DIGITAL DEFENSE DIGEST

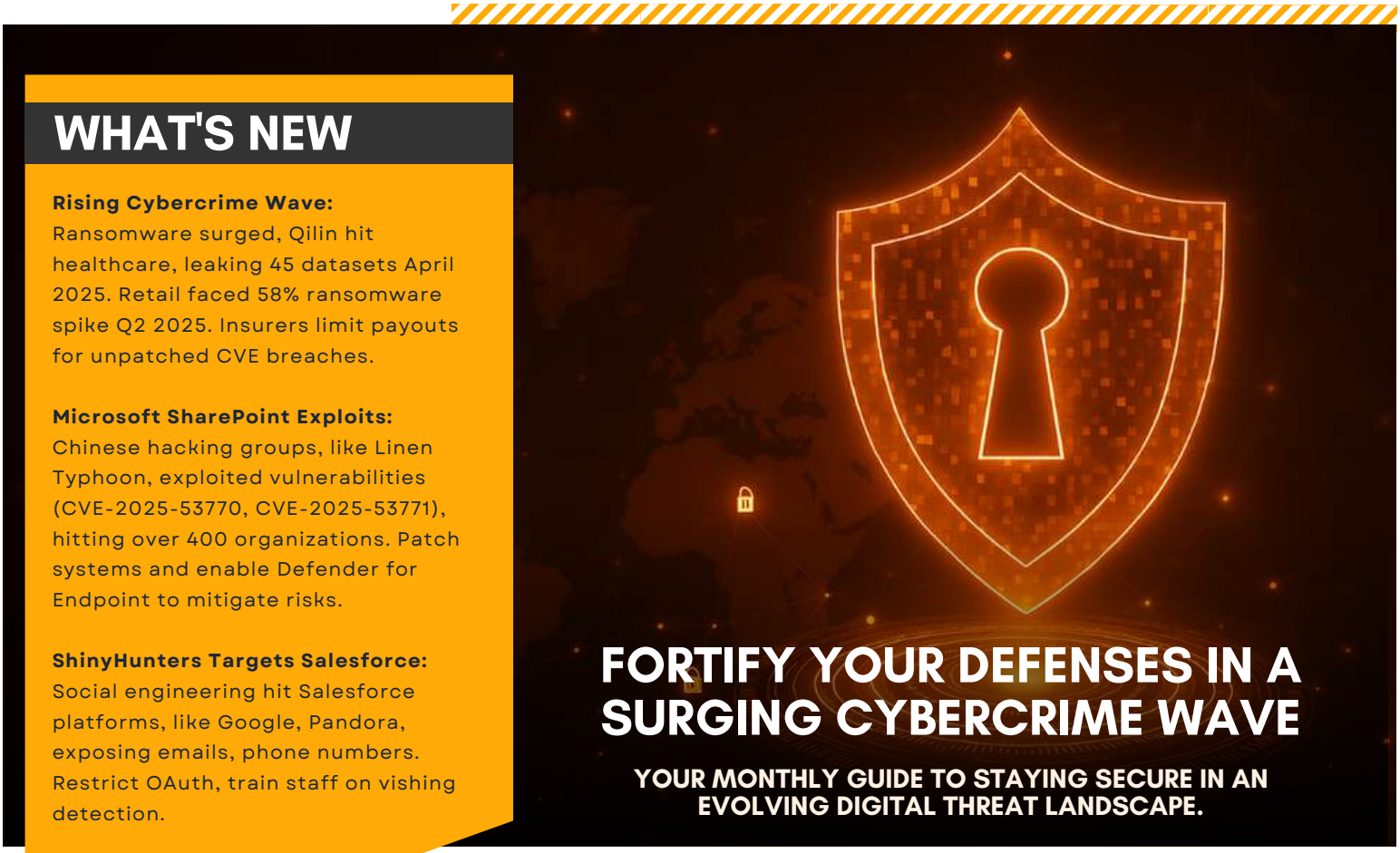
Insider Tips To Make Your Business Run Faster, Easier And More Profitably

WHAT'S NEW

Rising Cybercrime Wave: Ransomware surged, Qilin hit healthcare, leaking 45 datasets April 2025. Retail faced 58% ransomware spike Q2 2025. Insurers limit payouts for unpatched CVE breaches.

Microsoft SharePoint Exploits: Chinese hacking groups, like Linen Typhoon, exploited vulnerabilities (CVE-2025-53770, CVE-2025-53771), hitting over 400 organizations. Patch systems and enable Defender for Endpoint to mitigate risks.

ShinyHunters Targets Salesforce: Social engineering hit Salesforce platforms, like Google, Pandora, exposing emails, phone numbers. Restrict OAuth, train staff on vishing detection.



