

Cyren Threat InDepth

Malware URL Intelligence

Challenge

Malware attacks cost the average business well over \$2 million. Threat actors are constantly compromising genuine websites and replacing them with authentic-looking URLs that serve malware. Innocent users can get unintentionally compromised, leading to stolen credentials and data theft - inflicting considerable damage on an organization. Security teams rely on timely, contextual threat intelligence to protect the organization against malicious URLs. Lack of timely intelligence can result 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 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, malicious files, and web traffic to provide unique, timely insights.

Threat InDepth's Malware URL Intelligence

- Analyzes billions of internet transactions in web, file, and email traffic to provide real-time info on URLs serving malware.
- Achieved by applying unique technologies and algorithms to gather a rich data set of malicious URLs and its associated artifacts.
- Contextual information includes first seen and last seen timestamps, associated IP addresses, and associated files.

```

{
  "type": "url",
  "url": "http://192.168.1.100:8080/malware",
  "first_seen": "2020-03-24T01:33:41.333Z",
  "last_seen": "2020-03-24T01:33:41.333Z",
  "malware": {
    "category": "malware"
  }
}

{
  "detectable": "2020-03-24T01:33:41.333Z",
  "meta": {
    "post": "GET",
    "protocol": "http"
  },
  "relationship": {
    "relationship_type": "access",
    "relationship_to": "2020-03-24T01:33:41.333Z",
    "subject": "http://192.168.1.100:8080/malware",
    "related_entity_reason": "malware",
    "relationship_description": "access malware file"
  }
}

```

Benefits of Threat InDepth Malware URL Intelligence

- **Unique visibility to protect against malicious URLs:** Cyren GlobalView™ threat intelligence cloud processes billions of transactions a day to provide the earliest possible indication of malicious URLs hiding in email, web, and file traffic. Malware URL Intelligence leverages GlobalView to detect new malicious URLs allowing security teams to block them and prevent threat actors from inflicting damage on your organization.
- **Accelerate threat detection & incident response:** With attackers leveraging malicious links to continually attack enterprises—timely, actionable threat intelligence empowers security teams to make smart, rapid, and meaningful decisions to protect themselves against financial and reputational damage.