Ransomware gang now lets you search their stolen data

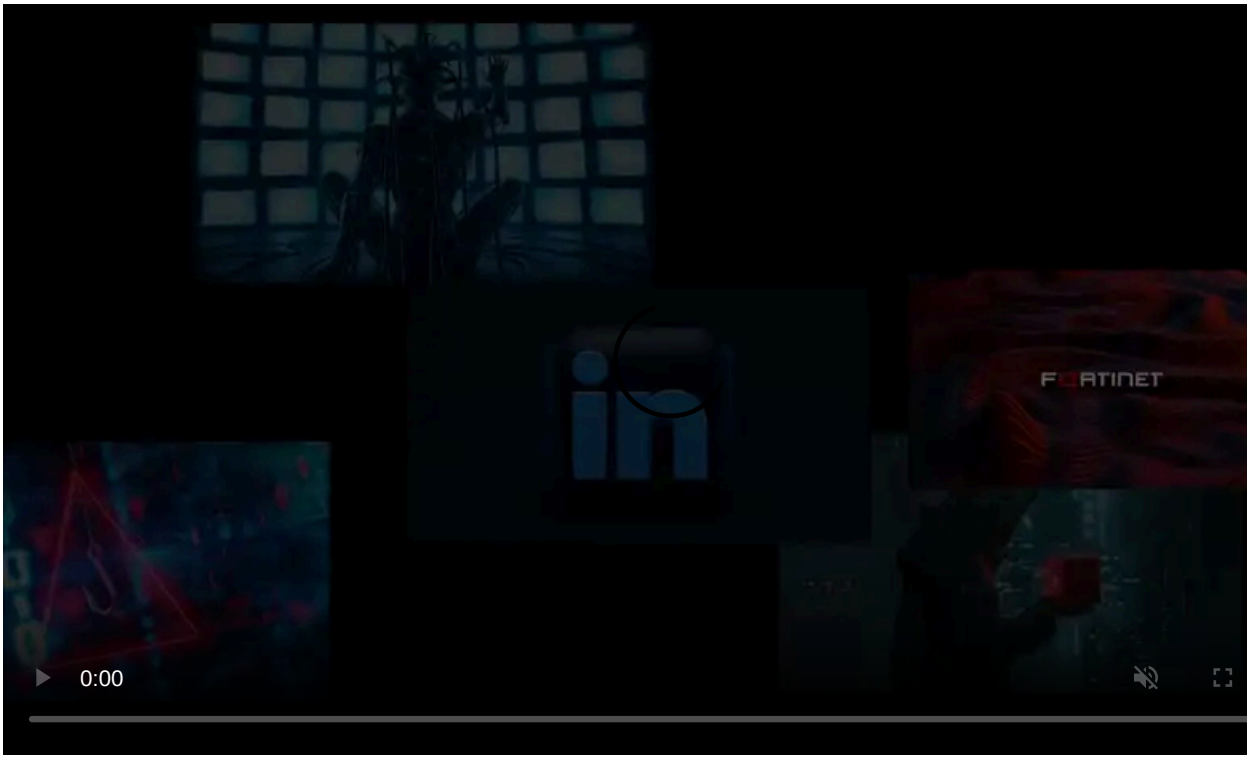
By Ionut Ilascu

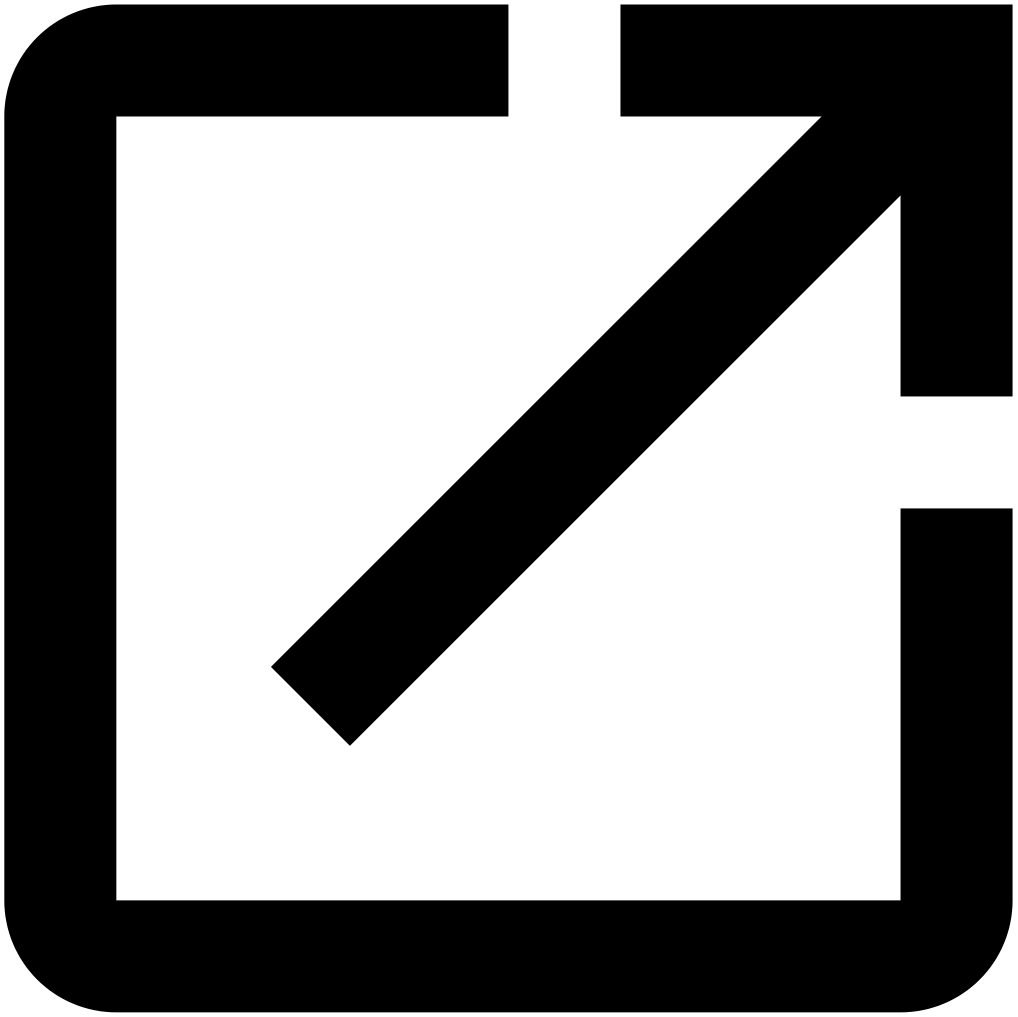
Published: 2022-07-11 · Archived: 2026-04-05 20:02:23 UTC

Two ransomware gangs and a data extortion group have adopted a new strategy to force victim companies to pay threat actors to not leak stolen data.

The new tactic consists in adding a search function on the leak site to make it easier to find victims or even specific details.

