Chainalysis in Action: U.S. Authorities Disrupt NetWalker Ransomware

By Chainalysis Team

Published: 2021-01-27 · Archived: 2026-04-05 23:41:28 UTC

Today, the U.S. Department of Justice (DOJ) announced a coordinated international law enforcement action to disrupt the NetWalker ransomware, including the seizure of nearly half a million dollars in cryptocurrency, the disablement of a dark web resource used to communicate with NetWalker ransomware victims, and the arrest of a Canadian national, Sebastien Vachon-Desjardins, who obtained tens of millions of dollars by acting as a NetWalker affiliate.

This case highlights the sophistication with which NetWalker operated, the global impact of ransomware attacks, and the substantial funds ransomware actors steal from their victims.

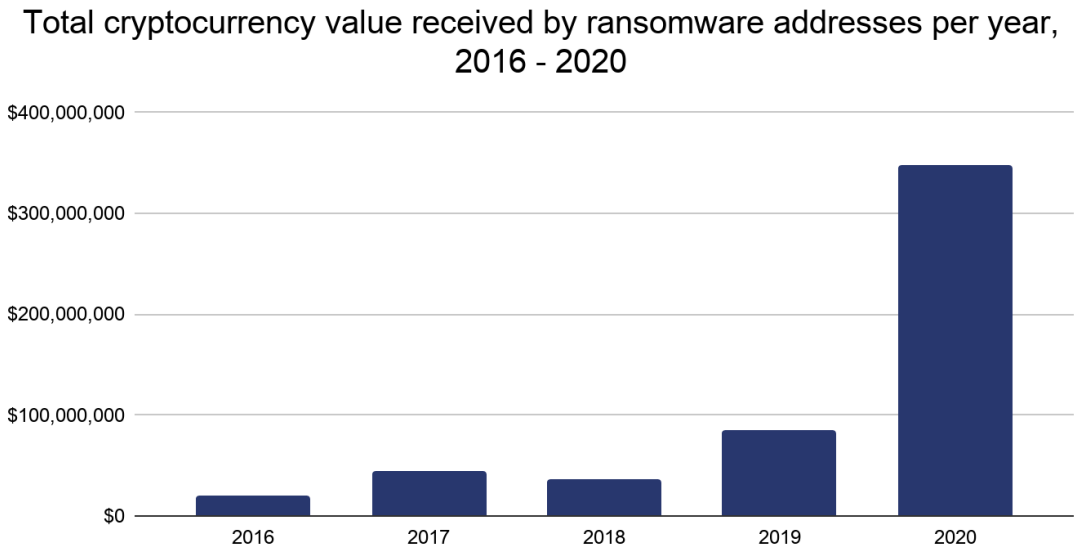
Chainalysis congratulates our government partners for their success in disrupting NetWalker's operations, and we're proud that Chainalysis investigative tools helped them track down ransomware funds. We're also proud to provide exchanges with the transaction monitoring tools necessary to prevent these funds from being traded on their platforms.

Homepage of the seized dark web communications site

Below, we'll break down what blockchain analysis tells us about the NetWalker strain of ransomware and highlight specific elements of the investigation to show how law enforcement was able to trace the illicit funds.

