Priority

GOVERNMENT OF PAKISTAN
CABINET DIVISION
******

SUBJECT: CYBER SECURITY ADVISORY FAKE CAPTCHA BASED PHISHING CAMPAIGN DELIVERING LUMMA STEALER MALWARE (ADVISORY NO. 04/2025)

Introduction. A large-scale phishing campaign has been identified, exploiting fake CAPTCHA images in PDF files to distribute the Lumma Stealer malware. This campaign has already compromised thousands of users across various sectors, including technology, financial services, and manufacturing, with a focus on North America, Asia, and Southern Europe.

Threat actors are using search engine manipulation to lure victims into downloading malicious PDFs that redirect them to fraudulent sites. These sites either steal financial information or infect systems with malware using PowerShell-based techniques. This advisory provides detailed insights into the attack methodology, indicators of compromise (IOCs) and recommended security measures:

2. **Campaign Details**

a. **Attack Mechanism**

i. **Malicious PDFs with Fake CAPTCHAs:** Attackers distribute PDF files containing deceptive CAPTCHA images.

ii. **Redirection to Malicious Websites:** Clicking the CAPTCHA leads users to phishing sites that either steal sensitive financial data or deploy malware.

iii. **PowerShell and MSHTA Exploits:** The malware is executed via a hidden PowerShell script triggered through an MSHTA command, enabling silent installation of Lumma Stealer.

iv. **SEO Poisoning:** Malicious PDFs are hosted on platforms like PDFCOFFEE, PDF4PRO, and Internet Archive, appearing in legitimate search engine results.

b. **Lumma Stealer Capabilities:** Lumma Stealer is a Malware-as-a-Service (MaaS) tool capable of:

i. Stealing login credentials, browser cookies, and cryptocurrency wallet data.
ii. Using GhostSocks, a proxy malware, to exploit victims' internet connections.
iii. Selling stolen credentials on underground hacking forums like Leaky[.]pro.

c. **Indicators of Compromise (IOCs)**

Malicious Domains

i. hxxps://pdf-freefiles[.]com

ii. hxxps://webflow-docs[.]info

iii. hxxps://secure-pdfread[.]site

iv. hxxps://docsviewing[.]net

d. **SHA256 Hashes of Malicious Files**

i. 8a5f1c9b2e4a64e192c09c04f1b10c71615c62b3aa0a34c4c051e3b8d5314b4d

ii. d4623a7f7c9b8c42a6735c6f812e9d06ab6c614f3325a17db7bc2b5e2f9a90c7

3. **Recommendations and Action Items**

a. **Prevention Measures**

i. **User Education:** Train employees on identifying phishing tactics, including fake CAPTCHAs and malicious PDFs.

ii. **Endpoint Protection:** Deploy advanced endpoint detection and response (EDR) solutions to block PowerShell abuse.

iii. **SEO Monitoring:** Organizations should track and report fraudulent domains impersonating legitimate services.

iv. **Restrict PowerShell and MSHTA Execution:** Implement Group Policy restrictions to prevent unauthorized execution of scripts.

b. Detection Measures

i. **PowerShell Logging:** Enable detailed logging to monitor for unauthorized PowerShell execution.

ii. **Threat Intelligence Feeds:** Subscribe to security feeds to detect new malicious URLs and file hashes.

iii. **Use Sigma Rules:** Implement the following Sigma detection rules for monitoring PowerShell download and execution (**attached**)

4. Incident Response and Mitigation

a. **Block Malicious Domains:** Add identified domains to DNS and web filters to prevent access.

b. **Deploy Behavioral Analysis Tools:** Monitor network traffic for anomalies linked to Lumma Stealer.

c. **Backup and Disaster Recovery:** Regularly back up critical data and validate recovery procedures.

a. **Patch Management:** Ensure all systems are updated to mitigate vulnerabilities exploited by PowerShell and MSHTA.

b. **Restrict Admin Privileges:** Limit administrative access to essential personnel to prevent privilege escalation.

c. **Multi-Factor Authentication (MFA):** Enforce MFA to mitigate credential theft risks.

d. **Application Whitelisting:** Allow only trusted applications and scripts to run on enterprise systems.

6. **Conclusion:** This advisory underscores the evolving nature of phishing campaigns using fake CAPTCHAs to distribute malware. Given the increasing sophistication of such attacks, National CERT strongly urges organizations to enhance their cybersecurity defenses through proactive monitoring, endpoint protection, and user awareness training.

7. Kindly disseminate the above information to all concerned in your organization, attached/affiliated departments and ensure implement the recommended security measures to mitigate the risk posed by this growing threat.

