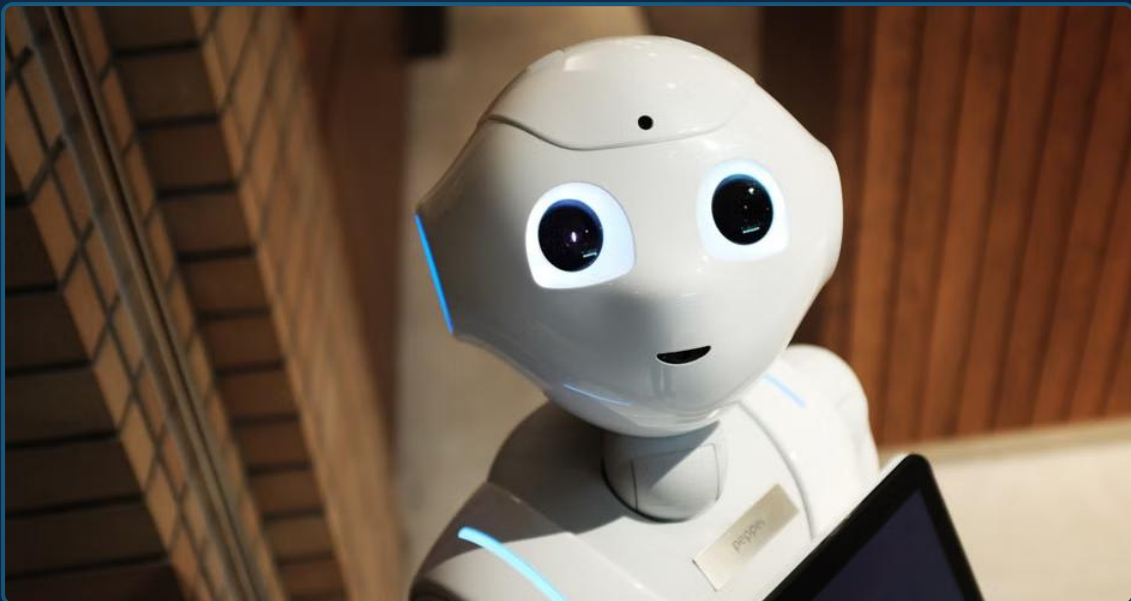




VOL. 1 • ISSUE 53

Cyber Shield

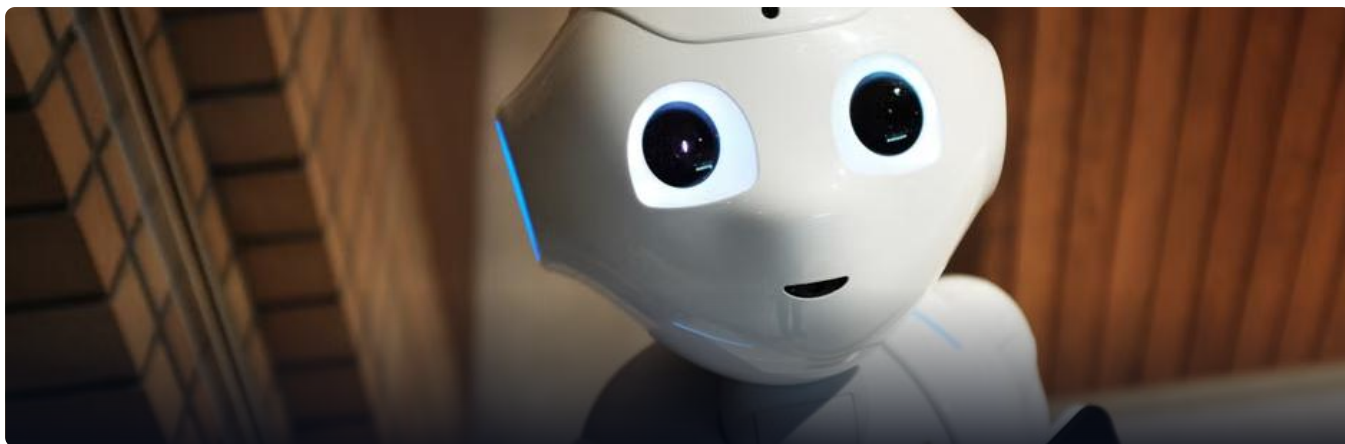
September 28, 2026

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

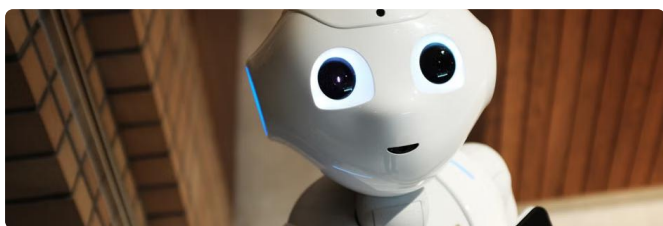
INTELLIGENT AUTOMATION, LLC • INTELAMATION.COM • FAIRFIELD, NJ

FEATURE

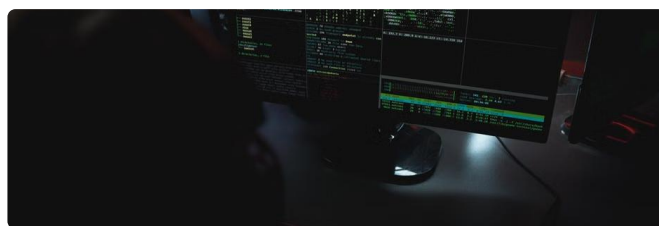
