Reddit hackers threaten to leak data stolen in February breach

By Lawrence Abrams

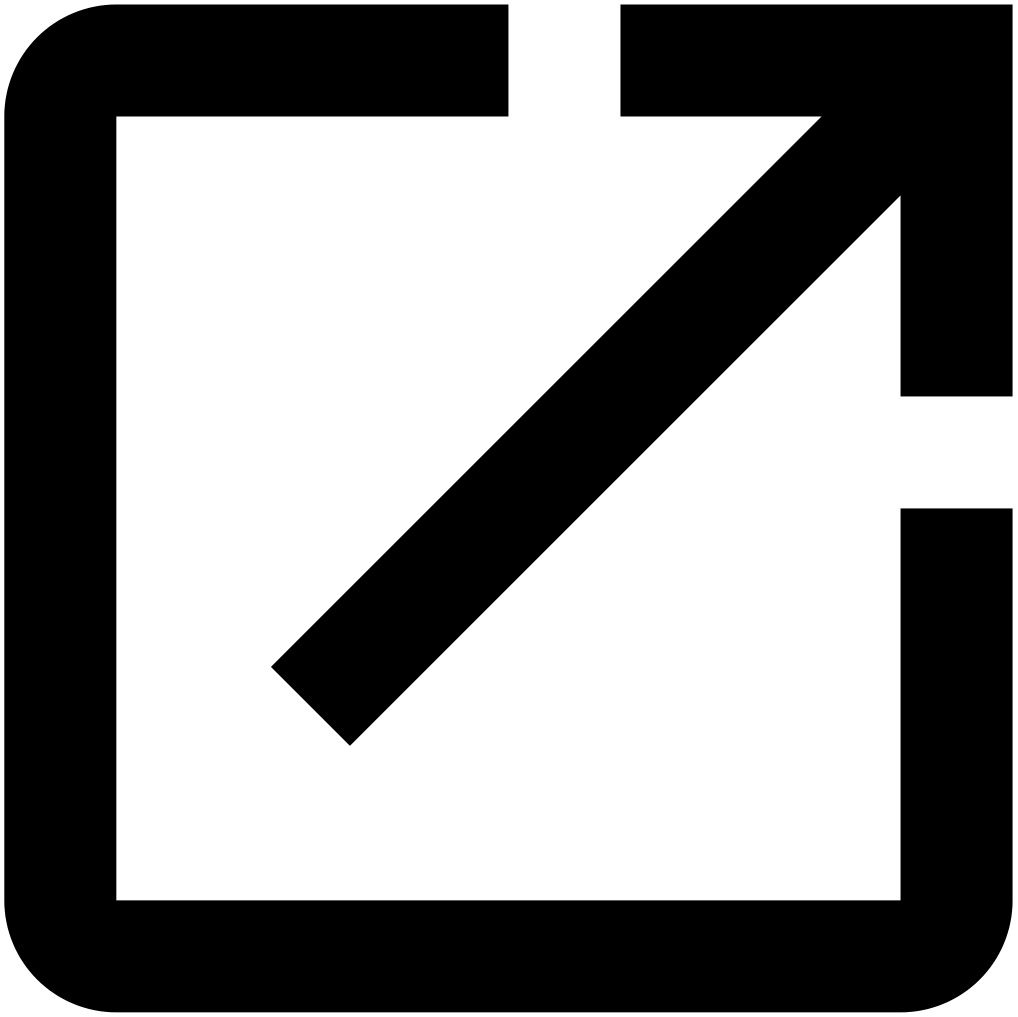
Published: 2023-06-18 · Archived: 2026-04-05 13:39:32 UTC

The BlackCat (ALPHV) ransomware gang is behind a February cyberattack on Reddit, where the threat actors claim to have stolen 80GB of data from the company.

On February 9th, Reddit disclosed that its systems were hacked on February 5th after an employee fell victim to a phishing attack.

This phishing attack allowed the threat actors to gain access to Reddit's systems and steal internal documents, source code, employee data, and limited data about the company's advertisers.


