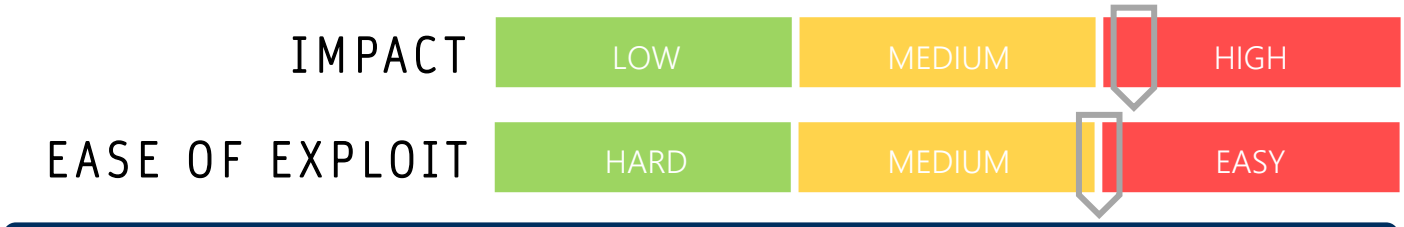
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00072

MAGECART WEBSITE CREDIT CARD SKIMMING

DATE ISSUED: 30th November 2020



OVERVIEW

Magecart is a term used to describe a number of different threat groups that operate in the same manner, by adding credit-card skimming scripts to legitimate websites in order to steal unsuspecting shoppers payment details and other personal information entered at checkout.

BREAKDOWN

An increasing number of websites have been attacked by various Magecart related groups and researchers are particularly worried by the recent uptick in such events as the holiday shopping season draws closer. In September, Magecart groups were seen to be exploiting the secure messaging service Telegram to siphon off and exfiltrate customer data. Most users are unaware the online credit card skimming is even possible so raising awareness may be a key method of avoiding becoming victim to such attacks. Attackers have also been known to create replica apps for download in app stores that offer incredible discounts in an effort to lure in victims to steal their money, payment details and personal information.

REMEDIATION STEPS

- Avoid entering payment details into websites, but rather use trusted payment platforms like PayPal
- Be vigilant of spoofed emails and domains and check for things like grammatical errors and slight differences in the URL layout in the browser address bar e.g. different suffixes or prefixes to normal
- Look for the padlock in the browser address bar when visiting any websites that ask for entry of personal information
- Ensure any app downloads are related to the legitimate retailers and be way of those that offer "too-good-to-be-true" discounts and other deals. Look for strong domain and app developer reputation.
- Use application penetration testing and web crawlers to search for rogue scripts on your e-commerce websites to protect your customers

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/threatlist-cyber-monday-looms-retail-threats/161563/
RiskIQ https://www.riskiq.com/what-is-magecart/