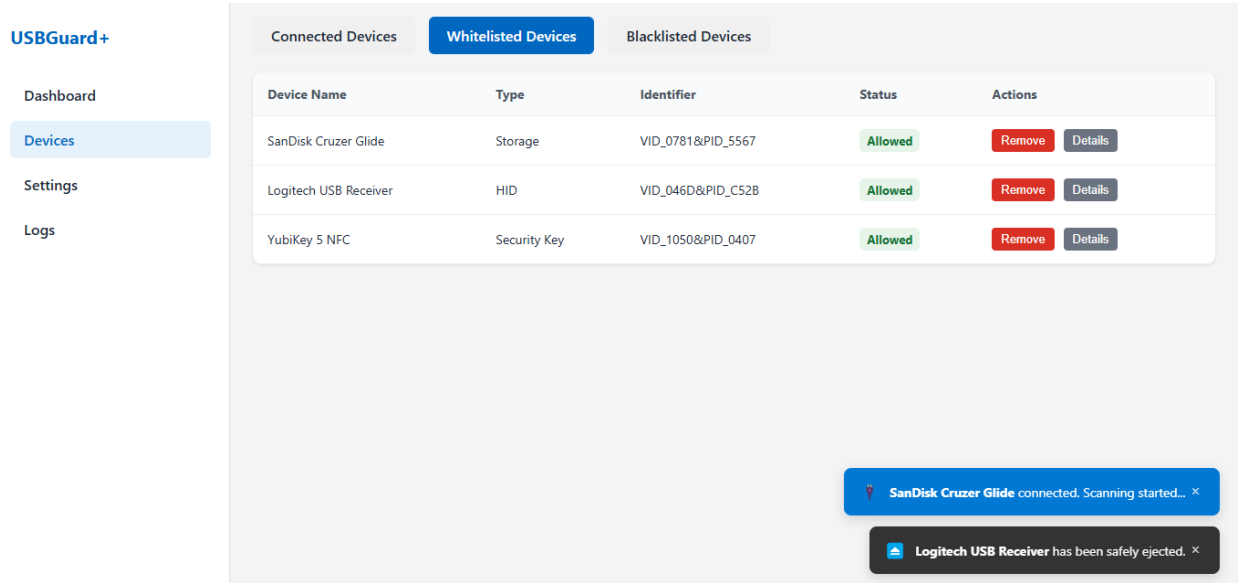
D. MAIN DASHBOARD (Whitelisted Devices)



E. MAIN DASHBOARD (Blacklisted Devices)



F. MAIN DASHBOARD (Notification Alert/Bar)



REFERENCES

A. Related Literature

Liu, H., Spolaor, R., Turrin, F., Bonafede, R., & Conti, M. (2021). USB powered devices: A survey of side-channel threats and countermeasures. High-Confidence Computing, 1, 100007. https://doi.org/10.1016/j.hcc.2021.100007

Wang, C.-Y., & Hsu, F.-H. (2024). USBIPS Framework: Protecting hosts from malicious USB peripherals. arXiv. https://arxiv.org/abs/2409.12850

Nissim, N., Yahalom, R., & Elovici, Y. (2017). USB-based attacks: A comprehensive survey. Computers & Security, 72, 216–232. https://doi.org/10.1016/j.cose.2017.09.008

Hernandez, G., Fowze, F., Tian, D., Yavuz, T., & Butler, K. R. B. (2017). FirmUSB: Vetting USB device firmware using domain informed symbolic execution. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2245–2262. https://doi.org/10.1145/3133956.3134050

Griscioli, F., & Pizzonia, M. (2018). USBCaptchaIn: Preventing (un)conventional attacks from promiscuously used USB devices in industrial control systems. arXiv. https://arxiv.org/abs/1810.05005

B. Related Systems

Smadav Antivirus. (n.d.). Smadav Antivirus 2023 Rev. 15.0. Retrieved May 4, 2025, from https://www.smadav.net

DataLocker. (n.d.). SafeConsole Anti-Malware for Secure USB Drives. Retrieved May 4, 2025, from https://datalocker.com/products/safeconsole/

Kanguru. (n.d.). Kanguru Defender Antivirus USB Drives. Retrieved May 4, 2025, from https://www.kanguru.com/antivirus-usb-drives/

CoSoSys. (n.d.). Endpoint Protector by CoSoSys. Retrieved May 4, 2025, from https://www.endpointprotector.com/

CrowdStrike. (n.d.). Device Control – USB Management | CrowdStrike Falcon. Retrieved May 4, 2025, from https://www.crowdstrike.com/products/endpoint-security/device-control/