DIE LINKE.
0:00



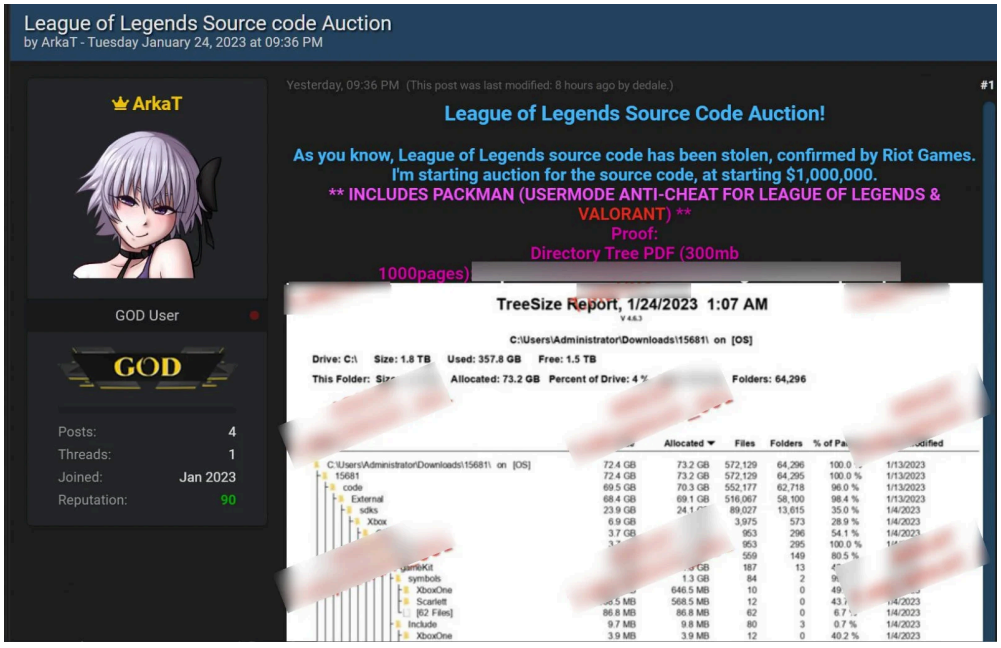
"After successfully obtaining a single employee's credentials, the attacker gained access to some internal docs, code, as well as some internal dashboards and business systems," explained a post by Reddit CTO Christopher Slowe, aka KeyserSosa.

"We show no indications of breach of our primary production systems (the parts of our stack that *run* Reddit and store the majority of our data)."

However, Reddit said that production systems were not breached, and no user passwords, accounts, or credit card information were impacted.

While Reddit did not share many details on the phishing attack, they said it was similar to a phishing attack on Riot Games that allowed hackers to gain access to systems and steal source code for League of Legends (LoL), Teamfight Tactics (TFT), and the company's Packman legacy anti-cheat platform.

During the attack on Riot, the threat actors demanded $10 million not to leak the stolen data. However, when a ransom was not paid, the threat actors attempted to sell the data for $1 million on a hacking forum.



Forum post selling Riot Games source code
Source: BleepingComputer

BlackCat behind Reddit hack

As first spotted by Dominic Alvieri and shared with BleepingComputer, the ALPHV ransomware operation, more commonly known as BlackCat, now claims to be behind the February 5th cyberattack on Reddit.

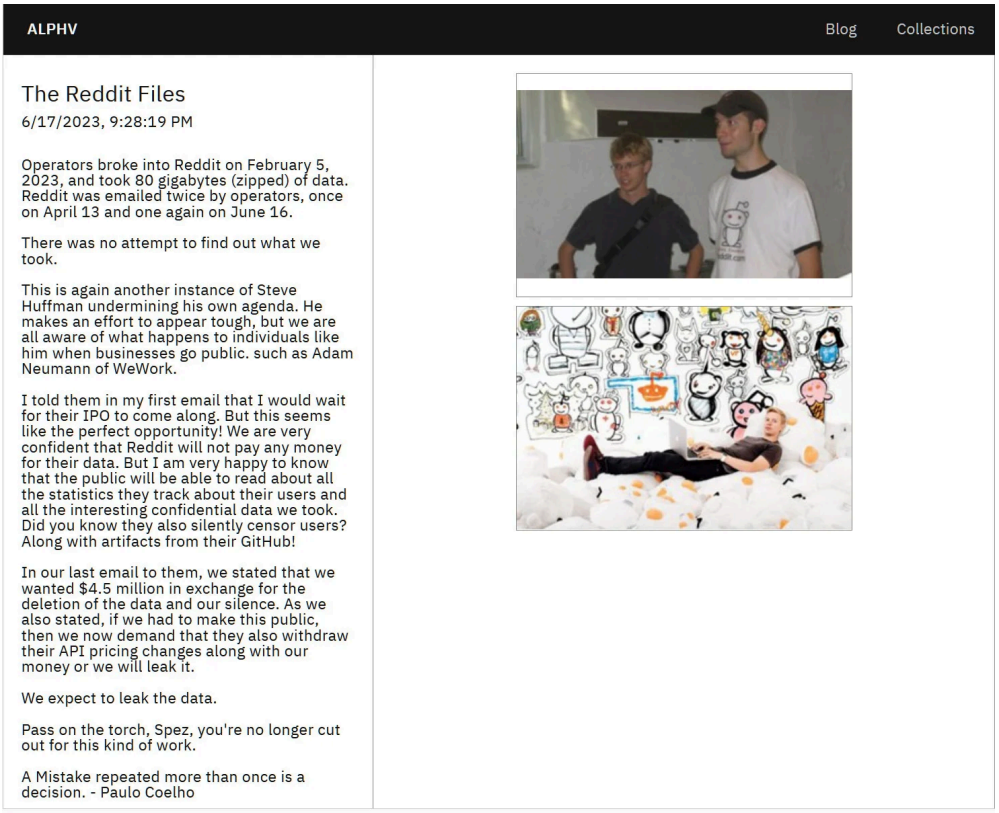
In a "Reddit Files" post on the gang's data leak site, the threat actors claim to have stolen 80 GB of compressed data from the company during the attack and now plan on leaking the data.

