I4C cautions corporates and finance professionals against ‘Boss Scam’: WhatsApp account takeover through malicious ‘Statement of Account’, ‘MCA’ and ‘RBI’ files aimed at high-value financial fraud

Self-propagating malware disguised as account statements and RBI communications spreading over WhatsApp, SMS and e-mail; Chartered Accountants, Company Directors, CFOs and corporate finance teams the prime targets

Compromised WhatsApp accounts of senior executives misused to instruct finance staff to transfer funds to mule accounts

I4C has intimated over 58000 potential victims through SMS header ‘I4CMHA-G’ in last 30 days; threat signals shared with CERT-In, Microsoft, Indian Anti-virus & Threat Intelligence companies

More than 10,000 Indians protected from the campaign so far by geo-blocking C2 Servers through Sahyog Portal

प्रविष्टि तिथि: 07 AUG 2026 1:01PM by PIB Delhi

The Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs (MHA), has observed a sharp rise in complaints on the National Cyber Crime Reporting Portal (NCRP) relating to the takeover of WhatsApp accounts of professionals and businesspersons through malicious files circulated in the guise of account statements and regulatory communications. In the last few days, incidents following an identical modus operandi have been reported from multiple States, including Delhi, Gujarat, Maharashtra and Rajasthan. I4C had alerted citizens to this emerging threat through its Advisory issued on 22nd June, 2026, titled *“Regulatory and Executive Impersonation for WhatsApp Account Takeover using Malicious Windows Executables and High Value Financial Fraud”*.

In the reported incidents, victims receive a compressed (.zip) file over WhatsApp, SMS or e-mail bearing names such as **“Statement of Account.zip”** (often prefixed with a date, e.g. “0714 Statement of Account.zip”) or **“RBI.zip”, “MCA.zip”**. The accompanying message is crafted to appear either as a

routine account statement or as an urgent notice from a regulator such as the Reserve Bank of India (RBI) and Ministry of Corporate Affairs, demanding compliance within a very short timeframe. The archive contains a malicious Windows executable (.exe) accompanied by a Dynamic Link Library (.dll) file. When the file is extracted and opened on a Windows desktop or laptop, a Trojan is installed which compromises the device and hijacks the victim's active WhatsApp Web session. In many case emails are also sent impersonating Income Tax Department.

The compromised WhatsApp account is thereafter misused to automatically circulate the same malicious file to all the contacts and groups of the victim, typically with a request to forward the file to the recipient's *"company finance manager for verification"* and to open it on a computer, thereby extending the chain of infection deeper into corporate networks. In the advanced stage of the fraud, commonly referred to as the **"Boss Scam" or CEO impersonation fraud**, the fraudsters use the genuine WhatsApp account of a senior executive – or covertly save an attacker-controlled number under the name of the "CEO" in the compromised device – to instruct accounts and finance employees to make urgent transfers of funds to mule bank accounts.

Technical analysis carried out by the National Cybercrime Threat Analytics Unit (NCTAU) of I4C indicates that the campaign is being operated by organised networks acting across national borders and employs advanced malware with sophisticated propagation and detection-evasion capabilities through DLL Sideloading method. Investigation is being pursued in coordination with the concerned law enforcement and technical agencies.

Since the malware activates only on Windows computers and the lure documents reference account statements and regulatory compliance, the campaign poses a particular risk to **Chartered Accountants, Company Directors, Chief Financial Officers (CFOs) and finance and accounts personnel of companies**. All corporate entities are advised to immediately sensitise their employees, especially finance teams, and to independently verify – through a direct voice call or in-person confirmation – any urgent fund-transfer instruction or account-change request received over WhatsApp or e-mail before acting upon it.

To counter this threat, I4C has taken the following measures:

(i) Victim Intimation: Victims and potential victims identified through complaint analysis and technical intelligence are being proactively intimated by I4C so that timely remedial action, such as logging out of linked devices and securing accounts, can be taken.

(ii) Threat Signal Exchange: Threat signals and technical indicators of the malware have been shared with the Indian Computer Emergency Response Team (CERT-In), Microsoft Defender and leading Indian anti-virus companies, namely Quick Heal, K7 Computing and Net Protector, to enable rapid detection, blocking and removal of the malicious files across platforms and security products.

(iii) Citizens Protected: Through these coordinated interventions, more than 10,000 Indians have been protected from this campaign so far. Malwares are being blocked regularly through Sahyog Portal.

(iv) Alerts through SMS header 'I4CMHA-G': I4C is sending alerts to affected citizens through the SMS header 'I4CMHA-G'. I4C has intimated over 58000 potential victims through SMS header 'I4CMHA-G' in last 30 days; threat signals shared with CERT-In, Microsoft, Indian Anti-virus & Threat Intelligence companies. Citizens are requested to keep a watch on messages received from the SMS header 'I4CMHA-G' and to act promptly on the advice contained therein.

Citizens and organisations are further advised to observe the following precautions:

- Do not download, extract or open .zip files or executables received from unknown or unverified sources. Regulators such as the RBI never distribute software updates, security fixes or account

statements through WhatsApp attachments.

- Regularly review linked devices in the WhatsApp application (Settings > Linked Devices) and log out of WhatsApp Web sessions that are no longer in active use.
- System administrators should enforce software restriction policies to block the execution of unknown .exe and .dll files from user profile directories, and ensure that all Windows endpoints run up-to-date anti-malware solutions.
- If an account is compromised, immediately log out of all linked devices, alert contacts not to open any file received from the account, and get the computer scanned with an updated anti-virus.

Cyber frauds and suspicious communications of this nature should be reported immediately on the National Cyber Crime Helpline number **1930** or on the National Cyber Crime Reporting Portal **www.cybercrime.gov.in**. The detailed Advisory is available on the portal.

***

RK/RR/PR/PS

(रिलीज़ आईडी: 2295889) आगंतुक पटल : 2804