TIEVA

FULCRUM IT PARTNERS

CYBER NEWS

Stay Secure: The Latest in Cyber News & Updates

THREATS

NEWS

MORE

September 2025 - VOL.6

TIEVA

FULCRUM IT PARTNERS

Cyber News

INTRODUCTION

Welcome

Packed with the latest cybersecurity news, insights into emerging threats, free tools you can leverage, and expert analysis you can trust—Cyber News is designed to keep you informed and protected in an ever-evolving digital landscape.

Written by seasoned professionals, each edition brings you practical guidance, industry updates, and actionable tips to help you stay one step ahead. Whether you're an IT leader, security analyst, or simply passionate about digital safety, there's something here for you.

Let’s dive in - This Is TIEVA Cyber

TIEVA
FULCRUM IT PARTNERS

Cyber News

NEWS & EMERGING THREATS

News

Salesloft Drift Supply Chain Attack

A supply chain attack on the Salesloft Drift AI chatbot compromised over 700 organizations' Salesforce instances between August 8–18, 2025. Threat actors, tracked as UNC6395 by Google Threat Intelligence, stole OAuth tokens, gaining trusted access and bypassing security controls.

High-profile victims include Cloudflare, Zscaler, Palo Alto Networks, and PagerDuty, showing strategic targeting of cybersecurity vendors. Stolen data included business contacts, customer support cases, and 104 Cloudflare API tokens. Attackers exfiltrated Salesforce Account, Contact, Case, and Opportunity data, then scanned for more credentials.

Salesloft took Drift offline, paused Salesforce integrations, and is working with Mandiant and Coalition on incident response. Cloudflare's response to the Salesloft Drift incident

TransUnion Credit Bureau Breach Affects 4.4 Million

Major US credit bureau TransUnion confirmed a data breach on July 28, 2025, affecting 4.4 million customers. Hackers accessed names, dates of birth, Social Security numbers, addresses, email addresses, and phone numbers through a compromised third-party application. The breach has been linked to the ShinyHunters cybercrime group. TransUnion discovered the incident within hours but didn't notify customers until around August 28, 2025. The company is offering affected customers two years of free credit monitoring services. Bleeping Computer – TransUnion suffers data breach

ShinyHunters Salesforce Attack Campaign

The notorious ShinyHunters cybercrime group has conducted a coordinated campaign targeting Salesforce environments across multiple major organizations. Using voice phishing (vishing) attacks, the group tricks employees into authorizing malicious OAuth apps that provide access to company Salesforce instances. Confirmed victims include Adidas, Google, Workday, Farmers Insurance, Air France-KLM, Allianz Life, Cisco, and Pandora. ShinyHunters claims to have compromised 91 organizations total, though this figure comes from ransom messages and has not been independently verified. SOCRadar – Salesforce-Related Data Breach Affecting Multiple Companies

Emerging Threats

As recent news illustrates, OAuth is becoming the vector of choice for cybercriminals.

OAuth tokens and integrations let third-party applications connect to business systems like Salesforce, Microsoft 365, and Google Workspace without sharing passwords. Cybercriminals now target these connections because they bypass traditional security defences and can remain active for months undetected.

How SMEs Can Protect Themselves:

- Disable end-user ability to authorise OAuth applications and integrations
- Centralise app approvals through IT or security teams
- Audit connected apps and integrations monthly, removing unused ones
- Set mandatory token expiration periods
- Monitor for unusual data access patterns from connected applications
- Train staff to verify authorisation requests through official channels

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-2025-57819 - FreePBX Authentication Bypass

Description: FreePBX versions 15, 16, and 17 contain critical authentication bypass and SQL injection vulnerabilities allowing unauthenticated remote attackers to gain administrative access and execute arbitrary code. This affects the web-based management interface used to configure telephony systems. NIST Link

10.0 Critical

CVE-2025-7775 - Citrix NetScaler Memory Overflow

Description: Memory overflow vulnerability in NetScaler ADC and Gateway appliances that could allow unauthenticated remote code execution and denial of service. Affects appliances configured as Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA virtual servers. NIST Link

9.2 Critical

CVE-2025-55177 - WhatsApp Device Synchronization

Description: Incomplete authorization of linked device synchronization messages in WhatsApp for iOS and Mac could allow unrelated users to trigger processing of content from arbitrary URLs on target devices. Exploited in combination with Apple vulnerability for sophisticated spyware attacks. NIST Link

8.0 High

CVE-2025-43300 - Apple ImageIO Out-of-Bounds Write

Description: Out-of-bounds write vulnerability in Apple's ImageIO framework affecting iOS, iPadOS, and macOS. Processing malicious image files may result in memory corruption. Used alongside WhatsApp vulnerability in targeted attack campaigns. 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

The rise of Fake Voices & Fake Faces threaten UK Businesses

In 2025, one of the most concerning cyber risks for UK organisations is the rise of AI-generated fake voices and fake faces. These tools, once seen as experimental, are now being weaponised at scale. Criminals are using them to impersonate senior executives, manipulate staff, and bypass traditional verification methods. The impact is already being felt across both the private and public sector.

