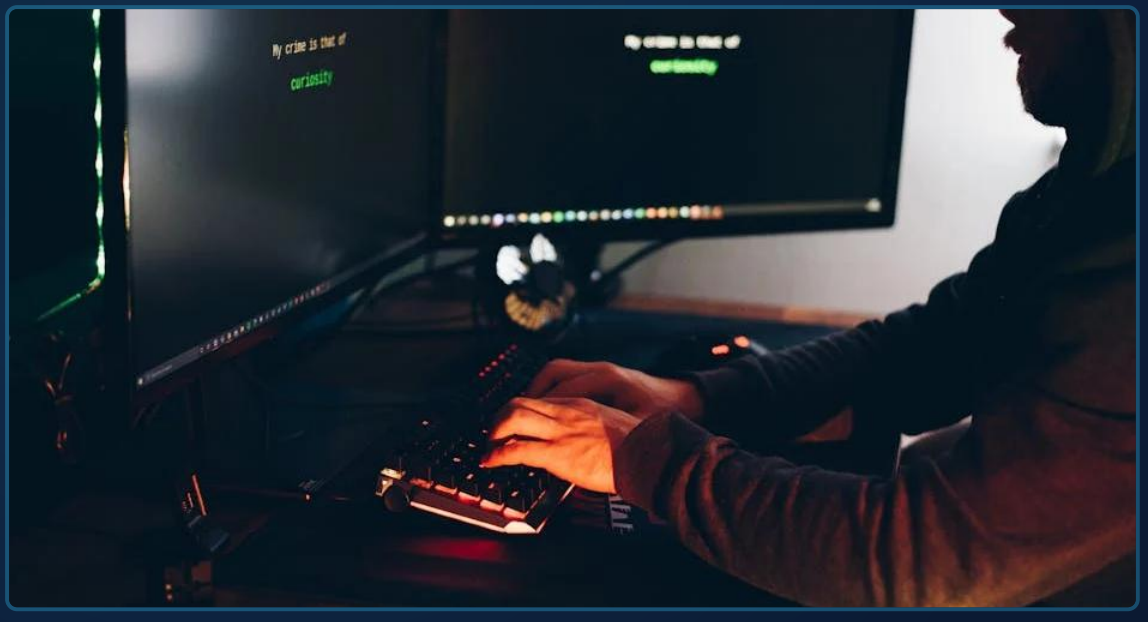
Intelligent Automation

Solutions that are powered by a SECURE Cloud.

MCSP

Managed Cybersecurity Service Provider



VOL. 1 · ISSUE 31

Cyber Shield

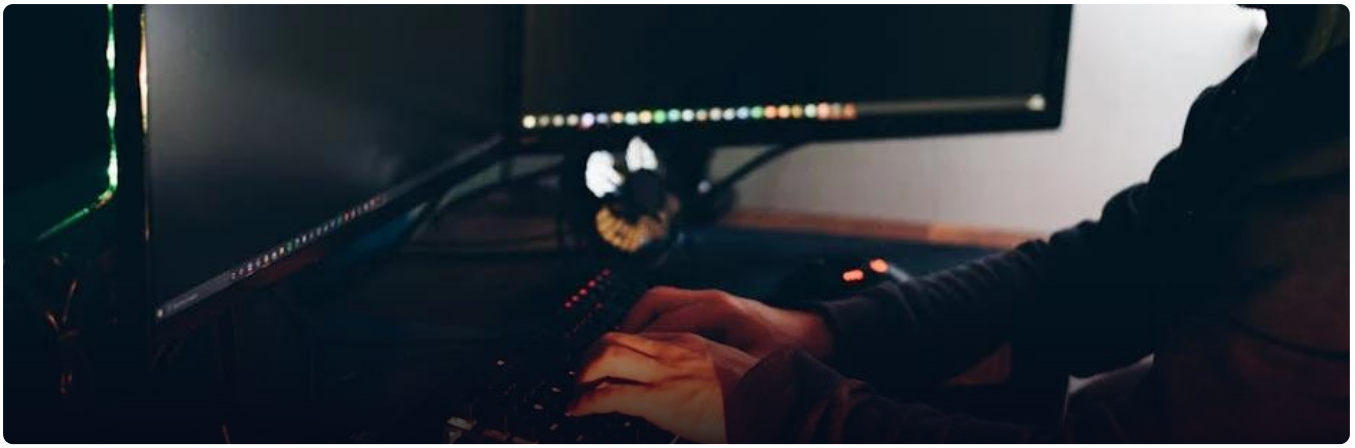
May 05, 2026

Essential cybersecurity intelligence for small and mid-sized businesses — powered by AI, delivered by Intelligent Automation, LLC.

