Ransomware recruits affiliates with huge payouts, automated leaks

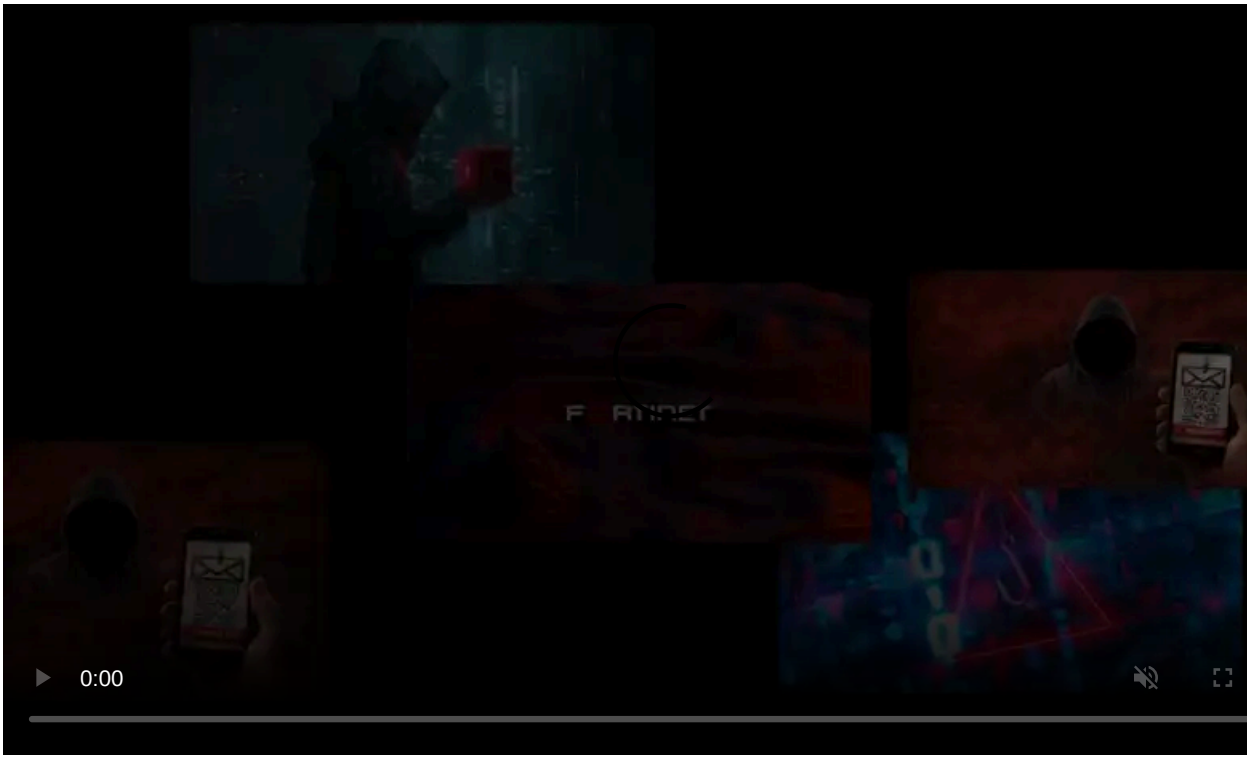
By Lawrence Abrams

Published: 2020-05-15 · Archived: 2026-04-06 03:31:23 UTC

The Netwalker ransomware operation is recruiting potential affiliates with the possibility of million-dollar payouts and an auto-publishing data leak blog to help drive successful ransom payments.

Started as Mailto and responsible for high profile attacks, the ransomware operators rebranded as Netwalker in March 2020 when it began to recruit potential affiliates to distribute their ransomware.

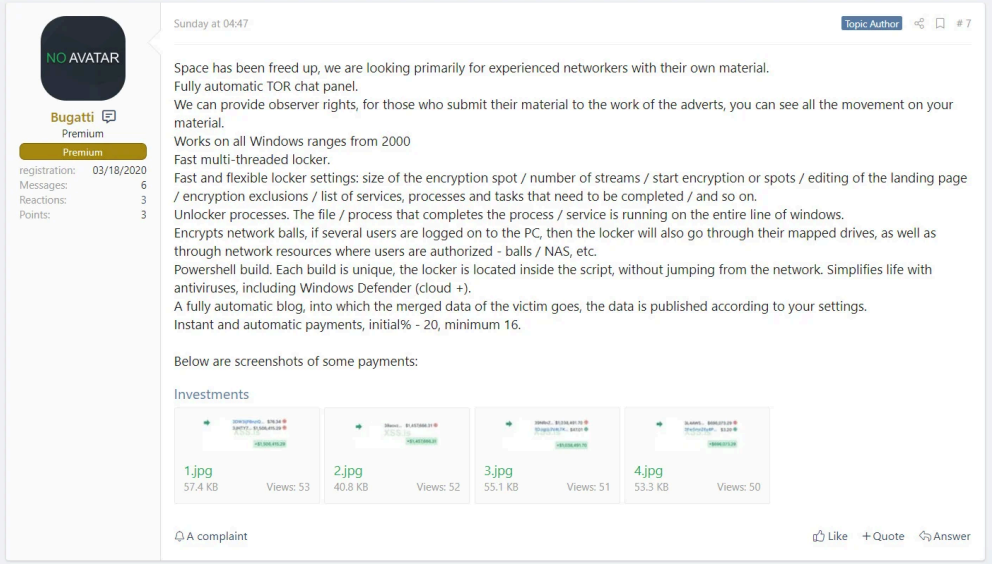
These affiliates would be in charge of breaching networks and deploying the ransomware, and in return, would receive the lion's share of any ransom payments they bring in.


