ICICI Lombard

CYBER INSIGHTS DIGEST

June Edition

NEWS BYTES - DOMESTIC

Fake DigiYatra Website Was Targeting Indian Flyers With Lookalike Porta

A fake DigiYatra website, "digiyatra[.]in," was impersonating the official portal to scam Indian air travelers. Discovered by ThreatWatch360, this phishing site mimicked a booking platform to harvest personal data, posing significant privacy and security risks.

AI-Powered Cyberattacks Hit 72% of Indian Firms

A recent Fortinet-IDC survey reveals 72% of Indian organizations faced AI-powered cyberattacks in the past year, with only 14% feeling adequately prepared. These AI-driven threats are faster, more targeted, and harder to detect, leading to a significant increase in security challenges for Indian businesses.

India Faces Barrage of Hacktivist Cyberattacks

Over 40 hacktivist groups are targeting India, launching cyberattacks against government entities, critical infrastructure, and private organizations, primarily motivated by geopolitical and ideological reasons.

Cyber Threats Surge in India's Financial Sector

India's financial sector is experiencing a surge in sophisticated cyber threats, including phishing, deepfakes, and credential theft. This rise is attributed to rapid digital transformation and increased adoption of digital banking, highlighting critical security gaps and vulnerabilities.

Dance of the Hillary Virus Targets India

A new variant of the 'Tarbot' Android banking trojan is targeting over 750 apps, including banking and crypto wallets. It captures credentials and bypasses multi-factor authentication using overlay attacks.

Microsoft Aids CBI in Call Center Scam Bust

Microsoft collaborated with India's CBI to dismantle two illegal call centers in India targeting Japanese citizens with tech support scams. "Operation Chakra V" led to six arrests, exposing a transnational fraud leveraging social engineering and AI to coerce victims into transferring funds.

NEWS BYTES - INTERNATIONAL

IT Staff Targeted by Fake Tool Malware Sites

Malicious websites impersonating legitimate network tools like Zenmap and WinMRT are targeting IT professionals. These sites distribute Bumblebee malware, designed to compromise systems and facilitate further cyberattacks.

US, UK, Canada Financial Firms Hit by Nitrogen Ransomware

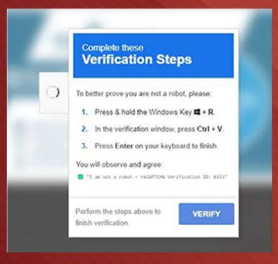
The new Nitrogen ransomware, active since September 2024, is actively targeting financial institutions in the US, UK, and Canada. This double-extortion threat encrypts critical data and steals sensitive information, demanding payment to avoid public release.

Fake Google Meet Page Spreads PowerShell Malware

A deceptive Google Meet phishing page is tricking users into executing malicious PowerShell scripts. This scheme aims to compromise systems, highlighting the ongoing threat of social engineering and malware disguised as legitimate applications.

AI TikTok Videos Spreading Infostealer Malware

Threat actors are using AI-generated videos on TikTok to distribute infostealer malware. These deceptive videos often promote fake software or cryptocurrency schemes, tricking users into downloading malicious files that compromise their systems.



Fake CAPTCHA Pages Deliver Multi-Stage Malware

New attacks use fake CAPTCHA pages to trick users into running malicious commands, deploying infostealers (like Lumma Stealer) and RATs (like AsyncRAT) through complex, multi-stage payload chains via phishing and malvertising.

UK Military Forms New Cyber and Electromagnetic Command

The UK military is establishing a new Cyber and Electromagnetic Activities (CEMA) Command. This command will integrate cyber, electronic warfare, and spectrum operations to enhance defensive and offensive capabilities in the modern battlespace.

KEY TRENDS

1/3RD

InfoSecurity Magazine

More than One-Third of Online Users Hit by Account Hacks Due to Weak Passwords

3596

CVE Details

3596 CVEs (Common Vulnerabilities and Exposures) created in May.

60S

PauBox

Modern AI systems can generate convincing voice replicas from just 60 seconds of sample audio.

$ 38.37B

Splunk

By 2026, 81% of organizations plan to implement zero trust. Its market is expected to hit $38.37 billion in 2025.

$ 2.73M

SentinelOne

RaaS has been flagged by many experts as a focal point, with cost of recovering from a ransomware attack now averaging USD 2.73 million.

66%

Palo Alto Networks

66% of transportation organizations have been affected by ransomware attacks

CYBER INCIDENT ANALYSIS

Third Party Breach in Retail Sector

INDUSTRY

- Retail

BRIEF SUMMARY

- A major retail enterprise suffered a data breach traced to an IT services provider with backend access. The attack exposed loyalty program members' personal data, raising concerns about third-party risk and data security in shared infrastructure environments.

ROOT CAUSE ANALYSIS

- Misconfigured Systems: Vendor misconfigurations exposed client data to unauthorized access.
- Weak Access Controls: Poor segmentation let attackers reach sensitive customer environments.
- Lack of Oversight: Third-party issues delayed breach detection and response efforts.
- Shared Infrastructure Risk: Multiple clients' data exposed via overlapping vendor access.

LOSS CATEGORIES TO VICTIM

- Data Exposure, Reputational Damage, Compliance Risk, Operational Disruption

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Digital Forensics: Identified breach path, affected data, and vendor's involvement.
- Legal & Regulatory Support: Assisted with notifications and global privacy law compliance.
- Communication Strategy: Guided public messaging to reduce reputational damage.

