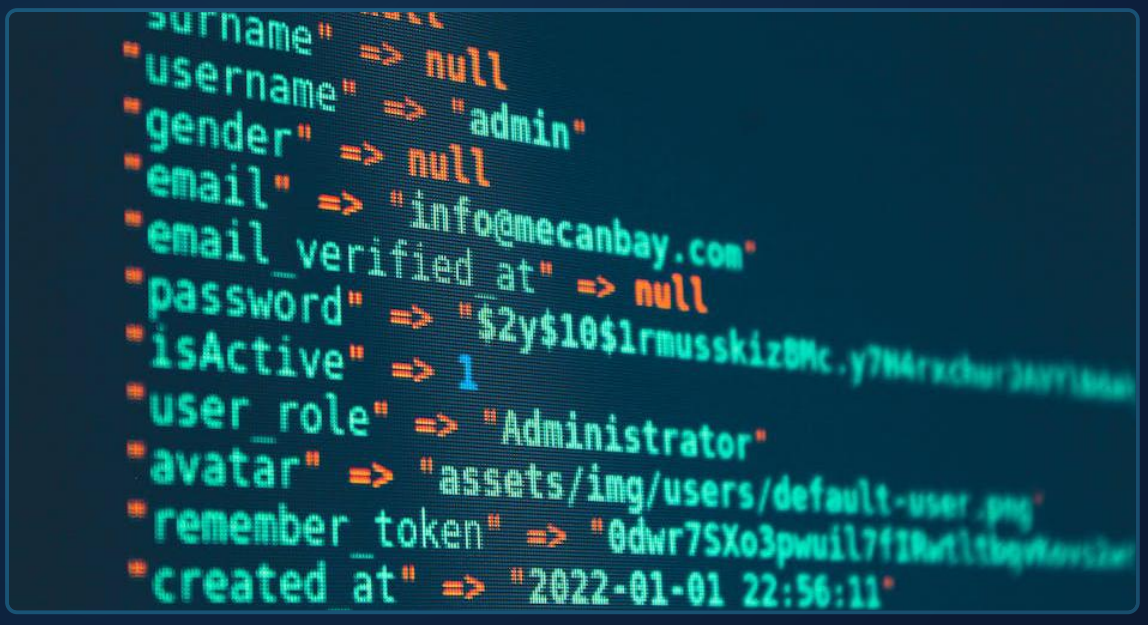
Intelligent Automation

Solutions that are powered by a SECURE Cloud.

