NIGC Tech Alert

Tribal Gaming Operation attacked by “Hafnium” Microsoft Exchange Global Attack

The threat of attacks on Information Technology (IT) systems is always present and one of the many reasons for the need for strong IT system controls and security measures. Recently, a tribal operation was the victim of the latest Microsoft Exchange Global Attack better known as the “Hafnium” attack.

This particular attack has been detected lurking in many live environments, in some cases going undetected for months. It cannot be understated that this is not a typical vulnerability. The evidence of the Hafnium vulnerability and resulting attacks only became apparent in early March 2021 and the scope continues to grow. This attack is particularly damaging because Hafnium uses on premise Microsoft Exchange Servers to siphon critical information from your environments and gain administrative level access to other systems via Microsoft Active Directory. To date, the vulnerability is not known to impact Exchange Online or Microsoft 365 cloud email services. At this point, what is known is the most recent attack originated in China using a previously unknown vulnerability in Microsoft Exchange. After Microsoft revealed the attack, other criminal groups obtained the vulnerability and began exploiting it. Criminals are utilizing the vulnerability to steal sensitive banking and bill payment information, to siphon computer power for cryptocurrency mining, and to hold systems hostage via ransomware.

In the recent tribal operations case, each of your accounting and financial officers need to be vigilant and verify directives received via email prior to making large payments or transfer of funds. Also, confirm routing and account numbers have not been supplanted with nefarious information by the threat actor.   These actors are intruding and watching for regular or repeated directives and will catch and replace one with their own spoof email causing the operation to issue or transfer payment to the threat actors account.

In the NIGC Cybersecurity Readiness document, we discussed ransomware: a family of malicious software that acts like a Trojan horse. The software runs quietly in the background of an infected system and searches for and encrypts key files such as players club databases and casino management systems. The files become locked and unusable to the victim until a decryption key is applied. Once the encryption process is complete, the attacker notifies the victim and demands a ransom.

The Hafnium attack is known as a “zero-day vulnerability” which means the vulnerability had no patch at the time of discovery. Microsoft has identified the attack as underway and therefore could not have been prevented via system or network scans or regular patch cycles. Microsoft has sent out a security patch to update Exchange server systems and a script to verify if the vulnerability has already been exploited on your system. It is highly recommended by security experts that if you are running an affected Exchange Server to run both the script and the patch as soon as possible.

March 18, 2021

Tribal Gaming Operation attacked by “Hafnium” Microsoft Exchange Global Attack

If your organization is determined to have been previously compromised in weeks or months past, threat actors could have installed one of many types of back-doors for persistent access to that Exchange server and possibly on other servers and systems inside your network. To repeat, if an organization was compromised, even after running the Microsoft security patch and removing the vulnerability on the infected Exchange Server, there are very likely other infected systems within the same network or networks. Monitoring closely for signs of an attack especially in the coming weeks and preparations to minimize the impact of such an attack are strongly recommended.

While criminal organizations exploiting this vulnerability appear to be mostly working out of Eastern Europe and Asia, there is evidence of criminals utilizing domestic servers such as Amazon’s AWS to facilitate the attack. Normal geoblocking firewall rules may not be sufficient to minimize the threat of an attack.

The FBI advises against paying ransom fees. Doing so rewards these criminals’ illegal actions and provides no guarantee that the files will be decrypted after payment. NIGC recommends strong IT controls be put in place at tribal regulatory agencies and gaming operations to mitigate these threat actors.

Should assistance be necessary regarding the types of systems and controls to put in place to reduce the risk of ransomware or other such IT vector attacks, please do not hesitate to reach out to the NIGC at itsupport@nigc.gov. The NIGC offers technical assistance, training, IT audits, and other tools and resources to help identify potential vulnerable areas and improve security and IT controls.

Resources

CISA posting on the Hafnium attack:
https://us-cert.cisa.gov/ncas/alerts/aa21-062a

Additional information regarding Hafnium from Microsoft:
https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/

Microsoft Security Response Center Patch link:
https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/

FBI recommendation on ransomware:
https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

March 18, 2021