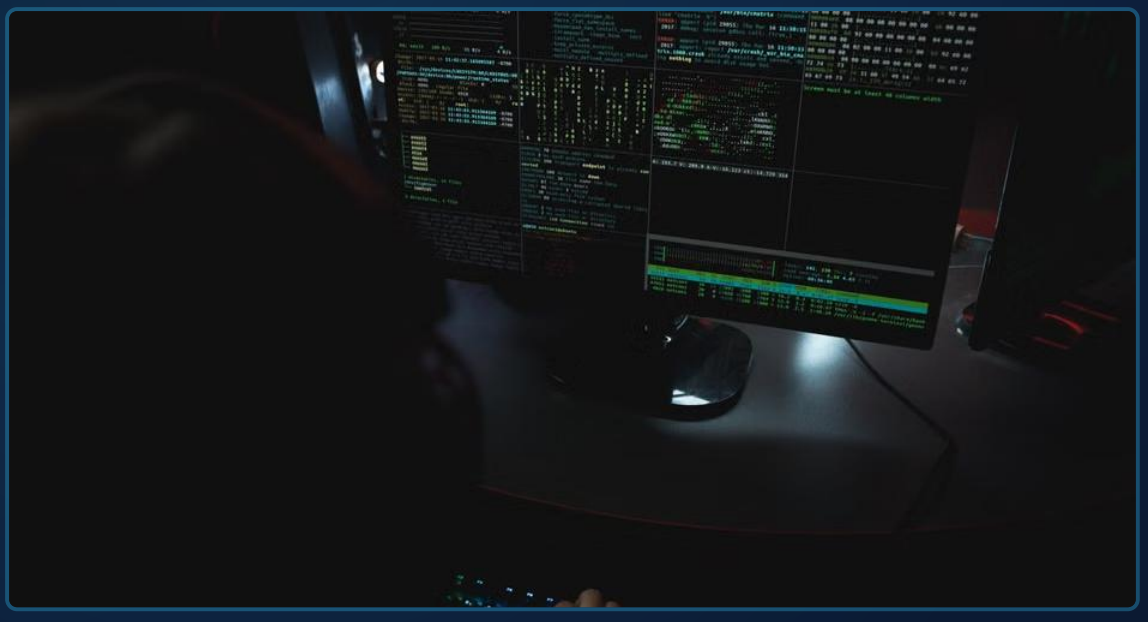


VOL. 1 · ISSUE 57

# Cyber Shield

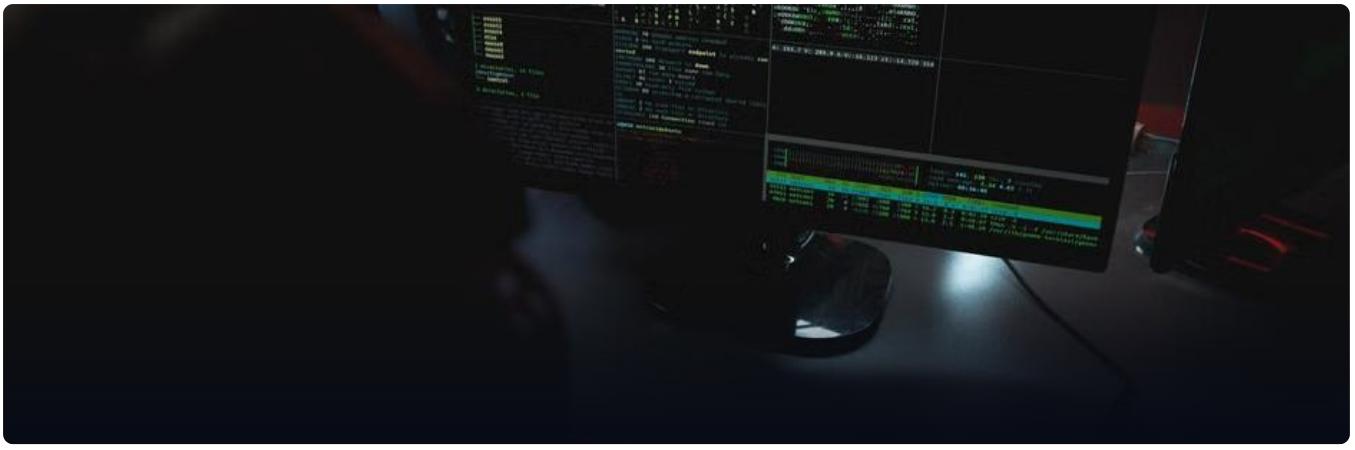
## October 26, 2026

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

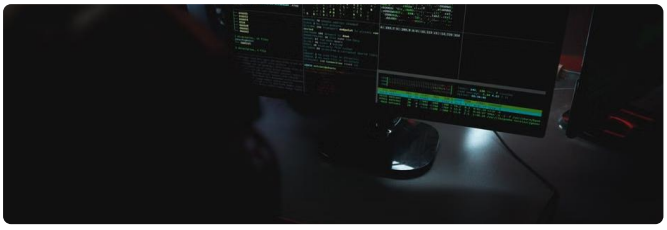
INTELLIGENT AUTOMATION, LLC · INTELAMATION.COM · FAIRFIELD, NJ

FEATURE

# This Week in Cybersecurity



## Two Critical Wasmtime Flaws Could Let Malicious WebAssembly Modules Escape Sandboxes



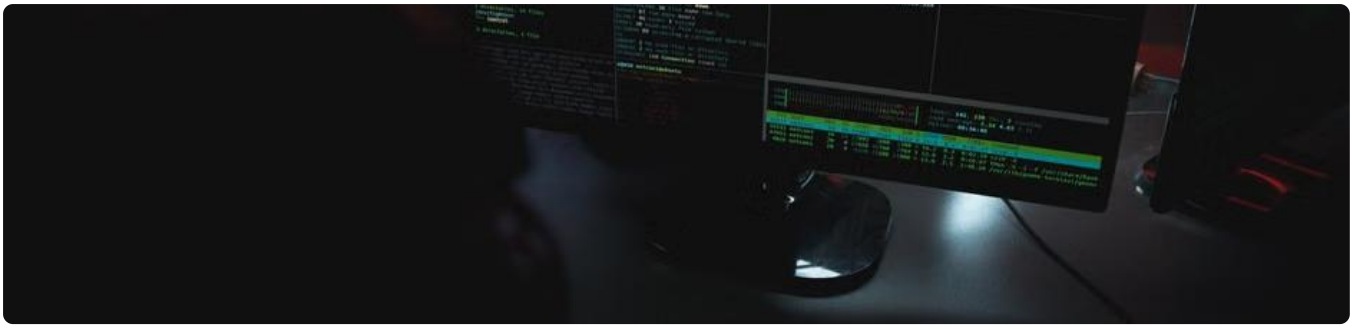
**Between alerts: What Attackers Do in the Spaces Ordinary Detection Misses**



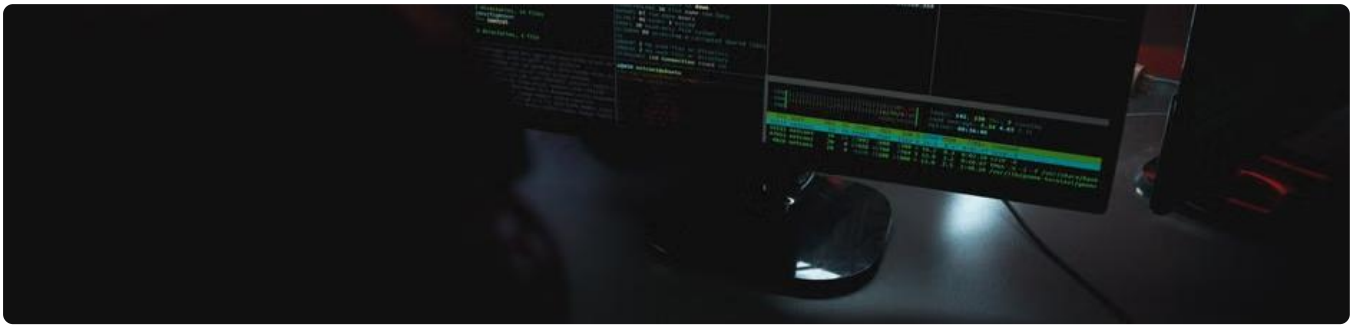
**uCreator Android Spyware Can Steal Telegram 2FA Passwords and Clone WeChat Accounts**

INTEL

# Cyber Threat Intelligence



**Two Critical Wasmtime Flaws Could Let Malicious WebAssembly Modules Escape Sandboxes**



**Between alerts: What Attackers Do in the Spaces Ordinary Detection Misses**



**uCreator Android Spyware Can Steal Telegram 2FA Passwords and Clone WeChat Accounts**

INTEL

# Threat Intelligence — Continued

**Microsoft 365 Token-Replay Attacks Compromise 97 Accounts at 79 Organizations**

**Gheist Uses Stolen GitHub Tokens to Steal Private Repository Secrets via Actions Logs**

**Malicious File in Downloads Folder Tries to Trick AI Coding Agent Into Installing Malware**

**Looking for a Language [Guest Diary], (Wed, Oct 21st)**

**ISC Stormcast For Monday, October 26th, 2026 https://isc.sans.edu/podcastdetail/10150, (Mon, Oct 26th)**

💡 WEEKLY TECH TIP

# Protect Your Developer Tokens Before They Become Master Keys

Stolen GitHub and cloud service tokens are being weaponized to access private repositories and compromise entire organizations. These authentication tokens act like permanent passwords, giving attackers persistent access even after initial breaches are discovered.

