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

CYBER GUIDANCE ISSUE 00075

MAGECART IMPERSONATE PAYPAL

DATE ISSUED: 7th December 2020

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Magecart have come up with a new, creative credit card skimming attack just in time for the holiday shopping season. Using postMessage, attackers are hijacking PayPal transactions at checkout using convincing iframes and skimming credit card details for purchases

BREAKDOWN

This particular attack appears to have had a great deal of investment in ensuring the look and feel of these fake PayPal pages are convincing to users, unlike many other previously seen attacks. PostMessage circumvent the need for scripts to have access to the same protocols, port numbers and hosts to be able to access each other's pages and are being used to transmit payment information in a manner that is convincing to general users. Steganography is the art of hiding malicious scripts or links within a seemingly benign image and this technique is assisting Magecart to perform their attacks under images hosted on shopping sites. Once clicked and the script runs, the user is presented with a pre-filled fake PayPal form already containing some of the users input information and provide an accurate total taken from items in the shoppers cart, which heightens the likelihood of the user then entering their payment details. Once submitted, this data is then exfiltrated to the tawktalk.com domain and redirects the user back to the legitimate checkout page for transaction completion.

REMEDIATION STEPS

- Set up multifactor authentication and transaction alerts on your PayPal account
- Use a single credit card to process shopping purchases online and track transactions and spending frequently
- Check URLs for any suspicious looking changes or grammatical errors that differ from normal

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/magecart-hijacks-paypal-transactions/161697/
KimKomando: https://www.komando.com/security-privacy/magecart-paypal-scam/767790/