Dmitry Khoroshev named as alleged leader of ransomware gang LockBit

Publication Date: 2024-05-07

Author: Alex Hern

Section: Technology

Tags: Cybercrime, NCA (National Crime Agency), Crime, Russia, Internet, news

Article URL: https://www.theguardian.com/technology/article/2024/may/07/dmitry-khoroshev-named-as-alleged-leader-of-ransomware-gang-lockbit

The alleged leader of what was once the world's largest ransomware outfit, LockBit, has been named as Russian national Dmitry Khoroshev by the UK's National Crime Agency (NCA), after the seizure of the criminal gang's infrastructure. Khoroshev, who lived his online life under the name LockBitSupp, has been sanctioned by the UK, US and Australia as a result of the unmasking. He was so certain of his anonymity that he once offered a $10m (£8m) reward to anyone who could reveal his identity. The US government is now offering a reward of up to $10m for anyone who can share information leading to his arrest or conviction. LockBit was seen as one of the world's most dangerous ransomware groups and its high-profile victims included delivery firm Royal Mail and aerospace company Boeing. In February, LockBit's entire "command and control" apparatus was seized by law enforcement after a joint international operation. Graeme Biggar, the director general of the National Crime Agency (NCA), said: "These sanctions are hugely significant and show that there is no hiding place for cybercriminals like Dmitry Khoroshev, who wreak havoc across the globe. He was certain he could remain anonymous, but he was wrong. "We know our work to disrupt LockBit thus far has been extremely successful in degrading their capability and credibility among the criminal community. The group's attempt at rebuilding has resulted in a much less sophisticated enterprise with significantly reduced impact." UK security minister Tom Tugendhat said: "Cybercriminals think they are untouchable, hiding behind anonymous accounts as they try to extort money from their victims. "By exposing one of the leaders of LockBit, we are sending a clear message to these callous criminals. You cannot hide. You will face justice." But Khoroshev, who is believed to be resident in Russia, is likely to remain at large for some time. The Russian state has never formally extradited cybercriminals, and the freezing of relations after its full-scale invasion of Ukraine in 2022 led to a near-total cessation of all enforcement action domestically. The NCA and its international partners have hit LockBit commercially, however, by releasing damaging information taken from the group's own servers. The criminal gang operated on an "affiliate" basis, charging a commission to allow others to carry out hacks using its tools. But the NCA said its data shows that more than half the affiliates it could identify were never paid any money from their criminality – despite paying thousands to be a member, and attracting criminal liability from their hacking activities. The gang also broke its promise to victims to delete stolen data if they paid the ransom, the NCA said, citing the discovery of supposedly deleted information on the group's servers.