

# HAFNIUM, Operation Exchange Marauder, Silk Typhoon, Group G0125

Archived: 2026-04-05 18:20:50 UTC

Enterprise [T1098 Account Manipulation](#)

[HAFNIUM](#) has granted privileges to domain accounts and reset the password for default admin accounts. <sup>[2][3]</sup>

Enterprise [T1583 .003 Acquire Infrastructure: Virtual Private Server](#)

[HAFNIUM](#) has operated from leased virtual private servers (VPS) in the United States. <sup>[1]</sup>

[.005 Acquire Infrastructure: Botnet](#)

[HAFNIUM](#) has incorporated leased devices into covert networks to obfuscate communications. <sup>[3]</sup>

[.006 Acquire Infrastructure: Web Services](#)

[HAFNIUM](#) has acquired web services for use in C2 and exfiltration. <sup>[1]</sup>

Enterprise [T1071 .001 Application Layer Protocol: Web Protocols](#)

[HAFNIUM](#) has used open-source C2 frameworks, including [Covenant](#). <sup>[1]</sup>

Enterprise [T1560 .001 Archive Collected Data: Archive via Utility](#)

[HAFNIUM](#) has used 7-Zip and WinRAR to compress stolen files for exfiltration. <sup>[1][2]</sup>

Enterprise [T1119 Automated Collection](#)

[HAFNIUM](#) has used MSGraph to exfiltrate data from email, OneDrive, and SharePoint. <sup>[3]</sup>

Enterprise [T1110 .003 Brute Force: Password Spraying](#)

[HAFNIUM](#) has gained initial access through password spray attacks. <sup>[3]</sup>

Enterprise [T1059 .001 Command and Scripting Interpreter: PowerShell](#)

[HAFNIUM](#) has used the Exchange Power Shell module `Set-0abVirtualDirectoryPowerShell` to export mailbox data. <sup>[1][2]</sup>

[.003 Command and Scripting Interpreter: Windows Command Shell](#)

[HAFNIUM](#) has used `cmd.exe` to execute commands on the victim's machine. <sup>[5]</sup>

Enterprise [T1584 .005 Compromise Infrastructure: Botnet](#)

[HAFNIUM](#) has used compromised devices in covert networks to obfuscate communications.<sup>[3]</sup>

Enterprise [T1136 .002 Create Account: Domain Account](#)

[HAFNIUM](#) has created domain accounts.<sup>[2][3]</sup>

Enterprise [T1555 .006 Credentials from Password Stores: Cloud Secrets Management Stores](#)

[HAFNIUM](#) has moved laterally from on-premises environments to steal passwords from Azure key vaults.<sup>[3]</sup>

Enterprise [T1132 .001 Data Encoding: Standard Encoding](#)

[HAFNIUM](#) has used ASCII encoding for C2 traffic.<sup>[1]</sup>

Enterprise [T1530 Data from Cloud Storage](#)

[HAFNIUM](#) has exfiltrated data from OneDrive.<sup>[3]</sup>

Enterprise [T1213 .002 Data from Information Repositories: Sharepoint](#)

[HAFNIUM](#) has abused compromised credentials to exfiltrate data from SharePoint.<sup>[3]</sup>

Enterprise [T1005 Data from Local System](#)

[HAFNIUM](#) has collected data and files from a compromised machine.<sup>[5][3]</sup>

Enterprise [T1114 .002 Email Collection: Remote Email Collection](#)

[HAFNIUM](#) has used web shells and MSGraph to export mailbox data.<sup>[1][2][3]</sup>

Enterprise [T1567 .002 Exfiltration Over Web Service: Exfiltration to Cloud Storage](#)

[HAFNIUM](#) has exfiltrated data to file sharing sites, including MEGA.<sup>[1]</sup>

Enterprise [T1190 Exploit Public-Facing Application](#)

[HAFNIUM](#) has exploited multiple vulnerabilities to compromise edge devices and on-premises versions of Microsoft Exchange Server.<sup>[1][2][6][7][8][3]</sup>

Enterprise [T1068 Exploitation for Privilege Escalation](#)

[HAFNIUM](#) has targeted unpatched applications to elevate access in targeted organizations.<sup>[3]</sup>

Enterprise [T1083 File and Directory Discovery](#)