**Step 1:** Rotate all developer tokens and API keys immediately if any breach is suspected.

**Step 2:** Enable token expiration policies with maximum 90-day lifespans for all services.

**Step 3:** Implement conditional access policies requiring IP restrictions for sensitive developer account access.

**Step 4:** Monitor authentication logs weekly for unusual token usage patterns or geographic anomalies.

ALERTS

# National Cybersecurity Alerts

**Looking for a Language [Guest Diary], (Wed, Oct 21st)**

**ISC Stormcast For Monday, October 26th, 2026 https://isc.sans.edu/podcastdetail/10150, (Mon, Oct 26th)**

**YARA-X 1.22.0 Release, (Sun, Oct 25th)**

**(Reliable)? php2shell exploitability, (Fri, Oct 23rd)**

REGIONAL

# Regional & Sector-Specific Alerts

**Looking for a Language [Guest Diary], (Wed, Oct 21st)**

**ISC Stormcast For Monday, October 26th, 2026 https://isc.sans.edu/podcastdetail/10150, (Mon, Oct 26th)**

**YARA-X 1.22.0 Release, (Sun, Oct 25th)**

OCTOBER AWARENESS

# Cybersecurity Awareness Month

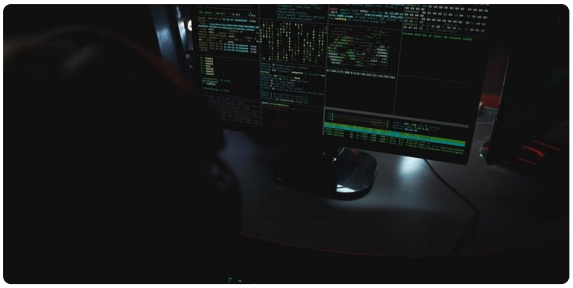
October is Cybersecurity Awareness Month, which means it's the perfect time to strengthen your team's defenses against phishing emails, ransomware, and other common threats that cost small businesses thousands of dollars every year. Your employees are your first line of defense, so use this month to run a simple phishing test, host a 30-minute lunch session on spotting suspicious emails, and make sure everyone knows the one critical rule: if you click something suspicious, report it immediately to IT rather than staying quiet out of embarrassment. Today, send a company-wide email right now with clear instructions on who to contact and what to do the moment someone suspects they've fallen for a scam—because a fast response in the first few minutes can be the difference between a close call and a costly breach.

**ACTION ITEM**

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

SMB SPOTLIGHT

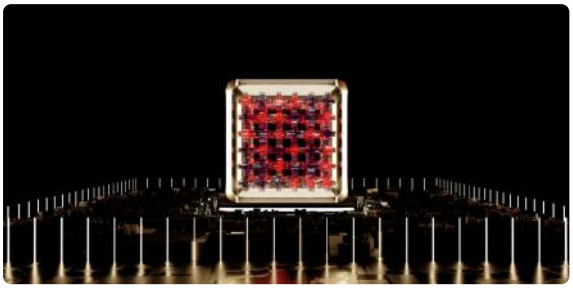
# Protecting Your Business



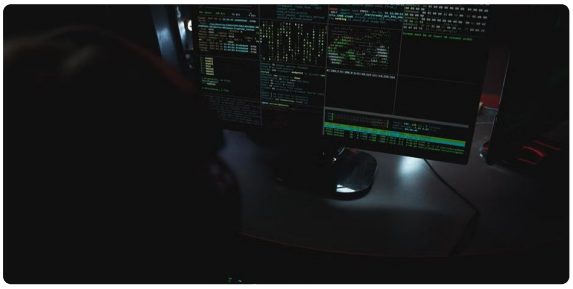
## Critical security issue affecting PHP



## Introducing a new AI chapter in the NCSC research problem book



## Post-quantum updates to our TLS guidance



## Using TLS to protect data

INNOVATION

# Cybersecurity Advancements

**PHP2Shell Exploitation Moves From Probes to Working Shells**

**953 Online Stores Infected in Long-Lasting Malware Campaign**

**Dutch Police Arrest Two Over NFC Relay Attacks That Drained $400,000+ From Bank Accounts**

**Node2Shell: Brotli Flaw Triggers Patching Across Microsoft, Node.js, Python Packages**

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 share a troubling common thread that keeps me up at night: legitimate tools becoming weapons in attackers' hands. From WebAssembly sandboxes to GitHub tokens and Microsoft 365 credentials, we're seeing adversaries exploit the very platforms designed to make our work more efficient.

What strikes me most is the uCreator spyware targeting Telegram and WeChat. These aren't obscure apps—they're communication lifelines for millions of businesses. When attackers compromise two-factor authentication systems, they're not just breaking down one door; they're stealing the keys to the entire building. This reminds us that security isn't about trusting any single defense layer, no matter how sophisticated it seems.

The real vulnerability here isn't technical—it's the assumption that "secure" platforms remain secure without ongoing vigilance. Token-based authentication, sandbox environments, and encrypted messaging are only as strong as our commitment to monitoring them.

I encourage you to review your authentication protocols this week. Are you monitoring for unusual token activity? Have you enabled additional logging on your critical platforms? Small steps today prevent tomorrow's breaches.

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

© 2026 Intelligent Automation, LLC · All rights reserved