MCSP

Managed Cybersecurity Service Provider



VOL. 1 · ISSUE 33

Cyber Shield

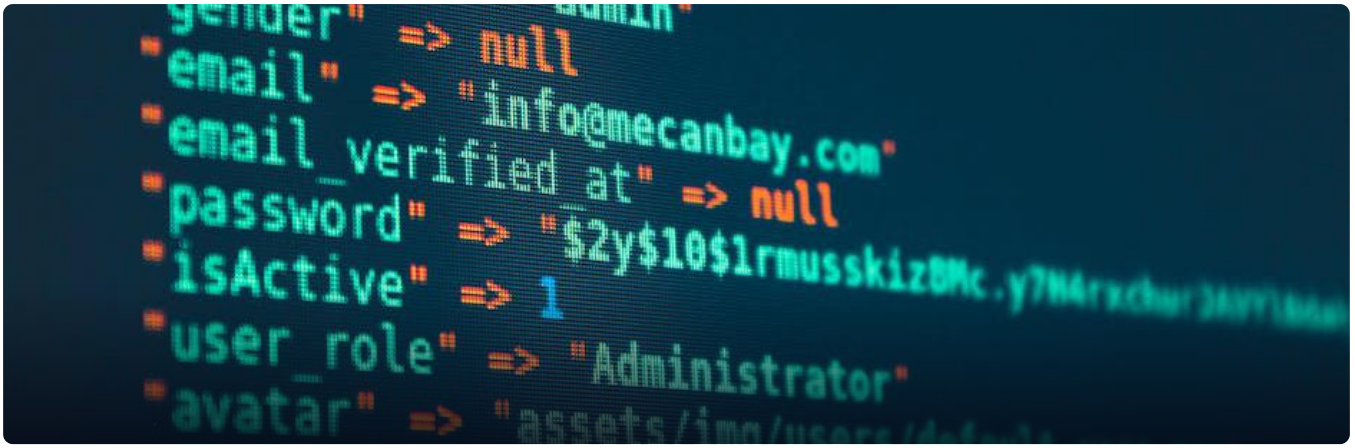
May 19, 2026

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

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

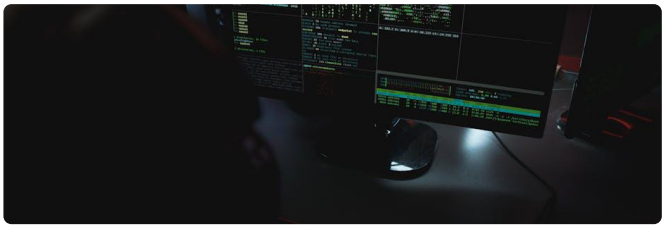
FEATURE

This Week in Cybersecurity



DirtyDecrypt PoC Released for Linux Kernel CVE-2026-31635 LPE Vulnerability

The New Phishing Click: How OAuth Consent Bypasses MFA



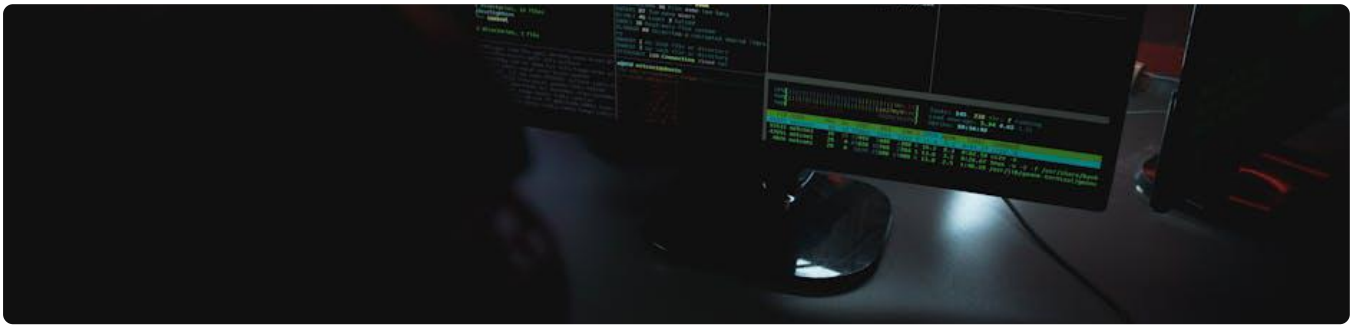
Drupal to Release Urgent Core Security Updates on May 20, Sites Told to Prepare

INTEL

Cyber Threat Intelligence

DirtyDecrypt PoC Released for Linux Kernel CVE-2026-31635 LPE Vulnerability

The New Phishing Click: How OAuth Consent Bypasses MFA



Drupal to Release Urgent Core Security Updates on May 20, Sites Told to Prepare

INTEL

Threat Intelligence — Continued

SEPPMail Secure E-Mail Gateway Vulnerabilities Enable RCE and Mail Traffic Access

Compromised Nx Console 18.95.0 Targeted VS Code Developers with Credential Stealer

Popular GitHub Action Tags Redirected to Imposter Commit to Steal CI/CD Credentials

ISC Stormcast For Tuesday, May 19th, 2026 https://isc.sans.edu/podcastdetail/9936, (Tue, May 19th)

TeamPCP Supply Chain Campaign: Activity Through 2026-05-17, (Mon, May 18th)

WEEKLY TECH TIP

Audit OAuth Apps Before They Bypass Your MFA

OAuth consent phishing lets attackers gain account access without stealing passwords or bypassing MFA directly. Malicious apps trick users into granting excessive permissions that persist even after password changes.

Step 1: Review all third-party apps connected to your business accounts monthly.

Step 2: Revoke access for unused or unfamiliar applications immediately.

Step 3: Train employees to scrutinize OAuth permission requests before clicking "Allow."

Step 4: Implement conditional access policies that restrict OAuth app integrations.

