Intelligent Automation

Solutions that are powered by a SECURE Cloud.

MCSP

Managed Cybersecurity Service Provider

VOL. 1 · ISSUE 48

Cyber Shield

August 24, 2026

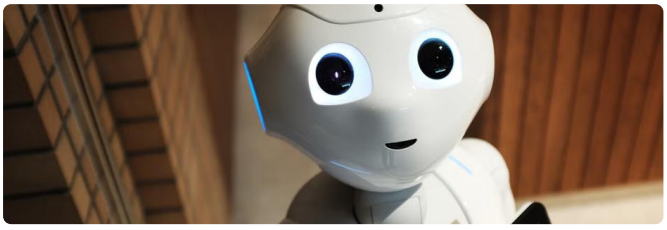
Essential cybersecurity intelligence for small and mid-sized businesses — powered by AI, delivered by Intelligent Automation, LLC.

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

FEATURE

This Week in Cybersecurity

WordlistLoader Delivers Amatera via ClickFix, SynkLoader Phishes Windows Passwords



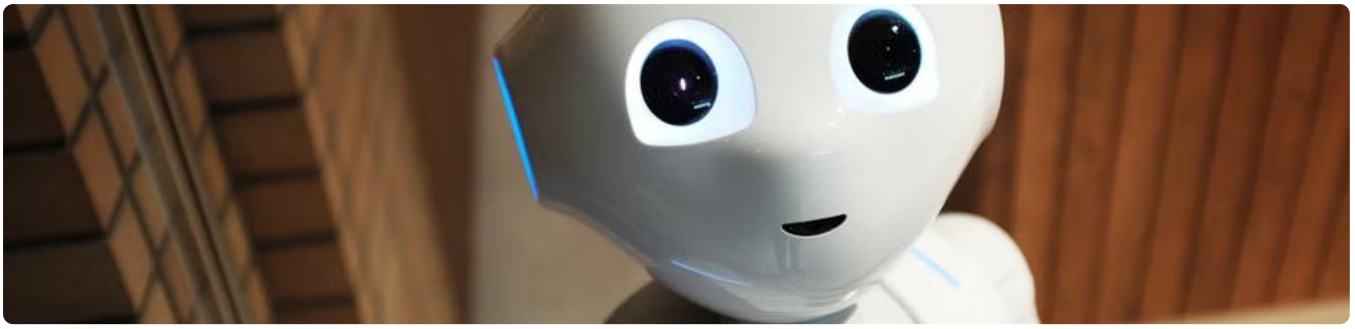
Shipping More AI Code Than You Can Secure? Watch How to Control Remediation Debt

Critical Keycloak Password Reset Flaw Could Let Unauthenticated Attackers Take Over Any Account

INTEL

Cyber Threat Intelligence

WordlistLoader Delivers Amatera via ClickFix, SynkLoader Phishes Windows Passwords



Shipping More AI Code Than You Can Secure? Watch How to Control Remediation Debt

Critical Keycloak Password Reset Flaw Could Let Unauthenticated Attackers Take Over Any Account

INTEL

Threat Intelligence — Continued

Operation QUICSILVER Targets Myanmar Government and IT with QUICAgent Backdoor

The Outsized Shadow: Why 5% of AI Users Are Your Biggest Security Risk

UAT-10147 Uses AI to Scale Server Attacks, Deploys SPECTRE With EDR Bypass and Linux Rootkit

DOUBLECUP's PNG Payload, (Mon, Aug 24th)

ISC Stormcast For Monday, August 24th, 2026 https://isc.sans.edu/podcastdetail/10064, (Mon, Aug 24th)

💡 WEEKLY TECH TIP

Verify Before You Click Password Reset Links

Attackers are exploiting password reset flows and social engineering tactics like ClickFix to deliver malware and steal credentials. A single compromised account can give attackers complete access to your business systems.

Step 1: Never click password reset links from unexpected emails, even if legitimate-looking.

