TIEVA

FULCRUM IT PARTNERS

CYBER NEWS

Stay Secure: The Latest in Cyber News & Updates

THREATS

NEWS

MORE

May 2025 - VOL.2

TIEVA

FULCRUM IT PARTNERS

Cyber News

INTRODUCTION

Welcome

The cyber threat landscape continues to evolve—and so do the tactics used by attackers. At TIEVA, we're 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 diving into current threat trends, spotlighting critical security services, and sharing practical tips to strengthen your defences. Don’t forget to check out our “Quick Wins” section for powerful free tools you can start using today to boost your cyber resilience.

We’re here to make cybersecurity clear, relevant, and actionable.

Stay vigilant, stay informed—this is TIEVA Cyber.

TIEVA

FULCRUM IT PARTNERS

Cyber News

NEWS & EMERGING THREATS

News

Marks & Spencer recently suffered a cyberattack that disrupted its online services. The attack caused delays in home deliveries and led to the suspension of the click-and-collect service, a popular feature for many customers. Although the company has reassured customers that no personal data was compromised, the incident brings to light the vulnerabilities in cybersecurity within the retail sector. As online shopping becomes an ever more integral part of daily life, this attack serves as a reminder of the growing risks retailers face in protecting their digital operations.
M&S says 'cyber incident' hitting click and collect orders - BBC News

Bristol-based startup KETS Quantum Security has developed a quantum encryption prototype now being tested by BT. The technology aims to future-proof communications against quantum computing threats.
UK startup KETS delivers miniaturised quantum security for telecom networks | Capacity Media

Verizon's 2025 Data Breach Investigations Report (DBIR) reveals a significant uptick in cyberattacks, with a notable increase in the growing sophistication of cybercriminal tactics, including advanced phishing schemes and supply chain attacks. These evolving threats underscore the need for organizations to adopt more robust cybersecurity measures and to remain vigilant against emerging risks.

Verizon's 2025 DBIR report finds spike in cyberattacks, complexity in threat landscape amid rising supply chain threats - Industrial Cyber

Emerging Threats

Quantum Computing and its Threat to Encryption Quantum computing, though still developing, threatens to break current encryption methods that protect sensitive data, including government, banking, and private communications. This has triggered a global push to create encryption that can withstand quantum attacks. Cybersecurity experts are urging businesses to start preparing for a post-quantum world by adopting quantum-resistant encryption. However, the shift is costly and complex, leaving many organizations unprepared for the potential disruption.

AI and Quantum: A Double Threat AI and quantum computing together could be a dangerous combo. AI can speed up the exploitation of weaknesses created by quantum computing, allowing cybercriminals to break through encryption faster than ever. This could completely change the landscape of cybercrime, making it easier for attackers to access sensitive data. As these technologies evolve, it's clear that traditional cybersecurity won't be enough.

TIEVA
FULCRUM IT PARTNERS

Cyber News

Seen by TIEVA

The Hidden Danger in Your Search Results

"I just searched for it and clicked the first link."

This seemingly innocent explanation came from a client's IT manager after discovering malware had spread to several systems across their network. The source? An employee who needed specialized software for a time-sensitive project and, unable to wait for IT approval, took the initiative to find and download it themselves.

What makes this incident particularly concerning isn't that someone ignored policy and procedure, it's that they followed what most of us would consider perfectly normal behaviour. They used a reputable search engine, clicked a top result, and downloaded what appeared to be legitimate software from a professional-looking website.

This is the evolving reality of SEO poisoning attacks. Unlike traditional phishing that arrives uninvited in your inbox, SEO poisoning exploits our active search behaviour and trust in search engine rankings. Attackers strategically manipulate search results to position malicious websites high in rankings for popular software searches, creating a perfect trap for even security-conscious users.

Breaking the Pattern

Traditional defences focus heavily on email security and user training to spot suspicious messages. But how do you protect against threats that users actively seek out, believing they're making safe choices?:

Our team recommends a different approach:

Create Clear Software Procurement Channels

Develop an easily accessible internal software catalogue with straightforward request processes. When legitimate needs can be met quickly through official channels, employees are less likely to resort to searching online.

Deploy Context-Aware Security Controls

Modern security solutions can analyse web content beyond simple blocklists, identifying suspicious patterns even on previously unknown websites. These tools can detect when a supposed "download" button leads to unexpected executable types or when websites exhibit known deception patterns.

Implement Runtime Application Protection

Since prevention isn't always possible, ensure your endpoint protection can contain damage even when malicious software executes. Solutions that monitor behaviour patterns can quickly identify and isolate systems exhibiting signs of compromise.

The reality is that expecting perfect human judgment in every online interaction is unrealistic. Even with training, the sophistication of these attacks continues to increase, with fake sites including authentic logos, privacy policies, and even user reviews.