At least two ransomware operations and a data extortion gang have adopted the strategy recently and more threat actors are likely to do the same.


0:00



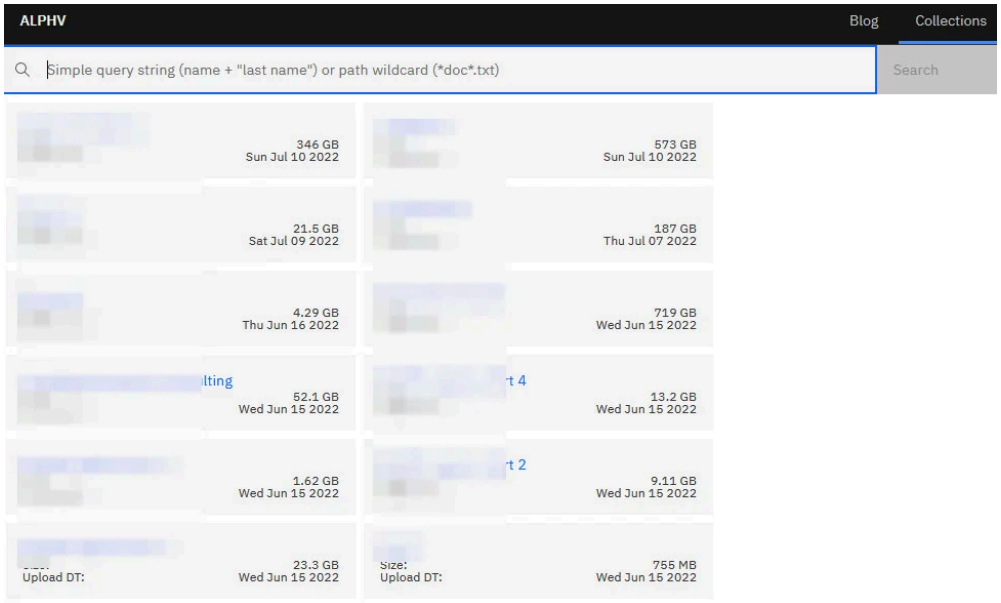
Visit Advertiser websiteGO TO PAGE

Easy finding victim data

Last week, the ALPHV/BlackCat ransomware operation announced that they created a searchable database with leaks from non-paying victims.

