Intelligent Automation

Solutions that are powered by a SECURE Cloud.

MCSP

Managed Cybersecurity Service Provider



VOL. 1 · ISSUE 56

Cyber Shield

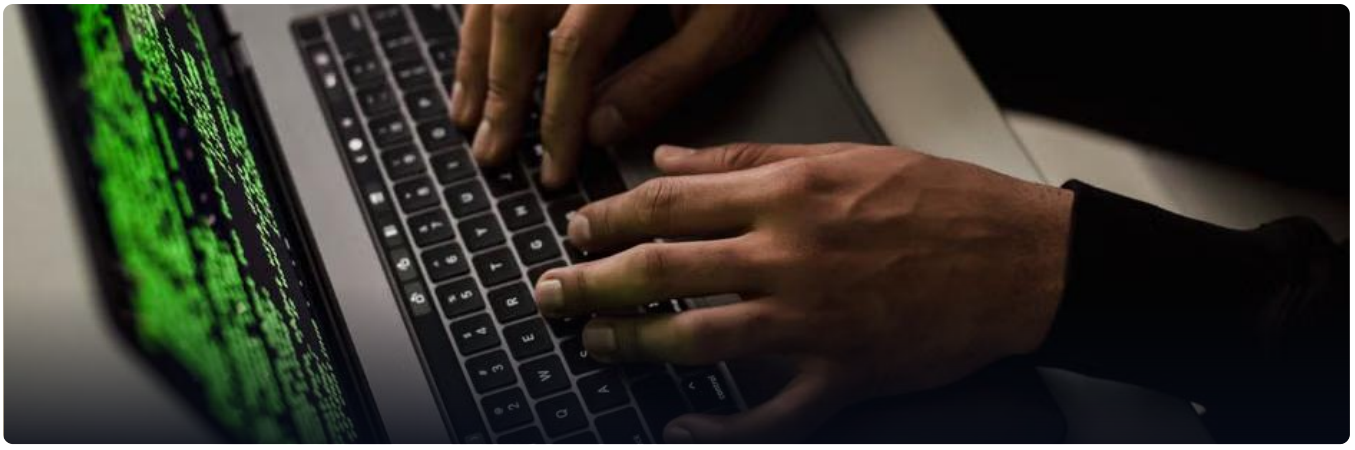
October 19, 2026

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

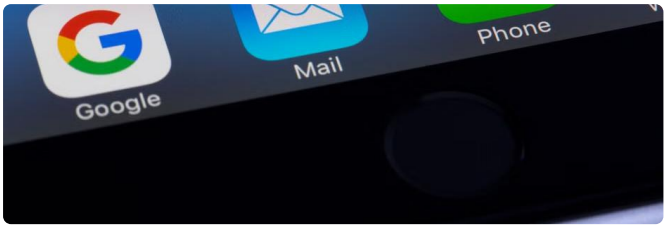
INTELLIGENT AUTOMATION, LLC · INTELAMATION.COM · FAIRFIELD, NJ

FEATURE

This Week in Cybersecurity



GhostAction Attackers Plant Credential Stealer Disguised as Font in 94 GitHub Repositories



From Email-to-Case to the Boardroom: How Inherited Agents Break Governance Built for Software



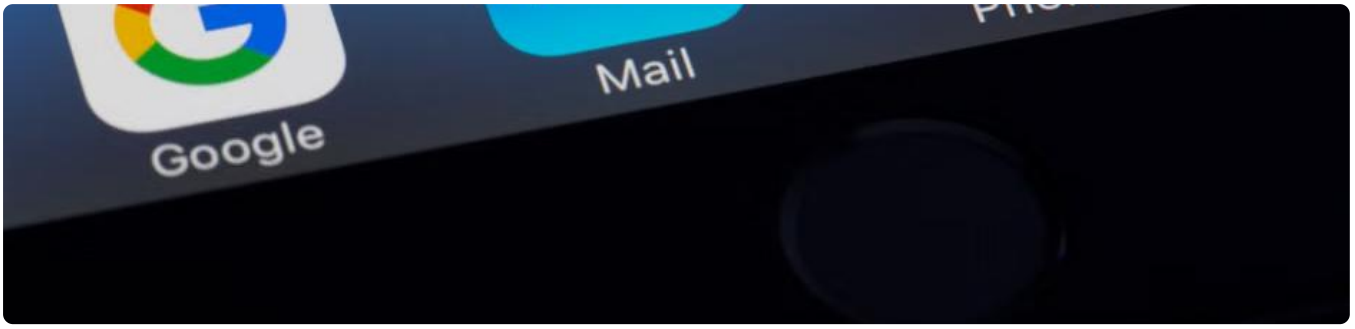
Fake Web3 Accelerator Uses npm Packages to Spread Malware and Hijack AI Agent Traffic

INTEL

Cyber Threat Intelligence



GhostAction Attackers Plant Credential Stealer Disguised as Font in 94 GitHub Repositories



From Email-to-Case to the Boardroom: How Inherited Agents Break Governance Built for Software



Fake Web3 Accelerator Uses npm Packages to Spread Malware and Hijack AI Agent Traffic

INTEL

Threat Intelligence — Continued

Unpatched Broadcom Wi-Fi Flaw Lets Attackers in Range Run Code as Root on Routers

OpenCode Console Breach May Have Exposed OpenAI, Anthropic, and Google API Keys

ConnectWise Suspends Cloud Backup After Attackers Compromise Microsoft 365 Tenants

Orphaned VBA Projects Inside DWG Files: YARA Rule, (Sun, Oct 18th)

ISC Stormcast For Friday, October 16th, 2026 https://isc.sans.edu/podcastdetail/10140, (Fri, Oct 16th)

💡 WEEKLY TECH TIP

Audit Your Developer Dependencies Before They Audit You

Attackers are increasingly hiding malware in seemingly legitimate development resources like fonts, npm packages, and GitHub repositories. A single compromised dependency can give hackers access to your systems, credentials, and sensitive API keys.

