NCA-16.091324 – National CERT Advisory: Phishing Email Attack Targeting Government Organizations

Introduction

A recent investigation has revealed a sophisticated phishing email campaign targeting the email systems of several government organizations. The phishing emails were crafted to deceive users into compromising their credentials by clicking on malicious links or opening attachments. These emails were traced to multiple public IP addresses and were designed to hide the identity of the attackers by using cloud-based services. Forensic analysis has identified the nature of the attack, the tactics employed, and potential risks. This advisory details the technical findings, indicators of compromise (IOCs), and recommended security measures to mitigate the threats.

Campaign Details

The phishing attacks leveraged compromised public IP addresses and cloud-based infrastructure to target government employees. The attackers used fraudulent email addresses and social engineering tactics to lure recipients into interacting with malicious attachments and links. Notable findings include:

1. **Phishing Email Crafting**:

   The phishing emails were sent from a compromised email address and utilized multiple public IP addresses to obscure the origin of the attack. The emails contained PDF attachments and links that directed recipients to phishing websites, designed to collect login credentials.

2. **Phishing Domain**:

   The domain used to host the phishing website was registered and hidden using Cloudflare services. This method of hosting makes it difficult to trace the real identity and origin of the attackers. The phishing links were intended to steal usernames and passwords from government employees for unauthorized access.

3. **Malware Analysis**:

   Although the attached PDF document did not contain embedded files, executable codes, or malicious scripts, it was designed to deceive recipients into clicking on phishing links embedded within the document. This form of attack relies on social engineering and user trust rather than technical malware to compromise systems.

Indicators of Compromise (IOCs)

1. **Source IP Addresses of Phishing Emails**:

   - 113.203.221.25
   - 154.81.250.19

- 154.81.249.48
- 154.91.150.129

2. **File Hashes**:
    - **SHA256**: ef891d3f0ddddc3ac23d888cf8db723c17f8e43c20a643e2d58a14831d99d128
    - **MD5**: 1d854debbeae39c444ab4517a1f3de3

Recommendations and Action Items

In light of the findings, all government organizations, ministries, divisions, and attached departments are urged to take the following actions to protect against phishing attacks and enhance their cybersecurity defenses:

1. **Email Security Enhancements**:
    a. Implement advanced email filtering and anti-phishing solutions capable of detecting suspicious links, malicious attachments, and domain spoofing attempts. These solutions should be integrated with threat intelligence feeds to automatically block known phishing domains and IP addresses.

    b. Deploy and enforce email authentication protocols such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting & Conformance) to prevent attackers from sending phishing emails that appear to come from trusted government domains.

2. **Strengthening Access Controls**:
    a. Mandate the use of multi-factor authentication (MFA) for all email systems and sensitive applications to provide an additional layer of security against compromised credentials. This will ensure that even if login information is stolen, unauthorized access is prevented.

    b. Conduct a full reset of usernames and passwords for all employees who have interacted with the phishing email to eliminate potential access risks.

3. **Awareness and Education**:
    a. Provide regular phishing awareness training to all employees, educating them about identifying and reporting suspicious emails. This should include simulated phishing exercises to assess readiness and reinforce secure behavior.

b. Instruct all employees to avoid opening emails from unknown sources or clicking on links and attachments unless they are verified through a secure process.

4. **Endpoint Detection and Protection**:

    a. Deploy Endpoint Detection and Response (EDR) solutions across all government systems to monitor for unusual behavior and quickly detect and block malicious activity at the endpoint level. EDR systems can also assist in identifying phishing-related malware, should it be introduced to the environment.

    b. Ensure that all systems are regularly updated with the latest security patches, and restrict the execution of unauthorized applications and scripts through application whitelisting.

5. **Secure Document Handling**:

    a. Implement document security policies that restrict the execution of macros or scripts within office documents and PDFs, thereby reducing the risk of inadvertently triggering malware.

    b. Use sandboxing tools to automatically open and analyze suspicious attachments in a secure, isolated environment before they are allowed to reach end-users.

    c. Implement digital signatures and encryption in all official document handling to ensure authenticity and prevent tampering.

6. **Network and Domain Security**:

    a. Immediately block the identified IP addresses and phishing domains at the national internet gateway level and within the organization's firewalls and intrusion prevention systems.
    b. Continuously monitor incoming and outgoing network traffic for any signs of communication with the identified phishing domains or IP addresses, and apply security measures to prevent further exploitation.

7. **Incident Response and Coordination**:

    a. All organizations are encouraged to implement robust incident response plans to quickly identify and contain phishing attacks. This includes notifying relevant authorities, such as government CERTs, sectoral CERTs, National CERT and collaborating on sharing IOCs and threat intelligence.

b. Maintain logs and audit trails for email and network systems to facilitate investigation and help trace the origin of attacks.

8. **Threat Intelligence Sharing**:

   a. Share any newly identified indicators of compromise (IOCs) with National CERT. Proactive sharing of threat intelligence helps the broader community defend against emerging threats.

   b. Leverage threat intelligence platforms to continuously update your security tools with real-time data on known phishing campaigns and threat actors.

Conclusion

All government organizations, ministries, divisions, and attached departments must remain vigilant and adopt the recommended security practices. Phishing campaigns continue to evolve, and strong technical, procedural, and user-level defenses are critical to maintaining the integrity of government communication systems.