Seized ransomware network LockBit rewired to expose hackers to world

Publication Date: 2024-02-20

Author: Alex Hern

Section: Technology

Tags: Cybercrime, NCA (National Crime Agency), Internet, FBI, Malware, Data and computer security, Crime, news

Article URL: https://www.theguardian.com/technology/2024/feb/20/uk-and-fbi-lock-cybercrime-group-out-of-lockbit-website

The entire “command and control” apparatus for the ransomware group LockBit is now in possession of law enforcement, the UK’s National Crime Agency has revealed, after it emerged that it had seized the criminal gang’s website in a coordinated international operation. The flood of data hacked back from the hackers has already led to four arrests, and the authorities promised on Tuesday to repurpose the technology to expose the group’s operations to the world. The joint operation, between the NCA, the FBI, Europol and a coalition of international police agencies, was revealed with a post on LockBit’s own website, which read: “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 taskforce Operation Cronos.” Europol said that two LockBit actors had been arrested in Poland and Ukraine, and that a further two defendants, thought to be affiliates, had been arrested and charged in the US. Two more individuals have been named, and are Russian nationals still at large. Authorities have also frozen more than 200 cryptocurrency accounts linked to the criminal organisation. Disruption to the LockBit operation is significantly greater than first revealed. As well as taking control of the public-facing website, the NCA seized LockBit’s primary administration environment, the infrastructure that allowed it to manage and deploy the technology that it used to extort businesses and individuals around the world. “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,” said Graeme Biggar, the NCA’s director general. “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.” The organisation is a pioneer of the “ransomware as a service” model, whereby it outsources the target selection and attacks to a network of semi-independent “affiliates”, providing them with the tools and infrastructure and taking a commission on the ransoms in return. As well as ransomware, which typically works by encrypting data on infected machines and demanding a payment for providing the decryption key, LockBit copied stolen data and threatened to publish it if the fee was not paid, promising to delete the copies on receipt of a ransom. However, the NCA said that promise was false. Some of the data it discovered on LockBit’s systems belonged to victims who had paid the ransom. The home secretary, James Cleverly, said: “The NCA’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 “hack back” campaign also recovered more than 1,000 decryption keys earmarked for victims of LockBit’s attacks, and will be contacting those victims to aid them in the recovery of encrypted data. In a

blogpost last month, the former National Cybersecurity Centre boss, Ciaran Martin, said the involvement of Russian hackers in cybercrime undercut many common tactics of law enforcement. “Impose costs when we can: there are things we can do to harass and harry cybercriminals,” he warned. “But this will not be a strategic solution for as long as the Russia safe haven exists.”