ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 11, Issue 2, pp: (97-99), Month: April - June 2023, Available at: www.researchpublish.com

Removable Media Threats to Industrial Plants

Saad Al-Amri[1], Bader Al-Khaldi[2], Saad Al-Harbi[3], Ahmad Al-Barrak[4], Mashary Al-Otaibi[5]

[1]Saudi Aramco, Dhahran, Saudi Arabia

DOI: https://doi.org/10.5281/zenodo.7962048

Published Date: 23-May-2023

Abstract: **This article focuses on the threats associated with the USB removable media that adversaries use as an attack vector to disrupt Industrial Control Systems (ICSs) as these USB devices are the main source for distributing malwares, ransomware campaigns and attacking against industrial plants and operational technology (OT) systems. Moreover, weaponized Human interface devices (HID) devices such as keyboards and mice, charging cables for smartphones are serious threats that can be used to compromise industrial plants control systems.**

Keywords: **Cybersecurity, USB threats, Universal Serial Bus attacks, attacks, Attackers, OT, Operational Technologies, Industrial Plants, Control Systems, Weaponized, Penetrate, Risk mitigation, Sophisticated attacker.**

I. INTRODUCTION

Industrial plants control systems' cybersecurity is very critical and essential for national security. Therefore, most of industrial plants and operational technology (OT) systems are totally isolated from the internet in order to keep these systems safe from external attacks. Attackers use removable media and USB devices as an initial attack vector to penetrate industrial plants network systems and to establish major attacks. Introduces load more advanced malware on plug-in devices to instantaneously impact the intended targeted industrial plants network systems through sophisticated coding that can damage and destroy plants computer systems or generate backdoors to establish attacks. Attackers can then command and control the targeted network systems.

Most of maintenance engineers are still using removable media, Universal Serial Bus (USB) and the reasons for that can be summarized as follow:

- Process control systems and industrial plants networks are commonly designed to be well isolated with strong physical and logical access controls in place. Therefore, these removable devices still are required to transfer files between systems for deploying the required operating systems' security patches, updating Anti-virous, upgrading farmwears, copying required documents between computers, and etc.
- Removable devices can be the only way to get the required files and updates from Industrial Control Systems (ICS) vendors.
- Convenient to carry around and easy to use.

With the abovementioned reasons, the removable media is still highly used as part of operations needs and therefore, remains one of the top vectors for posing serious cybersecurity threats.

II. THREATS

In fact, during industrial plants equipment installation, upgrade or maintenance windows it is a common practice to allow external entities to be part of the operational environments with USB devices, laptops, etc, that are required for vendors to perform the job. However, this is considered a main opportunity for attackers to penetrate and attack the industrial plants network systems.

In 2018 Schenider Electric company raised a concern for potential critical risks that are associated with USB devices that might be shipped with products and infected with malicious software and malwares targeting industrial sectors. Attackers always came up with smart ways to attack isolated network such as industrial plants and operational technology (OT) environment through leveraging compromised third party companies or vendors. According to the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), two power plants in 2012 reported malware infections and both infections were spread through USB removable devices that were plugged into critical systems used to control power generation equipment.

In a recent report that was released by Honeywell industrial cybersecurity in 2022, USB malwares infection increased to 52% and these USB removable media are being highly used to exploit isolated network systems in many industrial and operational technology (OT) environments. The report has shown that USB removable media are one of the top threat vectors and risks disrupting industrial plants control systems.

The Universal Serial Bus (USB) physical port connection has become a world standard for both charging and data transfers. A sophisticated attacker can exploit USB connectivity of mobile phones such as Android smartphone by deploying a custom driver into the smartphone which will then trick the computer as the compromised smartphone appears as a USB device, keyboard or mice once connected in order to compromise targeted computer systems.

III. THREATS MITIGATION

Considering the increased threats vector that USB removable media pose to industrial plants network systems, USB security must include technical controls and enforcement. Since Stuxnet attack via a USB device, cybersecurity companies and experts have looked to address serious threats that are associated with removable media devices. The below recommended security actions should be taken to protect these critical infrastructures against USB removable media threats.

- Establish a comprehensive USB security policy and strictly enforce these policies to avoid cybersecurity breaches that can be caused by these removable media. These policies should be revisited regularly for improvements following the ongoing best practices.
- Ensure employees are well trained and aware of different kinds of threats, including weaponized USB devices such as trojanized mice, keyboards, etc. Focusing on the human aspect is the key approach for mitigating the threats that are associated with USB devices.
- Minimize the number of employees who are authorized to use USB device in the plants. Only authorized administrators, engineers and technicians can use USB with tracking mechanism for critical business needs such as systems patching, upgrading, etc.
- Keep Anti-Virus software updated on daily basis and ensure all systems are fully patches and OT systems are hardened.
- Ensure to use whitelisting technology to guarantee only pre-approved protected applications or content are permitted to run in the plant endpoints while all other applications /data is prohibited to run or enter the network by default.
- Ensure to disable USB removable media access by default on all the plant endpoints and shall only be enabled temporarily for short work requirement on pre-determined machine.
- Ensure to scan and encrypt USB before start using it in the plant networks & Systems.
- Ensure to document and track all the approved USB removable media. Thus, each USB removable media shall be officially assigned to a specific authorized employee.
- Ensure to have security physical control to protect plant’s USB removable media from any security threats or data leakage.
- Enforce security technologies that are capable to detect all kinds of threats including unauthorized USB usage and responds to potential threats with real-time log activity monitoring.

IV. CONCLUSION

Using removable media devices come with serious threats that are specifically targeting industrial plants network systems as sophisticated attackers take advantages of removable media to penetrate into these critical isolated networks and consider this technique as initial attack vector to compromise the targeted network. Following removable media cybersecurity best

practices and technologies are very essential to mitigate the associated risks of using USB removable media in the plants. Furthermore, implementing the recommended security actions shall help to protect industrial plants against attackers.

REFERENCES

[1] Anastasios Arampatzis "USB threats to ICS systems have nearly doubled" https://www.tripwire.com/state-of-security/ics-security/report-usb-threats-to-ics-systems-have-nearly-doubled/

[2] Honeywell "USB Security - myths vs. reality" https://honeywellprocess.blob.core.windows.net/public/Marketing/White-Paper-USB-Security-Myths-vs-Reality.pdf

[3] Honeywell "Industrial Cybersecurity USB Threat Report 2022" https://www.honeywellforge.ai/content/dam/forge/en/documents/cybersecurity/Industrial-Cybersecurity-USB-Threat-Report-2022.pdf

[4] Dragos "North American Electric Cyber Threat Perspective" https://www.dragos.com/wp-content/uploads/NA-EL-Threat-Perspective-2019.pdf

[5] ICS-CERT "ICS-CERT Monitoring" https://www.cisa.gov/uscert/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2012.pdf

[6] Gail Reitenbach, PhD "USB Drives Spread Malware in Control System Environment at Two Power Plants" https://www.powermag.com/dhs-usb-drives-spread-malware-in-control-system-environment-at-two-power-plants/

[7] Fireeye, Andrew Ginter, VP Industrial Security "THE TOP 20 CYBERATTACKS on Industrial Control Systems" https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/wp-top-20-cyberattacks.pdf