The hackers made it clear that the repositories have been indexed and the search works when looking for information by filename or by content available in documents and images.

The results are pulled from the “Collections” part of BlackCat’s leak site and may not have the best accuracy but it is still an evolution of the cybercriminal’s extortion strategy.

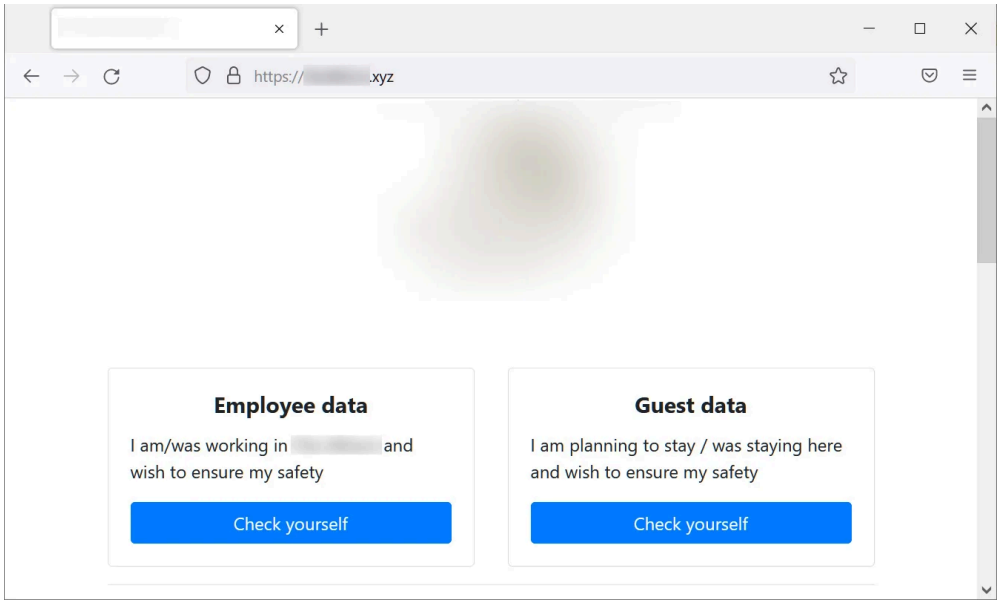


Search option on ALPHV ransomware leak site
Source: BleepingComputer

BlackCat ransomware operators claim that they do this to make it easier for other cybercriminals to find passwords or confidential information about companies.

The gang already tried this strategy in mid-June, when they created a searchable site with data allegedly stolen in an attack at a hotel and spa in Oregon.

The site allowed guests at the spa locations and employees to check if their personal information had been stolen during the ransomware attack.

