Hive ransomware: modern, efficient business model

January 27 2023, by Paul HANDLEY

On the so-called dark web, providers of ransomware services and support pitch their products openly.

The US Justice Department's shutdown Thursday of the Hive ransomware operation—which extorted some $100 million from more

than 1,500 victims worldwide—highlights how hacking has become an ultra-efficient, specialized industry that can allow anyone to become a cyber-shakedown artist.

Modern business model

Hive operated in what cybersecurity experts call a "ransomware as a service" style, or RaaS—a business that leases its software and methods to others to use in extorting a target.

The model is central to the larger ransomware ecosystem, in which actors specialize in one skill or function to maximize efficiency.

According to Ariel Ropek, director of cyber threat intelligence at cybersecurity firm Avertium, this structure makes it possible for criminals with minimal computer fluency to get into the ransomware game by paying others for their expertise.

"There are quite a few of them," Ropek said of RaaS operations.

"It is really a business model nowadays," he said.

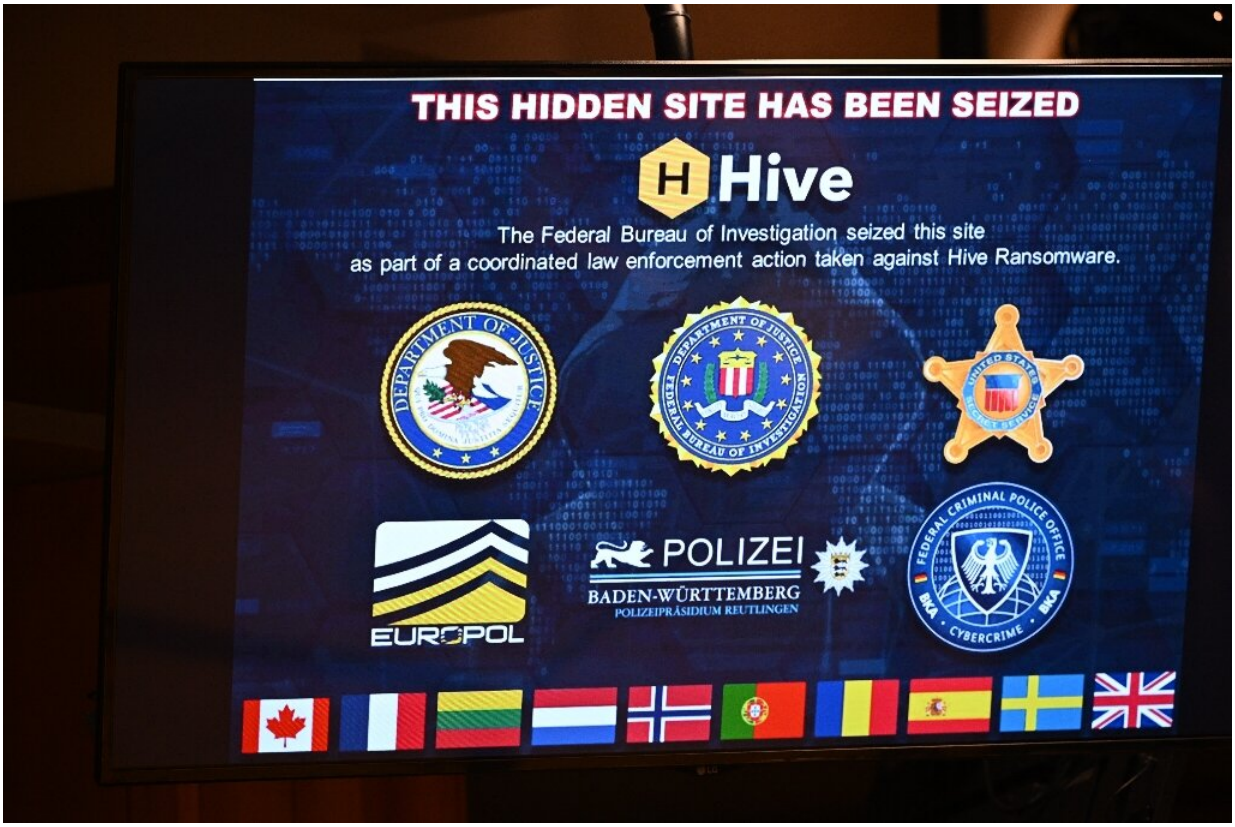
How it works

On the so-called dark web, providers of ransomware services and support pitch their products openly.

At one end are the initial access brokers, who specialize in breaking into corporate or institutional computer systems.

They then sell that access to the hacker, or ransomware operator.

But the operator depends on RaaS developers like Hive, which have the programming skills to create the malware needed to carry out the operation and avoid counter-security measures.



The US Justice Department announced January 26, 2023 it had shut down the Hive ransomware operation, which had extorted more than $100 million from more than 1,500 victims worldwide.

Typically, their programs—once inserted by the ransomware operator into the target's IT systems—are manipulated to freeze, via encryption, the target's files and data.

The programs also extract the data back to the ransomware operator.

RaaS developers like Hive offer a full service to the operators, for a large share of the ransom paid out, said Ropek.

"Their goal is to make the ransomware operation as turnkey as possible," he said.

Polite but firm

When the ransomware is planted and activated, the target receives a message telling them how to correspond and how much to pay to get their data unencrypted.

That ransom can run from thousands to millions of dollars, usually depending on the financial strength of the target.

Inevitably the target tries to negotiate on the portal. They often don't get very far.

Menlo Security, a cybersecurity firm, last year published the conversation between a target and Hive's "Sales Department" that took place on Hive's special portal for victims.

In it, the Hive operator courteously and professionally offered to prove the decryption would work with a test file.

But when the target repeatedly offered a fraction of the $200,000 demanded, Hive was firm, insisting the target could afford the total amount.

Eventually, the Hive agent gave in and offered a significant reduction—but drew the line there.

FBI Director Christopher Wray with Deputy Attorney General Lisa Monaco (2L), and US Attorney General Merrick Garland (R), announce an international ransomware enforcement action against Hive on January 26, 2023.

"The price is $50,000. It's final. What else to say?" the Hive agent wrote.

If a target organization refuses to pay, the RaaS developers hold a backup position: they threaten to release the hacked confidential files online or sell them.

Hive maintained a separate website, HiveLeaks, to publish the data.

On the back end of the deal, according to Ropek, there are specialist operations to collect the money, making sure those taking part get their

shares of the ransom.

Others, known as cryptocurrency tumblers, help launder the ransom for the hacker to use above-ground.

Modest blow

Thursday's action against Hive was only a modest blow against the RaaS industry.

There are numerous other ransomware specialists similar to Hive still operating.

The biggest current threat is LockBit, which attacked Britain's Royal Mail in early January and a Canadian children's hospital in December.

In November, the Justice Department said LockBit had reaped tens of millions of dollars in ransoms from 1,000 victims.

And it isn't hard for Hive's operators to just start again.

"It's a relatively simple process of setting up new servers, generating new encryption keys. Usually there's some kind of rebrand," said Ropek.

Citation: Hive ransomware: modern, efficient business model (2023, January 27) retrieved 9 April 2024 from https://techxplore.com/news/2023-01-hive-ransomware-modern-efficient-business.html