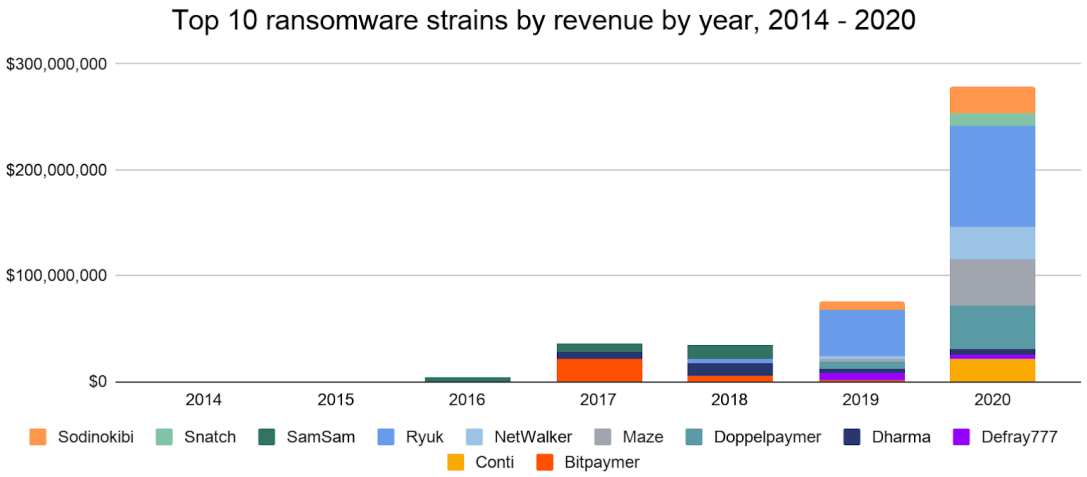
Ransomware's Growth and Increasing Sophistication

Chainalysis data shows that the total amount paid by ransomware victims increased 311% in 2020 to reach nearly $350 million worth of cryptocurrency. This number is a lower bound of the true total, as underreporting means we likely haven't categorized every victim payment address in our datasets.

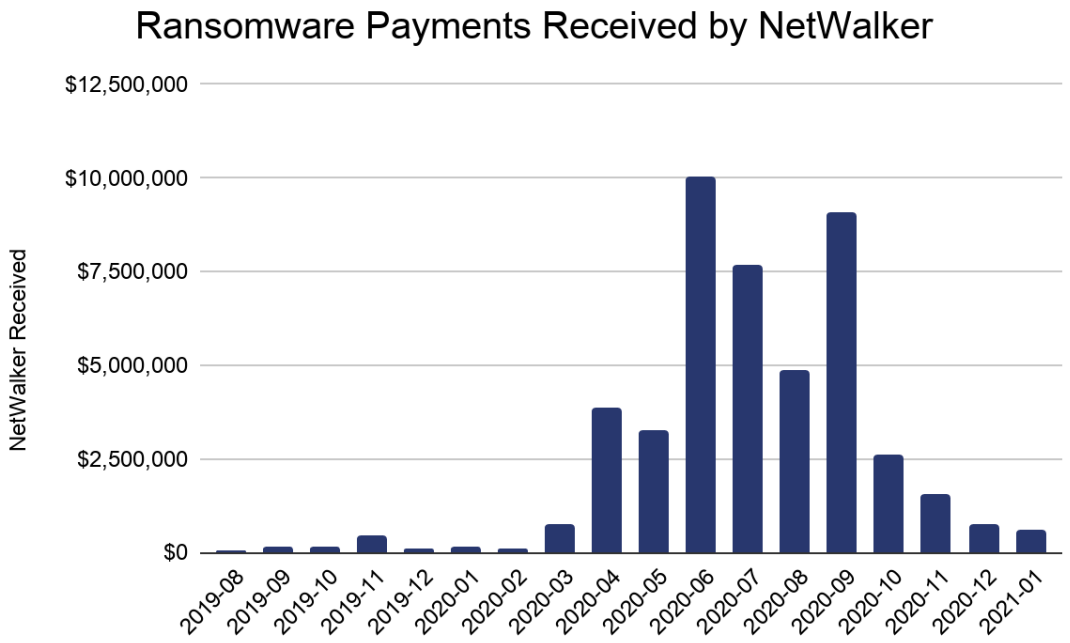


Many strains, including NetWalker, function on the Ransomware as a Service (RaaS) model, in which attackers known as affiliates "rent" usage of a particular ransomware strain from its creators or administrators, who in exchange get a cut of the money from each successful attack affiliates carry out. RaaS has led to more attacks, making it even more difficult to quantify the full financial impact. But the trend is clear; no other category of cryptocurrency-based crime had a higher growth rate than ransomware in 2020.

