VOL. 1 · ISSUE 47

Cyber Shield

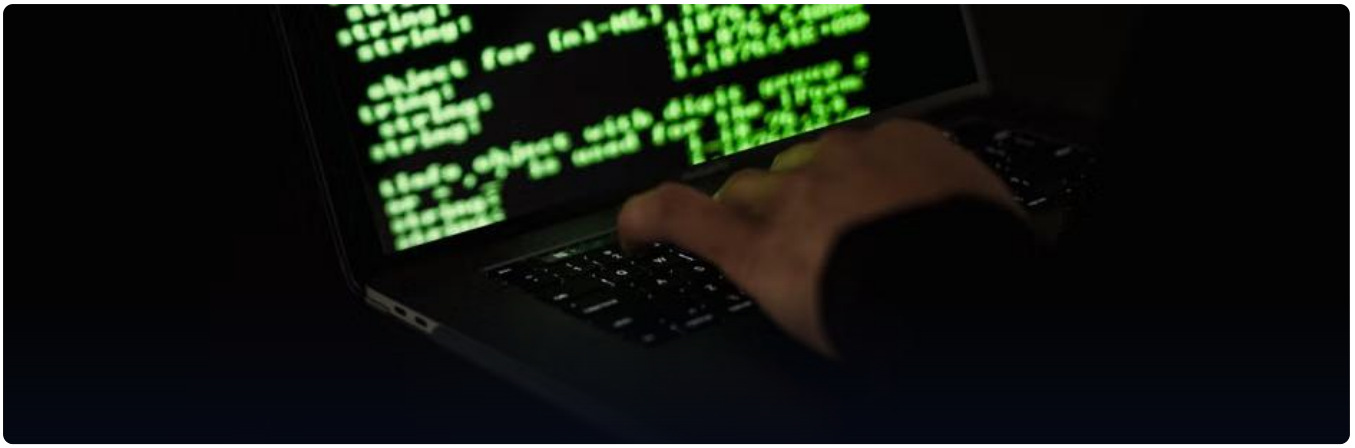
August 17, 2026

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

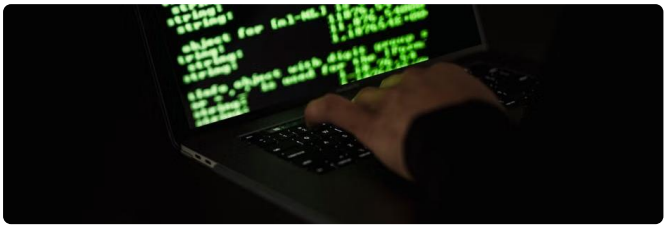
INTELLIGENT AUTOMATION, LLC · INTELAMATION.COM · FAIRFIELD, NJ

FEATURE

This Week in Cybersecurity



⚡ Weekly Recap: VMware Exploits, Windows 0-Day, MCP Attacks, Browser Hijacks and More

