ST. KITTS BRANCH
Financial Services Regulatory Commission

NewsLetter

October 2024
Issue No. 124

DIGITAL SKIMMING

What is Digital Skimming?

In cybersecurity, skimming refers to the act of illegally obtaining data from a payment card or financial device for fraudulent purposes. Cybercriminals employ various techniques to capture sensitive information including credit card numbers, Personal Identification Numbers (PINs), and other personal information, which can then be used to commit financial fraud. Skimming attacks can occur in both physical and digital forms, with criminals deploying sophisticated tactics to extract data without a victim's knowledge or consent.

Digital Skimming Broken Down

A major cybersecurity threat

Digital skimming is the action of stealing credit card information or other payment card data from customers of an online store. The transaction data is intercepted during the online purchase checkout process, without customers noticing anything unusual.

A crime known by many names

Digital skimming attacks are also known as web skimming, online card skimming, e-skimming, formjacking or **Magecart**.

Magento was the primary open source eCommerce platform initially targeted, inspiring the name '**Magecart**' (a combination of 'Magento' and 'shopping cart'), which also refers to the criminal group behind the attacks.

How Does Digital Skimming Work?

There are generally three (3) stages in a digital skimming attack:

Breach

Criminals get access to the source code/server of an online store or the source code of a third party tool. This can happen through vulnerabilities in the system, configuration errors or brute force.

Inject

Malware is inserted in the payment flow.

Collect

The customer and payment data are duplicated. Data can be collected immediately or hidden on the server and collected later to minimize the risk of discovery.

Affected customers are unaware that their card was copied (skimmed). From their perspective, the order was placed and the item will be received, leaving no room for suspecting something went wrong.

Types of Digital Skimming

- **Credit Card Skimming** - Involves the unauthorized capture of data directly from credit cards during point-of-sale transactions. Criminals often tamper with the card reader devices or use hidden cameras to record PIN entries. This stolen data can then be used to create cloned credit cards or make fraudulent purchases.
- **ATM Skimming** - Occurs when cybercriminals tamper with the card slot or PIN pad of an automated teller machine (ATM) to gather card information and PINs. Skimming devices installed on the ATM can read the magnetic stripe on the card or capture keystrokes, allowing criminals to gain access to a victim's bank account.
- **Data Skimming** - Also known as web skimming or form jacking, targets online payment platforms or e-commerce websites. Cybercriminals inject malicious codes into legitimate websites or create fake websites that mimic legitimate ones. When victims input their payment information, the skimming code captures the data and sends it to the attacker, enabling fraudulent activities.

Group-IB, a leading creator of cybersecurity technologies to investigate, prevent, and fight digital crime, announced that **it has contributed important data and intelligence to INTERPOL, as part of an ongoing initiative code named "Operation Contender 2.0"**. The international operation, led by INTERPOL, resulted in the arrest of two individuals by the Nigerian Police Force on 27 April 2024, who had orchestrated a romance scam that caused substantial financial losses for a victim in Finland.

How Can I Protect Myself or My Business?

One can make it harder for cybercriminals by:

- Using a malware monitor with web skimming-specific capabilities.
- Ensuring Multi-Factor Authentication and strong password policies are implemented for staff.
- Training staff to deal with phishing attacks.
- Running automated vulnerability audits on the e-commerce platform including the installation of third party components on a regular basis.
- Ensuring that only specific IPs can access the control panel of the computer system. Deny staff access from unknown locations.
- Ensuring timely installation of security patches and critical software updates.
- Implementing Content Security Policy (CSP) and Subresource Integrity (SRI). This will make it harder to inject malicious code into the computer system.

What Should Be Done If I Become a Victim?

- In the case of malware infection, change all administrative and database passwords immediately.
- Use a malware scanner to find any backdoors the attackers may have installed.
- Collect all available evidence and report the attack to the police.
- In the case of a personal data breach, comply with the applicable local data protection legislation.

References:

Drake, V. (2022, July 18). *What is E-Skimming? Detecting and Defending Against Digital Fraud.* https://flashpoint.io/blog/what-is-e-skimming/

Group-BI (2024, October 8). *Group-IB supports INTERPOL in "Operation Contender 2.0" leading to the arrest of cybercriminals behind a romance scam. https://www.group-ib.com/media-center/press-releases/operation-contender/*

South Independence Square Street, P.O. Box 898, Basseterre, St. Kitts
Tel: (869) 466-5048 | 467-1019/1591
Website: www.fsrc.kn / Email: info@fsrc.kn