FORTIFY YOUR DEFENSES IN A SURGING CYBERCRIME WAVE

YOUR MONTHLY GUIDE TO STAYING SECURE IN AN EVOLVING DIGITAL THREAT LANDSCAPE.

This monthly publication is provided by Black Belt Secure

OUR MISSION:

To empower businesses of all sizes with the knowledge and tools they need to thrive in today's increasingly complex cyber threat landscape. We are dedicated to providing cutting-edge cybersecurity solutions and expert guidance to help our clients

Welcome to the September edition of Digital Defense Digest! This month, we tackle rising ransomware threats, AI-driven phishing scams, and new insurance policies pushing for proactive patching. With cybercrime surging—ransomware alone hit 58% more retailers in Q2 2025—our actionable insights will keep you ahead. Let's secure your digital world!

What's Happening in Cybersecurity

1 Qilin Ransomware Targets Healthcare

The Qilin ransomware group intensified its campaign in August 2025, focusing heavily on healthcare organizations, with 45 significant data leaks reported in April 2025 alone. Leveraging the sophisticated NETXLOADER malware, attackers infiltrated systems to steal highly sensitive patient data, including medical records and personal identifiers, demanding ransoms in the multimillion-dollar range. The healthcare sector's reliance on outdated, legacy systems—often running unsupported software—creates critical vulnerabilities that amplify the risk of successful breaches. These systems, still prevalent in many hospitals and clinics, lack modern security features, making them prime targets for ransomware. To combat this, organizations should prioritize deploying immutable backups, which cannot be altered or deleted by attackers, ensuring data recovery without paying ransoms.

continued on page 2...

...continued from cover

Additionally, comprehensive staff training to recognize phishing emails—often the entry point for ransomware like Qilin—is essential. Regular simulations and awareness programs can significantly reduce human error. **Tip:** Implement immutable, offline backups with quarterly restore testing and conduct phishing awareness training to fortify defenses against social engineering attacks.

2 Microsoft SharePoint Exploits Persist

In July 2025, Chinese hacking groups, notably Linen Typhoon, aggressively exploited vulnerabilities in Microsoft SharePoint Server, specifically CVE-2025-53770 and CVE-2025-53771, impacting over 400 organizations globally. These unpatched flaws allowed attackers to execute remote code, gain unauthorized access, and exfiltrate sensitive data, including proprietary business information and customer records. The persistence of these attacks highlights the critical need for timely patch management, as unpatched systems remain a primary entry point for cybercriminals. Microsoft has released patches to address these vulnerabilities, but many organizations lag in applying them due to operational constraints or lack of awareness. Beyond patching, rotating ASP.NET keys is crucial to prevent session hijacking, and enabling Microsoft Defender for Endpoint provides real-time threat detection and response capabilities. Organizations should also conduct regular vulnerability scans to identify and prioritize remediation efforts. **Tip:** Apply Microsoft's patches, rotate ASP.NET keys, and enable Defender for Endpoint.

3 Insurers Crack Down on Unpatched CVEs

Cyber insurers are tightening policies, limiting payouts for breaches involving unpatched CVEs, per Dark Reading. With cybercrime spiking—ransomware payments hit $50 million for Qilin alone in 2024—insurers now scrutinize patch management closely. Unpatched vulnerabilities, like those in SharePoint or SonicWall firewalls, fueled major2025 breaches. Organizations failing to patch risk full liability for losses. Tip: Automate patch deployment and track CVEs to meet insurance standards and counter rising cyber threats.

4 ShinyHunters Hits Salesforce Platforms

In August 2025, the notorious ShinyHunters group targeted Salesforce platforms, exploiting brands like Google and Pandora through sophisticated social engineering tactics. Attackers used phishing and vishing (voice

phishing) to trick employees into granting access, resulting in the theft of sensitive customer data, including emails and phone numbers. These breaches highlight the vulnerabilities in third-party platforms, particularly those with permissive OAuth configurations that allow excessive access to connected applications. Weak OAuth settings enabled attackers to move laterally across integrated systems, amplifying the scope of the breach. To mitigate such risks, organizations must restrict OAuth permissions to the minimum required for functionality and implement strict access controls. Employee training on detecting vishing attempts, such as verifying caller identities through trusted channels, is critical to preventing social engineering attacks. Regular security reviews of third-party integrations can further reduce exposure. **Tip:** Restrict OAuth permissions and train staff on vishing detection.

PRACTICAL CYBERSECURITY TIPS FOR SEPTEMBER

1 Defend Against AI-Powered Phishing

AI-driven phishing attacks, surging 30% in 2025, leverage advanced voice cloning and highly tailored emails to deceive unsuspecting users. Recent scams have convincingly mimicked corporate executives, tricking employees into divulging sensitive credentials or approving fraudulent transactions. These attacks exploit behavioral data scraped from public sources, making them alarmingly personalized and difficult to detect without scrutiny. To counter this, organizations must train staff to verify sender domains meticulously and contact suspicious senders through trusted, independent channels, avoiding direct replies to potentially compromised messages. Implementing email filtering tools with AI detection can further reduce risks by flagging anomalies in real time. **Action:** Verify sender domains rigorously, contact suspicious senders via verified channels, and deploy AI-based email filters to catch sophisticated phishing attempts.

