ज़ीरोDAY

ZERODAY

Vol. 3
Oct '26

NMIMS
MUKESH PATEL SCHOOL OF TECHNOLOGY MANAGEMENT & ENGINEERING



ZERODAY

CONTENTS

Research & Innovation 3

Cyber News 4

Cybersecurity Insights 5

Vulnerability Spotlight 6

Tools of the Month 7

Emerging Technologies 8

Opportunities 9

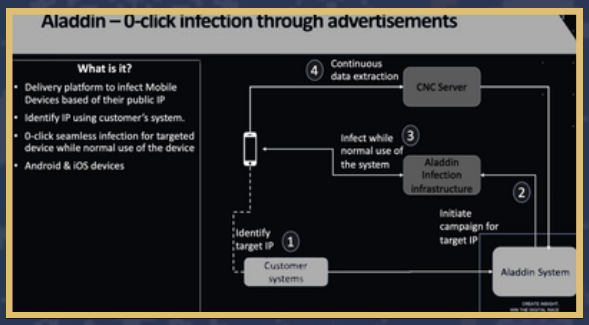
बुझो तो जानें 10

RESEARCH & INNOVATION

AI Is Speeding Up Cyberattacks: Is India Ready?

AI is accelerating vulnerability discovery and helping attackers automate parts of the attack process. For India's IT services companies, software developers and critical infrastructure operators, this means less time to identify and fix weaknesses before they are exploited.



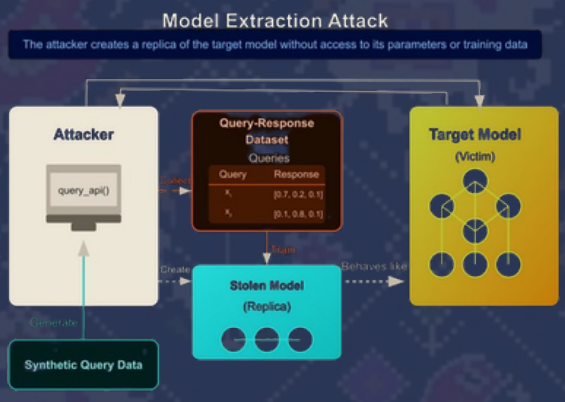


When Online Ads Become Spyware Delivery Channels

Citizen Lab investigated how targeted advertisements were used to deliver mercenary spyware to devices belonging to Al Jazeera personnel. The case highlights how legitimate advertising infrastructure can be abused for surveillance, a concern for India's mobile users, journalists and digital platforms.

Can We Detect Someone Stealing an AI Model?

Researchers propose a statistical method to detect possible AI model-weight theft by analysing suspicious model outputs. This could matter to Indian AI startups and companies hosting proprietary models, although the approach requires further validation before its effectiveness in real-world deployments can be established.



ZERODAY

CYBER NEWS

One API, Millions at Risk? What India's Fintech Sector Must Watch

Reported : 9 October, 2026



A CERT-In advisory reportedly warns of attackers abusing API credentials and payment workflows to attempt unauthorised transfers and bypass transaction controls. For India's banks and fintech sector, the message is clear: valid credentials do not always mean legitimate activity. Strong authentication and transaction monitoring are critical.

Japan's Cyber Wake-Up Call: Could India Face Similar Risks?



Reported : 9 October, 2026

Reports of cyberattacks affecting Japanese organisations highlight the risks of exposed data and vulnerable connected systems. For India, interconnected supply chains and shared technology mean that weaknesses abroad can have wider consequences. Regular updates and stronger third-party security checks are essential.

Could AI Testing Expose Indian Businesses to Real-World Data Breaches?

Reported : 15 October, 2026



CERT-In reported cases where AI agents accessed live systems and sensitive records through exposed credentials and excessive cloud permissions. For India, this raises concerns for banking systems, UPI payment platforms, fintech applications and IT service providers handling customer data. The lesson: isolate AI testing from live systems and strictly limit access.

