TIEVA

FULCRUM IT PARTNERS

CYBER NEWS

Stay Secure: The Latest in Cyber News & Updates

THREATS

NEWS

MORE

June 2025 - VOL.3

TIEVA
FULCRUM IT PARTNERS

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.

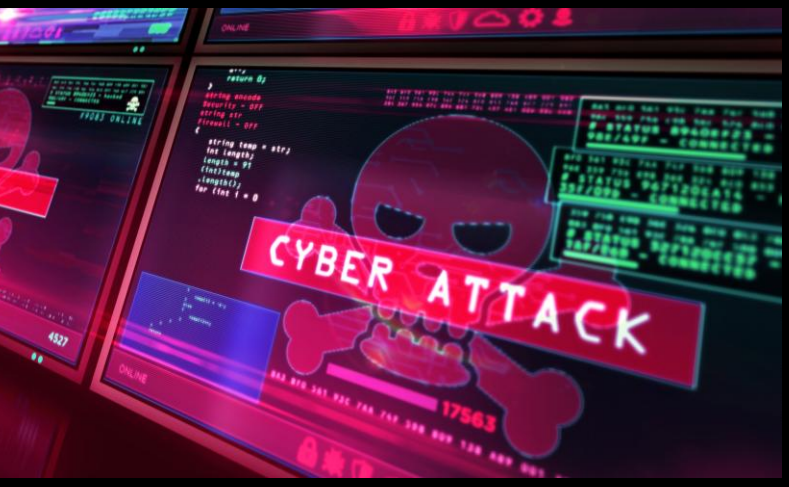
Cybersecurity doesn't need to be complicated. We're here to make it clear, relevant, and actionable.

Stay vigilant. Stay informed. This is TIEVA Cyber.

TIEVA
FULCRUM IT PARTNERS

Cyber News

NEWS & EMERGING THREATS



News

Scattered Spider hacker group claimed they had long-term access to **Co-op's** network before detection. This stealthy infiltration could have been achieved through a successful phishing email, unpatched software vulnerabilities, or stolen credentials purchased via dark web leaks. They exfiltrated customer data (including names, addresses, and phone numbers) before attempting to deploy ransomware. However, Co-op's IT team detected the attack mid-execution and "pulled the plug" a defensive takedown, successfully stopping the full encryption of their systems, which helped them recover within days.

Scattered Spider also targeted **Harrods**, this time using spear-phishing emails sent to senior staff and IT personnel. The objective was to install malware that would provide long-term access to critical internal systems. Harrods' IT team detected unusual outbound traffic shortly after the malware activated and immediately launched a defensive protocol a "kill switch" to contain the breach. No systems were encrypted, no data was exfiltrated, and the attackers were ejected before causing any lasting damage.

Scattered Spider once again gained access to **M&S** systems via a third-party contractor, likely by harvesting login credentials through social engineering. Once inside, the attackers moved laterally, elevating privileges to reach critical systems by exploiting weak points in Multi-Factor Authentication (MFA). They quietly exfiltrated customer data over several weeks, including names, email addresses, dates of birth, and purchase history. The objective was to cripple logistics and online retail operations. At the ransomware deployment phase, M&S security systems triggered internal alarms, prompting the IT team to isolate affected infrastructure, which limited the spread of encryption. Despite this, core services were disrupted, affecting online orders and resulting in an estimated £300+ million in lost profits.

Emerging Threats

Russian State-Sponsored Cyber Espionage
Russian intelligence groups, notably APT28 (Fancy Bear), ramped up cyber-espionage targeting logistics and tech firms aiding Ukraine. NSA-Russian threat

Rise of New Ransomware Groups
New groups like FunkSec and Kairos are leveraging AI to hit sectors like healthcare and manufacturing. Europol seized 300 servers and €3.5M in a global crackdown. Dragos IR Analysis

Supply Chain Vulnerabilities
Cyberattacks on UK retailers disrupted small suppliers and revealed deep flaws in vendor security. Experts call for stronger safeguards across supply chains. WeForum

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-2025-22247

An insecure file handling vulnerability in VMware Tools was privately reported to VMware. Updates are available to remediate this vulnerability in the affected VMware products.

6.1 Medium

CVE-2025-32701 / CVE-2025-32706

High-severity vulnerability in the Windows Common Log File System (CLFS) driver, disclosed by Microsoft on May 13, 2025. This flaw allows an authenticated local attacker to elevate privileges to SYSTEM level by exploiting improper input validation within the CLFS driver.

7.5 High

CVE-2025-32709

Critical vulnerability in Microsoft's Windows Ancillary Function Driver for WinSock (AFD.sys), identified as a use-after-free flaw (Type of Memory Control Bug). This vulnerability allows authenticated local attackers to escalate privileges to SYSTEM level, posing a significant security risk.

7.8 High

CVE-2025-3935

Connectwise ScreenConnect versions 25.2.3 and earlier versions may be susceptible to a ViewState code injection attack. ASP.NET Web Forms use ViewState to preserve page and control state.

8.1 High

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

TIEVA

FULCRUM IT PARTNERS

Cyber News

Case Study

Social Engineering – It's On The Phone Too

In a sobering example of the power of social engineering, a UK-based firm—was recently the target of a cyber attack that led to a widespread ransomware outbreak. The attacker exploited human trust rather than technical flaws, gaining access to internal systems

The breach began when an attacker, impersonating an employee, contacted the internal IT support team by phone. Claiming to have been locked out of their account during a time-sensitive task, the individual used urgent language and convincing insider knowledge to manipulate the IT team into resetting their account credentials. Trusting they were helping a legitimate staff member, the IT team reset the password and communicated the new details over the phone

Once inside the network, the attacker swiftly deployed ransomware, encrypting sensitive financial data and critical operational systems.