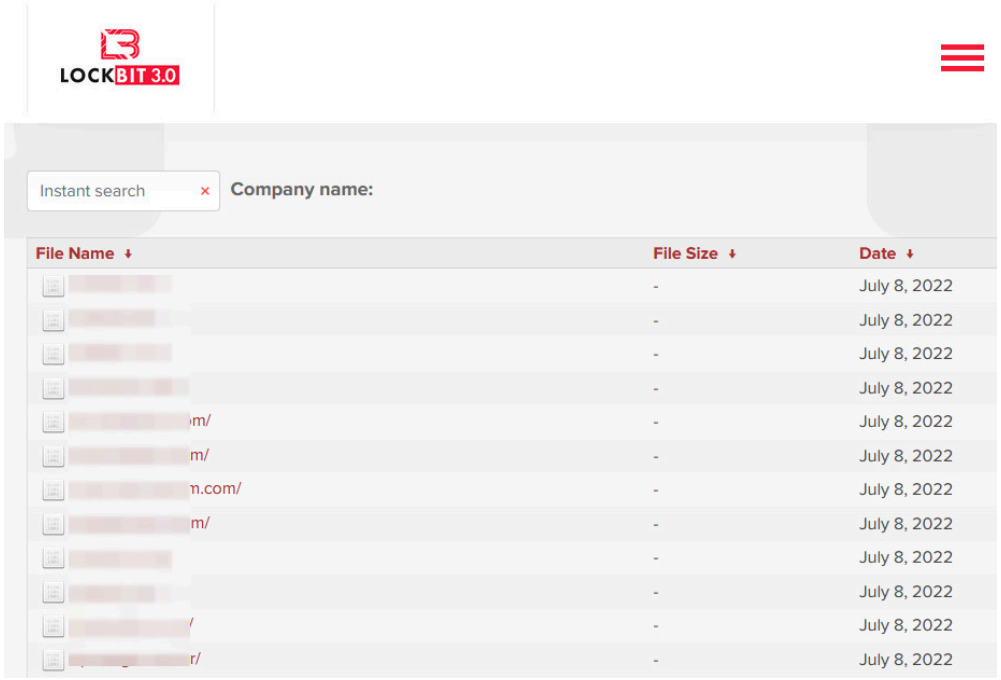


Victim's search data leak site

Source: BleepingComputer

This is a step forward in the extortion business as it puts pressure on the victim to pay the ransom and have the data removed from the web and avoid the potential risk of class action lawsuits.

Towards the end of last week, BleepingComputer noticed that LockBit offered a redesigned version of their data leak site that allowed searching for listed victim companies.



LockBit added instant search option on data leak site

Source: BleepingComputer

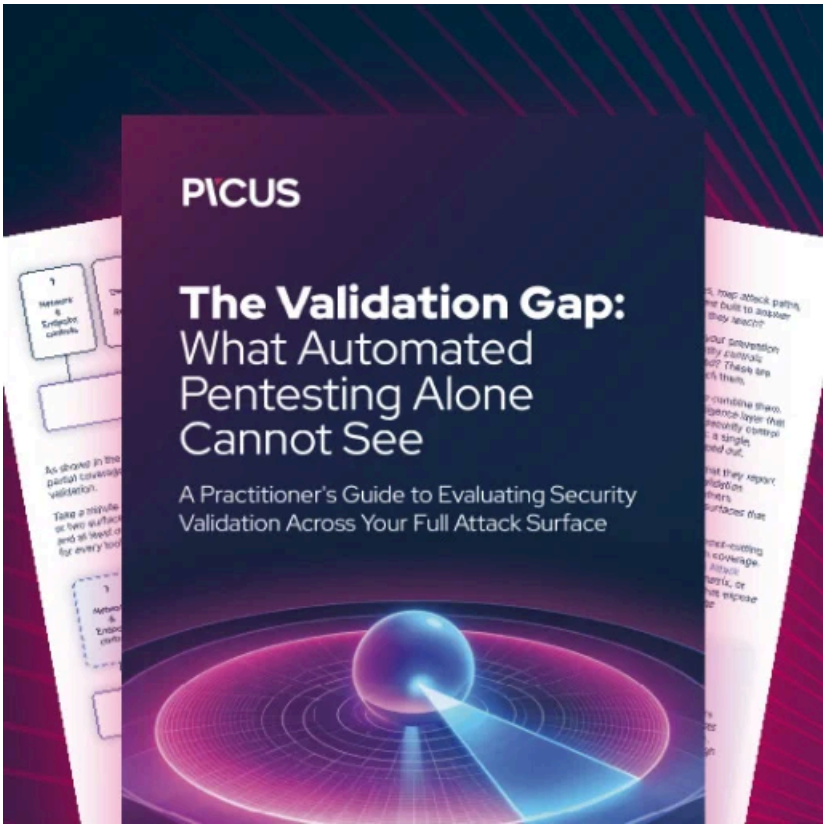
LockBit's search is not as advanced as the variant touted by BlackCat, and it is limited to only finding victims by name.

However, even in this basic form, the gang's implementation of the search function still makes it easier to locate on their leak site data from specific companies.

Another leak site that has implemented a search function is the one published by the Karakurt data extortion gang. BleepingComputer's attempts to use the option showed that it did not work properly, though.

Search bar on Karakurt data extortion gang's site
Source: BleepingComputer

Data extortionists are just starting to explore the search feature. It is unclear if making stolen data searchable is a successful tactic but with multiple extortionist gangs adopting it, the option seems to be an attractive one.



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/ransomware-gang-now-lets-you-search-their-stolen-data/