Ransomware gang creates site for employees to search for their stolen data

By Lawrence Abrams

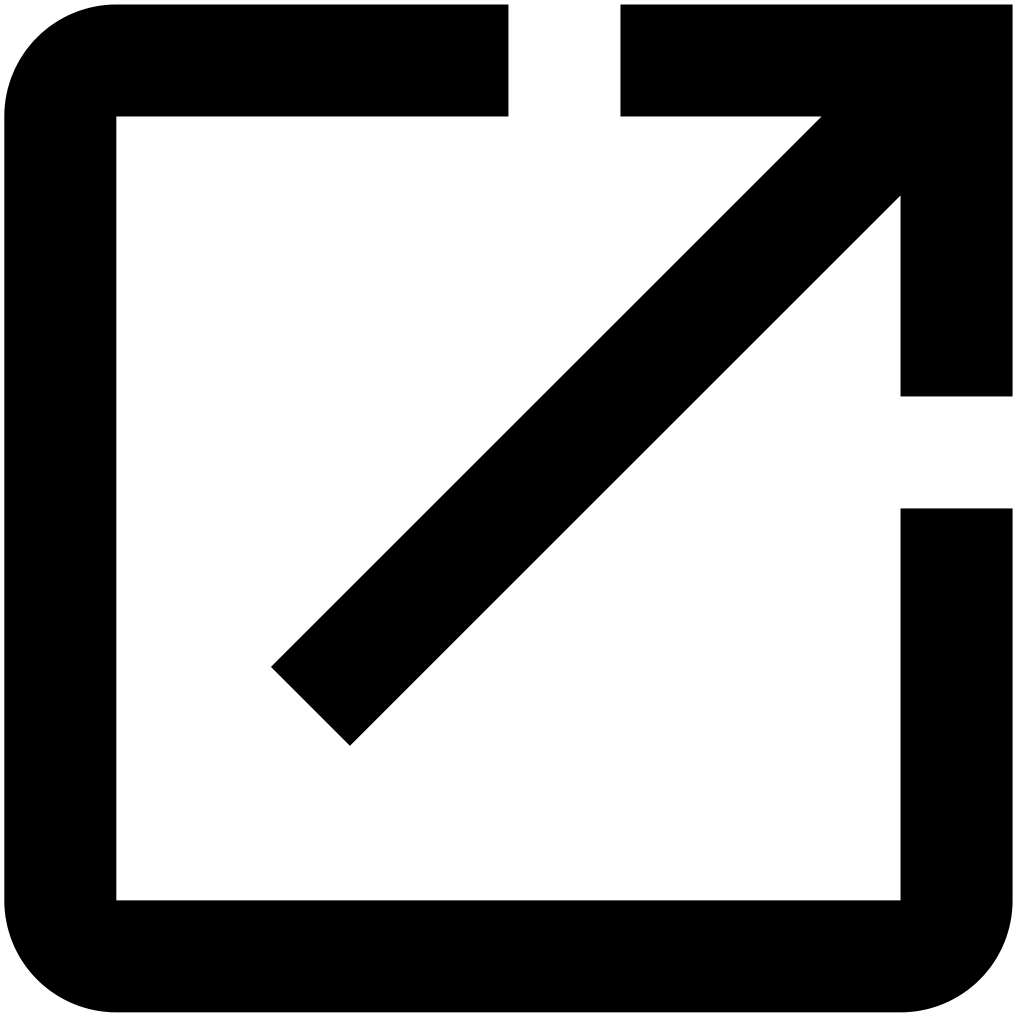
Published: 2022-06-14 · Archived: 2026-04-05 12:35:42 UTC

The ALPHV ransomware gang, aka BlackCat, has brought extortion to a new level by creating a dedicated website that allows the customers and employees of their victim to check if their data was stolen in an attack.

