HAFNIUM

attack.mitre.org/groups/G0125/

HAFNIUM is a likely state-sponsored cyber espionage group operating out of China that has been active since at least January 2021. HAFNIUM primarily targets entities in the US across a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs.[1][2]

ID: G0125

ⓘ

Associated Groups: Operation Exchange Marauder

Contributors: Daniyal Naeem, BT Security; Matt Brenton, Zurich Insurance Group; Mayuresh Dani, Qualys; Harshal Tupsamudre, Qualys

Version: 1.1

Created: 03 March 2021

Last Modified: 16 April 2022

Version Permalink
Live Version

Associated Group Descriptions

Name	Description
Operation Exchange Marauder	[2]

Techniques Used

Domain	ID	Name	Use	
Enterprise	T1583	.003	Acquire Infrastructure: Virtual Private Server	HAFNIUM has operated from leased virtual private servers (VPS) in the United States.[1]
		.006	Acquire Infrastructure: Web Services	HAFNIUM has acquired web services for use in C2 and exfiltration.[1]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	HAFNIUM has used open-source C2 frameworks, including Covenant.[1]
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	HAFNIUM has used 7-Zip and WinRAR to compress stolen files for exfiltration.[1][2]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	HAFNIUM has used the Exchange Power Shell module `Set-OabVirtualDirectoryPowerShell` to export mailbox data.[1][2]
Enterprise	T1136	.002	Create Account: Domain Account	HAFNIUM has created and granted privileges to domain accounts.[2]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	HAFNIUM has used ASCII encoding for C2 traffic.[1]
Enterprise	T1114	.002	Email Collection: Remote Email Collection	HAFNIUM has used web shells to export mailbox data.[1][2]
Enterprise	T1567	.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	HAFNIUM has exfiltrated data to file sharing sites, including MEGA.[1]

Domain	ID	Name	Use	
Enterprise	T1190	Exploit Public-Facing Application	HAFNIUM has exploited CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065 to compromise on-premises versions of Microsoft Exchange Server, enabling access to email accounts and installation of additional malware.[1][2][3]	
Enterprise	T1592	.004	Gather Victim Host Information: Client Configurations	HAFNIUM has interacted with Office 365 tenants to gather details regarding target's environments.[1]
Enterprise	T1589	.002	Gather Victim Identity Information: Email Addresses	HAFNIUM has collected e-mail addresses for users they intended to target.[2]
Enterprise	T1590	Gather Victim Network Information	HAFNIUM gathered the fully qualified domain names (FQDNs) for targeted Exchange servers in the victim's environment.[2]	
		.005	IP Addresses	HAFNIUM has obtained IP addresses for publicly-accessible Exchange servers.[2]

Domain	ID	Name	Use
Enterprise	T1105	Ingress Tool Transfer	HAFNIUM has downloaded malware and tools--including Nishang and PowerCat--onto a compromised host.[1]
Enterprise	T1095	Non-Application Layer Protocol	HAFNIUM has used TCP for C2.[1]
Enterprise	T1003	.001	OS Credential Dumping: LSASS Memory	HAFNIUM has used `procdump` to dump the LSASS process memory.[1][2]
		.003	OS Credential Dumping: NTDS	HAFNIUM has stolen copies of the Active Directory database (NTDS.DIT).[2]
Enterprise	T1505	.003	Server Software Component: Web Shell	HAFNIUM has deployed multiple web shells on compromised servers including SIMPLESEESHARP, SPORTSBALL, China Chopper, and ASPXSpy.[1][2][3]
Enterprise	T1218	.011	System Binary Proxy Execution: Rundll32	HAFNIUM has used `rundll32` to load malicious DLLs.[2]
Enterprise	T1078	.003	Valid Accounts: Local Accounts	HAFNIUM has used the NT AUTHORITY\SYSTEM account to create files on Exchange servers.[3]

Software

ID	Name	References	Techniques
S0073	ASPXSpy	[2]	Server Software Component: Web Shell

ID	Name	References	Techniques
S0020	China Chopper	[2][3]	Application Layer Protocol: Web Protocols, Brute Force: Password Guessing, Command and Scripting Interpreter: Windows Command Shell, Data from Local System, File and Directory Discovery, Indicator Removal on Host: Timestomp, Ingress Tool Transfer, Network Service Discovery, Obfuscated Files or Information: Software Packing, Server Software Component: Web Shell
S0029	PsExec	[2]	Create Account: Domain Account, Create or Modify System Process: Windows Service, Lateral Tool Transfer, Remote Services: SMB/Windows Admin Shares, System Services: Service Execution

References

MSTIC. (2021, March 2). HAFNIUM targeting Exchange Servers with 0-day exploits. Retrieved March 3, 2021. Gruzweig, J. et al. (2021, March 2). Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities. Retrieved March 3, 2021. Bromiley, M. et al. (2021, March 4). Detection and Response to Exploitation of Microsoft Exchange Zero-Day Vulnerabilities. Retrieved March 9, 2021.