CYBERSECURITY BLIND SPOT: THE RISING THREAT OF DIGITAL SUPPLY CHAIN ATTACKS

Cybersecurity and AppSec Measures Fall Short in Addressing Digital Threats

Digital trust & safety platform for safeguarding your customer experience across digital assets

WASHINGTON DC, DC, USA, July 16, 2024 /EINPresswire.com/ -- The recent exploit of the widely-used Polyfill[.]io JavaScript library sent shockwaves across more than 110,000 online destinations, impacting major media, government, and education platforms. This event, reminiscent of the SolarWinds attack on the software supply chain, underscores a growing vulnerability in our digital supply chain—a vulnerability that existing cybersecurity and Application Security frameworks and vendors are ill-equipped to handle.

The essence of the problem lies in the way digital ecosystem cybersecurity is approached. websites, mobile, and CTV apps are digital media – and digital media by its nature is responsive to the persona engaging it. Current security solutions and strategies are predominantly designed to secure static assets, ignoring the dynamic nature of today's digital experience. This oversight is critical, as it fails to account for the increasingly sophisticated methods employed by cyber criminals leveraging third-party services that dominate 90% of website and mobile App source code.

Imagine the consequences of discovering that your ostensibly secure digital platform has been diverting users to malicious sites and code for weeks. This is not just a hypothetical scenario but a grim reality that website owners face while current practices persist.

"Malicious actors are leveraging the dynamic nature of websites, mobile, and CTV apps as a strength. Not only do they use it for mass malware campaigns against online users - they use every day targeting capabilities to drop source code on hyper-specific targets as a first step in larger attacks against governments and corporations," said Chris Olson, CEO of The Media Trust.

"From a technical standpoint, the failure to adapt cybersecurity measures to the dynamic web

environment is a glaring oversight," explains Pat Ciavolella, Digital Security & Operations Director at The Media Trust. "For instance, entities affected by the Polyfill[.]io incident had categorized it merely as "source code" in their inventories—a critical misclassification that overlooks the fact that digital assets are not static but subject to change and manipulation."

The mindset needs to shift; cybersecurity is not just about protecting machines but also about safeguarding people. This approach requires a granular observation of how websites perform and interact with users whoever they are and however they visit the content. Ciavolella notes, "At The Media Trust, we identified vulnerabilities in Polyfill[.]io two weeks before the wider acknowledgment of the breach, spotting unusual redirects and changes in domain ownership in some geographies, but not in others which indicated compromise.

The implications to companies of such attacks are profound, ranging from severe reputation damage to hefty fines for non-compliance with regulatory standards, and significant revenue losses. To combat these threats, businesses must adopt continuous, third-party, client-side scrutiny of digital properties using a variety of devices and profiles to recreate true consumer experience, not just to manage vendor risks and compliance but to ensure the overall safety of their end-users.

As digital platforms continue to evolve, so too must our approaches to cybersecurity. The Polyfill[.]io incident is not an isolated event but a clarion call for a fundamental reassessment of how we look at the digital ecosystem.

Olson emphasizes the ongoing risk, "With current solutions and mindsets, these attacks will continue to happen every day. Digital assets modify depending upon consumer behavior. Criminals understand this, cyber and AppSec do not. The good news is that every innovation by digital attackers can be beaten by a counter-innovation. The question is, will AppSec, Risk, and Cybersecurity practitioners wake up?"

###

About The Media Trust

The Media Trust is on a mission to make the internet a healthier, more valuable place for publishers and consumers. Working with the world's largest, most-heavily trafficked digital properties and their upstream partners, The Media Trust delivers real-time security, data privacy, performance management and quality assurance solutions that help protect, monetize and optimize the user experience across desktop, smartphone, tablet and gaming devices. More than 600 enterprises, media publishers, ad networks/ exchanges, and agencies—including 40 of comScore's AdFocus Top 50 websites—rely on The Media Trust to protect their website, their employee internet use, their revenue and, most importantly, their brand. www.MediaTrust.com.

Kristine Jacobson

The Media Trust
+1 703-867-0575
kjacobson@conveyancemarketinggroup.com
Visit us on social media:
LinkedIn