2K Games says hacked help desk targeted players with malware

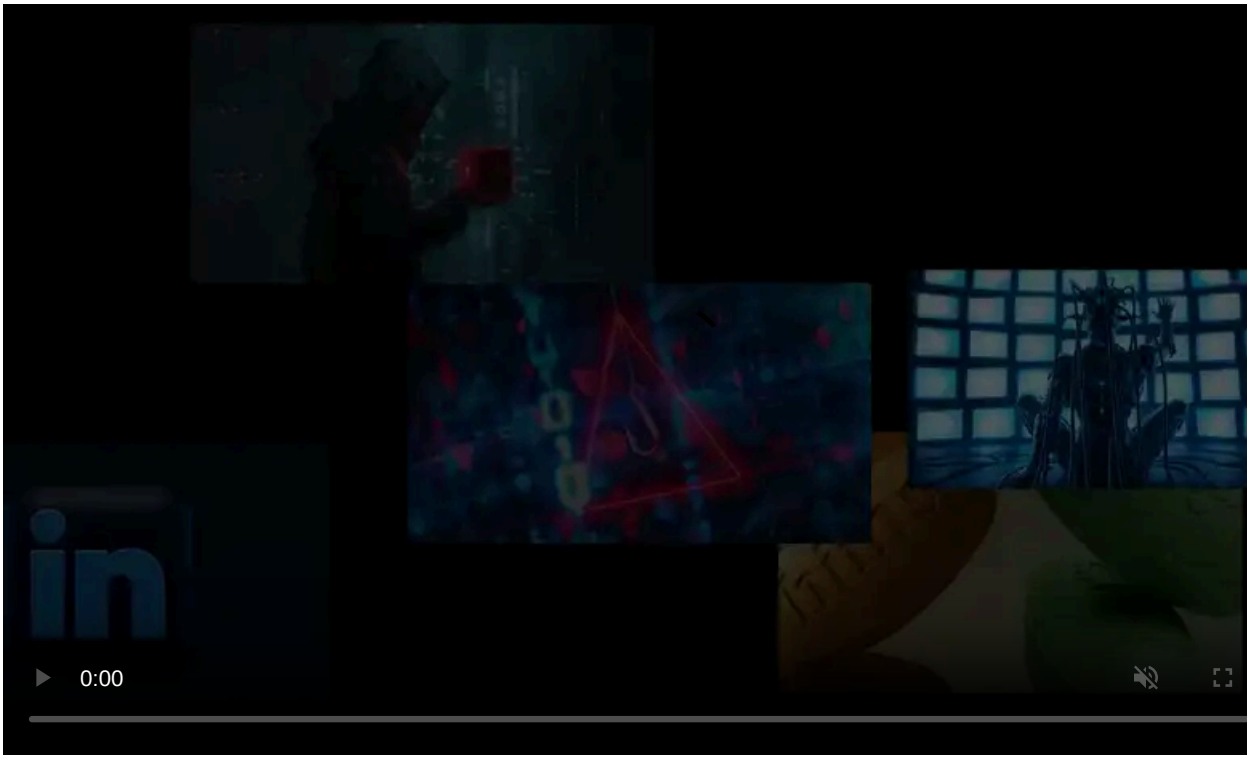
By Sergiu Gatlan

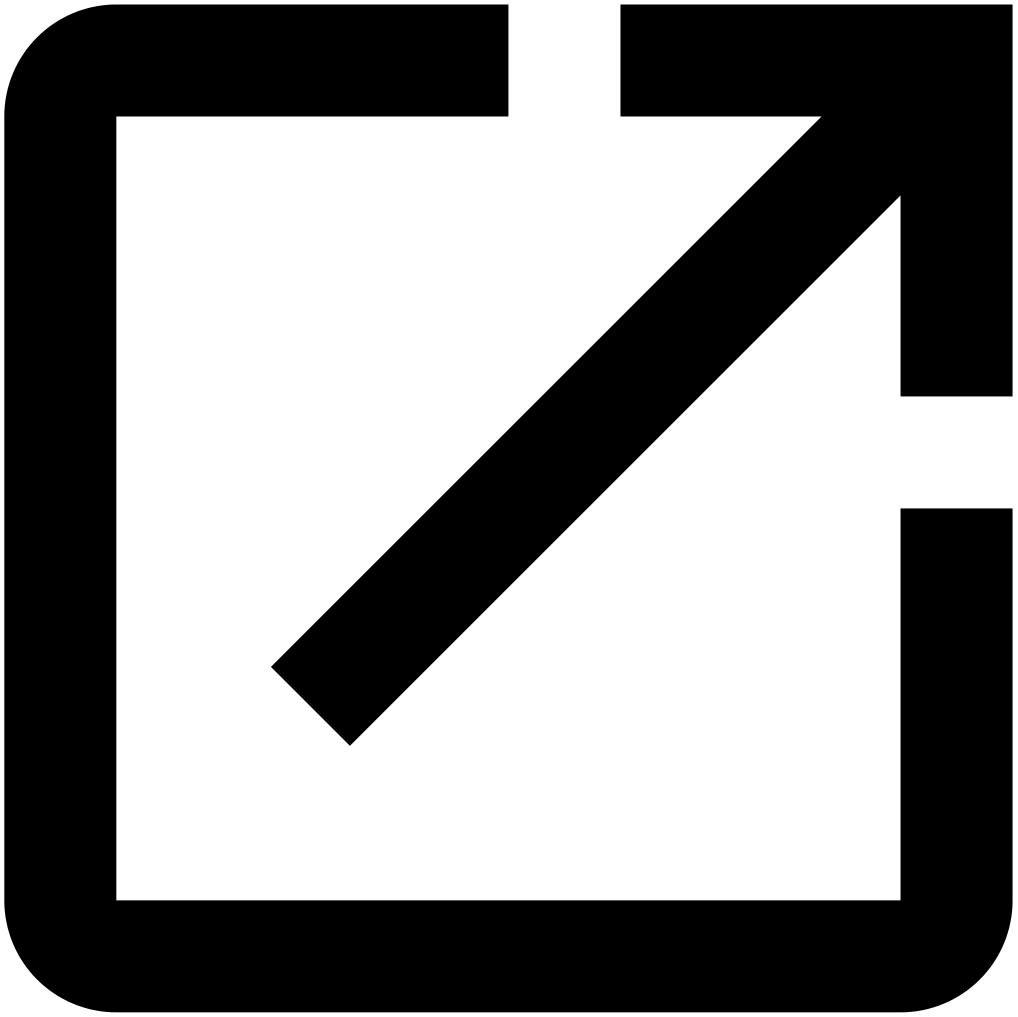
Published: 2022-09-20 · Archived: 2026-04-05 17:23:44 UTC

American video game publisher 2K has confirmed that its help desk platform was hacked and used to target customers with fake support tickets pushing malware via embedded links.

"Earlier today, we became aware that an unauthorized third party illegally accessed the credentials of one of our vendors to the help desk platform that 2K uses to provide support to our customers," 2K's support account tweeted on Tuesday after BleepingComputer broke the story on the security breach.

"The unauthorized party sent a communication to certain players containing a malicious link. Please do not open any emails or click on any links that you receive from the 2K Games support account."


0:00



The company advised those who might have clicked one of the malicious links sent by the attackers to take steps to mitigate the potential impact immediately:

- Reset any user account passwords stored in your web browser (e.g., Chrome AutoFill)
- Enable multi-factor authentication (MFA) whenever available, especially on personal email, banking, and phone or Internet provider accounts. If possible, avoid using MFA that relies on text message verification - using an authenticator app would be the most secure method
- Install and run a reputable anti-virus program
- Check your account settings to see if any forwarding rules have been added or changed on your personal email accounts

2K added that its support portal was taken offline earlier while the video game publisher investigates and addresses the incident's fallout.

