NetWalker ransomware affiliate sentenced to 80 months in prison

Sergiu Gatlan

By
Sergiu Gatlan

- February 8, 2022
- 07:45 AM
- 0

Image: Ye Jinghan

Sebastien Vachon-Desjardins, a Canadian man charged by the US for his involvement in NetWalker ransomware attacks, was sentenced to 6 years and 8 months in prison after pleading guilty before an Ontario judge to multiple offenses linked to attacks on 17 Canadian victims.

On Monday, the judge said that, although Desjardins cooperated with the authorities to help identify victims and their losses, he still "played a dominant, almost exclusive, role in these offenses," aggravated by an unrelated drug trafficking criminal record and a prior sentence of 54 months imprisonment in Quebec.

The FBI discovered Desjardins's true identity after linking email accounts (Microsoft, Gmail, and Protonmail) he used to register accounts on XSS.is and HackForums with online activity (searches and emails) with various online services (including MEGA and ZoomInfo) he used to upload files stolen from victims' networks and find financial info on his victims.

He also made it easier by sharing personal information on public forums, including that he worked as an IT technician for the Canadian government (Public Works and Government Services Canada) for more than four years.

Tens of millions in losses

The attacks Desjardins participated in resulted in losses of millions of dollars after the victims had data stolen from their networks and were extorted into paying millions worth of cryptocurrency as ransoms.

"Between May 2020 and January 2021, the Defendant victimized 17 Canadian entities and others throughout the world by breaching private computer networks and systems, hi-jacking their data, holding the stolen data for ransom, and distributing stolen data when ransoms were not paid," the judge added.

The US Department of Justice said in January 2021 that Desjardins allegedly obtained more than $27.6 million after multiple successful attacks and extortion attempts since April 2020, when he first took up his new ransomware affiliate role.

"The Defendant admitted to investigators that over 1,200 Bitcoins related to his NetWalker malware activities passed through his e-wallet and were shared with his unindicted co-conspirators and the developer of the NetWalker ransomware," the judge said on Monday.

"As well, the Defendant admits that his entire ransomware activities involved over 2000 Bitcoins. The [Royal Canadian Mounted Police] RCMP seized slightly less than 720 Bitcoins from the Defendant's e-wallets and accounts."

Besides the 719.99591411 BTC seized from the Desjardins' BTC wallet in January 2021, according to a restraining order filed in January 2022, the police also seized 15.725489349111 XMR from a Monero wallet, CAD $299,150 from his residence, and over CAD $330,000 from several deposit boxes at National Bank of Canada held in his name.

After searching his home, law enforcement also seized many devices containing approximately 20 TB of data that, "if printed, would fill an entire hockey arena."

Netwalker ransomware operation sites seized

On January 27, 2021, when the US DOJ charged Desjardins, law enforcement from the USA and Bulgaria also seized dark websites associated with the Netwalker ransomware operation, including their Tor payment and data leak sites.

The seizure was the result of a joint investigation conducted by the FBI, the US DOJ, the Bulgarian National Investigation Service, and Bulgaria's General Directorate Combating Organized Crime.

Netwalker was a Ransomware-as-a-Service (RaaS) operation that surfaced in late 2019, enlisting affiliates to deploy the ransomware in return for a 60-75% share of all ransom payments.

This ransomware operation was immensely profitable for all the threat actors involved, seeing that an August 2020 report estimated that they collected $25 million from victims within just five months.

Some of the high-profile victims Netwalker targeted over the years include the Enel Group, Equinix, the University of California San Francisco (UCSF), the Argentian immigration agency, and K-Electric.

However, Netwalker affiliates were never picky. They also attacked and attempted to extort other private and public organizations, including hospitals, law enforcement organizations, emergency services, municipalities, school districts, colleges, and universities.

Related Articles:

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

- Canada
- Netwalker
- Ransomware

Sergiu Gatlan

Sergiu Gatlan is a reporter who covered cybersecurity, technology, Apple, Google, and a few other topics at Softpedia for more than a decade. Email or Twitter DMs for tips.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: