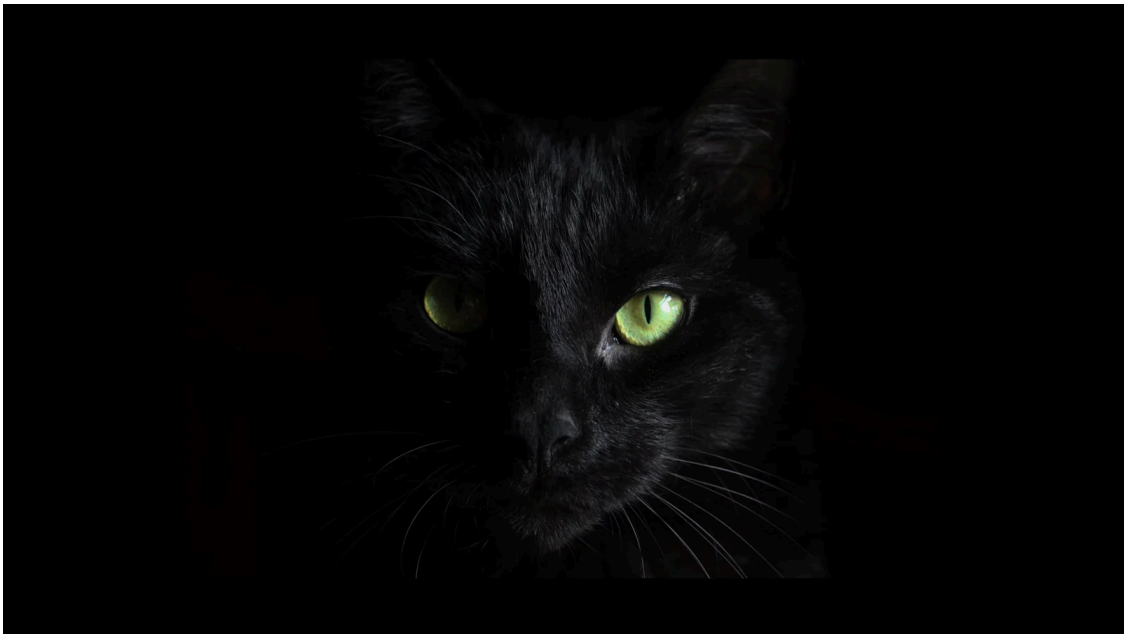
BlackCat ransomware fails to extort Australian commercial law giant