Step 1: Maintain an inventory of all third-party code libraries and packages your developers use.

Step 2: Use automated scanning tools to check dependencies for known vulnerabilities before deployment.

Step 3: Restrict developer ability to install packages from unverified or newly created repository sources.

Step 4: Rotate all API keys quarterly and immediately if any development tool breach occurs.

ALERTS

National Cybersecurity Alerts

Orphaned VBA Projects Inside DWG Files: YARA Rule, (Sun, Oct 18th)

ISC Stormcast For Friday, October 16th, 2026 https://isc.sans.edu/podcastdetail/10140, (Fri, Oct 16th)

Small Agents, Smaller Blast Radius: Controlling What AI Can Do, (Fri, Oct 16th)

Panchan's Mining Island [Guest Diary], (Wed, Oct 14th)

REGIONAL

Regional & Sector-Specific Alerts

Orphaned VBA Projects Inside DWG Files: YARA Rule, (Sun, Oct 18th)

ISC Stormcast For Friday, October 16th, 2026 https://isc.sans.edu/podcastdetail/10140, (Fri, Oct 16th)

Small Agents, Smaller Blast Radius: Controlling What AI Can Do, (Fri, Oct 16th)

🛡 OCTOBER AWARENESS

Cybersecurity Awareness Month

Security Awareness Spotlight: Cybersecurity Awareness Month October is Cybersecurity Awareness Month, and it's the perfect time to strengthen your team's defenses against the most common threat your business faces: phishing emails that trick employees into clicking malicious links or sharing passwords. This month, run a simple test by sending a fake phishing email to your staff (free tools like KnowBe4's phishing simulator can help), then use the results to hold a 30-minute lunch training where you show real examples of scams and walk everyone through the critical steps: never click links in unexpected emails, verify requests by calling the person directly, and immediately report suspicious messages to you or your IT person. Most importantly, make sure every employee knows they won't get in trouble for reporting a mistake—because a clicked link that gets reported in five minutes causes way less damage than one that goes unreported for five hours. **Today's action:

ACTION ITEM

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

SMB SPOTLIGHT

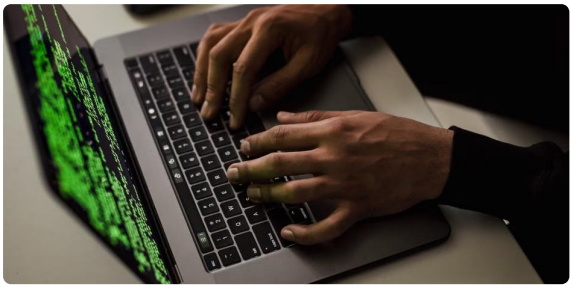
Protecting Your Business



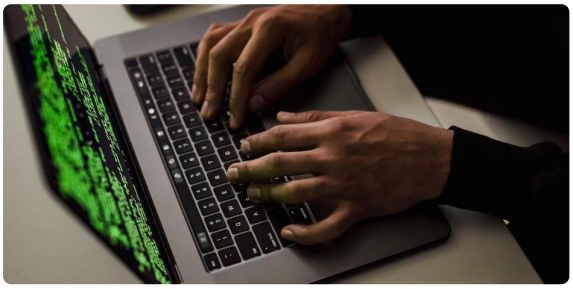
Using TLS to protect data



Post-quantum updates to our TLS guidance



Help the NCSC understand how organisations approach external attack surface risk



China-linked malicious actors called out by UK and international partners for targeting sensitive data globally

INNOVATION

Cybersecurity Advancements

ConnectWise Suspends Cloud Services in Response to Cyberattack

Plex2Shell Exploit Chain Weaponized Against Plex Servers Hours After Disclosure

One Compromised Login Exposed Millions of California Students' Records

Exploited Fortinet Bug Linked to Stealthy FortiGate Implant in Telecom Hack

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 underscore a critical shift I've been watching: attackers are no longer just targeting our networks—they're poisoning the very tools developers trust. The GhostAction campaign disguising credential stealers as fonts in GitHub repositories is particularly concerning because it exploits something fundamental: developers need to pull code from repositories every single day.

What troubles me most is how these supply chain attacks blend into legitimate workflows. A malicious npm package or a compromised GitHub repository doesn't trigger the same alarm bells as a phishing email. Your team downloads what looks like a standard component, and suddenly your credentials are walking out the door.

For businesses relying on development tools and cloud services, this is your wake-up call. If your organization uses GitHub, npm, or any code repositories, you need visibility into what's being pulled into your environment. Basic antivirus won't catch these threats because they're designed to look legitimate.

The good news? These attacks are preventable with proper software composition analysis and code scanning protocols. Let's talk about hardening your development pipeline before you become next week's headline.

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