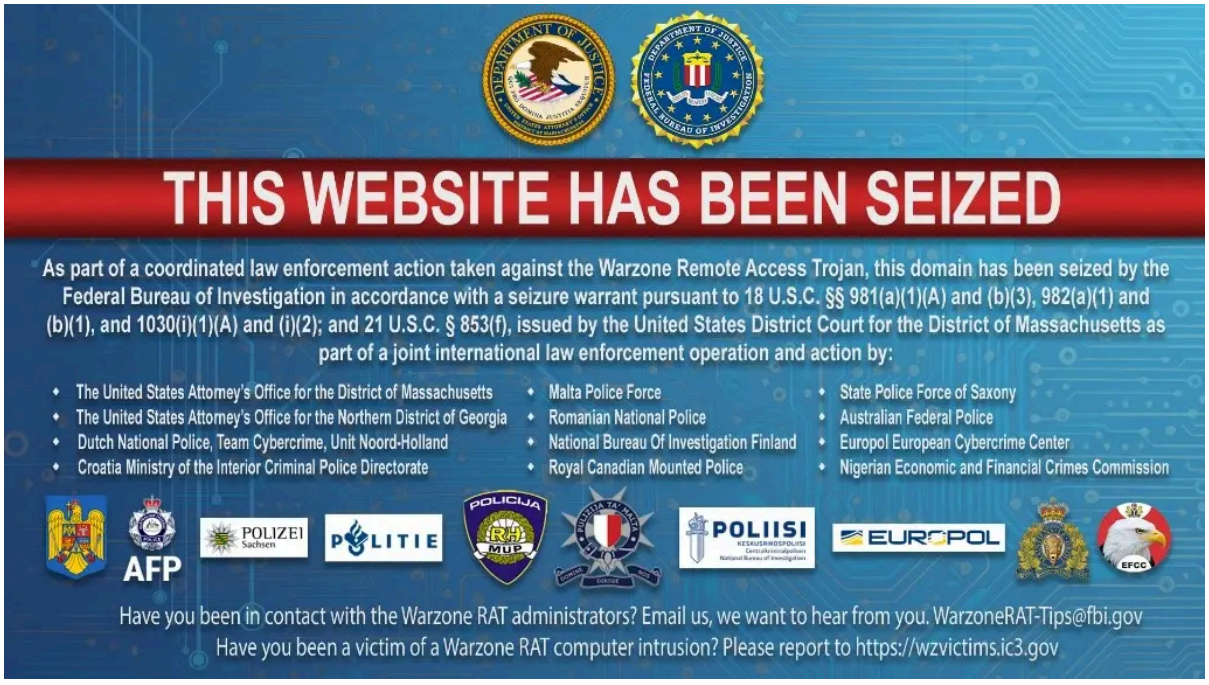
International cybercrime malware service targeting thousands of unsuspecting consumers dismantled

By Europol

Published: 2024-02-12 · Archived: 2026-04-05 19:40:00 UTC

An international operation has resulted in the seizure of several internet domains that were used by cybercriminals to sell malware. Through use of this malware, cybercriminals could secretly access and connect to victims' computers for malicious purposes. The operation was led by the FBI and supported by Europol and the Joint Cybercrime Action Taskforce (J-CAT).

- 

On 7 February, two suspects were arrested in Malta and Nigeria in the framework of the operation. The suspects are accused of selling the malware and supporting cybercriminals who used the malware for malicious purposes. Europol provided analytical support to the investigation which led to the operation involving Australia, Canada, Croatia, Finland, Germany, Malta, the Netherlands, Nigeria, Romania and the United States. These countries provided valuable assistance securing the servers hosting the Warzone RAT infrastructure.

The Warzone RAT malware, a sophisticated Remote Access Trojan (RAT), was on sale via internet domains. The RAT malware enabled cybercriminals to browse victims' file systems, take screenshots, record keystrokes, steal victims' usernames and passwords, and watch victims through their web cameras, all without the victims' knowledge or permission.

Avoid RAT-ing

The public and businesses can follow simple steps to help protect themselves from malware:

- Update your software, including anti-virus software;
- Install a good firewall;
- Don’t open suspicious email attachments or URLs – even if they come from people on your contact list;
- Create strong passwords.

Find out how to protect yourself against Remote Access Trojans.

Source: https://www.europol.europa.eu/media-press/newsroom/news/international-cybercrime-malware-service-targeting-thousands-of-unsuspecting-consumers-dismantled