This Week in Cybersecurity



Webinar: How to Govern AI Agents, Reduce Excessive Access, and Control Shadow AI



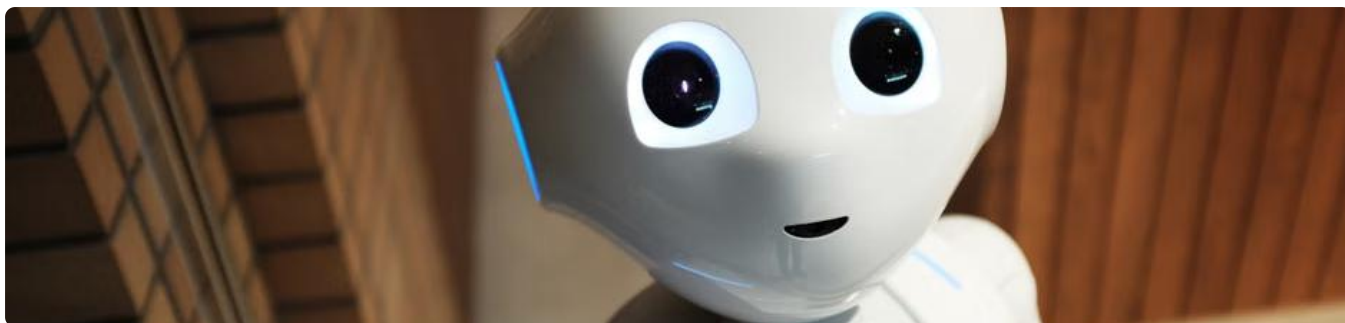
Carbonato Botnet Compromises Docker Hosts to Deploy Telegram-Controlled Hermes AI Agent



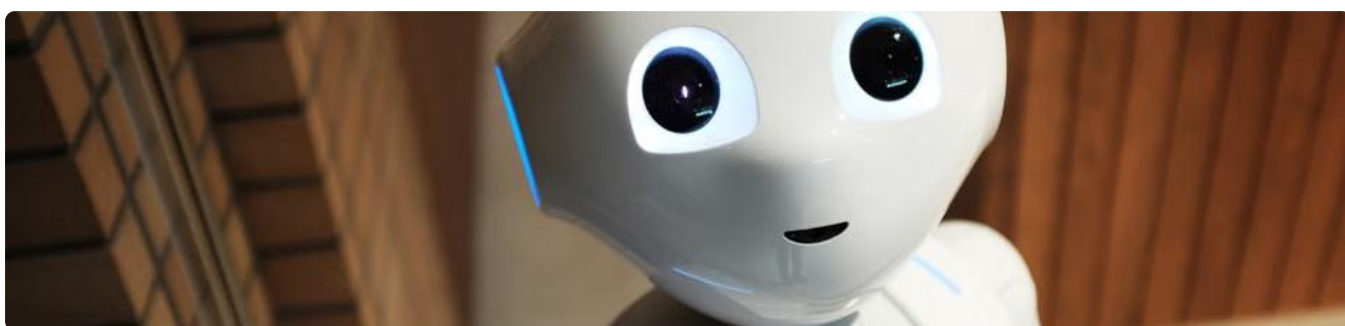
JADEPUFFER-Linked Attackers Used Compromised Service Principals to Delete Azure Resources

