Intelligent Automation

Solutions that are powered by a SECURE Cloud.

MCSP

Managed Cybersecurity Service Provider

VOL. 1 · ISSUE 36

Cyber Shield

June 01, 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

⚡ Weekly Recap: New Linux Flaw, PAN-OS Exploit, AI-Powered Attacks, OAuth Phishing and More

China-Aligned Groups Ramp Up Attacks: Dragon Weave Hits Czech Republic & Taiwan

The Security Growth Platform: Why MSPs Are Moving Beyond vCISO Tools

INTEL

Cyber Threat Intelligence

⚡ Weekly Recap: New Linux Flaw, PAN-OS Exploit, AI-Powered Attacks, OAuth Phishing and More

China-Aligned Groups Ramp Up Attacks: Dragon Weave Hits Czech Republic & Taiwan

The Security Growth Platform: Why MSPs Are Moving Beyond vCISO Tools

INTEL

Threat Intelligence — Continued

OpenAI Codex Authentication Tokens Stolen in codexui-android npm Supply Chain Attack

Critical WP Maps Pro Flaw Actively Exploited to Create Admin Accounts

Dutch Authorities Dismantle Botnet Linked to 17 Million Infected Devices

ISC Stormcast For Monday, June 1st, 2026 https://isc.sans.edu/podcastdetail/9952, (Mon, Jun 1st)

Unidentified RAT pushes NetSupport RAT, (Mon, Jun 1st)

WEEKLY TECH TIP

Audit Your WordPress Plugins Before Attackers Do

The active exploitation of WP Maps Pro highlights how plugin vulnerabilities create backdoor admin accounts, giving attackers full control of your website. Outdated or poorly maintained plugins are prime targets for automated attacks that can compromise your entire business presence.

Step 1: Remove all unused or inactive WordPress plugins from your site immediately.

Step 2: Update remaining plugins to their latest versions within 24 hours of release.

Step 3: Enable automatic security updates for WordPress core and trusted plugins.

Step 4: Use a security plugin to monitor unauthorized admin account creation attempts.

ALERTS

National Cybersecurity Alerts

ISC Stormcast For Monday, June 1st, 2026 https://isc.sans.edu/podcastdetail/9952, (Mon, Jun 1st)

Unidentified RAT pushes NetSupport RAT, (Mon, Jun 1st)

YARA-X 1.17.0 Release, (Sun, May 31st)

ISC Stormcast For Friday, May 29th, 2026 https://isc.sans.edu/podcastdetail/9950, (Fri, May 29th)

REGIONAL

Regional & Sector-Specific Alerts

ISC Stormcast For Monday, June 1st, 2026 https://isc.sans.edu/podcastdetail/9952, (Mon, Jun 1st)

Unidentified RAT pushes NetSupport RAT, (Mon, Jun 1st)

YARA-X 1.17.0 Release, (Sun, May 31st)

JUNE AWARENESS

Internet Safety Month

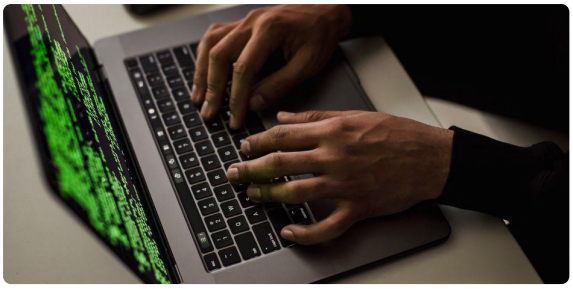
June is Internet Safety Month, making it the perfect time to strengthen your team's defenses against online threats. Most cyberattacks succeed because employees click malicious links in convincing emails or visit compromised websites, so spend 15 minutes this month reviewing what suspicious emails look like with your staff—watch for urgent requests for passwords, unexpected attachments, and sender addresses that are slightly misspelled versions of legitimate companies. Today, forward one recent phishing email your business received to your team and ask them to identify the red flags together, turning a real threat into a teaching moment.

ACTION ITEM

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

SMB SPOTLIGHT

Protecting Your Business



Designing secure access with ZTNA

Thinking carefully before adopting agentic AI

10 questions to ask when using AI models to find vulnerabilities

Preparing for a ‘vulnerability patch wave’

INNOVATION

Cybersecurity Advancements

Dutch Police Dismantle Massive 17-Million-Device Botnet

Critical Windows Netlogon Vulnerability in Attackers' Crosshairs

Dragos Acquires xIoT Security Firm Phosphorus

As the Pentagon Pushes for Battlefield AI, Some Military Leaders Urge Caution

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 familiar but unsettling picture: adversaries are everywhere, attacking everything from Linux systems to WordPress plugins. But here's what keeps me up at night—and what should matter most to you: the fundamental shift in how these attacks succeed.

Notice the pattern? The OpenAI token theft, the WP Maps Pro vulnerability, the OAuth phishing campaigns—these aren't sophisticated zero-days requiring nation-state resources. They're supply chain compromises and credential theft, exploiting the trust relationships we've built into our digital ecosystems. The scariest part? Your security perimeter now extends far beyond your firewall into every third-party tool, plugin, and service your business relies on.

The good news is that awareness is half the battle. Start by inventorying your digital supply chain—every integration, every API connection, every plugin. Then implement basic hygiene: multi-factor authentication everywhere, regular access reviews, and vendor security assessments. These aren't glamorous solutions, but they work.

You don't need to become a security expert overnight. You just need to start asking the right questions about what's connected to your business—and who has the keys.

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