Department of Justice
U.S. Attorney's Office
Southern District of Texas

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 tools and patches, we are together showing the strength that public-private partnership brings to our country's cybersecurity. There's no doubt that more work remains to be done, but let there also be no doubt that the Department is committed to playing its integral and necessary role in such efforts."

"Combatting cyber threats requires partnerships with private sector and government colleagues," said Acting U.S. Attorney Jennifer B. Lowery of the Southern District of Texas. "This court-authorized operation to copy and remove malicious web shells from hundreds of vulnerable computers shows our commitment to use any viable resource to fight cyber criminals. We will continue to do so in coordination with our partners and with the court to combat the threat until it is alleviated, and we can further protect our citizens from these malicious cyber-breaches."

"This operation is an example of the FBI's commitment to combatting cyber threats through our enduring federal and private sector partnerships," said Acting Assistant Director Tonya Ugoretz of the FBI's Cyber Division. "Our successful action should serve as a reminder to malicious cyber actors that we will impose risk and consequences for cyber intrusions that threaten the national security and public safety of the American people and our international partners. The FBI will continue to use all tools available to us as the lead domestic law enforcement and intelligence agency to hold malicious cyber actors accountable for their actions."

On March 2, Microsoft announced that a hacking group used multiple zero-day vulnerabilities to target computers running Microsoft Exchange Server software. Various other hacking groups also have used these vulnerabilities to install web shells on thousands of victim computers, including those located the United States. Because the web shells the FBI removed each had a unique file path and name, they may have been more challenging for individual server owners to detect and eliminate than other web shells.

Throughout March, Microsoft and other industry partners released detection tools, patches and other information to assist victim entities in identifying and mitigating this cyber incident. Additionally, the FBI and the Cybersecurity and Infrastructure Security Agency released a Joint Advisory on Compromise of Microsoft Exchange Server on March 10. Despite these efforts, by the end of March, hundreds of web shells remained on certain United States-based computers running Microsoft Exchange Server software.

This operation was successful in copying and removing those web shells. However, it did not patch any Microsoft Exchange Server zero-day vulnerabilities or search for or remove any additional malware or hacking tools that hacking groups may have placed on victim networks by exploiting the web shells. The Department strongly encourages network defenders to review Microsoft's remediation guidance and the March 10 Joint Advisory for further guidance on detection and patching.

The FBI is attempting to provide notice of the court-authorized operation to all owners or operators of the computers from which it removed the hacking group's web shells. For those victims with publicly available contact information, the FBI will send an e-mail message from an official FBI e-mail account (@FBI.gov) notifying the victim of the search. For those victims whose contact information is not publicly available, the FBI will send an e-mail message from the same FBI e-mail account to providers (such as a victim's ISP) who are believed to have that contact information and ask them to provide notice to the victim.

If you believe you have a compromised computer running Microsoft Exchange Server, please contact your local FBI Field Office for assistance. The FBI continues to conduct a thorough and methodical investigation into this cyber incident.