Epic Games: "Zero evidence" we were hacked by Mogilevich gang

By Lawrence Abrams

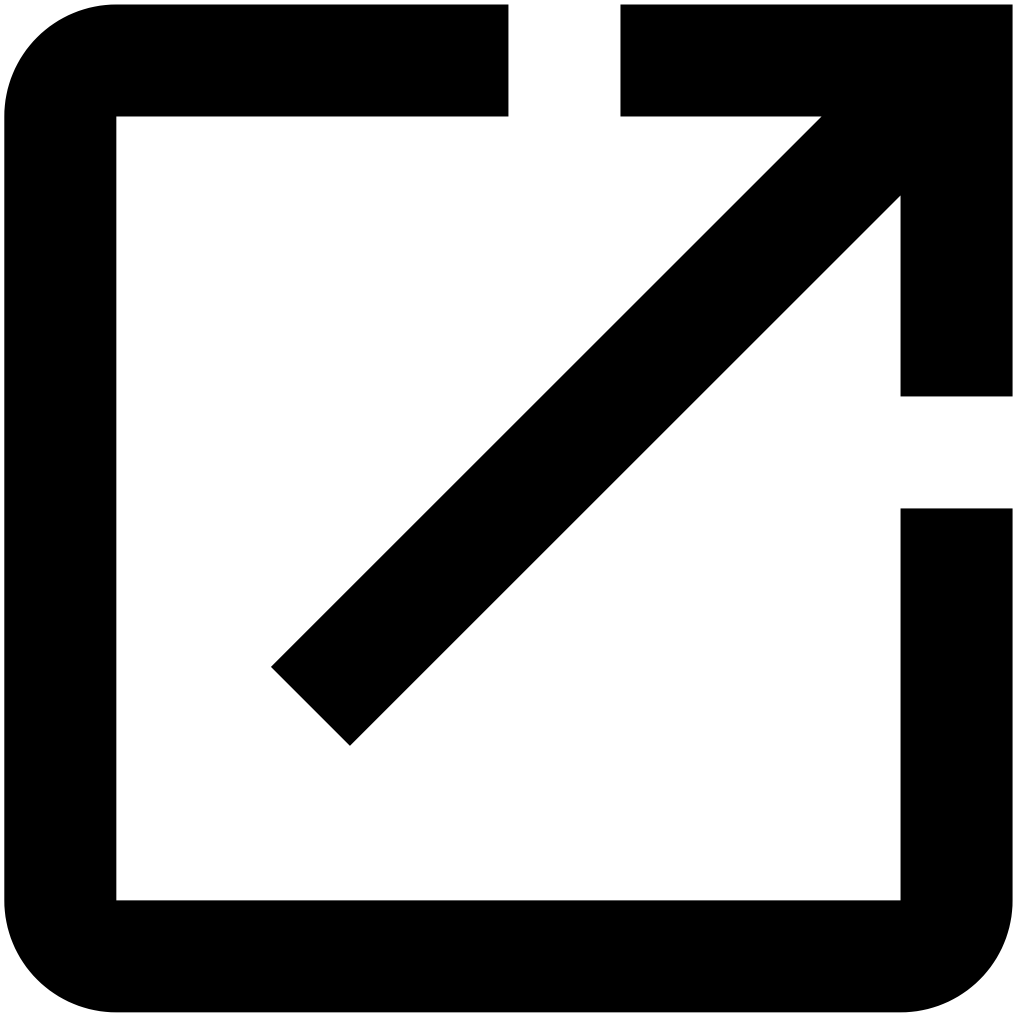
Published: 2024-02-28 · Archived: 2026-04-05 13:24:25 UTC

Epic Games said they found zero evidence of a cyberattack or data theft after the Mogilevich extortion group claimed to have breached the company's servers.

"We are investigating but there is currently zero evidence that these claims are legitimate," Epic Games told BleepingComputer in a statement.

"Mogilievich has not contacted Epic or provided any proof of the veracity of these allegations."