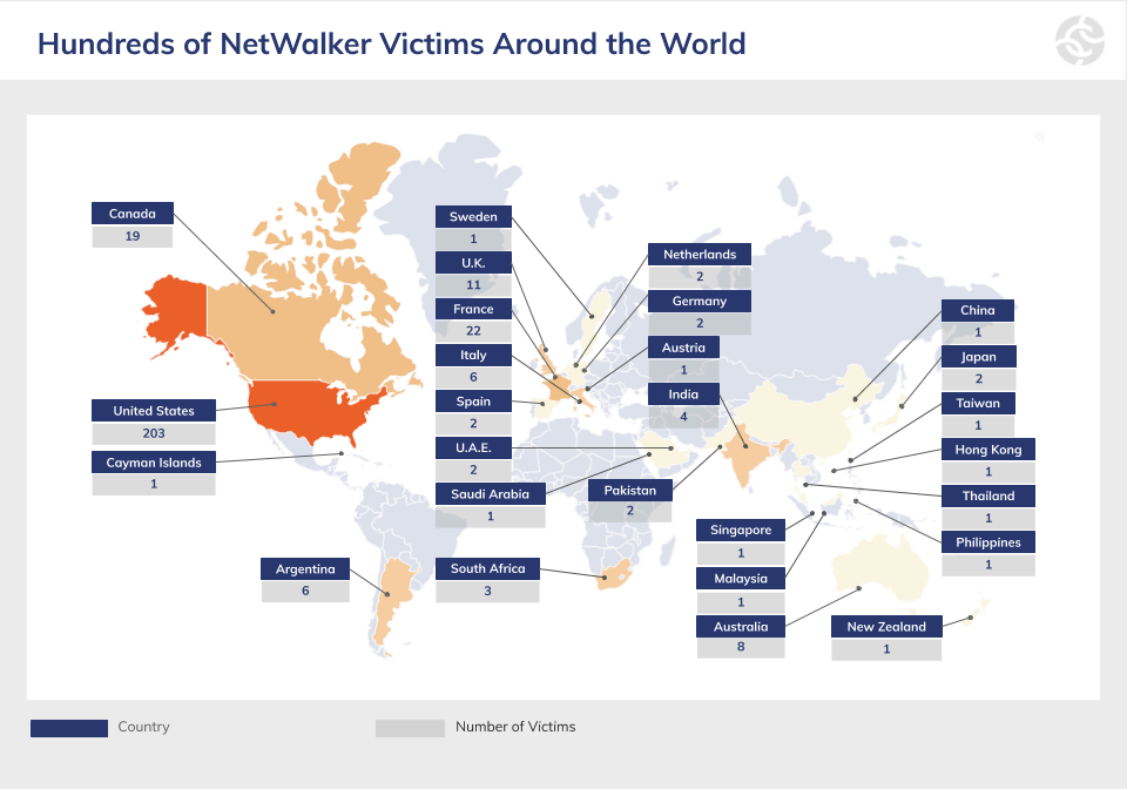
NetWalker was a top ransomware strain by revenue this year, along with Ryuk, Maze, Doppelpaymer, and Sodinokibi.



Chainalysis has traced more than $46 million worth of funds in NetWalker ransoms since it first came on the scene in August 2019. It picked up steam in mid-2020, growing the average ransom to $65,000 last year, up from $18,800 in 2019.

