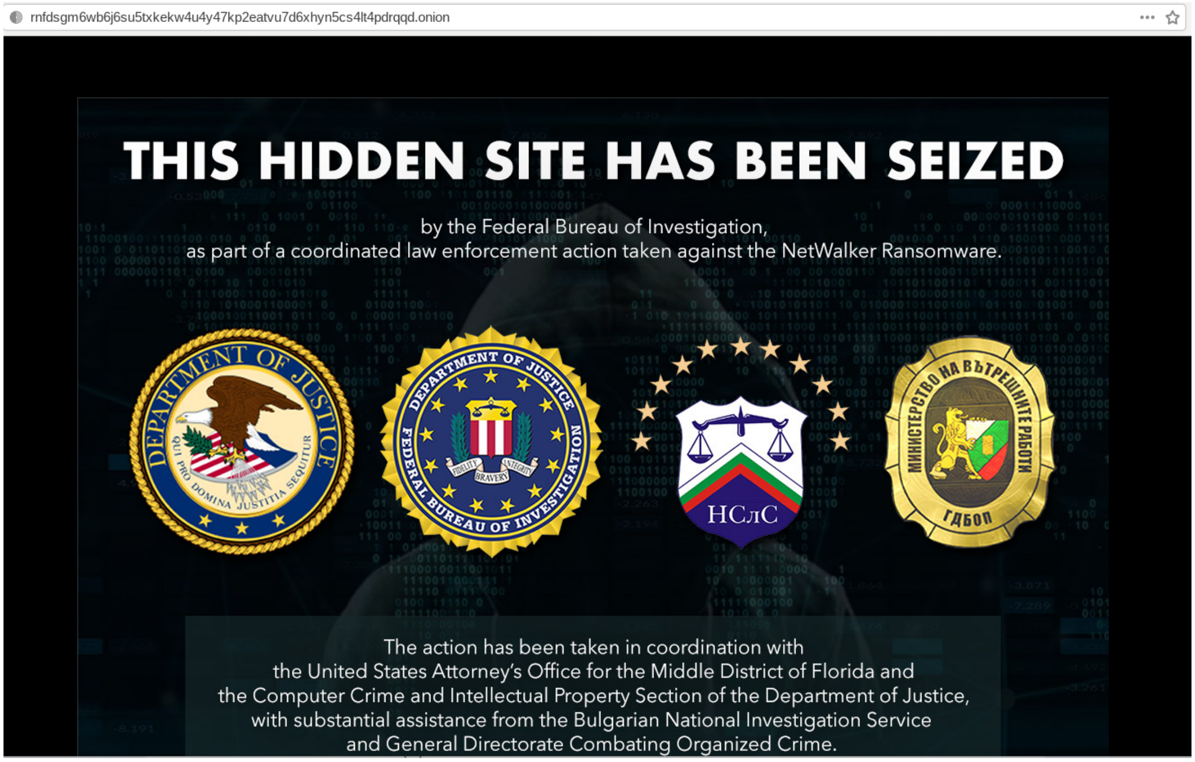
Arrest, Seizures Tied to Netwalker Ransomware

krebsonsecurity.com/2021/01/arrest-seizures-tied-to-netwalker-ransomware

U.S. and Bulgarian authorities this week seized the darkweb site used by the **NetWalker** ransomware cybercrime group to publish data stolen from its victims. In connection with the seizure, a Canadian national suspected of extorting more than $27 million through the spreading of NetWalker was charged in a Florida court.



rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion

THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
as part of a coordinated law enforcement action taken against the NetWalker Ransomware.

DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY
НСлС
МИНИСТЕРСТВО НА ВЪТРЕШНИТЕ РАБОТИ
ГДБОП

The action has been taken in coordination with
the United States Attorney's Office for the Middle District of Florida and
the Computer Crime and Intellectual Property Section of the Department of Justice,
with substantial assistance from the Bulgarian National Investigation Service
and General Directorate Combating Organized Crime.

The victim shaming site maintained by the NetWalker ransomware group, after being seized by authorities this week.

NetWalker is a ransomware-as-a-service crimeware product in which affiliates rent access to the continuously updated malware code in exchange for a percentage of any funds extorted from victims. The crooks behind NetWalker used the now-seized website to publish personal and proprietary data stolen from their prey, as part of a public pressure campaign to convince victims to pay up.

NetWalker has been among the most rapacious ransomware strains, hitting at least 305 victims from 27 countries — the majority in the United States, according to Chainalysis, a company that tracks the flow virtual currency payments.

“Chainalysis has traced more than $46 million worth of funds in NetWalker ransoms since it first came on the scene in August 2019,” the company said in a blog post detailing its assistance with the investigation. “It picked up steam in mid-2020, growing the average ransom to $65,000 last year, up from $18,800 in 2019.”

