Ransomware groups warned there is no money in attacking British state

Publication Date: 2024-03-12

Author: Alex Hern

Section: Technology

Tags: Cybercrime, Internet, Hacking, British Library, news

Article URL: https://www.theguardian.com/technology/2024/mar/12/ransomware-groups-warned-there-is-no-money-in-attacking-british-state

BRITISH LIBRARY BRITISH LIBRARY BRITISH LIBRARY BRITISH LIBRARY BRITISH
Welcome

Ransomware gangs have been warned that there is no money in attacking the British state, after the British Library revealed that it weathered a damaging cyber-attack without paying – or even speaking to – the hackers behind it. The library, which was hit by a ransomware attack in October 2023, issued the warning as part a review of its response to the incident. “The library has not made any payment to the criminal actors responsible for the attack, nor engaged with them in any way,” it said. “Ransomware gangs contemplating future attacks such as this on publicly-funded institutions should be aware that the UK’s national policy, articulated by NCSC [National Cyber Security Centre], is unambiguously clear that no such payments should be made.” State institutions around the world are common targets for ransomware gangs, who operate by encrypting or stealing sensitive data before extorting a ransom to delete it or restore access. Councils, hospitals, schools and universities are all favoured, with reputations for poor cybersecurity and operational needs to restore functionality rapidly, leading to a reputation for rapid payment of ransoms. UK government policy has long been to discourage the payment of ransoms, but the British Library incident report is a major sign that the National Cyber Security Centre, the GCHQ subsidiary tasked with tackling the ransomware threat nationally, is focusing increased efforts on deterring ransomware attacks before they happen, in part by cutting off the flow of funds. The library is still not operating at full capacity, with research services remaining “incomplete” five months after they were first hit. The criminal gang responsible stole 600GB of data, the incident report reveals, and when it was clear that no payment would be proffered, dumped it on the dark web. But the most damage was done before the attack was even completed: in order to make it harder to recover systems and track the attackers, they destroyed some servers outright. “While we have secure copies of all our digital collections – both born-digital and digitised content, and the metadata that describes it – we have been hampered by the lack of viable infrastructure on which to restore it,” the library says. Efforts to fight ransomware gangs globally hit a wall when Russia launched its full-scale invasion of Ukraine, and subsequently disengaged from international cooperation into fighting cybercrime. While it had rarely been a full and enthusiastic partner in investigations, the Russian state still came down on the worst criminals – an important threat in a country where extradition is flatly illegal. As a result, international law enforcement has turned to other approaches, including embracing so-called “hack back” operations designed to disrupt and expose the actions of ransomware gangs who might otherwise be out of reach. Last month, a coalition of police seized the command and control apparatus of LockBit, the largest ransomware gang currently operating, which had previously run a $100m annual cybercrime operation. On Monday, however, the government was accused of an “ostrich strategy” in response to the ransomware threat, after it responded to the Joint Committee on the National Security Strategy’s year-long inquiry into ransomware by insisting “all is well”, Margaret Beckett, the committee’s chair, said. “It is ever clearer that government does not know the extent or costs of cyber-attacks across the country – though we’re the third most cyber-attacked country in the world – nor does it have any intention of commensurately upping the stakes or resources in response,” Beckett added.