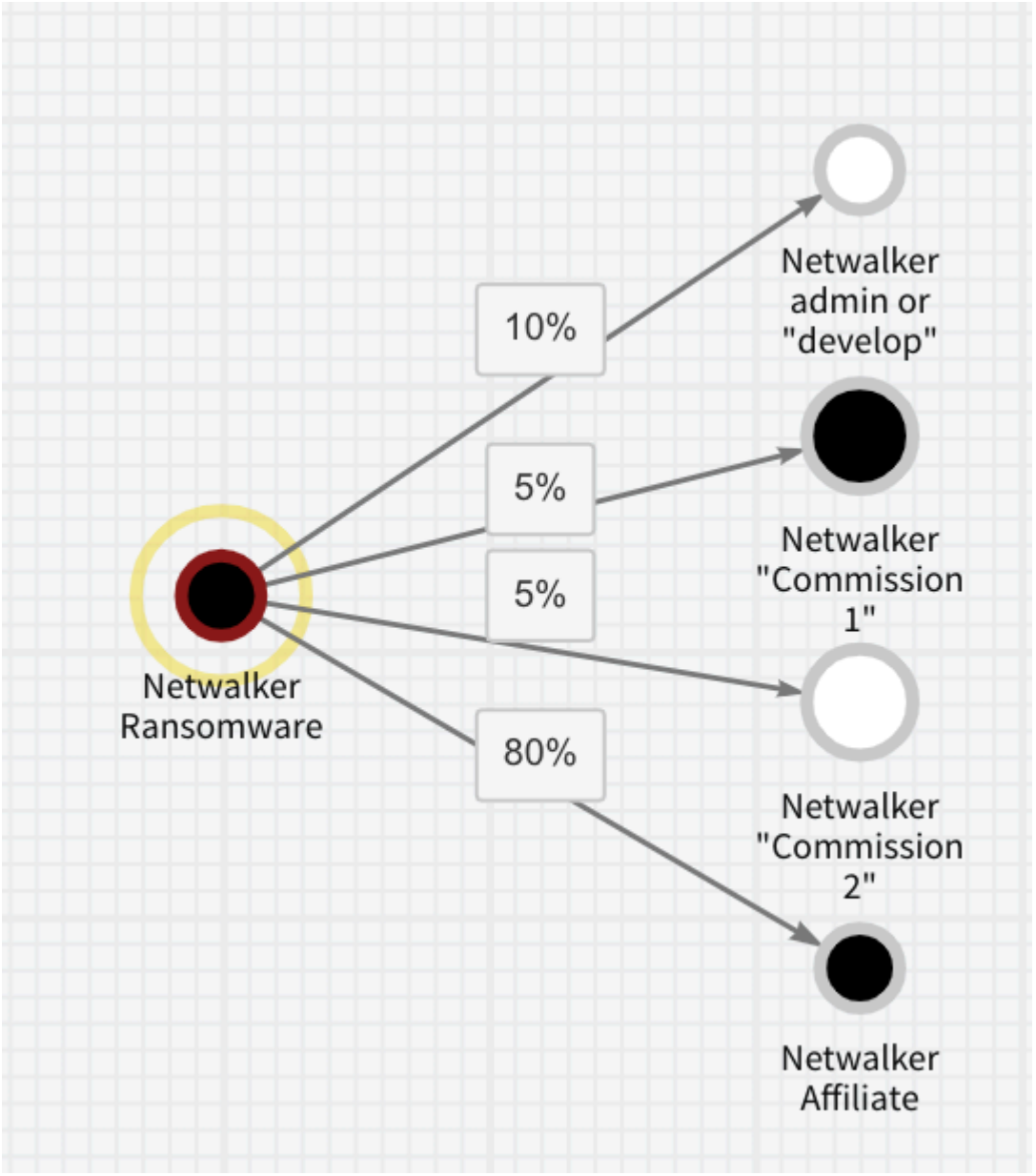


According to U.S. authorities, NetWalker has impacted at least 305 victims from 27 different countries, including 203 in the U.S.

