No. DG-II/CERT/4/124/2023/P-1
GOVERNMENT OF SINDH
SCIENCE & INFORMATION TECHNOLOGY DEPARTMENT
Karachi, dated the 14th July 2026

To,

1. The Chairman, Enquires, Anti-Corruption, Establishment Sindh, Karachi.
2. The Chairman, Planning & Development Board Sindh, Karachi
3. The Chairman/Chairperson, CMIT Sindh, Karachi
4. The Chairman Sindh HEC Karachi.
5. The Senior Member Board of Revenue (BOR) Sindh, Karachi
6. The Additional Chief Secretary, Govt of Sindh
7. The Principal Secretary to Governor Sindh, Governor Secretariat, Karachi.
8. The Principal Secretary to Chief Minister Sindh, CM Secretariat, Karachi
9. The Administrative Secretary, GoS (All)
10. The Provincial Ombudsman, Sindh.
11. The Inspector General of Police Sindh, Karachi
12. The Divisional Commissioner (All) in Sindh
13. The Chief Executive Officer Sindh IT Company (SITC), Karachi.

SUBJECT: **CYBERSECURITY ADVISORY ON LARGE-SCALE PHISHING CAMPAIGNS DISTRIBUTING LUMMA STEALER, KEYLOGGERS, AND RANSOMWARE**

With reference to the letter received from National Cyber Emergency Response Team (NCERT) (**copy enclosed**), Government of Pakistan, regarding a large-scale phishing campaign targeting government entities, public sector organizations, and critical digital services has recently been identified. The campaign is reportedly distributing credential stealers, information-stealing malware, keyloggers, and ransomware through malicious PDF documents, fake CAPTCHA pages, and phishing websites. In this regard, the attached Advisory titled "NCA-35.150626 - National CERT Advisory - Large-Scale Phishing Campaign Distributing Lumma Stealer, Keyloggers, and Ransomware Through Malicious PDFs and Fake CAPTCHA Pages" (**Annexure**) has been issued by the National Cyber Emergency Response Team (National CERT)

2. In this regard, it has been requested that the **attached Advisory** may kindly be disseminated to all concerned departments, organizations, and personnel under the administrative control to facilitate awareness and ensure timely implementation of the recommended preventive, detection, and mitigation measures.

(AYAZ AHMED UQAILI)
Member (IT Industry) S&ITD
0345-8219899

Annexure: NCA-36-150626 - National CERT Advisory - Large-Scale Phishing Campaign Distributing Lumma Stealer, Keyloggers, and Ransomware Through Malicious PDFs and Fake CAPTCHA Pages

A copy is forwarded for information and necessary action to: -
1. Director General (nCERT). L Block, Pak Secretariat, Islamabad
2. Staff Officer to SACM for S&IT Department, Govt. of Sindh, Karachi.
3. Staff Officer to Secretary S&IT Department, Govt. of Sindh, Karachi.

Annexure

NCA-35.150626 – National CERT Advisory

Large-Scale Phishing Campaign Distributing Lumma Stealer, Keyloggers, and Ransomware Through Malicious PDFs and Fake CAPTCHA Pages

A sophisticated and ongoing phishing campaign has been identified targeting government entities, public sector organizations, and critical digital services through malicious PDF lures and fake CAPTCHA pages. The campaign uses deceptive CAPTCHA images embedded in PDF files to redirect users to phishing websites and malware delivery infrastructure, with the primary objectives of credential theft, unauthorized access, browser session hijacking, deployment of information stealers and keyloggers, and potential follow-on ransomware infections.

The campaign specifically targets government websites, administrative portals, official email accounts, browser sessions, and other sensitive digital assets. Threat actors use social engineering, search engine optimization (SEO) poisoning, fake CAPTCHA verification lures, and PowerShell/MSHTA abuse to facilitate credential theft and the delivery of malware such as Lumma Stealer and associated payloads.

This advisory outlines the threat landscape, indicators of exposure and compromise, potential operational impact, and recommended defensive measures to help organizations strengthen protection against phishing-enabled malware delivery and credential theft.

1. DOCUMENT SUMMARY

Field	Details
Advisory ID	NCA-35.150626
Threat Type	Phishing / Credential Theft / Information Stealer / Keylogger / Malware Delivery
Severity	Critical
Attack Vector	Malicious PDF lures, fake CAPTCHA pages, phishing websites, SEO poisoning, and malicious script execution via PowerShell/MSHTA.
Authentication Required	No
User Interaction	Opening malicious PDF files, clicking deceptive CAPTCHA images, visiting phishing websites, and in some cases executing attacker-delivered commands or scripts.
CVSS Score	9.1 (Critical – Credential Theft and System Compromise)

2. IMPACT ANALYSIS

Successful exploitation may result in:

a. **Credential Theft** – Government email, portal, and application credentials compromised
b. **Unauthorized Access** – Adversaries gaining access to systems and services
c. **Information Disclosure** – Theft of sensitive organizational and citizen data
d. **Session Hijacking** – Browser cookies and active session data may be stolen to bypass authentication controls and maintain unauthorized access.
e. **Financial Fraud** – Theft of financial information and online account compromise
f. **Malware Persistence** – Installation of keyloggers, information stealers, and proxy malware
g. **Network Abuse** – Victim systems used as proxy nodes through GhostSock-type malware
h. **Ransomware Deployment** – Follow-on delivery of ransomware payloads including Conti-related threats
i. **Operational Disruption** – Service interruptions and degradation of critical functions
j. **Reputational Damage** – Loss of public confidence following compromise or data exposure

