Rewterz Threat Alert - 'NewsPenguin' Threat Actors Targeting Pakistani Entities With Malicious Campaign - Active IOCs - Rewterz

Published: 2023-02-09 · Archived: 2026-04-05 17:07:15 UTC

Severity

High

Analysis Summary

A new cyber threat group known as "NewsPenguin" has been linked to a phishing attack aimed at marine-related entities in Pakistan and using the PIMEC-23 maritime expo as a lure.

According to the researchers, NewsPenguin has launched a phishing campaign targeting Pakistani entities by leveraging the upcoming PIMEC-23, an international maritime expo organized by the Pakistan Navy.

> "The attacker sent out targeted phishing emails with a weaponized document attached that purports to be an exhibitor manual for PIMEC-23. The document utilizes a remote template injection technique and embedded malicious Visual Basic for Applications (VBA) macro code to deliver the next stage of the attack, which leads to the final payload execution."

PIMEC is a Pakistan Navy initiative organized under the auspices of the Ministry of Maritime Affairs. It gives the marine industry, both public and private, the opportunity to showcase products and create business relationships. The event would also highlight Pakistan's marine potential and offer a boost to national economic growth.

The method employed in the attack, known as remote template injection, is a technique that allows attackers to fetch the next-stage payload from a server controlled by the attacker. This technique is often used to avoid detection by the security software, as the payload is only delivered if the request is sent from a specific location, in this case, an IP address located in Pakistan.

The server was found to be hosting two ZIP archive files which contained a Windows executable (updates.exe) that functions as a covert spying tool capable of bypassing sandboxes and virtual machines. The backdoor was encrypted using the XOR encryption algorithm with the key "penguin", hinting at the name of the threat actor.

"The final payload is an advanced espionage tool that is XOR encrypted with a "**penguin**" encryption key. The content-disposition response header name parameter is set to "**getlatestnews**" during the HTTP response."

The domain hosting the payloads was registered since June 30, 2022, suggesting that the attack was planned in advance. The timeframe and planning for this campaign by the threat actor demonstrate that the attacker is constantly enhancing the tools they use to infiltrate target systems. It is rare for criminal organizations to plan ahead and create network infrastructure months before an event.

"As the target is an event run by the Pakistan Navy, it implies that the threat actor is actively targeting government organizations, rather than this being a financially motivated attack."

It is crucial for individuals and organizations to be vigilant when receiving emails with attachments, especially when they appear to be from unfamiliar or unexpected sources. Before opening any attachments, it is recommended to verify the identity of the sender and to scan the file with updated antivirus software. In addition, organizations should have strong security protocols in place to prevent and detect phishing attacks, including implementing multi-factor authentication, regularly training employees on security best practices, and having a incident response plan in place.

Impact

- Access To Sensitive Information
- Remote Template Injection

Indicators of Compromise

MD5

- fcae6b88640b58d289df42ae2d15e3ca
- 28e5fceaa9878bfbe967639cf2a2fb9b
- 314328e63b2e55a9c20bbda313ab4d04

SHA-256

- 80326b1e151e8348307114c8115e275c2fd63f0d2eb1dfacb6eca9840cf98525
- 26b113ba29b037034ee34a7f0fea81f6d5452950e0d26058d9b96946d78570c5
- 55f43319b910037d5b2eb8a5e57a14fca88e22bb0f40e453e510cc375a42bf43

SHA-1

- 80f4abc3ebe62229f964122dff078187be960874
- b9ad129f15e565201d860a04e0e26cce97a254e8
- 75b2a98f69d457ad22e77fb766f059e5d99634a5

Remediation

- Block all threat indicators at your respective controls.
- Search for Indicators of compromise (IOCs) in your environment utilizing your respective security controls
- It is important for individuals and organizations to be aware of these types of attacks and to have robust security measures in place to protect against them. This may include using up-to-date antivirus software, implementing multi-factor authentication, regularly backing up important data, and providing security awareness training for employees.
- Enable antivirus and anti-malware software and update signature definitions in a timely manner. Using multi-layered protection is necessary to secure vulnerable assets
- Patch and upgrade any platforms and software timely and make it into a standard security policy. Prioritize patching known exploited vulnerabilities and zero-days.
- Emails from unknown senders should always be treated with caution.
- Never trust or open " links and attachments received from unknown sources/senders.
- Implement multi-factor authentication systems that can help protect systems from malicious attacks
- Organizations should ensure that they have an incident response plan in place to be able to contain and investigate any security incidents quickly and efficiently.