UK consumers and businesses alike are reporting a sharp increase in AI-driven scams. A recent survey found that a quarter of people in the UK received a deepfake voice call in the past year, and worryingly, 40% of those targeted lost money, with average losses of around £13,000. While personal fraud is growing, the bigger threat lies in corporate compromise. Attackers have begun cloning the voices of CEOs and CFOs to instruct finance teams to transfer large sums. In one global case, a CFO's cloned voice was used to authorise fraudulent transfers totalling £20 million. A scenario that could just as easily play out in the UK.

The corporate risk extends beyond finance. Deepfaked video calls are being used to trick HR and IT teams into handing over sensitive data, while synthetic identities are threatening the reliability of biometric security systems. For UK organisations aiming for ISO27001 compliance or tightening internal controls, this presents a clear and present danger. A single lapse could lead to reputational damage, regulatory fines, and loss of customer trust.

Defending against these threats requires more than technology alone. UK businesses should implement strict verification protocols for high-value transactions, ensuring no decision is made solely on the basis of a phone call or video conference. Awareness training is equally important: staff must know how to spot red flags, such as unusual urgency or unexpected requests from senior leaders. Technical defences like deepfake detection tools and liveness checks for biometric systems are beginning to emerge, but for now, vigilance and process remain the strongest line of defence.

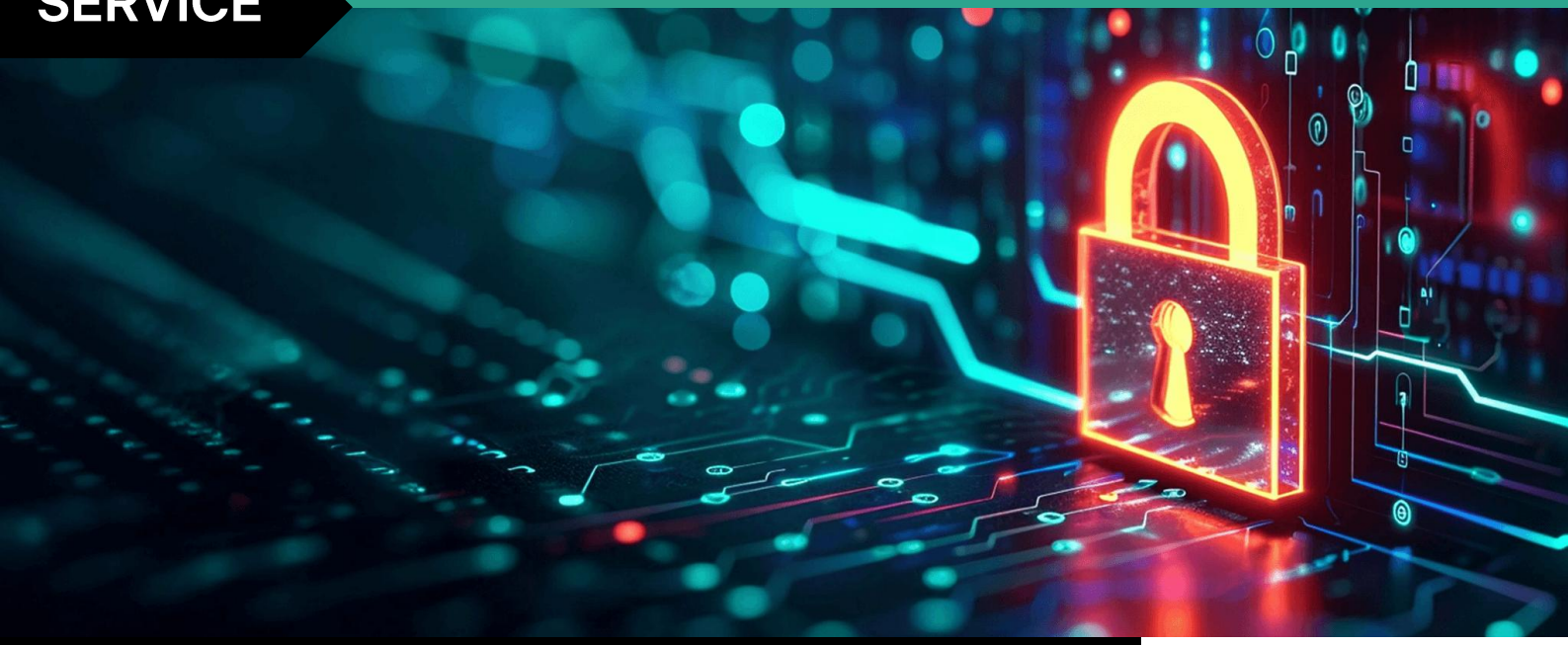
The message for UK organisations is clear: fake voices and faces are not a distant risk. They are here and now!
By strengthening verification processes and fostering a culture of skepticism towards unexpected digital communications, businesses can stay ahead of a fast-evolving cyber threat.

TIEVA

FULCRUM IT PARTNERS

Cyber News

SERVICE



Safeguard Your Data with Veeam:
Backup as a Service, Simplified

Backups are essential to any effective cyber security strategy. With threats like ransomware and data breaches on the rise, organisations must ensure their critical data is protected and recoverable.

