Rhysida, the new ransomware gang behind British Library cyber-attack

Publication Date: 2023-11-24

Author: Dan Milmo

Section: Technology

Tags: Cybercrime, British Library, Data and computer security, Hacking, Russia, Cryptocurrencies, Libraries, news

Article URL: https://www.theguardian.com/technology/2023/nov/24/rhysida-the-new-ransomware-gang-behind-british-library-cyber-attack

A new name was added to the cyber-rogues' gallery of ransomware gangs this week after a criminal group called Rhysida claimed responsibility for an attack on the British Library. The library confirmed that personal data stolen in a cyber-attack last month has appeared for sale online. While the name behind the attack might be relatively new, the criminal technique is not. Ransomware gangs render an organisation's computers inaccessible by infecting them with malicious software – malware – and then demanding a payment, typically in cryptocurrency, to unlock the files. In recent years, however, in a process dubbed "double extortion", the majority of gangs steal data at the same time and threaten to release it online, which they hope will strengthen their negotiating hand. Rhysida emerged as the assailant this week by posting low-resolution images of personal information gathered in the attack online, offering the stolen data for sale on its leak site with a starting bid of 20 bitcoin, or about £590,000. Rafe Pilling, the director of threat research at cybersecurity firm Secureworks, said: "This a classic example of a double extortion ransomware attack and they are using the threat of leaking or selling stolen data as leverage to extort a payment." While the British Library is a high-profile UK victim for Rhysida – named after a type of centipede – the group is also responsible for attacks on government institutions in Portugal, Chile and Kuwait. In August, it claimed responsibility for an attack on the US hospital group Prospect Medical Holdings. US government agencies released an advisory note on Rhysida last week, stating that the "emerging ransomware variant" had been deployed against the education, manufacturing, IT and government sectors since May. The agencies said they had also seen the Rhysida gang running a "ransomware as a service" (Raas) operation, where it hires out the malware to criminals and shares any ransom proceeds. Rhysida's name is new to the public, but according to Secureworks it has emerged from a criminal operation established in 2021. Secureworks calls that group Gold Victor and it operated a ransomware scheme called Vice Society. This rebranding exercise is common among criminal gangs – they are often named after the ransomware variant they deploy – if their existing "brand" becomes excessively notorious and attracts too much attention from law enforcement. The brand is often attached at the end of the encrypted file names left after an attack, in an act that Rafe describes as leaving a "calling card". The exact identity of the Rhysida gang is not known, but Pilling assumes that it follows the pattern of similar operatives who are usually from Russia or members of the Commonwealth of Independent States, whose constituents include Russia, Belarus and Kazakhstan. "I would assume that they are probably Russian-speaking but we don't have any hard evidence," said Pilling. According to the US agencies, gangs using the Rhysida ransomware have used organisations' virtual private networks – the systems used by staff to access their employers' systems remotely – to get into systems, or

have deployed the familiar technique of phishing attacks, where victims are tricked, usually via email, into clicking on a link that downloads malicious software or tricks them into handing over details such as passwords. “These are common access techniques,” said Spilling. Once inside, the gangs typically lurk in the system for a period of time. According to Secureworks, that dwell time for attacks has fallen to less than 24 hours for cybergangs in general, compared with more than four days in 2022. This helps avoid detection. According to the US agencies document, cryptocurrency is a common form of ransom demand for Rhysida attackers, in line with the rest of the criminal hacking fraternity. A digital asset like bitcoin is popular with ransomware gangs because it is decentralised – it operates outside the conventional banking system and therefore bypasses standard checks – and transactions can be obscured, making them more difficult to track. Rhysida attackers send their ransom notes with the title “CriticalBreachDetected” in a PDF file. The note provides each recipient with a unique code and instructions to contact the group via a specialist web browser that makes communications untraceable. Paying ransomware demands in the UK is heavily frowned upon but it not illegal, unless you know – or suspect – that the proceeds are going into terrorists’ pockets. According to the National Cyber Security Centre: “Law enforcement does not encourage, endorse nor condone the payment of ransom demands.” In the US, payment of ransoms is also discouraged by the government, but an advisory note from the US Treasury in 2020 emphasised this was “explanatory only” and did “not have the force of law”. Ransomware payments are rising, according to the British cybersecurity firm Sophos. It reported that average ransomware payments have nearly doubled to £1.2m over the past year. Against this backdrop, new ransomware “brands” will continue to emerge.