



Week of April 21, 2025

## Cybersecurity Headlines

### Official Security Bulletins

Headlines from List of Official Government Sources

#### CISA, DHS S&T, INL, LSU Help Energy Industry Partners Strengthen Incident Response and OT Cybersecurity

WASHINGTON – The Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS) Science and Technology Directorate (S&T) and the Idaho National Laboratory (INL) hosted Louisiana State University (LSU) and several energ...

#### Statement from Matt Hartman on the CVE Program | CISA

The CVE Program is an invaluable public resource relied upon by network defenders and software developers alike. As the nation's cyber defense agency, it is a foundational priority for CISA.

<https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4163002/nsa-publishes-recommendations-for-smart-controller-security-controls-and-techni/>



#### NSA Publishes Recommendations for Smart Controller Security Controls and Technical Requirements for OT Environments > National Security Agency/Central Security Service > Press Release View

FORT MEADE, Md. – The National Security Agency (NSA) is releasing a Cybersecurity Technical Report (CTR) to share recommendations for security policies and technical requirements for operational

### Cybercrimes, Scams & Incidents

Headlines related to cybercrimes and scams including international cybersecurity news and high-profile incidents like ransomware and malware attacks



#### Financially-motivated cyber crime remains biggest threat source

Mandiant's latest annual threat report reveals new data on how financially-motivated cyber criminals, such as ransomware gangs, dominate the cyber security landscape



#### North Korean IT workers seen using AI tools to scam firms into hiring them

North Korean IT workers illicitly gaining employment at U.S. and European tech companies are increasingly using generative artificial intelligence in a variety of ways to assist them throughout the job application and interview process.

### Industry News

Headlines collected from across the cybersecurity industry related to legislation, business, and big tech



#### Easterly calls for united front against 'politicizing' of the cyber industry

The former head of the Cybersecurity and Infrastructure Security Agency warned against silence "when experienced, mission-driven leaders are sidelined or sanctioned."



#### UK bans export of video game controllers to Russia to hinder attack drone pilots

In a sanctions package including more than 150 new measures, the British government said it was closing loopholes being exploited by the Kremlin.

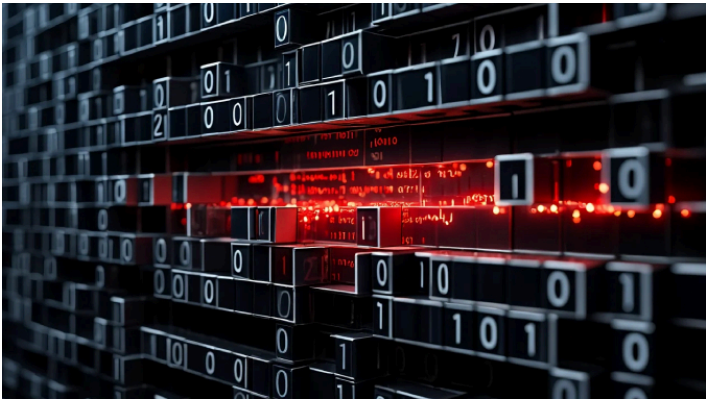




DragonForce expands ransomware model with white-label branding scheme - BleepingComputer

www.bleepingcomputer.com

The ransomware scene is re-organizing, with one gang known as DragonForce working to gather other operations under a cartel-like structure. DragonForce is now incentivizing ransomware actors with ...



159 CVEs Exploited in Q1 2025 — 28.3% Within 24 Hours of Disclosure - The Hacker News

thehackernews.com

As many as 159 CVE identifiers have been flagged as exploited in the wild in the first quarter of 2025, up from 151 in Q4 2024. "We continue to see vulnerabilities being exploited at a fast pace with 28.3% of vulnerabilities being exploited within 1-...

DOGE Worker's Code Supports NLRB Whistleblower

krebsonsecurity.com

A whistleblower at the National Labor Relations Board (NLRB) alleged last week that denizens of Elon Musk's Department of Government Efficiency (DOGE) siphoned gigabytes of data from the agency's ...



As Trump Shifts Cybersecurity to States, Many Are Unprepared

www.govtech.com

States and localities are taking steps to address the problems, such as establishing new penalties for tampering with critical infrastructure, centralizing state IT personnel and setting standards ...

Please be advised that the following resources and materials are for informational purposes only. The opinions and views expressed in these materials are the opinions of the designated authors and do not reflect the opinions or views of the Commonwealth of Massachusetts, the Executive Office of Technology Services and Security, and/or the Enterprise Risk Management Office, (the Commonwealth). The information posted on this website includes hypertext links or pointers to information created and maintained by other public and/or private organizations. These links and pointers are provided solely for the information and convenience of the user. By selecting a link to an outside website, the user is subject to the privacy, copyright, security, and information quality policies of that website. The Commonwealth is not responsible for transmissions users receive from linked websites.

Official Quick Links

-  [CISA](#)
-  [CIS/MS-ISAC](#)
-  [CyberCom](#)
-  [DHS](#)
-  [DOJ](#)
-  [FBI](#)
-  [NIST](#)
-  [NSA](#)

External Quick links

-  [AIScoop](#)
-  [BleepingComputer](#)
-  [Cisco Talos Intelligence Group](#)
-  [CSO Online](#)
-  [CyberScoop](#)
-  [Cybersecurity Dive](#)
-  [Cyware](#)
-  [CyberWire](#)
-  [FedScoop](#)
-  [Government Executive](#)
-  [Government Technology](#)
-  [ISACA](#)
-  [ISSA International](#)
-  [Krebs on Security](#)
-  [MITRE ATT&CK®](#)
-  [NASCIO](#)
-  [Schneier on Security](#)
-  [SC Media](#)
-  [StateScoop](#)
-  [The Hacker News](#)
-  [The Record](#)