[HAFNIUM](#) has searched file contents on a compromised host.<sup>[5]</sup>

Enterprise [T1592 .004 Gather Victim Host Information: Client Configurations](#)

[HAFNIUM](#) has interacted with Office 365 tenants to gather details regarding target's environments.<sup>[1]</sup>

Enterprise [T1589 .002 Gather Victim Identity Information: Email Addresses](#)

[HAFNIUM](#) has collected e-mail addresses for users they intended to target.<sup>[2]</sup>

Enterprise [T1590 Gather Victim Network Information](#)

[HAFNIUM](#) gathered the fully qualified domain names (FQDNs) for targeted Exchange servers in the victim's environment.<sup>[2]</sup>

[.005 IP Addresses](#)

[HAFNIUM](#) has obtained IP addresses for publicly-accessible Exchange servers.<sup>[2]</sup>

Enterprise [T1564 .001 Hide Artifacts: Hidden Files and Directories](#)

[HAFNIUM](#) has hidden files on a compromised host.<sup>[5]</sup>

Enterprise [T1070 .001 Indicator Removal: Clear Windows Event Logs](#)

[HAFNIUM](#) has cleared actor-performed actions from logs.<sup>[3]</sup>

Enterprise [T1105 Ingress Tool Transfer](#)

[HAFNIUM](#) has downloaded malware and tools--including Nishang and PowerCat--onto a compromised host.<sup>[1][5]</sup>

Enterprise [T1095 Non-Application Layer Protocol](#)

[HAFNIUM](#) has used TCP for C2.<sup>[1]</sup>

Enterprise [T1003 .001 OS Credential Dumping: LSASS Memory](#)

[HAFNIUM](#) has used `procdump` to dump the LSASS process memory.<sup>[1][2][5]</sup>

[.003 OS Credential Dumping: NTDS](#)

[HAFNIUM](#) has stolen copies of the Active Directory database (NTDS.DIT).<sup>[2][3]</sup>

Enterprise [T1057 Process Discovery](#)

[HAFNIUM](#) has used `tasklist` to enumerate processes.<sup>[5]</sup>

Enterprise [T1018 Remote System Discovery](#)

[HAFNIUM](#) has enumerated domain controllers using `net group "Domain computers"` and `nltest /dclist`.<sup>[5]</sup>

Enterprise [T1593 .003 Search Open Websites/Domains: Code Repositories](#)

[HAFNIUM](#) has discovered leaked corporate credentials on public repositories including GitHub.<sup>[3]</sup>

Enterprise [T1505 .003 Server Software Component: Web Shell](#)

[HAFNIUM](#) has deployed multiple web shells on compromised servers including SIMPLESEESHARP, SPORTSBALL, [China Chopper](#), and [ASPXSpy](#).<sup>[1][2][6][7][5][3]</sup>

Enterprise [T1218 .011 System Binary Proxy Execution: Rundll32](#)

[HAFNIUM](#) has used `rundll32` to load malicious DLLs.<sup>[2]</sup>

Enterprise [T1016 System Network Configuration Discovery](#)

[HAFNIUM](#) has collected IP information via IPInfo.<sup>[5]</sup>

[.001 Internet Connection Discovery](#)

[HAFNIUM](#) has checked for network connectivity from a compromised host using `ping`, including attempts to contact `google[.]com`.<sup>[5]</sup>

Enterprise [T1033 System Owner/User Discovery](#)

[HAFNIUM](#) has used `whoami` to gather user information.<sup>[5]</sup>

Enterprise [T1199 Trusted Relationship](#)

[HAFNIUM](#) has used stolen API keys and credentials associated with privilege access management (PAM), cloud app providers, and cloud data management companies to access downstream customer environments.<sup>[3]</sup>

Enterprise [T1550 .001 Use Alternate Authentication Material: Application Access Token](#)

[HAFNIUM](#) has abused service principals with administrative permissions for data exfiltration.<sup>[3]</sup>

Enterprise [T1078 .003 Valid Accounts: Local Accounts](#)

[HAFNIUM](#) has used the NT AUTHORITY\SYSTEM account to create files on Exchange servers.<sup>[6]</sup>

[.004 Valid Accounts: Cloud Accounts](#)

[HAFNIUM](#) has abused service principals in compromised environments to enable data exfiltration.<sup>[3]</sup>

---

Source: <https://attack.mitre.org/groups/G0125/>