NCA-08.051324 – NCERT Advisory: Sidewinder APT Campaign Targeting Government Organizations

Introduction

Recent investigations have revealed a sophisticated cyber campaign targeting high offices and government organizations in Pakistan. The threat actors, believed to be associated with the Sidewinder APT group, have been employing advanced tactics to infiltrate systems and compromise sensitive information. One of the primary methods employed in this campaign is the distribution of phishing PDF documents themed around the highest executive offices and ministries of Pakistan.

Campaign Details

The campaign utilizes various tactics and techniques, including but not limited to:

- **Initial Access (TA0001):** Spear phishing link tactics (T1566.002) via clickable URLs in the phishing PDF document.
- **Execution (TA0002):** Exploitation techniques for client execution (T1203) through compromised client applications.
- **Defense Evasion (TA0005):** Masquerading (T1036), hiding artifacts (T1564), and creating files inside user directories to conceal malicious activity.
- **Credential Access (TA0006):** OS credential dumping (T1003) and stealing web session cookies (T1539) for unauthorized access.
- **Discovery (TA0007):** Gathering system and software information through registry queries (T1012) and system information discovery (T1082).
- **Collection (TA0009):** Acquisition of sensitive data by searching for files of interest on local systems (T1005).
- **Command and Control (TA0011):** Utilizing application layer protocols (T1071) and encrypted channels (T1573) for communication.
- **Impact (TA0034 & TA0040):** Disruption of system availability and network resources through data destruction (T1485).

Indicators of Compromise (IOCs)

To aid in detection and mitigation efforts, the following indicators of compromise (IOCs) have been identified:

1. **File Hashes:**
    - MD5: d4eb4cee8aeb6f2ea36afadeda9dbb23
    - MD5: 38f96b882363cb659d4cabec49bf605c
    - SHA-1: f3d38a0cc1f4e0a8ac734fdf035ebff93158aa05
    - SHA-256: 23f3a046884bf94ec706f98000a9efbda48455b4dd86f0665409937b1fb811cb
2. **Vhash & SSDEEP:**
    - Vhash: 9b6dc8d90ed2c55b367655413f716376a
    - SSDEEP 3072: lAn81BGocEm5bBzRgUO0Sh+sPLbs617VP6Fmd:lAn81B5cB3Olh+osc7oFw
3. **TLSH:**
    - T1DFD3E030F59C8CCDECDAD81EC97A38088AFCB25347DD74DBA01ECA52B1506A98B165D2
4. **Domains:**
    - info.goverment-pk-update.top
    - docs.mofa-services-server.top

[**Note:** The shared links can be of malicious nature and may lead to security issues, thereby they are not clickable, however for the utilization of security professionals, these links can be copied as potential threat intelligence info]

Recommendations and Action Items

To mitigate the risks posed by this cyber campaign, government organizations and high offices are advised to take the following actions:

1. **Email Security Enhancements:** Deploy advanced email filtering solutions capable of detecting and quarantining suspicious attachments and URLs. Utilize email authentication mechanisms such as SPF, DKIM, and DMARC to verify the authenticity of incoming emails and prevent domain spoofing.

2. **Secure Document Handling:** Implement document security policies that restrict the execution of macros and scripts within office documents, thereby mitigating the risk of malware embedded within attachments. Utilize sandboxing and static analysis tools to analyze suspicious documents in a controlled environment, identifying and mitigating potential malware threats before they reach end-users. Utilize PDF security features such as digital signatures and document encryption

to prevent unauthorized tampering and modification of PDF content, ensuring the integrity and authenticity of official documents.

3. **Endpoint Protection:** Deploy endpoint detection and response (EDR) solutions capable of detecting and blocking malicious activities at the endpoint level, including file-less malware execution and credential theft attempts. Implement application control measures to restrict the execution of untrusted binaries and scripts on endpoints, reducing the attack surface for adversaries.

4. **Threat Intelligence Integration:** Integrate threat intelligence feeds into security monitoring systems to proactively identify indicators of compromise associated with known APT groups and emerging cyber threats. Leverage threat intelligence platforms to correlate IOCs with historical attack data and identify patterns indicative of ongoing or impending cyber campaigns.

Government organizations, ministries and divisions are urged to remain vigilant and implement necessary security measures to protect against cyber threats. Collaboration and proactive measures are essential to safeguard sensitive information and maintain the integrity of government systems.