OWN IT. SECURE IT. PROTECT IT.

OCTOBER 2019
National Cybersecurity Awareness Month
#BeCyberSmart

E-SKIMMING

Skimming Online Customer Payment Data From Website Checkout Forms

The Internet touches almost all aspects of our daily lives. We are able to shop, bank, connect with family and friends, and handle our medical records all online. These activities require you to provide personally identifiable information (PII) such as your name, date of birth, account numbers, passwords, and location information. #BeCyberSmart when sharing personal information online to reduce the risk of becoming a cybercrimes victim.

WHAT IS IT?

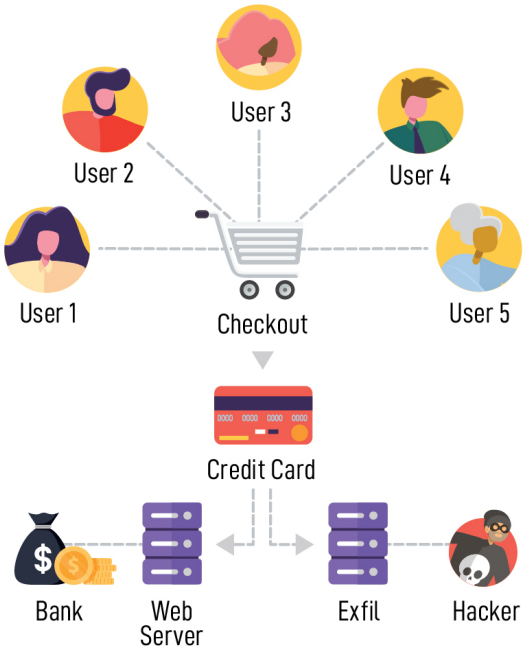
Cyber criminals introduce skimming code on e-commerce payment card processing web pages to capture credit card and personally identifiable information and send the stolen data to a domain under their control.

HOW DOES IT WORK?

Skimming code is introduced to payment card processing websites by:

- Exploiting a vulnerability in the website's e-commerce platform
- Gaining access to the victim's network through a phishing email or brute force of administrative credentials
- Compromising third-party entities and supply chains by hiding skimming code in the JavaScript loaded by the third-party service onto the victim website
- Cross site scripting which redirects customers to a malicious domain where malicious JavaScript code captures their information from the checkout page

The malicious code captures credit card data as the end user enters it in real time. The information is then sent to an Internet-connected server using a domain name controlled by the actor. Subsequently, the collected credit card information is either sold or used to make fraudulent purchases.



WHO IS BEING TARGETED?

Any business accepting online payments on their website is at risk of an e-Skimming attack. This threat has impacted e-commerce companies in the retail, entertainment, and travel industries as well as utility companies and third-party vendors. E-Skimming is also commonly targeting third-party vendors such as those who provide online advertisements and web analytics. The cyber criminals are evolving their tactics and have also been seen using malicious code that targets user and administrative credentials in addition to customer payment information.

OWN SECURE PROTECT IT. OCTOBER 2019 National Cybersecurity Awareness Month #BeCyberSmart

WHAT ARE THE WARNING SIGNS?

- Complaints of fraudulent activity on several customers' accounts after making a purchase from victim company.
- Identifying a new domain not known to be registered by victim company.
- JavaScript code has been edited.

HOW CAN YOU MINIMIZE RISK?

The FBI recommends taking precautionary measures to mitigate the threat of e-Skimming attacks. In an attempt to make attribution, the FBI determined the malicious skimmer code has varied in complexity, which limits the ability to identify a specific set of indicators of compromise. Vulnerable companies should secure websites to prevent malicious code injection. In addition, companies should implement proper network segmentation and segregation to limit network exposure and minimize lateral movement of cyber criminals.

- Perform regular updates to payment software.
- Install patches from payment platform vendors.
- Implement code integrity checks.
- Keep anti-virus software updated.
- Ensure you are PCI DSS compliant.
- Monitor and analyze web logs.
- Refer to your Incident Response Plan, if applicable.

WHAT CAN YOU DO IF YOU ARE A VICTIM?

- Identify source of skimming code to determine access point - network, third party, or other.
- Save a copy of skimming script or malicious loader domain to report to law enforcement.
- Change pertinent credentials.
- Refer to your Incident Response Plan, if applicable.
- File a detailed complaint at www.IC3.gov and review additional resources under the "Press Room" link.

For more information about connecting with confidence visit:
https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019