Cynet Publishes New Information on HAFNIUM APT Attack on Microsoft Exchange

Additional APT groups seem to be targeting known vulnerabilities in MS Exchange

BOSTON, MA, UNITED STATES, March 17, 2021 /EINPresswire.com/ -- Cynet (http://www.cynet.com), provider of the world's first autonomous XDR platform, today announced a post-mortem of the HAFNIUM APT attack, involving the active exploitation of on-premises Microsoft Exchange Server deployments through remote code execution attacks. Over the past several days, the Cynet Cyber Research team identified a large number of China Chopper-related web-shell attacks linked to the recent zero-day attacks on Microsoft Exchange.

China Chopper is a web shell backdoor that allows threat groups to remotely access an enterprise network by abusing the client-side application to gain remote control of the compromised system. The threat group gains an initial foothold on the compromised machine for further post-exploitation activities such as persistence, privilege escalation, lateral movement and impact. China Chopper contains a GUI interface allowing the threat groups to manage and control the web-shell attack commands. Threat groups identified using China Chopper backdoor include:

- Leviathan
- Threat Group-3390
- Soft Cell
- APT41

The Cynet cyber threat researchers, along with the use of Cynet 360, detected and prevented China Chopper web shell activity on several customers' Exchange Servers. In all cases, the compromised servers were Internet Information Services (IIS), which potentially means that these attacks were related to the Microsoft vulnerabilities just discovered. Because certain APT groups use the China Chopper tool and it was specifically used to attack the vulnerable Microsoft services, it is now believed that additional APT groups may be targeting the identified vulnerabilities in MS Exchange.

"Cynet is working around the clock to monitor this situation and provide businesses with the best protection possible, ensuring that every aspect of this attack scenario is covered," said Max Malyutin, Senior Threat Researcher for Cynet. "In addition to the use of Cynet 360, minimize the damage potential of this attack by installing the latest patches to keep your environment up-to date in accordance with Microsoft's most current recommendations."

To view the complete Cynet analysis of this attack, please visit the Cynet blog at: https://www.cynet.com/blog/china-chopper-observed-in-recent-ms-exchange-server-attacks/

Tweet this: @Cynet Publishes Review of HAFNIUM APT Attack - https://bit.ly/2UgxHCE

Resources
To learn more about Cynet:
- Visit Cynet at https://cynet.com
- Follow Cynet on Twitter at http://www.twitter.com/cynet360
- Follow Cynet on LinkedIn at https://www.linkedin.com/company/cynet-security/

About Cynet
Cynet 360 is the world's first Autonomous Breach Protection platform that natively integrates XDR endpoint, user and network attack prevention and detection capabilities with an incident engine that fully automates investigation and remediation actions, backed by a 24/7 world-class MDR service. End to end, fully automated breach protection is now within reach of any organization, regardless of security team size and skill level. Visit: https://www.cynet.com.

- END -

Joe Austin
Public Relations
+1 818-332-6166
email us here
Visit us on social media:
Facebook
Twitter
