

 BRIEF

THREATS FROM RETAIL STORE-BASED INTRUSIONS ZEROFOX INTELLIGENCE

B-2022-10-12a

Classification: TLP:CLEAR

Criticality: Medium

Intelligence Requirements: Cyber Threats to Physical Locations

October 12, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 5:00 PM (EDT) on September 27, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Threats from Retail Store-based Intrusions

Executive Summary

External cyber intrusion targeting retail organizations poses a real and ongoing threat. However, threat actors entering physical locations of retail stores to conduct cyber intrusions also poses a very real and present danger. Threat actors are able to gain initial access to and attack companies after having a physical presence on site by way of card skimmers, unsecured Point-of-Sale (PoS) systems, unsecured or public Wi-Fi networks, USB drives and other physical hacking equipment, vulnerable Internet of Things (IoT) devices, social engineering, and insider threats. Retailers have had their customer data stolen, their networks degraded, and their infrastructure compromised via these threat vectors.

Details

There are several methods that threat actors can utilize in order to conduct cyber intrusions in physical locations. Card skimmers and unsecured PoS systems can be used to steal credit card information and clone smart cards. In addition, unsecured or public Wi-Fi networks can be exploited to infect connected devices with malware, provide backdoors to company systems, and eavesdrop on user activity. Furthermore, USB devices can be planted to install malware on store equipment, and keylogging devices, specialized equipment, and microcomputers can be utilized to capture passwords, access RAM, and provide access to network ports. Threat actors can also obtain default technical information or credentials from IoT devices and steal or hack vulnerable devices. Lastly, untrained employees, social engineering, and insider threats are additional vectors for cyber intrusion that can be exploited.

Types of Threats

Card Skimmers and Unsecured Point-of-Sale (PoS) Systems

There are various intrusion vectors that can be used by threat actors to gain access to and attack a company's systems after physically setting foot in the company's facilities.



Fake card readers known as “skimmers” can be physically placed in a store to skim or copy a card’s data. These are often used to steal credit card information; however, they can also be used for other smart cards, like ID cards. Skimmers can be attached to legitimate card readers in poorly-secured areas like ATMs or gas pumps. Skimmers are easy to install and rely on Bluetooth to transmit collected data. Once the device stores enough information, a threat actor can return to the location and download the data while in proximity to the device.¹

Smart cards can be cloned by writing the data to a blank card and creating a copy of an existing card. Moreover, smart cards that use radio frequency identification (RFID) technology do not require an attacker to be in physical contact to copy them. Small hardware allowing an attacker to automatically steal the data of any nearby RFID cards can be easily concealed; for example, an attacker can sit in front of a store with a backpack and steal the card data of an employee that sits next to them. Cloning a smart card can provide the attacker both physical and digital access to company resources to conduct cyberattacks.²

While usually perpetrated remotely, unsecured PoS devices can be infected with malware designed to steal payment card and financial data. Sophisticated malware is able to move laterally and infect a retailer’s IT network and critical databases.³

Unsecured or Public Wi-Fi Networks

Unsecured or public Wi-Fi networks can be accessed by attackers to infect connected users’ devices by installing malware. Rogue networks or rogue access points, which can be installed on a network’s wired infrastructure without the administrator’s knowledge, can be used as backdoors into a company’s systems. These pose as legitimate Wi-Fi networks to trick users into connecting to them, facilitating man-in-the-middle attacks. If facilities have an encryption-free connection, hackers can monitor all file sharing and traffic that is sent between a user and a server on a public Wi-Fi network. A well-positioned attacker can track the network users connected to the router of an unsecured network to inject malicious JavaScript into their devices. Public Wi-Fi networks can also allow for snooping when malicious software is installed to remotely monitor the activity on a third party’s laptop.⁴

Malicious USB Devices

Attackers can use USB drives in store locations to deliver and execute malware directly on company machines, whether manually or automatically, once such a drive is

¹

[hXXps://abc7news\[.\]com/credit-card-skimming-devices-bay-area-warning-7-eleven-chevron/12167064/](https://abc7news.com/credit-card-skimming-devices-bay-area-warning-7-eleven-chevron/12167064/)

² [hXXps://www.codecademy\[.\]com/article/physical-attacks](https://www.codecademy.com/article/physical-attacks)

³ [hXXps://colortokens\[.\]com/blog/cybersecurity-for-brick-and-mortar-retailers/](https://colortokens.com/blog/cybersecurity-for-brick-and-mortar-retailers/)

⁴ [hXXps://www.wgu\[.\]edu/blog/7-dangers-public-wifi-businesses2112\[.\]html](https://www.wgu.edu/blog/7-dangers-public-wifi-businesses2112[.]html)



connected to a target computer. There have been documented cases of malicious USB charging cables and charging stations as well. One incident involved a USB charging cable for an electronic cigarette that contained a small chip loaded with malware hidden inside the connector. When it was plugged into a computer, it attempted to install a malicious payload onto the device.⁵

Physical Hacking

By having a bodily presence in a retail store, an attacker is able to physically install a keylogging device to steal a device's password. Furthermore, they can externally access the RAM of a computer while it is running if they have specialized equipment. Hackers can also gain physical access to a network port by connecting a microcomputer to the network and then accessing cellular data. A microcomputer can act as a backdoor into the network, allowing the threat actor to target computers on that network without having to go through a firewall.⁶

Vulnerable IoT Devices

While vulnerable IoT devices can be exploited remotely, physical presence in facilities can enable attackers to intercept cellular connections or hack into IoT devices. Some IoT devices rely on cellular connections instead of Wi-Fi. For equipment costing USD 500-600, an attacker who is in the proximity of a call can set up a fake cell site and listen into the call, read text messages, or breach IoT devices.⁷

