Governor's Office of Homeland Security and Emergency Preparedness (GOHSEP)
Cyber Threat Analytics Center (CTAC)

CTAC Cyber Threat Intelligence Report (24MAR26)

Executive Summary

Over the past week, CTAC observed **elevated cyber threat activity driven by nation-state targeting, exposure of sensitive public safety data, and continued exploitation of user behavior through social engineering**.

A reported breach involving **Navigate360's P3 Global Intel platform** highlights risks associated with third-party systems supporting law enforcement and school safety operations. Additionally, federal partners have identified **Russian Intelligence Services (RIS) actively targeting commercial messaging applications**, emphasizing a growing trend of exploiting trusted communication platforms rather than technical vulnerabilities.

These developments, combined with persistent credential theft and geopolitical cyber activity, indicate a **highly active threat environment with increased risk to government, public safety, and critical communication systems**.

Overall Risk Level: MODERATE - ELEVATED

Primary drivers: third-party data exposure, nation-state social engineering campaigns, credential compromise, and messaging platform exploitation.

Threat of the Week – Navigate360 / P3 Global Intel Data Exposure

A reported breach involving Navigate360's **P3 Global Intel platform**—used by law enforcement, schools, and government agencies—remains under investigation.

A threat actor claims to have accessed **millions of confidential tips (~93GB of data)**; while the company has not confirmed the full scope,

independent verification of portions of the dataset increases confidence that sensitive data exposure may have occurred.
Initial reporting indicates access was obtained through **social engineering and account compromise**, rather than direct exploitation of platform vulnerabilities.

If validated, this incident presents significant risks including:

- Exposure of sensitive law enforcement and school safety data
- Potential identification of anonymous tipsters
- Increased targeting of individuals referenced in reports
- Erosion of trust in public safety reporting systems

This event reinforces the critical risk posed by **third-party platforms handling sensitive government and public safety data**.

Geopolitical Cyber Watch – Russia & Iran Activity

Russian Intelligence Targeting Messaging Platforms (See https://www.ic3.gov/PSA/2026/PSA260320)

CISA and the FBI report that **Russian Intelligence Services (RIS)** are actively conducting phishing and impersonation campaigns targeting commercial messaging applications, including Signal.

Key tactics include:

- Impersonating platform support or trusted contacts
- Requesting verification codes or credentials
- Linking unauthorized devices to user accounts

These campaigns target:

- Government personnel
- Military members
- Journalists and high-value individuals

Notably, **encryption remains intact**, but attackers are successfully exploiting **user behavior to bypass security protections**.

Iran-Linked Cyber Activity

Iran-aligned actors continue to demonstrate **elevated cyber activity**, including:

- Website defacement
- Distributed denial-of-service (DDoS) attacks
- Opportunistic targeting of U.S. organizations

Cyber activity remains aligned with broader geopolitical tensions and is likely to continue in the near term.

Louisiana-Specific Risk Indicators

While no major publicly reported cyber incidents are directly tied to Louisiana this week, the following risks remain relevant:

- Exposure risks from **third-party vendors used by schools and law enforcement systems** (e.g., platforms similar to Navigate360)
- Continued phishing attempts targeting **state and local government email systems**
- Persistent vulnerabilities in **VPN and remote access infrastructure**
- Potential downstream impacts from national-level incidents affecting **public safety and healthcare systems**

Organizations should remain vigilant and ensure vendor risk management processes are actively enforced.

Credential Theft & Social Engineering

Credential theft remains the **primary initial access vector** in recent incidents, including the Navigate360 breach.

Threat actors continue to leverage:

- Phishing emails and vishing (phone-based attacks)
- AI-enhanced social engineering
- Credential stuffing and MFA fatigue techniques

These methods are particularly effective against **help desks, vendors, and administrative accounts**.

Remote Access & Network Exposure

Threat actors continue scanning for:

- VPN appliances
- Remote Desktop Protocol (RDP) services
- Administrative web portals

Unpatched or misconfigured systems remain one of the **most exploited vulnerabilities nationwide**.

Physical Cyber Intrusion & Impersonation Risks

Federal advisories continue to highlight threat actors **impersonating employees, vendors, or IT personnel** to gain access to facilities or systems.
Once access is obtained, actors may:

- Install unauthorized devices
- Access internal systems or networks
- Target sensitive infrastructure such as server rooms

These incidents reinforce the importance of integrating **physical security controls with cybersecurity practices**.

Priority Actions for Louisiana State and Local Government

- Review use of third-party platforms handling sensitive or law enforcement data
- Increase monitoring for credential-based attacks and social engineering activity
- Ensure all systems are patched and externally exposed services are secured
- Enforce multi-factor authentication (MFA) across all critical systems
- Conduct vendor risk assessments for platforms used in public safety and education

- Reinforce physical security and visitor access controls
- Educate staff on impersonation and social engineering threats

In the News: Massive Data Exposure Raises Concerns About "Anonymous" Reporting Systems

A reported breach involving Navigate360's P3 Global Intel platform remains under investigation; however, independent verification of portions of the dataset suggests that sensitive law enforcement and school safety information may have been exposed, highlighting ongoing risks associated with third-party platforms and credential-based attacks.

What this means for everyday people:
Systems marketed as "anonymous" may still be vulnerable to cyberattacks, potentially exposing sensitive personal information.

Simple ways to protect yourself:

- Avoid sharing highly sensitive personal details unless necessary
- Verify platforms and apps before submitting information
- Use caution when reporting information through third-party applications
- Stay informed about data breaches involving services you use

Cyber incidents like this highlight how **personal data shared for safety purposes can still be at risk if systems are compromised**.

Cybersecurity is not just an IT issue—it can impact daily life, services, and personal information.

Article can be found at:
https://www.reuters.com/legal/government/hacker-says-they-compromised-millions-confidential-police-tips-held-by-us-2026-03-18/

https://www.edweek.org/technology/a-potential-breach-of-an-anonymous-tip-app-could-have-exposed-sensitive-student-data/2026/03

- 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

Louisiana Cyber Assurance Program Service Request

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

GOHSEP CTAC (Cyber Threat Analysis Center)
Contact: ctac.intel@esf2.la.gov