Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
The dangers of the Microsoft Exchange Server vulnerabilities

Satnam Narang, Tenable

In March, Microsoft issued an out-of-band update addressing four critical zero-days in Microsoft Exchange Server that were exploited in the wild by an advanced persistent threat group known as Hafnium. In April, Microsoft patched four more critical, yet unrelated, Exchange Server vulnerabilities.

The moment the zero-days became public, it opened up a can of worms, and the original groups exploiting these flaws were no longer the only ones looking to take advantage of these vulnerabilities. The presence of these Exchange Server flaws meant every organisation was potentially at risk. After the vulnerabilities were disclosed, reports suggested that over 60,000 organisations had been compromised.

Looking at the original threat actors’ approach, it appears the plan was to exploit the flaws with a view to maintain persistence wherever they could. From what has since been published, these attackers were using automated scanning and exploitation to capitalise on the vulnerabilities and successfully implanted web shells so that they could maintain persistence, assuming the organisation did nothing else besides applying the patches.

It is important to recognise that these attackers weren’t focused just on attacking big-name organisations. Instead, they were looking for any and every organisation that was open and vulnerable, and there were many. The truth is that no potential target is ‘valueless’ to cyber criminals just because of its size or low profile.

Once Microsoft disclosed the zero-day vulnerabilities, other threat actors looked to get in on the action, knowing that not all organisations would be able to apply patches quickly, if at all.

The reason this is a serious concern among the security community, not least because these attacks were ongoing, were the systems involved and the information being exposed. When you think of how an organisation functions today, particularly given the current work-from-home strategy, the vast majority of communication occurs via email. That means a lot of sensitive data travels in and out of individuals’ mailboxes, including customer correspondence, financial information, intellectual property and medical data, to name a few.

Of course, compromising the server is just the initial entry point. Typically, having gained an initial foothold in an environment, attackers will look to move laterally to further infiltrate other systems, move into private areas to cause damage or steal data, and stay within the infrastructure for as long as possible. Once inside, simply closing the hole they climbed through doesn’t completely eliminate the threat.

It’s imperative that organisations follow the guidance that vendors issue when vulnerabilities are identified and take direct action and/or update affected systems – on this occasion Exchange Servers – as a matter of urgency. Beyond that, security teams need to assess systems to determine if an attacker is already ‘through the door’ and take the necessary steps to evict them.

Microsoft published indicators of compromise (IOCs) associated with these attacks that list files known to be malicious to help organisations find the webshells. It has also released a detection tool for the vulnerabilities – details here: http://bit.ly/MS-IOC-tool. Additionally, the FBI and the US Cyber security and Infrastructure Security Agency (CISA) issued a joint cyber security advisory about the Exchange Server attacks and included a list of file path indicators to examine for potential compromise. The advisory can be found here: http://bit.ly/CFS-FBI-CISA.

There are always lessons to be learned from these situations, but perhaps the biggest is that Microsoft does not issue an out-of-band update lightly. When it does, security teams should drop everything and be ready to take immediate action.