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 Friday July 17, 2026 through Sunday July 19, 2026
(Reported on Monday July 20, 2026)

Local Government

Government Agencies Falling Victim to Ransomware Daily, Warns Study | Ransomware | Infosecurity Magazine

Research reveals government entities face daily ransomware attacks exploiting their inability to tolerate service disruptions.

In Other News: Cybercrime group claims naval defense manufacturer hack, CrashStealer macOS Malware, CVD Blueprint | Multiple Threats | Security Week

A weekly cybersecurity roundup covering CrashStealer malware on macOS, third-party data exposure affecting Lidl customers, severe operational disruptions from cyberattacks, a WhatsApp-linked AI agent vulnerability, and new guidance for building effective vulnerability disclosure programs.

Financial Institutions

Ernst & Young discloses data breach after support system hack | Supply Chain | BleepingComputer

Big Four accounting firm EY suffered breach through compromised third-party ticketing platform exposing customer data.

Fake Coding Tests Deliver OtterCookie-Aligned Malware Hidden in SVG Flag Images | Social Engineering | The Hacker News

North Korean hackers use fake job interviews with coding tests to deploy credential-stealing malware concealed in SVG images.

Healthcare

Abbott probes two cyber incidents amid extortion claims | Data Breach | BleepingComputer

Medical device manufacturer Abbott faces dual security incidents involving unauthorized system access and extortion threats.

Atrium Health Pays Up to $1.8M to Resolve Pixel Lawsuit | Data Breach | HIPAA Journal

Charlotte hospital system settles class action for $1.8M over unauthorized tracking pixel data exposure on patient portals.

Other

Critical ServiceNow code execution flaw now exploited in attacks | Vulnerability | BleepingComputer

Active exploitation detected of critical remote code execution vulnerability in ServiceNow AI Platform.

Critical NGINX Vulnerability Can Crash Workers and May Allow Remote Code Execution | Vulnerability | The Hacker News

F5 patched a critical heap overflow flaw in NGINX web server allowing unauthenticated attackers to crash services or execute code.

WordPress Core "wp2shell" RCE flaws get public exploits, patch now | Vulnerability | BleepingComputer

Critical remote code execution flaws in WordPress Core now have public exploits available, requiring immediate patching.

SonicWall SMA Zero-Days Exploited Before Disclosure to Gain Root Access | Zero-Day | The Hacker News

Threat actor exploited SonicWall VPN appliance vulnerabilities as zero-days to achieve root access before patches were available.