



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Cyber Attack Campaign against UAE & Saudi Arabia**  
Tracking #:432315826  
Date:07-05-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a recent announcement by a threat actor group to intensify cyber-attacks against UAE & Saudi Arabia.

## TECHNICAL DETAILS:

Threat Intelligence was notified of a Telegram post where threat actor group “Sylhet Gang-SG” threatens to target UAE and Saudi Arabia. While the credibility and specific methods of the threat are unclear, it's crucial for entities to take proactive measures.

### Alert Reference:

#### SYLHET GANG-SG



We announced our suspension of attacks against UAE  
But there is no more we suspended that because they said they  
ended relationship with Israel  
but we saw when Iran Striked Israel  
They gave Zionists intelligence support. Which shows the ending of  
Relationship with Israel was just a trick to show themselves as  
innocent and supporter of gaza before the muslim world.  
We now officially announce that UAE And Saudi is again Legitimate  
Target and will be struck soon  
Muhammad Al Kuwaiti Prepare yourself for Long term Pressure  
I think this time you will have a heart stroke countering it because  
we saw how you panicked while countering attacks from Sudan

202  edited 22:38

**Threat Actor:** SYLHET GANG-SG

**Site:** [hxxps\[:\]//t\[.\]me/SylhetGangSgOfficial](https://t.me/SylhetGangSgOfficial)

## RECOMMENDATIONS:

- Remain vigilant and attentive to any unusual events or actions that may indicate malicious intent.
- Consider anti-DDoS solutions from ISPs or security vendors, if already subscribed then verify the anti-DDoS configuration.
- Notify immediately if any unusual or concerning findings are discovered.
- Implement strong authentication methods, such as multi-factor authentication (MFA), for all critical systems and applications.
- Ensure that all software, operating systems, and security applications are up to date with the latest patches and updates.
- Regularly back up the data and store it in a secure location
- Monitor network traffic for unusual or suspicious activities using intrusion detection systems (IDS) and intrusion prevention systems (IPS).

The UAE Cyber Security Council extends its appreciation for the continued collaboration.