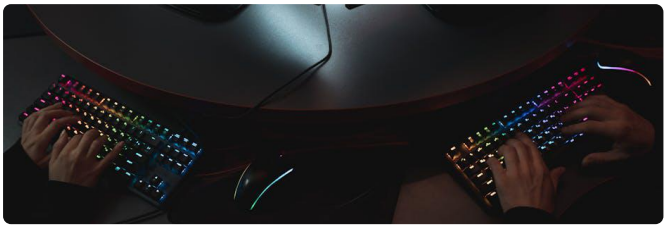
INTELLIGENT AUTOMATION, LLC · INTELAMATION.COM · FAIRFIELD, NJ

FEATURE

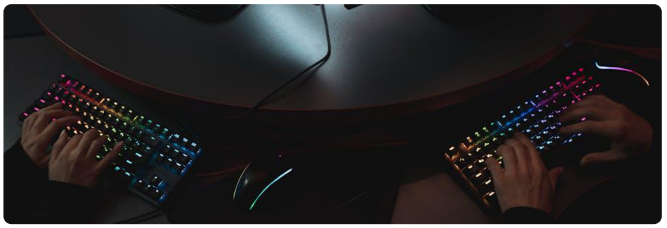
This Week in Cybersecurity



China-Linked UAT-8302 Targets Governments Using Shared APT Malware Across Regions



The Back Door Attackers Know About — and Most Security Teams Still Haven’t Closed

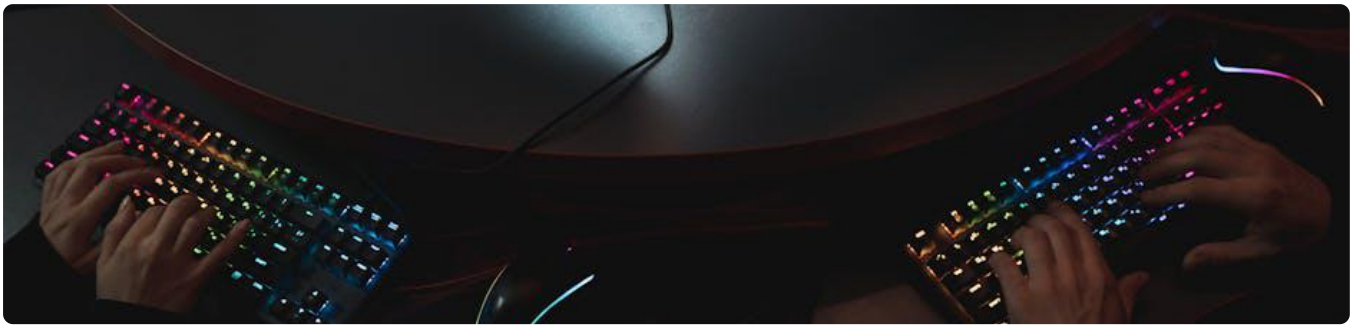


MetInfo CMS CVE-2026-29014 Exploited for Remote Code Execution Attacks

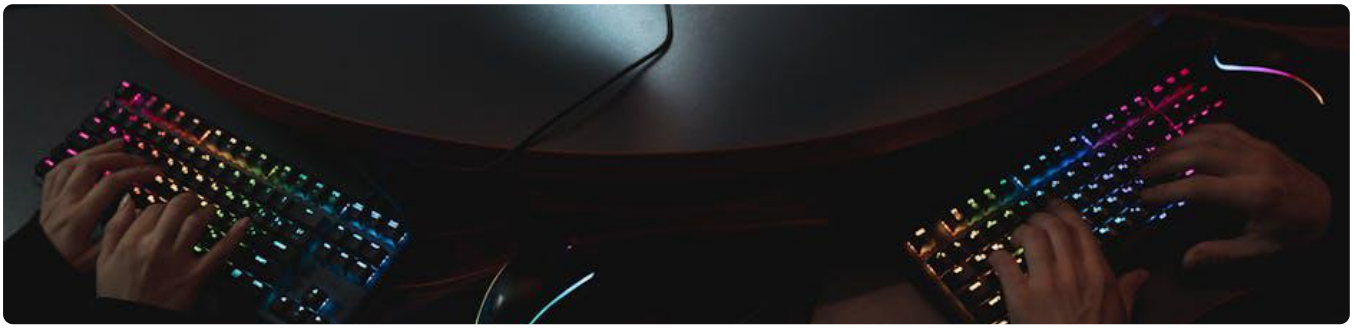
INTEL

Cyber Threat Intelligence

China-Linked UAT-8302 Targets Governments Using Shared APT Malware Across Regions



The Back Door Attackers Know About — and Most Security Teams Still Haven’t Closed



MetInfo CMS CVE-2026-29014 Exploited for Remote Code Execution Attacks

INTEL

Threat Intelligence — Continued

We Scanned 1 Million Exposed AI Services. Here's How Bad the Security Actually Is

ScarCruft Hacks Gaming Platform to Deploy BirdCall Malware on Android and Windows

Weaver E-cology RCE Flaw CVE-2026-22679 Actively Exploited via Debug API

WEEKLY TECH TIP

Audit Your External Services Before Attackers Do

Recent scans reveal that AI services and cloud-exposed applications often have critical security gaps that attackers actively exploit. Many organizations don't realize what services are publicly accessible or how vulnerable they are.