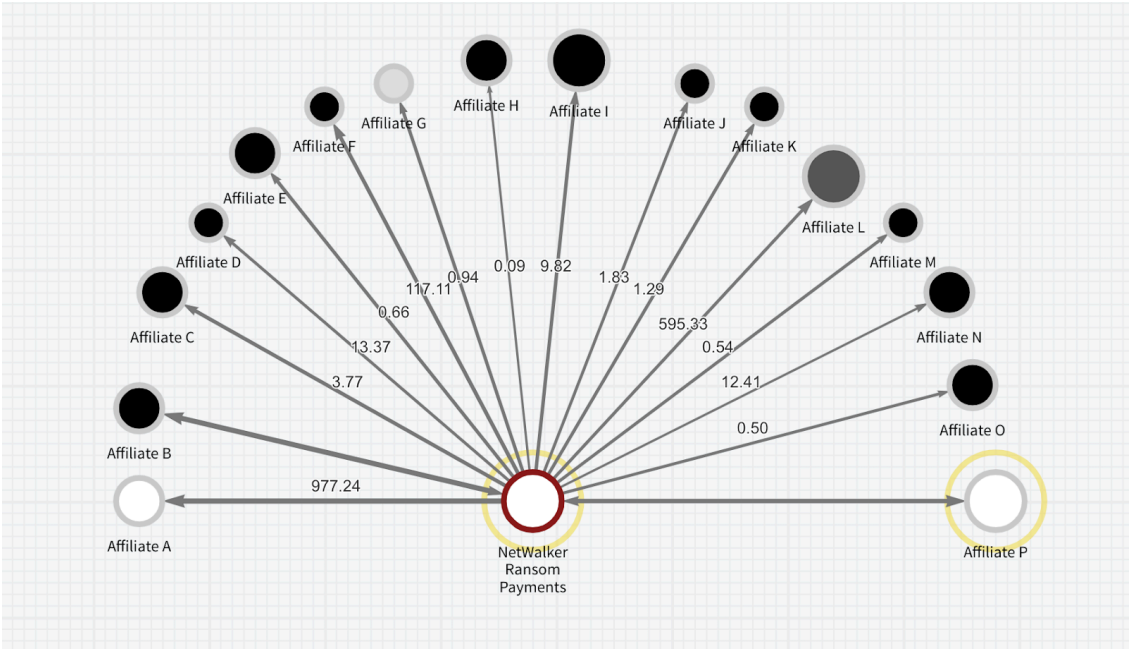


What Blockchain Analysis Tells Us about NetWalker Operations and Financials

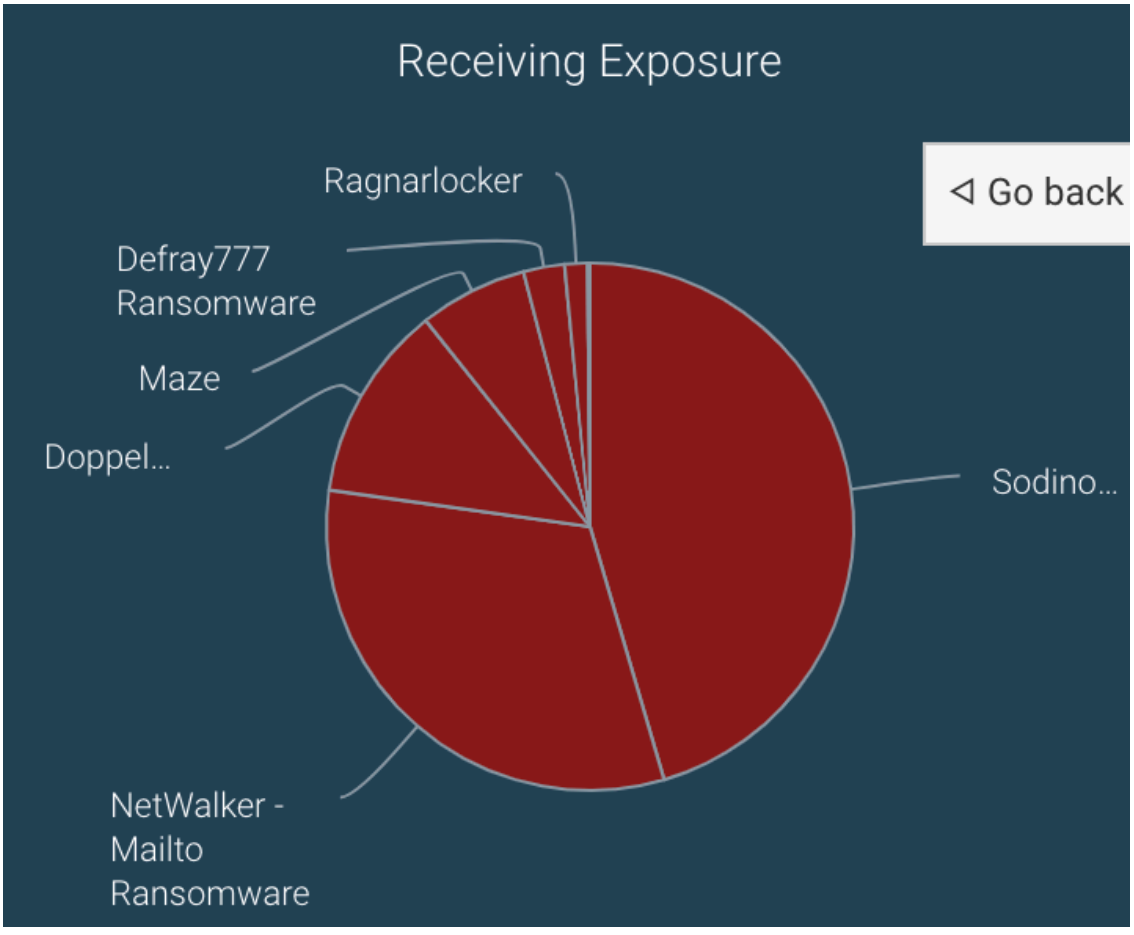
Typically, there are four roles that receive proceeds from NetWalker attacks: the likely administrator or developer (8-10%), the affiliate (76-80%), and two commissioned roles (2.5%-5% each). An affiliate, like Vachon-Desjardins, is usually responsible for obtaining access to the victim network and deploying the malware. There are also cases when one wallet gets 100% of the payment, which we believe belongs to the NetWalker administrator and indicates that he or she may also be directly involved in some of the attacks.



