



## Daily threat bulletin

21 January 2025

### Vulnerabilities

#### [Microsoft fixes Windows Server 2022 bug breaking device boot](#)

BleepingComputer - 20 January 2025 13:29

Microsoft has fixed a bug that was causing some Windows Server 2022 systems with two or more NUMA nodes to fail to start up. [...]

#### [Details Disclosed for Mercedes-Benz Infotainment Vulnerabilities](#)

SecurityWeek - 20 January 2025 14:17

Kaspersky has disclosed the details of over a dozen vulnerabilities discovered in a Mercedes-Benz MBUX infotainment system.

### Threat actors and malware

#### [PNGPlug Loader Delivers ValleyRAT Malware Through Fake Software Installers](#)

The Hacker News - 21 January 2025 12:15

Cybersecurity researchers are calling attention to a series of cyber attacks that have targeted Chinese-speaking regions like Hong Kong, Taiwan, and Mainland China with a known malware called ValleyRAT.

#### [DoNot Team Linked to New Tanzeem Android Malware Targeting Intelligence Collection](#)

The Hacker News - 20 January 2025 21:23

The Threat actor known as DoNot Team has been linked to a new Android malware as part of highly targeted cyber attacks. The artifacts in question, named Tanzeem (meaning "organization" in Urdu) and Tanzeem Update, were spotted in October and December 2024 by cybersecurity company Cyfirma.

#### [HPE is investigating IntelBroker's claims of the company hack](#)

Security Affairs - 20 January 2025 23:46

HPE is probing claims by the threat actor IntelBroker who is offering to sell alleged stolen source code and data from the company. Last week, the notorious threat actor IntelBroker announced on a popular cybercrime forum the sale of data allegedly stolen from HPE. IntelBroker, known for leaking data from major organizations, made the headlines [...]

#### [Phishing Attacks Are the Most Common Smartphone Security Issue for Consumers](#)



Scottish  
Cyber  
Coordination  
Centre

darkreading - 20 January 2025 15:00

New hands-on testing results show that most devices are unable to catch phishing emails, texts, or calls, leaving users at risk.

## UK related

### [Ransomware attack forces Brit high school to shut doors](#)

The Register - 20 January 2025 13:03

Students have work to complete at home in the meantime A UK high school will have to close for at least two days, today and tomorrow, after becoming the latest public-sector victim of ransomware criminals.