Major Hafiz Adnan Rana
Assistant Secretary NTISB-II

Secretary To The President, AIWAN-E-SADR(PS), Islamabad
Addl Secretary-I, Prime Minister's Office(PMO), Islamabad
Secretary Establishment Division, Establishment Division(ESTAB), Islamabad
Secretary-(AV-DIV), Ministry of Defence (Defence Division)(MOD), Rawalpindi
Secretary, Ministry of Commerce(MOC), Islamabad
Secretary, Ministry of Defence (Defence Division)(MOD), Rawalpindi
Secretary (DP), Ministry of Defence Production(MODP), Rawalpindi
Secretary (EAD), Economic Affairs Division(EAD), Islamabad
Secretary, Ministry of Energy (Petroleum Division)(MOPNR), Islamabad
Secretary, Ministry of Energy Power Division, Islamabad(MOEPWD), Islamabad
Secretary (Education), Ministry of Federal Education and Professional Training(MOFEPT), Islamabad
Secretary, National Heritage and Culture Division(NHCD), Islamabad

Secretary Finance, Ministry of Finance(MOF), Islamabad
Secretary, Revenue Division(REVDIV), Islamabad
Foreign Secretary, Ministry of Foreign Affairs(MOFA), Islamabad
Secretary, Ministry of Housing and Works(MOHW), Islamabad
Secretary, Ministry of Human Rights(MOHR), Islamabad
Secretary, Ministry of Industries & Production(MOIP), Islamabad
Secretary MoIBC, Ministry of Information and Broadcasting(MOIBC), Islamabad
Secretary IT, Ministry Of Information Technology and Telecommunication(MoIT), Islamabad
Secretary of Interior, Ministry of Interior and Narcotics Control(MOI), Islamabad
Secretary Kashmir Affair,Gilgit Baltistan & SAFRON, Ministry of Kashmir Affairs & Gilgit Baltistan(MOKAGB), Islamabad
Secretary LAW & Justice, Ministry of Law and Justice(MOLJ), Islamabad
Secretary, Ministry of Maritime Affairs(MOMA), Islamabad
Secretary, Ministry of Interior and Narcotics Control(MOI), Islamabad
Secretary, Ministry of National Food Security and Research(MONFSR), Islamabad
Federal Secretary of MoNHS, Ministry of National Health Services Regulations and Coordination(MONHS), Islamabad
Secretary, Ministry of Overseas Pakistanis & Human Resource Development(MOPHRD), Islamabad
Secretary Ministry of Parliamentary Affairs, Ministry of Parliamentary Affairs(MOPA), Islamabad
Secretary Planning, Ministry of Planning Development & Special Initiatives(PC), Islamabad
Secretary, PA&SS Division, Poverty Alleviation and Social Safety(PASS), Islamabad
Secretary, Privatisation Division(PRIDIV), Islamabad
Secretary (Railways), Ministry of Railway, Islamabad(MOR), Islamabad
Secretary, Ministry of Religious Affairs and Inter-Faith Harmony(MORA), Islamabad
Secretary Science and Technology, Ministry of Science and Technology(MOST), Islamabad
Secretary SAFRON, Ministry of Kashmir Affairs & Gilgit Baltistan(MOKAGB), Islamabad
Federal Secretary, Ministry of Water Resources(MOWR), Islamabad
Secretary, National Security Division(NSD), Islamabad
Secretary SIFC, Special Investment Facilitation Council(SIFC), Islamabad
Additional Secretary, Ministry of Climate Change and Environmental Coordination(MOCC), Islamabad
Additional Secretary, Ministry of Inter-Provincial Coordination(MOIPC), Islamabad
Secretary, SENATE of PAKISTAN(SENATE), Islamabad
Secretary ECP, Election Commission of Pakistan(ECP), Islamabad
Secretary BoI, Board of Investment(BOI), Islamabad
Secretary, FEDERAL OMBUDSMAN OF PAKISTAN(FOP), Islamabad
Secretary (Mgt/HR.IR-III), Federal Board of Revenue(FBR), Islamabad
Secretary Revenue Div/Chairman FBR, Federal Board of Revenue(FBR), Islamabad
Chairman, Pakistan Electronic Media Regularity Authority, Islamabad(PEMRA), Islamabad
Chairman HEC, Higher Education Commission(HEC), Islamabad
Chairman OGRA, Oil and Gas Regulatory Authority (OGRA)(OGRA), Islamabad
Chief Executive Officer (NITB), National Information Technology Board(NITB), Islamabad
Director General FIA, Federal Investigation Agency, G-9/4 , Mauve Area, Islamabad(FIA), Islamabad
Director General, Directorate General Immigration & Passports(DGIP), Islamabad
AD (Admin), National Telecommunication Corporation, Islamabad(NTC), Islamabad
Director General (IDB), Intelligence Bureau Division(IBD), Islamabad
Accountant General, Accountant General Pakistan Revenues (AGPR)(AGPR), Islamabad
Additional Secretary-III, Cabinet Division(CAB), Islamabad
Section Officer(Coord), Cabinet Division(CAB), Islamabad
Deputy Director-IT, Cabinet Division(CAB), Islamabad

Cabinet Division No.1-5/2003/24(NTISB-II) Dated 26 March , 2025