FBI and international cops catch a NetWire RAT

theregister.com/2023/03/10/fbi_netwire_seizure/

Jessica Lyons Hardcastle

International law enforcement agencies have claimed another victory over cyber criminals, after seizing the website, and taking down the infrastructure operated by crims linked to the NetWire remote access trojan (RAT).

Police in Croatia on Tuesday arrested a suspect who allegedly administered the worldwiredlabs website, which has sold the NetWire malware for several years. On the same day, a US judge approved a seizure warrant that allowed federal authorities in Los Angeles to seize the internet domain, and Swiss law enforcement seized the server hosting the NetWire RAT infrastructure.

The malware, first discovered in 2012, is often hidden in malicious files. The RAT is a favourite of cyber crime gangs and state-backed groups, and is frequently delivered by phishing attacks. After infecting a victim's smartphone or laptop, the RAT's capabilities include stealing passwords, keylogging, and remotely controlling the device.

"By removing the NetWire RAT, the FBI has impacted the criminal cyber ecosystem," Donald Alway, the assistant director in charge of the FBI's Los Angeles field office, declared in a statement.

"The global partnership that led to the arrest in Croatia also removed a popular tool used to hijack computers in order to perpetuate global fraud, data breaches and network intrusions by threat groups and cyber criminals," Alway added.

The FBI's Los Angeles bureau opened an investigation into the malware distributor in 2020. As part of this, undercover agents created accounts on the website, paid for a subscription, and "constructed a customized instance of the NetWire RAT using the product's Builder Tool," according to the affidavit in support of the seizure warrant.

As described in a warrant [PDF], Verisign redirected the worldwiredlabs domain to servers controlled by the FBI.

Neither US nor Croatian authorities released the suspect's name. However infosec journalist Brian Krebs has identified Mario Zanko of Zapresic, Croatia, as the owner of the domain since 2012.

The malware peddler allegedly sold NetWire licenses for between $10 and $1,200, according to Croatian police, who have yet to determine the total illicit haul from selling the RAT.

Other criminals who bought the malware used NetWire to target healthcare organizations and banks, they added.

The NetWire takedown follows several other international law enforcement operations over recent months intended to disrupt high-profile cyber crime gangs.

Earlier this month German and Ukrainian cops, working with Europol and the FBI, arrested suspected members of the DoppelPaymer ransomware crew and issued warrants for three other "masterminds" behind the global operation.

In January, US and international law enforcement partners shut down Hive's ransomware infrastructure following a seven-month covert operation. During that time, the FBI hacked Hive's network and used that access to provide decryption keys to more than 300 victims – saving them $130 million in ransomware payments, we're told.

That same month European cops arrested 15 suspected scammers and shut down a multi-country network of call centers selling fake cryptocurrency that law enforcement alleged stole upwards of hundreds of million euros from victims. ®

Similar topics

- Cybercrime
- FBI
- Security

×

Similar topics

- Cybercrime
- FBI
- Security

Narrower topics

Broader topics

United States Department of Justice

Similar topics

4 COMMENTS

Similar topics

- Cybercrime
- FBI
- Security

×

Similar topics

- Cybercrime
- FBI
- Security

Narrower topics

- 2FA
- Advanced persistent threat
- Application Delivery Controller
- Authentication
- BEC
- Black Hat
- Bug Bounty
- Common Vulnerability Scoring System
- Cybersecurity
- Cybersecurity and Infrastructure Security Agency
- Cybersecurity Information Sharing Act
- Data Breach
- Data Protection

- Data Theft
- DDoS
- Digital certificate
- Encryption
- Exploit
- Firewall
- Hacker
- Hacking
- Identity Theft
- Incident response
- Infosec
- Kenna Security
- NCSAM
- NCSC
- Palo Alto Networks
- Password
- Phishing
- Quantum key distribution
- Ransomware
- Remote Access Trojan
- REvil
- RSA Conference
- Spamming
- Spyware
- Surveillance
- TLS
- Trojan
- Trusted Platform Module
- Vulnerability
- Wannacry
- Zero trust

Broader topics

United States Department of Justice

TIP US OFF

Send us news