The company said it would issue a notice to let players know when it will be safe to start interacting with its support staff again.

"We will issue a notice when you can resume interacting with official 2K help desk emails, and we will also follow-up with additional information as to how you can best protect yourself against any malicious activity," 2K said.

Malicious emails pushed RedLine info-stealer

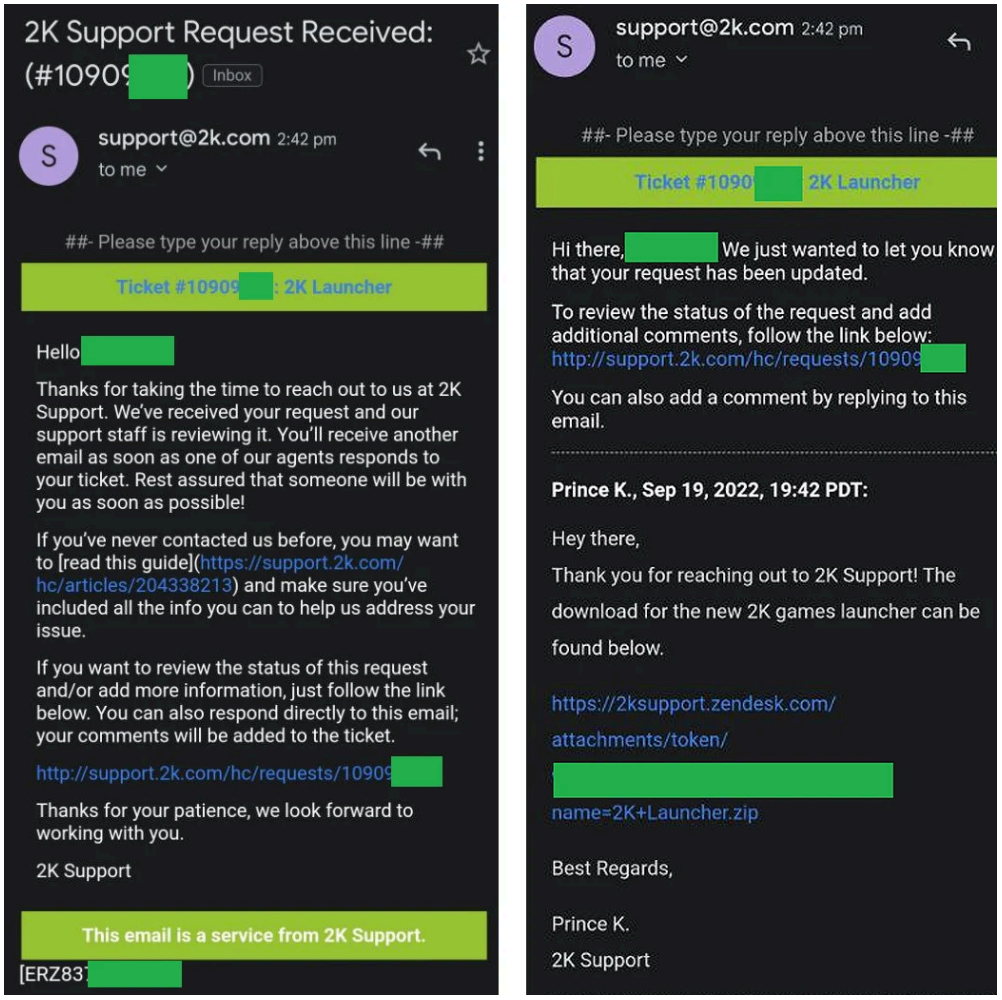
As BleepingComputer reported previously, 2K customers started receiving emails earlier today saying they opened support tickets on 2ksupport.zendesk.com, 2K's online support ticketing system.