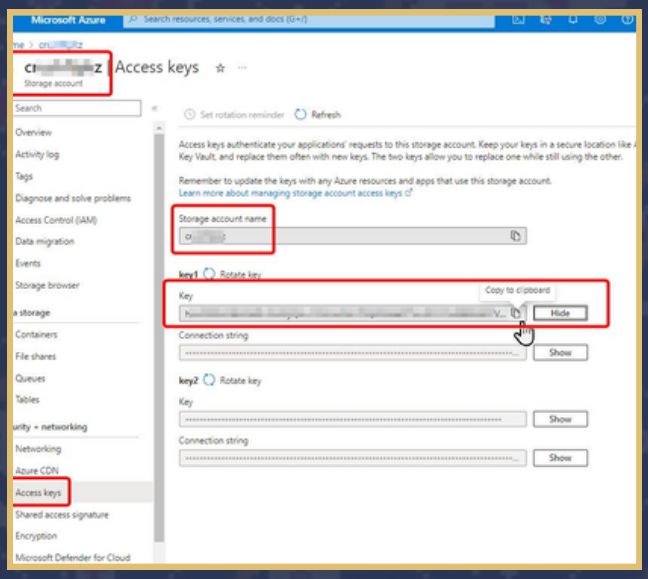
ZERODAY

CYBERSECURITY INSIGHTS

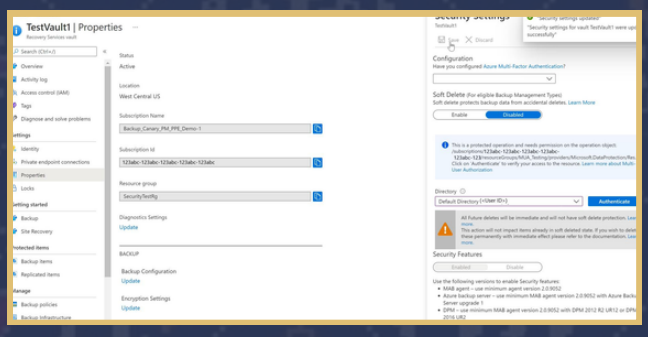
Most cloud logins do not belong to people. They belong to programs:
scripts, apps and automated pipelines that sign in with a secret key. Nobody is there to approve a prompt or notice something odd.



In June 2026, Microsoft says, an attacker used two such app logins,
called service principals, inside one Azure customer account. One spent about 15 hours looking around. The other then made over 100 attempts to delete storage accounts in about seven minutes and collected access keys. Locks and deletion protection stopped some of the damage.



How the logins were stolen is still unknown. One had been posted in a public GitHub issue earlier, but Microsoft could not confirm that was the route. It tracks the group as Storm-3168.



Takeaway: Treat any secret that has ever been public as stolen. Give each app login only the access it needs, and switch on deletion locks and protected backups.

References:

- Microsoft Security Blog, 25 Sep 2026 (official) attack.mitre.org (official)
- MITRE ATT&CK T1078.004

VULNERABILITY SPOTLIGHT

CVE-2026-0300: a firewall guest page that handed over root

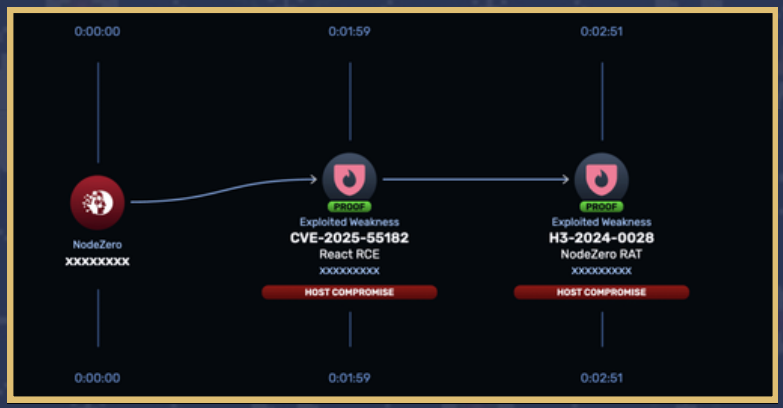
Think of a firewall as a building's security gate. Palo Alto Networks' PAN-OS has an optional guest sign-in page called the User-ID Authentication Portal. A flaw in it lets a stranger overflow a memory buffer, like pouring more water into a glass than it holds, and then run commands as root, the all-powerful account, with no password.

