Public.

United States

NEWS
POLITICS AND POLICY
BUSINESS AND ECONOMY
ARTS AND CULTURE
LIFESTYLE AND LEISURE
SPORTS

Search Companies, Topics, Organizations, Governments...

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 also comes with a control panel and builders for:

MS Word Macros

XLL Excel add-ins

MS Publisher Macros

A Remote Access Trojan is capable of:

Collecting information about a targeted system (basic system information, installed AV products, GPU and CPU information and more)

Browsing and downloading of files on attached drives

Dropping files

Executing files and commands.

When used with malicious Word documents, the trojan's main functions are implemented in a one-time VBA macro template. When the document is reopened, the server rejects the request to download the macro template and all subsequent requests for installation actions.

[Link]

Figure 1: Ekipa RAT advertisement on the XSS forum

[Link]

Figure 2: EkipaRAT is continuously updated with new features as seen in presented screenshot from the XSS forum.

ANALYSIS OF MICROSOFT WORD DOCUMENTS WITH REMOTE TEMPLATE

There are multiple documents related to Ekipa RAT on popular malware analysis

Related Announcements

News

UNITED STATES BANKRUPTCY COURT FOR[...]
24 20521 In re: Samuel Aaron Laurion and Heather Renee Laurion

CITY OF TULSA, OK
City Encourages Sustainable Halloween Practices

CORNELL UNIVERSITY
Potential drugs for cancer treatment may help tackle tuberculosis

more

Science and Technology

NIAGARA UNIVERSITY
Niagara University Student Presents at Math Conference

CTS CORPORATION
Quarterly Report for Quarter Ending September 30, 2024 (Form 10-Q)

DASNY - DORMITORY AUTHORITY OF THE[...]
DASNY President Robert J. Rodriguez joins Medgar Evers

more