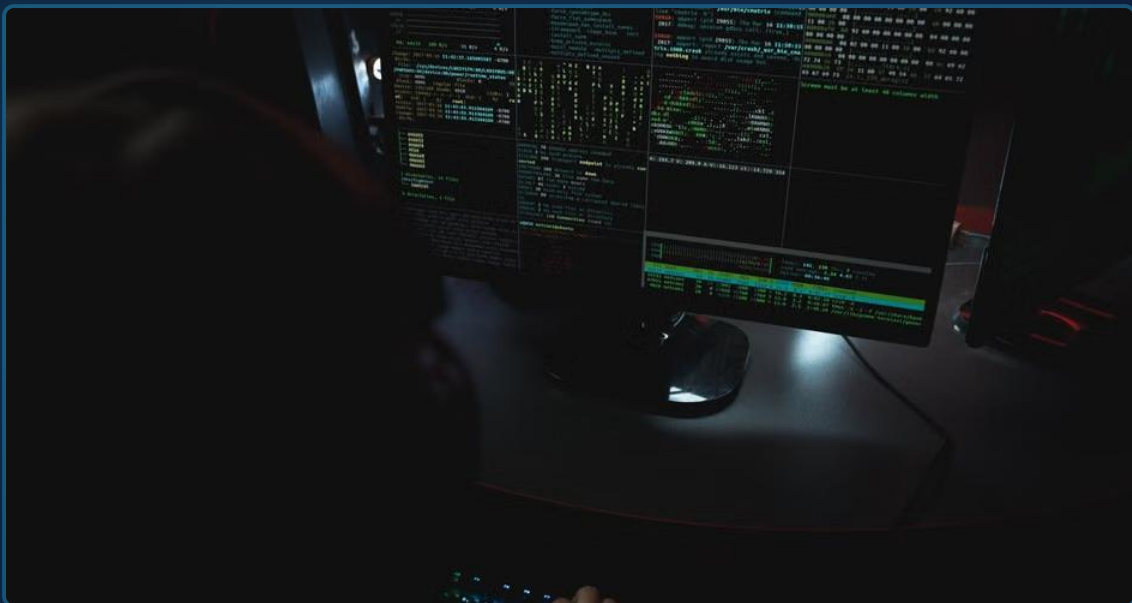




VOL. 1 • ISSUE 54

Cyber Shield

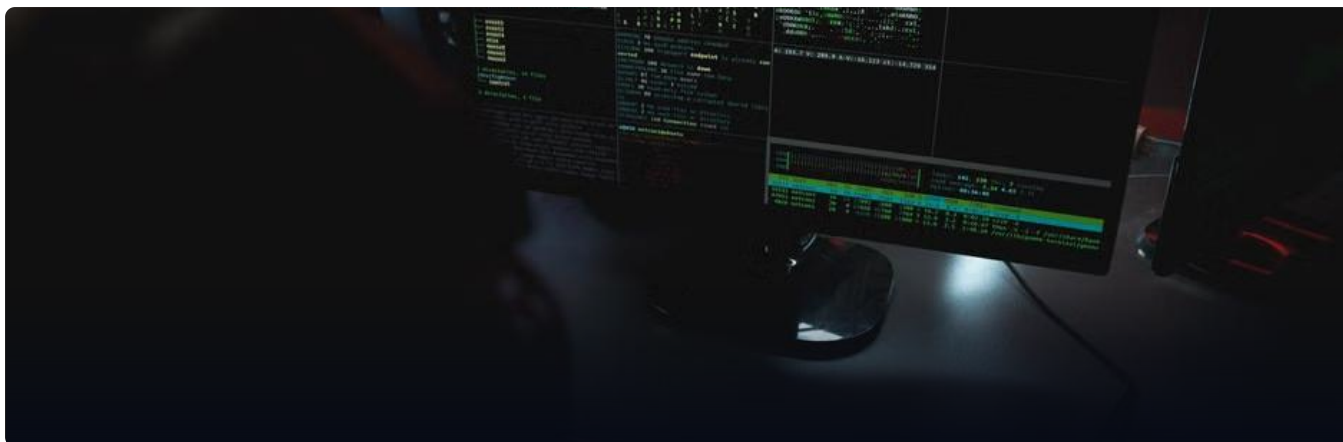
October 05, 2026

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

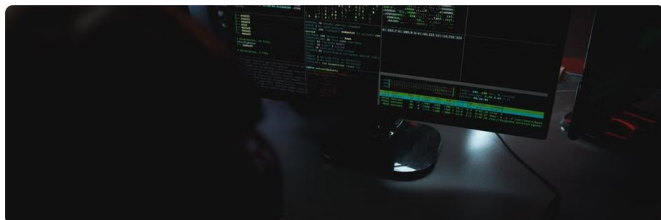
INTELLIGENT AUTOMATION, LLC • INTELAMATION.COM • FAIRFIELD, NJ

FEATURE

This Week in Cybersecurity



The Credential Layer Is Expanding Faster Than Security Teams Can See It



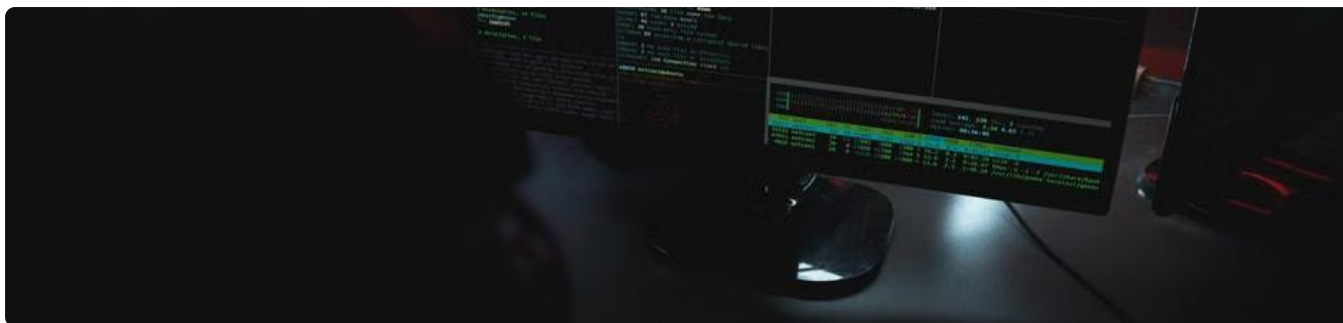
Realtek Jungle SDK Exploit Attempts Deliver Cling Botnet With STUN-Based C2



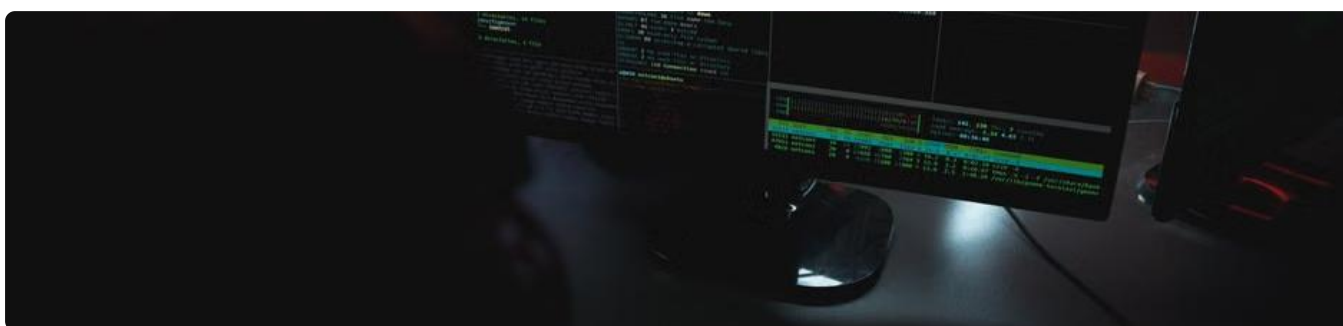
Apple Plans Tighter macOS Full Disk Access Controls Over AI Agent Data Access

INTEL

Cyber Threat Intelligence



The Credential Layer Is Expanding Faster Than Security Teams Can See It



Realtek Jungle SDK Exploit Attempts Deliver Cling Botnet With STUN-Based C2



Apple Plans Tighter macOS Full Disk Access Controls Over AI Agent Data Access

INTEL

Threat Intelligence — Continued

Attackers Target Rejetto HFS Flaw That Enables Admin Session Forgery and RCE

New NetScaler Zero-Day Exploited in Targeted Attacks Can Knock SAML Deployments Offline

ShinyHunters Suspect Rey Reportedly Detained in Jordan, Helping FBI Identify Group Members

ISC Stormcast For Monday, October 5th, 2026 <https://isc.sans.edu/podcastdetail/10122>, (Mon, Oct 5th)

TTY Logs and the Data it Captures, (Sun, Oct 4th)

 WEEKLY TECH TIP

Audit Your Credential Sprawl Before Attackers Find It

Modern businesses use dozens of cloud services, APIs, and integrations that create authentication points faster than security teams can track them. Unmonitored credentials become easy targets for attackers exploiting vulnerabilities in third-party systems and SDKs.

Step 1: Inventory all active service accounts, API keys, and SSO integrations monthly.

Step 2: Revoke unused credentials and rotate active ones every 90 days minimum.

Step 3: Implement centralized identity management to control access across all systems.