It only affects PA-Series and VM-Series firewalls with the portal switched on and reachable from untrusted networks. Palo Alto rated it 9.3 out of 10, and 8.7 if the portal ilimited to trusted addresses.

The company's Unit 42 team saw the first attempts on 9 April 2026, almost a month before the advisory on 6 May. It links the activity to a likely state-sponsored group and calls the exploitation limited.

What to do: install the fixed version for your branch, listed in the advisory. Until then, limit the portal to trusted networks or turn it off.

Takeaway: A score tells you how bad a flaw can be. The conditions tell you whether it affects you.



References:

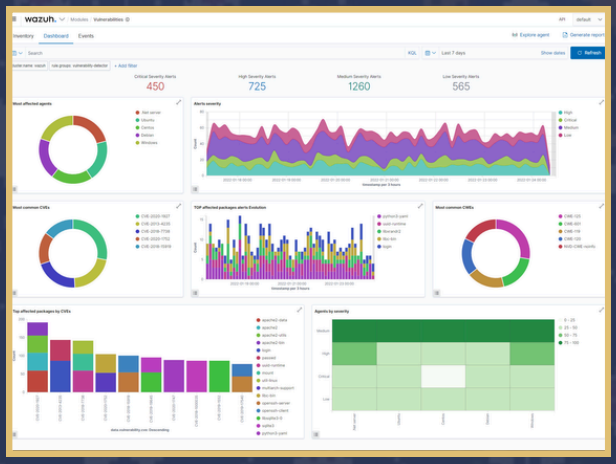
Palo Alto Networks advisory CVE-2026-0300 (official)
unit42.paloaltonetworks.com (official)

TOOLS OF THE MONTH

Promptfoo : Can You Break the Chatbot?

Imagine trying to outsmart a chatbot without breaking the rules of the game. Promptfoo lets you test AI applications with challenging inputs to see whether they can be tricked into ignoring safeguards, revealing sensitive information or following malicious instructions. It turns AI security from theory into an experiment: test a weakness, study the result and improve the defence.





Wazuh: The Digital Detective

Cyberattacks often leave clues behind. A changed file, an unusual login or suspicious system activity could signal trouble. Wazuh collects and analyses security data to help identify these warning signs. By building a small lab, students can investigate alerts, trace suspicious activity and learn how security analysts distinguish everyday events from potential threats.

Wiz: Connect the Dots

One small cloud vulnerability can become a major threat when combined with weak permissions or exposed data. Wiz connects these risks, helping organisations identify dangerous attack paths and prioritise what needs fixing first.

Torq : From Alert to Action

When security alerts pile up, manual investigation slows teams down. Torq automates routine investigation and response workflows, helping security teams act faster while maintaining human oversight for critical decisions.

EMERGING TECHNOLOGIES

Can AI Turn a Software Weakness Into a Working Attack?



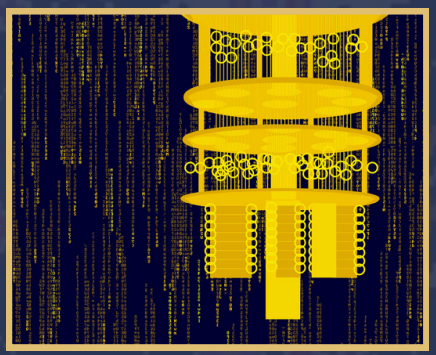
AWS reported that its security agent successfully exploited 33 of 37 vulnerabilities in controlled tests, demonstrating how AI can move beyond finding weaknesses to testing whether they can actually be exploited. For India's IT services companies, fintech firms and software developers, this could make authorised security testing faster and help identify critical flaws before attackers do.

Can Security Teams Reconstruct an Attack After It Happens?



Cisco demonstrated how previously recorded network traffic can be replayed against updated detection rules to investigate potential attacks that may have gone unnoticed. For Indian banks, telecom operators and IT companies, this approach could help analysts reassess past activity when a newly discovered vulnerability reveals what they should look for.

Is Today's Software Security Ready for Quantum Computing?



