Russia-based LockBit ransomware hackers attempt comeback

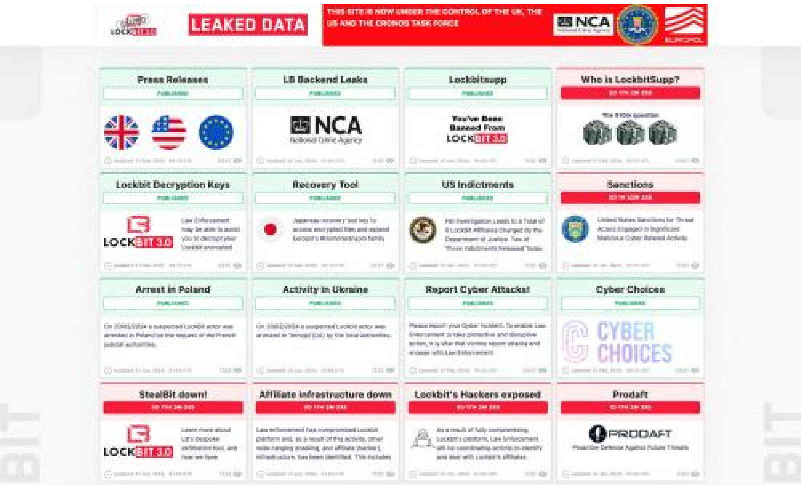
Publication Date: 2024-02-26

Author: Dan Milmo

Section: Technology

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

Article URL: https://www.theguardian.com/technology/2024/feb/26/russian-based-lockbit-ransomware-hackers-attempt-comeback



THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE

The LockBit ransomware gang is attempting a comeback days after its operations were severely disrupted by a coordinated international crackdown. The Russia-based group has set up a new site on the dark web to advertise a small number of alleged victims and leak stolen data, as well as releasing a rambling statement explaining how it had been hobbled by the UK’s National Crime Agency, the FBI, Europol and other police agencies in an operation last week. The group said law enforcement had hacked its former dark web site using a vulnerability in the PHP programming language, which is widely used to build websites. “All other servers with backup blogs that did not have PHP installed are unaffected and will continue to give out data stolen from the attacked companies,” said the statement, which was published in English and Russian. The statement also referred to “my personal negligence and irresponsibility”, declared an intention to vote for Donald Trump in the US presidential election and offered a job to whoever hacked LockBit’s main site. LockBitSupp, the group’s administrator and presumed author of the statement, does not live in the US, according to law enforcement. The agencies involved in the LockBit operation have also added that “LockBitSupp has engaged with law enforcement”. In a statement, the NCA said LockBit remains “completely compromised”. A spokesperson said: “We recognised LockBit would likely attempt to regroup and rebuild their systems. However, we have gathered a huge amount of intelligence about them and those associated to them, and our work to target and disrupt them continues.” The US this month charged two Russian nationals with deploying LockBit ransomware against companies and groups around the world. Police in Poland made an arrest, and in Ukraine police arrested a father and son they said carried out attacks using LockBit’s malicious software. The message on the new LockBit site also threatened to attack US government sites more often. Its revamped website, launched on Saturday, showed a number of purported hacking victims. Rafe Pilling, director of threat research at the cybersecurity firm Secureworks, said the statement and website showed “the real, genuine LockBit group attempting to re-establish their operations”. However, he said LockBit would still have to overcome reputational damage caused by the international operation, which not only involved taking control of the group’s public-facing website but also resulted in the seizure of its primary administration environment, or the infrastructure that deploys its technology. LockBit works under a ransomware-as-a-service model, where it leases out its software to criminal affiliates in exchange for a cut of any ransomware payments. Pilling said LockBit would have to convince affiliates to use its services despite the public relations hit from the international law enforcement operation. “There will be a knock to their reputation within the criminal community as a result of the NCA-led action,” he said. Ransomware attacks typically involve hackers entering a target’s computer system and paralysing it with malware, which encrypts files and makes them inaccessible. A new trend in attacks involves assailants extracting data from the IT system, such as staff or customer details. The gang then asks for payment in cryptocurrency, usually bitcoin, to unlock the files or to delete their copy of the stolen data. Ransomware victims last year paid out a record $1.1bn (£870m) to assailants.