Who is behind the latest wave of UK ransomware attacks?

Publication Date: 2023-09-14

Author: Dan Milmo

Section: Technology

Tags: Cybercrime, Hacking, Internet, Police, explainers

Article URL: https://www.theguardian.com/technology/2023/sep/14/who-is-behind-latest-wave-of-ransomware-attacks

The Greater Manchester police force has become the latest entity to fall victim to a now well-established form of cyberattack: the ransomware hack. GMP said on Thursday a third-party supplier holding information on its employees had been breached. It is understood that data potentially exposed in the hack included the details of officers' name badges such as ranks, photos and serial numbers. The Metropolitan police announced in August that data for officers and staff was also exposed in an attack on the same supplier. Companies and public bodies affected by ransomware attacks in the UK this year alone include the Royal Mail, outsourcing firm Capita, and the Barts Health NHS trust. The Guardian was also hit by a ransomware attack last year. What is a ransomware attack? Ransomware is malicious software inserted into an organisation's computer network. This can occur via a "phishing attack", where a staff member is tricked – often via email – into downloading the malware. The malware then encrypts the computers it has accessed, making it impossible to access their content. The criminal gang behind the attack then offers to decrypt your network in exchange for a ransom payment typically paid in cryptocurrency: hence the phrase ransomware. There is another ransomware tactic known as "double extortion", where the attacker takes data as well and uses that as leverage in negotiations, by threatening to sell it or release it into the public domain. According to the Information Commissioner's Office (ICO), the UK's data watchdog, 706 ransomware incidents were reported last year, a slight increase on the 694 reported in 2021. Have police forces been targeted deliberately? Ransomware attacks are prevalent across the public and private sector, according to Secureworks, a cybersecurity firm. "This is not a problem that affects the public sector or public sector supply chain specifically," says Rafe Pilling, a director for threat research at Secureworks. "It is happening across businesses and organisations of all shapes and sizes." He says his firm sees victims across various different sectors, with manufacturing being particularly hard hit. Nevertheless, Pilling says the attack underlines that entities where staff details can be extra sensitive – such as law enforcement bodies – need to be careful about vetting third-party suppliers who handle their data. "People need to think about the fact that sensitive data can be exposed even when it is an attack on an innocuous-seeming supplier. It can have a big knock-on effect in terms of the data that gets extracted." Who is behind these attacks? Most ransomware groups are linked to eastern Europe, former Soviet republics and Russia in particular. This year, British Airways, the BBC and Boots were targeted by an attack from the Clop group, named after the strain of ransomware they use. "There are multiple criminal gangs conducting this activity at the moment," says Pilling. "The vast majority are Russian speaking or have Russian links." Is it legal to pay a ransomware group? Paying ransomware gangs is heavily frowned upon by UK authorities. Last year the UK's data watchdog and National Cyber Security Centre clarified that they did "not encourage" the payment of ransoms – although

payments were not usually unlawful. It is, however, illegal to pay a ransom if you know – or suspect – that the proceeds are going into terrorists' pockets. Nonetheless, UK firms are making payments. Sophos, a British cybersecurity firm, estimates that the average ransomware payment by UK organisations is higher than the global average, at $2.1m (£1.7m). Do the police forces face punishment from the data regulator? The ICO is likely to investigate whether GMP and the Met selected their third-party supplier properly and carried out a proper contracting process. However, the ICO said last year it was planning to reduce the use of fines on public sector organisations for breaches of the UK's implementation of GDPR. But the supplier involved, Stockport-based Digital ID, will also be scrutinised. Digital ID makes identity cards and lanyards for a number of UK organisations including several NHS trusts and universities.