EINPRESSWIRE

WMC Global launches GUI for KITIntel, streamlining access to the largest private repository of unique phishing kits

WMC Global takes first steps to simplify client access to their cyber threat intelligence (CTI) product suite

FAIRFAX, VA, UNITED STATES, September 10, 2024 / EINPresswire.com/ -- WMC Global, an 18-year industry leader in digital threat intelligence and a specialist in mobile phishing protection, today announces their release of a graphical user interface (GUI) for KITIntel, its phishing kit analysis product. The freshly launched website provides a streamlined new way to access the existing KITIntel dataset and improved data visualization. Organizations can procure an increased level of clarity around which threat actors are targeting their brand and gain instant visibility into the largest private repository of phishing kits, including intelligence from active kits.

> The best way to protect our clients is to give them immediate access to crucial information that can prevent a phishing attack.”
>
> *Ian Matthews, CEO of WMC Global*

KITIntel is a tool for investigating and comparing phishing kit content within single or multiple kits. Clients can use the GUI to search in the KITIntel dataset for file hashes and content, as well as to retrieve content, and submit external phishing kits for cross-analysis. All files are stored in their original form, allowing users to run complex searches against file content and then retrieve the complete file for offline analysis or additional indicators of compromise (IoC) extraction. Referred to as “The Search Engine for Phishing Kits,” KITIntel was built by threat hunters for threat hunters, CTI Teams and all security analysts.

WMC Global deals with credential phishing as a daily occurrence and understands that the complexity of phishing kits—and the speed at which they morph—creates a challenge for many organizations’ phishing defenses. Phishing kits are an untapped resource for proactive defense, and the data within allows not only for improved detection engineering, but also for attribution and disruption, enabling security teams to rapidly detect exfiltration locations at scale and proactively secure the accounts of compromised victims.

"Launching a GUI for KITIntel was the natural progression to increase our product's ease of use," says Ian Matthews, CEO of WMC Global. "The best way to protect our clients is to give them immediate access to crucial information that can prevent or stop a phishing attack, and the GUI allows for straightforward access to our extensive phishing kit repository. We've also taken into consideration the simplicity with which we can offer product trials to potential clients. Their immediate understanding of what our data can offer their security teams is paramount."

Phishing kits contain all the files and code related to a phishing website. This can include images, JavaScript, CSS code, PHP code, and directory structures. Kits can deploy malware, collect credentials, detect bots, block IP ranges, generate QR codes, and update dynamically. Phishing kits also include artifacts that can assist in tying different kits together to show they are related and leave vital clues that offer the opportunity to attribute mass campaigns back to the responsible threat actor(s).

"Credential phishing can feel like an endless onslaught for security teams," explains Jake Sloane, Threat Intelligence Manager at WMC Global. "KITIntel provides security teams access to generate their own actionable intelligence and is an unparalleled resource of phishing kit data. It never ceases to amaze me what people find within the dataset."

Learn more about KITIntel 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, stopping cyber criminals from targeting large brands, financial institutions, and governments, and monitoring consumer experiences for industry compliance. 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