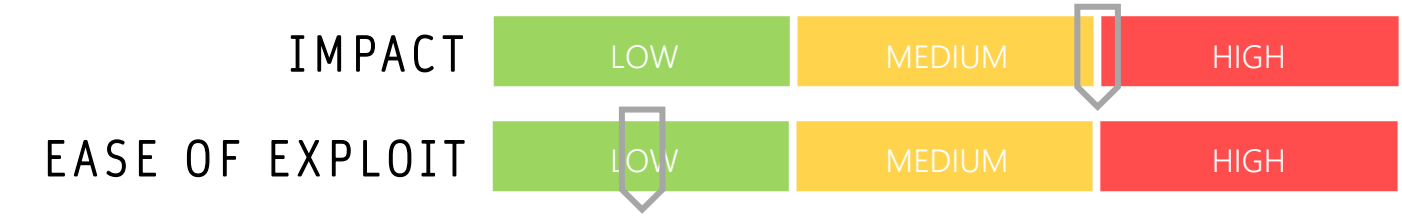
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0006

PHISHING TARGETS PANDEMIC & CURRENT EVENTS

DATE ISSUED: 25th June 2020



OVERVIEW

Targeting current global and political events such as the COVID-19 pandemic, Black Lives Matter and environmental activism has become prevalent in recent phishing campaigns.

BREAKDOWN

Targeting of the health and finance sectors in relation to the impact of the COVID-19 global pandemic offering financial support, information on health care or certification and training for preparedness in dealing with the illness and returning to work have heavily featured in recent phishing campaigns. Using novel training sites and cloned web pages as a base, users are redirected to malicious sign up/in pages to harvest credentials. Surveys and requests for donation to support activists in their chosen cause have resulted in credit card skimming installation of malware including the Trickbot Trojan through illegitimate Office365 updates, which corresponded to downloadable .doc files. Trickbot may be used in modular form to carry out any number of infiltration, exfiltration and encryption tasks, altering itself to evade any detection.

REMEDIATION STEPS

- Ensure security updates and patching is up to date on all devices
- Ensure web application firewalls are updated and configured correctly
- Ensure your organization has up to date Endpoint and Network Protection in place on all devices
- Restrict user ability to download and install updates
- Provide information and training to all employees regarding social engineering and phishing, how to spot an attack and what to do if an attack is suspected.

REFERENCES & RESOURCES

Threatpost: https://threatpost.com/office-365-users-targeted-by-coronavirus-employee-training-phish/156899/
https://threatpost.com/trickbot-attack-covid-19docusign-themed-malw/155391/
MetaCompliance: https://www.metacompliance.com/blog/black-lives-matter-phishing-scam-distributes-malware/
CERT NZ: https://www.cert.govt.nz/individuals/alerts/attackers-using-covid-19-themed-scams-updated-alert/