At TIEVA, we're seeing SEO poisoning attacks targeting business software increasing at an alarming rate. We can help assess your current vulnerability to these threats and implement practical protections that work with and not against your employees' natural workflows.

This article is part of our ongoing security awareness series, helping businesses stay ahead of emerging threats.

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-2025-22457

Ivanti Connect Secure, Policy Secure, and ZTA Gateways are impacted by a stack-based buffer overflow vulnerability. An unauthenticated remote attacker may leverage this flaw to trigger remote code execution on the affected device. This issue affects Connect Secure prior to version 22.7R2.6, Policy Secure prior to 22.7R1.4, and ZTA Gateways prior to 22.8R2.2.

9.0 Critical

NVD - CVE-2025-22457

CVE-2025-3102

OttoKit (formerly SureTriggers) for WordPress is impacted by an authorization bypass vulnerability. An unauthenticated remote attacker may exploit this flaw to create administrator accounts and gain full control of the affected website. This issue affects all plugin versions up to and including 1.0.78 when the plugin is activated but not configured with an API key. The vulnerability has been addressed in version 1.0.79.

8.1 HIGH

NVD - CVE-2025-3102

CVE-2024-0132

NVIDIA Container Toolkit is affected by an incomplete patch for a previously fixed TOCTOU vulnerability, which may allow container escape and host-level code execution. Tracked as CVE-2025-23359 (CVSS 9.0), the flaw affects version 1.17.4 when allow-cuda-compat-libs-from-container is enabled. An attacker with code execution inside a container could exploit this issue to run commands on the host. The vulnerability has been addressed in version 1.17.4.

8.1 HIGH

NVD - CVE-2024-0132

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

TIEVA

FULCRUM IT PARTNERS

Cyber News

Case Study

Unauthorized Access Through an Outdated VPN Appliance

A company relied heavily on a legacy VPN appliance to support remote work for staff across multiple offices. While it served its purpose during COVID and the shift to remote work in 2021, the system had not been updated in over a year due to perceived downtime risks and lack of internal patch management processes.

Unbeknownst to the internal IT team, a critical vulnerability had been disclosed six months earlier—one that allowed remote code execution (RCE) with no authentication required. Exploit code was publicly available, and threat actors were actively scanning the internet for unpatched devices.

The Attack

An attacker discovered the firm's exposed VPN endpoint using automated scanning tools. Within hours, they exploited the vulnerability and gained full access to the device's administrative interface. From there, they were able to:

- **Establish persistent remote access**
- **Move laterally into internal systems**

The Impact

1. **Internal disruption:** Remote access for all staff had to be disabled temporarily.
2. **Data exposure:** Deploy Several confidential client files were accessed.
3. **Incident response:** Required external forensic support and full credential resets.
4. **Cost :** Significant IT remediation and reputational risk.

The Key Take-Aways

- Patch management is not optional. Even appliances with limited user interaction can pose major risks if left unpatched.
- Perimeter systems need continuous monitoring. Externally facing systems should be scanned, monitored, and risk-assessed regularly.
- Zero Trust could have minimized the blast radius. Segmented access and strict authentication would have slowed lateral movement.
- Vulnerability disclosures should trigger immediate review. Organizations must have a process to respond to critical CVEs

TIEVA can help defend against these threats with Patching, Scanning, Monitoring and so much more. – Contact Us Today!

Click here

TIEVA
FULCRUM IT PARTNERS

Cyber News

Zero Trust – Myth or Legend?

Busting the Myths of Zero Trust: Why It's Essential for Your Business

"Never trust, always verify" – it's the core principle of Zero Trust, but the concept is often misunderstood. Some see it as a rigid, all-or-nothing security model, or think it's just about firewalls and multi-factor authentication. The truth? Zero Trust is a flexible, strategic framework that adapts to your business and protects against today's most sophisticated cyber threats.

At TIEVA, we believe it's time to bust the myths. Zero Trust isn't about distrusting your people — it's about securing your data, wherever it lives, through continuous verification, least privilege access, and strong identity management. Microsoft's Zero Trust model gives organisations a clear path, but many don't know where to start.... That's where we come in.

At TIEVA, we are committed to helping you secure your assets. Reach out today to take advantage of a free external vulnerability scan and gain valuable insight into your business's external threat exposure.

Our expert team at TIEVA can carry out a comprehensive Zero Trust gap analysis, benchmarking your current security posture against Microsoft's six key pillars.

You'll get a clear, actionable roadmap tailored to your environment — not a one-size-fits-all solution. Zero Trust isn't a buzzword — it's a business imperative. Let's work together to close the gaps and build a more resilient, future-ready security foundation.

KEY ADDITIONAL BENEFITS:

Stronger breach containment - Limits lateral movement across your network, reducing the impact of compromised accounts or devices.

Improved compliance posture - Aligns with key regulations like ISO27001, CE+, and GDPR through continuous access controls and activity monitoring.

