191 Australian organisations affected by the ZircoDATA Breach

riskassociates.com/blogs/191-australian-organisations-affected-by-zircodata-breach-linked-to-russian-ransomeware-gang/

May 8, 2024

A Russian-linked ransomware gang has launched a significant cyberattack impacting approximately 200 Australian organisations, including federal government agencies. This breach has exposed the data of numerous individuals, including victims of family violence and sexual assault, students, and passport holders.

As reports circulate in local media, the cyber ring known as Black Basta claims responsibility for this breach, boasting a haul totalling 395 gigabytes of sensitive data. This includes scans of passports, individual immigration identifiers, and other confidential documents allegedly looted from ZircoDATA's clients, a Victorian data management firm.

Risk Associate's Threat Intelligence platform, powered by Cyble, is a leading solution that tracks hacking rings and monitors dark web chatter for breaches. Cyble, is actively engaged in providing comprehensive support to numerous companies impacted by these breaches, it has highlighted that the precise correlation or causation between the two incidents is yet to be definitively established from a technical standpoint. This warrants further investigation and analysis into the intricate technical nuances and potential overlaps within the attack vectors and methodologies employed.

We've found 191 Australian organisations affected by the ZircoDATA hacks. This breach has had a significant impact on businesses across the country, highlighting the critical need for robust cybersecurity measures.

– *Sameer Pradhan, Cybersecurity Manager at Risk Associates*

The repercussions extend beyond organisational boundaries, affecting vital services such as Monash Health, Victoria's largest health service. Monash Health, utilizing ZircoDATA for scanning archived records, now faces the daunting task of identifying and assisting approximately 4000 affected patients. Other affected ZircoDATA clients include an Australian legal translation service and a US investment firm.

Another hacking group, Crypmans, also targeted ZircoDATA in January, according to other dark web posts and breach alerts. On Friday, it was revealed that Victoria's largest health service, Monash Health, which had been using ZircoDATA to scan archived records from family violence and sexual support units in Melbourne's east between 1970 and 1993, was also affected.

Kapil Barman, an associate at Cyble, mentioned that, the gangs seemed to exploit the same vulnerability to access ZircoDATA's systems, using Russian-language ransomware in both cases.

Despite the severity of the breach, government entities utilizing ZircoDATA's services are still in the process of assessing the extent of the impact. The Department of Home Affairs, along with other agencies, remains vigilant in investigating the matter and identifying the responsible parties, as per the Federal Government's National Cyber Security Co-ordinator.

Melbourne Polytechnic also disclosed on Friday that enrollment details of about 60,000 current and former students had been compromised in the breach. However, the information taken was considered low risk and limited to names, student ID numbers, dates of birth, and addresses.

Amidst these challenges and alarming increase in cyberattacks Risk Associates remains committed to safeguarding Australian organisations against cyber threats.

Risk Associates is steady with its award-winning Threat Intelligence platform, powered by Cyble. This cutting-edge solution serves as a beacon of security in the digital landscape, diligently tracking hacking rings and monitoring dark web chatter for potential breaches.

The content of this article was adapted from the original piece 'Russian gang behind hack exposing family violence victims, government agencies' published in The Sydney Morning Herald and authored by Sherryn Groch.