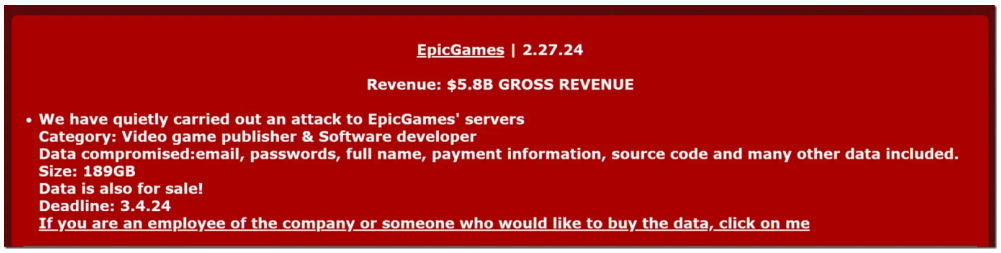

DIE LINKE.
0:00



Epic Games told BleepingComputer that they immediately began investigating the incident after seeing a screenshot of the dark web page promoting the breach and attempted to contact the threat actor.

However, the company told us they never received a response from Mogilevich, and the only information they had was from a tweet I posted yesterday.

Yesterday, after news of the alleged breach spread through Twitter, I spoke to a representative of the Mogilevich extortion group, asking if they would share proof of the attack.



Mogilevich claiming to be selling data stolen from Epic Games
Source: BleepingComputer

The threat actors told BleepingComputer that they were selling the stolen data for $15,000 but would only share samples with those who showed "proof of funds," meaning that they had demonstrated that they had the available cryptocurrency assets to make the purchase.

They claimed they shared samples of this allegedly stolen data with three people who showed proof of funds.

Who is Mogilevich

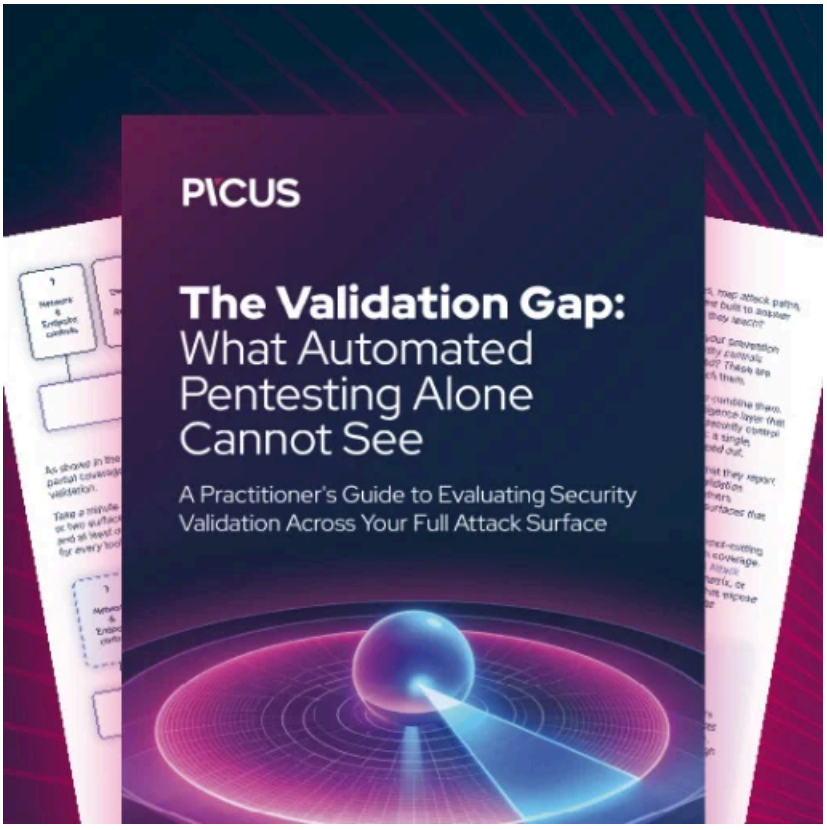
Mogilevich is a relatively new extortion group that claims to have breached numerous organizations, including Ireland's Department of Foreign Affairs and Infinity USA.

However, unlike other extortion groups, Mogilevich does not share samples of stolen data and claim only to be selling directly to proven buyers.

This lack of proof has led many security researchers whom BleepingComputer has spoken with to believe that the threat actors are attempting to scam buyers with fake data.

The threat actors also claim to be a Ransomware-as-a-Service operation, recruiting other hackers (affiliates) to work with them in exchange for a working ransomware encryptor and negotiation panel. When an affiliate conducts an attack and a ransom is paid, the affiliate and operators split the payment based on negotiated percentages.

However, no samples of any ransomware encryptor have been found at this time linking them to encryption attacks.



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/epic-games-zero-evidence-we-were-hacked-by-mogilevich-gang/