TIEVA

FULCRUM IT PARTNERS

CYBER NEWS

Stay Secure: The Latest in Cyber News & Updates

THREATS

NEWS

MORE

July 2025 - VOL.4

Cyber News

INTRODUCTION

Welcome

The cyber threat landscape continues to shift—and so do the tactics used by attackers. At TIEVA, we remain committed to helping you stay informed and protected, which is why our cybersecurity experts (not AI) are back with the latest insights that matter.

In this edition, we're unpacking current threat trends, highlighting essential security services, and sharing practical advice to help strengthen your defences. Don't miss our "Quick Wins" section—packed with free, actionable tools you can start using today to boost your cyber resilience.

Cybersecurity doesn't need to be complicated. We're here to make it clear, relevant, and actionable.

Stay vigilant. Stay informed. This is TIEVA Cyber.

TIEVA
FULCRUM IT PARTNERS

Cyber News

NEWS & EMERGING THREATS

News

Echo Chamber AI attack

Bypassing safety filters through clever conversation steering with an alarming success rate of 90% for harmful content using new “Echo Chamber” attacks. Instead of brute-force hacking, this approach slowly undermines AI security by manipulating long-term conversational memory. Businesses using AI chatbots or support systems are vulnerable to these indirect attacks that can generate misinformation or biased responses. Security experts recommend real-time monitoring and behavior analysis to counter these easy-to-execute attacks.

Record-breaking DDoS attack

Cloudflare mitigated the most powerful DDoS attack in history, reaching 7.3 terabits per second – sufficient to deliver 37.4TB of data in just 45 seconds (comparable to 9,350 HD films). The UDP-based assault originated from over 122,000 IPs across 161 nations, with Brazil and Vietnam as primary sources, exploiting outdated protocols and Mirai botnets. Though automated systems repelled the attack, this incident underscores how absolutely essential proper DDoS protection has become for any online operation. As cyber threats continue evolving in both scale and complexity, businesses must prioritise comprehensive security measures including multi-layered defences, constant monitoring, and incident response strategies to protect their digital assets from such potentially catastrophic disruptions.

WordPress Malware

Security researchers have exposed an advanced malware campaign targeting WordPress sites, stealing payment details and credentials through a fake "WordPress Core" plugin. Active since 2023, the malware uses innovative evasion tactics, including live backend systems on infected sites and convincing Cloudflare-branded fake payment screens with multi-language support.

The malware's modular design also hijacks Google Ads, replaces legitimate links, and steals logins. Stolen data is exfiltrated through Telegram channels or disguised as image URLs, making detection particularly challenging.

Emerging Threats

Quishing on the rise

QR code phishing (quishing) is surging, with scams hiding in everyday scans. Always check URLs before opening links.
Quashing alert

Geopolitical Tensions

Pro-Russian hackers target UK infrastructure with disruptive DDoS attacks, threatening critical services and public confidence.
Pro Russian Hacktivists

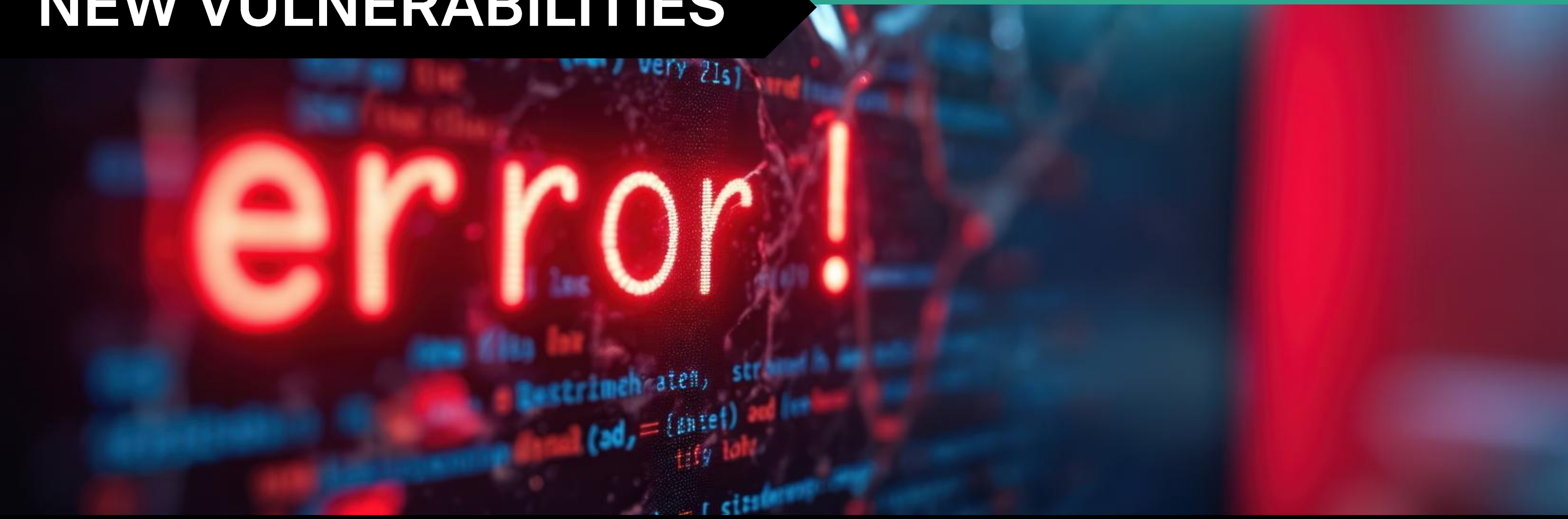
Smart Devices, Smarter Threats: The AI-IoT Risk

