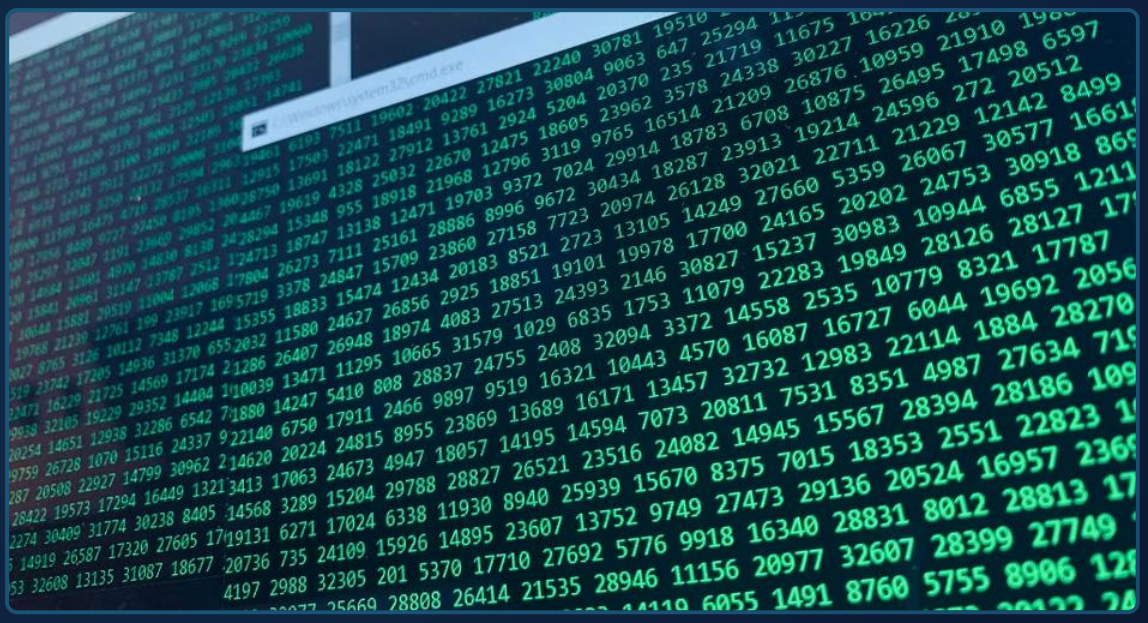
Intelligent Automation

Solutions that are powered by a SECURE Cloud.

MCSP

Managed Cybersecurity Service Provider



VOL. 1 · ISSUE 38

Cyber Shield

June 15, 2026

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

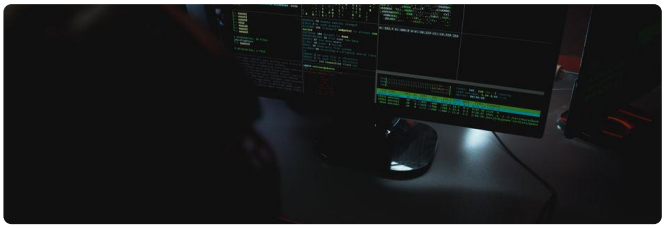
INTELLIGENT AUTOMATION, LLC · INTELAMATION.COM · FAIRFIELD, NJ

FEATURE

This Week in Cybersecurity

LiteLLM Vulnerability Chain Lets Low-Privilege Users Take Over AI Gateway Servers

One-Click Microsoft 365 Copilot Flaw Could Have Let Attackers Steal Emails, Files, and MFA Codes



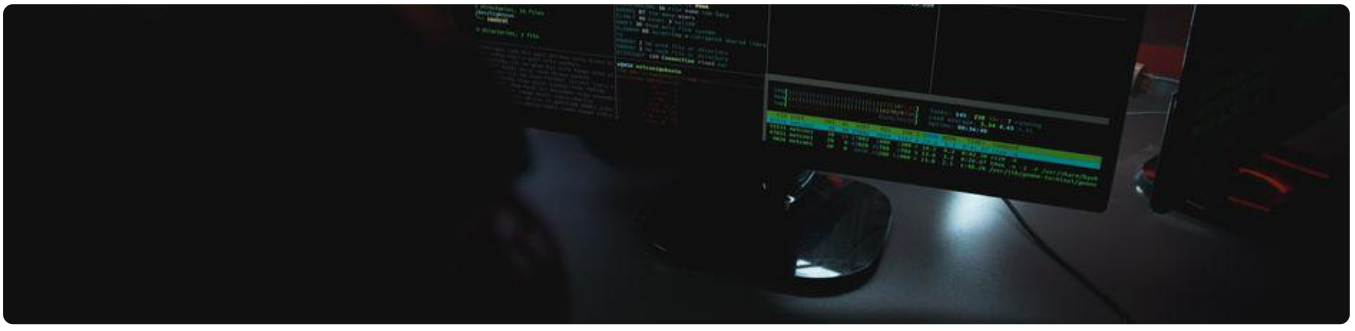
⚡ Weekly Recap: Chrome 0-Day, UniFi Exploits, macOS Stealers, VPN Flaw and More

