NCA-20.050625 – National CERT Advisory – Malicious Campaigns Leveraging Compressed Files and Social Engineering Techniques

Introduction

A new wave of phishing and spoofing attacks is actively targeting organizations through fraudulent emails impersonating trusted authorities and official platforms exploiting user trust in official-looking digital communications. Attackers are using compressed file formats (.rar, .zip) to deliver malware and gain unauthorized access to organizational systems through social engineering and impersonation of trusted authorities or platforms.

These threat actors craft emails that closely mimic legitimate institutional correspondence, often incorporating organizational branding, government insignia, and standard document formats. Malicious payloads are concealed within multi-level compressed files and delivered via convincingly spoofed messages, aiming to deceive recipients into executing harmful content without suspicion.

The campaign demonstrates advanced evasion techniques and has targeted multiple sectors. The tactics align with Advanced Persistent Threat (APT) methods, including lateral movement, privilege escalation, and prolonged surveillance. In some cases, attackers have disseminated malicious attachments through legitimate accounts on official online platforms, further increasing the likelihood of user engagement.

Scope and Impact

These campaigns can cause disruption of operations, leak sensitive information leading to the compromise of the integrity of internal networks and public facing platforms.

- **Credential Harvesting**: Users who open malicious contents can inadvertently expose their login credentials, enable attackers to get an unauthorized access to internal platform, impersonate employees, elevate user privileges.
- **Systemic Network Infiltration**: After gaining access to a system, attackers can use secondary payloads to maneuver internal infrastructure, potentially infecting multiple endpoints and shared resources.
- **Data Exfiltration**: These malware types typically contain mechanisms to steal sensitive information quietly—such as documents, session tokens, and metadata—and send them to attacker-controlled servers beyond the organization's perimeter.
- **Command Execution and Remote Access**: After compromise, systems can beacon out to Command-and-Control, C2, infrastructure, allowing attackers to run remote commands, download additional exploits, or preserve uninterrupted access.

- **Reputational and Operational Fallout**: Internal communication or data exposures by such attacks may lead to public distrust, regulatory fines, and reputational damage over time.

Tactics, Techniques, and Procedures (TTPs)

- **Compressed File Usage for Obfuscation**: Malicious payloads are frequently inserted, sometimes in layers, in.rar,.zip, or.7z files. File names like "Budget_Document_2025.rar" and "InternalMemo.zip" frequently resemble those of real document types.
- **Spoofed Senders and Domain Impersonation**: Domains that outwardly mimic legitimate email addresses are often the source of attacks. Subtle character changes or unofficial TLDs (such as.com.pk,.org.pk,.govportal.net, govpk.email, etc.) are examples of variations.
- **Social Engineering Hooks**: Email content can include important corporate memoranda, policy deadlines, invoice payments, or IT system improvements. The layout and tone are designed to resemble authentic internal messages.
- **Beaconing and C2 Infrastructure**: During file execution, embedded malware may create silent outward connections to attacker-controlled infrastructure using HTTP/S, DNS tunneling, or other special protocols. Attackers use these channels to transmit secondary payloads, exfiltrate data, and exert control.
- **Persistence Mechanisms**: Some malware strains use scheduled processes or modify system registry settings to grant ongoing access following a system reboot.

Recommendations and Best Practices

1. For General Users, Administrative Staff, and Department Heads

a. **Exercise Extreme Caution**: Do not open compressed attachments unless you have explicitly verified their origin via a trusted secondary channel (e.g. phone confirmation with sender). Scan all compressed attachments using a well-reputed AntiVirus solution before opening them.

b. **Confirm Email Validity**: Check sender addresses attentively, even where the display name is accurate. Be cautious about:

    - Spelling discrepancies.
    - Unofficial domain suffixes (e.g., .email, .govportal.com)
    - Generic greetings in lieu of custom communication

c. **Avoid Clicking Unknown Links**: Do not click embedded links in emails asking for credentials or requiring immediate action.

d. **Secure Authentication Practices**:

- Utilize strong, one-of-a-kind passwords
- Employ multi-factor authentication (MFA) where supported
- Never share login credentials with support staff or colleagues

e. **Environment Hygiene**:
- Make sure real-time protection is active in antivirus/EDR solutions
- Have systems and applications kept up to date with the most recent security patches

2. For IT Administrators, SOC Teams, and Network Security Engineers

a. **Domain Blocking**: Blacklist immediately all known malicious domains, such as those posing as government platforms (e.g. gov-pakistan.com, govpk.email, e-office.org.pk).

b. **Compressed File Inspection:**
- Set up email gateways to inspect within compressed archives.
- Utilize sandboxing environments to scan attachments prior to delivery to users.

c. **Endpoint Monitoring and Response:**
- Deep scan user endpoints, especially those that have processed .rar or.zip attachments.
- Monitor unusual file execution, privilege escalation attempts, and unknown process activity.

d. **Network Anomaly Detection:**
- Configure notifications for suspicious outbound connections, particularly to non-standard ports or unknown geographic regions.
- Look for beaconing behavior indicative of C2 communication.

e. **IOC Integration and Threat Intelligence Sharing:**
- Input newly identified IOCs (hashes, URLs, IPs, behavioral patterns) into internal SIEM or XDR systems
- Share any found indicators with National CERT and peer organizations

f. **User Awareness Campaigns:**
- Conduct regular training and simulated phishing exercises
- Offer clear reporting channels for users to report suspicious emails or attachments.

Call to Action

National CERT calls on all organizations—particularly those dealing with sensitive information or government duties—to:

1. Treat all compressed email attachments suspicious until confirmed from the originated department. Counter check from the department even the email is disseminated through legit accounts of an official online platform.
2. Conduct an examination and boost current email security measures, such as attachment scanning and domain validation mechanisms.
3. Conduct a recent email traffic and endpoint activity audit for indications of compromise, specifically compressed file runs and unusual outbound traffic.
4. Report every suspected phishing attack or malicious attachments to [cert@pkcert.gov.pk].
5. Ensure cross-functional coordination among IT, cybersecurity, and end-user departments to bridge communication gaps and enhance overall cyber resilience.