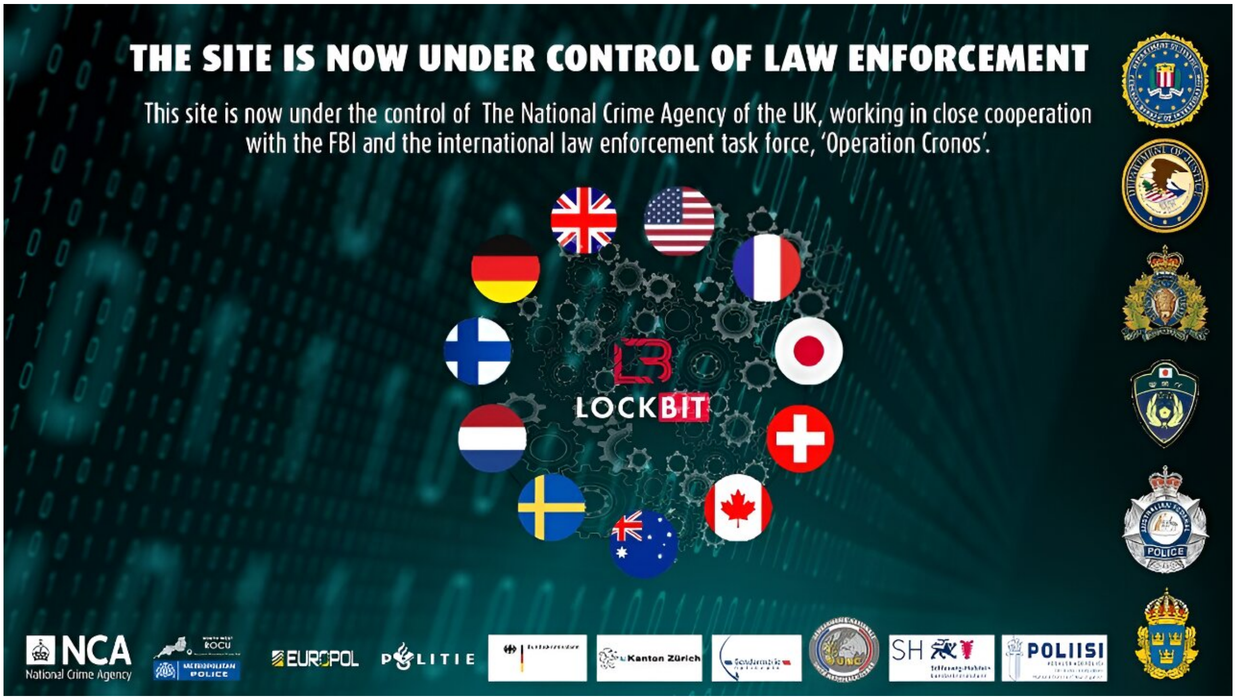
TechXplore

Stuck in cyberattack nightmare? Call the negotiators

February 20 2024, by James PHEBY



THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

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

Criminals have overtaken your computer network, they are threatening to leak your most sensitive secrets and your share price is tumbling. It's time to call in the negotiators.

They might not wear capes, but this new breed of mediator—who often has had prior careers in law enforcement and intelligence—is increasingly on hand to help in such a nightmare scenario.

Britain's National Crime Agency (NCA) and law enforcement partners from several other countries announced Tuesday that they had smashed the cybercrime giant LockBit, whose ransomware attacks have caused billions of dollars of damage and stolen tens of millions from victims.

The gang had targeted governments, major companies, schools and hospitals since 2020.

Institutions of all shapes and sizes are still prey to the growing criminal threat, though.

In a ransomware attack, gangs—sometimes state-backed—hack into networks and demand payment either to unlock the system or prevent the release of top-secret data.

