CYREN BY DATA443

Cyren Threat InDepth

Phishing and Fraud URL Intelligence

Challenge

With more than 90% of enterprise breaches starting with a single email, security operations (SOC) teams are constantly locked in a battle to protect their enterprise against evolving email-borne threats. Phishing emails with malicious attachments or links continue to bypass most organizational defenses and reach the end user. Security teams rely on timely, contextual threat intelligence to provide actionable insights that help them stay ahead of these email-borne threats. Any threat intelligence that does not provide the right context can increase a security analyst's workload, resulting in overwhelmed security teams and increased organizational vulnerability.

What is Cyren Threat InDepth?

Cyren Threat InDepth is contextualized, correlated threat intelligence that allows security teams to gain a comprehensive and multi-dimensional view of evolving email-borne threats and make meaningful decisions to combat them. This high-fidelity, actionable intelligence is gathered by analyzing and processing billions of daily transactions across email content, suspicious files, and web traffic to provide unique, timely insights faster than other vendors.

Phishing and Fraud URL Intelligence

- Analyzes billions of internet transactions in web and email traffic to provide real-time info on URLs that are known to serve phishing pages
- Achieved by applying unique technologies and algorithms to gather a rich data set including brand and industry fields
- Context Includes brand and industry information


```
"payload": {
        "action": "=",
        "type": "url",
        "identifier": "585dea02-ca9b-5899-92bb-15bf3b977eb4",
        "first_seen": "2020-03-12T00:45:46.000Z",
        "last_seen": "2020-03-27T01:32:36.000Z",
        "detection": {
            "category": [
                "phishing"
            ],
            "detection_ts": "2020-03-12T02:49:20.000Z",
            "industry": [
                "finance"
            ]
        },
        "meta": {
            "port": 443,
            "protocol": "https"
        },
        "relationships": [ {
                "relationship_type": "resolves to",
                "relationship_ts": "2020-03-12T02:49:20.000Z",
                "ip": "145.14.145.16",
                "related_entity_category": "phishing",
                "relationship_description": "resolves to phishing ip"
```


Benefits of Threat InDepth Phishing and Fraud URL Intelligence

- **Early visibility to new and emerging phishing attacks:** Cyren GlobalView™ Threat Intelligence cloud processes billions of transactions a day to provide the earliest possible indication of evolving phishing threats. Phishing and Fraud URL Intelligence leverages GlobalView to detect new, emerging email-borne threats hiding in plain sight, ensuring early detection.
- **Accelerate threat detection & incident response:** With attackers leveraging phishing emails to continually attack enterprises, timely, contextualized threat intelligence empowers security teams to make smart and meaningful decisions against evolving attacker tactics. By providing security teams with timely, actionable insights, Phishing and Fraud URL Intelligence helps them rapidly prioritize and respond to threats, thereby reducing Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).

DATA443

4000 Sancar Way, Suite 400
Research Triangle, NC 27709

Website: www.data443.com
Email: info@data443.com

US: +1 919 526 1070
UK: +44 203 7693 700