Unsecured IoT devices are emerging as prime targets for cyberattacks, exposing networks to data breaches and disruptive incidents worldwide.
AI+IoT supercharging DDoS

TIEVA
FULCRUM IT PARTNERS

Cyber News

NEW VULNERABILITIES



CVEs

CVE Vulnerabilities Update. In this section, we highlight the latest discovered vulnerabilities (CVE) affecting a wide of systems and applications. Stay informed about these critical security threats to ensure you're equipped to protect your environment from emerging risks.

CVE-2025-5777 - Citrix NetScaler Gateway Input Validations Issue

Description: Insecure input handling on the Citrix Gateway enables attackers to send malformed traffic, allowing for unauthorized actions or device compromise. Often chained with other flaws for full exploitation. NIST Link

9.3 Critical

CVE-2025-24472 - FortiOS/FortiProxy Authentication Bypass

Description: This bug allows attackers to bypass authentication on administrative interfaces. By sending a specific request, an attacker can gain super admin privileges on FortiOS and FortiProxy devices without needing valid credentials. NIST Link

9.8 Critical

CVE-2025-32701 -Windows CLFS Use-After-Free

Description: A critical use-after-free vulnerability in Windows CLFS that enables attackers to run code with SYSTEM privileges. Known to be actively exploited by advanced persistent threat (APT) groups. NIST Link

7.8 High

CVE-2025-5419 - Chromium V8 OOB Read/Write

Description: Out-of-bounds read/write vulnerability in the V8 JavaScript engine used in Chromium, Google Chrome, and Microsoft Edge. Can be exploited to escape the browser sandbox. NIST Link

8.8 High

For assistance remediating these or any vulnerabilities please call 0333 043 0333

TIEVA
FULCRUM IT PARTNERS

Cyber News

Case Study

Third-Party Exposure – A Hidden Backdoor into Your Business

In a stark reminder of the risks posed by third-party relationships, a UK financial services firm recently suffered a major data breach—not through its own systems, but via a compromised vendor. The incident highlights how even the strongest cybersecurity defenses can be undermined by weak links in the supply chain.

The Breach: Exploiting a Trusted Partner

The attack began when cybercriminals targeted a small IT services provider used by the firm for cloud storage and data processing. The vendor, lacking robust security controls, fell victim to a phishing attack, granting attackers access to client data—including sensitive financial records. Once inside the vendor's network, the attackers moved laterally, using stolen credentials to infiltrate the firm's systems. They exfiltrated customer data and deployed malware, causing widespread disruption before the breach was detected.

The Impact

Data Loss: Confidential client information, including bank details and transaction histories, was stolen.

Operational Downtime: Critical systems were taken offline for days, delaying customer transactions and regulatory reporting.

Compliance Fallout: The firm faced scrutiny from the Financial Conduct Authority (FCA) and ICO, with potential fines under UK GDPR for failing to ensure third-party security.

Reputational Harm: Clients and investors questioned the firm's due diligence processes, leading to a loss of trust.

Lessons Learned

Strict Vendor Vetting: All third parties must now undergo rigorous security assessments before onboarding, with regular audits to ensure compliance.

Contractual Safeguards: Agreements now include enforceable cybersecurity clauses, requiring vendors to meet strict standards.

Limited Access Controls: Access controls have been revised to adopt a Zero Trust model, ensuring users only access.

Continuous Monitoring: Real-time monitoring tools now track vendor access, flagging unusual activity for immediate review.

TIEVA can help defend against these threats by putting the protections in place - Contact Us Today!

