



VOL. 1 · ISSUE 55

Cyber Shield

October 12, 2026

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

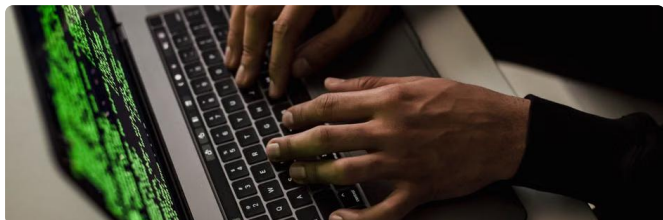
INTELLIGENT AUTOMATION, LLC · INTELAMATION.COM · FAIRFIELD, NJ

FEATURE

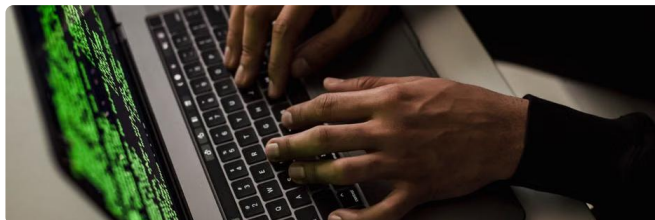
This Week in Cybersecurity



Bring Your Own Agent: Your Employees' Assistants Are Already Logged In



Ledger Finds Unauthorized Hardware Implant in CryptoBilis-Sold Wallet Amid Fund Theft Reports



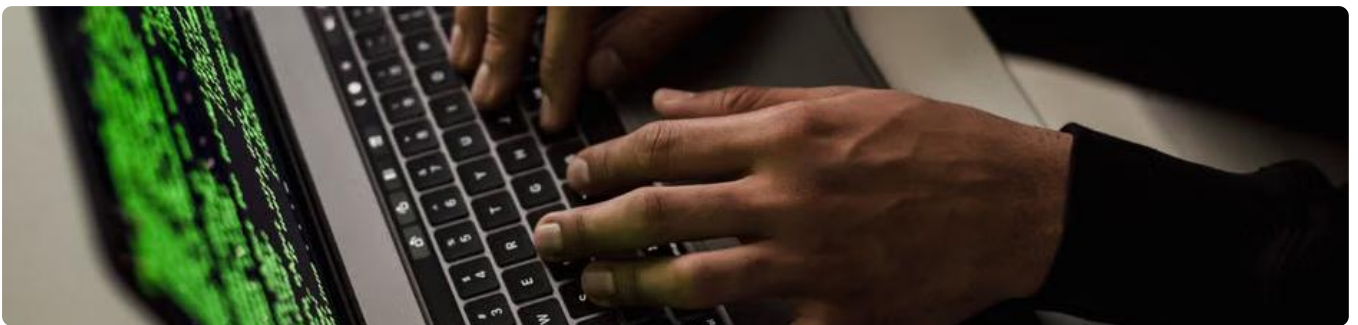
Critical SonicWall SMA 1000 Flaw Targeted in 135 Exploitation Attempts After Patch

INTEL

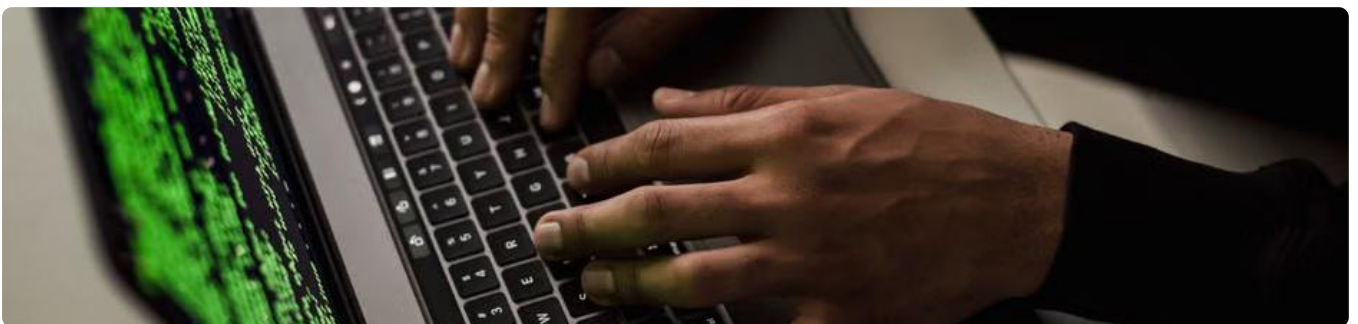
Cyber Threat Intelligence



Bring Your Own Agent: Your Employees' Assistants Are Already Logged In



Ledger Finds Unauthorized Hardware Implant in CryptoBilis-Sold Wallet Amid Fund Theft Reports



Critical SonicWall SMA 1000 Flaw Targeted in 135 Exploitation Attempts After Patch

