Intelligent Automation

Solutions that are powered by a SECURE Cloud.

MCSP

Managed Cybersecurity Service Provider

VOL. 1 · ISSUE 52

Cyber Shield

September 21, 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

ClickFix Lures Deploy ChainScript RAT Using Polygon to Rotate C2 Infrastructure

Jade Sleet Linked to Indian IT Provider Breach With FLATROOF and ROOFDECK Backdoors

Claude Opus 5 Helped Researchers Take Over OpenAI Staff Accounts via Chained Flaws

INTEL

Cyber Threat Intelligence

ClickFix Lures Deploy ChainScript RAT Using Polygon to Rotate C2 Infrastructure

Jade Sleet Linked to Indian IT Provider Breach With FLATROOF and ROOFDECK Backdoors

Claude Opus 5 Helped Researchers Take Over OpenAI Staff Accounts via Chained Flaws

INTEL

Threat Intelligence — Continued

Can You Prove a New CVE Is Exploitable Before Attackers Do? Learn How in This Webinar

Identity Visibility in 2026: The Foundation of Identity Security

SolarWinds Patches ARM Hard-Coded Key Flaw Enabling Unauthenticated RCE

TerminalFix: PNG Steganography, (Mon, Sep 21st)

ISC Stormcast For Monday, September 21st, 2026 https://isc.sans.edu/podcastdetail/10102, (Mon, Sep 21st)

💡 WEEKLY TECH TIP

Don't Click That Fix Button It's Malware

Cybercriminals are using fake error messages with "fix" buttons to trick users into downloading malware that gives attackers remote access to your systems. These convincing pop-ups appear on legitimate-looking websites and can bypass traditional security measures.

Step 1: Train employees to never click "fix" buttons on unexpected browser error messages.

Step 2: Close suspicious pop-ups using Task Manager, not the X button.

Step 3: Verify any system errors directly through your official IT support channels first.

Step 4: Enable browser security settings to block automatic downloads and suspicious scripts.

ALERTS

National Cybersecurity Alerts

TerminalFix: PNG Steganography, (Mon, Sep 21st)

ISC Stormcast For Monday, September 21st, 2026 https://isc.sans.edu/podcastdetail/10102, (Mon, Sep 21st)

HTTP QUERY Method: The Grey Zone Between GET And POST., (Fri, Sep 18th)

ISC Stormcast For Friday, September 18th, 2026 https://isc.sans.edu/podcastdetail/10100, (Fri, Sep 18th)

REGIONAL

Regional & Sector-Specific Alerts

TerminalFix: PNG Steganography, (Mon, Sep 21st)

ISC Stormcast For Monday, September 21st, 2026 https://isc.sans.edu/podcastdetail/10102, (Mon, Sep 21st)

HTTP QUERY Method: The Grey Zone Between GET And POST., (Fri, Sep 18th)

SEPTEMBER AWARENESS

Disaster Recovery Month

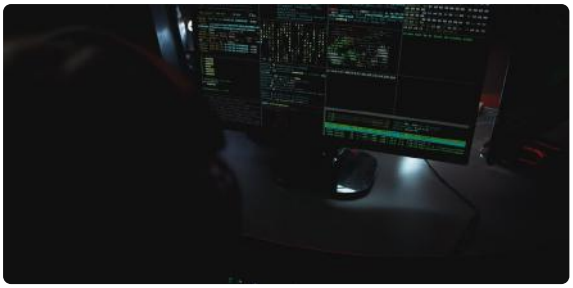
Security Awareness Spotlight: Disaster Recovery Month September is Disaster Recovery Month, and it's the perfect time to make sure your business can survive when things go wrong—whether that's a ransomware attack, a fire, a flood, or simply a failed hard drive. Most small businesses that lose their data for more than a few days never fully recover, yet many owners have never actually tested whether their backups work or confirmed everyone knows what to do in an emergency. Today, take 15 minutes to restore one file from your backup system to verify it actually works—if you can't do this simple test successfully, your disaster recovery plan is just wishful thinking.

ACTION ITEM

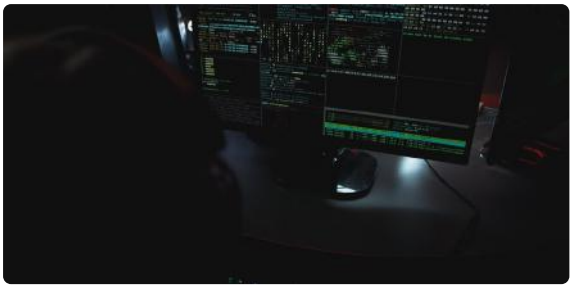
Schedule a 15-minute team security review this week using this month's theme as your agenda.

SMB SPOTLIGHT

Protecting Your Business

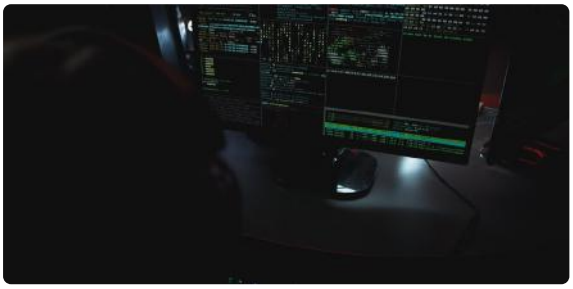


One does not simply defend agentically



Adversary simulation: what you need to know

Cyber Adversary Simulation (CyAS): scheme documents now available



Iranian cyber targeting of dissidents, activists and journalists

INNOVATION

Cybersecurity Advancements

RatHat Android Trojan Uses AI for Automation

Rust Team Members and Popular Crate Owners Targeted via Video Calls

CrowdSec Confirms Source Code Stolen in Supply Chain Attack

Colorado Water Utilities Hit by Cyberattacks Targeting OT Systems

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 story that should concern every business leader: attackers are evolving faster than most organizations can respond. What strikes me most isn't the technical sophistication of threats like ChainScript RAT or the Jade Sleet backdoors—it's the fundamental shift happening beneath the surface.

Look at the Claude Opus 5 incident where AI helped researchers compromise OpenAI staff accounts. We're entering an era where the same tools we use to defend ourselves can be weaponized against us with unprecedented speed and creativity. Meanwhile, the Jade Sleet breach reminds us that trusted IT providers can become unwitting gateways into your network.

Here's my takeaway: technical defenses alone won't save us anymore. The common thread in every story this week is identity—who has access, how we verify them, and how quickly we can detect anomalies. This is why identity visibility isn't just another buzzword; it's your first and last line of defense.

I encourage you to audit your identity infrastructure this week. Know who has access to what, review your provider relationships, and implement continuous monitoring. The threats are real, but so are the solutions.

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