مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Spear-Phishing Campaign by Midnight Blizzard

Tracking #:432316456

Date:30-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed an ongoing spear-phishing campaign by Midnight Blizzard, targeting government, academia, defense, non-governmental organizations, and other sectors.

TECHNICAL DETAILS:

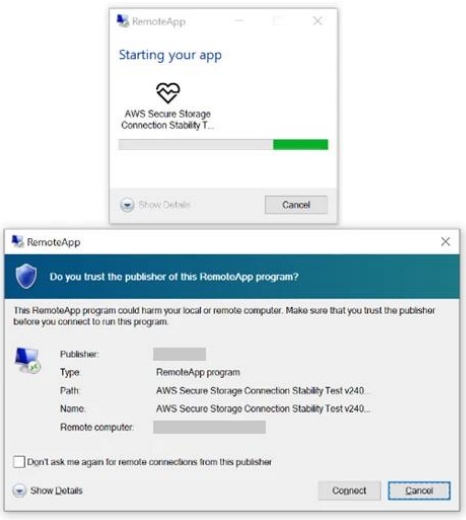
Microsoft has reported an ongoing spear-phishing campaign orchestrated by the threat actor Midnight Blizzard(also known as APT29, UNC2452, and Cozy Bear), targeting government, academia, defense, non-governmental organizations, and other sectors.This campaign exploits three critical remote code execution (RCE) vulnerabilities using malicious Remote Desktop Protocol (RDP) configuration files. The campaign aims to collect intelligence by compromising systems and deploying various forms of malware, including ransomware.

Attack Vector:

- **Spear-Phishing Emails**: Thousands of targeted emails were sent to over 100 organizations. These emails featured social engineering lures related to Microsoft Microsoft, Amazon Web Services (AWS), and the concept of Zero Trust with a signed RDP configuration file.
- **RDP Configuration File**: The malicious .RDP file, signed with a LetsEncrypt certificate, enabled bidirectional mapping of resources between the target's system and an actor-controlled server. This included sensitive information like files, Point of Service (also known as Point of Sale or POS) devices,clipboard data, and authentication features.

Key Characteristics of the Attack:

- **Malicious RDP Connection**: Upon opening the .RDP file, the target's device connects to the attacker's server, exposing sensitive resources and potentially allowing for malware installation.
- **Use of Legitimate Domains**: Emails were sent using addresses from previously compromised legitimate organizations, increasing the credibility of the phishing attempt.



Malicious remote connection

INDICATORS OF COMPROMISE(IOCs):

Attached in Excel File

RECOMMENDATIONS:

- **Strengthen Firewall Configurations**: Use Windows Firewall or equivalent to restrict outbound RDP connections to external networks.
- **Implement Multi-Factor Authentication (MFA)**:Enforce MFA across all accounts, especially for access to critical applications.
- **Use Phishing-Resistant Authentication**: Leverage authentication methods such as FIDO tokens and Microsoft Authenticator with number matching. Avoid telephony-based MFA to mitigate SIM-jacking risks.
- **Conditional Access Policies**: Require phishing-resistant authentication methods for employees and external users accessing critical applications.
- **Browser Security**: Encourage users to use Microsoft Edge or other browsers with Microsoft Defender SmartScreen to identify and block phishing and malware sites.
- **User Education:** Train users to recognize spear-phishing attempts and the dangers of opening unexpected email attachments.
- **Email Filtering:** Implement advanced email filtering solutions to detect and block phishing attempts.
- **Incident Response:** Establish a robust incident response plan to quickly address suspected phishing incidents.

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://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/