Oct 30th, 2:00 PM - 2:30 PM

Warshipping: Hacking the Mailroom

Jackson Szwast
University of North Georgia, jmszwa9638@ung.edu

Bryson Payne
University of North Georgia, bryson.payne@ung.edu

Abstract

Everyone knows what package shipping is, but not everyone knows what warshipping is. Corporate mailrooms are rarely considered as part of the cybersecurity attack surface of most organizations, but they offer physical access to millions of uninspected packages daily. UPS shipped 5.5 billion items last year, with their daily average being 21.9 million items and operating through 1,800 locations in 2020. FedEx shipped 6.5 million packages daily and operates 2,150 locations. The United States Postal Service delivered 143 billion pieces of mail in 2019. Increasingly the world's consumers are relying on e-commerce, and during the recent COVID-19 pandemic, package deliveries reached record levels according to the US Government Accountability Office. E-commerce sales represented 14.5% of all retail sales in the United States with deliveries made via major carriers such as USPS, UPS, and FedEx, making the corporate mailroom an increasingly attractive and vulnerable surface of attack. The goal of this research is to demonstrate how warshipping attacks work by creating a low-cost physical device using readily available commodity parts, provide some background on warshipping, and provide guidance to organizations and individuals on how to defend against this type of cyber-physical attack.

Location

Online Zoom Session

Disciplines

Hardware Systems | Information Security | Management Information Systems | Technology and Innovation

Comments

Addressed reviewer's recommendations by adding two sections, one on Motivation to discuss how warshipping devices can obtain sensitive information and why cyber and physical security teams would benefit from considering warshipping and similar cyber-physical threats in their approach to their organization's security architecture. Also included competing technologies like drone surveillance/ intrusions, and refined the implications and limitations of this research as recommended by the review team.

EXTENDED ABSTRACT

Physical security is often overlooked in the cybersecurity architecture approaches of midsize and smaller organizations. And, cyber-physical intrusions like warshipping are novel enough that even larger, more mature organizations have not built their physical security with these kinds of attacks in mind. Warshipping is a type of cyberattack in which an attacker sends a device that is usually low-cost and low-power to a potential victim using a mail delivery carrier such as USPS, FedEx, or UPS. Furthermore, a small, war-shipped package like the one described and built in this research could easily be concealed in a promotional item or gift, from a stuffed animal to a smart speaker or desktop toy that might either be placed in the organization for ongoing surveillance or tossed in the trash, enabling easy recovery through dumpster-diving by the attacker.

Corporate mailrooms are rarely considered as part of the cybersecurity attack surface of most organizations, but they offer physical access to millions of uninspected packages daily. UPS shipped 5.5 billion items last year, with their daily average being 21.9 million items and operating through 1,800 locations in 2020. FedEx shipped 6.5 million packages daily and operates 2,150 locations. The United States Postal Service delivered 143 billion pieces of mail in 2019. Increasingly the world's consumers are relying on e-commerce, and during the recent COVID-19 pandemic, package deliveries reached record levels according to the US Government Accountability Office. E-commerce sales represented 14.5% of all retail sales in the United States with deliveries made via major carriers such as USPS, UPS, and FedEx, making the corporate mailroom an increasingly attractive and vulnerable surface of attack. The goal of this research is to demonstrate how warshipping attacks work by creating a low-cost (under $100 USD) physical device using readily available commodity parts, provide some background on warshipping, and provide guidance to organizations and individuals on how to defend against this type of cyber-physical attack.

Warshipping is a low-risk, low-cost, relatively low-tech means of cyber-physical surveillance and attack delivery, and we expect similar cyber-physical approaches to become more common. For this reason, organizational information security teams and cybersecurity researchers will benefit from thinking through their cyber and physical security architectures and mitigation systems to ensure that they account for warshipping, drones, and similar cyber-physical threats.