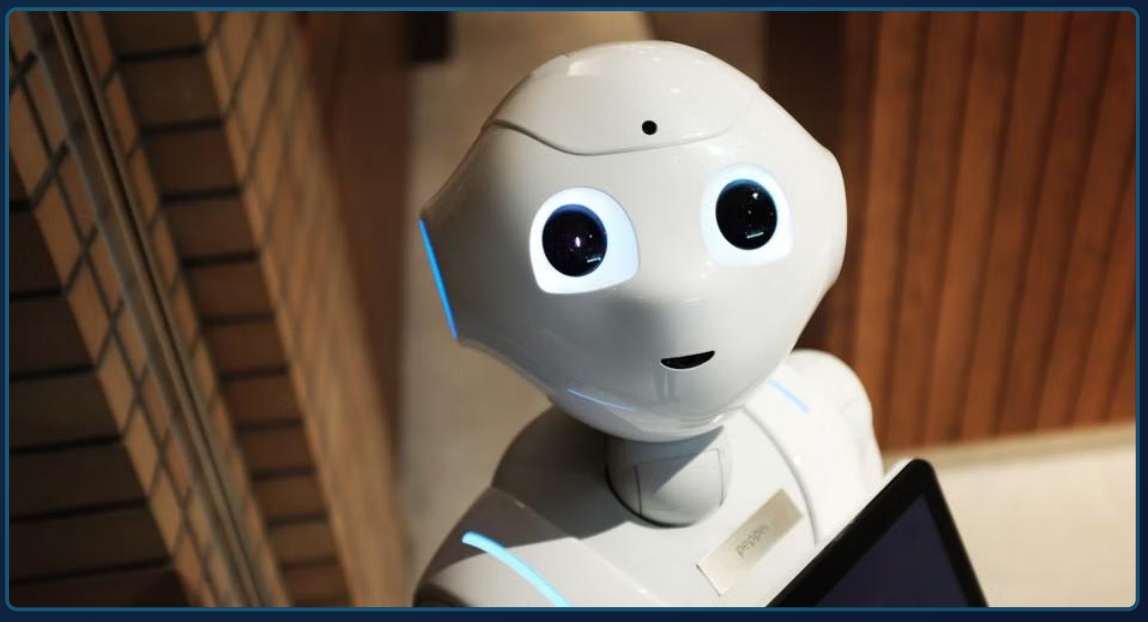
Intelligent Automation

Solutions that are powered by a SECURE Cloud.

