Global operation smashes 'most harmful cyber crime group'

February 20 2024, by Helen ROWE, Peter HUTCHISON

A message on LockBit's site said law envorcement agencies had taken it over.

An international operation led by UK and US law enforcement has severely disrupted "the world's most harmful cybercrime group", the Russian-linked ransomware specialist LockBit, officials announced Tuesday.

LockBit and its affiliates have targeted governments, major companies,

schools and hospitals, causing billions of dollars of damage and extracting tens of millions in ransoms from victims.

Britain's National Crime Agency (NCA), working with the Federal Bureau of Investigation, Europol and agencies from nine other countries in Operation Cronos, said it had infiltrated LockBit's network and taken control of its services.

"We have hacked the hackers, we have taken control of their infrastructure, seized their source code, and obtained keys that will help victims decrypt their systems," NCA director general Graeme Biggar told reporters in London.

LockBit's website—selling services that allow people to organize cyber attacks and hold data until a ransom is paid appears—was taken over on Monday evening.

A message appeared on the site stating that it was "now under control of law enforcement".

"As of today LockBit is effectively redundant, LockBit has been locked out," Biggar said.

The US Justice Department (DOJ) said the agencies had seized control of "numerous public-facing websites used by LockBit to connect to the organization's infrastructure" and taken control of servers used by LockBit administrators.

The NCA added that it had obtained more than 1,000 decryption keys and will be contacting UK-based victims in the coming days and weeks to offer support and help them recover encrypted data.

Biggar said the network had been behind 25 percent of all cyber attacks

in the past year.

LockBit has targeted over 2,000 victims and received more than $120 million in ransom payments since it formed four years ago, according to the DOJ.

Those targeted have included Britain's Royal Mail, US aircraft manufacturer Boeing, and a Canadian children's hospital.

In January 2023, US law enforcers shut down the Hive ransomware operation which extorted some $100 million from more than 1,500 victims worldwide.

Since then, LockBit has been seen as the biggest current threat.

Dark Web

Hive and LockBit are part of 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 money.

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

On the so-called dark web, providers of ransomware services 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 or LockBit, which have the programming skills to create the malware needed to carry out the operation.

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

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

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

That ransom can run from thousands to millions of dollars.

On Tuesday, the US unsealed an indictment against two Russian nationals, bringing to five the number of Russians it has charged in connection with LockBit.

In a separate notice, the US Treasury Department said it is imposing sanctions on the pair, affiliates of LockBit, who "actively engaged" in ransomware attacks.

Biggar said a "large concentration" of the cyber criminals are in Russia and are Russian-speaking, but law enforcement agencies have not seen any direct support for LockBit from the Russian state.

"There is clearly some tolerance of cyber criminality within Russia," he added.