The Impact

1. **Business Disruption:** Online services and internal operations were severely affected, disrupting client transactions and investment activities.
2. **Financial Cost:** The total financial impact was great, covering forensic analysis, system recovery, lost business, and legal costs.
3. **Regulatory Consequences:** The breach must be reported to the Financial Conduct Authority (FCA) and the Information Commissioner's Office (ICO), prompting compliance reviews under GDPR and sector regulations.
4. **Reputational Damage:** The business experienced a decline in client confidence and faced difficult questions from investors and partners regarding their cyber resilience.

Lessons Learned

1. **Robust Identity Verification :** All requests for password resets must undergo strict multi-factor verification—no exceptions.
2. **Ongoing Security Training :** Staff across all departments, particularly those in IT and customer service, now receive regular training to detect and respond to social engineering tactics.
3. **Zero Trust Approach:** Access controls have been revised to adopt a Zero Trust model, ensuring users only access.

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

Click here

TIEVA
FULCRUM IT PARTNERS

Cyber News

Email Security

Why Email Security should be a top priority

Email remains the backbone of business communication—but it's also one of the most targeted vectors for cyberattacks. In recent years, we've seen a sharp rise in phishing scams, business email compromise (BEC), and ransomware campaigns,
all of which often begin with a single malicious email.

Despite advancements in cybersecurity, attackers continue to evolve their tactics, using increasingly sophisticated methods to bypass traditional filters and deceive users. According to gov.uk 84% of businesses in 2024 were breached or attacked due to a Phishing email. Without proper email security in place, your business could be one click away from a costly breach.

Email security isn't just about blocking spam—it's about safeguarding your data, protecting your people, and maintaining trust with your clients.
A comprehensive solution inspects every message, attachment, and link, using AI and threat intelligence to detect and neutralize threats in real time.
At TIEVA, we believe prevention is better than cure. That's why we offer advanced email security solutions tailored to your business needs. Whether you're a small team or a growing enterprise, we'll help you stay one step ahead of cybercriminals.

Reach out to talk Email Security: 0333 043 0333

KEY ADDITIONAL BENEFITS:

Protection Against Phishing: Stops deceptive emails designed to steal credentials or trick users into harmful actions.

Data Loss Prevention (DLP): Email security can also help prevent accidental or intentional data leaks. DLP features monitor outgoing messages for sensitive information, ensuring compliance with data protection regulations.

Malware & Ransomware Defence: Blocks malicious attachments and links before they reach your inbox.

TIEVA

FULCRUM IT PARTNERS

Cyber News

Quick Wins

Microsoft Active Directory

Free Active Directory Security Assessment Tools:

Purple Knight & Ping Castle Active Directory (AD) is the backbone of most business networks, but security experts consistently identify it as a critical vulnerability. It holds the "keys to the kingdom" and successful AD takeover can give attackers access to all domain-joined machines. Independent security professionals emphasize the importance of regular AD assessments.

Purple Knight is Semperis' free AD security assessment tool that scans for over 150 security indicators, including Kerberoasting vulnerabilities, weak password policies, and dangerous privilege escalations. It provides a clear risk score and prioritized remediation guidance.

Ping Castle offers detailed AD security analysis with a focus on trust relationships, delegation issues, and attack path identification. It generates easy-to-read reports that highlight your most critical vulnerabilities first.

How to Use These Tools

Purple Knight:

- Download from Semperis' website (registration required).
- Run on a domain controller or member server with appropriate permissions.
- Review the generated report focusing on "Critical" and "High" risk items.
- Address identified misconfigurations using the provided remediation steps.

Ping Castle:

- Download the standalone executable from pingcastle.com.
- Execute with domain admin privileges.
- Analyse the HTML report, starting with items marked as "Critical".
- Implement suggested security improvements.

Quick Wins You Can Implement Today

Both tools will identify common AD-internal issues like unused service accounts, overprivileged users, weak password policies, and dangerous trust relationships—problems your IT team can often resolve within hours.

For more complex vulnerabilities like advanced persistence techniques or enterprise-wide trust relationship issues, our Managed Detection and Response service can provide ongoing monitoring and expert remediation support.

TIEVA

FULCRUM IT PARTNERS

Cyber News

THOUGHT OF THE MONTH

Cyber Attacks Happen – Are You Truly Prepared?

In today's digital landscape, cyber threats are a constant reality. From ransomware to supply chain attacks, no organisation is immune. While strong cybersecurity controls help, risk can never be fully eliminated—making resilience just as critical as prevention.
This is where Business Continuity Planning (BCP) becomes essential. In a cyber crisis, there's no time to waste. Clear communication, fast decision-making, and minimal downtime are key. But a plan alone isn't enough—it must be tested and practiced.

Enter tabletop exercises: structured simulations that help organisations rehearse their cyber response. These exercises bring together key teams—IT, legal, HR, communications, leadership—to walk through realistic scenarios, clarify roles, and test response plans under pressure.

Tabletops surface critical gaps: unclear decision-making authority, slow impact assessment, communication breakdowns, or unrealistic recovery assumptions. They highlight weaknesses before they become failures..

The takeaway?

Resilience is a muscle. It's built through practice, not theory. Organisations that respond well to incidents don't wing it—they prepare, test, and learn.

Ask yourself: When was your last BCP review? Have your leaders rehearsed a major cyber event? Could you recover quickly and protect your reputation?

Final Thought:

Cyber resilience isn't about being flawless. It's about being ready.

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