Predictive Threat Intelligence: Introducing the New Early DGA Detection Feed

Posted on May 3, 2023

The current cyber threat landscape leaves security teams with no option but to be proactive and continuously aim to stay one step ahead of threat actors. To supplement existing threat intelligence feeds that keep track of known bad properties, WhoisXML API recently launched the Early DGA Detection Feed. This predictive threat intelligence source tracks new domains created algorithmically, leveraging a combination of Machine Learning and Artificial Intelligence, typically identifying pre-weaponizationed domains as they get registered.

Why Include DGA Detection in Your Threat Intel Stack

Threat actors are known to algorithmically create and register large numbers of domains and often purposely delay their weaponization to avoid detection by traditional security engines.

This practice can catch organizations and security teams off guard when the domains are mobilized and become command-and-control (C&C) servers, malware and phishing hosts, or serve as other attack vehicles. Even when security solutions detect the already-malicious DGA domains early, there may already be victims.

Detecting DGA domains as they get registered can help security teams prepare mitigation steps or even preventively block them for optimum security and stricter zero-trust policy implementation.

About Our Early DGA Detection Feed

Early DGA Detection feed predicts DGA domains through the identification of suspicious domain

registration patterns that can only be recognized by Machine and Artificial Intelligence. These domains are already pre-filtered and grouped, saving security teams and researchers processing time and computing resources.

The DGA domain files are made available daily and enriched with in-depth contextual information, including WHOIS registration details and IP host association with data points that can help reveal hidden connections and uncover malicious domain footprints.

“The increasing number of zero-day threats highlights that reactive cybersecurity is no longer enough to protect organizations. The Early DGA Detection Feed aims to help security teams get access to suspicious properties before it’s too late,” Ed Gibbs, Field CTO and world recognized industry expert at WhoisXML API.

Early DGA Detection Feed comes in CSV file format for seamless integration into most systems. ***You may download a sample file here or contact us for more information.***