CTAC Cyber Threat Intelligence Report

Executive Summary

Over the past week, winter weather conditions across Louisiana created elevated cyber risk for state and local government entities. Threat actors exploited operational disruption, staffing shortages, and increased reliance on remote access to conduct phishing, credential theft, and opportunistic ransomware activity. While no single large-scale campaign was weather-exclusive, multiple threat patterns directly leveraged storm-related condition s, messaging, and outages.

Overall Risk Level: MODERATE

Primary drivers: social engineering, remote access exposure, and reduced defensive posture during outages.

Weather-Themed Phishing & Impersonation

- Phishing emails spoofing utilities, state agencies, school systems, and courts
- Subject lines referencing power outages, closures, billing credits, and emergency notices
- Credential harvesting via fake Microsoft 365, VPN, and payroll portals

Ransomware Timing Around Outages & Staffing Gaps

- Increased scanning for exposed RDP and VPN services during storm periods
- Ransomware affiliates favor weekend and overnight execution
- Targeting organizations with public-facing service disruption risk

Remote Access & VPN Exploitation

- Credential stuffing and brute-force attempts against VPNs
- MFA fatigue attempts against email and remote access portals
- Targeting of older or unpatched VPN appliances

Power Disruptions Creating Security Blind Spots

- Firewalls, IDS/IPS, badge systems, and cameras are temporarily offline
- Logging and alerting gaps during outages
- Emergency network reconfigurations left in place post-storm

Priority Actions for Louisiana State and Local Government

- Issue staff advisory on weather-themed phishing
- Enforce MFA on email, VPN, and remote access
- Review logs for activity during power/internet outages
- Validate backup integrity following power events
- Audit VPN, RDP, and firewall exposure
- Remove or review temporary emergency network changes

WhatsApp bug lets malicious media files spread through group chats:

What: Google's Project Zero has just disclosed a WhatsApp vulnerability where a malicious media file, sent into a newly created group chat, can be automatically downloaded and used as an attack vector. The bug affects WhatsApp on Android and involves zero-click media downloads in group chats. You can be attacked simply by being added to a group and having a malicious file sent to you.

How to Secure Whatsapp:

Goal: ensure that no photos, videos, audio, or documents are pulled to the device without an explicit decision.

- Open WhatsApp on your Android device.
- Tap the three-dot menu in the top-right corner, then tap **Settings**.
- Go to **Storage and data** (sometimes labeled **Data and storage usage**).
- Under **Media auto-download**, you will see **When using mobile data**, **when connected on Wi-Fi**. and **when roaming**.

- For each of these three entries, tap it and uncheck all media types: **Photos**, **Audio**, **Videos**, **Documents**. Then tap **OK**.
- Confirm that each category now shows something like “No media” under it.

Doing this directly implements Project Zero’s guidance to “disable Automatic Download” so that malicious media can’t silently land on your storage as soon as you are dropped into a hostile group.

Stop WhatsApp from saving media to your Android gallery

Even if WhatsApp still downloads some content, you can stop it from leaking into shared storage where other apps and system components see it.

- In **Settings**, go to **Chats**.
- Turn off **Media visibility** (or similar option such as **Show media in gallery**). For particularly sensitive chats, open the chat, tap the contact or group name, find **Media visibility**, and set it to **No** for that thread.

This article can be found at:

https://www.malwarebytes.com/blog/news/2026/01/a-whatsapp-bug-lets-malicious-media-files-spread-through-group-chats

- For more information and to request LCAP services, please scan the QR Code or click on the following link.
  - https://forms.office.com/g/YzD8n1xjEq

- Please report all cyber incidents to the Louisiana State Analytical and Fusion Exchange at 1-800-434-8007
- Visit https://getagameplan.org/make-aplan/cybersecurity-plan/

GOHSEP CTAC (Cyber Threat Analysis Center)

Contact: ctac.intel@esf2.la.gov