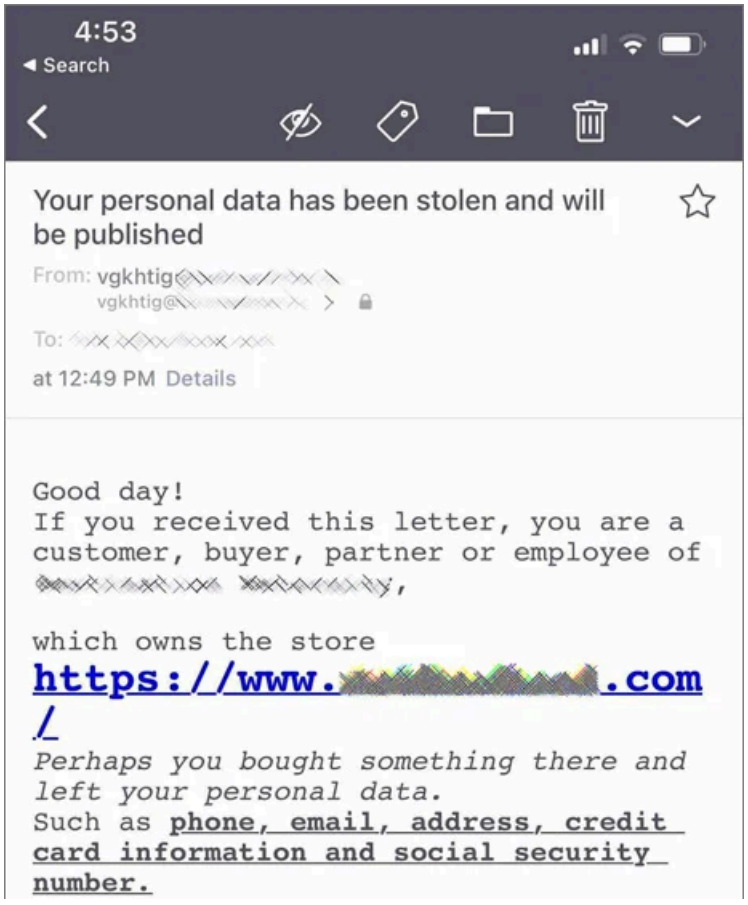
When ransomware gangs conduct attacks, they quietly steal corporate data. After harvesting everything of value, the threat actor starts to encrypt devices.

The stolen data is then used in double-extortion schemes, where the hackers demand a ransom payment to deliver a decryptor and prevent the public release of corporate data.


DIE LINKE.
0:00



To pressure victims into paying, ransomware gangs create data leak sites where they slowly release portions of the stolen data or email customers and employees warning them that their info was stolen.



Clop ransomware gang emailing a victim's customer

However, these extortion techniques do not always work and companies simply decide not to pay even though their corporate, employee, and customer data is at risk of being leaked.

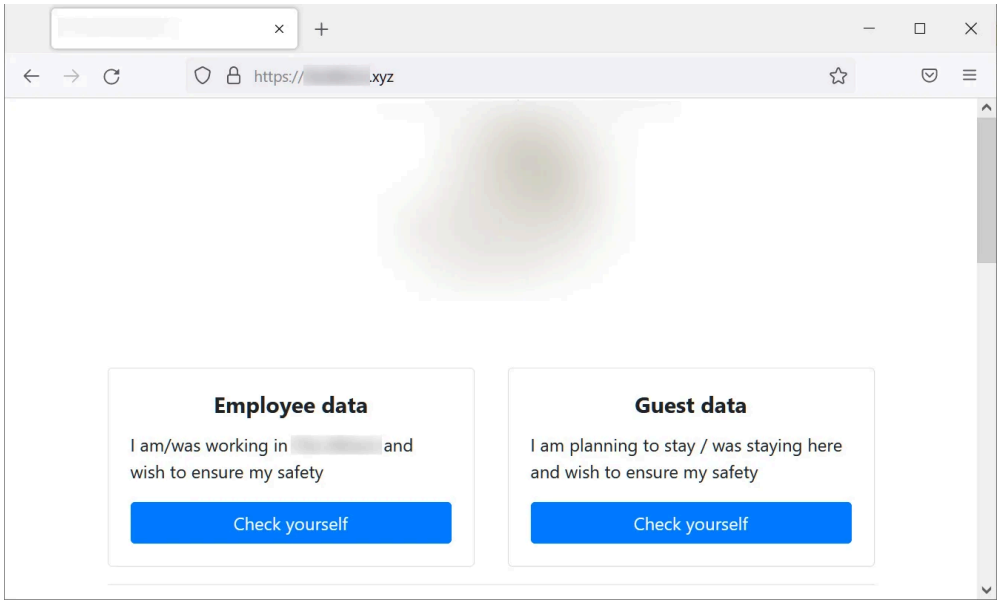
For this reason, ransomware gangs constantly evolve their tactics to apply additional pressure on victims.

Taking extortion to the next level

Today, the AlphV/BlackCat ransomware operation began releasing allegedly stolen data that they claim was stolen from a hotel and spa in Oregon.

