CYREN

Cyren Threat InDepth

Malware File Intelligence

Challenge

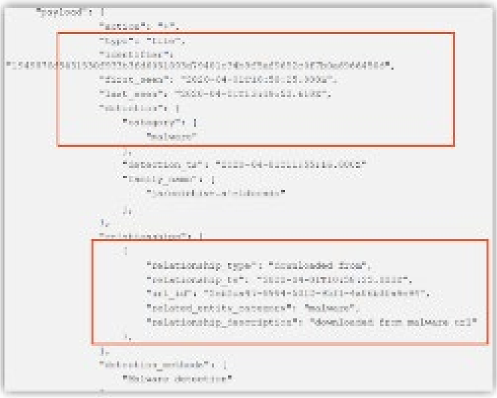
With nearly 94% of Malware being delivered via email, it is clear that threat actors have continued innovating and updating malware in hopes of bypassing organizational defenses and inflicting damage. Cybercriminals are operating in "always on mode" and security teams cannot afford to rest on their laurels and hope that their existing security posture will effectively protect them against advanced, sophisticated attacks. Timely, contextual threat intelligence can help security teams understand the scope of the attack and protect the organization against evolving malware and its associated artifacts. Lack of context 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 File Intelligence

- Analyzes billions of internet transactions in web, file, and email traffic to provide real-time info on files serving malware.
- Achieved by applying unique technologies and algorithms to detect 1000s of new malicious files daily.
- Contextual information includes URL and IP information (including FQDNs within file), malware behavior characteristics, malware family, and relationships to IP addresses and links.



```
    "payload": {
            "action": "[illegible]",
            "type": "file",
            "identifier":
"[illegible]",
            "first_seen": "2020-04-[illegible]",
            "last_seen": "2020-04-[illegible]",
            "detection": {
                "category": [
                    "malware"
                ],
                "detection_ts": "2020-04-[illegible]",
                "family_name": [
                    "[illegible]"
                ],
            },
            "relationships": [
                {
                    "relationship_type": "downloaded from",
                    "relationship_ts": "2020-04-[illegible]",
                    "url_id": "[illegible]",
                    "related_entity_category": "malware",
                    "relationship_description": "downloaded from malware url"
                },
            ],
            "detection_methods": [
                "Malware detection"
```

Benefits of Threat InDepth Malware File Intelligence

- **Context-rich intelligence to provide insight into malicious behavior:** Cyren GlobalView™ threat intelligence cloud processes billions of transactions a day to provide the earliest possible indication of malware hiding in email, web, and file traffic. Malware File Intelligence leverages GlobalView to detect new malware allowing security teams to identify and block advanced threats and prevent them from inflicting damage on your organization.
- **Accelerate threat detection & incident response:** With attackers leveraging malware 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.

www.Cyren.com sales@cyren.com