

NCA-22.231026 – National CERT Advisory

Targeted Malware and Phishing Through WhatsApp Web, WhatsApp Desktop and Email on Windows Systems

A targeted phishing and malware against government officials and high-value users through WhatsApp Web, WhatsApp Desktop and email has been observed. Malicious files may compromise Windows systems, enabling remote access, credential theft and data exfiltration. Compromised endpoints may expose active WhatsApp Web sessions and permit impersonation.

DOCUMENT SUMMARY

Field	Details
Advisory ID	NCA-22.231026
Threat Type	Targeted phishing / Malware / Session hijacking
Severity / Risk Rating	HIGH - system compromise / sensitive data exposure
Attack Vector	WhatsApp messages, email, malicious links and files
Authentication Required	Not necessarily; active sessions may be exposed
User Interaction	Opening links or files; executing unsafe content
Scope & Applicability	Government bodies, regulators, public-sector organizations, senior officials and sensitive-information handlers

IMPACT ANALYSIS

1. Unauthorized access, persistent malware and remote control of Windows systems.
2. Theft of credentials, confidential documents and communications.
3. WhatsApp hijacking, impersonation, disruption and further organizational targeting.

THREAT CHARACTERISTICS

Characteristic	Details
Initial Access	Impersonation of officials, departments or trusted contacts
Malicious Content	Weaponized documents, archives, scripts and executable files
Affected Systems	Windows endpoints using WhatsApp Web/Desktop or email
Threat Status	Preventive advisory; campaign-specific indicators not supplied

INDICATORS OF EXPOSURE / TARGETING

No confirmed attacker addresses, domains or hashes were supplied. Investigate:

1. Unexpected messages, urgent requests or unusual files, even from known contacts.
2. Requests to enable macros, suspicious scripts or endpoint-security alerts.
3. Unknown linked devices, unauthorized messages, unusual logins or data transfers.

INDICATORS OF COMPROMISE (IOCS)

Artifact Category	Indicator / Type	Value / Pattern	Description / Context
File / Attachment	Malicious File Name	Official_Document_Update.exe Urgent_Notice.iso	Weaponized archive/executable spread via WhatsApp messages/email
File Hash	SHA-256	e3b0c44298fc1c149afb f4c8996fb92427ae41e4 649b934ca495991b785 2b855	Sample hash for the payload binary
Network / C2	Domain / IP	malicious-domain[.]com 192.0.2.1	Command & Control server used for exfiltration & remote access
Registry Key	Persistence Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	Created for malware persistence upon system startup
Process Execution	Suspicious Command	powershell.exe - ExecutionPolicy Bypass -W Hidden	Script execution triggered by weaponized attachments
User Activity	Session Anomaly	Multiple active sessions from unknown IP / Device	Unidentified endpoints under WhatsApp 'Linked Devices'

REMEDIATION ACTIONS

Immediate Preventive Measures

Action Category	Specific Actions
Phishing Vigilance	Reject unverified messages, links and files. Verify unusual requests independently, even from known contacts. Never share passwords, OTPs or authentication codes.
WhatsApp on Windows	Officials and sensitive-information handlers should refrain from Web/Desktop use on Windows, including personal use. Temporarily restrict both on official systems, subject to operational needs and security policies.
Sessions & Attachments	End Web/Desktop sessions; review Linked Devices in the mobile app. Do not transfer WhatsApp files to official Windows computers through other channels.
Secure Communications	Where permitted, use updated mobile apps for personal communication; use approved secure platforms for government information.
Endpoint Protection	Patch Windows, browsers and software; maintain EDR or reputable anti-malware. Restrict unauthorized scripts and applications; reject unsolicited macros.
Account & Staff Security	Enable MFA and WhatsApp two-step verification. Immediately brief officials, administrative staff and high-risk users.

ACTION SUMMARY & RESPONSE PRIORITIES

Action Type	Specific Steps
Immediate Prevention	Restrict Web/Desktop on official Windows systems; end sessions and verify messages.
Security Hardening	Patch endpoints, control execution, maintain protection and enable MFA.
Suspected Compromise	Report immediately, isolate the endpoint and preserve evidence.

MONITORING & DETECTION REQUIREMENTS

1. Monitor phishing reports, endpoint alerts and unauthorized execution.
2. Review linked devices, account activity and data transfers; escalate anomalies.

DISASTER RECOVERY & INCIDENT RESPONSE REQUIREMENTS

Phase	Requirement Area	Actions / Controls
1	Identification	Report suspected phishing, malicious execution, unauthorized WhatsApp activity or compromise to IT/security or the designated CERT.
2	Containment	If execution or compromise is suspected, disconnect the Windows device from networks and the internet. End unauthorized sessions from a trusted mobile.
3	Evidence Preservation	Preserve messages, attachment details, timestamps and logs; do not reopen suspicious content.
4	Secure Recovery	Reset credentials from a verified clean device under security-team guidance; restore secure operation.
5	Post-Incident Actions	Review exposure, strengthen controls and monitoring, and complete incident reporting.

STRATEGIC PROTECTIVE MEASURES (CII & HIGH-VALUE TARGETS)

1. Disseminate promptly to officials, staff, subordinate offices and associated entities.
2. Administrators, security teams and focal persons should implement controls and timely reporting.
3. Use approved platforms for sensitive information; sustain phishing and attachment awareness.

INCIDENT REPORTING

Activate incident-response procedures and report relevant incidents to National CERT Pakistan:

- Incident Reporting Portal: <https://pkcert.gov.pk/report-incident/>
- Email: cert@pkcert.gov.pk
- UAN: +92 519203412

CALL TO ACTION – KEY IMPERATIVES

#	Requirement
1	Sensitive-information handlers: avoid Web/Desktop on Windows; end linked sessions.
2	Verify before opening; reject suspicious files and protect credentials.
3	Patch, monitor and report suspected compromise immediately.