Intelligent Automation

Solutions that are powered by a SECURE Cloud.

MCSP

Managed Cybersecurity Service Provider

VOL. 1 · ISSUE 42

Cyber Shield

July 13, 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

Forg365 PhaaS Targets Microsoft 365 with Device Code and AitM Session Theft

Meta Files Patent for AI That Can Listen All Day and Track How You're Feeling

Thinking Fast and Slow in the SOC: The Case for Combining Autonomous AI with Analyst Copilots

INTEL

Cyber Threat Intelligence

Forg365 PhaaS Targets Microsoft 365 with Device Code and AitM Session Theft

Meta Files Patent for AI That Can Listen All Day and Track How You're Feeling

Thinking Fast and Slow in the SOC: The Case for Combining Autonomous AI with Analyst Copilots

INTEL

Threat Intelligence — Continued

Attacker Uses Suspected AI-Generated PowerShell Script to Map Active Directory

Misconfigured Server Reveals Three Evilginx Phishing Operations Targeting Microsoft 365

iCagenda and Balbooa Forms Joomla Flaws Reportedly Exploited as Zero-Days

Someone Is Scanning for Your MCP Servers and AI Assistant Credentials, (Mon, Jul 13th)

ISC Stormcast For Monday, July 13th, 2026 https://isc.sans.edu/podcastdetail/10004, (Mon, Jul 13th)

💡 WEEKLY TECH TIP

Defend Against Microsoft 365 Phishing and Session Hijacking

Sophisticated phishing attacks are now bypassing multi-factor authentication by stealing active sessions and using device code authentication tricks. These AI-powered threats specifically target Microsoft 365 credentials, making traditional security measures insufficient.

Step 1: Enable Conditional Access policies to restrict sign-ins from unfamiliar locations or devices.

Step 2: Disable device code authentication flow unless specifically required for legitimate business applications.

Step 3: Implement phishing-resistant authentication like passkeys, FIDO2 tokens, or Windows Hello for Business.

Step 4: Monitor sign-in logs weekly for suspicious session activity and impossible travel alerts.

ALERTS

National Cybersecurity Alerts

Someone Is Scanning for Your MCP Servers and AI Assistant Credentials, (Mon, Jul 13th)

ISC Stormcast For Monday, July 13th, 2026 https://isc.sans.edu/podcastdetail/10004, (Mon, Jul 13th)

Wireshark 4.6.7 Released, (Sat, Jul 11th)

My Stack Simulator, (Wed, Jul 8th)

REGIONAL

Regional & Sector-Specific Alerts

Someone Is Scanning for Your MCP Servers and AI Assistant Credentials, (Mon, Jul 13th)

ISC Stormcast For Monday, July 13th, 2026 https://isc.sans.edu/podcastdetail/10004, (Mon, Jul 13th)

Wireshark 4.6.7 Released, (Sat, Jul 11th)

JULY AWARENESS

System Administrator Day

July's System Administrator Appreciation Day is a perfect reminder that the person managing your technology systems is your first line of defense against hackers, data breaches, and costly downtime. If your system administrator is constantly firefighting problems instead of preventing them, or if they're locked out of critical systems because passwords are scattered across sticky notes and personal email accounts, they can't protect your business effectively. Today, schedule 30 minutes with your sysadmin to ask what tools, access, or training would make their security work easier—then commit to getting them at least one of those resources this quarter.

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 Allies urge critical sectors to improve defences against Russian intelligence targeting

Cyber Essentials Pathways: from proof of concept to cyber confidence

Cyber Shield: The path to an agentic AI future for cyber defence

Building more resilient CNI: what industry pen testers told us

INNOVATION

Cybersecurity Advancements

Cybersecurity M&A Roundup: 37 Deals Announced in June 2026

RabbitMQ Vulnerability Threatens Enterprise Systems

Zimbra Patches Critical Code Execution Vulnerability

EU Targets Russian Intelligence Officers Accused of Running a Yearslong Cyber Spying Campaign

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 unifying thread we can't ignore: attackers are increasingly sophisticated in their pursuit of one specific target—your Microsoft 365 environment.

From the Forg365 phishing-as-a-service platform to the Evilginx operations, cybercriminals are laser-focused on stealing Microsoft 365 credentials and session tokens. Why? Because once they're inside your M365 tenant, they have access to email, documents, financial data, and customer information—essentially your entire business.

What concerns me most is how these attacks bypass traditional defenses. Device code phishing tricks users into authenticating seemingly legitimate requests, while adversary-in-the-middle techniques steal active sessions, rendering even multi-factor authentication ineffective. Add AI-generated attack scripts to the mix, and we're seeing threats that adapt faster than ever before.

The good news is that awareness is half the battle. Now is the time to audit your Microsoft 365 security posture. Verify that conditional access policies are enforced, review authentication logs regularly, and ensure your team can recognize device code phishing attempts. Don't wait for a breach to discover your gaps—let's close them together today.

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