



VOL. 1 · ISSUE 39

Cyber Shield

June 22, 2026

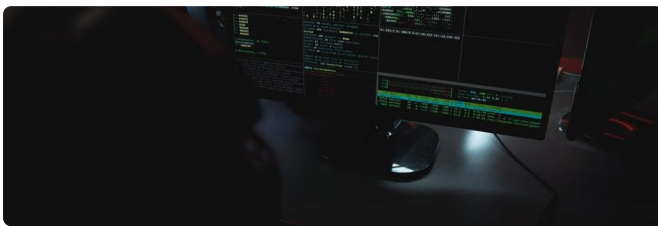
Essential cybersecurity intelligence for small and mid-sized businesses —
powered by AI, delivered by Intelligent Automation, LLC.
INTELLIGENT AUTOMATION, LLC · INTELAMATION.COM · FAIRFIELD, NJ

FEATURE

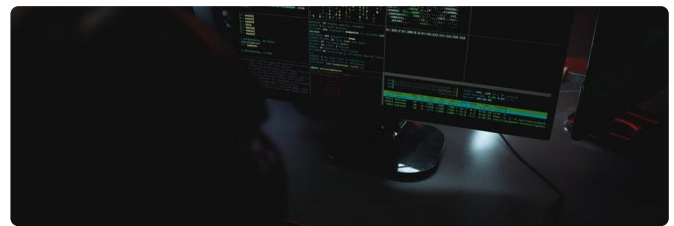
This Week in Cybersecurity



Researchers Detail DifyTap Flaws in Dify That Could Expose AI Chats Across Tenants



29-Year-Old Squid Proxy Bug 'Squidbleed' Can Leak Cleartext HTTP Requests



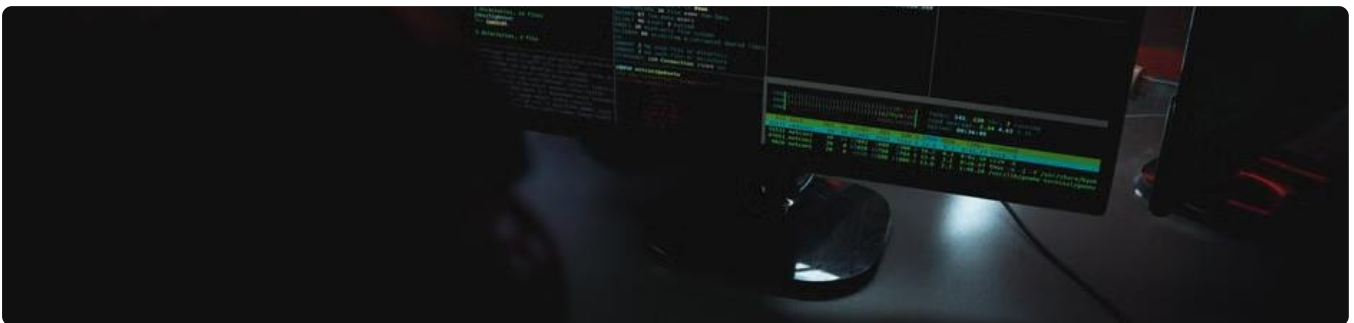
New OXLOADER Loader Uses Malicious Google Ads to Deliver CastleStealer

INTEL

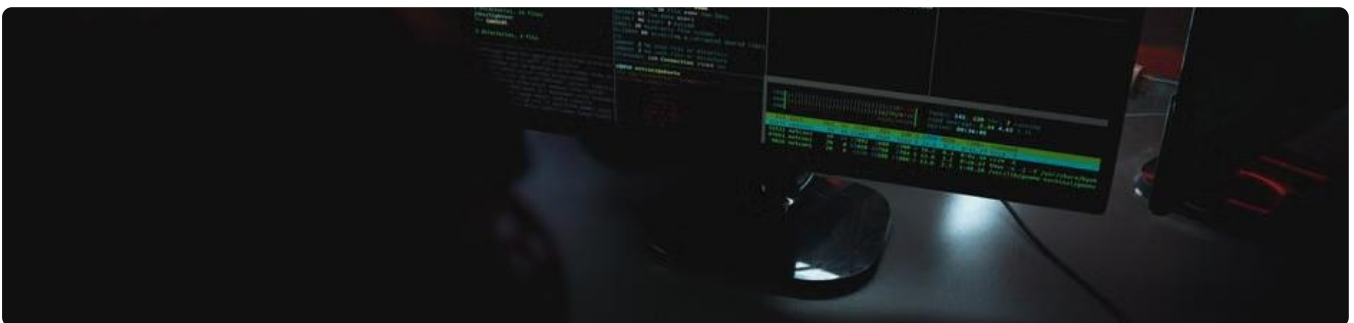
Cyber Threat Intelligence



Researchers Detail DifyTap Flaws in Dify That Could Expose AI Chats Across Tenants



29-Year-Old Squid Proxy Bug 'Squidbleed' Can Leak Cleartext HTTP Requests



New OXLOADER Loader Uses Malicious Google Ads to Deliver CastleStealer

INTEL

Threat Intelligence – Continued

Google Sets Sept. 30 Deadline for Android Developer Verification in Four Countries

Stop Your Legacy Infrastructure from Hijacking Your AI Agents

Weekly Recap: Browser Bugs, EDR Killers, TV Botnet, OpenBSD Flaw, Android Trojan, and More

Webshells Remain Popular, (Mon, Jun 22nd)

ISC Stormcast For Monday, June 22nd, 2026 <https://isc.sans.edu/podcastdetail/9980>, (Mon, Jun 22nd)

WEEKLY TECH TIP

Audit Your AI Tools Before Data Leaks Out

Multi-tenant AI platforms can expose your sensitive conversations to other organizations due to configuration flaws. Recent vulnerabilities show that AI chat tools need the same security scrutiny as traditional applications.