This screenshot of Chainalysis Reactor shows the typical transfer of funds from the ransom payment address to the different NetWalker actors.



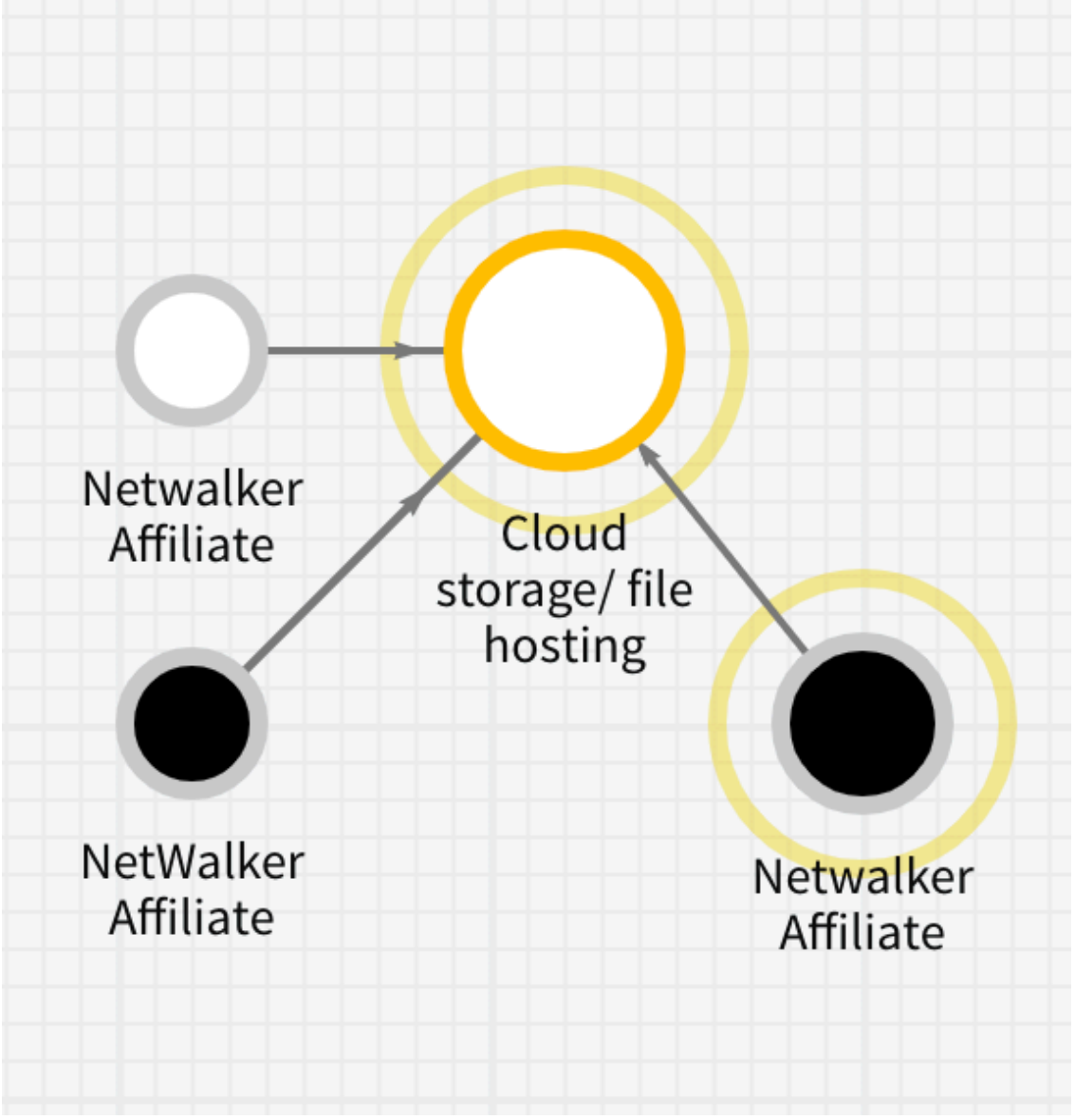
Blockchain analysis reveals that there were actually fewer than 20 unique affiliates. Of those affiliates, some rarely deployed NetWalker. Some moved on to other RaaS strains, and we can use the Chainalysis Reactor exposure wheel to show that some affiliates have received payments from other variants.



