



Security Newsletter

19 April 2021

[Subscribe to this newsletter](#)

FBI Accesses Computers in the US to Delete Microsoft Exchange Hacks



On Tuesday the Department of Justice announced the FBI was given approval to access hundreds of computers across the United States running vulnerable versions of Microsoft Exchange Server software to remove web shells left by hackers who had earlier penetrated the systems.

The news shows some of the more proactive steps law enforcement may take when faced with large scale hacking operations, and victims who are not willing or able to swiftly patch their systems.

In short, the FBI obtained permission to access computers to remove artifacts of an earlier, high profile hacking operation in order to prevent further access to those machines by hackers.

[Read More on Vice](#)

[Even More on Bleeping Computer](#)

More #News

- [CS:GO, Valve Source games vulnerable to hacking using Steam invites](#)
- [Hackers flood the web with 100,000 pages offering malicious PDFs](#)
- [Ryuk ransomware operation updates hacking techniques](#)
- [HackBoss malware poses as hacker tools on Telegram to steal digital coins](#)
- [Dutch supermarkets run out of cheese after ransomware attack](#)
- [SolarWinds: US and UK blame Russian intelligence service hackers for major cyberattack](#)
- [Phishing attack ramps up against COVID-19 vaccine supply chain](#)
- [High-level organizer of notorious hacking group FIN7 sentenced to ten years in prison](#)

#Breach Log

- [Attack on Codecov Affects Customers](#)
- [New NAME:WRECK Vulnerabilities Impact Nearly 100 Million IoT Devices](#)
- [Cyberattack on UK university knocks out online learning, Teams and Zoom](#)
- [Swinburne University confirms over 5,000 individuals affected in data breach](#)
- [ParkMobile Breach Exposes License Plate Data, Mobile Numbers of 21M Users](#)
- [Facebook faces 'mass action' lawsuit in Europe over 2019 breach](#)
- [A hard disk with data of 30,000 people stolen from the Amsterdam tax office](#)
- [Clubhouse data leak: 1.3 million scraped user records leaked online for free](#)

#Patch Time!

- [Microsoft Patches 4 Additional Exchange Flaws](#)
- [Update Your Chrome Browser to Patch 2 New In-the-Wild 0-Day Exploits](#)
- [Severe Bugs Reported in EtherNet/IP Stack for Industrial Systems](#)
- [New WhatsApp Bugs Could've Let Attackers Hack Your Phone Remotely](#)
- [SAP fixes critical bugs in Business Client, Commerce, and NetWeaver](#)
- [NSA discovers critical Exchange Server vulnerabilities](#)
- [Microsoft April 2021 Patch Tuesday fixes 108 flaws, 5 zero-days](#)
- [Adobe fixes critical vulnerabilities in Photoshop and Digital Editions](#)

#Tech and #Tools

- [New JavaScript Exploit Can Now Carry Out DDR4 Rowhammer Attacks](#)
- [Major BGP leak disrupts thousands of networks globally](#)
- [Airstrike Attack - FDE bypass and EoP on domain joined Windows workstations](#)
- [Allow arbitrary URLs, expect arbitrary code execution](#)



This content was created by [Kindred Group Security](#). Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at <https://news.infosecgur.us>