Ransomware gang cloned victim’s website to leak stolen data

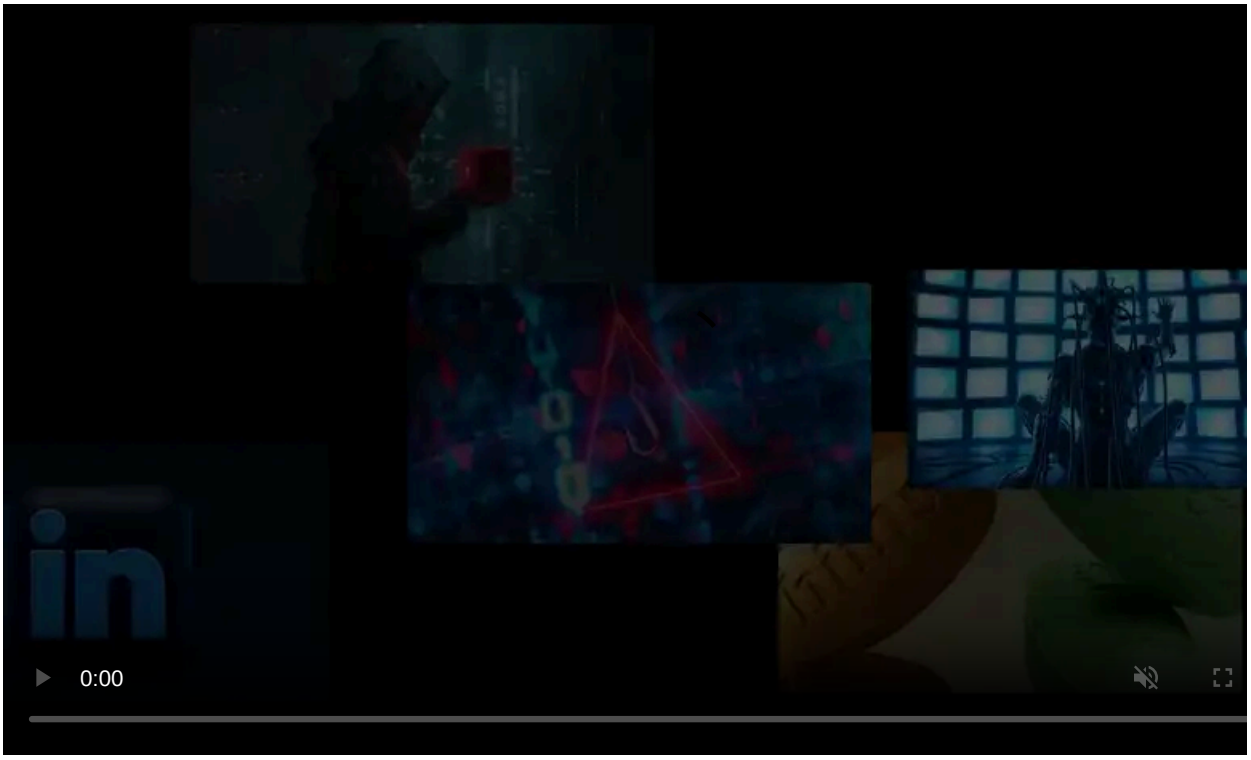
By Ionut Ilascu

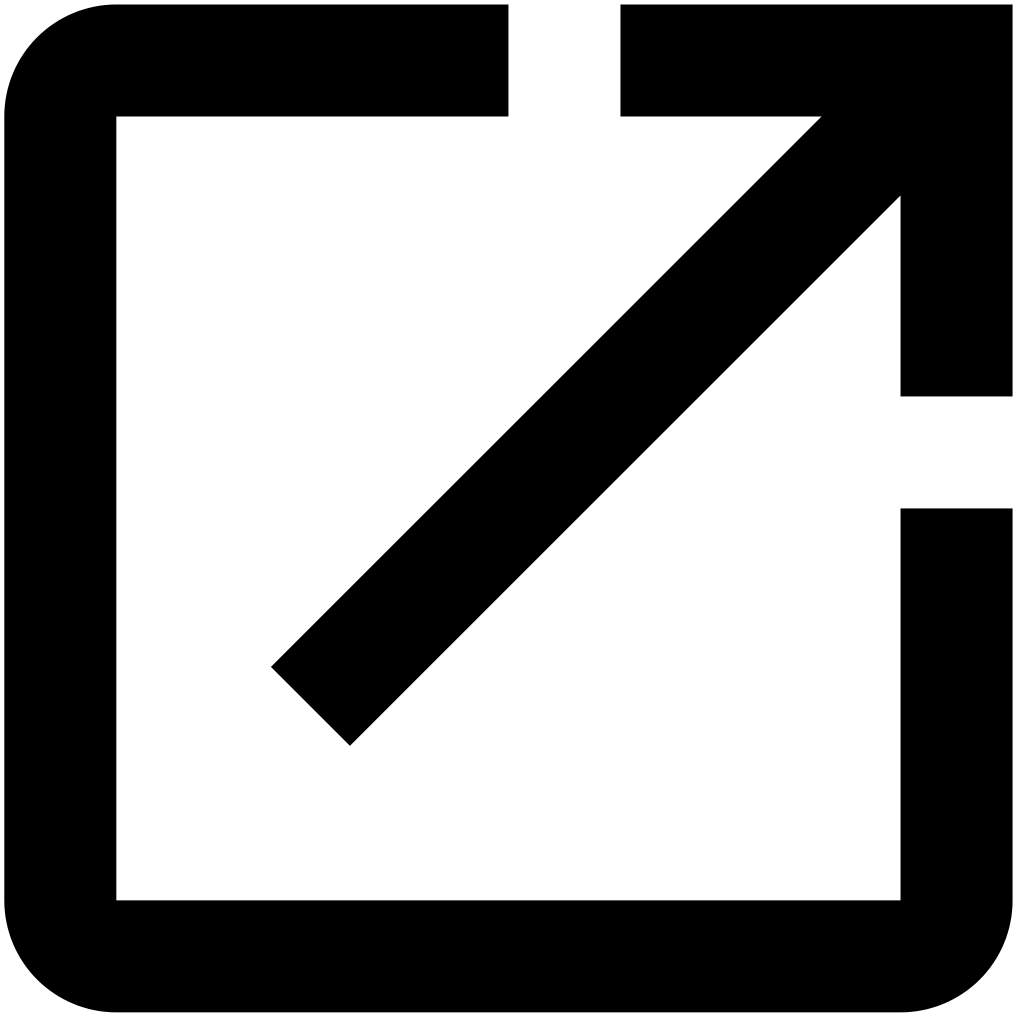
Published: 2023-01-01 · Archived: 2026-04-05 18:54:14 UTC

The ALPHV ransomware operators have gotten creative with their extortion tactic and, in at least one case, created a replica of the victim's site to publish stolen data on it.