2 Upgrade to Strong MFA

The Astaroth 2FA phishing campaign, a growing threat in 2025, exploits vulnerabilities in SMS-based multi-factor authentication, bypassing it with alarming ease. Attackers intercept SMS codes through social engineering or SIM-swapping techniques, compromising accounts. App-based or hardware token MFA, such as YubiKey or authenticator apps like Authy, provides significantly stronger protection by eliminating reliance on vulnerable SMS channels. Transitioning to these methods is critical as attackers increasingly target SMS-based systems. Organizations should prioritize disabling SMS MFA by September's end and educate users on secure authentication practices to prevent credential theft. **Action:** Switch to authenticator apps like Authy and disable SMS MFA by September's end.

3 Stay Ahead with Patching

Unpatched CVEs, such as those affecting Microsoft SharePoint, accounted for 40% of cyber exploits in 2025, fueling widespread breaches. Cyber insurers now mandate timely patching as a condition for coverage, denying payouts for losses tied to unpatched systems. Delays in applying updates expose organizations to ransomware, data theft, and regulatory penalties, as seen in recent high-profile attacks. Automated patch management systems can streamline updates across complex IT environments, while monthly audits ensure no vulnerabilities are overlooked. Establishing a robust patch management policy is essential to meet insurer standards and mitigate evolving cyber threats. **Action:** Enable auto-updates for systems, conduct monthly audits for unpatched software, and implement a formal patch management policy to ensure compliance and security.

4 Secure Third-Party Platforms

Recent Salesforce breaches underscore the growing risks of supply chain attacks, where attackers exploit weak OAuth settings to access sensitive data, including customer records and proprietary information. Misconfigured third-party platforms allow unauthorized access, enabling lateral movement across connected systems and amplifying breach impacts. Regular audits of third-party access, coupled with strict permission controls, are critical to minimizing exposure. Organizations should also enforce least-privilege principles, ensuring vendors and integrations only access essential functions. Ongoing monitoring of third-party security practices can prevent exploitation of supply chain weaknesses. **Action:** Audit third-party access and limit permissions to essential functions.

QUICK TIP SIDEBAR

Immutable Backups Are Key
Ransomware like Qilin targets backups. Use immutable, offline backups and test restores quarterly to ensure recovery.

> ***"Patching isn't optional—80% of 2025 breaches exploited outdated systems."***

BLACK BELT SECURE

READER CHALLENGE:

Share your best patching strategy! Top tips will be featured in October's issue.

Ask the Expert:
Got a question? Email us at info@blackbeltsecure.com!

THE FUTURE OF CYBERSECURITY: WHAT TO WATCH

AI-as-a-Service Powers Cybercrime

AI-as-a-Service platforms are fueling 2025's cybercrime wave, enabling low-skill hackers to launch sophisticated phishing and malware attacks. The February 2025 OpenAI leak of 20 million credentials supercharged AI-driven scams, including voice-cloned vishing targeting executives. With ransomware payments soaring (e.g., $50 million for Qilin in 2024), unpatched systems amplify risks, as insurers now limit payouts for CVE-related breaches.
What to Do: Deploy AI-based detection, secure API keys, and patch systems promptly to meet insurance standards and counter evolving threats.

Supply Chain Attacks Surge

Supply chain attacks, like ShinyHunters' Salesforce exploits, spiked in 2025, targeting third-party platforms to steal sensitive data, including customer records. Weak vendor security and unpatched CVEs remain prime entry points, with 58% of retail firms hit by ransomware in Q2 2025, causing significant financial losses. These attacks exploit lax configurations, enabling lateral movement across systems.
What to Do: Conduct regular vendor security audits, enforce strict least-privilege access controls, ensure all systems are patched promptly, and monitor third-party integrations to avoid liability and strengthen defenses.

Cloud Misconfiguration Risks

Misconfigured cloud settings caused a 5.5 million record leak at Yale New Haven Health, exposing sensitive patient data, including medical records. As cloud adoption surges in 2025, weak access controls, like overly permissive IAM roles or unsecured APIs, fuel breaches with severe regulatory and financial consequences. Attackers exploit these missteps to access unprotected systems, risking data theft.
What to Do: Conduct regular cloud configuration audits using automated tools, enforce least-privilege access controls, enable robust logging and encryption, and train IT staff on cloud security best practices to prevent data exposure and ensure regulatory compliance.