Step 2: Go directly to the website by typing the URL yourself.

Step 3: Enable multi-factor authentication on all accounts, especially administrative and email accounts.

Step 4: Train employees monthly to recognize phishing attempts and report suspicious password requests.

ALERTS

National Cybersecurity Alerts

DOUBLECUP's PNG Payload, (Mon, Aug 24th)

ISC Stormcast For Monday, August 24th, 2026 https://isc.sans.edu/podcastdetail/10064, (Mon, Aug 24th)

Who Got Missed in the MFA Rollout? More Powershell + Graph + Entra scripting!, (Fri, Aug 21st)

ISC Stormcast For Friday, August 21st, 2026 https://isc.sans.edu/podcastdetail/10062, (Fri, Aug 21st)

REGIONAL

Regional & Sector-Specific Alerts

DOUBLECUP's PNG Payload, (Mon, Aug 24th)

ISC Stormcast For Monday, August 24th, 2026 https://isc.sans.edu/podcastdetail/10064, (Mon, Aug 24th)

Who Got Missed in the MFA Rollout? More Powershell + Graph + Entra scripting!, (Fri, Aug 21st)

AUGUST AWARENESS

Back to School / New Devices

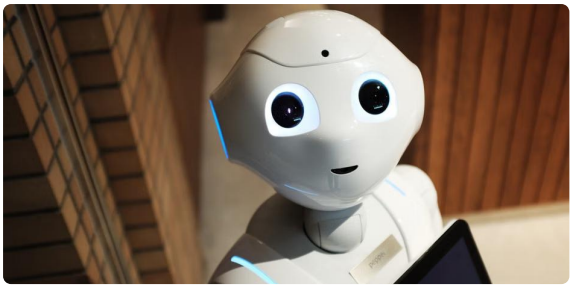
Security Awareness Spotlight: Back to School / New Devices August means new laptops, tablets, and phones for students and staff heading back to work, but every device that connects to your network is a potential door for hackers if it's not properly secured. Before anyone uses a new device for work—even their personal phone checking email—make sure it has the latest updates installed, antivirus software running, and requires a strong password or PIN to unlock. Today, create a simple checklist that every employee must complete before connecting any new device to your Wi-Fi or accessing company data, and send it to your team right now so everyone knows the rules before school starts.

ACTION ITEM

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

SMB SPOTLIGHT

Protecting Your Business



Managing the cyber risk of agentic AI

How BitLocker PINs help protect your data and devices

Help shape the future of resilient private 5G

Water sector example added to the NCSC's Secure connectivity principles

INNOVATION

Cybersecurity Advancements

Uber Fined Nearly $1 Billion by Dutch Regulators Over Automated Suspensions of Driver Accounts

91 Vulnerabilities Patched in Spring Application Framework

Venezuelan Gets Record Federal Prison Term for ATM Jackpotting

Personal Information Exposed in Apollo Global Data Breach

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 paint a troubling picture, but there's a silver lining if you know where to look. Whether it's WordlistLoader exploiting user trust through ClickFix tactics or SynkLoader phishing for credentials, the pattern is clear: attackers are increasingly manipulating human behavior rather than just exploiting software vulnerabilities.

What strikes me most isn't the sophistication of these attacks—it's how they all share a common denominator. The critical Keycloak flaw, the Myanmar government breach, even that statistic about five percent of AI users creating outsized risk—they all succeed when organizations lack visibility into who's doing what with their access privileges. We're shipping code faster than ever and adopting AI tools at breakneck speed, but our identity management practices haven't kept pace.

The good news? Unlike zero-day exploits that require vendor patches, you can take control of identity security right now. Start by auditing who has access to what, enforce multi-factor authentication everywhere, and establish clear policies around AI tool usage. These aren't sexy solutions, but they're the foundation that stops most attacks cold. Your security posture doesn't need to be perfect—it just needs to be stronger than the next target.

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