Hackers can physically open an IoT device to gain access to the inner components, ports, pins, and circuitry, allowing them to connect to the network. Criminals can steal these devices from retail stores or facilities and then hack them at a private location. A device's credentials and IP information are often placed inside its case or on the bottom of the device itself, making it easy to do. Additionally, conductors can carry data or analog signals inside IoT devices but are typically left unsecured. Attackers can probe these conductors through simple and readily-available testing instruments.⁸

Untrained Employees, Social Engineering, and Insider Threats

Threat actors can operate in physical locations to infiltrate company systems through the exploitation of inexperienced employees. Social engineering is commonly used to trick employees into divulging credentials, providing account information, or granting access to company resources. Actors can also work in collaboration with a company

⁵ [hXXps://www.codecademy\[.\]com/article/physical-attacks](https://www.codecademy.com/article/physical-attacks)

⁶ *Ibid.*

⁷

[hXXps://www.hologram.io/blog/4-ways-cyber-attackers-may-be-hacking-your-iot-devices-right-now](https://www.hologram.io/blog/4-ways-cyber-attackers-may-be-hacking-your-iot-devices-right-now)

⁸

[hXXps://www.techtarget\[.\]com/iotagenda/tip/Dont-forget-IoT-physical-security-when-planning-protection](https://www.techtarget.com/iotagenda/tip/Dont-forget-IoT-physical-security-when-planning-protection)



insider to obtain this information as a first step in conducting a larger-scale cyberattack.

Case Studies

San Francisco Area Skimmer Devices

Between July and August 2022, at least six law enforcement agencies across the San Francisco Bay Area issued warnings about skimmer devices. The Marin County Sheriff's Office confirmed it took a report about a device found at a Tamalpais Valley 7-Eleven. On July 15, a device was reported at a Sunnyvale Chevron 7-Eleven. Petaluma PD reported skimmers and small cameras found between a bank ATM and three 7-Eleven stores. Oakland PD also shared surveillance photos of a man planting a device in mid-July. In August, a skimmer found at a 7-Eleven was reported by Broadmoor Police near Daly City, and Morgan Hill PD was alerted to a skimming device and small camera above a bank ATM keypad.⁹

Akubra's Unsecured Wi-Fi Networks

Akubra, a Tasmanian retail and manufacturing company, noticed an increase in cybersecurity incidents involving unsecured Wi-Fi networks in its stores. Akubra was experiencing network interference and device connectivity issues as a result. After implementing secure Wi-Fi access points for physical stores, the company reduced the number of incidents. The Akubra case indicates the need for retailers to address cybersecurity measures due to the increasingly omnichannel nature of the retail sector.¹⁰

Costco Skimmer Devices

In November 2021, five card skimmers were found on payment card devices in four of Costco's Chicago-area warehouses. The skimmers had the ability to capture information on the magnetic stripe of a payment card, including name, card number, expiration date, and CVV. According to Costco, less than 500 customers were affected. During this time, customers reported fraudulent charges on their Costco credit cards or accounts.¹¹

Stuxnet Worm

While dated and unrelated to the retail sector, Stuxnet is an example of how actors were able to cause significant cyber and physical damage initiated by a physical

⁹

[hXXps://abc7news\[.\]com/credit-card-skimming-devices-bay-area-warning-7-eleven-chevron/12167064/](https://abc7news.com/credit-card-skimming-devices-bay-area-warning-7-eleven-chevron/12167064/)

¹⁰ [hXXps://www.watchguard\[.\]com/wgrd-resource-center/case-study/akubra](https://www.watchguard.com/wgrd-resource-center/case-study/akubra)

¹¹

[hXXps://www.zdnet\[.\]com/article/costco-says-card-skimmers-were-found-at-chicago-area-warehouses-less-than-500-people-affected/](https://www.zdnet.com/article/costco-says-card-skimmers-were-found-at-chicago-area-warehouses-less-than-500-people-affected/)



delivery. In June 2010, Stuxnet, a cyberweapon designed to target Iranian nuclear enrichment facilities, was delivered via malicious USB drives.¹² The worm eventually destroyed physical centrifuges used to refine uranium, demonstrating how cyber exploits can have a physical delivery—similar in general concept to how cyberattacks can be conducted by threat actors operating in physical retail stores.

Recommendations

- Install working surveillance cameras around retail stores.
- Consider using physical card skimmer detectors and applications.
- Protect PoS systems with efficient endpoint security.
- Implement secure Wi-Fi access points.
- Advise employees to turn off Wi-Fi auto-connect and Bluetooth discoverability settings.
- Educate employees about the dangers of using public Wi-Fi.
- Refrain from plugging unknown USB drives into company devices.
- Employ security guards in physical stores.
- Add basic security measures to store devices, like lockboxes or closing off unused ports.
- Require keys or access codes to physically access store devices.
- Use role-based access mechanisms similar to those used for software applications or services.
- Add a function to disable devices whenever they are tampered with, such as an electrostatic discharge or short circuit.
- Bury conductors inside the layers of a multilayer circuit board and only allow non-sensitive conductors to reach the board's top layers.
- Continually scan for and patch vulnerable IoT devices.
- Install detectors to identify stolen devices or equipment.
- Regularly conduct security awareness training.

¹² [hXXps://www.codecademy\[.\]com/article/physical-attacks](https://www.codecademy.com/article/physical-attacks)



Appendix: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.