SECURITY ADVISORY

Advisory No.	BtCIRT_ADV01_2026-27
Date Issued	July 6, 2026
Severity	HIGH
Threat Category	Malware / Social Engineering / Account Compromise
Affected Platforms	WhatsApp Desktop, WhatsApp Web (Windows systems)

Subject: **Active Global Malware Campaign Abusing Compromised WhatsApp Accounts to Distribute Malicious VBScript Files**

1. Overview

The Bhutan Computer Incident Response Team (BtCIRT) is issuing this advisory to alert government agencies, businesses, and the general public in Bhutan to an active, large-scale malware campaign spreading through WhatsApp Desktop and WhatsApp Web.
This advisory is based on corroborated reporting from multiple trusted sources:

- **Kaspersky's Global Research and Analysis Team (GReAT)** first disclosed the campaign through original technical research published on Securelist
- **MyCERT (Malaysia Computer Emergency Response Team)**, under CyberSecurity Malaysia, issued Advisory MA-1464.062026 (dated June 22, 2026), confirming the campaign targeting Malaysian WhatsApp Desktop/Web users.
- **CERT-In (Indian Computer Emergency Response Team)** issued a formal advisory (dated June 25, 2026) warning of the campaign targeting WhatsApp Web and Desktop users.

The campaign exploits trust in existing contact relationships rather than a software vulnerability. Attackers first take over a victim's WhatsApp account, then use that hijacked account to silently push malicious file attachments to the victim's own contacts: friends, family, and colleagues; making the messages appear to come from someone the recipient already trusts.

2. Who Is Affected

While the campaign has been reported to have affected many countries, BtCIRT has not received confirmed reports of this specific campaign inside Bhutan at the time of this advisory. However, because the attack travels through personal and business contact networks rather than targeting a specific country, and because WhatsApp Desktop/Web usage is widespread in Bhutan, the risk to Bhutanese individuals, businesses, and government offices is considered real and immediate.

3. How the Attack Works

3.1. Account takeover: Attackers first gain control of a WhatsApp account through means such as session hijacking or credential theft. The exact takeover method used in this campaign has not yet been confirmed by researchers.

3.2. Trusted delivery: Using the hijacked account, the attacker sends a file, with no accompanying message, to the account's existing contacts. Because it appears to come from someone known to the recipient, the file is opened far more readily than an unsolicited message from a stranger would be.

3.3. Disguised lure: The attached file is a VBScript (.vbs) disguised as a routine business or financial document: for example, filenames resembling "Financial Reports," "Account Statement," "Outstanding Payment List," or "Debt Statement."

3.4. Multi-stage infection: Once opened, the script runs through Windows Script Host (wscript.exe), silently creates a working folder, and downloads further script components from attacker-controlled servers. The scripts contain code comments designed to imitate legitimate Microsoft Windows Update components to avoid raising suspicion.

3.5. Remote access installed: The final stage installs a legitimate Remote Monitoring and Management (RMM) tool (Kaspersky identified ManageEngine Endpoint Central being abused in this campaign), giving the attacker hands-on remote access to the victim's computer.

3.6. Impact: From there, attackers can steal saved browser passwords, capture keystrokes, exfiltrate financial or confidential documents, move laterally across a connected office network, or deploy further malware/ransomware.

4. Indicators to Watch For:

- An unexpected file attachment arriving on WhatsApp Desktop/Web from a known contact, with no message text.
- File names resembling invoices, bank/account statements, payment records, or debt notices, with a .vbs, .vbe, .js, .wsf, or similar script extension.
- Unexplained installation of remote-access/remote-support software (e.g., an unfamiliar RMM agent) on a work or personal computer.
- New entries under WhatsApp's "Linked Devices" that the account owner does not recognize.

5. Recommendations

For individuals:

- Do not open unexpected file attachments received via WhatsApp, even from known contacts, without first verifying with the sender through a separate channel (a phone call, for instance) that they intentionally sent it.

- Never open or run script files (.vbs, .vbe, .js, .wsf, .hta, .bat, .cmd, .ps1) received through any messaging app.
- Regularly check WhatsApp's Linked Devices settings and remove any session you don't recognize.
- Enable two-factor authentication on WhatsApp and other messaging/social accounts.
- Keep your operating system, browser, and WhatsApp application up to date, and run reputable endpoint/antivirus protection.

For organizations and government offices:

- Circulate this advisory to staff and reinforce a "verify before you click" culture for messaging-app attachments.
- Restrict or monitor the execution of Windows Script Host (wscript.exe/cscript.exe) on end-user machines where not required for business operations.
- Monitor endpoints for unauthorized installation of RMM/remote-access software.
- Ensure WhatsApp Business/Desktop use on corporate machines is covered by endpoint detection and response (EDR) tooling.
- Review and restrict administrative/UAC elevation settings, as this campaign has been observed attempting to weaken User Account Control prompts.

6. Reporting

If you suspect your device or account has been compromised as part of this campaign, or you receive a suspicious WhatsApp attachment matching this pattern, please report it to: cirt@btcirt.bt

7. Sources and References

1. CERT-In Advisory (June 25, 2026): large-scale malware campaign targeting WhatsApp Web and Desktop users: https://the420.in/cert-in-whatsapp-desktop-web-malware-advisory-hacked-accounts/
2. MyCERT (Malaysia) Advisory(June 22, 2026), "Malware Campaign Delivering Malicious VBScript via WhatsApp Desktop": https://mycert.org.my/portal/advisory?id=MA-1464.062026.
3. Kaspersky GReAT / Securelist(June 2026): "An unknown actor distributes malicious VBS scripts via WhatsApp," Securelist.com: https://securelist.com/whatsapp-vbs-rmm-campaign/120290/

This advisory will be updated if BtCIRT receives confirmed reports of this campaign affecting users/systems within Bhutan, or as further technical detail becomes available from the International community.