Click here

TIEVA

FULCRUM IT PARTNERS

Cyber News

Managed Detection & Response

Cyber Threats don't sleep, neither does MDR

Cybersecurity threats are no longer a matter of "if," but "when." As attackers grow more sophisticated, traditional security tools alone are no longer enough to keep your business safe. That's where Managed Detection and Response (MDR) comes in.

Unlike AV, which relies on known threat signatures to block malware, MDR takes a proactive approach. Expanding on Endpoint Detection and Response (EDR) a team of experts help continually monitor and detect suspicious behaviours, identifying unknown threats, and responding in real time.

It's not just about identifying threats but actively hunting them down and neutralising them before they cause damage.

According to the UK Government's 2024 Cyber Security Breaches Survey, 50% of medium-sized businesses and 70% of large businesses reported experiencing a cyberattack in the past 12 months. Many of these attacks went undetected for weeks or even months. MDR changes that.

Our MDR solutions are designed to give you peace of mind knowing that your business is protected by a team of experts who are always watching, always ready.

Whether you're a growing SME or a large enterprise, we'll help you stay ahead of evolving threats and keep your business secure.

Reach out to talk about protecting your devices:

0333 043 0333

KEY ADDITIONAL BENEFITS:

24/7 Threat Monitoring & Response: MDR provides round the clock surveillance of your IT environment. When a threat is detected, security experts act immediately often before you even know there's a problem.

Expert-Led Threat Hunting: MDR isn't just automated alerts. It's powered by real people who understand attacker behaviour and can identify subtle signs of compromise that traditional tools miss.

Faster Incident Containment: Time is critical during a breach. MDR services help rapidly contain and mitigate these.

TIEVA
FULCRUM IT PARTNERS

Cyber News

Quick Wins

Qualys. SSL Labs

Qualys SSL Labs

SSL Labs is created by Qualys, its a free online service that analyses the SSL/TLS configuration of your website. Simply put, it checks how secure your website is when it comes to encrypted connections, the kind that protect your data and your customer's privacy.

Think of it like grading your website's security. It grades your SSL certificate and configuration from A+ to F, highlighting any vulnerabilities or outdated settings that could put your business at risk.

How to Use SSL Labs

1. Go to https://www.ssllabs.com/ssltest/
2. Enter your website URL (e.g., yourcompany.com)
3. Click "Submit" and wait a few minutes while the tool runs a deep scan.
4. Review your grade and detailed report.

The Report will Show:

- Whether your SSL certificate is valid and trusted
- If your server supports outdated or insecure protocols
- How well your site resists known attacks like POODLE or Heartbleed
- Recommendations for improving your configuration

A poor SSL configuration can leave your site vulnerable to cyberattacks, damage your reputation,. Even affect your search engine rankings. Regularly testing your site with SSL Labs helps ensure your security is up to date and gives your customers peace of mind.

Cyber News

THOUGHT OF THE MONTH

Security Fatigue and Overengineering - Simplicity Is Sometimes Best

As cyber threats escalate, many organisations are rushing to bolster defences—but in doing so, they risk falling into a dangerous trap: security fatigue and overengineering.

Security fatigue is mental exhaustion from constant security demands. End users face relentless prompts and password rules, while cybersecurity teams drown in alerts, tools, and policies. This overload can obscure real threats and lead to burnout.

Overengineering happens when layered tools and policies create complexity without added value. Examples include tools that don't integrate, confusing policies, and overly strict controls that users bypass—ironically weakening security.

This complexity often results in:

- Slower incident response from alert fatigue
- Low engagement and higher human error
- Cyber team burnout and turnover
- Wasted spend on underused tools

Worse, it gives leadership a false sense of security, while attackers exploit the chaos.

What can be done?

- **Simplify:** Use fewer, well-integrated tools
- **Design for people:** Usable security is stronger security.
- **Automate smartly:** Free your analysts for deeper work.
- **Audit regularly:** Review tool use and overlap
- Support teams: Prioritise wellbeing and clarity

Final Thoughts

More isn't always better. In fact, in cyber security, more can sometimes mean less clarity, less effectiveness, and less resilience. The real challenge now is not how to add more controls, but how to design systems and teams that are sustainable, human-friendly, and fit for purpose.

> The next frontier in cyber security isn't just technological—it's psychological and architectural. If we can reduce fatigue and complexity, we may just build something truly secure.

Contact us

If you'd like to discuss how to strengthen your cybersecurity posture, our experts at TIEVA are here to help.

Contact us today to explore tailored solutions that protect your business from modern cyber threats.

Email TIEVA
hello@tieva.co.uk

Call TIEVA
+44(0) 333 043 0333

Find out more
www.tieva.co.uk

TIEVA

FULCRUM IT PARTNERS