While the users confirmed these tickets were accessible via 2K's help desk portal, numerous recipients stated on Twitter and Reddit that they were not the ones who opened these support tickets.

Soon after the tickets were opened, they also received another email in reply to the original ticket (from an alleged 2K support representative named 'Prince K'), emails that also included links to download a file named '2K Launcher.zip' from 2ksupport.zendesk.com.

As BleepingComputer found, the archive contained an executable that is actually the RedLine information-stealing malware, according to VirusTotal and Any.Run scans.

RedLine Stealer is an info-stealer malware that threat actors use to steal a wide range of data after infecting one's system, including web browser history, cookies, saved browser passwords, credit cards, VPN credentials, instant messaging content, cryptocurrency wallets, and more.



Fake 2K support tickets with RedLine stealer download links (Reddit)

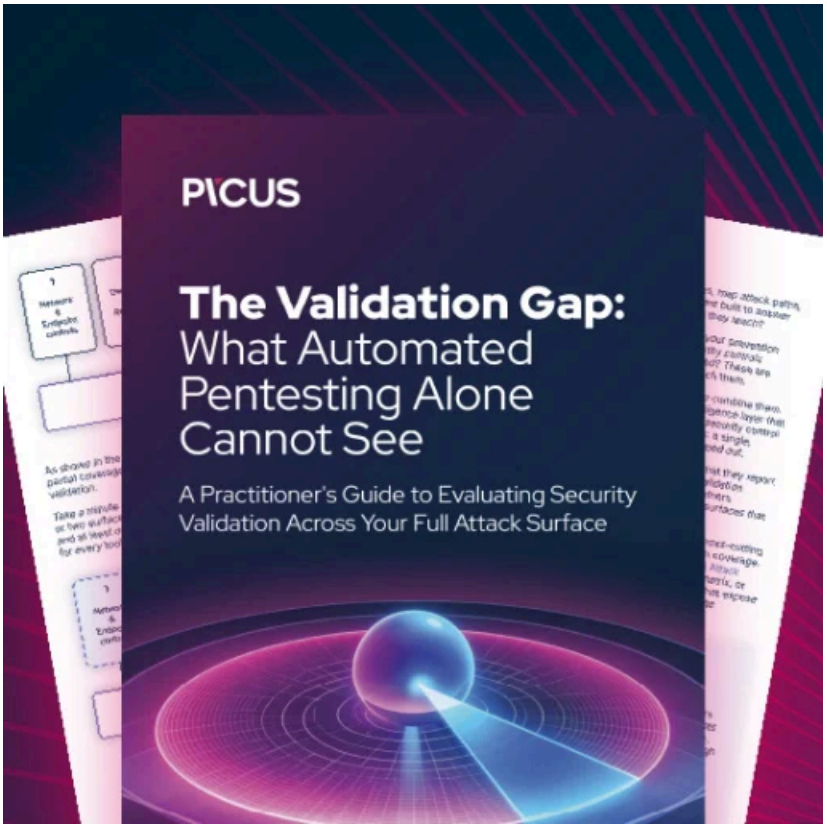
While 2K is yet to provide any information on this, it's unclear if the attack on its support system is linked to the Rockstar Games hack over the weekend, but the timing is definitely suspicious.

Both companies are subsidiaries of Take-Two Interactive, one of the largest video game publishers across the Americas and Europe.

The threat actor behind the Rockstar Games breach has also claimed the recent Uber hack, which believes the attack was orchestrated by a hacker affiliated with the Lapsus$ extortion group.

2K is the publisher behind numerous popular game franchises, including NBA 2K, Borderlands, WWE 2K, PGA Tour 2K, Bioshock, Civilization, and Xcom.

BleepingComputer had reached out to 2K about the hack of their support systems before the game publisher confirmed the attack, but we are still waiting for a reply.



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/2k-games-says-hacked-help-desk-targeted-players-with-malware/