Warning: ‘Hundreds of Thousands’ of Microsoft Servers Hacked in Ongoing Attack

Earlier this week, the Microsoft Threat Intelligence Center, Microsoft 365 Defender Threat Intelligence Team and Microsoft 365 Security issued a joint advisory warning that on-premises Exchange servers were being attacked. The nature of that attack, using no less than four zero-day exploits (for previously unreported vulnerabilities) meant that an out-of-band emergency patch had been released. Microsoft, along with the U.S. Department of Homeland Security, advised everyone to update immediately. The DHS even went as far as to issue an emergency directive requiring federal civilian branch agencies to do so in short order.

Initially, Microsoft stated that the attack, attributed to Chinese nation-state threat actors known as HAFNIUM, was "limited and targeted", but now reports are emerging that hundreds of thousands of servers have been compromised, with talk of an exploit rate in the region of 1,000 servers every hour. This attack has expanded way beyond the reach of those original nation-state players, it would seem, and it is now open season on Microsoft Exchange for cybercriminals.

Investigative cybersecurity journalist, Brian Krebs, has reported that, according to experts who have briefed U.S. national security advisors, hundreds of thousands of servers have been successfully hacked globally. In the U.S. alone, this number is said to be more than 30,000 compromised servers.

Given that the attacks are thought to have started on January 6, this might come as no great surprise. However, it would appear that the threat itself has changed gear this week, and there are now multiple campaigns compromising unpatched servers at a rate of knots.

Writing at Wired, Andy Greenberg quotes a security researcher "with knowledge of the investigation," saying that there are "thousands of servers compromised per hour" globally. This doesn't mean that all of those organizations have been targeted by HAFNIUM, but rather these are likely the result of automated scans looking for unpatched machines.

Indeed, Microsoft has confirmed that it "continues to see increased use of these vulnerabilities in attacks targeting unpatched systems by multiple malicious actors beyond HAFNIUM."

Obviously, the previously stated advice to update those on-premises Exchange servers now remains the best mitigation option. Even White House press secretary Jen Psaki warned, on March 5, that this should be done immediately. Microsoft has published interim mitigations for those unable to patch their Exchange servers.

But what if your server has already been got at? Indeed, how can you tell?

Microsoft has released a Nmap script for checking your Exchange server for indicators of compromise of these exploits, and you can find it on GitHub. The Cybersecurity and Infrastructure Security Agency (CISA) has also published a list of tactics, techniques and procedures. Meanwhile, FireEye Mandiant researchers have a list of investigation tips, including indicators of compromise.

References:

https://www.forbes.com/sites/daveywinder/2021/03/06/warning-hundreds-of-thousands-of-microsoft-servers-hacked-in-ongoing-attack/?ss=cybersecurity&sh=1e6ea47a28e6

https://newsrnd.com/life/2021-03-07-%0A---hacker-attack-on-microsoft--hundreds-of-thousands-of-email-servers-affected--apparently-germany-is-particularly-at-risk%0A--.S1K6qoGX_.html

https://oltnews.com/warning-hundreds-of-thousands-of-microsoft-servers-hacked-in-ongoing-attack-forbes

http://newsreadonline.com/microsoft-vulnerability-hundreds-of-thousands-of-companies-hacked/