


International investigation disrupts the world's most harmful cyber crime group

 nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group

The National Crime Agency is today, Tuesday 20 February, revealing details of an international disruption campaign targeting LockBit, the world's most harmful cyber crime group.

Today, after infiltrating the group's network, the NCA has taken control of LockBit's services, compromising their entire criminal enterprise.

LockBit have been in operation for four years and during that time, attacks utilising their ransomware were prolific. LockBit ransomware attacks targeted thousands of victims around the world, including in the UK, and caused losses of billions of pounds, dollars and euros, both in ransom payments and in the costs of recovery. The group provided ransomware-as-a-service to a global network of hackers or 'affiliates', supplying them with the tools and infrastructure required to carry out attacks.

When a victim's network was infected by LockBit's malicious software, their data was stolen and their systems encrypted. A ransom would be demanded in cryptocurrency for the victim to decrypt their files and prevent their data from being published.

The NCA has taken control of LockBit's primary administration environment, which enabled affiliates to build and carry out attacks, and the group's public-facing leak site on the dark web, on which they previously hosted, and threatened to publish, data stolen from victims. Instead, this site will now host a series of information exposing LockBit's capability and operations, which the NCA will be posting daily throughout the week.

The Agency has also obtained the LockBit platform's source code and a vast amount of intelligence from their systems about their activities and those who have worked with them and used their services to harm organisations throughout the world.

Some of the data on LockBit's systems belonged to victims who had paid a ransom to the threat actors, evidencing that even when a ransom is paid, it does not guarantee that data will be deleted, despite what the criminals have promised.

The NCA, working closely with the FBI, and supported by international partners from nine other countries, have been covertly investigating LockBit as part of a dedicated taskforce called Operation Cronos.

LockBit had a bespoke data exfiltration tool, known as Stealbit, which was used by affiliates to steal victim data. Over the last 12 hours this infrastructure, based in three countries, has been seized by members of the Op Cronos taskforce, and 28 servers belonging to LockBit affiliates have also been taken down.

The technical infiltration and disruption is only the beginning of a series of actions against LockBit and their affiliates. In wider action coordinated by Europol, two LockBit actors have been arrested this morning in Poland and Ukraine, over 200 cryptocurrency accounts linked to the group have been frozen.

The US Department of Justice has announced that two defendants responsible for using LockBit to carry out ransomware attacks have been criminally charged, are in custody, and will face trial in the US.

The US has also unsealed indictments against two further individuals, who are Russian nationals, for conspiring to commit LockBit attacks.

As a result of our work, the NCA and international partners are in a position to assist LockBit victims. The Agency has obtained over 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.

FBI and Europol will be supporting victims elsewhere.

National Crime Agency Director General, Graeme Biggar said: “This NCA-led investigation is a ground-breaking disruption of the world’s most harmful cyber crime group. It shows that no criminal operation, wherever they are, and no matter how advanced, is beyond the reach of the Agency and our partners.

“Through our close collaboration, we have hacked the hackers; taken control of their infrastructure, seized their source code, and obtained keys that will help victims decrypt their systems.

“As of today, LockBit are locked out. We have damaged the capability and most notably, the credibility of a group that depended on secrecy and anonymity.

“Our work does not stop here. LockBit may seek to rebuild their criminal enterprise. However, we know who they are, and how they operate. We are tenacious and we will not stop in our efforts to target this group and anyone associated with them.”

Home Secretary James Cleverly said: “The National Crime Agency’s world leading expertise has delivered a major blow to the people behind the most prolific ransomware strain in the world.

“The criminals running LockBit are sophisticated and highly organised, but they have not been able to escape the arm of UK law enforcement and our international partners.

“The UK has severely disrupted their sinister ambitions and we will continue going after criminal groups who target our businesses and institutions.”

U.S. Attorney General Merrick B. Garland said: “For years, LockBit associates have deployed these kinds of attacks again and again across the United States and around the world. Today, U.S and U.K. law enforcement are taking away the keys to their criminal operation.

“And we are going a step further - we have also obtained keys from the seized LockBit infrastructure to help victims decrypt their captured systems and regain access to their data. LockBit is not the first ransomware variant the U.S. Justice Department and its international partners have dismantled. It will not be the last.”

FBI Director Christopher A. Wray said: "Today, the FBI and our partners have successfully disrupted the LockBit criminal ecosystem, which represents one of the most prolific ransomware variants across the globe.

"Through years of innovative investigative work, the FBI and our partners have significantly degraded the capabilities of those hackers responsible for launching crippling ransomware attacks against critical infrastructure and other public and private organizations around the world. This operation demonstrates both our capability and commitment to defend our nation's cybersecurity and national security from any malicious actor who seeks to impact our way of life. We will continue to work with our domestic and international allies to identify, disrupt, and deter cyber threats, and to hold the perpetrators accountable."

The NCA leads the UK law enforcement response to tackling cyber crime, disrupting offenders where possible by enabling criminal justice outcomes, and also through a broad range of other means including online disruption, sanctions, travel bans, and working with partners like NCSC to ensure technology is secure and safe by design.

The NCA's National Cyber Crime Unit also works with a network of Regional Cyber Crime Units based in the nine Regional Organised Crime Units (ROCU) of England and Wales. This operation developed from work by the South West ROCU, and continues to be supported by personnel there.

Public engagement is key to this response so it is vital that organisations report if they are the victim of a ransomware attack. The earlier people report, the quicker the NCA and partners are able to assess new methodologies and limit the damage they can do to others.

If you are in the UK, you should use the Government's [Cyber Incident Signposting Site](#) as soon as possible for direction on which agencies to report your incident to.

20 February 2024

© Crown Copyright