INTEL

Threat Intelligence — Continued

Attackers Exploit CVSS 10.0 Bricksforge WordPress Flaw Enabling Unauthenticated RCE

CyberXero Uses Claude Code in Campaign That Stole Over 628,000 Ukrainian Records

P7 DarkSword iOS Exploit Kit Adds Crypto Wallet Data Theft and Remote Commands

ISC Stormcast For Monday, October 12th, 2026 <https://isc.sans.edu/podcastdetail/10132>, (Mon, Oct 12th)

Why TLP should not replace your internal information classification, (Sat, Oct 10th)

 WEEKLY TECH TIP

Lock Down AI Assistants Before They Unlock Your Data

Employees are connecting AI assistants like ChatGPT and Claude to corporate systems, creating unauthorized access points to sensitive data. These "bring your own agent" tools inherit your employees' permissions and can expose confidential information through poor prompts or compromised sessions.

Step 1: Audit which AI tools employees are using and what corporate accounts they've connected.

Step 2: Establish clear policies prohibiting AI assistant connections to sensitive business systems and data.

Step 3: Implement application controls to block unauthorized AI tools on corporate networks and devices.

Step 4: Train staff on secure AI usage and risks of sharing proprietary information with assistants.

ALERTS

National Cybersecurity Alerts

ISC Stormcast For Monday, October 12th, 2026 <https://isc.sans.edu/podcastdetail/10132>, (Mon, Oct 12th)

Why TLP should not replace your internal information classification, (Sat, Oct 10th)

ISC Stormcast For Friday, October 9th, 2026 <https://isc.sans.edu/podcastdetail/10130>, (Fri, Oct 9th)

Reconstructing AI Agent Activity: Two New Scripts for Forensic Review, (Thu, Oct 8th)

REGIONAL

Regional & Sector-Specific Alerts

ISC Stormcast For Monday, October 12th, 2026 <https://isc.sans.edu/podcastdetail/10132>, (Mon, Oct 12th)

Why TLP should not replace your internal information classification, (Sat, Oct 10th)

ISC Stormcast For Friday, October 9th, 2026 <https://isc.sans.edu/podcastdetail/10130>, (Fri, Oct 9th)

 OCTOBER AWARENESS

Cybersecurity Awareness Month

October is Cybersecurity Awareness Month, which makes it the perfect time to strengthen your team's defenses against scams and attacks. Most data breaches happen because someone clicks a malicious link or falls for a fake email, so your employees are truly your first line of defense. Today, send your team a simple reminder email with three actions to take if they accidentally click a suspicious link: disconnect from WiFi immediately, don't enter any passwords, and report it to you or your IT person right away.

ACTION ITEM

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

SMB SPOTLIGHT

Protecting Your Business



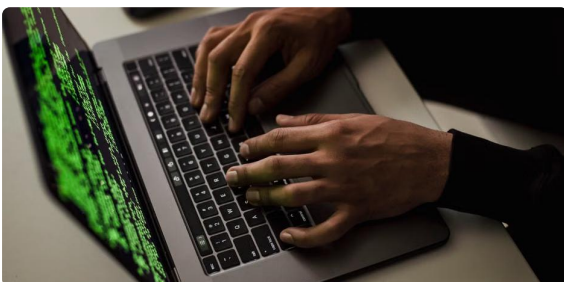
Help the NCSC understand how organisations approach external attack surface risk



China-linked malicious actors called out by UK and international partners for targeting sensitive data globally



Incident affecting ASOS customers



Exploitation of vulnerabilities affecting Citrix NetScaler ADC and Citrix NetScaler Gateway

INNOVATION

Cybersecurity Advancements

Bricksforge WordPress Plugin Vulnerability Exploited in the Wild

Canonical Websites Disrupted in Second DDoS Attack This Year

Mastermind of 15,000-Mule Cybercrime Laundering Network Pleads Guilty in US

iRhythm Data Breach Impacts at Least 360,000 People

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: the erosion of our traditional security perimeter. Whether it's employees bringing AI assistants into your network, compromised hardware arriving from suppliers, or attackers exploiting critical vulnerabilities before most organizations can patch them, the message is clear—we can no longer rely on simple perimeter defenses.

What concerns me most is the BYOA trend. Your team is already using ChatGPT, Claude, and other AI tools, often with company credentials and sensitive data. They're solving problems faster, but they're also creating shadow IT risks we haven't fully addressed. Combined with supply chain compromises like the Ledger implant and weaponized AI campaigns like CyberXero, we're facing threats that bypass traditional controls entirely.

The good news? You don't need to ban innovation or live in fear. Start by having honest conversations with your team about the tools they're using. Implement basic monitoring for anomalous access patterns. And yes, prioritize patching—those SonicWall attacks prove that criminals move fast.

Security isn't about building higher walls anymore; it's about visibility and rapid response. Let's talk about what that means for your organization.

CONNECT WITH DANIELlinkedin.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

© 2026 Intelligent Automation, LLC · All rights reserved