INTEL

Cyber Threat Intelligence

LiteLLM Vulnerability Chain Lets Low-Privilege Users Take Over AI Gateway Servers

One-Click Microsoft 365 Copilot Flaw Could Have Let Attackers Steal Emails, Files, and MFA Codes



⚡ Weekly Recap: Chrome 0-Day, UniFi Exploits, macOS Stealers, VPN Flaw and More

INTEL

Threat Intelligence — Continued

The Onboarding Password Mistake That Creates Unnecessary Risk

152 Chrome Wallpaper Extensions with 105K Installs Linked to Adware and Fake Traffic

Popular WordPress Plugin Scripts Tampered to Plant Hidden Backdoors on Sites

Evil MSI Background: BASE64 Statistical Analysis, (Mon, Jun 15th)

ISC Stormcast For Monday, June 15th, 2026 https://isc.sans.edu/podcastdetail/9972, (Mon, Jun 15th)

WEEKLY TECH TIP

Vet Browser Extensions Before They Compromise Your Business

Browser extensions can harbor malware, adware, or data-stealing code that compromises sensitive business information. Recent incidents show even popular extensions with thousands of installs can be malicious.

Step 1: Review all installed browser extensions and remove any that aren't essential.

Step 2: Only install extensions from verified developers with legitimate reviews and update history.

Step 3: Check extension permissions before installing—deny access to unnecessary data or sites.

Step 4: Implement a company policy requiring IT approval before employees install extensions.

ALERTS

National Cybersecurity Alerts

Evil MSI Background: BASE64 Statistical Analysis, (Mon, Jun 15th)

ISC Stormcast For Monday, June 15th, 2026 https://isc.sans.edu/podcastdetail/9972, (Mon, Jun 15th)

ISC Stormcast For Friday, June 12th, 2026 https://isc.sans.edu/podcastdetail/9970, (Fri, Jun 12th)

ISC Stormcast For Thursday, June 11th, 2026 https://isc.sans.edu/podcastdetail/9968, (Thu, Jun 11th)

REGIONAL

Regional & Sector-Specific Alerts

Evil MSI Background: BASE64 Statistical Analysis, (Mon, Jun 15th)

ISC Stormcast For Monday, June 15th, 2026 https://isc.sans.edu/podcastdetail/9972, (Mon, Jun 15th)

ISC Stormcast For Friday, June 12th, 2026 https://isc.sans.edu/podcastdetail/9970, (Fri, Jun 12th)

JUNE AWARENESS

Internet Safety Month

Security Awareness Spotlight: Internet Safety Month June is Internet Safety Month, and it's the perfect time to strengthen your team's defenses against online threats that target small businesses every day. Phishing emails and malicious websites are two of the easiest ways hackers break into your systems, often tricking employees into clicking dangerous links or entering passwords on fake login pages. Take action today by scheduling a 15-minute team meeting this week to show everyone real examples of phishing emails (check your spam folder) and establish one simple rule: when in doubt about any email or link, always verify by calling or texting the sender directly before clicking.

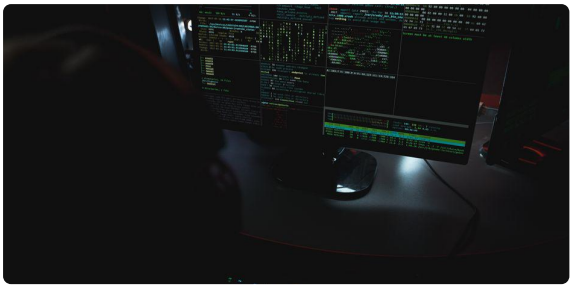
ACTION ITEM

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

SMB SPOTLIGHT

Protecting Your Business

Software supply chain attacks: check your dependencies



Designing secure access with ZTNA

Thinking carefully before adopting agentic AI

10 questions to ask when using AI models to find vulnerabilities

INNOVATION

Cybersecurity Advancements

Ransomware Attack Shuts Down Mills of Australia’s Second-Largest Sugar Producer

Chinese Hackers Target Medical, Military, and AI Research in North America

NewCore Emerges From Stealth Mode With $66 Million in Funding

Ukrainian Man Pleads Guilty in US to Conti Ransomware Charges

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 troubling story about trust. From AI gateway vulnerabilities to compromised browser extensions with over 100,000 downloads, we're seeing attackers exploit the very tools we rely on to make work easier and more efficient.

What strikes me most is the Microsoft 365 Copilot vulnerability. Here's a tool designed to boost productivity, yet a single click could have handed attackers the keys to your emails, files, and even multi-factor authentication codes. It's a stark reminder that innovative technology, while powerful, can become a significant liability without proper security controls.

The lesson? Every new tool you introduce into your business environment expands your attack surface. Before deploying AI assistants, productivity add-ons, or even something as simple as browser extensions, ask yourself: Who has verified this is safe? What access am I granting? Do we have visibility into what this tool is actually doing?

At Intelligent Automation, we're helping clients navigate this balance between innovation and security. If you're unsure whether your productivity tools are properly secured, let's talk. Your future success depends on embracing technology wisely, not fearfully.

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