By Bill Toulas

Published: 2023-06-09 · Archived: 2026-04-05 13:15:37 UTC

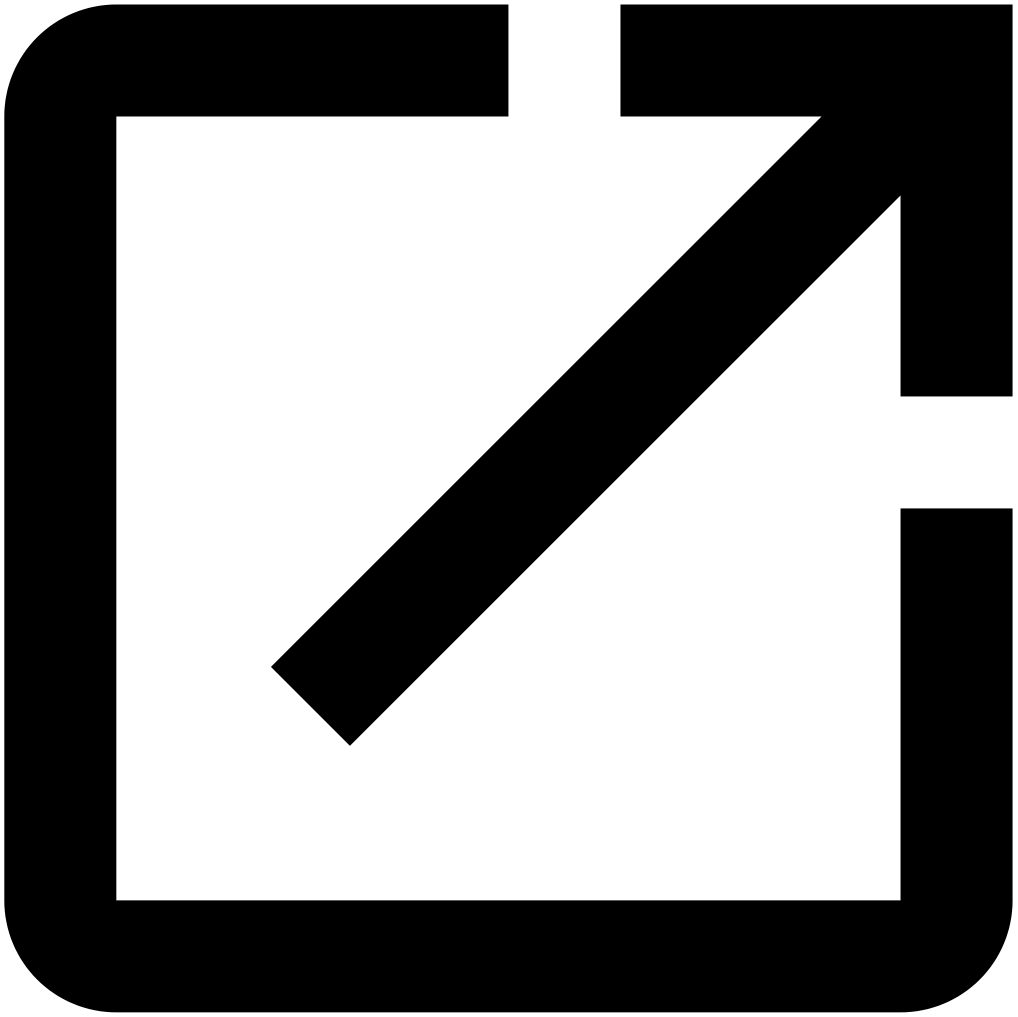


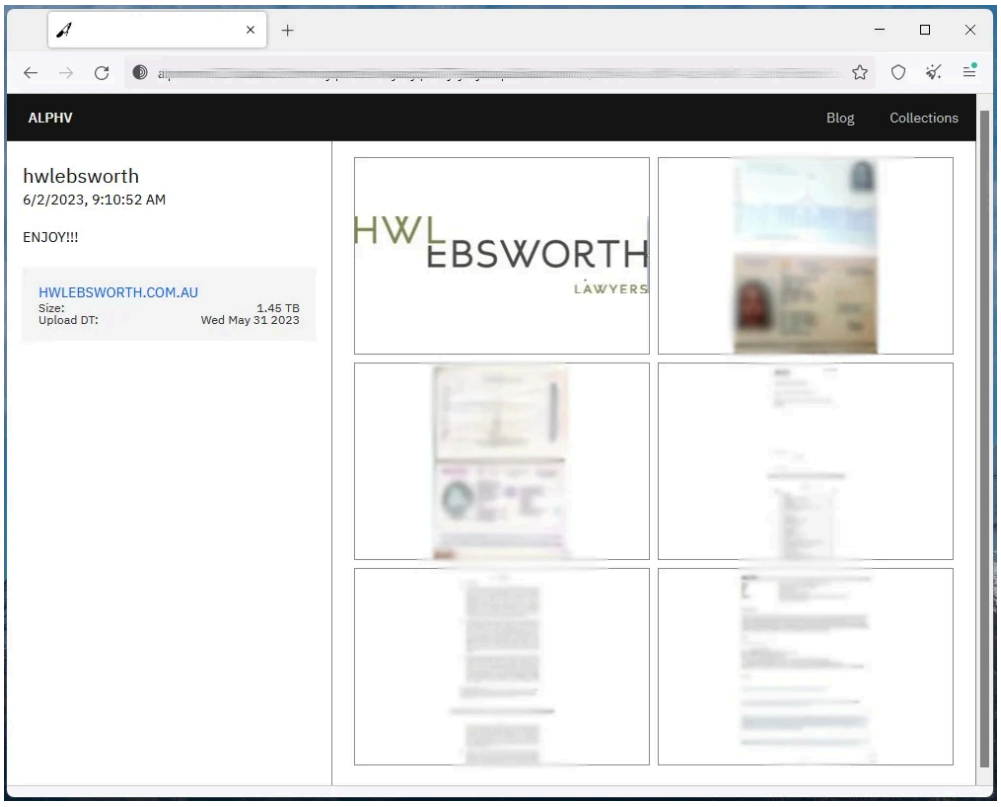
Australian law firm HWL Ebsworth confirmed to local media outlets that its network was hacked after the ALPHV ransomware gang began leaking data they claim was stolen from the company.