It appears that ALPHV, also known as BlackCat ransomware, is known for testing new extortion tactics as a way to pressure and shame their victims into paying.

While these tactics may not be successful, they introduce an ever-increasing threat landscape that victims need to navigate.


0:00

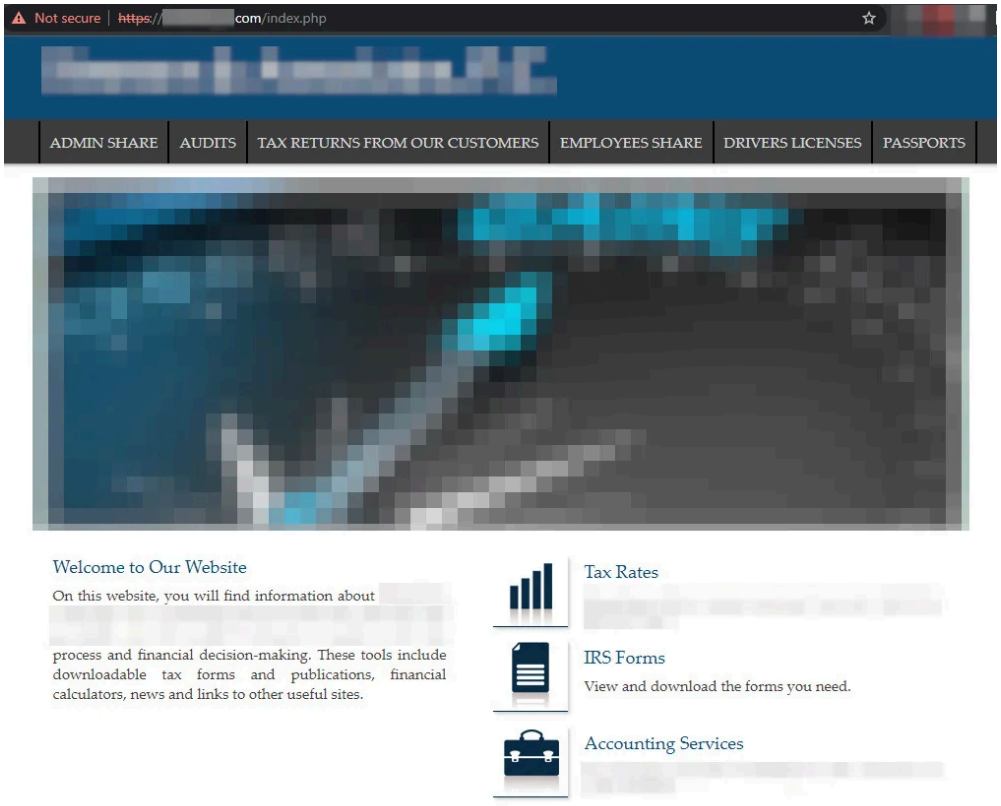


Hackers make stolen data easier to get

On December 26, the threat actor published on their data leak site hidden on the Tor network that they had compromised a company in financial services.