INTEL

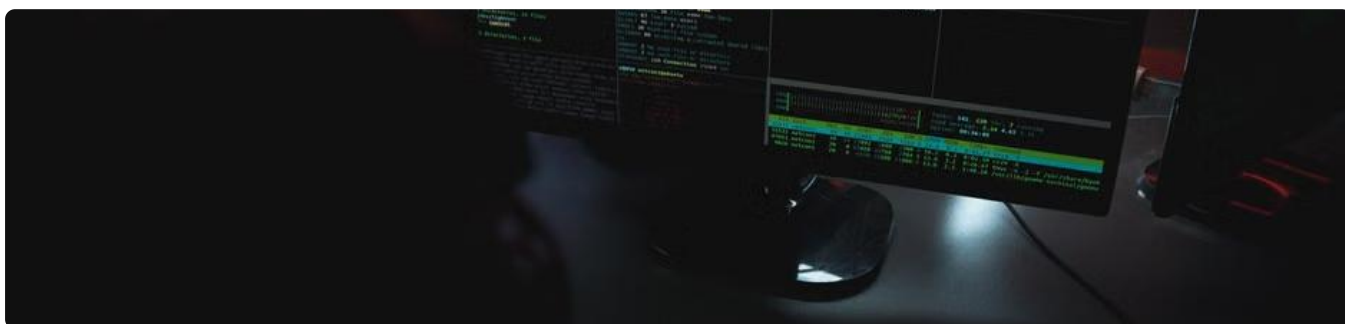
Cyber Threat Intelligence



Webinar: How to Govern AI Agents, Reduce Excessive Access, and Control Shadow AI



Carbonato Botnet Compromises Docker Hosts to Deploy Telegram-Controlled Hermes AI Agent



JADEPUFFER-Linked Attackers Used Compromised Service Principals to Delete Azure Resources

INTEL

Threat Intelligence — Continued

CISA Says Attackers Are Exploiting Two Critical Citrix NetScaler Flaws Globally

Warning: Two Unpatched Citrix NetScaler RCE Zero-Days Under Active Exploitation

Lunex Stealer Abuses AMD Driver to Disable Security Monitoring and Steal Browser Credentials

ISC Stormcast For Monday, September 28th, 2026 <https://isc.sans.edu/podcastdetail/10112>, (Mon, Sep 28th)

Wireshark 4.6.9 Released, (Sun, Sep 27th)

 WEEKLY TECH TIP

Patch Citrix NetScaler Immediately Against Active Exploits

Two critical zero-day vulnerabilities in Citrix NetScaler are being actively exploited worldwide, allowing attackers to remotely compromise systems. CISA has confirmed widespread exploitation, making immediate action essential for all NetScaler users.

- Step 1:** Check if you're running Citrix NetScaler ADC or Gateway appliances immediately.
- Step 2:** Apply Citrix security patches as soon as they become available from vendor.
- Step 3:** Monitor NetScaler logs for suspicious authentication attempts or unusual administrative activity.
- Step 4:** Implement network segmentation to isolate NetScaler appliances from critical internal systems.

ALERTS

National Cybersecurity Alerts

ISC Stormcast For Monday, September 28th, 2026 <https://isc.sans.edu/podcastdetail/10112>, (Mon, Sep 28th)

Wireshark 4.6.9 Released, (Sun, Sep 27th)

A Closer Look at Malware From the Macfinger ClickFix Campaign, (Fri, Sep 25th)

ISC Stormcast For Friday, September 25th, 2026 <https://isc.sans.edu/podcastdetail/10110>, (Fri, Sep 25th)

REGIONAL

Regional & Sector-Specific Alerts

ISC Stormcast For Monday, September 28th, 2026 <https://isc.sans.edu/podcastdetail/10112>, (Mon, Sep 28th)

Wireshark 4.6.9 Released, (Sun, Sep 27th)

A Closer Look at Malware From the Macfinger ClickFix Campaign, (Fri, Sep 25th)