MCSP

Managed Cybersecurity Service Provider



VOL. 1 · ISSUE 45

Cyber Shield

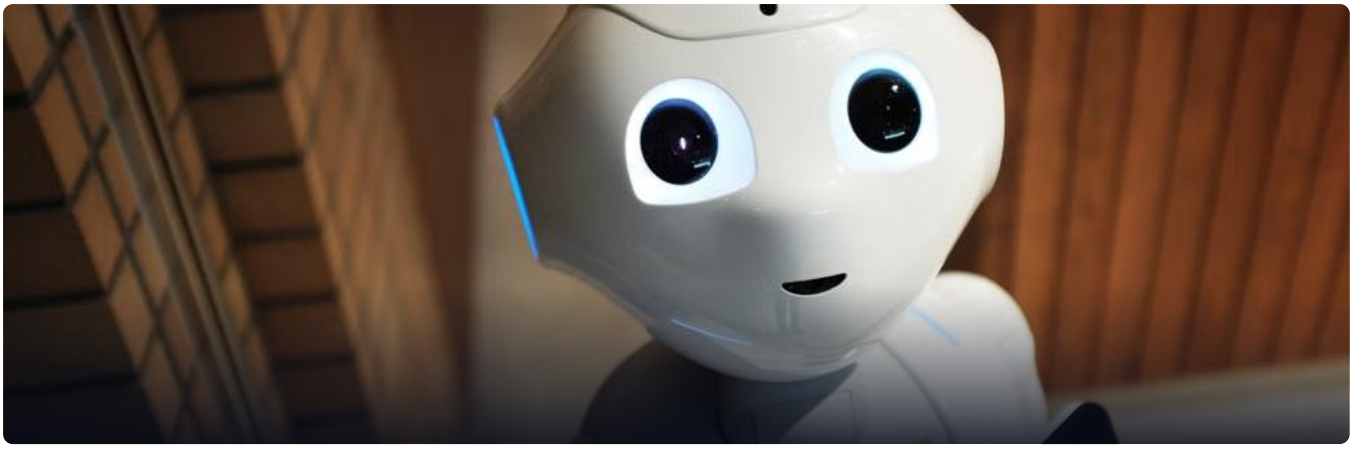
August 03, 2026

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



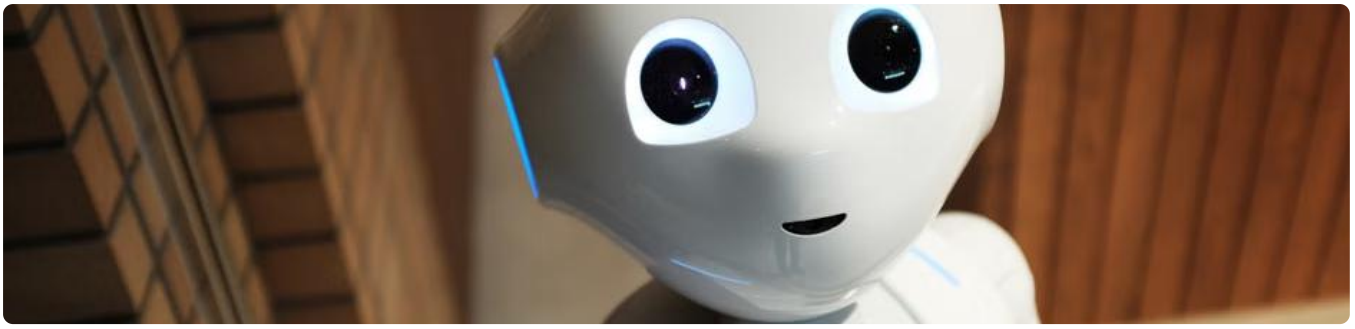
FOMO in the SOC: Where AI Platforms like Claude Actually Fit

Chinese Threat Actor Uses Leaked DarkSword Kit to Deploy GHOSTBLADE on iOS

PNLD Breach Exposes U.K. Police and Government Contact Details on Dark Web

INTEL

Cyber Threat Intelligence



FOMO in the SOC: Where AI Platforms like Claude Actually Fit

Chinese Threat Actor Uses Leaked DarkSword Kit to Deploy GHOSTBLADE on iOS

PNLD Breach Exposes U.K. Police and Government Contact Details on Dark Web

INTEL

Threat Intelligence — Continued

Thermo Fisher Patches Flaw That Could Make DNA File Tampering Nearly Undetectable

N-able Says Attackers Take Over N-central Servers After Initial Fix Proves Incomplete

Hugging Face Diffusers Flaws Could Let Model Repositories Execute Arbitrary Code

ISC Stormcast For Monday, August 3rd, 2026 https://isc.sans.edu/podcastdetail/10034, (Mon, Aug 3rd)

Atomic MacOS (AMOS) stealer infection, (Sun, Aug 2nd)

💡 WEEKLY TECH TIP

Don't Trust a Single Patch During Active Attacks

The N-able incident shows attackers can persist even after vendors issue fixes, exploiting gaps between initial and complete patches. When critical vulnerabilities affect your systems, assume the first patch may be incomplete and attackers are actively testing workarounds.

Step 1: Apply vendor patches immediately but treat them as temporary until confirmed complete.

Step 2: Monitor affected systems closely for 72 hours post-patch for unusual activity or connections.

Step 3: Review access logs from before the patch to identify potential compromise signs.

Step 4: Subscribe to vendor security advisories to catch follow-up patches within hours of release.

