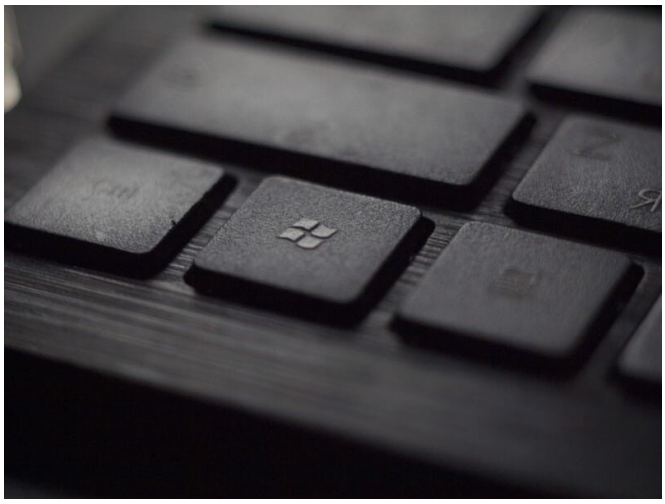
FBI launches an effort to mitigate attacker use of Microsoft Exchange vulnerabilities

14 April 2021, by Sarah Katz



Microsoft. Credit: Unsplash

While web shells have been removed that previously provided attackers access to Microsoft Exchange Servers, the FBI has revealed that some malicious software might remain that hackers are still using as backdoors into victim networks.

Now, U.S. Justice authorities have initiated the copy and removal of evil web shells from hundreds of computers running on-premises Microsoft Exchange Server software to operate their corporate email services.

These attacks began back in January and February of 2021 when various hackers discovered and exploited zero-day vulnerabilities in Microsoft Exchange Server software. The hackers took advantage of these vulnerabilities to set up backdoors and gain persistent access to these servers, right up until they were caught in March of 2021. Even after the initial hackers came to light, more attackers looked for ways to attack following patching and publication of these vulnerabilities.

While thousands of victims of this attack managed to remove these backdoors, hundreds of malicious web shells have gone unremedied. For the target servers that the FBI succeeded in salvaging, they ended up writing a command from the web shell to the server, triggering the server to delete the web shell after identifying the shell's unique file path.

So far, authorities have expressed positive sentiment regarding the ability of private and public organizations to join cybersecurity forces in order to oppose this threat. In fact, the FBI has already partnered with international colleagues in the field in order to keep an eye on further vulnerabilities and threats of this nature.

Indeed, since this attack came to light in March, Microsoft and its various partners have taken significant efforts to provide their thousands of customers with the information and tools to help mitigate this threat, even for those organizations whose servers have already been impacted.

However, despite many Microsoft Exchange Server users successfully removing evil web shells on their networks, the FBI warns that the original zero-day vulnerabilities have still not been fully patched. Therefore, the company recommends that all affected organizations continue to monitor and investigate their environments for potential malicious presence.

At this time, the FBI intends to notify all entities from whose servers malicious web shells associated with these attacks have been removed. They expect network defenders of impacted organizations might encounter the challenge of detecting these evil web shells based on their unique file name and path.

For now, the FBI and the Cybersecurity and Infrastructure Security Agency have collaborated toward a Joint Advisory on Microsoft Exchange Server to tackle this incident.

More information: U.S. Attorney's Office, Southern District of Texas. "Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities." The United States Department of Justice, U.S. Department of Justice, 13 Apr. 2021, www.justice.gov/usao-sdtx/pr/j … ploitation-microsoft