THE UNITED STATES DEPARTMENT of JUSTICE
JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Wednesday, January 27, 2021

Department of Justice Launches Global Action Against NetWalker Ransomware

NetWalker Defendant Charged, Dark Web Resource Disabled, Nearly $500,000 Seized

The Department of Justice today announced a coordinated international law enforcement action to disrupt a sophisticated form of ransomware known as NetWalker.

NetWalker ransomware has impacted numerous victims, including companies, municipalities, hospitals, law enforcement, emergency services, school districts, colleges, and universities. Attacks have specifically targeted the healthcare sector during the COVID-19 pandemic, taking advantage of the global crisis to extort victims.

"We are striking back against the growing threat of ransomware by not only bringing criminal charges against the responsible actors, but also disrupting criminal online infrastructure and, wherever possible, recovering ransom payments extorted from victims," said Acting Assistant Attorney General Nicholas L. McQuaid of the Justice Department's Criminal Division. "Ransomware victims should know that coming forward to law enforcement as soon as possible after an attack can lead to significant results like those achieved in today's multi-faceted operation."

The NetWalker action includes charges against a Canadian national in relation to NetWalker ransomware attacks in which tens of millions of dollars were allegedly obtained, the seizure of approximately $454,530.19 in cryptocurrency from ransom payments, and the disablement of a dark web hidden resource used to communicate with NetWalker ransomware victims.

"This action reflects the resolve of the U.S. Attorney's Office for the Middle District of Florida to target and disrupt sophisticated, international cybercrime schemes," said U.S. Attorney Maria Chapa Lopez for the Middle District of Florida. "While these individuals believe they operate anonymously in the digital space, we have the skill and tenacity to identify and prosecute these actors to the full extent of the law and seize their criminal proceeds."

According to court documents, NetWalker operates as a so-called ransomware-as-a-service model, featuring "developers" and "affiliates." Developers are responsible for creating and updating the ransomware and making it available to affiliates. Affiliates are responsible for identifying and attacking high-value victims with the ransomware, according to the affidavit. After a victim pays, developers and affiliates split the ransom.

"This case illustrates the FBI's capabilities and global partnerships in tracking ransomware attackers, unmasking them, and holding them accountable for their alleged criminal actions," said Special Agent in Charge Michael F. McPherson of the FBI's Tampa Field Office. "If you are a victim of ransomware, contact your local FBI field office or submit a tip to tips.fbi.gov. You can also file a complaint with the FBI's Internet Crime Complaint Center at www.ic3.gov."

Seizure page of dark web hidden resource used to communicate with NetWalker ransomware victims.

According to the affidavit, once a victim's computer network is compromised and data is encrypted, actors that deploy NetWalker deliver a file, or ransom note, to the victim. Using Tor, a computer network designed to facilitate anonymous communication over the internet, the victim is then provided with the amount of ransom demanded and instructions for payment.

Actors that deploy NetWalker commonly gain unauthorized access to a victim's computer network days or weeks prior to the delivery of the ransom note. During this time, they surreptitiously elevate their privileges within the network while spreading the ransomware from workstation to workstation. They then send the ransom note only once they are satisfied that they have sufficiently infiltrated the victim's network to extort payment, according to the affidavit.

According to an indictment unsealed today, Sebastien Vachon-Desjardins of Gatineau, a Canadian national, was charged in the Middle District of Florida. Vachon-Desjardins is alleged to have obtained at least over $27.6 million as a result of the offenses charged in the indictment.

The Justice Department further announced that on Jan. 10, law enforcement seized approximately $454,530.19 in cryptocurrency, which was comprised of ransom payments made by victims of three separate NetWalker ransomware attacks.

This week, authorities in Bulgaria also seized a dark web hidden resource used by NetWalker ransomware affiliates to provide payment instructions and communicate with victims. Visitors to the resource will now find a seizure banner that notifies them that it has been seized by law enforcement authorities.

The investigation was led by the FBI's Tampa field office.

Trial Attorneys S. Riane Harper and Brian Mund of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorneys Carlton C. Gammons and Suzanne Nebesky of the U.S. Attorney's Office for the Middle District of Florida are prosecuting the case against Vachon-Desjardins.

Substantial assistance was provided by the Department of Justice's Office of International Affairs. Additionally, the Bulgarian National Investigation Service and General Directorate Combating Organized Crime provided substantial assistance in the seizure of the dark web hidden resource.

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

Attachment(s):
Download NetWalker splash page

Topic(s):
Cyber Crime

Component(s):
Criminal Division
Criminal - Computer Crime and Intellectual Property Section
Criminal - Office of International Affairs
Federal Bureau of Investigation (FBI)
USAO - Florida, Middle

Press Release Number:
21-96

Updated January 27, 2021