Annexure

NCA-30.070326 – National CERT Advisory – APT Sidewinder - Phishing Attack on Government Organizations

1. Introduction

A sophisticated phishing campaign has been launched by the Indian-origin Advanced Persistent Threat (APT) group known as "SideWinder" (also tracked as Rattlesnake, Hardcore Nationalist (HN2), and T-APT-04). Active since 2012, this group is historically engaged in cyber espionage against government and military institutions in South Asia. The current campaign aggressively targets employees of Pakistani public sector organizations through the use of impersonated domains and malicious files. The Threat Actor (TA) has registered several fake domains to lure victims, necessitating the immediate blocking and flagging of the identified Indicators of Compromise (IoCs) on all organizational Email servers, Firewalls, Endpoint security solutions, and Security Information and Event Management (SIEM) systems.

2. Threat Indicators (IoCs)

The following malicious domains and files have been identified as part of this campaign and require immediate action:

Ser	Malicious Domains / URLs	Impersonated Organizations	Malicious File / Link
a.	cabinet-gov-pk[.]fetchdrive[.]org	Cabinet Div	-
b.	buildtheations[.]info/Build_Nation	Ministry of Defence (MOD)	https://hitpak[.]org
c.	(1) finance-gov-tpk[.]fetchdrive[.]org/ (2) finance-gov-tpk[.]grabfiles[.]net/	Ministry of Finance	-
d.	nepra-org-pk[.]grabfiles[.]net/	NEPRA	-
e.	Commerce-gov-pk[.]fetchdrive[.]org	Ministry of Commerce	-
f.	buildtheations[.]info/PKCERT/pkcert.html	National CERT	https://hitpak[.]org

3. Action Requested

All recipient organizations are requested to treat this as an urgent alert.

a. **Directorate General ISI Only:** The domains listed above are requested to be flagged at the highest priority.
b. **All Setups:** The domains and URLs in the table above must be immediately blocked on email servers, Firewalls, Endpoint Detection and Response (EDR) tools, and SIEM solutions to prevent any interaction from users within the network.

4. Deploy Detection Rules

Endpoint Detection & Response (EDR)

a. Detect Microsoft Office applications spawning command interpreters or PowerShell processes
b. Monitor abnormal child processes initiated by email attachments
c. Alert on credential dumping or suspicious privilege escalation behavior

5. Execute Immediate Technical Mitigation Actions (24-Hour Response)

1. Block all identified malicious domains, URLs, and IP addresses at gateway and DNS levels
2. Reset credentials for users interacting with suspected phishing infrastructure
3. Review previous 14 days of email gateway, proxy, and EDR telemetry logs
4. Enforce Multi-Factor Authentication (MFA) across email, VPN, and privileged systems
5. Validate and enforce SPF, DKIM, and DMARC configurations
6. Disable or isolate compromised user accounts immediately
7. Verify integrity of backups and ensure offline backup availability

6. Modus Operandi - Phishing Attacks

a. In this particular campaign TA attempts to steal victim's credentials email for launching of further phishing attacks.
b. Cyber Threat Actor (TA) sends deceptive emails or links/files/media that appear to originate from trusted sources (Govt offices, banks, online services etc).
c. Emails/ links contain official messages/ orders or some appealing content such as security alert instructions, account suspension warnings or password reset requests, urging the receiver for immediate action.

7. Potential Consequences.

Following are possible consequences if attack remained successful:

a. Credentials Compromise.

b. System compromise for expanding malicious ingress.

c. Installation of malware.

8. Suggested Measures - Users & Administrators

a. Communication Vigilance:

1. All users and administrators are advised to remain vigilant regarding phishing emails. Moreover, all organizations' administrators are advised to change all user passwords for their mail server.

2. Verify identities through independent channels if any email or msg claims affiliation with relevant organizations.

b. Device Security: Update Email, other social media applications and device operating system regularly to **patch vulnerabilities**.

c. Digital Hygiene:

(1) Do not click on **unknown links & URLs** received through emails, social & communication media.

(2) Strong password policy & multifactor authentication be implemented for all users.

(3) Email spam filter on mail server settings be set to max security level.

(4) AV & URL/ Link scanners be integrated with email server for scanning of email attachments before receipt by users.

(5) Personal mobile phones must not be connected to official PCs/ Laptops.

d. **Use Reputable Security Software:** Keep your AV and anti-malware software up-to-date and actively scan your system for threats.