Cyber attacks often aim to encrypt or destroy valuable information, causing disruption and financial loss. A secure backup allows businesses to restore systems quickly, reducing downtime and maintaining continuity.

However, backups must be properly secured, encrypted, regularly tested, and stored separately from live systems to prevent them from being compromised.

Ultimately, backups are not just about recovery. They're about resilience. Solutions like TIEVA's Backup as a Service offer scalable, automated protection, helping organisations stay secure

TIEVA's fully managed Backup as a Service (BaaS) provides a complete data protection solution that is designed, deployed and managed according to the business's availability goals.

Backups of customer data are taken from the production systems and transferred to a local back up repository allowing for rapid recovery. For additional resilience and as per best practice, backup data is then transferred to a secure offsite location.

All fully monitored round the clock!

Reach out to talk about BaaS:
0333 043 0333

KEY ADDITIONAL BENEFITS:

Peace of mind: Designed, deployed and managed by data protection experts with many years of backup and recovery experience.

Rapid Recovery: Advanced recovery features to ensure quick recovery of critical data and workloads with minimal data loss.

Ransomware Protection: Options for data immutability to ensure data cannot be deleted, changed or destroyed.

TIEVA
FULCRUM IT PARTNERS

Cyber News

QUICK WINS

What is Shodan and how can it help you?

Shodan is a search engine that scans and indexes internet connected devices, everything from servers and webcams to routers and industrial control systems. Unlike Google, which indexes websites, Shodan indexes the metadata of devices: IP addresses, open ports, services running, and even software versions.

This makes it an invaluable tool for cybersecurity to help:

- Discover exposed devices on your network
- Identify outdated or vulnerable services
- Monitor your attack surface in real time

How to Use Shodan

Getting started with Shodan is easy:

- Visit https://www.shodan.io
- In the search bar, enter your public IP address, domain name, or keywords like Apache, RDP, or camera
- Review the results to see what services are exposed and how they're configured

You can also use filters like:

- country: GB to narrow results to the UK
- port: 22 to find devices with SSH exposed
- org: "Your Company Name" to see assets associated with your organisation

Real World Examples

Here are a few eye-opening cases where Shodan has made a real impact. In 2018, researchers used Shodan to discover thousands of unsecured medical devices, including MRI machines and patient monitors, exposed to the internet. Many were running outdated software and lacked proper authentication a major privacy and safety risk.

Security analysts have found internet connected baby monitors and webcams with default passwords using Shodan. These devices were accessible to anyone online, allowing unauthorised viewing and control.

Why it Matters

Shodan can reveal if your business has devices exposed to the internet that shouldn't be, like an unsecured printer, a misconfigured firewall, or a forgotten test server. These are often the entry points attackers look for.

- By regularly checking Shodan, we can:
- Spot vulnerabilities before attackers do
- Ensure your network is properly segmented
- Validate firewall and VPN configurations
- Keep your cloud and on-prem assets secure

Need help interpreting your results? Contact us for further information and assistance

TIEVA

FULCRUM IT PARTNERS

Cyber News

THOUGHT OF THE MONTH

Beyond the Firewall: August's Surge in Cyber Threats

August highlighted the growing scale and persistence of cyber threats facing UK businesses. The UK is now the third most targeted country for malware, with over 100 million attacks in just three months, a sharp rise driven by increasingly sophisticated threat actors exploiting a wider range of vulnerabilities. From convincing HMRC-themed phishing emails to ransomware delivered via trusted platforms, attackers are combining technical skill with social engineering to bypass traditional defences.

Remote working tools and digital dependencies remain a major risk, with researchers warning of weak points in VPNs and cloud-based apps that are often overlooked or misconfigured. These gaps are being exploited in broader campaigns, including those run by ransomware groups like Akira.

August also brought several high-profile breaches exposing the fragility of third-party relationships. Chanel and Pandora confirmed customer data leaks via external systems, while a CRM platform linked to Cisco was compromised through targeted voice-based phishing (vishing). These incidents underscore a critical lesson: cybersecurity isn't just about securing your own network, it's about knowing who else has access to your data and how well they protect it.

What can be done?

- Audit VPN usage, apply strict access policies, enforce multi-factor authentication, and monitor for unusual login patterns especially from third-party vendors.
- Deliver regular, role-specific training on phishing, vishing, and social engineering tactics. Make sure employees know how to spot and report suspicious activity.
- Don't wait for a breach to test resilience. Run tabletop exercises, review backup and recovery processes, and ensure clear roles and responsibilities in the event of an incident.

Final Thoughts

As the volume and complexity of attacks continue to rise, the conversation needs to shift, from short-term fixes to long-term resilience. It's no longer enough to focus on individual incidents or isolated defences. Cybersecurity should be seen as an ongoing discipline, embedded into every level of the organisation from boardroom strategy to day-to-day operations. Building trust, securing data, and staying ahead of threats isn't just an IT concern - it's a business priority.

Whether it's supply chain risk, ransomware resilience, or shifting compliance needs, TIEVA is ready to help.

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