ALERTS

National Cybersecurity Alerts

ISC Stormcast For Tuesday, May 19th, 2026 https://isc.sans.edu/podcastdetail/9936, (Tue, May 19th)

TeamPCP Supply Chain Campaign: Activity Through 2026-05-17, (Mon, May 18th)

[Guest Diary] New Malware Libraries means New Signatures, (Fri, May 15th)

ISC Stormcast For Friday, May 15th, 2026 https://isc.sans.edu/podcastdetail/9934, (Fri, May 15th)

REGIONAL

Regional & Sector-Specific Alerts

ISC Stormcast For Tuesday, May 19th, 2026 https://isc.sans.edu/podcastdetail/9936, (Tue, May 19th)

TeamPCP Supply Chain Campaign: Activity Through 2026-05-17, (Mon, May 18th)

[Guest Diary] New Malware Libraries means New Signatures, (Fri, May 15th)

MAY AWARENESS

World Password Day (May 1)

Security Awareness Spotlight: World Password Day (May 1) World Password Day on May 1st is the perfect reminder to fix the weakest link in your business security: passwords. If your team is still using "Summer2024!" or reusing the same password across multiple accounts, you're leaving the door wide open for hackers who can break into your bank accounts, customer data, and email in minutes. Start today by signing up for a business password manager like 1Password or Bitwarden, then schedule 30 minutes this week to require multi-factor authentication on your most critical accounts—your bank, email, and accounting software.

ACTION ITEM

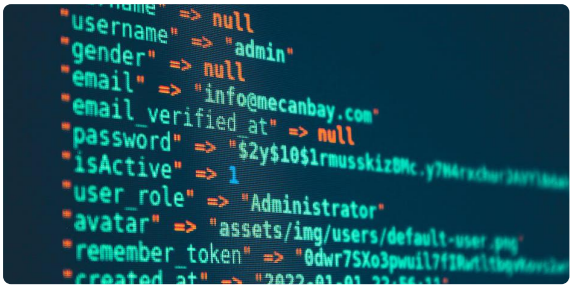
Schedule a 15-minute team security review this week using this month's theme as your agenda.

SMB SPOTLIGHT

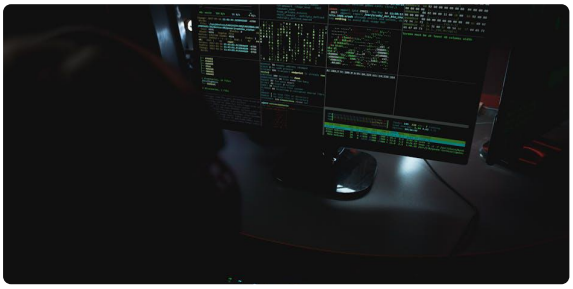
Protecting Your Business

Thinking carefully before adopting agentic AI

10 questions to ask when using AI models to find vulnerabilities



Preparing for a ‘vulnerability patch wave’



Could your choice of metrics be harming your SOC?

INNOVATION

Cybersecurity Advancements

Legacy Windows Tool MSHTA Fuels Surge in Silent Malware Attacks

Unpatched ChromaDB Vulnerability Can Lead to Server Takeover

B1ack’s Stash Marketplace Gives Away 4.6 Million Stolen Credit Cards

Cyber Resilience is the New Business Continuity Plan

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 watching unfold for months: the attack surface is no longer just about firewalls and antivirus software. When I see vulnerabilities like the DirtyDecrypt kernel exploit alongside compromised development tools targeting VS Code users, it's clear that cybercriminals are getting uncomfortably creative about finding ways into our systems.

What concerns me most is the OAuth phishing technique bypassing MFA. We've spent years convincing businesses that multi-factor authentication is their security cornerstone, and now attackers have found a workaround that exploits user trust rather than technical weakness. This isn't about sophisticated hacking—it's about tricking your team into clicking "allow" on what looks like a legitimate login screen.

The takeaway? Your security strategy must evolve beyond technical controls to include ongoing user awareness. The human element remains your greatest vulnerability and your strongest defense. Talk to your team about these threats. If you haven't reviewed your security training lately or want help implementing stronger OAuth policies, now is the time to act.

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