EINPRESSWIRE

WMC Global Bolsters Cybersecurity Checks in RISQ Score, Ensuring Rapid ATO Detection at Companies Sending 10DLC

WMC Global cyber threat intelligence (CTI) data offers exclusive insight into which partners are being actively targeted by threat actors

FAIRFAX, VA, UNITED STATES, December 5, 2024 /EINPresswire.com/ -- WMC Global, an 18-year industry leader in mobile and digital threat intelligence and a specialist in mobile phishing protection, today announces the release of new informational cybersecurity checks for RISQ Score, its 10DLC vetting product. This cybersecurity protection, using WMC Global's Compromised Credential Recovery product, supports 10DLC campaign service providers (CSPs) and their partners by providing a clear view into the active threat landscape and protecting their messaging connections from being used for malicious purposes.

> "It's more important than ever to secure access to messaging infrastructure and ensure that the rapid detection of these account takeovers is considered in the company vetting process."
>
> *Ian Matthews, CEO of WMC Global*

In recent years, WMC Global has monitored an increase in threat actors of varying degrees of sophistication targeting businesses to gain access to telecommunications messaging infrastructure. When successful, these fraudulent activities lead to account takeovers of communications platform as a service (CPaaS) systems. Last month, criminal charges were issued—including wire fraud, conspiracy, and aggravated identity theft—in the U.S. to five men tied to the prolific Scattered Spider cybercriminal gang that has leveraged telecommunications infrastructure to mass-deploy phishing targeting carrier and CPaaS employees, amongst other targets, for much of 2024. In many cases, WMC Global's Compromised Credential Recovery has detected such exposure in near real time. This underscores why it is crucial for CSPs to maintain a comprehensive understanding of what attack vectors—including unauthorized access to digital assets—threat actors are leveraging through account takeover (ATO) to shore up their infrastructure.

WMC Global's RISQ Score is an automated due diligence system delivering best-in-class vetting for partners looking to connect to carrier messaging pathways. WMC Global offers a proactive approach to messaging protection, ensuring brands receive a fair and unbiased vetting score that simultaneously reflects any ongoing ATO activity and the value they bring to the mobile ecosystem. WMC Global gives clear, documented reasons—supported by verifiable data — for why a CSP's partner receives a certain score and offers a user-friendly appeals process, offering the option to immediately appeal any score and assuring an open opportunity to rectify any issues they have with the ruling. RISQ Score provides a rapid pathway to carrier-approved messaging access for aggregators, content providers, message senders, and others looking to assess the benefits and security risk of their partner relationships.

"It's more important than ever to secure access to messaging infrastructure and ensure that the rapid detection of these account takeovers is considered in the company vetting process," explains Ian Matthews, CEO of WMC Global. "The base standard to gain access to 10DLC messaging is an upfront score, but we recommend more frequent vets to ensure information remains up to date. We continue to encourage CSPs to evaluate the maturity of their internal security posture and that of their downstream messaging partners when selecting a 10DLC vetting provider."

Learn more about RISQ Score and explore WMC Global's other CTI offerings at https://www.wmcglobal.com.

ABOUT WMC GLOBAL

WMC Global is a cybersecurity market leader in digital threat intelligence with specific expertise in mobile, having partnered with Tier 1 mobile carriers for the past two decades and launched the United States' first mobile market compliance program.

The WMC Global portfolio is at the forefront of fighting malicious text messages, eradicating phishing and smishing attacks, and stopping cyber criminals from targeting large brands, financial institutions, and governments. WMC Global helps security teams scale in response to mobile threats by providing its partners with proprietary data feeds of phishing attacks (including intelligence from active phishing kits), mobile investigation and disruption services, threat response and takedown services, automated partner due diligence, and customer experience monitoring.

WMC Global headquarters are in Fairfax, VA, with offices in London, UK. For more information, follow WMC Global on X and LinkedIn.

Kate Matthews
WMC Global
Kate.matthews@wmcglobal.com
Visit us on social media:
X
LinkedIn