 SEPTEMBER AWARENESS

Disaster Recovery Month

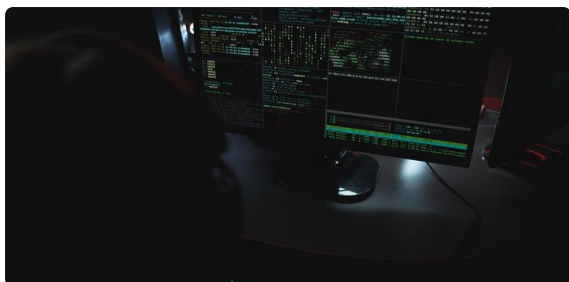
Security Awareness Spotlight: Disaster Recovery Month September is Disaster Recovery Month, and whether it's a ransomware attack, a fire, or a simple hard drive failure, every small business needs a plan for when things go wrong. Your customer data, financial records, and daily operations depend on systems that could fail at any moment, and hoping for the best isn't a strategy. This month, take one hour to write down the basic steps your team would follow if your main computer systems went down tomorrow—who would you call, how would you access your backups, and how would you keep serving customers? Your action for today: Open a document right now and write down where your most critical business data is stored and when you last verified you could actually restore it from backup.

ACTION ITEM

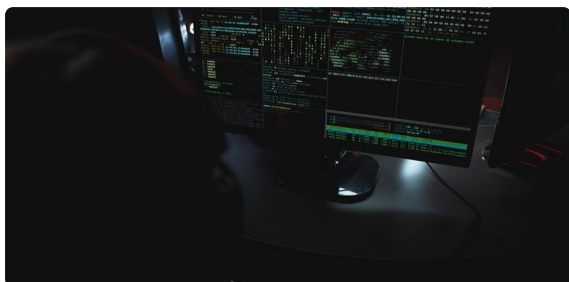
Schedule a 15-minute team security review this week using this month's theme as your agenda.

SMB SPOTLIGHT

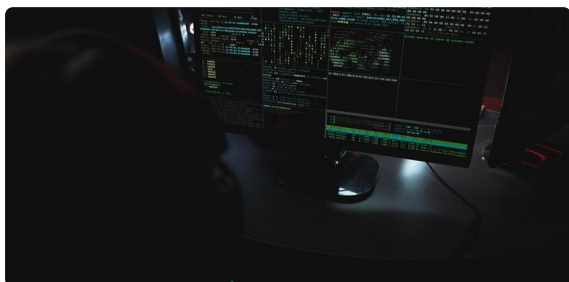
Protecting Your Business



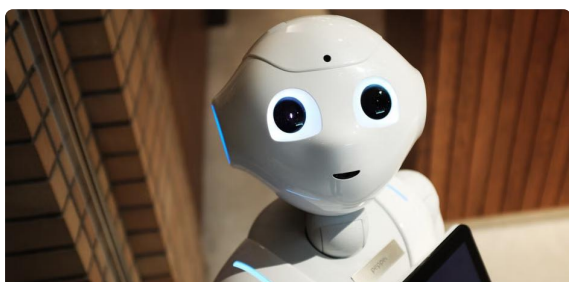
Exploitation of vulnerabilities affecting Citrix NetScaler ADC and Citrix NetScaler Gateway



One does not simply defend agentially



Adversary simulation: what you need to know



Cyber Adversary Simulation (CyAS): scheme documents now available

INNOVATION

Cybersecurity Advancements

Prison Sentence for Former US Soldier Who Hacked AT&T and Verizon

DC Health Agency Exposes 400,000 Beneficiary Records

Google Warns of ShinyHunters' Fresh Oracle PeopleSoft Campaign

New Mexico Jury Finds Facebook Liable for Deceiving Users About Privacy Protections

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 sobering picture, but there's a silver thread connecting them that every business leader needs to understand: the critical gap between deploying technology and actually controlling it.

Whether it's AI agents operating in the shadows, compromised Docker environments running rogue botnets, or unpatched NetScaler appliances creating open doors for attackers, the pattern is unmistakable. We're introducing powerful technologies faster than we're governing them. The Carbonato botnet case particularly concerns me—attackers are now weaponizing AI agents for their operations while many organizations haven't even inventoried the AI tools their own employees are using.

The solution isn't to fear innovation; it's to pair it with discipline. Every new technology in your environment—especially AI—needs clear governance from day one. Who approved it? Who monitors it? What access does it have? These aren't IT questions anymore; they're business survival questions.

Take thirty minutes this week to ask your team: what AI tools are we using, and do we actually control them? That conversation alone puts you ahead of most organizations—and miles ahead of becoming a cautionary tale in next week's headlines.

CONNECT WITH DANIEL

[linkedin.com/in/iamdanielramos](https://www.linkedin.com/in/iamdanielramos) · daniel.ramos@intellamation.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

© 2026 Intelligent Automation, LLC · All rights reserved