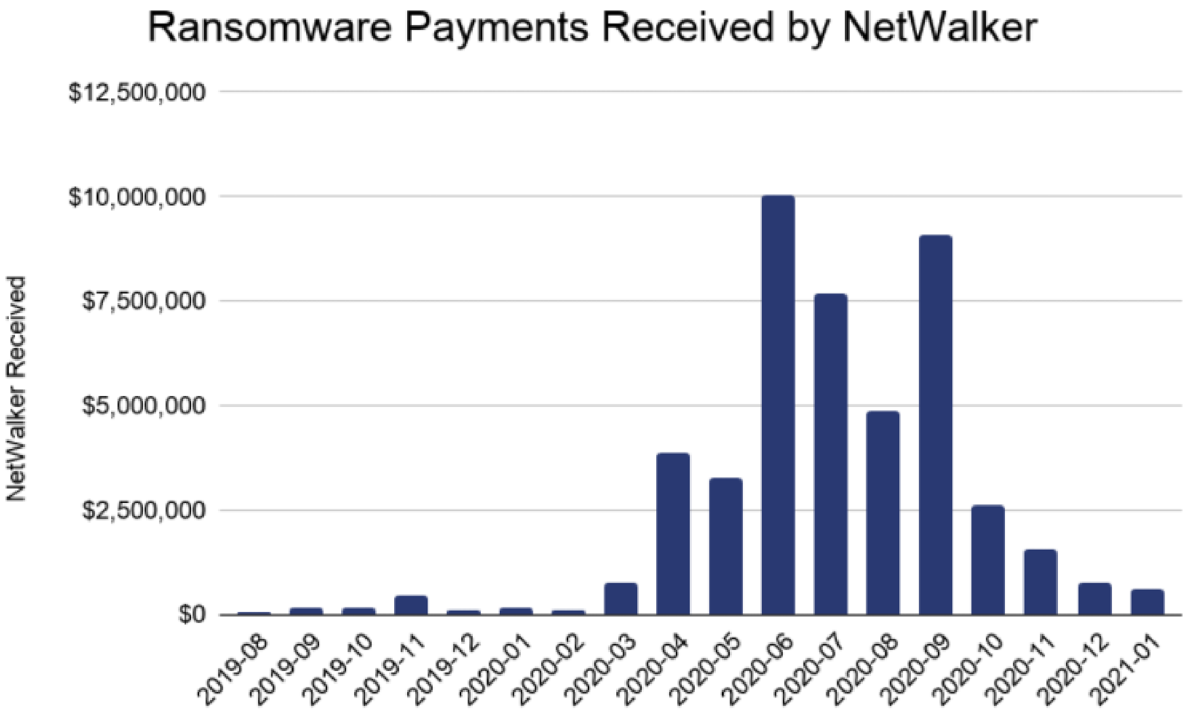


Image: Chainalysis

In a statement on the seizure, the Justice Department said the NetWalker ransomware has impacted numerous victims, including companies, municipalities, hospitals, law enforcement, emergency services, school districts, colleges, and universities. For example, the University of California, San Francisco paid $1.14 million last summer in exchange for a digital key needed to unlock files encrypted by the ransomware.

"Attacks have specifically targeted the healthcare sector during the COVID-19 pandemic, taking advantage of the global crisis to extort victims," the DOJ said.

U.S. prosecutors say one of NetWalker's top affiliates was **Sebastien Vachon-Desjardins**, of Gatineau, in Ottawa, Canada. An indictment unsealed today in Florida alleges Vachon-Desjardins obtained at least $27.6 million from the scheme.

The DOJ's media advisory doesn't mention the defendant's age, but a 2015 report in the Gatineau local news website ledroit.com suggests this may not be his first offense. According to the story, a then-27-year-old Sebastien Vachon-Desjardins was sentenced to more than three years in prison for drug trafficking: He was reportedly found in possession of more than 50,000 methamphetamine tablets.

The NetWalker action came on the same day that European authorities announced a coordinated takedown targeting the Emotet crimeware-as-a-service network. Emotet is a pay-per-install botnet that is used by several distinct cybercrime groups to deploy secondary malware — most notably the ransomware strain Ryuk and Trickbot, a powerful banking trojan.

The NetWalker ransomware affiliate program kicked off in March 2020, when the administrator of the crimeware project began recruiting people on the dark web. Like many other ransomware programs, NetWalker does not permit affiliates to infect systems physically located in Russia or in any other countries that are part of the Commonwealth of Independent States (CIS) — which includes most of the nations in the former Soviet Union. This is a prohibition typically made by cybercrime operations that are coordinated out of Russia and/or other CIS nations because it helps minimize the chances that local authorities will investigate their crimes.

The following advertisement (translated into English by cybersecurity firm Intel 471) was posted by the NetWalker affiliate program manager last year to a top cybercrime forum. It illustrates the allure of the ransomware affiliate model, which handles everything from updating the malware to slip past the latest antivirus updates, to leasing space on the dark web where affiliates can interact with victims and negotiate payment. The affiliate, on the other hand, need only focus on finding new victims.

> We are recruiting affiliates for network processing and spamming.
> We are interested in people whose priority is quality and not quantity.
> We prefer candidates who can work with large networks and have their own access to them.
> We are going to recruit a limited number of affiliates and then close the openings until they are available again.
>
> We offer you prompt and flexible ransomware, a user-friendly admin panel in Tor, an automated service.
>
> Encryption of shared accesses: if several users are logged in to the target computer, the ransomware will infect their mapped drives, as well as network resources where those users are logged in — shared accesses/NAS etc.
>
> Powershell build. Each build is unique, in that the malware is inside the script – it is not downloaded from the internet. This makes bypassing antivirus protection easier, including Windows Defender (cloud+).
>
> A fully automated blog where the victim's dumped data is directed. The data is published according to your settings. Instant and automated payouts: initially 20 percent, no less than 16 percent.
>
> Accessibility of a crypting service to avoid AV detections.
>
> The ransomware has been in use since September 2019 and proved to be reliable. The files encrypted with it cannot be decrypted.
>
> Targeting Russia or the CIS is prohibited.
>
> You'll get all the information about the ransomware as well as terms and conditions after you place an application via PM.
>
> Application form:
> 1) The field you specialize in.
> 2) Your experience. What other affiliate programs have you been in and what was your profit?
> 3) How many accesses [to networks] do you have? When are you ready to start? How many accesses do you plan on monetizing?