UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

# CYBER GUIDANCE ISSUE 00174

## MOSAICLOADER ZERO-DAY WINDOWS MALWARE

DATE ISSUED: 26th July 2021

| | | | |
|---|---|---|---|
| IMPACT | LOW | MEDIUM | [✓ HIGH] |
| EASE OF EXPLOIT | HARD | MEDIUM | [✓ EASY] |

## OVERVIEW

The new full-service malware delivery platform is spreading rapidly worldwide and is being used to infect target machines with Remote-Access Trojan's (RATs) used to steak Facebook cookies, steal passwords, install cryptominers, and much more using paid advertisements to ensnare victims.

## BREAKDOWN

Disguising itself as a cracked software installer and targeting victims searching for pirated software and games in paid advertisements, this never-before-seen malware sprayer downloading a list of URLs from its Command and Control (C2) server and can install any payload onto an infected system. Researchers have noted the use of Facebook cookie stealers to facilitate credential theft and account takeover to create new posts and spread further malware. It has also been seen to distribute the Glupteba backdoor and a number of RATs that log keystrokes, record audio or on the system's microphone and cameras, capture screenshots and deploy cryptominers. Using obfuscation techniques including establishing complex chains of processes and rearranging code blocks earned it the "mosaic" namesake.

## REMEDIATION STEPS

- Remove user's ability to search for and connect to sites/URLs that are associated with pirated software, games, and other media. Educate users on the dangers and legal implications of such activities.
- Remove user's ability to download unauthorised software and run executables.
- Run Next Generation Anti-Virus (NGAV) on endpoints to detect and isolate malicious behaviours and unauthorised downloads.

## REFERENCES & RESOURCES

| | |
|---|---|
| Threatpost | https://threatpost.com/mosaicloader-malware-facebook-stealers/167939/ |
| ZDNet | https://www.zdnet.com/article/this-password-stealing-windows-malware-is-distributed-via-ads-in-search-results |