EDME CYBER PLUGG IN
MONTHLY NEWSLETTER
FEB 2026

FEB ISSUE 12

Welcome to the latest edition of our Cyber Insights Newsletter, your comprehensive guide to staying informed about the ever-evolving world of cyber threats, trends, and insurance. As your trusted cyber insurance partner, we bring you curated updates on domestic and international developments, helping you mitigate risks and enhance resilience.

EMERGING TRENDS IN THE CYBER WORLD

The "Triple -Extortion" Surge:

Ransomware groups have moved past simple encryption to "Triple Extortion" (data theft, DDoS, and harassment). In January, the group ShinyHunters claimed responsibility for massive breaches at Crunchbase and Match Group, prioritizing the public leaking of corporate contracts and PII over locking local systems.

Agentic AI Identity Risks:

As organizations deploy autonomous AI agents to handle workflows, a new "Identity Crisis" has emerged. Nearly 1 in 5 AI-related breaches in January were traced back to unsanctioned or "Shadow AI" agents that lacked proper access controls, allowing them to leak sensitive internal data through unmonitored prompts.

India's AI & Deepfake Mandates:

Under the IT Rules Amendment (Feb 2026), digital intermediaries in India now face a strict 3-hour window to remove flagged unlawful synthetic content. New regulations also mandate the explicit labeling of AI-generated media (SGI) with permanent metadata to combat the rise of "digital arrests" and deepfake fraud.

Cloud Credential & Broker Exploits:

The threat actor Zestix emerged as a dominant Initial Access Broker (IAB) this month, successfully selling corporate credentials stolen from cloud-sharing platforms like ShareFile, Nextcloud, and OwnCloud. This shift confirms that attackers are targeting the "trusted cloud" as their primary entry point for corporate espionage.

MFA-Bypass as the New Standard:

Adversary-in-the-Middle (AiTM) attacks have surged by 146% year-over-year. Attackers are now using transparent proxy kits to capture session tokens in real-time, effectively "walking through the door" after the user provides a legitimate MFA approval, making standard SMS and Push-based MFA insufficient for high-value targets.

CYBER NEWS

India Faces 3,195 Weekly Cyber Attacks

According to the Check Point 2026 Cyber Security Report, Indian organizations are now facing an average of 3,195 attacks per week, a 2% increase year-over-year. The report highlights that the Education (7,684 attacks) and Business Services (3,747 attacks) sectors are the most frequent targets. Attackers are increasingly using AI-driven automation to scale reconnaissance and execute multi-channel campaigns across email, web, and phone.

READ MORE >

Escalation of AI-Driven "Agentic" Phishing

In January, domestic security analysts documented a shift from static phishing to "Agentic AI" campaigns. Unlike traditional scams, these autonomous AI agents can engage in real-time, multi-turn conversations with employees via chat and email, adapting their persuasion tactics based on the victim's responses. This method has proven highly effective at bypassing standard behavioral filters, as the AI mimics internal organizational context and regional language nuances with high precision.

READ MORE >

265.5 Million Cyber Threats Hit India in a Year

Between October 2024 and September 2025, Seqrite recorded 265.52 million detections across more than 8 million endpoints in India, averaging 505 detections every minute. Engineering and Manufacturing alone accounted for 3.79 million detections, or 14.22% of total industry volume, placing it among the top three most targeted sectors alongside education and healthcare, which together contributed nearly 47% of overall detections.

READ MORE >

Schneider Prototyping Ransomware Attack

The Indian arm of Schneider Prototyping was hit by the Black Shrantac ransomware group. The attackers claimed to have exfiltrated 2TB of sensitive data, including financial records and CXO-level internal communications, highlighting vulnerabilities in India's high-end manufacturing sector.

READ MORE >

New Cybersecurity Law on Cards

The Centre is considering a new legal framework to address emerging cybersecurity challenges and opportunities, Union IT Minister Ashwini Vaishnaw said. He further added, "underscoring the need for closer coordination between government and industry. We also have to create a new legal framework for cybersecurity with all these challenges that we are facing today and the new opportunities that we have. The time has come when we, as a government and industry, need to align together to handle these threats."