As the victim did not meet the threat actor's demands, BlackCat published all the stolen files as a penalty - a standard step for ransomware operators.

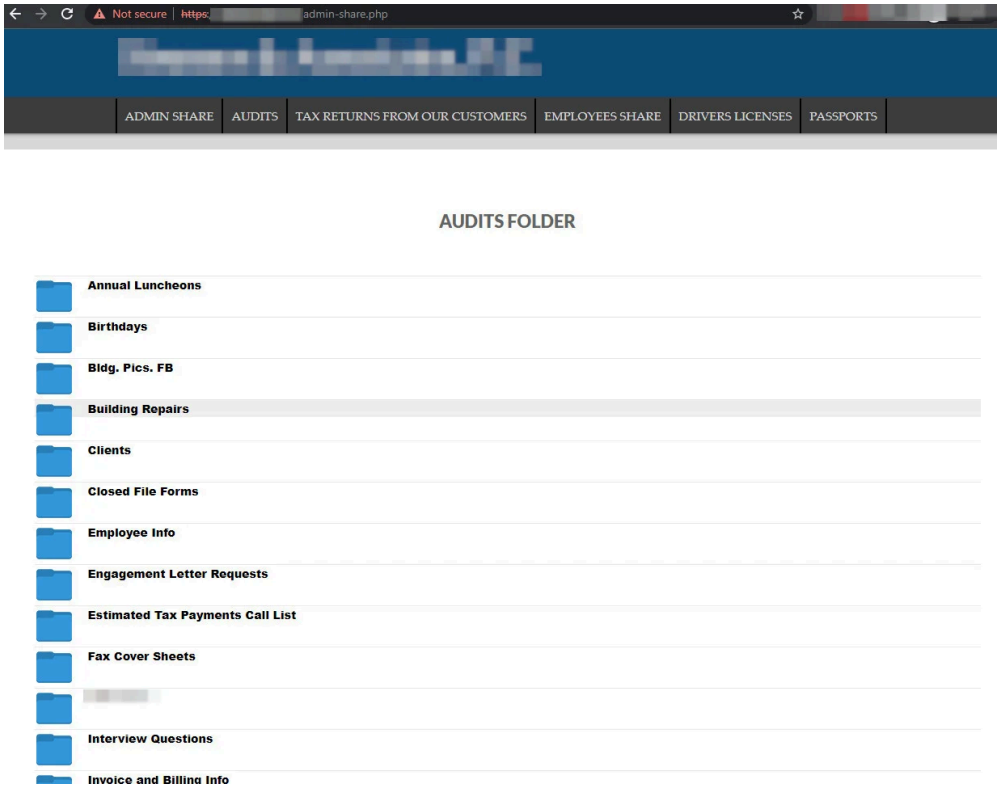
As a deviation from the usual process, the hackers decided to also leak the data on a site that mimics the victim's as far as the appearance and the domain name go.



ALPHV ransomware impersonates victim site to leak stolen data
source: BleepingComputer

The hackers did not keep the original headings of the site. They used their own headings to organize the leaked data.

The cloned site is on the clear web to ensure the wide availability of the stolen files. It currently shows various documents, from memos to staff, payment forms, employee info, data on assets and expenses, financial data for partners, and passport scans.



ALPHV ransomware publishes stolen data on site impersonating the victim
source: BleepingComputer

In total, there are 3.5GB of documents. ALPHV also shared the stolen data on a file-sharing service that allows anonymous uploading and distributed the link on its leak site.

New trend forming

Brett Callow, threat analyst at cybersecurity company Emsisoft, said that sharing the data on a typosquatted domain would be a bigger concern to the victim company than distributing the data through a website on the Tor network, which is known mainly by the infosec community.

“I wouldn't be at all surprised if Alphv had attempted to weaponize the firm's clients by pointing them to that website” Brett Callow

This tactic could represent the start of a new trend that may be adopted by other ransomware gangs, especially since the costs to do it are far from significant.

Ransomware operations have always looked for new options to extort their victims. Between publishing the name of the breached company, stealing data and threatening to publish it unless the ransom is paid, and the DDoS menace, this tactic could represent the start of a new trend that may be adopted by other ransomware gangs, especially since the costs to do it are far from significant.

It is unclear at this time how successful is this stratagem but it exposes the breach to a larger audience, putting the victim into a more delicate position as its data is readily available without any restriction.

ALPHV is the first ransomware gang to create a search for specific data stolen from their victims. The pages are for customers and employees of their victims to check if their data was stolen by the hackers.