The NetWalker administrator, who goes by the moniker “Bugatti” on darknet forums, posted an advertisement in May 2020 on a forum seeking additional Russian-speaking affiliates as vacancies had “freed up,” which confirms

our assessment of affiliates migrating to other strains.

Blockchain analysis can also show ransomware actors paying for services they need to operate their criminal enterprise. For example, we can see below that NetWalker actors paid for cloud storage hosting with cryptocurrency, likely used to host stolen victim data for further extortion. Indeed, NetWalker ramped up its extortion efforts in May 2020 by not only locking victims out of their data, but also by stealing it. Before encrypting computer files on a victim's network, NetWalker actors began to steal the data and automatically publish victim data on a leak site if the ransom was not paid by the deadline, another growing trend among several ransomware strains.



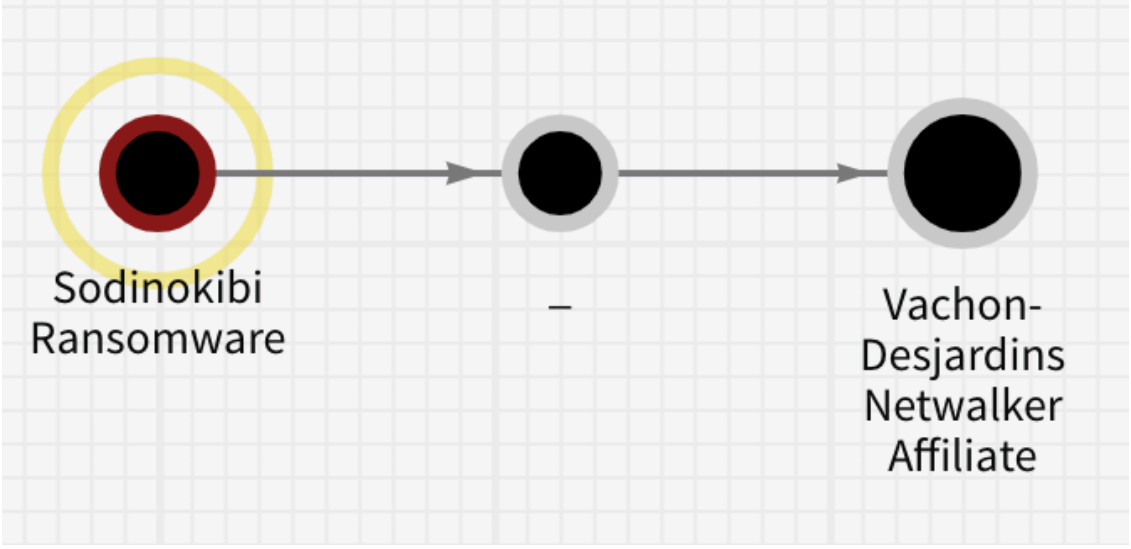
How Authorities Used Blockchain Analysis to Trace the Flow of NetWalker Funds

