H-ISAC
HEALTH - ISAC

THREAT BULLETINS

Warshipping

TLP:WHITE

Jul 28, 2022

Warshipping Overview:

Physical and cybersecurity risks continue to rise amid Russia's invasion of Ukraine, COVID-19 mandates, and other forms of social discord. Warshipping is no exception. Warshipping is the process of utilizing a physical package delivery service to deliver an attack on a victim's computer network. For example, a miniature computer is sent through physical mail, where it will land at its designated target. Targets can vary, however, threat actors are more likely to target sectors with a plethora of data and critical infrastructure sectors such as healthcare, technology and telecoms, manufacturing, government facilities, and financial services. There are two main methods of a warshipping attack. The first is to ship a Raspberry Pi to an intended target, where it will sit in a mailroom, latching onto an organization's Wi-Fi moving laterally through networks. The second method is shipping a USB device rigged with malware to its designated target and physically inserting the USB drive into the organization's system.

Once the warshipping package is delivered to its intended target or inserted into an organization system, the device can sit for months unattended in unopened mail on desks and in mailrooms, gathering data and exploiting vulnerabilities in a company's network. Building and employing a warshipping device is easy and inexpensive, putting organizations at an elevated risk.

Technical Background:

Threat actors typically use a small device such as a Raspberry Pi rigged with a Wi-Fi card, cellular modem, GPS receiver, and battery. The Raspberry Pi is a low-cost, credit-card size computer that enables the user to control electronic components for physical computing and explore the Internet of Things (IoT). Raspberry Pi's are relatively easy to obtain and inexpensive. The threat actor must establish remote access, which involves locating the Raspberry Pi's location using its internet protocol (IP) address. Once the warshipping device is shipped, the modem will regularly transmit GPS coordinates to the threat actor's command and control server (C2). Once the device has reached its destination, the device will work in one of two ways:

- The device will imitate the existing
- Wi-Fi router, harvesting users' login credentials who attempt to connect to the rogue access point.
- The device will intercept packets,
- looking for a handshake (the connection between a device and the Wi-Fi access point). The encoded handshake can then be sent back to the command and control server to be reverse-engineered and used to gain access to the network.

Raspberry Pi's come with their own operating system (OS). The Raspberry Pi operates in the open-source ecosystem where it runs Linux (a variety of distributions). Its main supported operating system, Pi OS, is open-source and runs a suite of open-source software, making it relatively easy for anyone to operate a Raspberry Pi.

Threat Analysis/Impacting Health Care:

Warshipping can prove disastrous for many organizations, especially in the health care sector. As the device becomes connected to the victim's Wi-Fi, the threat actor can pivot to exploiting existing vulnerabilities to compromise various systems, create a persistent backdoor for future attacks, and establish a foothold in the network. The health care sector relies heavily on the efficiency and effectiveness of medical devices to ensure patient health. Threat actors engaging in warshipping can halt or disable medical devices by using various attack vectors, resulting in patient harm such as illness, injury, or death due to delayed treatment or other impacts on device availability and functionality. For example, modern ransomware poses a perilous risk for healthcare organizations. The warshipping attack vector exposes sensitive data, such as protected health information (PHI) and personal identifiable information (PII), stored on an organization's network. Modern ransomware often encrypts the victim's data before leaking the data onto the dark web, the worst possible outcome for sensitive patient records.

Warshipping is a fairly new attack vector capable of significantly damaging an organization's network and systems. If an organization's network and systems are breached, increased financial, operational, reputational, and legal risks will ensue. For more information on Warshipping, visit the links below under the **Sources** section.

Physical Security Considerations:

While this threat vector could pose a risk during normal periods of operation, the current state of office environments as a result of the COVID-19 pandemic has only increased the seriousness of it. Not only has COVID-19 forced changes in general operational procedures which could allow for security oversights that would not normally be missed, but increases in the number of employees working remotely also gives the potential for this attack method to be given the time to access sensitive systems. Reviewing and updating mailroom procedures will go a significant way to minimizing this risk. It is imperative that in addition to fortifying the mailroom, those employees who receive packages at home are briefed on the risks and understand preventative measures.

Mitigation Strategies:

Warshipping has the ability to easily bypass nearly all physical perimeter defenses. With no proven defense specifically geared toward warshipping, the threat poses a substantial risk to private and public entities. However, proper pre-emptive mitigation strategies can halt or slow down the warshipping process. Pre-emptive mitigation strategies are as follows:

- **Upgrade**
- **to secure WI-Fi access points**:
- Upgrading Wi-Fi access points to use Wi-Fi protected access (WPA) at a minimum or WPA2 (an upgraded version of the original standard) can make it difficult for criminals to intercept useful data from your company's Wi-Fi due to the use of encrypted traffic.
- **Implement**
- **advanced network security services**:
- Virus detection and real-time intrusion detection and prevention that will continuously scan for new threats.
- **Monitor**
- **for rogue Wi-Fi devices**:
- Constantly monitoring your company network for new and suspicious devices allows you to identify rogue access points.
- **Educating**
- **employees:** Upgraded Wi-Fi
- and patched software are not enough to stop warshipping. Educating employees about the dangers of connecting to lookalike Wi-Fi networks can spread awareness of the threat and stop potential warshipping attacks.

Mailroom Considerations to help reduce the risk of Warshipping:

- **Conduct**
- **diagnostic risk assessments that**
- **include**: current screening,
- handling, containment, sorting and final delivery procedures. Organizations may want to consider off-site screening depending upon the results.
- **Establish**
- **thresholds for visual screening and x-ray scanning. Potential red flags are as follows:**
    - Mail
    - from an unexpected sender
    - Distorted
    - handwriting on the package
    - Appearance
    - of handmade labels
    - Unknown/absent
    - return address
    - Excessive
    - postage
- **Review**
- **delivery notification systems:** employees
- should implement policies so packages do not stay unattended in offices for significant lengths of time before being fully opened.
- **Organizations**
- **restrict receiving personal packages:** consider
- a ban on employees receiving personal packages at the workplace, as was recommended in a 2019
- Warshipping Alert from
- the New Jersey Office of Homeland Security and Preparedness. If employees are allowed to ship personal packages, consider the heightened risk associated with popular shopping seasons, and implement either temporary pauses in the delivery of personal items,
- or temporary mailroom staff increases in order ensure mail processing can happen in a timely manner.
- **Employ**
- **professional security personnel in the mail facility**:
- ensure multiple points of entry are constantly being monitored by security personnel or surveillance systems.
- **Establish**
- **standard operating procedures (SOP):** develop

- a review process in order to adjust to a changing threat environment.

In 2012, DHS published Best Practices for Mail Screening and Handling Processes: A Guide for the Public and Private Sectors which was primarily developed with considerations towards Chemical, Biological, Radiological, Nuclear, or Explosive (CBRNE) threats and contains overviews of mail screening facilities which may be useful to members.

Reference(s)	Dark Reading, spiceworks, NJCCIC, CISA, quostar, quest-technology-group

Sources
Warshipping Structure Guide

What is Warshipping?

How Warshipping Works

Protecting Against “Phygital Attacks”

Alert ID aec910a2

View Alert

Tags Warshipping

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

Access the Health-ISAC Intelligence Portal Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

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**