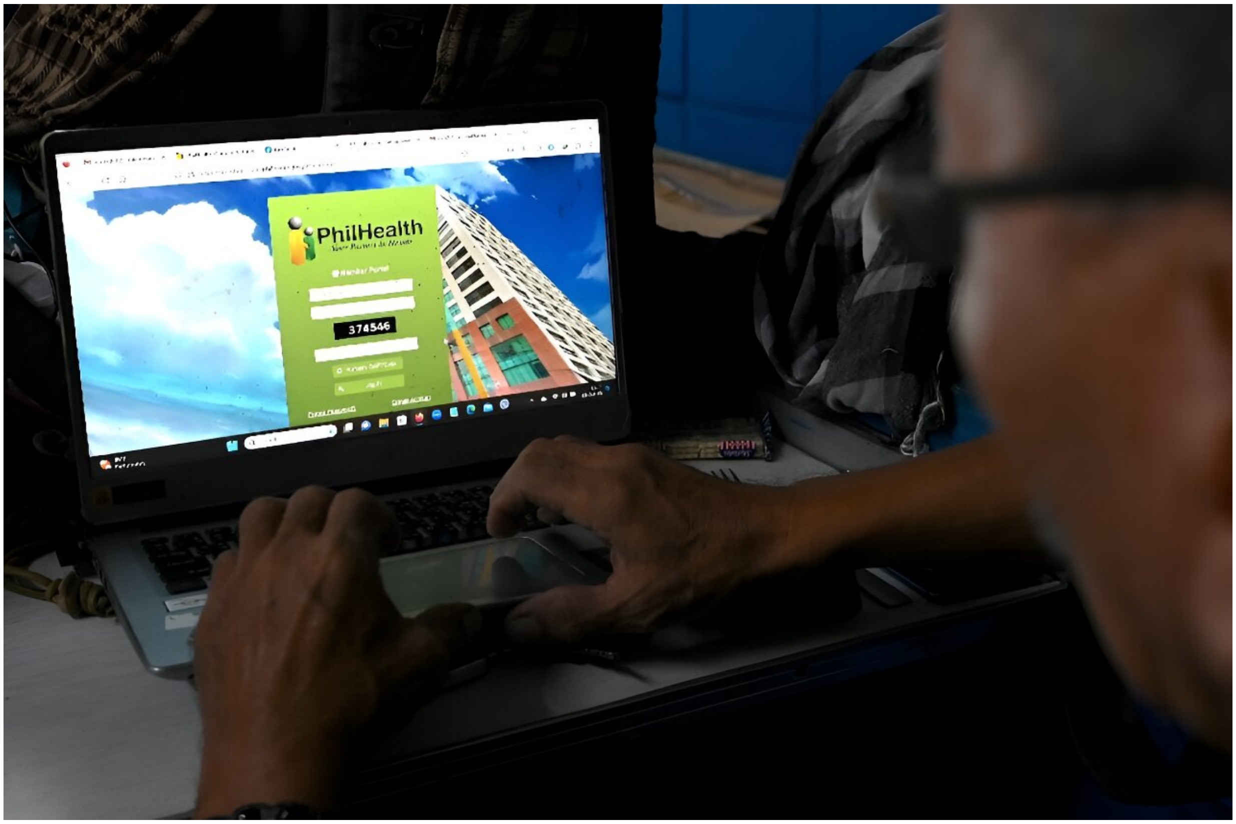
While cybercrime may conjure up images of lawless bandits operating in a world of anarchy, they are usually rational actors, according to Ram Elboim, CEO of US-based cybersecurity company Sygnia.

"It's not the Wild West, where people just shoot everywhere. Ransomware is a business. It's a huge economy," he told AFP during a London visit.

Elboim's company responds to desperate requests from clients under attack, often Fortune 500 companies, by setting up a team and jetting in to take on the criminals.

'Gun to your business'

Integral to this team are the negotiators, who use their experience of dealing with "real-world" criminals to act as a go-between with online crooks, either helping foil the attack, or working out a price if all else fails.



In a ransomware attack, gangs, sometimes linked to the state, hack into networks and demand payment either to unlock the system or prevent the release of top-secret data.

"Usually we get a call, usually it happens on a weekend or the middle of the night. This is the time where organizations let down their awareness," said Elboim.

The first tasks are to understand the nature of the attack, how the attacker got into the network, what systems are down, how to contain the spread and recover any lost data.

"Then there is a negotiation piece," said Elboim, a former member of Israel's military intelligence unit known as "8200".

"You're talking with a criminal—it's not a criminal who pulls a gun to your head, but there's a criminal holding a gun to your business.

"Usually, we advise you to start negotiations as soon as possible.

"If your only goal is to reduce the price from $50 million to $48 million then... just a good salesperson can do that.

"But usually attackers have some kind of a deadline, pay within 72 hours. The goal of the negotiation is to allow yourself more time to recover."

Another goal is to understand what the attackers are looking for and if you can attribute the attack to a specific group.

This is when the negotiators' expertise comes to the fore, setting up a channel of communication—usually via a chat app or email—and squeezing information from the criminals.

"It's not as if the attacker will give you information freely," said Elboim.

In the worst-case ranswomware scenario, when the system appears lost and with crucial data about to be leaked, many institutions have to decide whether to pay the criminals.

Great reward

In the best-case scenario, "we drag on the negotiations" for long enough and glean enough information to kick out the attackers and retrieve the data.

"After a few days of this game, the organization can just... tell the hacker 'I'm not paying, do whatever you want'."

In the worst case, when the system appears lost and with crucial data about to be leaked, many institutions then have to decide whether to pay.

"Some organizations do not want to pay on principal. In some cases, the organization is willing to pay but not willing to pay so much," with negotiators then haggling over a price.

Even if they pay the ransom and the network is decrypted, it is not plain sailing but rather the beginning of a long recovery process.

Attackers may promise not to attack again for a certain period of time, but there is no guarantee that the network is safe.

"We even had one case where we had a discussion with one attacker and he says 'okay, I move away' and then another came in and it's for sure they exchanged information, they knew everything the first one did," recalled Elboim.

But the rewards for a successful mission are great, he added.

"We had an attack... and the entire company was out, and this is a multinational organization."

After repelling the attackers, "one of the guards at the entrance stopped us and said, 'Thank you for rescuing my work, now, I will not be hungry'.

"This is one of the most satisfying moments you can have."

Citation: Stuck in cyberattack nightmare? Call the negotiators (2024, February 20) retrieved 8 May 2024 from https://techxplore.com/news/2024-02-stuck-cyberattack-nightmare.html