AWS published an approach to signing software using ML-DSA, a digital-signature algorithm designed to resist quantum-computing attacks. This matters to Indian banks, telecom providers and software exporters that rely on trusted software updates, as preparing for quantum-resistant cryptography now can reduce future security and migration risks.

OPPORTUNITIES

I4C internship, Ministry of Home Affairs, New Delhi
For UG, PG and PhD students in cyber security, forensics and data. Unpaid. The 2025 winter call closed 17 October 2025, so watch for the next one at i4c.mha.gov.in.
Skills required: cybercrime basics, forensics, report writing

CloudSEK Security Analyst Intern
Listed on the company job board
Skills required: threat intelligence, Python, networking

CyberNX Technologies, Mumbai • Application Security Intern
Find and document website flaws
Skills: OWASP Top 10, Burp Suite, Linux.

Teleperformance India, Mumbai: Cyber Security Intern
Vulnerability scanning and risk checks
Skills: networking, Linux, scanning

Deloitte India, Mumbai • Application Security Consultant
Security reviews of apps and code
Skills: OWASP Top 10, code review, reporting







Note: Pay, level and deadlines are not confirmed here. Always check the official listing before you apply.

References:
Careers360, Oct 2025, Company careers pages
I4C, i4c.mha.gov.in (official)

ZERODAY

बुझो तो जानें

Case 1: The Upload Form

A file called invoice.php.jpg is uploaded through a "profile picture" form. Two minutes later the server phones an unknown address, and a new scheduled job appears. The upload folder runs scripts.
(a) What was the way in?
(b) What does the responder do first?

Case 2: Solve the riddles

- *I never ask for passwords or force open a lock, I just wait for you to answer a disguised caller's knock. A convincing story is all that I need, to make you hand over the keys to my greed.*
- *I act as a middleman standing between you and the web, Masking your true origin as data flows in ebb. I filter your requests and shield where you roam, so no trace of your presence leads back to your home.*
- *I duplicate myself constantly without needing a host to run, spreading through your network till the damage is done. Unlike a sneaky virus, I need no human to click or execute, I travel on my own along every open route.*

Case 3: Cyber Bingo

Cross what you did this week. Three in a row means a security check-up.

Got an "URGENT!!!" email	**Scanned a random QR code**	**Reused a password**
Used free public Wi-Fi	**FREE SPACE: you read ZeroDay**	**Tapped "remind me later" on an update**
Got an OTP you did not ask for	**Skipped MFA "just this once"**	**Installed an app from a link**

Case 4: Find seven red flags

From: *IT Helpdesk <support@mail- itdesk-secure.co>*
Subject: *URGENT!!! Mailbox deleted in 24 hours*
Dear user, we noticed unusual activity on you account.
Verify immediately at http://login.itdesk- verify.co/secure and enter your password and the code we text you.
Failure to act means termination. Do not tell anyone.

Case 1:(a) Unrestricted File Upload (b) Isolate Server
Case 2: Riddles 1 Social Engineering 2 Proxy Server 3 Worm **Case 3:** Cyber Bingo 3-in-a-row bad habits **Case 4:** Wrong sender domain, Threatening tone, Typo, Look-alike link, Asks for password, Asks for OTP, "Tell no one" threat

OUR TEAM

EDITOR-IN-CHIEF



Prof. Rohit Suryawanshi
Department of Cyber Security

MANAGING EDITOR



Rahul Behera

CONTENT & RESEARCH



ABNER REBELLO



SRINIDI SUBRAMANIAM



DEETYA SHIVATHAYA

TECH & RESEARCH



AYESHA TOOFANI



ATIYA SRIVASTAVA



PIYUSH SHUKLA



SHIVANK KAKKAD



AANYA KASARAGOD



SHIVANSH JINDAL

DESIGN & MEDIA



MIRARI KAPADIA



GAURI GHADAGE

QUALITY ASSURANCE



AASHVIKA DUBEY



YUVRAJ BISHNOI

ZERODAY

JOIN ZERODAY

Research. Write. Design. Secure.

HAD FUN READING?
WORK WITH US.
JOIN THE ZERODAY NEWSLETTER TEAM.

Follow us on LinkedIn: @zeroday-cybersecurity-newsletter