KnowBe4
Human error. Conquered.

Setting the Trap

Crafty Ways the Bad Guys Trick Your Users to Own Your Network

Kevin Mitnick
Chief Hacking Officer
KnowBe4, Inc.

Perry Carpenter
Chief Evangelist & Strategy Officer
KnowBe4, Inc.

Kevin Mitnick
Chief Hacking Officer
KnowBe4, Inc.

Perry Carpenter
Chief Evangelist & Strategy Officer
KnowBe4, Inc.

KnowBe4
Human error. Conquered.


NEWS

FBI launches operation to remove backdoors from hacked Microsoft Exchange servers

Zack Whittaker @zackwhittaker / 6:33 PM CDT • April 13, 2021

Comment

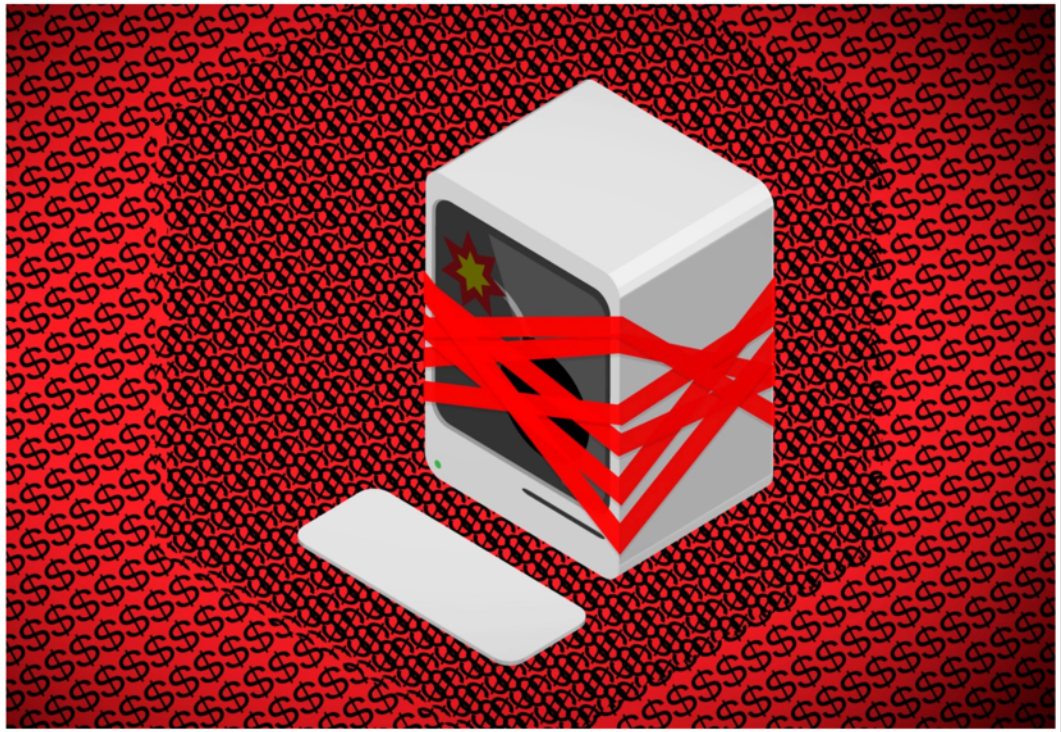


Image Credits: Bryce Durbin / TechCrunch

A court in Houston has authorized an FBI operation to "copy and remove" backdoors from hundreds of Microsoft Exchange email servers in the United States, months after hackers used four previously undiscovered vulnerabilities to attack thousands of networks.

The Justice Department announced the operation on Tuesday, which it described as "successful."

U.S. Attorneys » Southern District of Texas » News

Department of Justice

U.S. Attorney's Office

Southern District of Texas

SHARE

FOR IMMEDIATE RELEASE

Tuesday, April 13, 2021

Justice Department announces court-authorized effort to disrupt exploitation of Microsoft Exchange Server vulnerabilities

Action copied and removed web shells that provided backdoor access to servers, but additional steps may be required to patch Exchange Server software and expel hackers from victim networks.

HOUSTON – Authorities have executed a court-authorized operation to copy and remove malicious web shells from hundreds of vulnerable computers in the United States. They were running on-premises versions of Microsoft Exchange Server software used to provide enterprise-level email service.

Through January and February 2021, certain hacking groups exploited zero-day vulnerabilities in Microsoft Exchange Server software to access email accounts and place web shells for continued access. Web shells are pieces of code or scripts that enable remote administration. Other hacking groups followed suit starting in early March after the vulnerability and patch were publicized.

Many infected system owners successfully removed the web shells from thousands of computers. Others appeared unable to do so, and hundreds of such web shells persisted unmitigated. This operation removed one early hacking group's remaining web shells which could have been used to maintain and escalate persistent, unauthorized access to U.S. networks. The FBI conducted the removal by issuing a command through the web shell to the server, which was designed to cause the server to delete only the web shell (identified by its unique file path).

