مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

NEW BUGSLEEP BACKDOOR IN MUDDYWATER CAMPAIGNS

Tracking #:432316056
Date:16-07-2024

TLP: WHITE

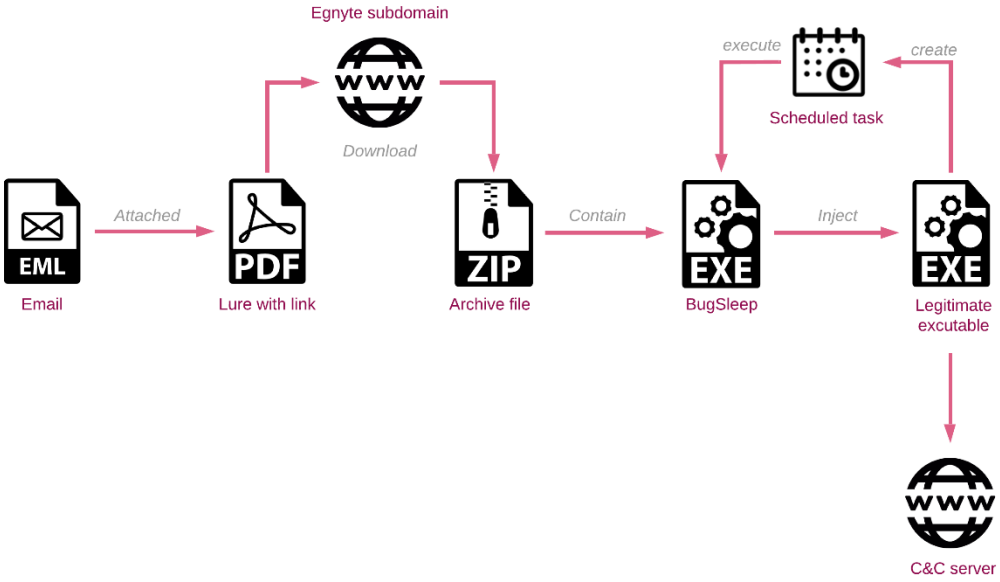
EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that the new BugSleep backdoor is being used by Muddy Water for its campaigns.

TECHNICAL DETAILS:

MuddyWater campaigns usually consist of sending large numbers of emails to a wide range of targets from a compromised email account. Although their lures are aimed at a large and varied set of organizations or individuals, they often focus on specific industries or sectors, highlighting the group's points of interest.

BugSleep is a backdoor designed to execute the threat actors' commands and transfer files between the compromised machine and the C&C server. The typical infection chain that delivers the BugSleep backdoor is as follows:



Egnyte is a secure file-sharing platform that allows employees and companies to easily share files via a web browser. Recently, MuddyWater has frequently used Egnyte subdomains, aligning them with the company names used in their phishing emails. Upon opening the shared link, recipients can see the name of the purported sender, which often appears legitimate, and matches the naming conventions of the targeted country.

Propagation and Delivery:

- MuddyWater primarily uses phishing campaigns sent from compromised email accounts.
- These emails target a wide range of organizations and individuals, with a focus on specific industries or sectors.
- The backdoor is delivered through malicious attachments or links in these phishing emails.

Functionality:

- **Command Execution:** BugSleep is designed to execute commands issued by the threat actors. It acts as a bridge between the compromised machine and the command-and-control (C&C) server.
- **File Transfer:** The backdoor facilitates file transfers between the compromised system and the C&C server.

Evading Detection:

- **Customization:** BugSleep is tailor-made, allowing the threat actors to adapt it to their specific needs.
- **Continuous Development:** The threat actors continuously improve BugSleep's functionality and address bugs. This dynamic development helps evade detection.

INDICATORS OF COMPROMISE:

RECOMMENDATIONS:

- **User Education and Awareness:** Educate users about phishing techniques and social engineering tactics. Regularly conduct security awareness training to help them recognize suspicious emails and attachments.
- **Email Filtering and Gateway Security:** Deploy robust email filtering solutions that can detect and block phishing emails.
- **Endpoint Protection:** Install and maintain up-to-date antivirus and anti-malware software on all endpoints.
- **Network Segmentation:** Segment your network to limit lateral movement. Isolate critical systems from less secure areas.
- **Patch Management:** Regularly apply security patches to operating systems, applications, and third-party software.
- **Least Privilege Principle:** Limit user privileges to the minimum necessary for their roles. Avoid granting administrative rights unless essential.
- **Network Monitoring and Threat Intelligence:** Continuously monitor network traffic for signs of communication with known malicious domains or IP addresses.

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://research.checkpoint.com/2024/new-bugsleep-backdoor-deployed-in-recent-muddywater-campaigns/