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

CYBER GUIDANCE ISSUE 00122

BUSINESS SOCIAL MEDIA ACCOUNTS TARGETED

DATE ISSUED: 22nd March 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A password and cookie stealer known as CopperStealer has been flying under the radar and discovered to have been compromising accounts on platforms such as Facebook, Apple, Amazon and Google since 2019.

BREAKDOWN

With similar behaviour to other well-known social media targeting malware SilentFade, StressPaint, FacebookRobot and Scranos; CopperStealer is able to both harvest credentials and cookies and deliver additional malware to victims. Additional versions have been identified to target the platforms listed above as well as Bing, PayPal, Tumblr and Twitter and have been delivered via multiple suspicious websites offering key generation and cracking capabilities to circumvent licensing restrictions or gain software for free. A number of service providers including the likes of Cloudflare have teamed up with the platforms to capture and analyse the malware and capture information on those attempting to visit the sites. After installation, CopperStealer downloads a config file from the command and control (C2) server, extracts a legitimate looking download manager and uses the incorporated exposed API to download follow up binary, other config files and malware or backdoors (such as Smokeloader). As this is an evolving threat, researchers will continue to monitor these types of activities for further insights.

REMEDIATION STEPS

- Use URL filtering to block known harmful or malicious websites.
- Disable user ability to download applications and run executable files on their machines.
- Ensure you have a robust acceptable use and technology standards policy in place to guide user on their behaviour and interactions.

REFERENCES & RESOURCES

Proof Point https://www.proofpoint.com/us/blog/threat-insight/now-you-see-it-now-you-dont-copperstealer-performs-widespread-theft

Threatpost https://threatpost.com/copperstealer-hijacks-accounts/164919/