

## Daily Threat Intelligence Briefing

Today's threat briefing contains live links that connect you to the original source articles. You can see the real URL by hovering your mouse over the links and checking that they match the source articles. These links were taken straight from the website of the source article. Tyler Technologies has not checked these sites or links for security.

### News from Wednesday July 23, 2025 (Reported on Thursday July 24, 2025)

#### Government

##### **Trump's AI Plan Sparks Industry Praise and Warnings of Risk**

Read more at [GovInfoSecurity](#)

##### **US Nuclear Agency Hacked in Microsoft SharePoint Frenzy**

Read more at [DarkReading](#)

##### **CISA Orders Urgent Patching After Chinese Hackers Exploit SharePoint Flaws in Live Attacks**

Read more at [TheHackerNews](#)

##### **Department of Education Site Mimicked in Phishing Scheme**

Read more at [DarkReading](#)

##### **CISA warns of hackers exploiting SysAid vulnerabilities in attacks**

Read more at [Bleeping Computer](#)

#### Financial Institutions

##### **Banking Trojan Coyote Abuses Windows UI Automation**

Read more at [DarkReading](#)

##### **Threat Actor Mimo Targets Magento and Docker to Deploy Crypto Miners and Proxyware**

Read more at [TheHackerNews](#)

##### **New Coyote Malware Variant Exploits Windows UI Automation to Steal Banking Credentials**

Read more at [TheHackerNews](#)

#### Healthcare

##### **Feds Warn Health, Other Sectors of Interlock Threats**

Read more at [HealthcareInfoSecurity](#)

##### **Cumberland County Hospital Data Breach Affects Almost 37,000 Individuals**

Read more at [TheHIPAAJournal](#)

##### **New York Surgery Center Pays \$250K to Settle HIPAA Risk Analysis; Breach Notification Violations**

Read more at [TheHIPAAJournal](#)



**News from Wednesday July 23, 2025  
(Reported on Thursday July 24, 2025)**

**Other**

**After \$380M hack, Clorox sues its “service desk” vendor for simply giving out passwords**

Read more at [Arstechnica](#)

**Kerberoasting Detections: A New Approach to a Decade-Old Challenge**

Read more at [TheHackerNews](#)

**Google Launches OSS Rebuild to Expose Malicious Code in Widely Used Open-Source Packages**

Read more at [TheHackerNews](#)

**Lumma Stealer Is Back & Stealthier Than Ever**

Read more at [DarkReading](#)

**Brave blocks Windows Recall from screenshotting your browsing activity**

Read more at [Bleeping Computer](#)

**How to harden your Active Directory against Kerberoasting**

Read more at [Bleeping Computer](#)

**What to know about ToolShell, the SharePoint threat under mass exploitation**

Read more at [Arstechnica](#)

