CYBER DEFENSE INTELLIGENCE CENTER

March 26, 2021

Microsoft Exchange On-Premise (Hafnium) Attack

SCOPE: This intelligence briefing affects all Microsoft Exchange On-Premise users, across all industries, worldwide.

Attack Description
On March 3, 2021 CISA issued an Emergency Directive (ED) 21-02 requiring federal civilian departments and agencies running Microsoft Exchange on-premises products to update or disconnect those products from their networks until the organizations can install Microsoft provided patches.

The attacke involved 4 zero-day vulnerabilities that targeted MS Exchange On-Premise. Vulnerabilities allow attackers to bypass authentication on the Exchange server, obtain administrator rights, install malware, and execute arbitrary commands. While patching will prevent future attacks of this nature, Patching does not remediate existing compromises. This attack has Exfiltrated entire mailboxes and data.

If you have Microsoft Exchange On-Premise you should assume you have been attacked.

Attack Methodology
The attack, while very sophisticated in nature, was very easy to execute.

The attack started with a "server-side forgery" allowing the execution of arbitrary code. Once compromised the attack embedded Web shells into the server allowing the exfiltration of data and entire mailboxes. Attackers furthered the hack by initiating lateral movement.

Multiple ransomware are now targeting unpatched servers with the same exploits (DearCry, Revil and BlackKingdom)

Impacts
At least 30,000 and up to 250,000 servers globally have been impacted by this attack. The amount of exfiltrated data is currently unknown but assumed to be significant.

Threat actors were able to

- Read sensitive information in mailboxes of users
- Exfiltrate entire mailboxes
- Dump local credentials
- Add new user accounts
- Dump Active Directory database (NTDS.DIT)
- Launch lateral attacks on other systems in the network

Mass amounts of sensitive information and data were compromised and can be used in future attacks.

Impacts are still being discovered and could include compromise of classified information, corporate secrets and private information.

Attack Attribution

Current attribution is to Chinese state-sponsored threat actor, Hafnium. It is possible that other cybercriminal organizations could be involved as well. Hafnium typically targets United States entities in the infectious disease research, legal, higher education institution, defense contractor, policy think tank, and NGO industry sectors. They look to leverage US-based hosting providers to launch attacks using VPS (Virtual Private Servers).

Actions – IMMEDIATE ACTIONS ARE REQUIRED

1. Immediately apply latest patches from Microsoft. (If you cannot patch, immediately deploy Microsoft interim attack prevention modifications)
2. Conduct analysis of the Exchange server to identify active compromises or indicators of compromise *(Microsoft and other vendors have released threat hunting tools to assist in the effort)*
3. If indicators of Compromise or active threats exist, remove all threats and then conduct a thorough analysis of the activities including any mailbox access and modifications.
4. Ensure all Anti-Malware tools are up to date.

Defense In Depth Protections

- Leverage Strong vulnerability management and patching process.
- Use vendor-supported versions of all operating systems and software. (Latest Supported versions where possible)
- Deploy Next-gen Endpoint protection
- Implement “Defense-in-depth” architecture providing “intelligent overlaps” in their detection and protection capabilities including systems that address the monitoring of the SCADA system.
- Ensure passwords meet complexity, length and management requirements
- Leverage Zero-trust Technologies and Multi-factor authentication
- Limit exposed services and leverage “blocking” rules to limit access to the services where possible
- Utilize Advanced file sanitization tools such as “Content Disarmament and Reconstruction” tools.
- Deploy strong monitoring and auditing capabilities
- Design an effective Vendor risk management process
- Understand Threat Intelligence and TTP’s (Tactics, Techniques and Procedures).

Prepared by the Cyber Defense Intelligence Center Analysis Team.