Intelligent Automation

Solutions that are powered by a SECURE Cloud.

MCSP

Managed Cybersecurity Service Provider

VOL. 1 · ISSUE 49

Cyber Shield

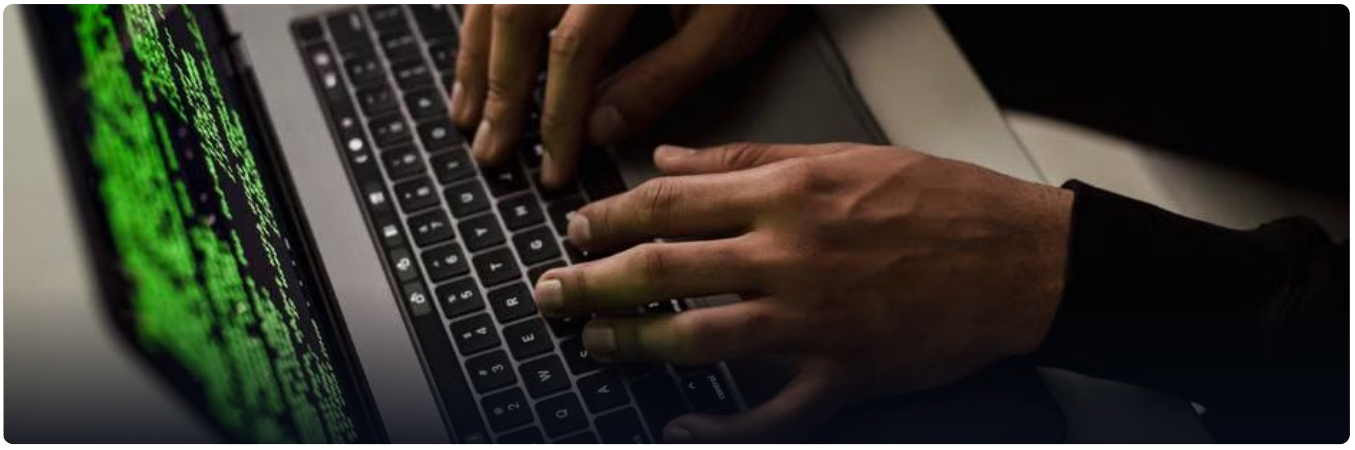
August 31, 2026

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

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

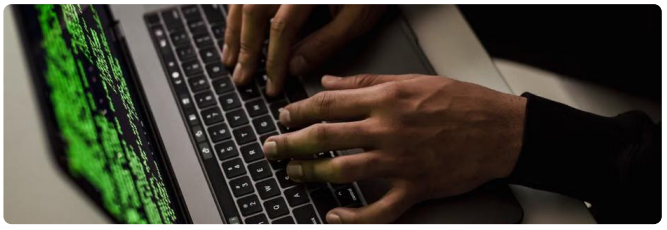
FEATURE

This Week in Cybersecurity



ValleyRAT Backdoor Hides in Signed Adware That Users Add to Antivirus Exclusions

Aurora Ransomware Operators Use Cursor AI in Attacks Against 10 Targets



Securing Claude Code: The New Compliance API, Local Visibility, and Identity Governance

INTEL

Cyber Threat Intelligence

ValleyRAT Backdoor Hides in Signed Adware That Users Add to Antivirus Exclusions

Aurora Ransomware Operators Use Cursor AI in Attacks Against 10 Targets

Securing Claude Code: The New Compliance API, Local Visibility, and Identity Governance

INTEL

Threat Intelligence — Continued

China-Linked Fire Ant Hijacks Cisco Routers to Steal Credentials and Blind Security Logs

DoJ Corrects China Hacking Claim, Says U.S. Agencies Were Targets, Not Victims

TerminalFix Uses Fake Cloudflare CAPTCHAs to Deploy Reverse-Tunnel Backdoor

ISC Stormcast For Monday, August 31st, 2026 https://isc.sans.edu/podcastdetail/10074, (Mon, Aug 31st)

YARA-X 1.20.0 Release, (Sun, Aug 30th)

💡 WEEKLY TECH TIP

Don't Trust Antivirus Exclusions Without Verification

Attackers are hiding malware in legitimate-looking signed software, then tricking users into adding it to antivirus exclusions. Once excluded, these threats operate undetected on your systems.

