Masslogger trojan

Article URL
malware.php?mal_id=105116029960535182a69755.15584662

Author
SecurityHome.eu

Published: 18 March 2021

Aliases :

There are no other names known for **Masslogger trojan**

.

Explanation :

Masslogger is a spyware program, which is written in .NET and steals browser, email and instant-messaging credentials. The trojan was released in April 2020 and has since been sold on underground forums.

Researchers uncovered the campaign targeting users in Italy, Latvia and Turkey starting in mid-January. When the Masslogger variant launched its infection chain, it disguised its malicious RAR files as Compiled HTML (CHM) files. This is a new move for Masslogger, and helps the malware sidestep potential defensive programs, which would otherwise block the email attachment based on its RAR file extension, said researchers on Wednesday.

The use of compiled HTML (usually used for Windows help files) can be advantageous for the attacker since the initial infection vector is email, Many organizations will not consider CHM files to be executables so it is more likely they will evade content filters filtering incoming email messages based on the attachment name or type.

The Masslogger payload contains the functionality to target and steal credentials from the following applications: Pidgin (a free and open-source multi-platform instant messenger client), the FileZilla File Transfer Protocol (FTP) client, the Discord group-chatting platform, NordVPN, Outlook, FoxMail, Firefox, Thunderbird, QQ Browser and Chromium-based browsers (Chrome, Chromium, Edge, Opera and Brave).

Last update 18 March 2021