TRUSTWAVE CORPORATION

12/21/2022 | News release | Distributed by Public on 12/21/2022 08:24

Malicious Macros Adapt To Use Microsoft Publisher To Push Ekipa RAT

After Microsoft announced this year that macros from the Internet will be blocked by default in Office**[1]**, many threat actors have switched to different file types such as Windows Shortcut (LNK), ISO or ZIP files, to distribute their malware. Nevertheless, Office documents are still actively leveraged in many campaigns and pose a large risk to organizations, especially with threat actors continuously finding new ways to avoid detection.

The Trustwave SpiderLabs' Research Team has analyzed samples of an Ekipa Remote Access Trojan (RAT) in the wild, and found interesting techniques for the use of malicious Office documents. As shown in this research, the Ekipa RAT was added to a sophisticated threat actors' cyber arsenal and used in the Russian - Ukraine war.

OVERVIEW OF FUNCTIONALITIES

Ekipa is a Remote Access Trojan used for targeted attacks and can be purchased on underground forums, as **CloudSEK** found in its research. The current price is set at $3,900, which is very high. The trojan leverages MS Office and Visual Basic for Applications as its main infection and operations vector. It

Related Announcemen

News

UNITED STATES BANKRUPTCY COUR

24 20521 In re: Samuel Laurion and Heather Re

CITY OF TULSA, OK

City Encourages Sustain Halloween Practices

CORNELL UNIVERSI

Potential drugs for canc may help tackle tubercu

Science and Techno

NIAGARA UNIVERSIT

Niagara University Stude at Math Conference

CTS CORPORATION

Quarterly Report for Qu September 30, 2024 (Fo