Step 1: Create a policy requiring IT approval before adding any antivirus exclusions.

Step 2: Regularly audit existing exclusion lists and remove unnecessary entries every quarter.

Step 3: Verify digital signatures match known publishers before trusting any software requests.

Step 4: Train employees never to disable security tools based on software prompts.

ALERTS

National Cybersecurity Alerts

ISC Stormcast For Monday, August 31st, 2026 https://isc.sans.edu/podcastdetail/10074, (Mon, Aug 31st)

YARA-X 1.20.0 Release, (Sun, Aug 30th)

Some Malicious PE Stats, (Thu, Aug 27th)

ISC Stormcast For Friday, August 28th, 2026 https://isc.sans.edu/podcastdetail/10072, (Fri, Aug 28th)

REGIONAL

Regional & Sector-Specific Alerts

ISC Stormcast For Monday, August 31st, 2026 https://isc.sans.edu/podcastdetail/10074, (Mon, Aug 31st)

YARA-X 1.20.0 Release, (Sun, Aug 30th)

Some Malicious PE Stats, (Thu, Aug 27th)

AUGUST AWARENESS

Back to School / New Devices

Security Awareness Spotlight: Back to School / New Devices August means new laptops, tablets, and phones for students and employees, but each one is a potential doorway for hackers if not properly secured. Before anyone connects a new device to your business network or accesses company email, make sure it has up-to-date security software installed, all available updates applied, and a strong password or PIN protecting it. Today, create a simple checklist for your team: "No new device connects until IT (or you) approves it" — then print it and tape it next to your router or on your office door.

ACTION ITEM

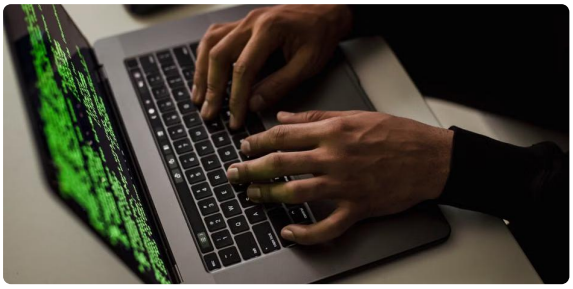
Schedule a 15-minute team security review this week using this month's theme as your agenda.

SMB SPOTLIGHT

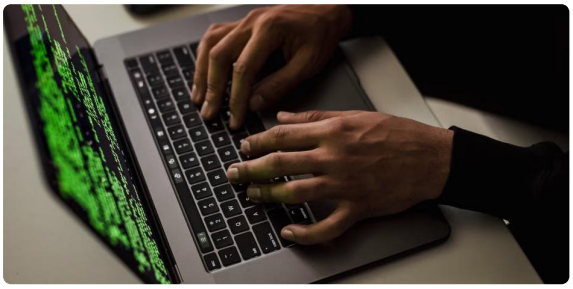
Protecting Your Business

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



Help shape the future of resilient private 5G

INNOVATION

Cybersecurity Advancements

ServiceNow Patches 3 Critical Code Injection Vulnerabilities

McKesson Confirms Data Breach as Attacker Deadline Looms

What the Hugging Face Incident Teaches Security Leaders About AI Agent Access

Anthropic Warns Claude Users of Infostealer Malware Infections

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: cybercriminals are weaponizing our trust. The ValleyRAT story particularly caught my attention because it exposes how attackers are exploiting the very tools we use to protect ourselves.

Think about it. Users are actively adding malicious software to their antivirus exclusion lists, believing they're installing legitimate adware. It's signed code, so it appears trustworthy. Meanwhile, threat actors are sitting back and watching organizations literally disable the defenses that would stop them.

This isn't just a technical problem—it's a human one. Your employees need to understand that digital signatures and professional-looking installers don't guarantee safety. The most sophisticated cyberattacks today don't break down your front door; they walk right through it wearing a convincing disguise.

At Intelligent Automation, we're seeing this social engineering trend accelerate across all our clients. The good news? Awareness is your strongest defense. Take thirty minutes this week to remind your team: when something asks to be excluded from security scanning, that's your red flag. Question it, verify it, and when in doubt, call us.

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