READ MORE >

CYBER NEWS

The European Space Agency (ESA) Massive Exposure:

In early January, the ESA confirmed a significant breach affecting external science servers. The hacking group Scattered Lapsus$ Hunters (and earlier, an actor named "888") claimed to have exfiltrated over 700 GB of data, including private Bitbucket repositories, source code, and sensitive contractor documentation linked to partners like SpaceX and Airbus.

READ MORE >

The Rise of AI-Industrialized Malware (VoidLink):

Researchers identified VoidLink, a sophisticated Linux malware framework written in Zig, which was developed almost entirely by AI. Using a "Spec-Driven Development" approach, a single actor was able to generate over 88,000 lines of code and a fully functional implant inunder a week.

READ MORE >

China's Amended Cybersecurity Law (CSL 2026):

Effective January 1, 2026, China's first major update to its 2017 law is now in force. It introduces a tiered penalty regime where "aggravated" violations (like massive data leaks) can now trigger fines of up to RMB 10 million (approx. $1.4M) or 5% of annual turnover, while specifically mandating new risk assessments for AI-driven systems.

READ MORE >

"ClickFix" Campaign Uses Fake BSOD to Push Malware

A sophisticated social engineering campaign known as ClickFix saw a massive global spike in January. The attackers, tracked as PHALT#BLYX,use fake "Windows Blue Screen of Death" (BSOD) overlays to trick hospitality and business travelers into executing malicious PowerShell commands. These commands deliver remote access malware (DCRat), allowing attackers to bypass traditional browser security and gain full control over infected workstations.

READ MORE >

AI-assisted Hacker Breached 600 Fortinet Firewalls in 5 Weeks

Amazon is warning that a Russian-speaking hacker used multiple generative AI services as part of a campaign that breached more than 600 FortiGate firewalls across 55 countries in five weeks. A new report by CJ Moses, CISO of Amazon Integrated Security, says that the hacking campaign occurred between January 11 and February 18, 2026, and did not rely on any exploits to breach Fortinet firewalls.

READ MORE >

01
CASE STUDY

Brief Summary:

A regional automotive parts manufacturer was hit by a double-extortion ransomware attack. The attackers gained entry via an unpatched vulnerability in an older VPN gateway. Once inside, they moved laterally across the network for 10 days, exfiltrating 400GB of proprietary CAD designs and financial records before deploying encryption payloads that halted three production lines.

Root Cause Analysis:

Vulnerability Management Failure:
The entry point was a known CVE from late 2025 in the company's edge VPN appliance. The IT team had deferred the patch due to concerns about "downtime" during a peak production cycle.

Lack of Network Segmentation:
The network was "flat," meaning once the attackers compromised the administrative VLAN, they had direct line-of-sight to the Industrial Control Systems (ICS) and the primary backup servers.

Compromised Service Account:
Attackers harvested credentials for a legacy service account used for printer management. This account had domain administrator privileges, which were never revoked after the hardware was decommissioned.

Loss and Insurance Applicability:

- The manufacturer experienced a complete halt in production for five days, leading to significant contract backlogs and a total cessation of factory floor output.
- Due to the exfiltration of sensitive employee PII alongside proprietary CAD data, the firm was required to engage external legal counsel and provide long-term identity protection services for the affected workforce.
- Insurance Applicability: The claim was contested under the "Maintenance of Security Standards" clause. The insurer argued that failing to patch a critical-rated vulnerability for over 90 days constituted "gross negligence," resulting in a 40% reduction in the final payout.

Recommended Post-Incident Measures:

Aggressive Patch Management: Implement a 72-hour "Critical Patch" mandate for all internet-facing devices, regardless of production schedules.

Network Micro-segmentation: Physically and logically separate the IT (corporate) and OT (manufacturing) networks so that an office breach cannot jump to the factory floor.