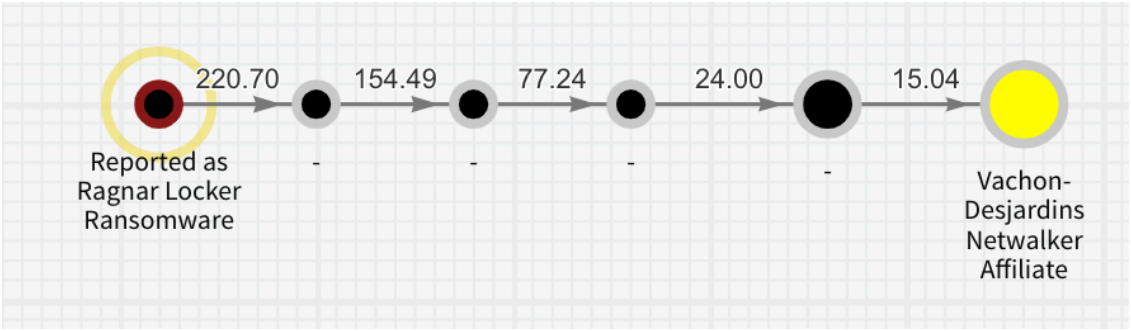
According to the indictment unsealed today, Vachon-Desjardins was charged with intentional damage to a protected computer and transmitting a demand in relation to it. This involved a NetWalker ransomware attack against a victim company located in Florida.

Blockchain analysis revealed at least 345 addresses associated with Vachon-Desjardins going back to February 2018 with transactions continuing to the date of this writing (January 27, 2021). He allegedly received more than $14 million worth of Bitcoin at the time of receipt of the funds, ultimately possessing at least $27.6 million given its rising value.

According to government partners, Vachon-Desjardins was involved in at least 91 attacks using NetWalker ransomware since April 2020, deploying the malware as an affiliate and receiving 80% of the ransom.

In addition to NetWalker, we suspect Vachon-Desjardins was involved in the deployment of other RaaS strains like Sodinokibi, Suncrypt, and Ragnarlocker. This is relatively common; we often see affiliates migrate to different strains over time. Additionally, the NetWalker admin Bugatti has listed proof of prior hacking experience as a prerequisite to become a NetWalker affiliate, so it would make sense that affiliates like Vachon-Desjardins would have a track record.





The Chainalysis Reactor graphs above show NetWalker affiliates with exposure to Sodinokibi and Ragnar Locker ransomware strains.

Government and industry must work together against ransomware

It’s important that cryptocurrency exchanges and government agencies continue to work together to prevent ransomware actors from cashing out their ill-gotten gains. We look forward to continuing to supply governments

and businesses around the world with the blockchain analysis tools necessary to accomplish those goals. Chainalysis has labeled in our products all NetWalker victim payment addresses, and Chainalysis KYT and Kryptos customers with exposure to these addresses will receive alerts in real-time.

Want to learn more about how law enforcement used Chainalysis to investigate ransomware? We have limited spots available for demos. Sign up for one to see for yourself — a Chainalysis specialist can walk you through the Reactor graphs we show above and answer all your questions.

To learn more about the latest trends in ransomware and more, sign up to get our full 2021 Crypto Crime report emailed to your inbox when it's released in February.
