JO-FinCERT – Security Advisory – 2023 – 42

1. Impersonation of the National Cybersecurity Center President

The National Cybersecurity Center (NCSC) has issued a warning concerning an incident involving phishing emails. These fraudulent emails are specifically targeting participants enrolled in the 'Cyber Warriors' competition. The deceptive messages are cleverly designed to appear as if they are originating from the president of the National Cybersecurity Center. It is essential to practice extra caution to protect yourself and your organization from phishing emails, which may include:

1. Verify sender address by paying attention to misspelling or suspicious domains.
2. Examine email content by paying attention to bad grammar and unprofessional formatting.
3. Be aware of urgent requests.
4. Hover over links instead of clicking directly to reveal the real the true destination of the link. Verify URLs by coping it to reputation websites.
5. Don't provide any sensitive information via email. Typically, organizations do not ask for sensitive information via email.

Please refer to **Jo-FinCERT cybersecurity framework for Jordan Financial Sector** for Email security controls **-** G.4.7 Email Security: https://www.cbj.gov.jo/Pages/viewpage.aspx?pageID=1498

Reference: Https://www.facebook.com/NCSCJO

2. Microsoft Detected a Multi-stage AiTM Phishing and BEC Campaign

Microsoft Defender Experts have recently discovered a sophisticated attack targeting banking and financial services institutions. These attacks involve multiple stages, combining adversary-in-the-middle (AiTM) phishing and business email compromise (BEC) techniques. It all started with the compromise of a trusted vendor, leading to a sequence of AiTM attacks and subsequent BEC activities across several organizations. This incident draw attention to the complicated nature of AiTM and BEC threats, as they exploit the trust placed in vendors, suppliers, and partner organizations to perpetrate financial fraud.

Reference: https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/

3. New SPECTRALVIPER Backdoor

A newly discovered backdoor called SPECTRALVIPER has been identified by security researchers. This backdoor is highly obfuscated and previously unknown. It operates on the x64 architecture and possesses several powerful capabilities, including PE (Portable Executable) loading and injection, file upload and download functionality, manipulation of files and directories, and the ability to impersonate tokens.

The attacks associated with this backdoor have been attributed to a threat actor that security experts are tracking under the name REF2754. This actor has overlaps with a Vietnamese cyber threat group that goes by various names, including APT32, Canvas Cyclone (previously known as Bismuth), Cobalt Kitty, and OceanLotus. These findings suggest a potential connection or involvement of this threat group in the deployment of SPECTRALVIPER and related attacks.

Reference: https://thehackernews.com/2023/06/new-spectralviper-backdoor-targeting.html