Step 4: Enable multi-factor authentication on every service that supports it, no exceptions.

ALERTS

National Cybersecurity Alerts

ISC Stormcast For Monday, October 5th, 2026 <https://isc.sans.edu/podcastdetail/10122>, (Mon, Oct 5th)

TTY Logs and the Data it Captures, (Sun, Oct 4th)

User Agent Strings Curiosities, (Sun, Oct 4th)

YARA-X 1.21.0 Release, (Sat, Oct 3rd)

REGIONAL

Regional & Sector-Specific Alerts

ISC Stormcast For Monday, October 5th, 2026 <https://isc.sans.edu/podcastdetail/10122>, (Mon, Oct 5th)

TTY Logs and the Data it Captures, (Sun, Oct 4th)

User Agent Strings Curiosities, (Sun, Oct 4th)

 OCTOBER AWARENESS

Cybersecurity Awareness Month

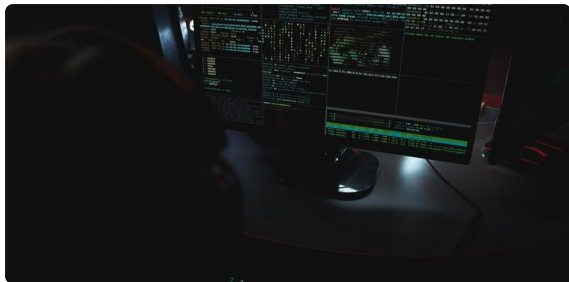
October is Cybersecurity Awareness Month, which means it's the perfect time to strengthen your team's ability to spot and stop cyber threats before they cost you money or customer trust. This month, run a fake phishing email test to see who on your team might accidentally let hackers in, host a 30-minute lunch session to walk through real examples of scam emails and texts, and make sure everyone knows the simple rule: if you click something suspicious, report it to your IT person or manager immediately instead of staying quiet. Today, send an email to your entire team right now asking this question: "If you accidentally clicked a link in a suspicious email, do you know exactly who to tell and how to reach them?" — then make sure they actually have that contact information saved.

ACTION ITEM

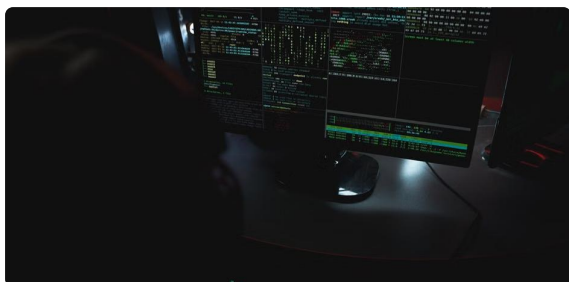
Schedule a 15-minute team security review this week using this month's theme as your agenda.

SMB SPOTLIGHT

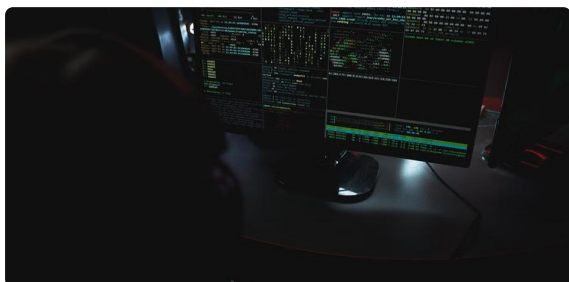
Protecting Your Business



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

Linux Backdoor Abuses STUN Protocol, Exploits Dozens of Flaws

250,000 Impacted by Data Breaches at New Jersey, Texas Healthcare Firms

Exploitation Hits Rejetto HFS Vulnerability Discovered by AI

Senate Passes Bipartisan Bill to Strengthen Healthcare Cybersecurity

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 I've been warning clients about for months: the perimeter has dissolved, and credentials are the new battleground. What concerns me most isn't any single vulnerability—it's how rapidly the credential layer is expanding while security teams struggle to maintain visibility.

We're seeing attackers exploit everything from router SDKs to legitimate file servers, and the common thread is clear: once they're in, they're after your credentials. The NetScaler zero-day targeting SAML implementations is particularly telling. These aren't random attacks—they're surgical strikes aimed at the authentication systems we've trusted to protect everything else.

Here's what keeps me up at night: most organizations still don't have complete visibility into where credentials live, how they're being used, or when they're being abused. We're defending yesterday's network while attackers are already inside today's identity systems.

The encouraging news? This is entirely addressable. Start by auditing your credential footprint—every service account, every API key, every authentication token. You can't protect what you can't see, but once you can see it, you can secure it.

CONNECT WITH DANIEL[linkedin.com/in/iamdanielramos](https://www.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

© 2026 Intelligent Automation, LLC · All rights reserved