Incident Report: USB Parking 2024-09-30 #1   
Samic Hospital

Scenery

As a cybersecurity employee at Samic Hospital, I am informed that one of the security employees found a USB flash drive with the hospital logo printed on it on the parking lot floor. There is no one nearby who could have identified it as having thrown it away, so he decides to pick it up and reports it to the security guard.

The USB stick is taken to the IT office, where the team has virtualization software installed on a workstation. Virtualization software can be used for this very purpose because it is one of the only ways to safely investigate an unknown USB stick.

The software works by running a simulated instance of the computer on the same workstation.

This simulation is not connected to any other files or networks, so the USB drive cannot affect other systems if it turns out to be infected with malware.

Inspecting the contents of the USB flash drive

A virtual environment is created and the USB drive is connected to the workstation. The contents of the device appear to belong to Jorge Horrisberger, director of human resources at Samic Hospital.

Jorge's drive contains a mix of personal and work-related files. For example, it contains folders that appear to store family and pet photos. There is also a new hire letter and an employee shift schedule.

I reviewed the types of information that Jorge has stored on this device. Below, in the content row of the table, it describes the type of information that is stored on the USB drive.

Note: USB drives often contain a variety of personally identifiable information (PII). Attackers can easily use this sensitive information to target the data owner or others in their environment.

Applying the attack mentality to the contents of the USB drive

The flash drive appears to contain a mix of personal and work-related files.

Consideration was given to how an attacker could use this information if they obtained it, and whether the entire event was staged.

For example, an attacker could have placed these files on the USB drive as a distraction.

They could have targeted Jorge or someone he knows, hoping they would find the device and plug it into their workstation.

By doing so, the attacker could establish a backdoor into the company's systems while the unsuspecting target browsed through files.

The "Attacker Mindset" row of the table describes how this information could be used against Jorge or the hospital.

*Pro Tip:* The *Cybersecurity and Infrastructure Security Agency (CISA) offers some* [*safety tips on how to be careful with USB drives*](https://www.cisa.gov/news-events/news/using-caution-usb-drives) *, such as keeping personal drives separate from company drives.*

Risk analysis of finding a USB

Attackers sometimes perform USB lure attacks to deliver malicious code they have crafted.

However, this USB drive was still a security risk even if it did not contain malicious code. It could have been easily found by an attacker who could have used its contents to plan various attacks.

Some of the risks associated with USB lure attacks were considered:

What types of malware could be hiding on these devices? What could have happened if the device was infected and discovered by another employee?

What sensitive information could a threat actor find on such a device?

How could that information be used against an individual or organization?

The Risk Analysis row of the table describes the technical, operational, or management controls that could mitigate USB lure attacks.

USB Incident Analysis

| **USB Incident Analysis** | |
| --- | --- |
| **Content** | Are there files that may contain personally identifiable information? Are there sensitive work files? Is it safe to store personal files along with work files?  The contents of the USB drive contain files that appear to belong to a specific person.  Contains a mix of personal and hospital-related information.  Personal files and work files should not be stored in the same place.  Some documents appear to contain personal information that Jorge would not want made public.  Work files include personally identifiable information about other people.  In addition, work files contain information about hospital operations. |
| **Mindset**  **of the attacker** | Could the information be used against other employees? Could the information be used against family members? Could the information provide access to the company?  Any information an attacker obtains can be used against someone.  If there is information that helps the attacker, it is possible.  Timesheets can give an attacker information about other people Jorge works with.  Both personal and work information could be used to deceive Jorge.  For example, a malicious email may be designed to look like it comes from a coworker or family member. |
| **Risk analysis** | What types of malware could be hidden on these devices? What could have happened if the device had become infected and been discovered by another employee? What sensitive information could a threat actor find on a device like this? How could that information be used against a person or an organization?  Promoting employee awareness of these types of attacks and what to do when a suspicious USB drive is found is a management control that can reduce the risk of a negative incident.  Establishing routine antivirus scans is an operational control that can be implemented.  Another line of defense could be a technical control, such as disabling autoplay on company PCs that will prevent a computer from automatically running malicious code when a USB drive is connected. |