As part of this attack, the ransomware gang claims to have stolen 112GB of data, including employee information, such as Social Security Numbers, for 1,500 employees.

However, instead of just leaking the data on their normal Tor data leak site, the ransomware gang took it a step further and created a dedicated website allowing employees and customers to check if their data was stolen during the attack on the hotel.



Victim's search data leak site

Source: BleepingComputer

Using this site, employees, customers, or anyone for that matter, can see information about hotel guests and their stays or the personal data of 1,534 employees.

While the customer guest data only contains names, arrival date, and stay costs, the employee data includes extremely sensitive information, such as names, Social Security Numbers, date of birth, phone numbers, and email addresses.

The threat actors even went as far as to create "data packs" for each employee that contain files related to that person's employment at the hotel.

As this site is hosted on the clear web, i.e. the public internet, it is indexable by search engines, and the exposed information will likely be added to search results, potentially making this even worse for victims.

Innovative or a waste of time?

The goal of this site is clear, to scare employees and guests into demanding the hotel remove their data from the web, which can only be done by paying a ransom.

Emisosft security analyst Brett Callow, who discovered this new extortion strategy and shared it with BleepingComputer, said that while the tactic is innovative, it is too early to tell if it will pay off.

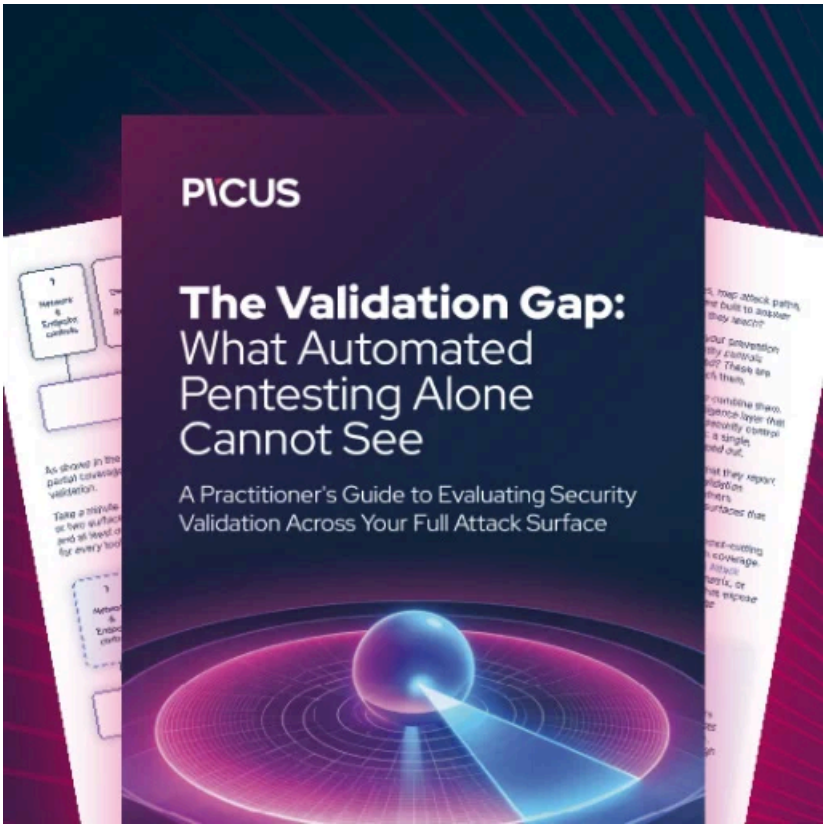
"Alphv is no doubt hoping that this tactic will increase the probability of them monetizing attacks. If companies know that information relating to their customers and employees will be made public in this manner, they may be more inclined to pay the demand to prevent it from happening - and to avoid potentially being hit with class action lawsuits," Callow told BleepingComputer in a conversation.

"While it's an innovative approach, it remains to be seen whether the strategy will be successful - and, of course, that will determine whether it becomes more commonplace."

AlphV is believed to be a rebrand of the DarkSide/BlackMatter gang responsible for the attack on Colonial Pipeline, which thrust these hacking groups into the media's attention and focused the full attention of international law enforcement and the US government.

This ransomware gang has always been considered one of the top-tier ransomware operations. However, they are also known for the mess-ups and crazy ideas that get them in trouble.

Setting up this website with individual employee data packs was definitely a time-consuming task for the ransomware gang. We will have to wait and see whether the effort pays off.



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-creates-site-for-employees-to-search-for-their-stolen-data/