  Remediation Funding: Covered audits, contract reviews, and stronger data controls.

LOSS INCURRED

- Operational Downtime, Reputation Recovery Costs, Potential Regulatory Fines

RECOMMENDED PREVENTIVE MEASURES

- Vendor Access Control: Enforce network segmentation and least privilege to limit vendor access scope and impact.
- Third-Party Risk Assessments: Conduct regular audits of vendors' security posture and supply chain dependencies.
- Continuous Monitoring: Implement real-time monitoring of vendor activity in shared or hosted environments.
- Zero Trust Architecture: Apply zero trust principles to prevent lateral movement from vendor-compromised accounts.
- DLP & UBA Tools: Deploy data loss prevention and behavior analytics to detect misuse or data exfiltration.
- Vendor Contractual Obligations: Mandate breach notification, liability clauses, and data protection standards in contracts.

CYBER INCIDENT ANALYSIS

Ransomware Attack on IT Services Firm

INDUSTRY

- Enterprise IT Services

BRIEF SUMMARY

- An organization was hit by RA World ransomware after attackers exploited Citrix Bleed (CVE-2023-4966). This allowed unauthorized access via stolen session tokens. Privileged accounts were compromised, ransomware deployed, and sensitive data exfiltrated using a cloud tool. Ransom demands followed, with proof of stolen files.

ROOT CAUSE ANALYSIS

- Citrix Vulnerability Exploited: Attackers leveraged unpatched CVE-2023-4966 on exposed Citrix perimeter systems.
- Token Reuse Enabled: Stolen session tokens remained valid due to lack of invalidation mechanisms.
- Weak Internal Controls: No MFA or endpoint protection allowed attackers to move laterally undetected.
- Over Privileged Accounts Abused: Service accounts had excessive permissions, enabling ransomware deployment and system changes.
- No Data Egress Controls: Attackers used third-party tools to exfiltrate data without detection.

LOSS CATEGORIES TO VICTIM

- Sensitive data exposure and potential public leakage.
- Business downtime due to system encryption and recovery delays.
- Reputational and regulatory impact, including potential fines.

INSURER'S ASSISTANCE IN INCIDENT MANAGEMENT

- Forensic analysis traced the entry point and attacker activities.
- Containment and recovery efforts included isolation and firewall updates.
- Legal support and negotiation with attackers and regulatory authorities.

LOSS INCURRED

- Incidence Response Costs, Downtime Loss, Regulatory Penalties

RECOMMENDED PREVENTIVE MEASURES

- Immediate patching of exposed and critical infrastructure.
- Enforce MFA across remote access and privileged interfaces.
- Implement least privilege, with regular audits of service accounts.

ADVISORIES

CISA ADVISORY ON LUMMAC2 MALWARE

- Critical Security Advisory: On May 21, 2025, CISA and the FBI issued a joint advisory warning about the LummaC2 malware, an advanced information stealer actively used by threat actors to exfiltrate sensitive data from organizations
- CISA Recommendation: Organizations are strongly urged to implement the mitigation strategies outlined in the advisory. These include blocking known indicators of compromise (IOCs), enhancing phishing defenses, and educating users on social engineering tactics. The advisory also recommends reviewing and applying endpoint protection and detection measures to identify and stop LummaC2 infections.
- Threat Overview: LummaC2, first seen in 2022 on Russian-language cybercriminal forums, is typically delivered via spear phishing emails containing malicious links or attachments. It uses deceptive tactics like fake CAPTCHA prompts to trick users into executing malicious PowerShell commands.
- Proactive Cybersecurity Measure: This advisory highlights the growing sophistication of malware delivery methods and the importance of layered security defenses. Regular user training, vigilant monitoring, and timely application of threat intelligence are essential to reducing exposure to such threats.

Read more at: CISA Releases Seven Industrial Control Systems Advisories | CISA

ADVISORY : RUSSIAN GRU TARGETING LOGISTICS ENTITIES AND TECHNOLOGY COMPANIES

- Critical Security Advisory: On May 21, 2025, CISA, along with international partners including the NSA, FBI, and cybersecurity agencies from the UK, Germany, Czech Republic, Poland, and Australia, issued a joint advisory warning of a Russian state-sponsored cyber campaign targeting Western logistics and technology companies.
- CISA Recommendation: Organizations in logistics and IT sectors are urged to heighten their cybersecurity vigilance. This includes increasing monitoring for known tactics, techniques, and procedures (TTPs), conducting proactive threat hunting, and assuming a posture of potential targeting by Russian GRU-affiliated actors.
- Targeted Entities: The campaign specifically focuses on companies involved in the coordination, transport, and delivery of foreign aid to Ukraine. The threat actors—linked to the Russian GRU's 85th Main Special Service Center (Unit 26165)—are known for cyber espionage and have previously exploited IP cameras and other infrastructure in Ukraine and NATO-bordering nations
- Proactive Cybersecurity Measure: This advisory underscores the persistent threat posed by nation-state actors and the need for continuous threat intelligence integration, network segmentation, and user awareness training to defend against sophisticated cyber espionage campaigns.

Read more at: Fortinet Releases Advisory on New Post-Exploitation Technique for Known Vulnerabilities | CISA