HWL Ebsworth is one of Australia's largest law firms, with an annual revenue of hundreds of millions of dollars, employing over 2,000 people and operating nine offices nationwide.

Last night, the ALPHV ransomware gang, also known as BlackCat, published 1.45 terabytes of data containing over a million documents allegedly stolen from the law firm's systems in April 2023. The cybercriminals are now threatening to leak more if the company doesn't meet their demands.


DIE LINKE.
0:00





HWL Ebsworth listed on BlackCat's extortion portal *(BleepingComputer)*

A spokesperson for the firm stated on ABC that they would not succumb to the threat actor's extortion demands, even if that means that they and their clients will have to suffer the consequences of a very exposing data leak.

"We take our ethical and moral duties to the community very seriously. We consider we have a fundamental civic duty to not, in any way, encourage or be seen to condone the criminal activity of extorting money by taking and threatening the publishing of other people's data," HWL Ebsworth told ABC.

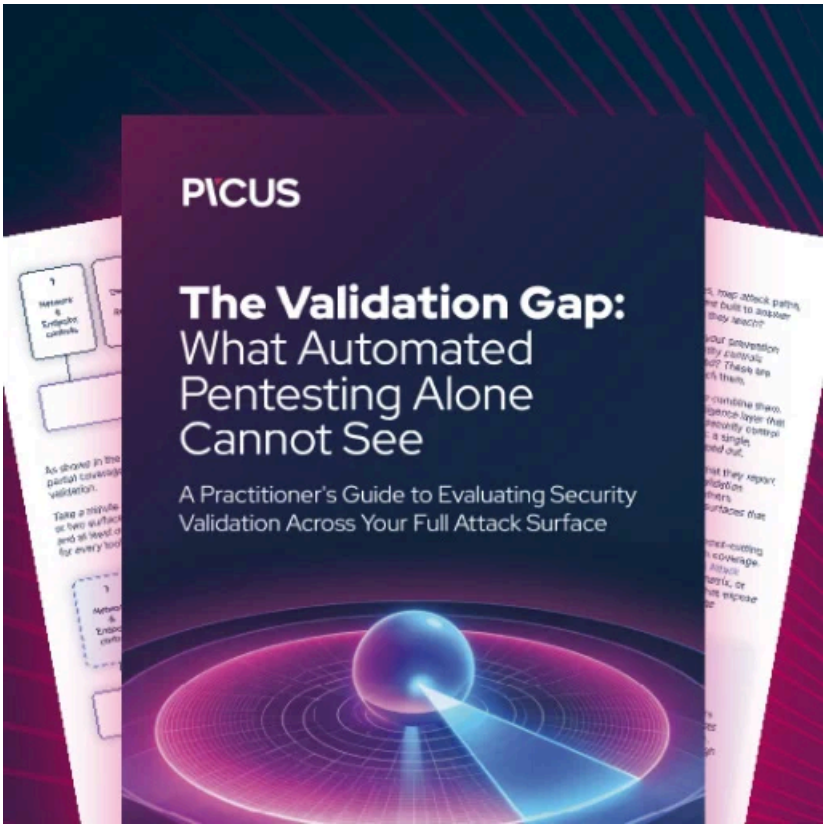
"The privacy and security of our client and employee data remains of the utmost importance. We acknowledge and understand the impact this may have, and we are communicating closely with our clients."

Because the law firm naturally had business with the public sector, too, there are worries about the leaked documents containing sensitive or confidential information relating to matters of the state.

ABC lists the ANZ banking group, the South Australian, Queensland, and ACT governments, the Environment and Human Services Department, and the Australian Taxation Office (ATO) as current or former clients of HWL Ebsworth and potentially impacted by this incident.

Unfortunately, the leaked documents on BlackCat's site are easy to explore thanks to the threat group's indexed database that allows visitors to filter search results by filename or file type.

BleepingComputer has contacted HWL Ebsworth requesting a comment on the status of its operations and the progress of its internal investigation on the validity of the leaked data, but we have yet to hear back.



[Automated Pentesting Covers Only 1 of 6 Surfaces.]

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/blackcat-ransomware-fails-to-extort-australian-commercial-law-giant/