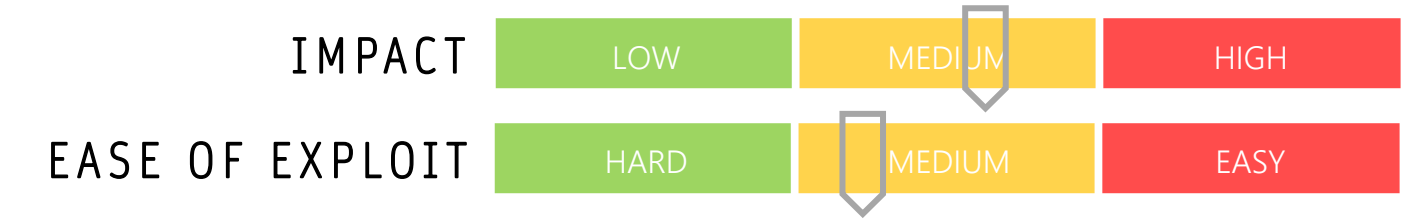
UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

# CYBER GUIDANCE ISSUE 00109

## NEW VERSION OF MASSLOGGER TROJAN

**DATE ISSUED:** 22nd February 2021




## OVERVIEW

With its sights set on Windows machines, a new version of Masslogger – a spyware trojan compiled in HTML(CHM) embedded with malicious JavaScript has set out to steal victims' credentials from Microsoft Outlook, Google Chrome, and a number of instant-messenger (IM) platforms.

## BREAKDOWN

The new strain was released in April 2019 and has been widely available for sale on underground forums. Disguising itself using HTML in an effort to avoid detection of the commonly block RAR extension, it has been initially dispensed through email. Most defensive programs and organisations do not consider CHM files to be an executable file so will manage to slip past email filters. This is also the same format used by Windows help documentation. The .NET malware steals browser, email and IM credentials and can be used as a keylogger which then exfiltrates the data to an external domain. A recent campaign has been seen in Italy, Latvia and Turkey, and other parts of Europe targeting businesses with legitimate looking content relating to their victim's business or employer.

## REMEDIATION STEPS

- Use email filtering and sandboxing for HTML (CHM) file types sent from unknown senders to discover malicious content.
- Educate users on the dangers of social engineering and email phishing attacks and what to do when they suspect and email or other communication.
- Use whitelisting or blacklisting to specify known legitimate senders and block known harmful senders.

## REFERENCES & RESOURCES

Threatpost https://threatpost.com/masslogger-microsoft-outlook-google-chrome/164011/
The Hacker News https://thehackernews.com/2021/02/masslogger-trojan-upgraded-to-steal-all.html
ZDNet https://www.zdnet.com/article/masslogger-trojan-reinvented-to-steal-outlook-chrome-credentials/
Tom's Guide https://www.tomsguide.com/news/masslogger-password-stealer