Intelligent Automation

Solutions that are powered by a SECURE Cloud.

MCSP

Managed Cybersecurity Service Provider

VOL. 1 · ISSUE 50

Cyber Shield

September 07, 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

Your Cloud Security Checklist Doesn't Work the Way You Think It Does

Rogue ScreenConnect Clients Spread Four-Stage VBScript Chain to Newly Connected Hosts

Telerik UI Padding-Oracle Bug Chained to Unauthenticated RCE — Public Exploit Released

INTEL

Cyber Threat Intelligence

Your Cloud Security Checklist Doesn't Work the Way You Think It Does

Rogue ScreenConnect Clients Spread Four-Stage VBScript Chain to Newly Connected Hosts

Telerik UI Padding-Oracle Bug Chained to Unauthenticated RCE — Public Exploit Released

INTEL

Threat Intelligence — Continued

N-able Issues Fourth N-central Hotfix in Five Weeks for Unauthenticated RCE Flaw

JSCeal Malware Can Bypass Google Authentication Using Stolen Session Cookies

Attackers Hijack MikroTik Routers Through Internet-Exposed SSH Without Authentication

Critical MikroTik Vulnerability - Patch Now, (Sun, Sep 6th)

numbat - AI agent observability, (Fri, Sep 4th)

💡 WEEKLY TECH TIP

Session Cookies Aren't Protected by Two-Factor Authentication

Malware like JSCeal can steal browser session cookies to bypass your multi-factor authentication completely. Even with strong passwords and 2FA enabled, attackers maintaining access through stolen sessions remain a critical blind spot.

Step 1: Enable session timeout policies forcing re-authentication every 8-12 hours across all business applications.

Step 2: Deploy endpoint detection software that monitors for suspicious cookie access and exfiltration attempts.

Step 3: Bind sessions to device fingerprints so stolen cookies won't work from different machines.

Step 4: Train staff to sign out completely when finishing work, not just closing browsers.

ALERTS

National Cybersecurity Alerts

Critical MikroTik Vulnerability - Patch Now, (Sun, Sep 6th)

numbat - AI agent observability, (Fri, Sep 4th)

ISC Stormcast For Friday, September 4th, 2026 https://isc.sans.edu/podcastdetail/10082, (Fri, Sep 4th)

Honeypot-Omaha and batch.py [Guest Diary], (Wed, Sep 2nd)

REGIONAL

Regional & Sector-Specific Alerts

Critical MikroTik Vulnerability - Patch Now, (Sun, Sep 6th)

numbat - AI agent observability, (Fri, Sep 4th)

ISC Stormcast For Friday, September 4th, 2026 https://isc.sans.edu/podcastdetail/10082, (Fri, Sep 4th)

SEPTEMBER AWARENESS

Disaster Recovery Month

September is Disaster Recovery Month, and there's no better time to ensure your business can survive when things go wrong—whether that's a ransomware attack, a fire, a flood, or simply a failed hard drive. Most small businesses never recover from a major disaster because they haven't tested whether their backups actually work or confirmed that key employees know what to do in an emergency. Today, schedule 30 minutes with your team to walk through one disaster scenario step-by-step: if your office became inaccessible right now, does everyone know how to reach each other, access critical files, and keep serving customers?

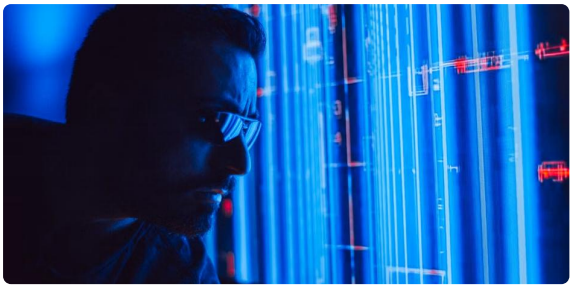
ACTION ITEM

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

SMB SPOTLIGHT

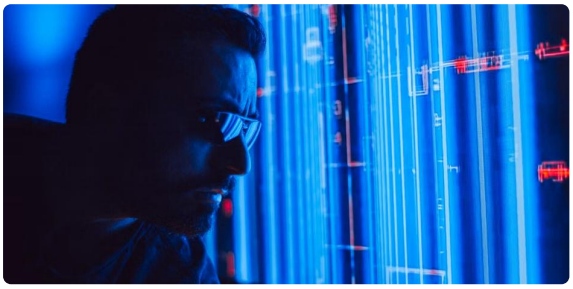
Protecting Your Business

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

Nightmare Eclipse Drops CrowdStrike, Nvidia, Avast Zero-Day Exploits

North Korean Hackers Deploy New Linux Espionage Toolkit

OpenAI Agents Hijack Another Victim Website

Adobe Commerce Zero-Day Exploited to Backdoor Online Stores

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 troubling story that keeps me up at night: the tools we trust to protect us are becoming our greatest vulnerabilities. Four of the five major threats we're tracking exploit legitimate software — ScreenConnect, Telerik UI, N-central, and even Google Authentication. These aren't obscure applications. They're enterprise-grade platforms that thousands of businesses depend on daily.

Here's what concerns me most. When attackers compromise trusted software, they bypass our natural defenses. Your team doesn't question ScreenConnect connections or authenticated Google sessions because they're supposed to be safe. That's precisely what makes these attacks so effective.

The lesson isn't to abandon these platforms. It's to fundamentally shift how we think about trust in our environments. Every authenticated session needs validation. Every remote access tool requires monitoring. Every third-party component deserves scrutiny, regardless of its reputation.

I encourage you to review your vendor management practices this week. Ask yourself: if one of your trusted tools was compromised tomorrow, would you detect it? If the answer gives you pause, let's talk about closing that gap.

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