Privileged Access Management (PAM): Implement a PAM solution to rotate service account passwords and enforce the Principle of Least Privilege (PoLP).

02
CASE STUDY

Brief Summary

A retail chain suffered a Point-of-Sale (POS) Supply Chain Compromise. Attackers successfully injected malicious code into a routine software update for a third-party payment processing plugin used by the retailer. This "skimming" script harvested credit card data from over 50,000 customers across 12 locations.

Root Cause Analysis:

Third-Party Software Trust:
The retailer automatically pushed updates from the vendor's repository without sandboxing or testing the "signed" update for anomalous outbound traffic.

Insecure Egress Filtering:
The POS terminals were permitted to communicate with any IP address on the internet. This allowed the malicious script to send harvested credit card data to a command-and-control (C2) server in Eastern Europe without being blocked.

Inadequate Log Monitoring:
While the security logs recorded the unusual outbound connections, the volume of logs generated by the POS systems meant the alerts were buried and never reviewed by a human analyst.

Loss and Insurance Applicability:

- PCI-DSS Fines: The company was hit with significant non-compliance fines from the payment card industry.
- Reputational Churn: The retailer saw an immediate 15% drop in store foot traffic following the mandatory public disclosure of the breach.
- The incident was verified under the "Cyber Extortion and Data Breach" provisions; however, the retailer was responsible for a substantial self-insured retention and experienced a significant escalation in subsequent renewal costs, with annual premiums effectively doubling.

Recommended Post-Incident Measures:

Egress Whitelisting: Strictly limit POS terminals to communicate only with verified payment processor IP addresses, blocking all other outbound web traffic.

Vendor Risk Assessments: Require third-party software vendors to provide a Software Bill of Materials (SBOM) and proof of independent security audits for any code interacting with the payment environment.

Enhanced File Integrity Monitoring (FIM): Deploy FIM tools on POS controllers to detect and alert on any unauthorized changes to the system files or binary code immediately.

DATA SPOTLIGHT

The Industrialization of Cloud Intrusions and API Warfare

Supporting Statistics:

- Cloud Intrusion Velocity: Approximately 35% of all cloud-based security incidents in January 2026 involved the abuse of valid accounts, a trend that has grown 136% over the previous year.
- Sovereign AI Vulnerability: A significant 99% of organizations remain exposed to "Shadow AI," but the focus has shifted to the "Sov-AI" stack, where 22% of breaches now target the underlying ML model IP.
- Cost of API Exploitation: Organizations reported that breaches originating from compromised API environments added an average of $810,000 to the total cost of a data breach in early 2026.
- Sector Shift to Services: The Professional Goods & Services sector became the primary target in January, recording 142 cases, surpassing Manufacturing as the most targeted industry for data extortion.
- Third-Party SaaS Fallout: The share of breaches traced to third-party integrations and connected SaaS platforms hit a new high of 32%, as attackers leveraged "island hopping" to move from vendors to primary targets.
- MFA Bypass Sophistication: Among credential-based attacks, 42% successfully utilized AI-automated phishing kits designed specifically to bypass non-phishing-resistant Multi-Factor Authentication (MFA).

Implications and Tactical Risks:

- The "Liability Vacuum": Attackers are increasingly deploying autonomous AI agents that mimic legitimate machine-to-machine (M2M) communications. This makes "point of intent" nearly impossible to verify, complicating cyber-insurance claims and forensic recovery.
- "Synthetic Insider" Recruitment: A new trend emerged in January where ransomware groups began actively recruiting "synthetic insiders" —AI-generated identities used to apply for remote IT and HR roles to gain Day 1 administrative access.
- API Environment Blind Spots: Modern attack chains are moving away from traditional phishing toward "API-first" exploitation. By compromising a single integration key (e.g., in Salesforce or ShareFile), attackers can exfiltrate terabytes of data without triggering standard endpoint alerts.

