ALPHV ransomware adds data leak API in new extortion strategy

By Ionut Ilascu

Published: 2023-07-26 · Archived: 2026-04-05 18:41:52 UTC

Image: Bing Create

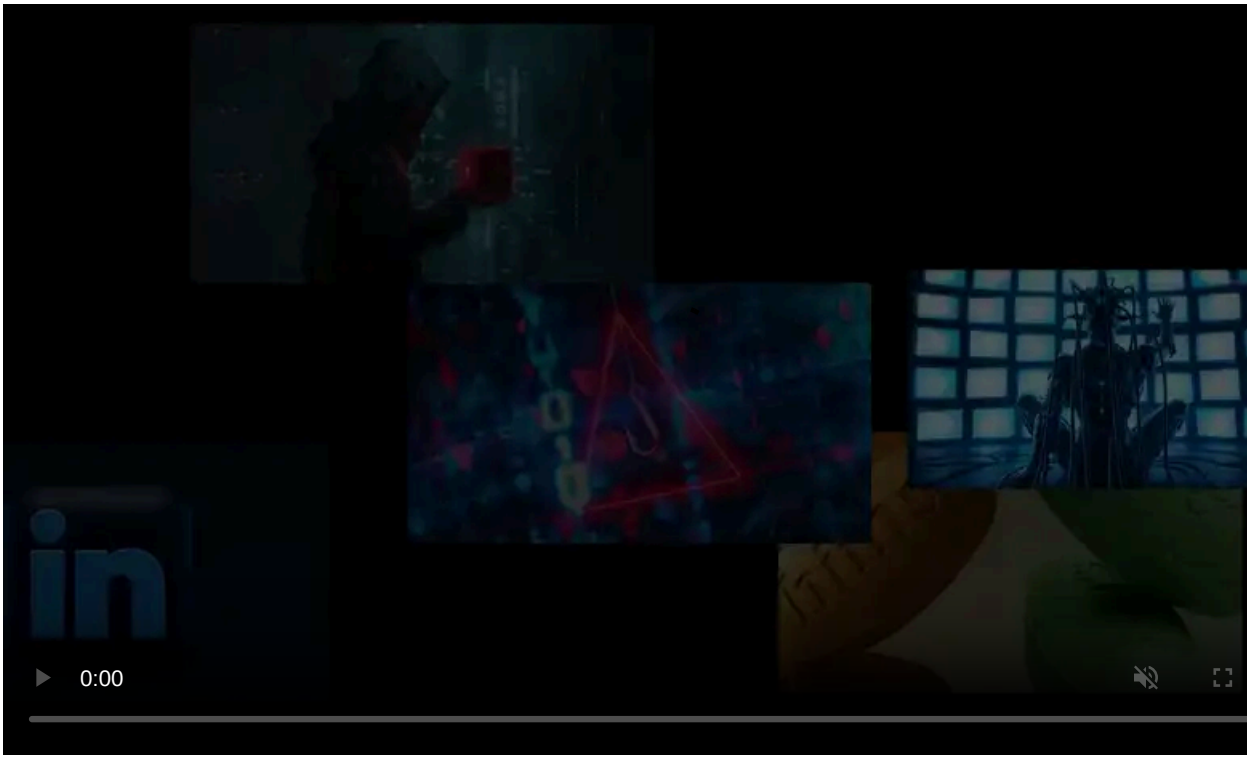
The ALPHV ransomware gang, also referred to as BlackCat, is trying to put more pressure on their victims to pay a ransom by providing an API for their leak site to increase visibility for their attacks.

