CTAC Cyber Threat Intelligence Report 01/06/26

Emerging Trends - AI Augmented Threats

- Nation-state campaigns continue to target government infrastructure, probing critical sectors such as water, energy, and telecommunications, with **AI-driven tools and exploitation techniques on the rise** as we enter 2026.
    - Ransomware groups are increasingly using modular, AI-enhanced extortion toolkits, which lower the barriers for less skilled attackers.
    - AI-driven phishing, malware generation, and automated reconnaissance are expected to intensify attack speed and sophistication across state and local government entities.

Event-Driven Cyber Threats - Mardi Gras

- Large gatherings like Mardi Gras — especially under a high federal security designation — draw not just physical security planning but also digital threat monitoring.
- Major events attract DDoS attempts against city networks or transportation systems, and attackers may try to exploit high-traffic times when defenders are stretched.
- Hostile UAS/Drone Activity - notice of unmanned aerial systems detected near parade routes — a combined physical/cyber threat vector that could include surveillance or data collection.

Threat Patterns Around Major Events Like Mardi Gras

Cybercrime historically spikes around holidays and large events because:

- IT/security staff are stretched or on leave
- Criminals exploit attention and distraction in both governmental and citizen populations
- Scam operations blend into event noise, making them harder to detect

Cyber in the News:

Aflac Data Breach: Insurance provider **Aflac** has begun notifying approximately **22.65 million individuals** that their personal information was compromised during a cyber intrusion detected in June 2025.

The compromised data may include:

- Full names and addresses
- Social Security numbers
- Dates of birth
- Driver's license and government ID numbers
- Medical and health insurance information

Smart Devices Run Outdated Browser Versions — An academic study by a team of Belgian researchers has found that a majority of smart devices, such as smart TVs, e-readers, and gaming consoles, come with an embedded web browser that runs extremely outdated versions, sometimes as much as three years. All five e-readers that were tested, and 24 of 35 smart TV models, used embedded browsers that were at least three years behind current versions available to users of desktop computers. These outdated, embedded browsers can leave users open to phishing and other security vulnerabilities. The authors said some of the issues lie in how development frameworks like Electron bundle browsers with other components. "We suspect that, for some products, this issue stems from the user-facing embedded browser being integrated with other UI components, making updates challenging – especially when bundled in frameworks like Electron, where updating the browser requires updating the entire framework," they said in the paper. "This can break dependencies and increase development costs."

IT personnel impersonators stealing info and money.