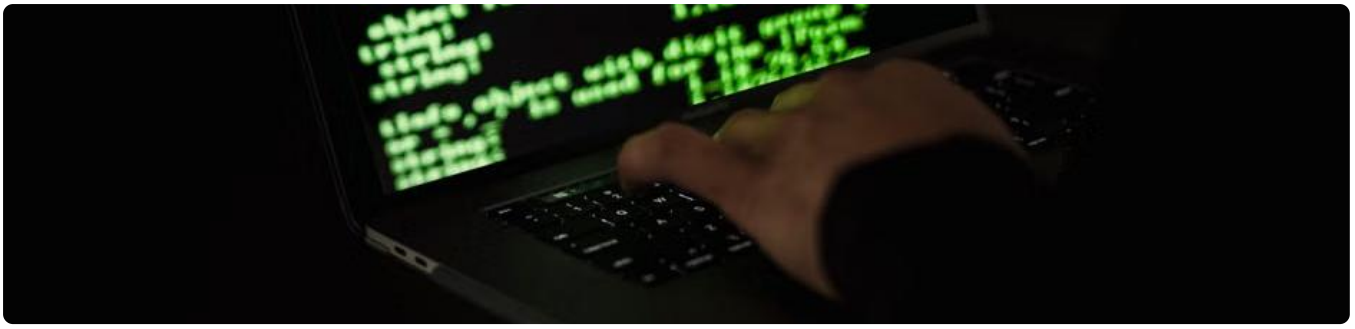


How MCP Servers Can Expose Enterprise Secrets

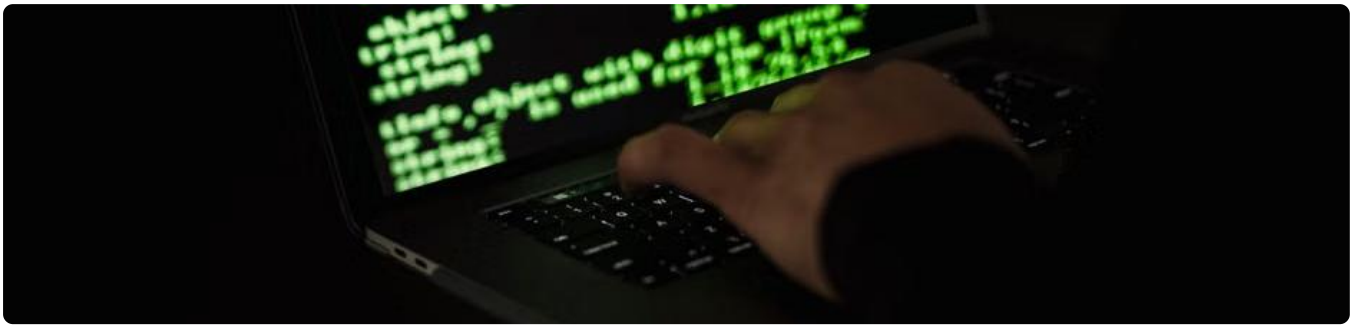
Unisoc VoLTE Video Call Exploit Chain Can Give Attackers Full Android Kernel Access

INTEL

Cyber Threat Intelligence



⚡ Weekly Recap: VMware Exploits, Windows 0-Day, MCP Attacks, Browser Hijacks and More



How MCP Servers Can Expose Enterprise Secrets

Unisoc VoLTE Video Call Exploit Chain Can Give Attackers Full Android Kernel Access

INTEL

Threat Intelligence — Continued

Evooo1Bot Linux Botnet Exploits Known Flaws to Turn Edge Devices Into SOCKS5 Proxies

Suspected China-Nexus Actor Exploits VMware vCenter Flaw, Deploys Babuk-Derived Ransomware

SAP Commerce Cloud CVE-2026-58231 Targeted in Exploitation Attempts Days After Patch

ISC Stormcast For Monday, August 17th, 2026 https://isc.sans.edu/podcastdetail/10054, (Mon, Aug 17th)

Wireshark 4.6.8 Released, (Sun, Aug 16th)

💡 WEEKLY TECH TIP

Patch VMware vCenter Now to Stop Ransomware

Attackers are actively exploiting VMware vCenter vulnerabilities to deploy ransomware that can cripple your entire virtual infrastructure. This critical flaw allows complete system takeover before you even detect the breach.

Step 1: Immediately update VMware vCenter to the latest patched version from vendor portal.

Step 2: Enable multi-factor authentication on all vCenter administrator and privileged service accounts.

Step 3: Segment your virtualization management network from general business networks using firewall rules.

Step 4: Monitor vCenter logs daily for unauthorized login attempts and unusual administrative activities.

