You Don’t Know the HAFNIUM of it…

cyborgsecurity.com/blog/you-dont-know-the-hafnium-of-it/

March 11, 2021

If you want to get access to Cyborg Security’s Community Defense Measures for the HAFNIUM attack, including our free detection content, click here or scroll down to the “Detection Content” section! Keep reading for an overview of the attack and what we know so far!

After little more than a month of reprieve, the infosec community is, once again, back into it. This time the target, though, is even more prevalent than SolarWinds’ Orion. Now the target is Microsoft’s Exchange, and the exploited vulnerability allows for remote code execution (or RCE). We’ve distilled down the facts of the HAFNIUM attack to answer the most important questions.

Table of Contents

What We Know So Far about HAFNIUM

Who Are They?

On 2 March 2021, Microsoft released a blog article detailing a new threat actor it had dubbed **HAFNIUM**. Microsoft, the blog identified, has observed the actor exploiting several 0-day vulnerabilities.

Microsoft also highlighted that the HAFNIUM group had previously targeted other organizations. The group, Microsoft identified, has focused on the exploitation of Internet-facing services in the past.

Later that same day, the company Volexity also released a blog article. In their article, they identified that they observed the attacks beginning as early as 3 January 2021.

Hot on the heels of the Microsoft and Volexity blogs, other vendors began to contribute information. On 4 March 2021, FireEye's Mandiant Intelligence release their own blog post. In it, FireEye identified that they tracked the activity under three separate activity clusters:

- UNC2639
- UNC2640
- UNC2643

One particularly important point in this blog article is that FireEye detected this activity all the way back in January 2021. The article also highlighted various TTPs and tools the actors used. This included:

- ASPXSPY
- Covenant
- China Chopper
- Nishang
- PowerCat
- Cobalt Strike

They also described the actors' method of deploying webshells on compromised Exchange servers. These webshells were unique though. The webshells detected the presence of specific security products and warn the actors. The security products it detected included FireEye, Carbon Black and Crowdstrike. They described the actors technique of dropping more complex webshells over time. This appears to be to avoid detection.

In time, other vendors have also come forward, including Symantec. They identified that they track HAFNIUM, under the name **Ant**.

Where is HAFNIUM From?

Attribution can be a tricky topic in cyber threat intelligence. Despite this fact, several sources, including Microsoft, have indicated that the HAFNIUM group is "… state-sponsored and operating out of China …"

Who is Being Targeted?

At this point, the targeting of HAFNIUM appears opportunistic. Indeed, since Microsoft released their initial blog, the actors have "… stepped up attacks on any vulnerable, unpatched Exchange servers (2013, 2016, and 2019) worldwide." The HAFNIUM group, though, has targeted organizations in the past.

As both Microsoft and FireEye mentioned, HAFNIUM is a group with a bit of track record. Microsoft identified that they have targeted several industries in the past. These included

- Infectious disease research

- Law firms
- Universities
- Defense contractors
- Think tanks
- Non-Governmental Organizations (NGOs)

FireEye also mentioned that they had observed several industries affected by the new attack, including

- Retailers
- Local Governments
- Universities
- Engineering Firms

They also identified that there is possible related activity observed in Asia as well

- Federal governments
- Telecommunications providers

What Are The Actors Doing?

Since early January, the actors have been exploiting several 0-day vulnerabilities in Exchange. The vulnerabilities, which affect on-premise versions of Microsoft Exchange only, are:

- CVE-2021-26855
- CVE-2021-26857
- CVE-2021-26858
- CVE-2021-27065

Once the actors establish a foothold in the environment, they will deploy one or more web shells. These are small bits of code that gives the actors control over the system. Once in the environment, the actors use a variety of techniques.

HAFNIUM MITRE ATT&CK Techniques

T1003.001 – OS Credential Dumping: LSASS Memory
T1059.001 – Command and Scripting Interpreter: PowerShell
T1114.001 – Email Collection: Local Email Collection
T1136 – Create Account
T1003.003 – OS Credential Dumping: NTDS
T1021.002 – Remote Services: SMB/Windows Admin Shares
T1005 – Data from Local System
T1027 – Obfuscated Files or Information
T1046 – Network Service Scanning

T1059 – Command and Scripting Interpreter
T1070 – Indicator Removal on Host
T1071 – Application Layer Protocol
T1074.002 – Data Staged: Remote Data Staging
T1083 – File and Directory Discovery
T1110 – Brute Force
T1190 – Exploit Public-Facing Application
T1505 – Server Software Component
T1560.001 – Archive Collected Data: Archive via Utility
T1589.002 – Gather Victim Identity Information: Email Addresses
T1590.002 – Gather Victim Network Information: DNS

When Did All This Happen?

Reporting from both FireEye and Volexity state that the attacks were first observed in January. It is unknown whether this was the start of the campaign.

The bulk of the campaign appears to have taken place over February and March 2021.

What Should I Do?

What you should do next will likely depend on a few factors.

- Cyborg Security has released new advanced detection content through its Community Defense Measures (CDM) project. This content will alert organization to malicious behaviors related to the attacks.
- Microsoft has released a tool that will scan Exchange logs for suspicious and malicious modifications.
- Microsoft has also released security updates for Microsoft Exchange
- The Cybersecurity and Infrastructure Security Agency (CISA) has also released Alert AA21-062A. An important note about this is that CISA warns organizations: "… [if] your organization [sees] evidence of compromise, your incident response should begin with conducting forensic analysis to collect artifacts and perform triage …."
- The US' Department of Homeland Security also issued Emergency Directive 21-02.

Detection Content

To get Cyborg Security's HAFNIUM Community Defense Measures, click the botton below. No sign up required!

FREE DETECTION CONTENT