SHARING SINCE 2010
Health-ISAC™
Collaborating for Resilience in Healthcare

PHYSICAL THREAT BULLETINS

Physical Security Bulletin - USB Bomb Attack

SHARING SINCE 2010
Health-ISAC™
Collaborating for Resilience in Healthcare

○○○ TLP:WHITE

Mar 23, 2023

Summary:

On March 23, 2023 it is being reported that multiple journalists are receiving fake USB drives in the mail accompanied by letters. The USB drives contained small capsules of plastic explosive. The explosives are set to detonate when plugged into a computer, using the computer as a power source to ignite them. One journalist fell victim to these drives, plugging in the USB resulting in an explosion. The device contained one centimeter of explosive, though only half of it detonated. It likely saved the journalist from harsher wounds than the mild injuries sustained to his hand and face.

Analysis:

Generally, USB attacks are meant to destroy information, not cause bodily harm. It is not uncommon for USBs to be sent to victims by cyber attackers with the intent to infect a computer, give a hacker remote access to a computer, or destroy a computer with an electrical charge. This particular instance was an attempt at causing physical harm to the individual who plugged in the device. The Ecuadorian government suspects that these drives were sent out as part of a terrorist attack on journalists by Cartel organizations, hoping to intimidate news agencies from reporting specific topics.

Currently, there is no known threat to the healthcare sector, but Health-ISAC is distributing this Threat Bulletin for your situational awareness. It is unclear whether other threat actors will begin copying this tactic and targeting critical infrastructure.

Mitigation:

While it is never safe to insert an unknown USB device, physical attacks have more severe consequences. Ensuring staff is knowledgeable about the risks of using unknown devices and the proper procedures when confronted with unknown devices can help to mitigate the potential risks.

- If a USB device is acquired from an unknown sender or found in a public place, it should be disposed of or reported to the appropriate authorities without being plugged in.
- Utilize hardware protections. Secure USB hubs or USB data blockers can help to prevent unauthorized access to devices or networks.
- Provide periodic training on the risks and proper channels to handle potential cyber threats including hardware risks.
- Ensure that policies exist to govern the use of USB devices and that protocols are in place for encryption, scanning, and safe disposal of unknown devices.

Knowing current risks are and ensuring that staff is aware of these risks can help to mitigate negative effects from these types of attacks. Understanding strategies used by nefarious actors and ensuring that organizational personnel are educated is the best method for protecting facilities, staff, and patients.

Sources:

Journalist plugs in unknown USB drive mailed to him—it exploded in his face

What Is a USB Drop Attack and How Can You Prevent It?

Ecuadorian TV presenter wounded by bomb disguised as USB stick

Bomb disguised as flash drive exploded when inserted

Reference(s)	Ars Technica, Boing Boing, The Guardian, MUO

Alert ID 73f05b22

View Alert

Tags Computer Attack, Physical Attack, Bomb, Journalist, Terrorism, USB, Attack

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Share Threat Intel

For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP “Share Threat Intel” Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Turn off Categories

For guidance on disabling this alert category, please visit the Knowledge Base article CSAP "Alert Categories" Toggle Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base

Knowledge Base

Check out our Knowledge Base for HITS integration documentation. https://health-isac.cyware.com/webapp/user/knowledge-base/f4b0c136/

Subscription Preferences Please click here to learn how to adjust your category subscription preferences. https://health-isac.cyware.com/webapp/user/knowledge-base/b919f599

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC’s Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.

Powered by Cyware