VULNERABILITY WATCH

Microsoft Patch Tuesday January 2026

Microsoft inaugurated 2026 by addressing 114 vulnerabilities in its January Patch Tuesday update. The release included eight Critical and 106 Important vulnerabilities affecting Windows, Office, and Azure. Notably, the update patched one actively exploited zero-day (CVE-2026-20805) in the Windows Desktop Window Manager (DWM). This information disclosure flaw allows local attackers to leak sensitive memory addresses, frequently used by threat actors to bypass Address Space Layout Randomization (ASLR) and chain more complex elevation-of-privilege attacks. Additionally, Microsoft addressed a high-risk security feature bypass in Windows Secure Boot (CVE-2026-21265) and removed legacy Agere Soft Modem drivers to eliminate a persistent class of "living off the land" vulnerabilities.

Adobe Patches for January 2026

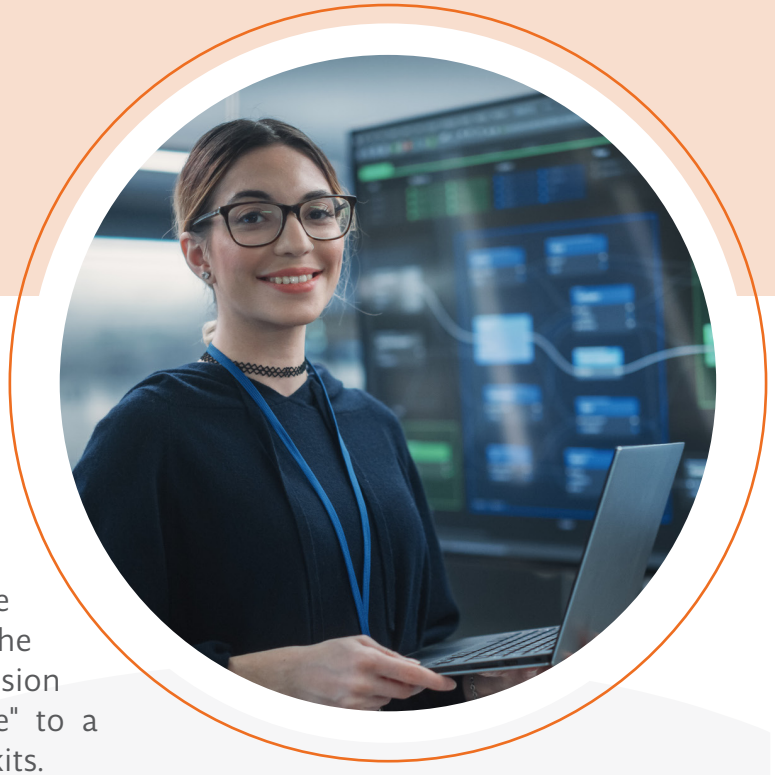
Adobe released several security bulletins in January 2026, primarily focusing on its creative and development suites. The Adobe Dreamweaver (APSB26-01) update was a significant highlight, resolving multiple critical flaws (including CVE-2026-21267) that could lead to arbitrary code execution via OS command injection. Critical updates were also issued for Adobe InDesign (APSB26-02) and Adobe Illustrator (APSB26-03), addressing heap-based buffer overflows and uninitialized pointer access that could allow attackers to execute code if a victim opens a specially crafted file. While no active exploitation was reported for these specific patches in January, Adobe warned of a late-quarter surge in targeted attacks against Adobe Commerce users, requiring separate prioritized hotfixes.

Google Chrome Security Updates January 2026

Google released a series of updates for the Chrome stable channel in January 2026, including a high-severity fix for a flaw in Chrome WebView (CVE-2026-0628) early in the month. By late January, Google addressed several use-after-free vulnerabilities within the browser's core components. While the first confirmed "in-the-wild" zero-day of the year (CVE-2026-2441) was fully disclosed and patched in early February, the January updates laid the groundwork for hardening the CSSFontFeatureValuesMap implementation. Users were urged to move to version 145.0.7632.75 or later to mitigate risks associated with sandbox escapes and remote code execution triggered by maliciously crafted HTML pages.