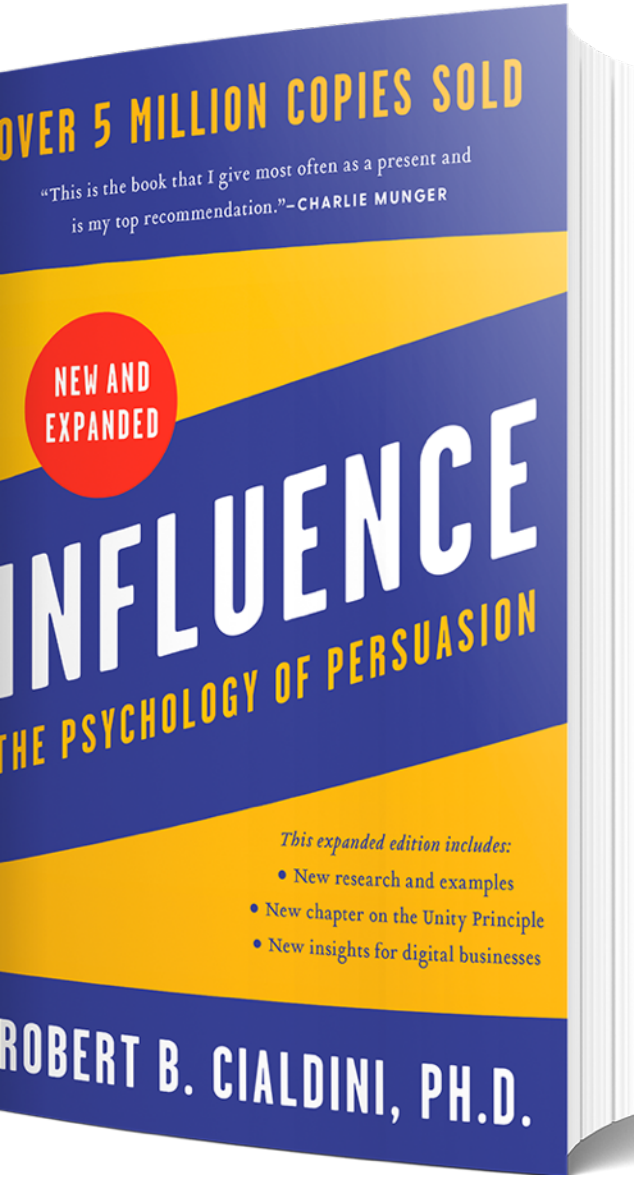
"Today's court-authorized removal of the malicious web shells demonstrates the Department's commitment to disrupt hacking activity using all of our legal tools, not just prosecutions," said Assistant Attorney General John C. Demers for the Justice Department's National Security Division. "Combined with the private sector's and other government agencies' efforts to date, including the release of detection

Demo
(Exchange)

Managed Services Providers and Third-Party Risk

Pretexting: The act of creating an invented scenario in order to…

…persuade a targeted victim to release information or perform some action.



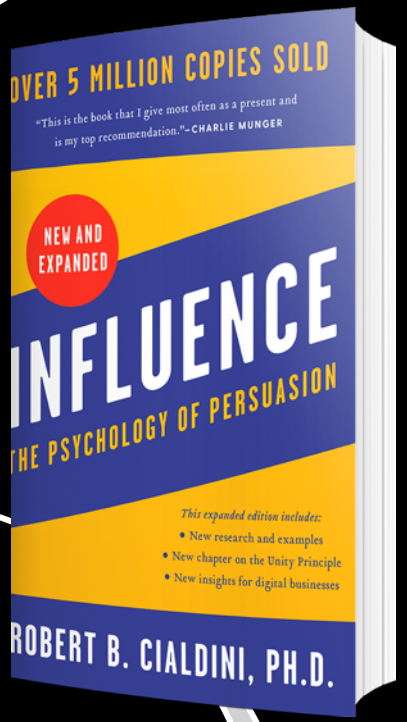
igation Team

"If it Hadn't Been for the Prompt Work of the Medics": FSB Officer Inadvertently Confesses Murder Plot to Navalny

December 21, 2020 FSB Navalny

- Bellingcat and its partners reported that Russia's Federal Security Service (FSB) was implicated in the near-fatal nerve-agent poisoning of Alexey Navalny on 20 August 2020. The report identified eight clandestine operatives with medical and chemical/biological warfare expertise working under the guise of the FSB's Criminalistics Institute who had tailed Alexey Navalny on more than 30 occasions since 2017. At least three of these operatives were in the close vicinity of Navalny near the time of his poisoning.
- During his year-end press conference on Thursday of last week, Russian president Vladimir Putin did not deny Bellingcat's findings, which detailed how these FSB operatives had been tailing Navalny,

Cialdini's Principles of Persuasion



1. Reciprocation
2. Commitment & Consistency
3. Social Proof
4. Liking
5. Authority
6. Scarcity
7. Unity

Demo
(VCenter)

Final Thoughts & Takeaways


Thank You
RISK ALERT
KnowBe4
Human error. Conquered.