FBI seizes Warzone RAT infrastructure, arrests malware vendor

bleepingcomputer.com/news/security/fbi-seizes-warzone-rat-infrastructure-arrests-malware-vendor/

Bill Toulas

By
Bill Toulas

- February 12, 2024
- 06:09 PM
- 1

The FBI dismantled the Warzone RAT malware operation, seizing infrastructure and arresting two individuals associated with the cybercrime operation.

Daniel Meli, 27, a resident of Malta, was arrested last week for his role in the proliferation of Warzone RAT (aka 'AveMaria'), a remote access trojan with a long history of use in cybercrime.

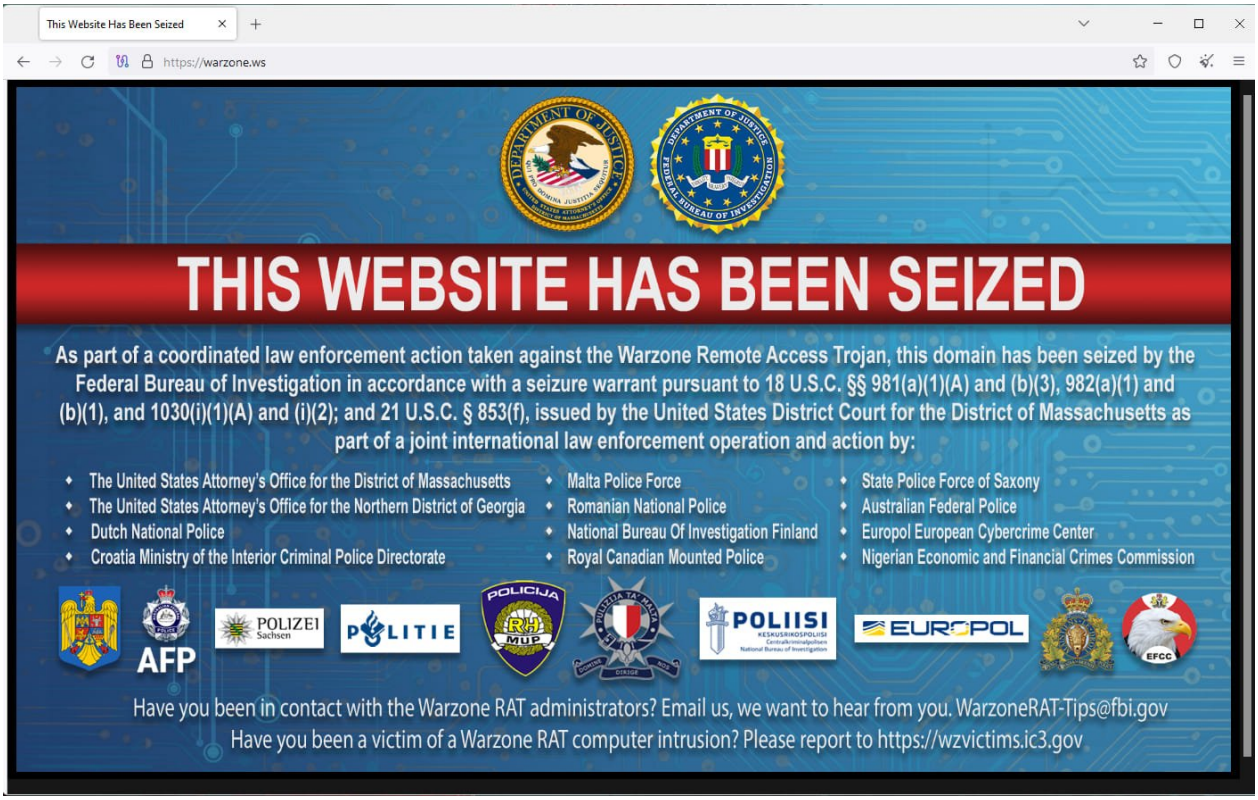
Warzone RAT is commodity malware created in 2018 that offers numerous features to aid cybercrime, including UAC bypass, hidden remote desktop, cookie and password stealing, keylogging, webcam recording, file operations, reverse proxy, remote shell, and process management.

The Malta police arrested Meli at the request of the U.S. law enforcement authorities, who issued an indictment against him on December 12, 2023.

The accusations concern offenses of unauthorized damage to protected computers, illegally selling and advertising an electronic interception device, and participating in a conspiracy to commit several computer intrusion offenses.

Meli was arrested on February 7, 2024, during a coordinated operation carried out by the Malta Police Force, the Office of the Attorney General of Malta, and supported by the U.S. Department of Justice (DoJ) and the FBI.

At the same time, Federal authorities in Boston seized four domains connected to Warzone RAT, including "warzone.ws," which was the malware's primary website.



Seizure notice *(BleepingComputer)*

A second indictment issued by a federal grand jury in the District of Massachusetts on January 30, 2024, targets Prince Onyeoziri Odinakachi, 31, of Nigeria, who is accused of providing customer support to cybercriminals buying access to Warzone RAT.

Odinakachi was arrested in Nigeria on February 7, simultaneously with Meli's arrest and the takedown of the malware's selling domains.

Apart from the arrests and seizure of the sites, the international law enforcement effort led by the FBI also resulted in identifying and confiscating server infrastructure linked to the malware, including in Canada, Croatia, Finland, Germany, the Netherlands, and Romania.

The U.S. DoJ announcement mainly implicates Meli in the distribution and customer support for the malware, so it is unclear if he is the original author or creator of the Warzone RAT, in which case, he would have developed it at the age of 21.

The announcement says that the man engaged as a seller in the space since at least 2012, when at the age of 15, selling hacking ebooks and the Pegasus RAT for the account of a criminal ring known as 'Skynet-Corporation.'

Meli faces a total of 15 years in prison with three years of supervised release and fines of $500,000 or twice the gross gain or loss (whichever is greater) for the charges against him.

The Northern District of Georgia is seeking the extradition of Daniel Meli from Malta to the United States, where he will stand trial.

Related Articles:

New Bifrost malware for Linux mimics VMware domain for evasion

Hacker arrested for selling bank accounts of US, Canadian users

Police disrupt Grandoreiro banking malware operation, make arrests

U.S. charges Iranian for hacks on defense orgs, offers $10M for info

Hackers used new Windows Defender zero-day to drop DarkMe malware