Westview

News > General > Beware the Masslogger Trojan!

Beware the Masslogger Trojan!

2021-02-22 - Don Guilbeault - Comments (0) - General

Cisco researchers warn of a powerful Windows malware which is aimed to steal your passwords. The malware is called Masslogger which is a trojan horse that arrives as an email attachment. It tries to steal usernames and passwords from Microsoft Outlook, Thunderbird email client, NordVPN, Discord and other email / Chat services as well as built in password managers of Google Chrome, Mozilla Firefox, Microsoft Edge and other browsers. The malware tries to evade detection by being mostly “Fileless,” or existing almost completely in memory.

The malware arrives in a compressed (ZIP) email attachment, if extracted the file unfolds into an HTML file, which contains a script that starts a chain of events resulting in malware that only exists in memory working to steal your passwords, the only trace of that malware is the original attachment that has been known to fool even the best antivirus programs.

Your best defense is exercising extreme caution when opening attachments, especially compressed (ZIP) file attachments from unsolicited emails and unknown sources. You the user are always the first line of defense to stop unwanted access to passwords and systems.

Regards,

Don Guilbeault
IT Analyst
Westview Co-operative Association Limited

P. 403.556.3335 Option 2 Option 0 | C. 403-899-9752 | F. 403.507.2405
P.O. Box 3970, Olds AB. T4H 1P6, Canada
don.guilbeault@westviewcoop.ca | www.westviewco-op.crs