3. THREAT CHARACTERISTICS

Sr. No.	Characteristic	Details
a.	Threat Category	Phishing-enabled malware delivery and credential theft
b.	Threat Status	Active and ongoing
c.	Root Cause	Social engineering through malicious PDF lures, fake CAPTCHA pages, SEO poisoning, and user interaction leading to phishing or script-based malware execution.
d.	Malware Families	Lumma Stealer, Keyloggers, GhostSock, Ransomware Payloads
e.	Attack Complexity	Low to Medium
f.	Privileges Required	Standard User Access
g.	Affected Systems	Windows Workstations, Government Portals, Email Systems, Browsers
h.	Delivery Methods	Malicious PDF files, phishing websites, fake CAPTCHA pages, and SEO-poisoned links or search results.
i.	Execution Methods	PowerShell abuse, MSHTA execution, clipboard-assisted command execution, and script-based malware delivery.
j.	CWE Classifications	CWE-601 (Open Redirect), CWE-798 (Credential Exposure), CWE-306 (Missing Authentication), CWE-494 (Download of Code Without Integrity Check), CWE-522 (Insufficiently Protected Credentials)

4. INDICATORS OF EXPOSURE (IoEs)

a. Receipt of unsolicited PDF documents containing CAPTCHA images
b. User redirection from PDF files to unfamiliar websites
c. Execution of mshta.exe or unusual PowerShell commands
d. Unexpected browser credential or cookie theft alerts
e. Connections to suspicious domains discovered through search engine results
f. Unusual authentication attempts against government email accounts
g. Unauthorized access to government web portals or administrative interfaces
h. Creation of PowerShell processes from document viewers or browsers
i. Suspicious outbound traffic to known malware command-and-control infrastructure
j. Discovery of credential-stealing malware or persistence mechanisms on endpoints

5. REMEDIATION ACTIONS

Sr. No.	Action Category	Specific Actions
a.	Endpoint Protection	Deploy and maintain advanced Endpoint Detection and Response (EDR) solutions
b.	PowerShell Controls	Restrict unauthorized PowerShell execution through Group Policy and application controls
c.	MSHTA Restrictions	Disable or restrict execution of mshta.exe where operationally feasible
d.	User Awareness	Conduct phishing awareness campaigns focused on fake CAPTCHA and malicious PDF techniques
e.	Email Security	Strengthen email filtering and attachment inspection controls
f.	DNS/Web Filtering	Block known malicious domains and phishing infrastructure
g.	Threat Intelligence	Subscribe to threat intelligence feeds and monitor emerging indicators
h.	Application Control	Implement application whitelisting and script execution controls
i.	Patch Management	Ensure operating systems and applications remain fully updated
j.	Access Control	Limit administrative privileges and enforce least-privilege principles

6. ACTION SUMMARY & RESPONSE PRIORITIES

Sr. No.	Action Type	Specific Steps
a.	Immediate Protection	Block identified malicious domains and URLs
b.	Credential Security	Reset potentially exposed credentials and review account activity
c.	MFA Enforcement	Enable Multi-Factor Authentication across all critical systems
d.	Endpoint Monitoring	Investigate PowerShell and MSHTA execution events
e.	User Awareness	Alert employees regarding malicious PDFs and fake CAPTCHA schemes
f.	Incident Response	Review systems for malware indicators and unauthorized access
g.	Recovery Readiness	Validate backup integrity and disaster recovery procedures

7. MONITORING & DETECTION REQUIREMENTS

Sr. No.	Monitoring Activity
a.	Enable detailed PowerShell logging and script block logging
b.	Monitor execution of mshta.exe and related scripting engines
c.	Detect downloads initiated from suspicious PDF documents
d.	Monitor authentication anomalies against email and portal services
e.	Review endpoint telemetry for Lumma Stealer indicators
f.	Track access to newly registered or suspicious domains
g.	Detect unusual browser cookie extraction activity
h.	Monitor credential dumping and information-stealing behaviors
i.	Review EDR alerts related to phishing and malware execution
j.	Correlate threat intelligence indicators with enterprise logs

8. INCIDENT REPORTING

All suspected compromise, anomalous VPN activity, phishing-related incidents, or any indication of exploitation attempts must be reported immediately to the National CERT through the official channels below:

- **Incident Reporting Portal:** https://pkcert.gov.pk/report-incident
- **Email:** cert@pkcert.gov.pk
- **UAN:** +92 51 9203412

9. CALL TO ACTION – KEY SECURITY PRACTICES

Sr. No.	Requirement
a.	Do not trust CAPTCHA prompts embedded within PDF documents
b.	Avoid opening links contained in unsolicited or unexpected PDFs
c.	Verify URLs before entering credentials or downloading files
d.	Enable Multi-Factor Authentication on all government accounts
e.	Report suspicious emails, PDFs, and websites immediately
f.	Restrict unauthorized PowerShell and scripting activity
g.	Maintain up-to-date endpoint protection solutions
h.	Apply security patches promptly across all systems
i.	Follow least-privilege access principles for all users
j.	Regularly review logs and threat intelligence for emerging indicators

WARNING: Failure to implement appropriate safeguards against phishing campaigns distributing information stealers and keyloggers may result in credential compromise, unauthorized access to systems, sensitive data theft, ransomware deployment, and significant operational disruption.