Behind the Digital Curtain: *How Cookie and Tag Management Help Stop Cyber Threats*

Gregory Crabb

September 26, 2024

Unmasking the Invisible: How Digital Breadcrumbs Led to the Fall of an International Cybercriminal

Kovalchuk’s Arrest in Bangkok, Thailand in May 2003

Poll 1

How involved are you in supporting security, fraud detection, or risk analytics for your organization’s website?

Common Website Attacks

- Weak security configurations make systems vulnerable.
- Weak access systems and user controls allow attackers to access user accounts and access restricted data.
- Various API vulnerabilities allow hackers to access or change sensitive data.
- Unencrypted data allows sensitive information to be leaked.

ChatGPT rendering of a leadership team in crisis for an incident Greg responded.

Investigating a Vulnerability

Scenario: Fraudulent Account Creation

- **Platform**: Major financial services website
- **Problem**: A surge of fraudulent account openings
- **Regulator Request**: Why has there been a surge in fraudulent accounts on your website?

- **Poll 2:** If this incident occurred at your organization, would you be part of the response and analysis team?

Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure

“And what many Americans may not be tracking closely is that China is positioning its enormous hacking enterprise—remember, 50 to 1—....to give itself the ability to physically wreak havoc on our critical infrastructure at a time of its choosing.”

“Companies need to familiarize themselves with each specific threat and its particularities, create a plan tailored to each of those threats, and then actually run through those plans with tabletop exercises. Most importantly, know where your crown jewels are, know how to get back up and running in the event of a breach”

- FBI Director Christopher Wray, April 18, 2024

https://www.ic3.gov/Media/News/2024/240708.pdf

What is Threat Informed Defense

A cybersecurity approach that integrates threat intelligence into security strategy, focusing on understanding and countering an adversaries' tactics, techniques, and procedures.

Six Steps Mastery

Identify: Understand the threats.

Define: Define intelligence needs.

Prioritize: Prioritize assets and services.

Collect and Analyze: Collect and analyze information.

Decide and Communicate: Make informed decisions and communicate effectively.

Improve: Continuously improve your threat intelligence program.

Benefits:

Ready

Responsive

Resilient

Poll 3:

Do you have the tools necessary to support the security analytics for your organization’s website?

Stay Connected

Get a free copy of “Mastering Threat Intelligence: Six Steps to Stay Ahead and Secure Your Business” and provide feedback:

Jotform

LinkedIn:

Gregory Crabb

CISO in Residence | Cyber Turnaround Leader | Ex US Federal Law Enforcemen..