0:00

Promises of riches

In a series of posts to a Russian hacker forum shared with BleepingComputer by cyber intelligence firm Advanced Intelligence, the public-facing operator of the Netwalker ransomware has been interviewing affiliates for their program since March.

In a new post created over the weekend, Netwalker outlines all the improvements made to their operation, which include some very revealing data about ransom payments and new ways that they are extorting their victims.

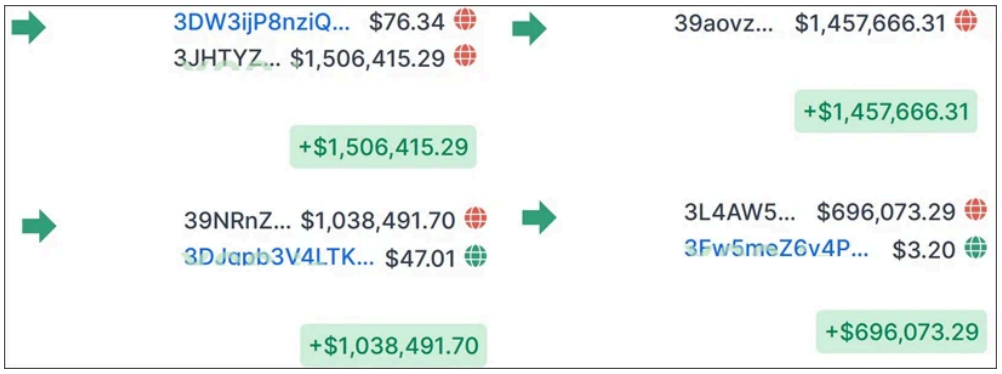


Recruitment post

Attached to the post are four images showing some of the large ransom payments they have received from victims who paid.

These ransom payments range from $696,000 up to $1.5 million.

As affiliates typically earn 70% of a ransom, if not more, they would receive between $487,000 to over a $1 million from a single ransom payment.



Netwalker ransom payments

Auto-publishing data leak site adds further leverage

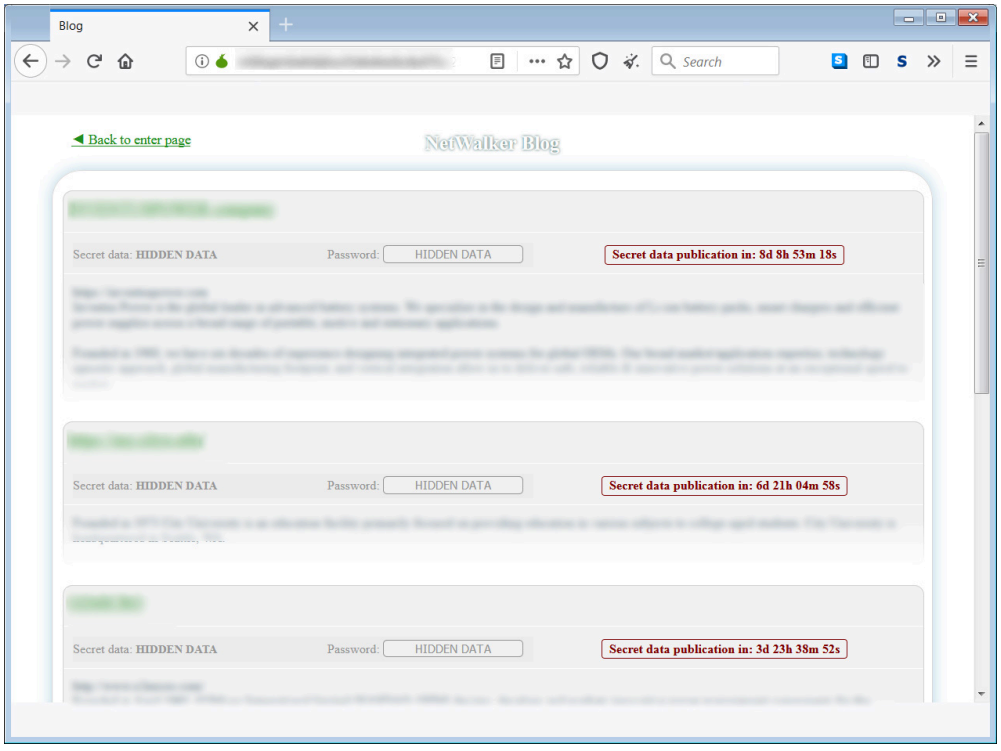
In addition to the million-dollar payouts, Netwalker is promoting an auto-publishing data leak site that allows an affiliate to upload links to stolen data and then set a date when it should be publicly released.

