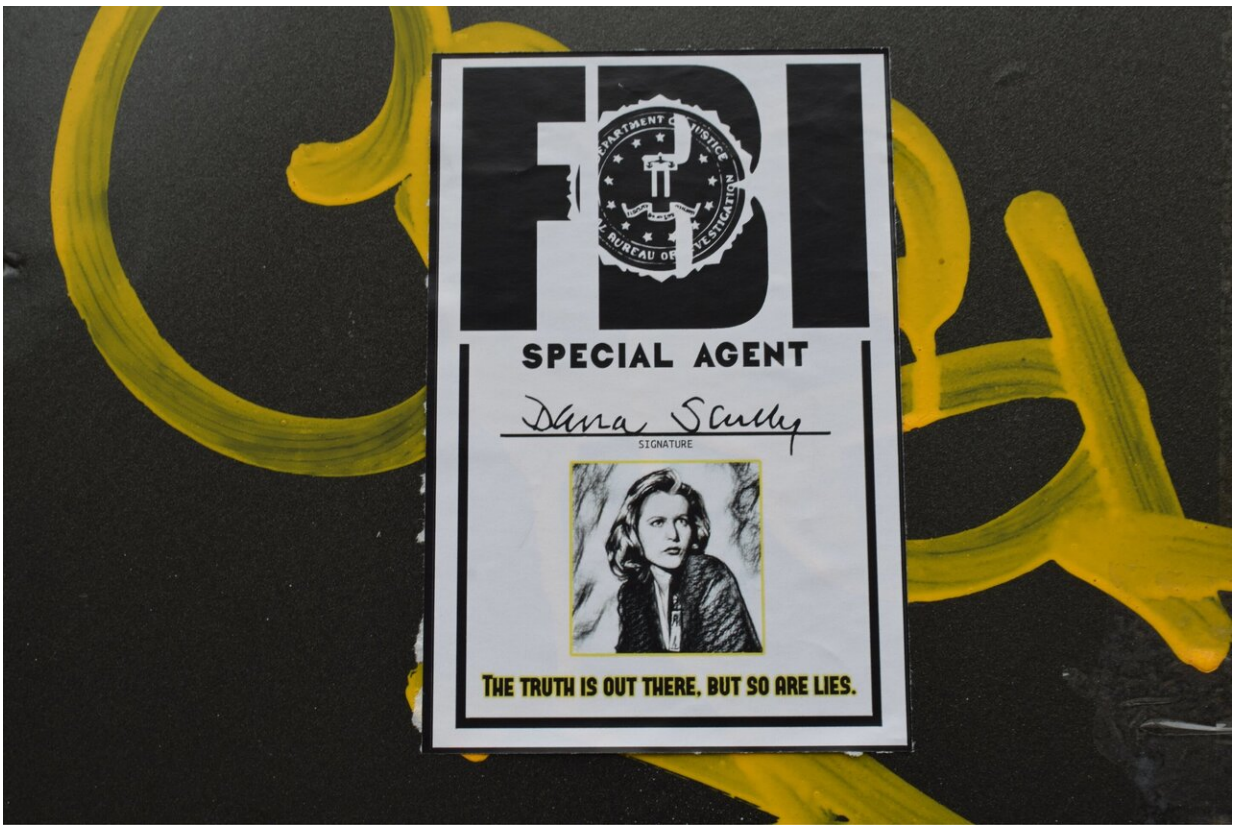
The FBI is breaking into corporate computers to remove malicious code: Cyber defense or overreach?

April 26 2021, by Scott Shackelford



Credit: Unsplash/CC0 Public Domain

The FBI has the authority right now to access privately owned computers without their owners' knowledge or consent, and to delete software. It's

part of a government effort to contain the continuing attacks on corporate networks running Microsoft Exchange software, and it's an unprecedented intrusion that's raising legal questions about just how far the government can go.

On April 9, the United States District Court for the Southern District of Texas approved a search warrant allowing the U.S. Department of Justice to carry out the operation.

The software the FBI is deleting is malicious code installed by hackers to take control of a victim's computer. Hackers have used the code to access vast amounts of private email messages and to launch ransomware attacks. The authority the Justice Department relied on and the way the FBI carried out the operation set important precedents. They also raise questions about the power of courts to regulate cybersecurity without the consent of the owners of the targeted computers.

As a cybersecurity scholar, I have studied this type of cybersecurity, dubbed active defense, and how the public and private sectors have relied on each other for cybersecurity for years. Public-private cooperation is critical for managing the wide range of cyber threats facing the U.S. But it poses challenges, including determining how far the government can go in the name of national security. It's also important for Congress and the courts to oversee this balancing act.

