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

CYBER GUIDANCE ISSUE 00077

SOCIAL MEDIA BUTTONS HIDE MALWARE

DATE ISSUED: 7th December 2020

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

Attackers are using credit card skimming malware in a similar fashion to Magecart by adding buttons that appear to be legitimate social media buttons that appear to allow users to share their shopping experience on the associated platform, but in reality skim any details entered into the online shopping site.

BREAKDOWN

As holiday shopping ramps up, users are jumping online to make their gift purchases and attackers are seeking to take advantage of this. By gaining access to website code, attackers are installing buttons that appear to be legitimate social media buttons at the checkout stage of purchasing to harvest user details and payment information. To make these seem even more legitimate under inspection, the payloads, which contain a source code and decoder, are named after their corresponding platform; e.g. facebook_full, Instagram_full etc. As these files appear legitimate, they are managing to escape the notice of many malware monitoring and detection software and firewall protections. These buttons do not leave signatures on the web servers, circumventing security controls here as well so there are no red flags for administrators. User interaction is not necessary to activate the skimming code, as a decoder ring JavaScript activates the code transforming it from benign to malicious. A total of 37 online stores have thus far been detected as containing this malicious payload.

REMEDIATION STEPS

- Ensure that your sites checkout page does not consist of any third, fourth, or fifth-party plug-ins
- Do not add social media sharing features to your checkout processing pages
- Continually monitor your site for malicious activity and code injection using active script monitoring

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/online-shopping-malware-social-media-buttons/161903/
Bleeping Computer: https://www.bleepingcomputer.com/news/security/credit-card-stealing-malware-hides-in-social-media-sharing-icons/
Security Affairs: https://securityaffairs.co/wordpress/111872/malware/software-skimmer-social-share-icon.html