Browne Jacobson

LockBit unlocked: International taskforce takes down major cyber criminal organisation

27 February 2024

International law enforcement, involving the FBI and Europol, led by the National Crime Agency (NCA) **infiltrated the website of major cyber criminal organisation, LockBit**, this month as part of a dedicated taskforce named 'Operation Cronos'.

The large scale operation involved seizing the site's infrastructure in three countries, taking down 28 servers, multiple arrests and criminal charges across the globe and the freezing of over 200 cryptocurrency accounts.

Emerging around 2019, LockBit provide services to allow individuals and organisations to carry out ransomware attacks. These attacks encrypt the victim's network and retain their data until the cryptocurrency ransom is paid. Although the group is believed to be based in Russia, LockBit has previously stated that it is "located in the Netherlands, completely apolitical and only interested in money".

The UK's National Cyber Security Centre stated that LockBit's software was the 'most deployed ransomware variant' in 2022 and the NCA referred to the group as 'the world's most harmful cyber crime group'. It has been involved in cyber attacks such as that on the Royal Mail, disrupting their international delivery services and has targeted more than 2000 victims and cost billions across the world, through demands for ransom and the costs spent on recovery.

In control of the site, the NCA left a message to notify visitors that it had been taken over and expressed their plans to use it to post information about LockBit. They retrieved the source code and insight into the group's systems and the individuals that have worked with them. The taskforce also obtained many decryption keys to assist victims with recovering their data.

They have vowed to continue to tackle cyber attack's and have highlighted the need for the public to report where they experience a ransomware attack, to continue the development of strategies and prevent further damage:

"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." Graeme Biggar, National Crime Agency Director General

What does this mean for insurers?

Whilst this development may reduce the number of ransomware attacks, and in turn ransomware claims, in the interim, it is clear that this triumph does not mark the end of ransomware attacks:

"LockBit is not the first ransomware variant the U.S. Justice Department and its international partners have dismantled. It will not be the last." - U.S. Attorney General Merrick B. Garland

Further, a representative from LockBit has reportedly provided a statement in Russian declaring that it has backup servers unaffected by the law enforcement action.

Recent figures show that in the fourth quarter of 2023, there were nearly 70% more ransomware incidents and 34% more active ransomware groups than in the same quarter of 2022. A greater increase in such attacks has been witnessed in industries significantly

impacted by business interruption, such as the Transportation, Logistics, and Storage industries, demonstrating the continuing need for insurance coverage for such businesses.

To balance providing adequate coverage, whilst managing the risk, insurers are advised to ensure that policyholders have measures in place to minimise cyber risks and continue to maintain and update their cyber security processes. It is estimated that over $1.1 billion was paid in ransomware payments alone last year and, whilst payments by insurers may be used to fund ransoms, it has been demonstrated that even where such ransom is paid, the stolen data is often still published or remains encrypted.

Previous

Parametric flood policies - Insurers no longer in uncharted waters?

Contents

Key contact

Tim Johnson

Partner

tim.johnson@brownejacobson.com

+44 (0)115 976 6557

Related expertise

Services

Cyber liability and data security insurance

Financial service and insurance advisory

Policy drafting and distribution