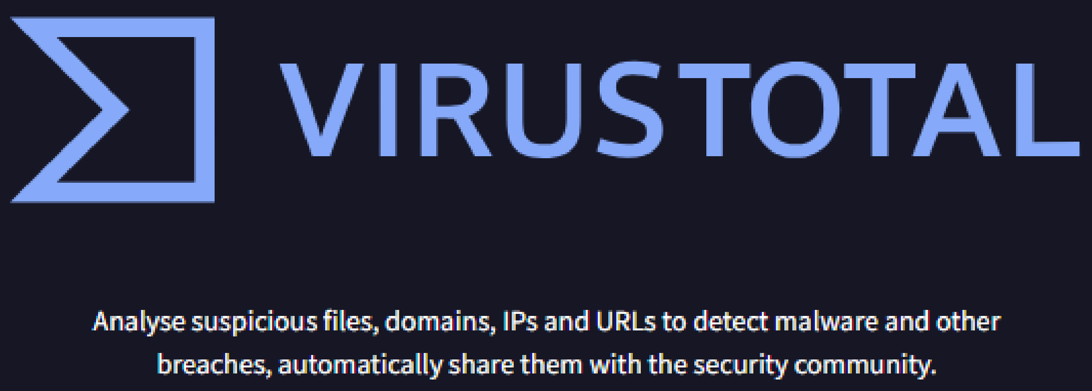
Better user experience: Enables secure, seamless access with modern tools like single sign-on (SSO) and conditional access policies.

Reach out for your GAP analysis Click here

TIEVA
FULCRUM IT PARTNERS

Cyber News

QUICK WIN



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

VirusTotal

VirusTotal is a online service created by Hispasec Sistemas in 2004, purchased by Google in 2012.It's a service that inspects items with over 70 scanners and multiple URL & domain blocking services. It utilises a vast range of tools to extract signals from studied content.
This and the mass of VirtualTotal Community members all sharing notes with each other will help provide you with the necessary information to make an informed decision about how to act upon the items submitted.
VirusTotal is a powerful ally in the fight against cyber threats, it provides quick wins that bolster your cybersecurity efforts. Incorporating VirusTotal into your investigative process before clicking that suspicious link or opening that suspicious file and help safeguard yourself.

How to Use VirusTotal

1. **Visit the website** – Go to virustotal.com.

2. **Upload your file, URL, IP or Domain**– The site will inspect the items **provided.**

3. **Review the results** – VirusTotal will identify whether a file or URL is malicious, but also provides detailed detection labels and additional information, such as specific malware types, targeted brands in phishing sites, and botnet associations.

4. **Take action** – Taking into consideration the reviewed results you can now make an informed decision on what action you wish to perform with the file or URL that raised concerns.

TIEVA
FULCRUM IT PARTNERS

Cyber News

THOUGHT OF THE MONTH

In Cyber Security – Free Apps and Giveaway, aren't always truly free

In a time where apps promise premium features “for free,” websites offer giveaways at the cost of a few clicks, and public Wi-Fi lures us in with convenience, it’s easy to forget the hidden costs. Free almost always comes with a catch.

The Hidden Price of “Free”

The moment you download a free app, click on a suspicious link, or connect to unsecured Wi-Fi, you might unknowingly be paying with your most valuable asset: your data. Here’s how that “free lunch” might actually cost you:

1. Free Apps, Expensive Data

Many “free” mobile apps aren’t really free. Sure, they don’t charge you money—but they often collect a staggering amount of personal data: contacts, location, browsing history, even keystrokes. That data can be sold to third parties or used to build detailed user profiles for targeted advertising or even identity theft.

2. Public Wi-Fi Traps

We’ve all done it— connected to free Wi-Fi at the airport or café. But without proper encryption, attackers can easily intercept your data, using simple tools.

3. Phishing in Disguise

Sometimes that too-good-to-be-true offer really is. Free gift cards, software, or prize notifications often come with a malicious twist—phishing scams designed to trick you into handing over credentials, banking info, or downloading malware.

How to Protect Yourself

1. **Be Skeptical** – If it seems too good to be true, it probably is.
2. **Check App Permissions** – Don’t give apps access to data they don’t need. Why would a flashlight app need your contacts?
3. **Use VPNs on Public Wi-Fi** – They encrypt your connection, making it harder for hackers to snoop.
4. **Antivirus Software** – Good security software can flag malicious downloads and phishing attempts.
5. **Keep Everything Updated** – Patches fix vulnerabilities that attackers exploit.
6. **Read the Privacy Policy (Yes, really)** – Or at least skim it to see what kind of data is being collected and why.

Final Thoughts

Cybersecurity is a constant trade-off between convenience and caution. The next time you’re offered something for free online, pause and ask yourself: What am I really giving in return?

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