Exchange server hack

Since at least January 2021, hacking groups have been using zero-day exploits—meaning previously unknown vulnerabilities—in Microsoft Exchange to access email accounts. The hackers used this access to insert web shells, software that allows them to remotely control the compromised systems and networks. Tens of thousands of email users and organizations have been affected. One result has been a series of

ransomware attacks, which encrypt victims' files and hold the keys to decrypt them for ransom.

On March 2, 2021, Microsoft announced that a hacking group code named Hafnium had been using multiple zero-day exploits to install web shells with unique file names and paths. This makes it challenging for administrators to remove the malicious code, even with the tools and patches Microsoft and cybersecurity firms have released to assist the victims.

The FBI is accessing hundreds of these mail servers in corporate networks. The search warrant allows the FBI to access the web shells, enter the previously discovered password for a web shell, make a copy for evidence, and then delete the web shell. The FBI, though, was not authorized to remove any other malware that hackers might have installed during the breach or otherwise access the contents of the servers.

What makes this case unique is both the scope of the FBI's actions to remove the web shells and the unprecedented intrusion into privately owned computers without the owners' consent. The FBI undertook the operation without consent because of the large number of unprotected systems throughout U.S. networks and the urgency of the threat.

The action demonstrates the Justice Department's commitment to using "all of our legal tools," Assistant Attorney General John Demers said in a statement.

The total number of compromised firms remains murky given that the figure is redacted in the court documents, but it could be as many as 68,000 Exchange servers, which would potentially affect millions of email users. New malware attacks on Microsoft Exchange servers continue to surface, and the FBI is continuing to undertake court-

authorized action to remove the malicious code.

Active defense

The shift toward a more active U.S. cybersecurity strategy began under the Obama administration with the establishment of U.S. Cyber Command in 2010. The emphasis at the time remained on deterrence by denial, meaning making computers harder to hack. This includes using a layered defense, also known as defense in depth, to make it more difficult, expensive and time-consuming to break into networks.

The alternative is to go after hackers, a strategy dubbed defend forward. Since 2018, the U.S. government has ramped up defend forward, as seen in U.S. actions against Russian groups in the 2018 and 2020 election cycles in which U.S. Cyber Command personnel identified and disrupted Russian online propaganda campaigns.

The Biden administration has continued this trend, coupled with new sanctions on Russia in response to the SolarWinds espionage campaign. That attack, which the U.S. government attributes to hackers connected to Russian intelligence services, used vulnerabilities in commercial software to break into U.S. government agencies. This new FBI action similarly pushes the envelope of active defense, in this case to clean up the aftermath of domestic breaches, though without the awareness—or consent—of the affected organizations.

The law and the courts

The Computer Fraud and Abuse Act generally makes it illegal to access a computer without authorization. This law, though, does not apply to the government.

The FBI has the power to remove malicious code from private computers without permission thanks to a change in 2016 to Rule 41 of the Federal Rules of Criminal Procedure. This revision was designed in part to enable the U.S. government to more easily battle botnets and aid other cybercrime investigations in situations where the perpetrators' locations remained unknown. It permits the FBI to access computers outside the jurisdiction of a search warrant.

This action highlights the precedent, and power, of courts becoming de facto cybersecurity regulators that can empower the Department of Justice to clean up large-scale deployments of malicious code of the kind seen in the Exchange hack. In 2017, for example, the FBI made use of the expanded Rule 41 to take down a global botnet that harvested victims information and used their computers to send spam emails.

Important legal issues remain unresolved with the FBI's current operation. One is the question of liability. What if, for example, the privately owned computers were damaged in the FBI's process of removing the malicious code? Another issue is how to balance private property rights against national security needs in cases like this. What is clear, though, is that under this authority the FBI could hack into computers at will, and without the need for a specific search warrant.

National security and the private sector

Rob Joyce, NSA's cybersecurity director, said that cybersecurity is national security. This statement may seem uncontroversial. But it does portend a sea change in the government's responsibility for cybersecurity, which has largely been left up to the private sector.

Much of U.S. critical infrastructure, which includes computer networks, is in private hands. Yet companies have not always made the necessary investments to protect their customers. This raises the question of

whether there has been a market failure in cybersecurity where economic incentives haven't been sufficient to result in adequate cyber defenses. With the FBI's actions, the Biden administration may be implicitly acknowledging such a market failure.

Provided by The Conversation