The threat actors say they attempted to contact Reddit twice, on April 13th and June 16th, demanding $4.5 million for the data to be deleted but did not receive a response.

"I told them in my first email that I would wait for their IPO to come along. But this seems like the perfect opportunity! We are very confident that Reddit will not pay any money for their data," threatened the ransomware operation.

"But I am very happy to know that the public will be able to read about all the statistics they track about their users and all the interesting confidential data we took. Did you know they also silently censor users? Along with artifacts from their GitHub!"

After not receiving a response, the threat actors now threaten to leak Reddit's data if the company doesn't pay the ransom and backtrack on their plans on charging for API access.



"The Reddit Files" post on BlackCat data leak site

Source: BleepingComputer

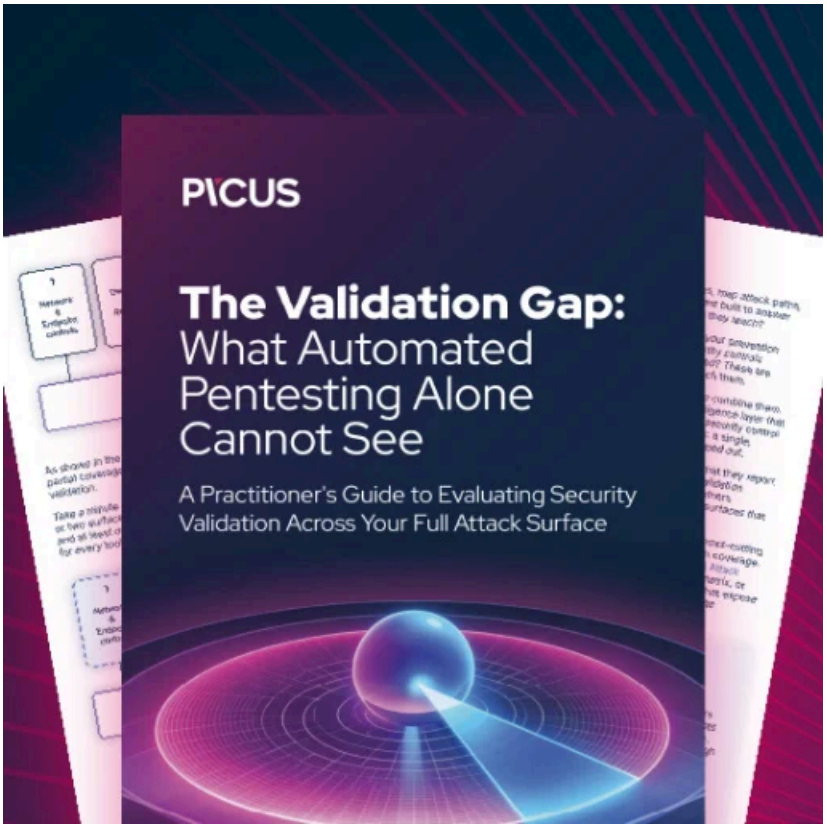
While Reddit declined to comment about BlackCat's post, BleepingComputer has been able to confirm that this is the same attack disclosed by Reddit in February.

It should be noted that while BlackCat is a ransomware gang, they did not encrypt devices in this attack.

The same hacking group is believed to be linked to a similar attack on Western Digital in March 2023, causing a massive outage to the company's My Cloud cloud service.

While the threat actors behind the Western Digital attack initially claimed not to have a name, screenshots of the stolen data were leaked on the ALPHV data leak site, with the threat actors taunting the company about the attack.

Western Digital sent data breach notifications in May, warning online store customers that their data was stolen during the attack.



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/reddit-hackers-threaten-to-leak-data-stolen-in-february-breach/