Predict Phishing Attacks with Our Early Warning Phishing Feed

Posted on July 26, 2023

WhoisXML API recently launched the Early Warning Phishing Feed (EWPF), a new predictive intelligence source that provides daily lists of domains likely to figure in phishing attacks. It aims to supplement and enhance existing phishing detection, brand protection, domain filtering, and law enforcement processes.

“Our Early Warning Phishing Feed provides predictive threat intelligence to help organizations stay ahead of phishing attacks amid today’s fast-moving cybercrime landscape. This new product rightly aligns with the company’s commitment to make the Internet safer,” says Jonathan Zhang, WhoisXML API CEO.

Why Include Early Warning Phishing Feed in Your Threat Intel Stack?

Phishing remains one of the top attack types threat actors use to infiltrate systems and launch more damaging incidents. As a form of social engineering, phishing typically involves seemingly trustworthy domain names often banking on the reputation of imitated entities.

Monitoring new domains posing as a brand or containing a widely used text string can help security teams, cyber solutions developers, and brand managers detect risky domains prior to activation for phishing and other malicious activities that can damage a company’s reputation, cause data breaches, or lead to other critical consequences.

Having the capability to zoom in on bulk-registered cybersquatting domains takes phishing detection a step further since malicious actors are known to register several domains in one go

and weaponize them sporadically.

About Our Early Warning Phishing Feed

EWPF contains two types of potentially risky domains separated into different files, namely:

- **Cybersquatting Newly Registered Domains (NRDs):** The NRD files provide daily lists of NRDs closely resembling those belonging to popular brands and containing widely used promotional strings.
- **Bulk-Registered Cybersquatting NRDs:** The typosquatting files contain new cybersquatting domains registered in bulk, listing all domains that belong to the same group.

Both files come with separate statistics or count files that break down the number of cybersquatting domains per brand name or string, providing users with a bird's eye view of how certain brands or terms are imitated in NRDs.

All files are updated and downloadable daily in a consistent CSV format for smooth integration into most systems and solutions.

You may download a sample file here or contact our sales team for more information.