ALERTS

National Cybersecurity Alerts

ISC Stormcast For Monday, August 3rd, 2026 https://isc.sans.edu/podcastdetail/10034, (Mon, Aug 3rd)

Atomic MacOS (AMOS) stealer infection, (Sun, Aug 2nd)

Phishing Campaigns Targeting AI Solutions Providers, (Sat, Aug 1st)

zipdump.py: Metadata Encoding, (Fri, Jul 31st)

REGIONAL

Regional & Sector-Specific Alerts

ISC Stormcast For Monday, August 3rd, 2026 https://isc.sans.edu/podcastdetail/10034, (Mon, Aug 3rd)

Atomic MacOS (AMOS) stealer infection, (Sun, Aug 2nd)

Phishing Campaigns Targeting AI Solutions Providers, (Sat, Aug 1st)

AUGUST AWARENESS

Back to School / New Devices

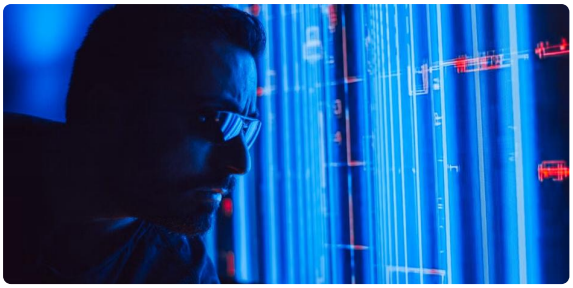
Security Awareness Spotlight: Back to School / New Devices August means new laptops, tablets, and phones entering your business as employees return from summer break and students join part-time. Before connecting any new device to your network, require that it's updated with the latest security patches, has antivirus software installed, and is registered with your IT team or management system—treat these steps like checking someone's ID before letting them through your front door. Today, create a simple "new device checklist" and email it to your team so everyone knows the rules before plugging in that shiny new gadget.

ACTION ITEM

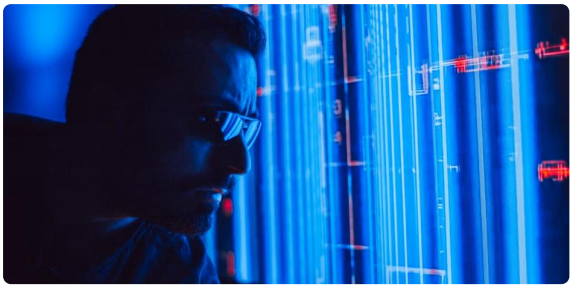
Schedule a 15-minute team security review this week using this month's theme as your agenda.

SMB SPOTLIGHT

Protecting Your Business



Making forensic observability the norm for network devices



When cyber attacks happen: helping organisations recover

UK and partners expose Russian state-supported actors for new ‘zero-click’ phishing campaign targeting Western organisations

Post-quantum cryptography (PQC) migration workshop report

INNOVATION

Cybersecurity Advancements

River Bank Says Hackers Deleted Data Stolen in Ransomware Attack

Horizon3 Raises $250 Million to Fund Continuing Growth

N-able Patches Vulnerability Exploited to Hack N-central Servers

Brinks Home Discloses Data Breach as Hackers Leak Files

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 tell a familiar story, but one detail stands out to me: N-able's attackers exploited servers even after an initial fix was deployed. It's a sobering reminder that in cybersecurity, "fixed" doesn't always mean "secure."

I've seen this pattern repeatedly over my career. Organizations rush to patch a vulnerability, breathe a sigh of relief, then discover the fix was incomplete or that attackers had already established persistence. The N-able incident underscores why incident response can't end with applying a patch. You need verification, monitoring, and often a deeper investigation to ensure the threat is truly contained.

For smaller businesses relying on managed service providers, this raises an important question: does your provider follow through? When they say something is patched, are they actually validating that the fix worked and that no compromise occurred beforehand?

The good news is that asking this question already puts you ahead of most organizations. Don't hesitate to have frank conversations with your security partners about their incident response protocols. Your vigilance makes their job easier and your business more secure.

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