مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Threat Actors Levering LinkedIn for Web3 Malware Delivery

Tracking #:432316297

Date:17-09-2024

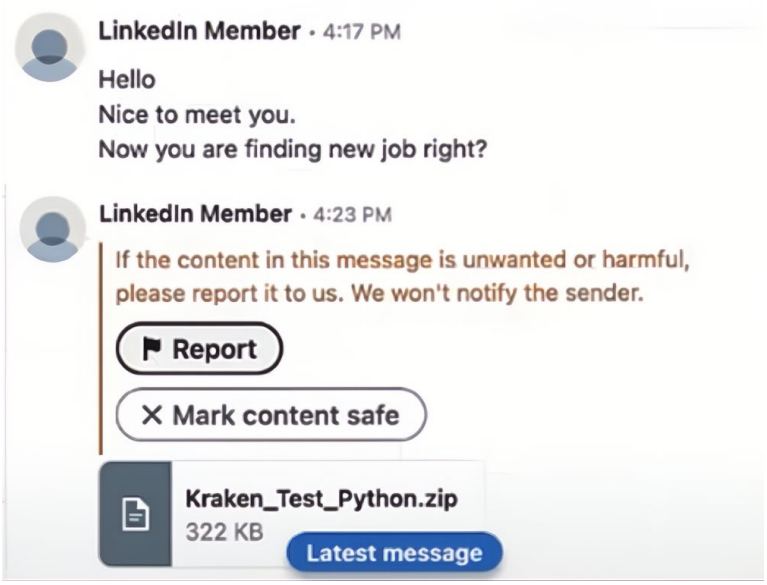
TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that recent intelligence indicates that threat actors are increasingly utilizing LinkedIn as a platform to target software developers through sophisticated social engineering tactics

TECHNICAL DETAILS:

Recent intelligence indicates that North Korean threat actors are increasingly utilizing LinkedIn as a platform to target software developers through sophisticated social engineering tactics. These attackers employ fake job recruitment schemes, embedding malware within seemingly benign coding challenges. The malware, identified as COVERTCATCH, is designed to compromise macOS systems and facilitate further malicious activities, particularly within the Web3 sector.



Fake job opportunity

Threat actors have been observed initiating contact with potential victims through LinkedIn, posing as recruiters. After establishing a conversation, they send a ZIP file containing COVERTCATCH malware disguised as a Python coding challenge. Once executed, this malware downloads a second-stage payload that compromises the target's macOS system by establishing persistence through Launch Agents and Daemons.

This tactic aligns with previous operations such as "Operation Dream Job" and "Contagious Interview," which similarly exploit job-related decoys to deploy malware. In addition to COVERTCATCH, other malware families like RustBucket have been employed in related campaigns. RustBucket is capable of gathering system information and maintaining persistence by masquerading as legitimate software updates.

The ongoing targeting of Web3 organizations highlights the need for heightened vigilance in the cryptocurrency sector. Attackers not only aim to infect systems but also pivot towards stealing credentials, conducting reconnaissance on internal systems, and accessing cloud environments to drain cryptocurrency wallet

IOCs:

- SHA 256: 2b8c579ecd1e4357e339012791aab058c58907f92ac292e1dca9eaccc8f0d054

RECOMMENDATIONS:

- Conduct regular training sessions on recognizing phishing attempts and suspicious job offers.
- Implement simulated phishing exercises to reinforce awareness.
- Utilize endpoint protection solutions that can detect and block malicious files before execution.
- Enforce strict policies regarding the downloading and execution of files from unknown sources.
- Implement least privilege access controls to minimize the impact of potential breaches.
- Regularly audit access permissions for sensitive systems and data.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

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

REFERENCES:

- https://cloud.google.com/blog/topics/threat-intelligence/examining-web3-heists/