Step 1: Conduct monthly external scans to inventory all internet-facing services and applications.

Step 2: Remove or restrict public access to non-essential services using firewall rules.

Step 3: Implement strong authentication on all remaining external services, especially AI tools.

Step 4: Enable logging and monitoring for all publicly accessible systems to detect attacks.

ALERTS

National Cybersecurity Alerts

We Scanned 1 Million Exposed AI Services. Here's How Bad the Security Actually Is

ScarCruft Hacks Gaming Platform to Deploy BirdCall Malware on Android and Windows

Weaver E-cology RCE Flaw CVE-2026-22679 Actively Exploited via Debug API

REGIONAL

Regional & Sector-Specific Alerts

ScarCruft Hacks Gaming Platform to Deploy BirdCall Malware on Android and Windows

Weaver E-cology RCE Flaw CVE-2026-22679 Actively Exploited via Debug API

MAY AWARENESS

World Password Day (May 1)

Security Awareness Spotlight: World Password Day May 1st is World Password Day, your annual reminder that weak passwords remain the easiest way for criminals to break into your business systems and steal your data. If your team is still reusing passwords across multiple accounts or writing them on sticky notes, you're leaving the front door wide open—no hacker skills required. This month, make it mandatory for everyone to use a password manager like Bitwarden or 1Password, turn on multi-factor authentication for every business account that offers it, and schedule 30 minutes to audit who has access to what in your most critical systems. **Your action today: Pick one password manager, sign up for a business account, and send the setup instructions to your entire team before lunch.**

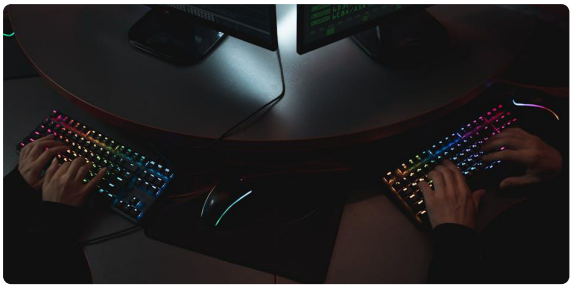
ACTION ITEM

Schedule a 15-minute team security review this week using this month's theme as your agenda.

SMB SPOTLIGHT

Protecting Your Business

Preparing for a ‘vulnerability patch wave’



Could your choice of metrics be harming your SOC?

Defending against China-nexus covert networks of compromised devices

NCSC: Leave passwords in the past - passkeys are the future

INNOVATION

Cybersecurity Advancements

Microsoft Warns of Sophisticated Phishing Campaign Targeting US Organizations

Hacker Conversations: Joey Melo on Hacking AI

Critical Bug Could Expose 300,000 Ollama Deployments to Information Theft

Critical Remote Code Execution Vulnerability Patched in Android

CTO'S DESK

From the Desk of Daniel Ramos

Daniel Ramos
Chief Technology Officer
Intelligent Automation, LLC | Fairfield, NJ
Managed Cybersecurity Service Provider

This week's headlines paint a troubling picture, but there's one thread connecting nearly every story: we're being compromised through doors we've left wide open ourselves. Whether it's the backdoor most security teams haven't closed, the exposed AI services with virtually no protection, or the MetInfo CMS vulnerability actively exploited in the wild, the pattern is clear—attackers aren't just getting more sophisticated, they're getting better at exploiting our basics.

What keeps me up at night isn't the nation-state actors or the exotic malware. It's the realization that many organizations still haven't implemented fundamental security hygiene. We're so focused on the latest AI-powered defense that we've forgotten to lock our windows and doors.

The good news? Unlike defending against a zero-day exploit, closing these gaps is entirely within your control. You don't need a massive budget or a team of specialists to patch known vulnerabilities, secure exposed services, or implement proper access controls. Start with an honest assessment of your current posture. Identify what's publicly exposed. Then methodically close those gaps, one at a time. Your future self will thank you.

CONNECT WITH DANIEL
linkedin.com/in/iamdanielramos · daniel.ramos@intelamation.com

Your Cybersecurity Partner for the Digital Age

Serving small and mid-sized businesses since 2013

336 US Highway 46, Fairfield, NJ 07004

(888) 711-4521 · intelamation.com

Read online: newsletters.intelamation.net