Intelligent Automation

Solutions that are powered by a SECURE Cloud.

MCSP

Managed Cybersecurity Service Provider

VOL. 1 · ISSUE 37

Cyber Shield

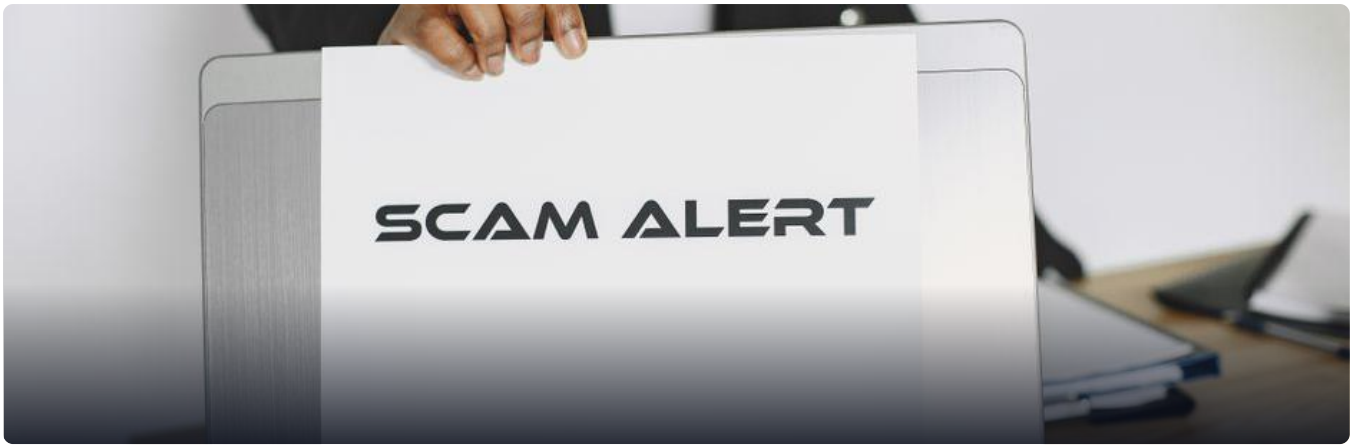
June 08, 2026

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



Meta Blocks NSO Group's New WhatsApp Phishing Attack, Files Contempt Order

Critical Check Point VPN Flaw Exploited to Bypass Passwords in IKEv1 Setups

AI Phishing Is Crushing SOCs with Alert Volume: How to Reduce Tier 1 Overload

INTEL

Cyber Threat Intelligence

Meta Blocks NSO Group's New WhatsApp Phishing Attack, Files Contempt Order

Critical Check Point VPN Flaw Exploited to Bypass Passwords in IKEv1 Setups

AI Phishing Is Crushing SOCs with Alert Volume: How to Reduce Tier 1 Overload

INTEL

Threat Intelligence — Continued

⚡ Weekly Recap: Instagram Account Hacks, Android Zero-Day, GitHub Worm and More

The Hardest Fork

VerdantBamboo Deploys BSD Variant of BRICKSTORM on Linux Appliances

TeamPCP Supply Chain Campaign: Activity Through 2026-06-07, (Mon, Jun 8th)

ISC Stormcast For Monday, June 8th, 2026 https://isc.sans.edu/podcastdetail/9962, (Mon, Jun 8th)

WEEKLY TECH TIP

Audit Your VPN Now: Critical Flaws Demand Immediate Action

Recent exploits targeting Check Point VPNs show attackers can bypass password authentication through outdated protocols. Legacy VPN configurations create invisible backdoors that cybercriminals actively exploit to gain network access.

Step 1: Immediately verify your VPN uses IKEv2 protocol, not vulnerable IKEv1 configurations.

Step 2: Apply all pending security patches from your VPN vendor within 48 hours.

Step 3: Enable multi-factor authentication for all VPN connections without exception.

Step 4: Schedule quarterly VPN security audits with your IT team or provider.

ALERTS

National Cybersecurity Alerts

TeamPCP Supply Chain Campaign: Activity Through 2026-06-07, (Mon, Jun 8th)

ISC Stormcast For Monday, June 8th, 2026 https://isc.sans.edu/podcastdetail/9962, (Mon, Jun 8th)

The Evil MSI Background is Back!, (Fri, Jun 5th)

ISC Stormcast For Friday, June 5th, 2026 https://isc.sans.edu/podcastdetail/9960, (Fri, Jun 5th)

REGIONAL

Regional & Sector-Specific Alerts

TeamPCP Supply Chain Campaign: Activity Through 2026-06-07, (Mon, Jun 8th)

ISC Stormcast For Monday, June 8th, 2026 https://isc.sans.edu/podcastdetail/9962, (Mon, Jun 8th)

The Evil MSI Background is Back!, (Fri, Jun 5th)

JUNE AWARENESS

Internet Safety Month

Security Awareness Spotlight: Internet Safety Month June is Internet Safety Month, and it's the perfect time to strengthen your team's first line of defense against cyber threats. Most data breaches start with a simple phishing email or a visit to a compromised website, which means your employees' daily browsing and email habits directly impact your business's security. Schedule a 15-minute team meeting today to show everyone how to spot suspicious emails by hovering over links before clicking, checking sender addresses carefully, and reporting anything that feels off to you immediately.

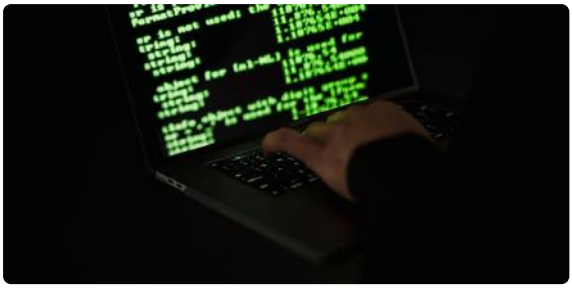
ACTION ITEM

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

SMB SPOTLIGHT

Protecting Your Business

Software supply chain attacks: check your dependencies



Designing secure access with ZTNA

Thinking carefully before adopting agentic AI

10 questions to ask when using AI models to find vulnerabilities

INNOVATION

Cybersecurity Advancements

A Security Raises $37 Million for Autonomous Offensive Security Platform

Everybody Is Vibe Coding But Nobody Told the Security Team

WhatsApp Catches Spyware Firm NSO Defying No-Hacking Court Order

Cybersecurity M&A Roundup: 26 Deals Announced in May 2026

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 reveal a troubling pattern I need you to understand: sophisticated attackers are simultaneously exploiting both cutting-edge AI and legacy infrastructure vulnerabilities. While everyone's buzzing about AI-generated phishing campaigns overwhelming security teams, the Check Point VPN flaw reminds us that yesterday's "set it and forget it" systems remain prime targets today.

Here's what keeps me up at night—and should concern you too. That VPN you configured five years ago? The one quietly protecting remote workers? It might be running IKEv1, and attackers are actively bypassing authentication as we speak. Meanwhile, AI-powered phishing has become so convincing and voluminous that even trained analysts struggle to keep pace.

The good news is you don't have to choose between defending against tomorrow's AI threats and yesterday's unpatched systems. Start with a simple audit of your remote access infrastructure this week. Verify every VPN is updated and properly configured. Then let's talk about how managed detection can help your team separate signal from noise in this AI-amplified threat landscape.

The best defense isn't just technology—it's knowing where you're actually vulnerable.

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