Digital Ghost Ships: A Threat to Global Security?

Sruthi Nair

Abstract: ***The Internet of Things (IoT) is characterized by an ever - expanding network of connected devices, actuators, and sensors that can interact with and collect data from their internal states and the external environment, using different protocols and standards. IoT allows physical objects, which were previously disconnected and without computing power, and people to interact remotely via the internet. Devices become smarter as they become more context - aware as a result of this characteristic. When an IoT device, or in fact any device connected to the internet has been abandoned, it becomes a digital ghost ship, much like the abandoned ships that float around in the vast ocean. When these online resources are abandoned they pose a major security threat. Security teams are concerned about the IoT explosion due to its fast production times and short life spans. Security updates may no longer be available for older devices. In addition, new devices pose a major risk due to zero - day exploits. Into this mix add all the forgotten resources including systems with default usernames and passwords. In the end, what we have is a cesspool of vulnerabilities that can attract sharks. This article talks about digital ghost ships in detail.***

Keywords: Cyber laws, Digital ghost ships, Internet of Things

1. Introduction

IoT devices are becoming increasingly common in our daily lives, from smart home devices to industrial sensors. These devices are designed to connect to the Internet and communicate with other devices or services to provide valuable data and functionality. However, as more devices are added to the network, it can become difficult to keep track of them all. In some cases, devices are forgotten or abandoned, but remain connected to the Internet. In the context of the Internet of Things, the term digital ghost ships refers to IoT devices that have been abandoned or forgotten, but remain connected to the Internet. These devices continue to send and receive data, but their owners have moved on to other devices or discontinued service. The term "ghost" is used because these devices are still active and connected to the network, but no one is actively monitoring or managing them.

These digital ghost devices can pose a security risk because they can potentially be exploited by attackers to gain access to the network or launch attacks. There are several reasons why IoT devices can be abandoned or forgotten. For example, the device may no longer be needed, the user may have switched to another device or service, or the device may have been lost or damaged.

2. Digital Ghost Ships

The first thing we need to understand is that the existence of digital ghost ships in the IoT is difficult to prove conclusively, as these devices are often abandoned or forgotten and not actively monitored. However, there are several signs that can indicate the presence of digital ghost ships in a network. To identify a digital ghost ship in the IoT, you need to look for devices that are connected to the network but not actively being used or monitored.

Here are some key indicators that can help identify a digital ghost ship:

- ***Unused IP addresses:*** If there are IP addresses assigned to devices that are not being used, this may indicate the presence of digital ghost ships.
- ***Lack of device activity:*** Devices that have not sent or received data for a long time may indicate that they are no longer in use.
- ***Outdated software or firmware:*** Devices running outdated software or firmware versions may be abandoned or forgotten.
- ***Unknown or unauthorized devices:*** If there are devices on the network that are not recognized or authorized, they may be digital ghost devices.
- ***No physical location or identification:*** If a device cannot be located or identified, it may be a digital ghost ship.

To identify digital ghost ships, organizations can conduct regular network scans and use network monitoring tools to identify and track device activity. It is also important to keep a clear inventory of all IoT devices connected to the network and remove any that are no longer needed or used.

There are many real - life examples of the existence of digital ghost ships. In 2016, the Mirai botnet was responsible for a massive DDoS attack targeting DNS provider Dyn. The attack caused major internet outages across the US. It later emerged that the botnet had been built using compromised IoT devices, including cameras, routers and digital video recorders. Many of these devices had been abandoned or forgotten by their owners, but were still connected to the Internet.

In 2018, researchers at F - Secure discovered a botnet called "Hide 'N Seek" that targeted IoT devices. The botnet was unique in that it used a peer - to - peer architecture that allowed compromised devices to communicate directly with each other instead of relying on a central command - and - control server. The researchers found that many of the compromised devices had been abandoned or forgotten, but were still connected to the Internet.

In 2019, security researchers discovered a vulnerability in a popular IoT device, the Sonos One speaker. The vulnerability allowed attackers to remotely take control of the device and play audio at full volume, potentially causing hearing damage. Many Sonos One devices were abandoned by their owners, but were still connected to the Internet and vulnerable to attacks.

It is difficult to predict how the threat of digital ghost ships will evolve due to a combination of factors including the introduction of new IoT devices, technological changes and the evolving security landscape. However, there are some possible directions in which this threat could evolve:

Increase in the number of devices: As the number of IoT devices continues to increase, the number of digital ghost ships could also increase. This could create a larger attack surface for cybercriminals.

More sophisticated attacks: As attackers become more familiar with IoT devices and their vulnerabilities, they could develop more sophisticated attacks that specifically target digital ghost ships. For example, they could use compromised devices to launch coordinated attacks against a specific target.

More attention to IoT security: As awareness of the risks associated with IoT devices increases, there could be more focus on improving IoT security. This could include the development of better security protocols and standards, more effective device management solutions, and stronger regulatory oversight.

Adoption of blockchain technology: Blockchain technology could be used to create a distributed ledger that records the activities of IoT devices. This could make it easier to identify and remove digital ghost ships from a network.

Now the evolution of the digital ghost ship threat will depend on a variety of factors. However, with a proactive approach to IoT security and device management, organizations can help minimize the risk of digital ghost ships and other potential security threats.

To prevent digital ghost ships, it is important to have a clear inventory of all IoT devices connected to the network. This can be done by regularly scanning the network for new devices and using network monitoring tools to track device activity. Any devices that are no longer needed or used should be removed from the network to prevent them from becoming a potential security risk.

It is also important to regularly update IoT devices with the latest security patches and firmware updates. This can help eliminate known vulnerabilities and prevent attackers from exploiting them. In addition, it is recommended to use strong passwords and other security measures to protect IoT devices from unauthorized access.

3. Conclusion

There are several cyber laws and regulations that address the security risks associated with IoT devices, including digital ghost ships. These laws are intended to protect the privacy and security of users' data and to ensure that IoT devices are used safely and responsibly.

One of the most notable laws in this area is the General Data Protection Regulation (GDPR) in the European Union. The GDPR requires companies to take appropriate measures to protect users' personal data, including data collected by IoT devices. Companies must also inform users about the data they collect and how it is used.

In the United States, the Federal Trade Commission (FTC) has issued guidelines for manufacturers and developers of IoT devices to ensure their products are secure and users' data is protected. The guidelines include recommendations for implementing security measures, ensuring transparency in data collection and use, and establishing effective device management procedures.

In addition, various countries around the world have enacted their own laws and regulations to address the security risks associated with IoT devices. In Japan, for example, the National Institute of Information and Communication Technology (NICT) has developed guidelines for IoT device security, while the Australian government has established a voluntary IoT Code of Practice to promote the safe design and development of IoT devices.

While there are no specific laws or regulations that specifically address digital ghost ships, there are numerous laws and regulations that aim to improve the security of IoT devices and protect user privacy.

References

[1] Setting out to sink the internet’s Digital Ghost Ships. DTU. (n. d.). https: //www.dtu. dk/english/newsarchive/2023/01/setting - out - to - sink - the - internets - digital - ghost - ships
[2] Shalhoub, Z. K. (2010). Cyber law and cyber security in developing and emerging economies. Edward Elgar.
[3] Cyber law, privacy, and security: Concepts, methodologies, tools, and applications. (2019). . IGI Global.
[4] GREENGARD, S. (2021). Internet of things. MIT PRESS.
[5] Waschke, M. (2017). Personal cybersecurity how to avoid and recover from cybercrime. Springer Verlag.