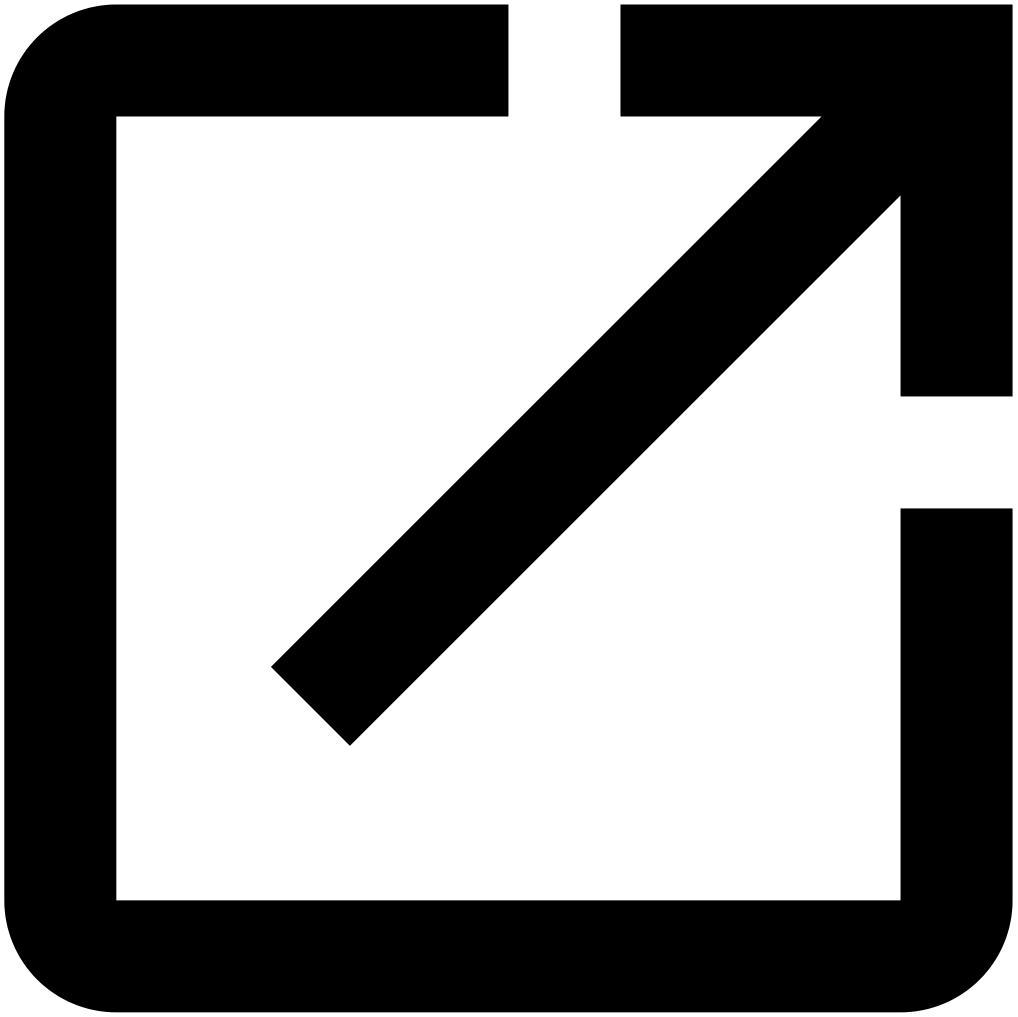
This move follows the gang's recent breach of Estée Lauder that ended with the beauty company completely ignoring the threat actor's effort to engage in negotiations for a ransom payment.

API calls and Python crawler

Multiple researchers spotted earlier this week that the ALPHV/BlackCat data leak site added a new page with instructions for using their API to collect timely updates about new victims.

APIs, or Application Programming Interfaces, are typically used to enable communication between two software components based on agreed definitions and protocols.

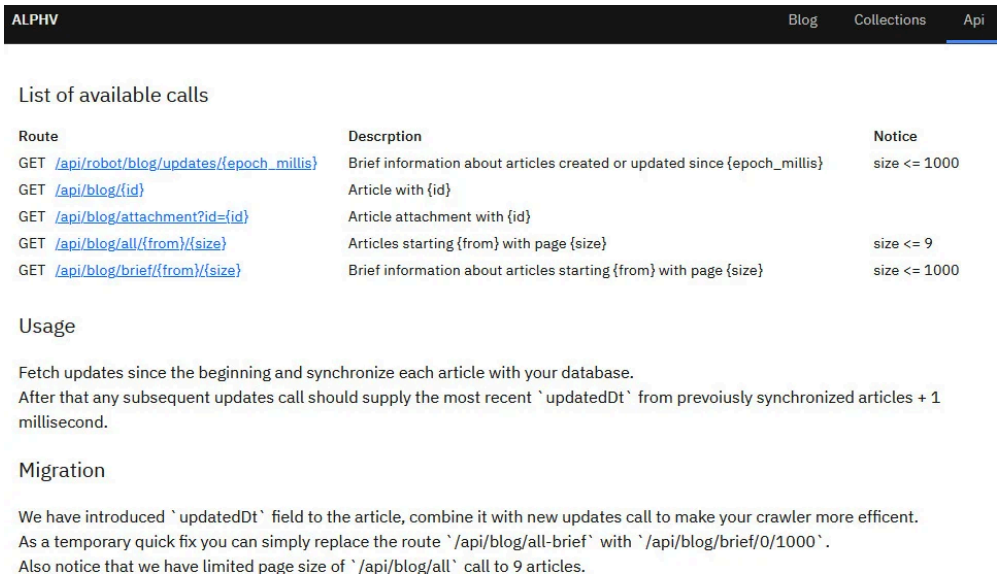

0:00



Malware research group VX-Underground pointed to the new section on ALPHV's site but it appears that the "feature" has been partially available for months though not to the larger audience.