SECURITY ADVISORIES

Key Recommendations to Protect Your Business



Mandatory Transition to Phishing-Resistant MFA

Traditional Multi-Factor Authentication (MFA) methods, such as SMS codes and mobile push notifications, are increasingly vulnerable to sophisticated "MFA Fatigue" and Adversary-in-the-Middle (AiTM) attacks. Organizations should prioritize the deployment of phishing-resistant credentials based on FIDO2/WebAuthn standards, such as hardware security keys or platform-native passkeys. By binding the authentication process to the specific hardware and the legitimate website URL, these tools eliminate the risk of session hijacking and credential relay. This shift moves security beyond "something you have" to a cryptographically verified link that cannot be intercepted by standard social engineering kits.

Continuous External Attack Surface Management (EASM)

As digital footprints expand across various cloud providers and remote environments, "Shadow IT, unmanaged assets like forgotten cloud buckets, legacy dev servers, or unauthorized SaaS apps becomes a primary entry point. Businesses must implement Continuous External Attack Surface Management (EASM) to gain an "attacker's eye view" of their internet-facing presence. Rather than relying on static annual audits, EASM tools provide real-time discovery and monitoring of all public-facing assets. This allows security teams to identify exposed ports, expired certificates, and unpatched software versions instantly, ensuring that the organization's actual perimeter matches its documented inventory.

CYBER QUIZ

FIND ANSWERS IN
THE NEXT EDITION

A technician from your "Internet Service Provider" calls your office claiming there is a critical security vulnerability on your router that requires immediate remote access to fix. What is the most secure response?

A. Grant remote access immediately to prevent a potential data breach or network downtime.
B. Provide your login credentials so the technician can perform the fix after business hours.
C. Decline the request, hang up, and call the provider's official support number to verify the claim.
D. Ask the technician to email you a link to a software patch that you can install yourself.

What is the primary difference between Symmetric and Asymmetric encryption?

A. Symmetric encryption uses one private key for both locking and unlocking; Asymmetric uses a public/private key pair.
B. Symmetric encryption is used only for emails, while Asymmetric is used only for hard drive storage.
C. Asymmetric encryption is significantly faster than Symmetric, making it ideal for large file transfers.
D. Symmetric encryption requires an internet connection to function, whereas Asymmetric works offline.

ANSWERS FOR JANUARY CYBER PLUGGED-IN NEWSLETTER QUIZ

Ans: **C** Use an "out-of-band" method, such as calling a known, trusted phone number for that vendor.

Ans: **B** To continuously monitor cloud environments for misconfigurations, such as publicly exposed data buckets.

GET IN TOUCH:

RUSHIK PATEL
Associate Director
Edme Insurance Brokers Limited
Email: rushik.patel@edmeinsurance.com
Phone: +91 9820390280

ROHIT SHARMA
Cyber Practice Leader
Edme Insurance Brokers Limited
Email: rohit.sharma@edmeinsurance.com
Phone: +91 7009612226

edme

Clarity in Complexity

Edme Insurance Brokers Ltd. (formerly known as Aditya Birla Insurance Brokers Ltd.) | Registered Office: 2nd Floor, Privillion, East Wing, Sarkhej - Gandhinagar Highway, Vikram Nagar, Bodakdev, Ahmedabad, Gujarat 380054 | IRDAI License Number: 146 |Composite Broker | License Valid till: 9th April, 2027 | CIN: U99999GJ2001PLC062239 | Corporate Office: 6th floor, VIOS Tower, Off Eastern Freeway, Near Wadala Truck Terminal, Wadala East, Mumbai- 400037 | Toll free no-1800 120 2510 | W: www.edmeinsurance.com | In case of any queries/complaints/grievances, please write to us at care@edmeinsurance.com I ISO 9001 Quality Management Certified by Intertek Certification Ltd. under certificate number 0145476

ankura®

Edme sourced the above content/ information through Ankura Consulting Group, LLC, an independent Global expert services and advisory firm. For more information, please visit: **www.ankura.com** or email **amit.jaju@ankura.com**