Step 1: Inventory all AI tools your team uses, including free trials and shadow IT.

Step 2: Verify each platform isolates tenant data and maintains SOC 2 Type II compliance.

Step 3: Disable conversation history features and implement data retention policies for AI chats.

Step 4: Review access logs monthly and revoke credentials for unused or untrusted AI services.

ALERTS

National Cybersecurity Alerts

Webshells Remain Popular, (Mon, Jun 22nd)

ISC Stormcast For Monday, June 22nd, 2026 <https://isc.sans.edu/podcastdetail/9980>, (Mon, Jun 22nd)

eBanking Phishing Delivered Through IPv4-Mapped IPv6 Address, (Fri, Jun 19th)

ISC Stormcast For Thursday, June 18th, 2026 <https://isc.sans.edu/podcastdetail/9978>, (Thu, Jun 18th)

REGIONAL

Regional & Sector-Specific Alerts

Webshells Remain Popular, (Mon, Jun 22nd)

ISC Stormcast For Monday, June 22nd, 2026 <https://isc.sans.edu/podcastdetail/9980>, (Mon, Jun 22nd)

eBanking Phishing Delivered Through IPv4-Mapped IPv6 Address, (Fri, Jun 19th)

□ JUNE AWARENESS

Internet Safety Month

June is Internet Safety Month, making it the perfect time to strengthen your team's first line of defense against cyber threats. Most data breaches start with a simple phishing email or a visit to a compromised website, which means training your employees to spot suspicious links and verify sender addresses before clicking can prevent costly security incidents. Today, schedule a 15-minute team huddle to show everyone three real examples of phishing emails (check your spam folder) and establish a simple rule: when in doubt about any email or link, ask your IT person or manager before clicking.

ACTION ITEM

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

SMB SPOTLIGHT

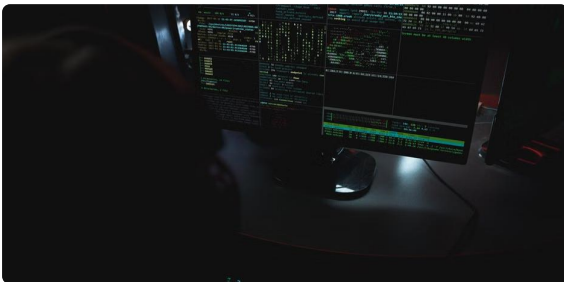
Protecting Your Business



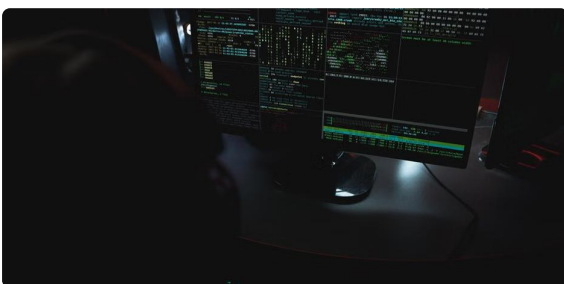
The AI shift in cyber risk: why leaders must act now



The 'vibe coding spectrum' approach to AI-assisted software development



Alert: NCSC issues advice following global targeting of Fortinet firewalls and VPN gateways



NCSC CEO: Hostile states linked to three-quarters of cyber attacks affecting UK's critical systems

INNOVATION

Cybersecurity Advancements

Decades-Old Squid Proxy Flaw ‘Squidbleed’ Can Expose User Data

Attackers Exploit Gravity SMTP Plugin Flaw to Harvest Valuable WordPress Data

North Korean Hackers Blamed for Mastra NPM Supply Chain Attack

What the Latest ShinyHunters Breaches Reveal About Modern Cyberattacks

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 reveal a pattern I want every business leader to understand: vulnerabilities don't discriminate by age or sophistication. Whether it's a 29-year-old flaw in Squid Proxy finally coming to light or brand-new AI chat security issues in Dify, the lesson remains the same—your attack surface is larger than you think.

What keeps me up at night isn't necessarily the zero-day exploits making headlines. It's the decades-old code still running in production environments, quietly processing your data while harboring known weaknesses. Squidbleed is a perfect example: a bug that's been lurking since 1995, waiting to leak sensitive HTTP requests. How many other "Squidbleeds" are hiding in your infrastructure right now?

The good news? You don't need to rip and replace everything overnight. Start with a comprehensive inventory of what you're actually running. Map your dependencies, identify legacy systems, and prioritize based on risk exposure. Small, deliberate steps toward modernization beat reactive panic every time. Let's work together to ensure your infrastructure serves your business goals rather than undermining them.

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