Intelligent Automation

Solutions that are powered by a SECURE Cloud.

MCSP

Managed Cybersecurity Service Provider

VOL. 1 · ISSUE 44

Cyber Shield

July 27, 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

n8n Sandbox Escape Lets Workflow Editors Run OS Commands as the n8n Process

Operation BlueDash Deploys Level RMM and ScreenConnect via Fake Teams Update

Cruciferra Crypter Uses BYOVD and Process Ghosting to Hide Windows Malware

INTEL

Cyber Threat Intelligence

n8n Sandbox Escape Lets Workflow Editors Run OS Commands as the n8n Process

Operation BlueDash Deploys Level RMM and ScreenConnect via Fake Teams Update

Cruciferra Crypter Uses BYOVD and Process Ghosting to Hide Windows Malware

INTEL

Threat Intelligence — Continued

TELESHIM Abuses Telegram for C2 in Attacks Against Middle East Governments

GitHub Adds 3-Day Dependabot Cooldown to Limit Poisoned Package Adoption

Malvertising Sends Malware in Pieces, Then Makes the Browser Build the Executable

Java Spring Boot "heapdump" scans, (Mon, Jul 27th)

ISC Stormcast For Monday, July 27th, 2026 https://isc.sans.edu/podcastdetail/10024, (Mon, Jul 27th)

💡 WEEKLY TECH TIP

Verify Software Updates Before Installing Them

Attackers are distributing fake software updates that install remote access tools, giving them complete control over your systems. The recent Operation BlueDash campaign used fraudulent Microsoft Teams updates to compromise businesses.

Step 1: Always download updates directly from official vendor websites, never from email links.

Step 2: Hover over download buttons to verify URLs match the legitimate vendor domain.

Step 3: Enable automatic updates within applications to bypass fake update prompts entirely.

Step 4: Train employees to report suspicious update requests to IT before clicking.

ALERTS

National Cybersecurity Alerts

Java Spring Boot "heapdump" scans, (Mon, Jul 27th)

ISC Stormcast For Monday, July 27th, 2026 https://isc.sans.edu/podcastdetail/10024, (Mon, Jul 27th)

Scans for ESAFENET CDG 3 Document Management System Weak Logins, (Sun, Jul 26th)

ISC Stormcast For Friday, July 24th, 2026 https://isc.sans.edu/podcastdetail/10022, (Fri, Jul 24th)

REGIONAL

Regional & Sector-Specific Alerts

Java Spring Boot "heapdump" scans, (Mon, Jul 27th)

ISC Stormcast For Monday, July 27th, 2026 https://isc.sans.edu/podcastdetail/10024, (Mon, Jul 27th)

Scans for ESAFENET CDG 3 Document Management System Weak Logins, (Sun, Jul 26th)

JULY AWARENESS

System Administrator Day

Security Awareness Spotlight: System Administrator Day Your system administrator is the person who stands between your business and a data breach, working behind the scenes to patch vulnerabilities, monitor for threats, and recover from disasters. Yet many small businesses expect their IT person to work miracles without giving them access to proper security tools, training budgets, or even admin-level passwords to critical systems. This July, recognize that investing in your sysadmin's capabilities isn't just good for morale—it's essential for your business security. **Take action today: Schedule a 30-minute meeting with your IT person to ask what security tools or access they need but don't currently have.**

ACTION ITEM

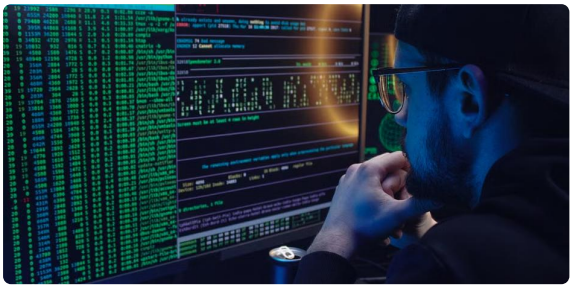
Schedule a 15-minute team security review this week using this month's theme as your agenda.

SMB SPOTLIGHT

Protecting Your Business

UK and partners expose Russian state-supported actors for new ‘zero-click’ phishing campaign targeting Western organisations

Post-quantum cryptography (PQC) migration workshop report



Helping small businesses with free, hands-on cyber consultancy

UK and Allies urge critical sectors to improve defences against Russian intelligence targeting

INNOVATION

Cybersecurity Advancements

PTC Windchill Vulnerability Exploited in Ransomware Campaign

MedusaHVNC Malware Uses Hidden Windows Desktops to Evade Detection

Nvidia and Tech Giants Launch AI Security Alliance

Coca-Cola Confirms Data Breach After Fairlife Ransomware Attack

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 threat landscape tells a sobering story that every business leader needs to understand: the tools we trust to make our work easier are increasingly becoming our greatest vulnerabilities.

Look at the pattern emerging from this week's incidents. The n8n workflow automation flaw, the fake Teams update delivering remote management tools, and even GitHub's response to package poisoning all point to the same reality: attackers have shifted their focus from breaking down doors to simply walking through the ones we've already opened. They're exploiting the legitimate software we rely on daily, knowing that we're less likely to question a Teams update than we are to click on a suspicious email from a Nigerian prince.

What strikes me most is how these aren't sophisticated zero-day exploits requiring nation-state resources. These are calculated attacks leveraging our trust in familiar tools and our dependency on automation. The attackers understand that in our rush toward digital transformation, security often takes a back seat to convenience.

The good news? Awareness is half the battle. Take thirty minutes this week to review what automation tools and remote access software your team is using, and verify that your security controls are actually monitoring them. Your future self will thank you.

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