Getting to Know Ian Thornton-Trump: “There Is No Such Thing as Unprecedented”

By Dan Raywood

Published: 2026-04-24 · Archived: 2026-04-26 02:10:44 UTC

Blog

Sometimes Changing the Password on Your Email Mailbox Isn't Enough

Have you ever taken a look at your Microsoft 365 mailbox rules? If not, it might be worth a few minutes of your time. Because newly released research reveals that hackers may already have beaten you to it.A new report from researchers at Proofpoint reveals that approximately one in ten Microsoft 365 accounts compromised in Q4 2025 had malicious mailbox rules created shortly after the attacker...

Blog

April 2026 Patch Tuesday Analysis

Today’s Patch Tuesday Alert addresses Microsoft’s April 2026 Security Updates. The FIRE team is actively working on coverage for these vulnerabilities and expect to ship that coverage as soon as it is completed.

Blog

Fortra Patch Priority Index for March 2026

Get the latest Patch Priority Index from Fortra which highlights critical Microsoft and Google vulnerabilities, covering Edge, Office, Windows, .NET, and key server components.

Blog

AI and Cryptocurrency Scams are Costing Americans Billions, FBI Reports

The FBI's Internet Crime Complaint Center (IC3) has released its 2025 Annual Report, and two threats dominate the headlines: artificial intelligence and cryptocurrency. Together, crypto and AI is reshaping the fraud landscape in ways that should concern organizations and individuals alike.According to its report, for the first time in the IC3's 25-year history, complaints of cybercrime crossed the...

Blog

Fortra Discovers Datto Living Off the Land Binary

Fortra researchers identified an active phishing campaign that delivers a Remote Access Trojan by abusing Datto’s legitimate RMM platform as its command-and-control channel, giving attackers persistent, full remote access

while blending into normal enterprise traffic. The campaign relies on social engineering rather than exploits and is difficult to detect because malicious activity is tunneled through trusted Datto RMM infrastructure over HTTPS.

Blog

BEC Global Insights Report: March 2026

March 2026 BEC threat intelligence from Fortra shows a 53% drop in attack volume, top cash-out methods, gift card trends, crypto scams, and average wire fraud amounts.

Blog

Manage Your Mismatched SOCs

Deciding whether to build an in-house security operations center (SOC) or outsource Security Operations (SecOps) in whole or in part is one of the most important decisions a security leader makes. The question might seem as simple as internal or external, but there are a huge number of factors at play. As a SOC leader, you must make sure the model you choose matches your organization. That means...

Blog

Inside RSAC 2026: Key Takeaways from the Fortra Team

With more than 40,000 attendees converging from around the world, the cybersecurity debates and ideas were constant at RSAC 2026. Here’s what stood out to some of Fortra’s team members who were at the event.

Blog

Data Security for AI Explained

What Is AI Fools? AI Fools Week (also referred to as AI Fools: Stay Sharp!) is an annual cybersecurity awareness campaign created by the National Cybersecurity Alliance. Inspired by the spirit of April Fool’s Day, the campaign highlights how AI-powered pranks and deceptions can go beyond harmless jokes. AI Fools Week’s goal is to educate individuals and organizations on how to spot and avoid AI...

Blog

World Leaks Data Extortion: What You Need to Know

What Is World Leaks?World Leaks is a cyber extortion operation that steals sensitive data from organizations and threatens to leak it via the dark web if a ransom is not paid.Hang on - Isn't That Just Ransomware by Another Name?Well, you can think of it like that if you want - but traditional ransomware attacks involve two things: stealing and encrypting your data, followed by demands for payments...

Blog

Stopping Zero-Day Threats with Cloud Email Security

What Is a Zero-Day Threat? A zero-day attack leverages a previously unknown vulnerability — one that hasn’t been detected by developers or security experts. Because the vulnerability is unknown, there is typically no existing patch or fix, leaving systems temporarily vulnerable until a solution can be developed and deployed. The term "zero-day" refers to the fact that defenders have "zero days" of...

Blog

The Dark Web Demystified: 6 Things You Should Know

Demystify the Dark Web: Learn the difference between the Deep Web and Dark Web, uncover legitimate uses, and explore key risks like doxing, ransomware-as-a-service, and brand impersonation that could impact your business.

Blog

LeakNet Ransomware: What You Need to Know

LeakNet is a ransomware operation that has been active since late 2024, encrypting, exfiltrating, and - if a ransom is not paid - leaking the data of compromised organisations.