A tactic that has become common this year is for ransomware operators to steal unencrypted data from networks before performing the encryption.

They then tell the victims that they will publicly release their files on data leak sites if a ransom is not paid.

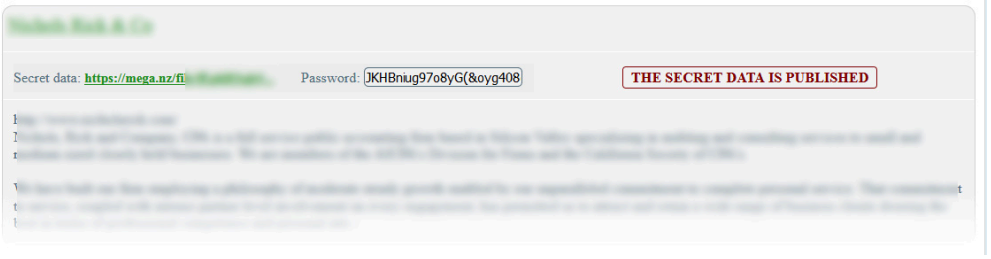
Netwalker has gone one step further and created a leak site that allows their affiliates to create posts containing a victim's name, their description, links to their data, a password to open the data file, and the date and time that the data should be posted.

The site will then show a countdown for a particular victim's data reveal to provoke anxiety within their victims in the hopes it will coerce them into making a ransom payment.



Stolen data leak blog

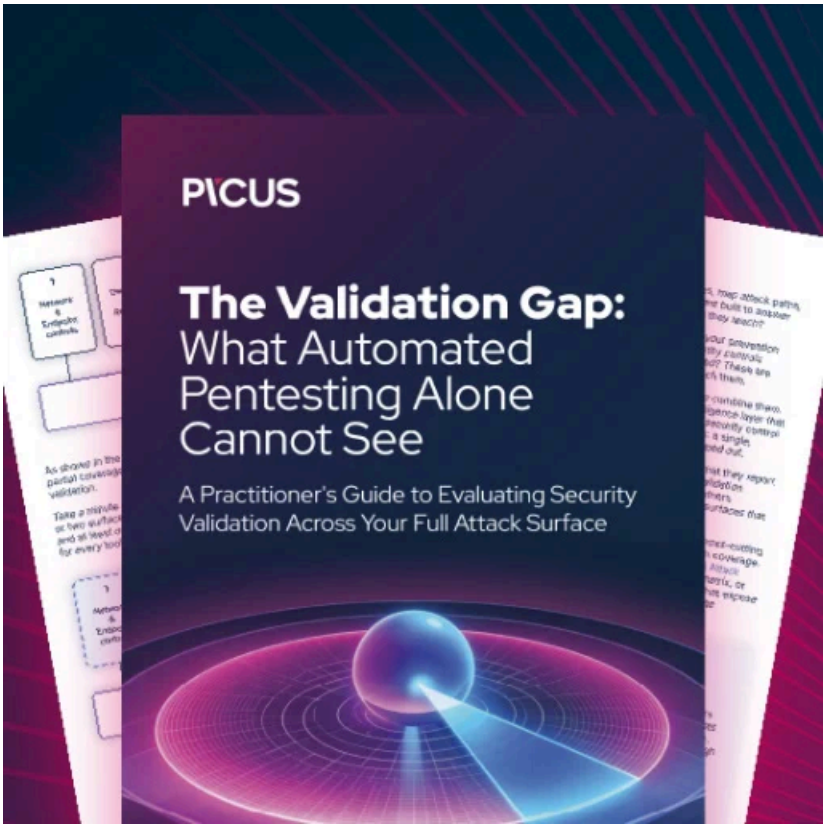
When the countdown reaches zero, the leak will automatically publish with a link and password for the stolen data. This data is usually hosted at the MEGA file-sharing site.



Link to leaked data

With ransomware operations generating such tremendous amounts of revenue, they are becoming more organized and selective as they try to recruit only the best talent.

Unfortunately, this also means that ransomware, and the data breaches they cause, are not going away any time soon.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/ransomware-recruits-affiliates-with-huge-payouts-automated-leaks/