ALERTS

National Cybersecurity Alerts

ISC Stormcast For Monday, August 17th, 2026 https://isc.sans.edu/podcastdetail/10054, (Mon, Aug 17th)

Wireshark 4.6.8 Released, (Sun, Aug 16th)

ISC Stormcast For Friday, August 14th, 2026 https://isc.sans.edu/podcastdetail/10052, (Fri, Aug 14th)

ISC Stormcast For Thursday, August 13th, 2026 https://isc.sans.edu/podcastdetail/10050, (Thu, Aug 13th)

REGIONAL

Regional & Sector-Specific Alerts

ISC Stormcast For Monday, August 17th, 2026 https://isc.sans.edu/podcastdetail/10054, (Mon, Aug 17th)

Wireshark 4.6.8 Released, (Sun, Aug 16th)

ISC Stormcast For Friday, August 14th, 2026 https://isc.sans.edu/podcastdetail/10052, (Fri, Aug 14th)

AUGUST AWARENESS

Back to School / New Devices

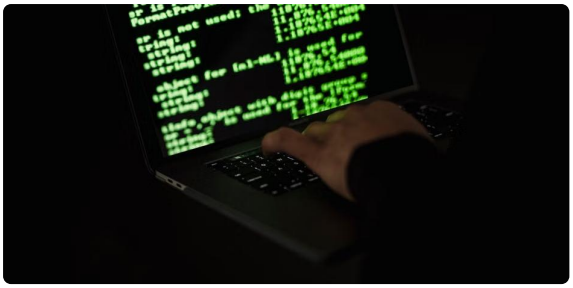
Security Awareness Spotlight: Back to School / New Devices August means new laptops, tablets, and phones for students and staff—but each new device is a potential open door for hackers if you don't secure it first. Before anyone connects a new device to your business network or email, make sure it has the latest security updates installed, antivirus software running, and strong passwords or biometric locks enabled. Today, create a simple checklist that anyone in your business can follow before connecting a new device, and share it with your team via email or post it near your Wi-Fi router.

ACTION ITEM

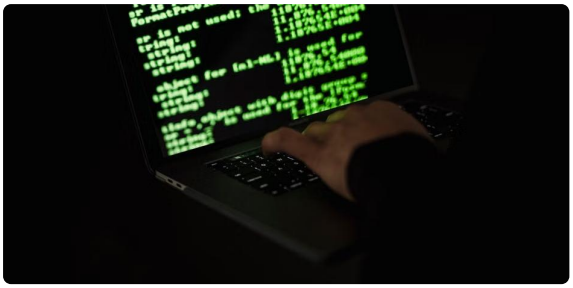
Schedule a 15-minute team security review this week using this month's theme as your agenda.

SMB SPOTLIGHT

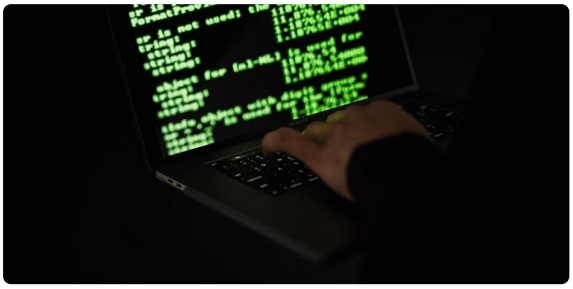
Protecting Your Business



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

NCSC statement in response to recent incidents resulting from frontier AI evaluations

INNOVATION

Cybersecurity Advancements

680,000 Impacted by French Tax Authority Data Breach

Irregular Details How a Naming Error Let AI Models Attack a Real Company

Conflicting Test Goals Pushed Claude Agents to Deploy Self-Replicating Malware

40,000 Impacted by SafePal 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 threat landscape tells a story we've seen before, but one that deserves our renewed attention: the dangerous gap between patch availability and patch deployment. The VMware vCenter exploitation by suspected state-sponsored actors isn't just another headline—it's a wake-up call about how quickly adversaries move once vulnerabilities become public knowledge.

What concerns me most isn't the sophistication of these attacks, but rather their predictability. Whether it's VMware flaws or the Evooo1Bot targeting edge devices, attackers are consistently exploiting *known* vulnerabilities in systems that should have been patched weeks or months ago. We're not talking about zero-days here; we're talking about documented fixes that organizations simply haven't applied.

I understand the hesitation. Patches can disrupt operations, and testing takes time. But here's the reality: threat actors aren't waiting for convenient maintenance windows. They're scanning networks right now, looking for these exact weaknesses.

Take this week as your catalyst. Review your patching cadence, prioritize internet-facing systems, and if you're feeling overwhelmed, reach out. Nobody should be fighting this battle alone.

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