Intelligent Automation

Solutions that are powered by a SECURE Cloud.

MCSP

Managed Cybersecurity Service Provider

VOL. 1 · ISSUE 51

Cyber Shield

September 14, 2026

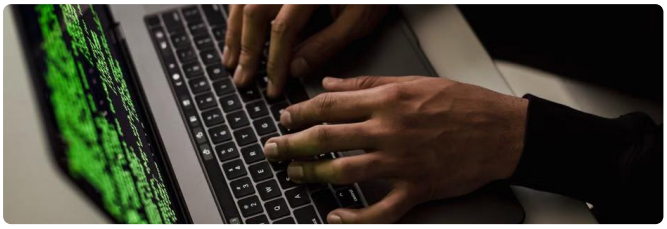
Essential cybersecurity intelligence for small and mid-sized businesses — powered by AI, delivered by Intelligent Automation, LLC.

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

FEATURE

This Week in Cybersecurity

AI Changed the Exposure Problem. Validation Needs to Change With It.



Malicious Twitch Browser Extension Leaks OAuth Tokens From Nearly 31,000 Users

Attackers Use Passkey Phishing to Hijack Microsoft Cloud Accounts and Exfiltrate Data

INTEL

Cyber Threat Intelligence

AI Changed the Exposure Problem. Validation Needs to Change With It.

Malicious Twitch Browser Extension Leaks OAuth Tokens From Nearly 31,000 Users

Attackers Use Passkey Phishing to Hijack Microsoft Cloud Accounts and Exfiltrate Data

INTEL

Threat Intelligence — Continued

CISA Adds 5 Actively Exploited Artifactory, ScreenConnect, and RouterOS Flaws to KEV

When the Whole Company Adopts AI: What It Does to Your SOC

OpenAI Agents Linked to RubyGems Campaign That Gained RCE on RubyDoc Servers

ISC Stormcast For Monday, September 14th, 2026 https://isc.sans.edu/podcastdetail/10092, (Mon, Sep 14th)

The Self-Expanding Stolen Inference Supply Chain: An AI Agent Harvesting and Re-Serving LLM Access, (Fri, Sep 11th)

💡 WEEKLY TECH TIP

Audit Your Browser Extensions Before They Leak Your Credentials

Browser extensions can silently harvest authentication tokens and sensitive data, as demonstrated by the malicious Twitch extension that compromised nearly 31,000 users. These seemingly helpful tools often request excessive permissions that enable data exfiltration without detection.

Step 1: Review all installed browser extensions across your organization and remove unused ones.

Step 2: Verify each extension's permissions and ensure they align with legitimate business needs.

Step 3: Implement browser management policies that restrict unapproved extension installations company-wide.

Step 4: Schedule quarterly extension audits and educate employees about extension security risks.

ALERTS

National Cybersecurity Alerts

ISC Stormcast For Monday, September 14th, 2026 https://isc.sans.edu/podcastdetail/10092, (Mon, Sep 14th)

The Self-Expanding Stolen Inference Supply Chain: An AI Agent Harvesting and Re-Serving LLM Access, (Fri, Sep 11th)

ISC Stormcast For Friday, September 11th, 2026 https://isc.sans.edu/podcastdetail/10090, (Fri, Sep 11th)

Redtail Payload Analysis [Guest Diary], (Wed, Sep 9th)

REGIONAL

Regional & Sector-Specific Alerts

ISC Stormcast For Monday, September 14th, 2026 https://isc.sans.edu/podcastdetail/10092, (Mon, Sep 14th)

The Self-Expanding Stolen Inference Supply Chain: An AI Agent Harvesting and Re-Serving LLM Access, (Fri, Sep 11th)

ISC Stormcast For Friday, September 11th, 2026 https://isc.sans.edu/podcastdetail/10090, (Fri, Sep 11th)

SEPTEMBER AWARENESS

Disaster Recovery Month

Security Awareness Spotlight: Disaster Recovery Month September is Disaster Recovery Month, and it's the perfect time to make sure your business can survive when things go wrong—whether that's a ransomware attack, a fire, a flood, or simply a failed hard drive. Many small businesses never recover from major disasters simply because they haven't tested whether their backups actually work or clarified who does what when systems go down. This month, gather your team and walk through what would happen if your most critical system failed tomorrow: Who would you call? Where are your backups stored? How long would it take to get back up and running? **Take action today:** Schedule 30 minutes on your calendar right now to verify that your most recent backup can actually be restored—don't just assume it works.

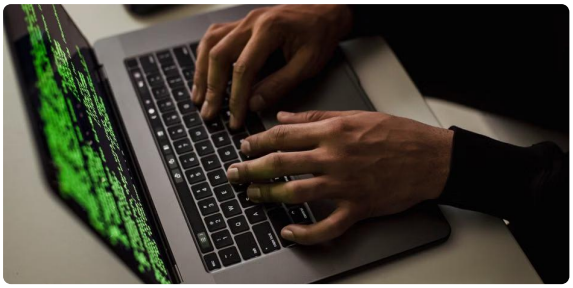
ACTION ITEM

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

SMB SPOTLIGHT

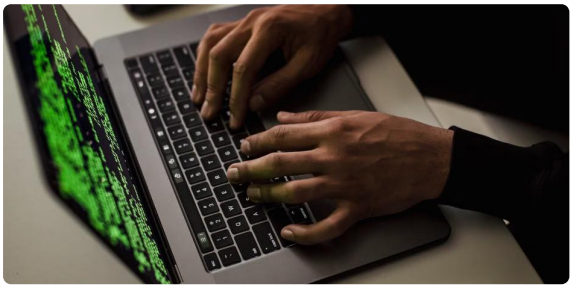
Protecting Your Business

The hidden risks of shadow AI



Disruptive cyber activity highlights risk from internet-exposed systems and edge devices

Managing the cyber risk of agentic AI



How BitLocker PINs help protect your data and devices

INNOVATION

Cybersecurity Advancements

New Warnings About the Risks of AI to Humanity Revive a Long-Running Debate

Personal, Financial Info Exposed in Revolut Data Breach

The Race to Control AI and Protect What Makes Us Human

Chinese Hackers Exploit Critical Tencent Software Flaw for One-Click Code Execution

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 clear picture: the attack surface isn't just expanding—it's evolving faster than our validation methods can keep up. What strikes me most is the common thread running through these stories, from OAuth token leaks to passkey phishing and AI-driven vulnerabilities. Attackers aren't just finding new doors to kick down; they're exploiting the trust mechanisms we've built into our modern systems.

Here's what keeps me up at night: we're still validating security using yesterday's playbook while threats are being written with tomorrow's technology. When CISA flags actively exploited vulnerabilities in tools like Artifactory and ScreenConnect—platforms many businesses depend on daily—it's a wake-up call that validation can't be a quarterly checkbox exercise anymore.

The good news? Awareness is the first line of defense. If your organization is adopting AI tools or cloud services, now's the time to ask hard questions about how you're validating access, monitoring for anomalies, and responding to threats. Don't wait for a breach to test your defenses. Let's have that conversation today.

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