International Cybercrime Malware Service Dismantled by Federal Authorities: Key Malware Sales and Support Actors in Malta and Nigeria Charged in Federal Indictments

justice.gov/opa/pr/international-cybercrime-malware-service-dismantled-federal-authorities-key-malware-sales

February 9, 2024

Press Release

RAT Malware Allowed Cybercriminals to Surreptitiously Connect to Victims' Computers to Steal Data and Engage in Other Malicious Activities Without Victims' Knowledge

The Justice Department announced today that, as part of an international law enforcement effort, federal authorities in Boston seized internet domains that were used to sell computer malware used by cybercriminals to secretly access and steal data from victims' computers. Federal authorities in Atlanta and Boston also unsealed indictments charging individuals in Malta and Nigeria, respectively, for their alleged involvement in selling the malware and supporting cybercriminals seeking to use the malware for malicious purposes.

Federal authorities in Boston seized www.warzone.ws and three related domains, which together offered for sale the Warzone RAT malware — a sophisticated remote access trojan (RAT) capable of enabling cybercriminals to surreptitiously connect to victims' computers for malicious purposes. According to court documents authorizing the seizures, the Warzone RAT provided cybercriminals the ability to browse victim file systems, take screenshots, record keystrokes, steal victim usernames and passwords, and watch victims through their web cameras, all without the victims' knowledge or permission.

Investigations by the FBI Boston and Atlanta Field Offices also led to two indictments against individuals involved in selling and supporting the Warzone RAT and other malware.

Daniel Meli, 27, of Zabbar, Malta, was arrested on Feb. 7 at the request of the United States, following a coordinated operation by the Malta Police Force and the Office of the Attorney General of Malta, with the support of the FBI and Justice Department. Meli made his initial appearance before a Magistrate Judge in Valletta, Malta. Meli was indicted by a federal grand jury in the Northern District of Georgia on Dec. 12, 2023, for four offenses, including causing unauthorized damage to protected computers, illegally selling and advertising an electronic interception device, and participating in a conspiracy to commit several computer intrusion offenses. According to charging documents, since at least 2012, Meli offered malware products and services for sale to cybercriminals through online computer-hacking forums. Specifically, Meli allegedly assisted cybercriminals seeking to use RATs for malicious purposes and offered teaching tools for sale, including an eBook. Meli also allegedly sold

both the Warzone RAT and, before that, malware known as the Pegasus RAT, which he sold through an online criminal organization called Skynet-Corporation. He also provided online customer support to purchasers of both RATs. The Northern District of Georgia is seeking Meli's extradition to the United States.

Separately, Prince Onyeoziri Odinakachi, 31, of Nigeria, was indicted by a federal grand jury in the District of Massachusetts on Jan. 30 for conspiracy to commit multiple computer intrusion offenses, including obtaining authorized access to protected computers to obtain information and causing unauthorized damage to protected computers. According to charging documents, between June 2019 and no earlier than March 2023, Odinakachi provided online customer support to individuals who purchased and used the Warzone RAT malware. Law enforcement officers of the Port Harcourt Zonal Command of Nigeria's Economic and Financial Crimes Commission arrested Odinakachi on Feb. 7.

The disruption of the Warzone RAT infrastructure was the result of an international law enforcement effort led by FBI special agents in Boston and Atlanta and coordinated with international partners in large part through Europol. According to court documents, in addition to discovering instances of the Warzone RAT being used to attack victim computers in Massachusetts, the FBI covertly purchased and analyzed the Warzone RAT malware, confirming its multiple malicious functions. Separately, law enforcement partners in Canada, Croatia, Finland, Germany, the Netherlands, and Romania provided valuable assistance securing the servers hosting the Warzone RAT infrastructure.

"Today's actions targeting the Warzone RAT infrastructure and personnel are another example of our tenacious and unwavering commitment to dismantling the malware tools used by cybercriminals," said Acting U.S. Attorney Joshua S. Levy for the District of Massachusetts. "We will turn over every stone to prevent cybercriminals from attacking the integrity of our computer networks, and we will root out those who support such cybercriminals so they will be held accountable. Those who sell malware and support cybercriminals using it should know that they cannot hide behind their keyboards or international borders."

"Daniel Meli will no longer escape accountability for his actions selling malware," said U.S. Attorney Ryan K. Buchanan for the Northern District of Georgia. "This alleged cybercriminal facilitated the takeover and infection of computers worldwide. Our office was proud to partner with our federal and international counterparts to find Meli and bring him to justice. We will continue to diligently investigate and prosecute cybercrime in the Northern District of Georgia, and in all parts of the globe where our district is impacted."

"This action highlights the FBI's commitment to disrupting cybercriminal actors and taking down their infrastructure," said Assistant Director Brian Vorndran of the FBI's Cyber Division. "The FBI is proud of the international coordination involved in this law enforcement effort,

and we will continue to build global partnerships to go after cybercriminals who seek to harm the American people."

The charges of conspiracy, obtaining authorized access to protected computers to obtain information, illegally selling an interception device, and illegally advertising an interception device each provide for a sentence of up to five years in prison, three years of supervised release and a fine of $250,000, or twice the gross gain or loss, whichever is greater. The charge of causing unauthorized damage to protected computers provides for a sentence of up to 10 years in prison, three years of supervised release, and a fine of $250,000, or twice the gross gain or loss, whichever is greater.

Assistant U.S. Attorneys James R. Drabick and Carol E. Head for the District of Massachusetts obtained the seizure warrants, and Drabick is prosecuting Odinakachi. Assistant U.S. Attorneys Bethany L. Rupert and Michael Herskowitz for the Northern District of Georgia are prosecuting Meli.

The Justice Department's Office of International Affairs provided substantial assistance during the investigation. Federal authorities also wish to acknowledge the cooperation and assistance of the FBI Boston and Atlanta Field Offices; Malta Police Force; Office of the Attorney General of Malta; Malta Ministry for Justice; Australian Federal Police; Croatian Ministry of the Interior Criminal Police Directorate; Dutch National Police; Europol European Cybercrime Center; Finland's National Bureau of Investigation; State Police Force of Saxony, Germany; Japan Ministry of Justice; Port Harcourt Zonal Command of Nigeria's Economic and Financial Crimes Commission (EFCC); Romanian National Police; and Royal Canadian Mounted Police for their valuable assistance.

Anyone who is a victim of a Warzone RAT computer intrusion is urged to report it to the FBI at https://wzvictims.ic3.gov.

An indictment is merely an allegation. All defendants are presumed innocent until proven guilty beyond a reasonable doubt in a court of law.

Warzone RAT splash page.

Updated February 12, 2024

Topic

Cybercrime

Press Release Number: 24-163