



# Week of May 26, 2025

## Cybersecurity Headlines

### Official Security Bulletins

Headlines from List of Official Government Sources

#### NSA, ASD's ACSC, and others guidance on SIEM and SOAR implementation

www.nsa.gov

The National Security Agency (NSA) has joined the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) and other agencies to release three publications providing guidance for cybersecurity executives and network defenders to consider when implementing Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms.

<https://www.justice.gov/usao-sdtx/pr/websites-selling-hacking-tools-cybercriminals-seized>



#### Websites selling hacking tools to cybercriminals seized

www.justice.gov

HOUSTON – A coordinated effort involving an international disruption of an online software crypting syndicate which provides services to cybercriminals to assist them with keeping their malicious software (malware) from being detected has resulted in...

#### CIS Statement on the Passing of CIS Co-Founder Board Ramon Barquin

www.cisecurity.org

The Center for Internet Security, Inc. (CIS ®) marks with deep sadness the passing of our dear friend and colleague, Dr. Ramon Barquin, Director of the CIS Board of Directors.. A gifted technologist with a global footprint, his career spanned more th...

### Cybercrimes, Scams & Incidents

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

#### Pakistan Arrests 21 in 'Heartsender' Malware Service

krebsonsecurity.com

Authorities in Pakistan have arrested 21 individuals accused of operating "Heartsender," a once popular spam and malware dissemination service that operated for more than a decade. The main clientele for HeartSender were organized crime groups that tried to trick victim companies into making payments to a third party, and its alleged proprietors were publicly identified by KrebsOnSecurity in 2021

#### U.S. Sanctions Cloud Provider 'Funnul' as Top Source of 'Pig Butchering' Scams

krebsonsecurity.com

The U.S. government today imposed economic sanctions on Funnul Technology Inc., a Philippines-based company that provides computer infrastructure for hundreds of thousands of websites involved in virtual currency investment scams known as "pig butchering."

#### China-linked hackers exploit Google Calendar in cyberattacks on governments

therecord.media

In a report released this week, analysts at Google attributed the campaign to APT41 — also tracked as Brass Typhoon, Wicked Panda and RedGolf — a long-running state-backed operation. The group's primary targets include foreign governments and organizations in sectors such as logistics, media, automobiles and technology.

### Industry News

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



#### Windows Server emergency update fixes Hyper-V VM freezes, restart issues

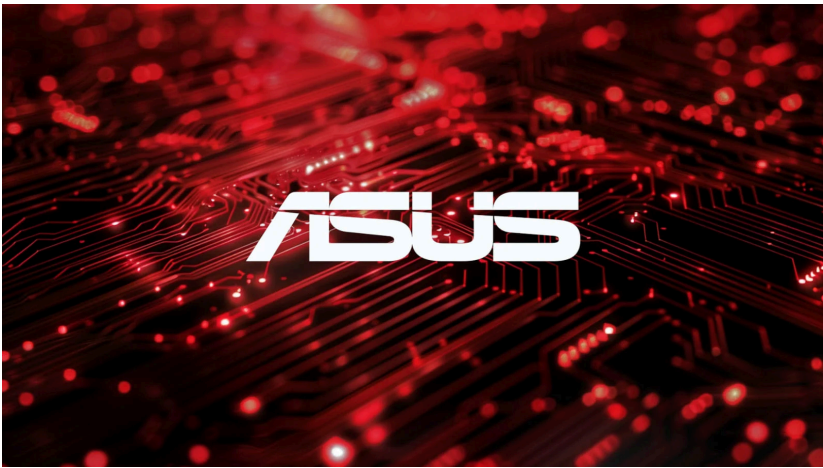
www.bleepingcomputer.com

Microsoft has released an emergency update to address a known issue causing some Hyper-V virtual machines with Windows 10, Windows 11, and Windows Server to freeze or restart unexpectedly.

#### Microsoft Authenticator now warns to export passwords before July cutoff

www.bleepingcomputer.com

The Microsoft Authenticator app is now issuing notifications warning that the password autofill feature is being deprecated in July, suggesting users move to Microsoft Edge instead.



Botnet hacks 9,000+ ASUS routers to add persistent SSH backdoor

www.bleepingcomputer.com

Over 9,000 ASUS routers are compromised by a novel botnet dubbed "AyySSHush" that was also observed targeting SOHO routers from Cisco, D-Link, and Linksys.

Four Senate Democrats call on DHS to reinstate Cyber Safety Review Board membership

cyberscoop.com

The lawmakers say the January purge has left the United States blind on the nature of the historic Salt Typhoon telecommunications breach.

Oregon becomes second state to ban sale of precise geolocation data

therecord.media



Maryland passed a similar bill last year that will take effect in October. Both bills also ban the sale of data belonging to children — Maryland for children under 18, and Oregon for children under 16. Although there is a federal Children’s Online Privacy Protection Act, the two state bills go further than it because the federal law only bans the sale of data for children under age 13...

*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

- |  |   |  |   |
|--|---|--|---|
|  <a href="#">CISA</a> |  <a href="#">CIS/MS-ISAC</a> |  <a href="#">CyberCom</a> |  <a href="#">DHS</a> |
|  <a href="#">DOJ</a>  |  <a href="#">FBI</a>         |  <a href="#">NIST</a>     |  <a href="#">NSA</a> |

External Quick links

- |  |  |  |   |
|--|--|--|---|
|  <a href="#">AIScoop</a>              |  <a href="#">BleepingComputer</a>     |  <a href="#">Cisco Talos Intelligence Group</a> |  <a href="#">CSO Online</a>      |
|  <a href="#">CyberScoop</a>           |  <a href="#">Cybersecurity Dive</a>   |  <a href="#">Cyware</a>                         |  <a href="#">CyberWire</a>       |
|  <a href="#">FedScoop</a>             |  <a href="#">Government Executive</a> |  <a href="#">Government Technology</a>          |  <a href="#">ISACA</a>           |
|  <a href="#">ISSA International</a>   |  <a href="#">Krebs on Security</a>    |  <a href="#">MITRE ATT&amp;CK®</a>              |  <a href="#">NASCIO</a>          |
|  <a href="#">Schneier on Security</a> |  <a href="#">SC Media</a>             |  <a href="#">StateScoop</a>                     |  <a href="#">The Hacker News</a> |
|  <a href="#">The Record</a>           |  |  |   |