The ransomware gang posted the API calls that would help fetch various information about new victims added to their leak site or updates starting a specific date.

"Fetch updates since the beginning and synchronize each article with your database. After that any subsequent updates call should supply the most recent `updatedDt` from prevoiusly [sic] synchronized articles + 1 millisecond," the gang explained.



BlackCat ransomware lists API calls for victim updates

source: BleepingComputer

The group also provided a crawler written in Python to help retrieve the latest information on the data leak site.

Fewer paying victims

Although the gang did not explain the release of the API, one reason could be that fewer victims are succumbing to ransomware demands.

A report from ransomware incident response company Coveware notes that the number of paying victims that suffered a ransomware attack "fell to a record low of 34%" in the second quarter of this year.

However, some threat actors continue to make big money by focusing on targeting the supply chain to breach a large number of organizations.

Clop ransomware, for instance, is estimated to make at least $75 million from their massive MOVEit data theft campaign.

Clop's breaches using a zero-day vulnerability in the MOVEit Transfer secure file transfer platform likely impacts hundreds of companies, including Estée Lauder which was also compromised by ALPHV/BlackCat.

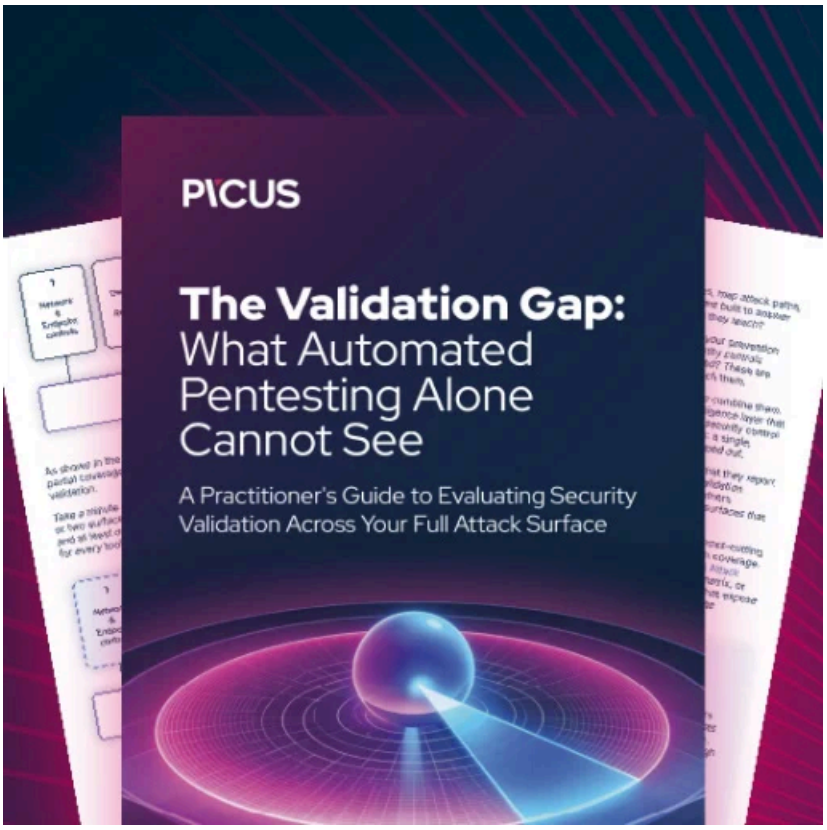
Estée Lauder did not respond to any messages from ALPHV, clearly stating that it would not pay the attacker for the stolen files.

This inflamed the ransomware gang and prompted a disgruntled message that mocked the company's security measures by saying that the security experts brought in following the breach did a poor job because the network was still compromised.

With fewer paying victims, ransomware gangs are looking for new methods to put pressure and get the money.

With fewer paying victims, ransomware gangs are looking for new methods to apply pressure and get the money. Making their leaks easily available to a larger audience appears to be the latest extortion layer from ransomware but it is likely

doomed to fail.



[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/alphv-ransomware-adds-data-leak-api-in-new-extortion-strategy/