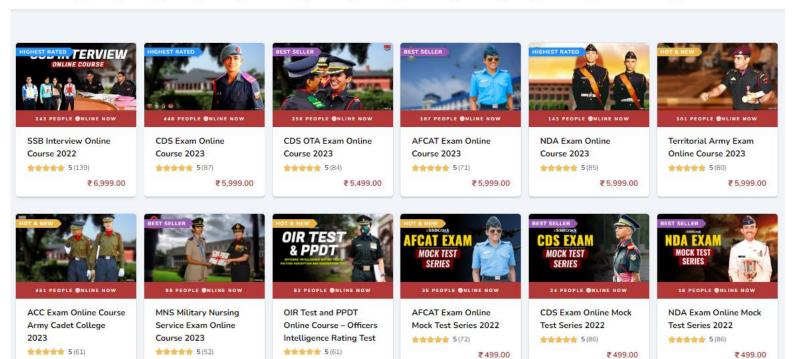


Courses

ACC AFCAT AIRMEN CAPF CDS EXAM INET OFFICER MNS MOCK TEST NDA EXAM PC(SL) SCO SSB INTERVIEW TERRITORIAL ARMY
(1) (1) (2) (1) (2) (1) (3) (1) (1) (1) (2) (1)





₹3,999.00

₹6,999.00

₹5,999.00

What Is Volt Typhoon? China-Backed Hackers Targeting "Critical Infrastructure" In USA

Why In The News?

- Microsoft Corp Said It Had Uncovered Malicious Activity By A State-sponsored Actor Based In China Aimed At Critical Infrastructure Organizations In Guam And The United States.
- Microsoft Said It Assessed With "Moderate Confidence" That This Volt Typhoon Campaign "Is Pursuing Development Of Capabilities That Could Disrupt Critical Communications Infrastructure Between The United States And Asia Region During Future Crises."



What Is Volt Typhoon?

- Its Name Is Redolent Of An Exotic Electrical Storm. But Currently, Denotes A
 Hacking Group "Volt Typhoon" Is Becoming An Imminent Danger To American
 Infrastructure.
- Volt Typhoon Has Been Active Since Mid-2021, Targeting Critical Infrastructure Organizations In Guam And Elsewhere In The United States.

How Does It Work?

- In This Campaign, The Affected Organizations Span The Communications,
 Manufacturing, Utility, Transportation, Construction, Maritime, Government,
 Information Technology, And Education Sectors.
- Observed Behavior Suggests That The Threat Actor Intends To Perform Espionage And Maintain Access Without Being Detected For As Long As Possible.
- To Achieve Their Objective, The Threat Actor Puts A Strong Emphasis On Stealth
 In This Campaign, Relying Almost Exclusively On Living-off-the-land Techniques
 And Hands-on-keyboard Activity.
- They Issue Commands Via The Command Line To:
 - o Collect Data, Including Credentials From Local And Network Systems,
 - Put The Data Into An Archive File To Stage It For Exfiltration, And Then
 - Use The Stolen Valid Credentials To Maintain Persistence.
- In Addition, Volt Typhoon Tries To Blend Into Normal Network Activity By Routing Traffic Through Compromised Small Office And Home Office (SOHO) Network Equipment, Including Routers, Firewalls, And VPN Hardware.
- They Have Also Been Observed Using Custom Versions Of Open-source Tools To Establish A Command And Control (C2) Channel Over Proxy To Stay Further Under The Radar.

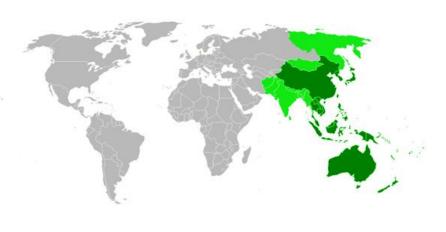




Current Situation:

• Guam Is Home To Major U.S. Military Facilities, Including The Andersen Air Force Base, Which Would Be Key To Responding To Any Conflict In The Asia-Pacific Region. Microsoft Said It Had Notified Targeted Or Compromised Customers And Provided Them With Information.



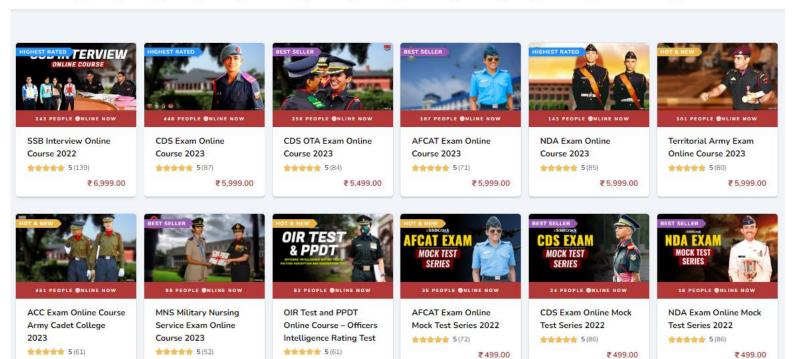


The Chinese Government Has Rejected Claims That Its Spies Are Penetrating
Western Infrastructure, Calling The Joint Warning Issued By The United States
And Its Allies A "Collective Disinformation Campaign."



Courses

ACC AFCAT AIRMEN CAPF CDS EXAM INET OFFICER MNS MOCK TEST NDA EXAM PC(SL) SCO SSB INTERVIEW TERRITORIAL ARMY
(1) (1) (2) (1) (2) (1) (3) (1) (1) (1) (2) (1)





₹3,999.00

₹6,999.00

₹5,999.00