Australian law firm HWL Ebsworth hit by Russian-linked ransomware attack

Publication Date: 2023-05-02

Author: Josh Taylor

Section: Technology

Tags: Data and computer security, Privacy, Cybercrime, Internet, Malware, news

Article URL: https://www.theguardian.com/technology/2023/may/02/australian-law-firm-hwl-ebsworth-hit-by-russian-linked-ransomware-attack

The Australian commercial law firm HWL Ebsworth has fallen victim to a ransomware attack, with Russian-linked hackers claiming to have obtained client information and employee data. Late last week, the ALPHV/Blackcat ransomware group posted on its website that 4TB of company data had been hacked, including employee CVs, IDs, financial reports, accounting data, client documentation, credit card information, and a complete network map. The news was first reported by the Australian Financial Review. Blackcat was one of the top three ransomware groups targeting Australia according to a recent study by cybersecurity firm Palo Alto Networks. The group operates as a “ransomware-as-a-service” product for hire, and has been active since late 2021. Cybersecurity company Sophos said that the group had consistently targeted large organisations. Sign up for Guardian Australia’s free morning and afternoon email newsletters for your daily news roundup The group previously hacked similar customer data from real estate firm LJ Hooker late last year. Sophos said last year the attackers have broken into networks by exploiting vulnerabilities in unpatched or outdated firewall or virtual private network devices. Professional and legal services is one of the top targeted industries for such attacks, the Palo Alto study stated, with Australia the most targeted in the Asia-Pacific region. Guardian Australia has sought comment from HWL Ebsworth. After the cyber-attacks on Optus and Medibank last year, the federal government has moved to beef up cybersecurity in Australia, including more resources for the Australian federal police and the appointment of a national cybersecurity coordinator. In a speech earlier this month, the home affairs and cybersecurity minister, Clare O’Neil said the Australian government saw groups acting for financial gain as “public enemy No 1”. “These groups subvert legitimate business models for financial gain, creating online portals for ‘hacking as a service’ where anyone can purchase the tools and support necessary to conduct a cyber incident or data, especially in the form of a ransomware attack,” she said. “These groups represent a threat to our national economic life because every sector, every business that can pay, is a target.” Medibank last week refused to release the findings of an external Deloitte report into the company’s hack – which resulted in the personal information of 10 million customers being posted on the dark web – citing security concerns and saying it could put other companies at risk.