CYREN BY DATA443

Cyren Threat InDepth

IP Reputation Intelligence

Challenge

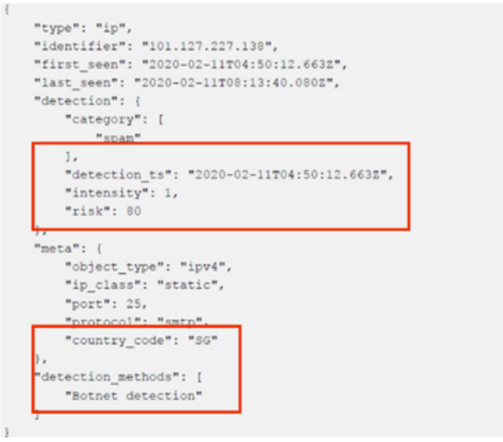
With only 1 in 20* of nearly 7.7 million active IoT devices currently behind a network security tool, it is clear that IoT devices are vulnerable to exploitation by botnet generating malware like Mirai. This continuing growth of botnets brings a new challenge for security teams — to ensure that the host you are transacting with really is 'trustworthy' and not compromised by malware. By leveraging botnet traffic such as distributed denial-of-service (DDoS), they can wreak havoc on organizational security and use the distraction to accomplish their objectives. Security teams rely on timely threat intelligence to help them identify and block malicious IP addresses and prevent their networks from being overwhelmed.

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 and web traffic to provide unique, timely insights.

Threat InDepth's IP Reputation Intelligence

- Analyzes billions of internet transactions in web and email traffic to provide real- time info on URLs that serve spam, phishing and malicious links, and malware files
- Achieved by applying unique technologies and algorithms to gather a rich data set including zombie hosts and their activity
- Contextual information includes threat intensity, risk score, country of origin, and relationships



```
{
    "type": "ip",
    "identifier": "101.127.227.138",
    "first_seen": "2020-02-11T04:50:12.663Z",
    "last_seen": "2020-02-11T08:13:40.080Z",
    "detection": {
        "category": [
            "spam"
        ],
        "detection_ts": "2020-02-11T04:50:12.663Z",
        "intensity": 1,
        "risk": 80
    },
    "meta": {
        "object_type": "ipv4",
        "ip_class": "static",
        "port": 25,
        "protocol": "smtp",
        "country_code": "SG"
    },
    "detection_methods": [
        "Botnet detection"
    ]
}
```

Benefits of Threat InDepth IP Reputation Intelligence

- **Protection against malicious traffic from compromised hosts:** Cyren GlobalView™ threat intelligence cloud processes billions of transactions a day to provide the earliest possible indication of high-risk IP addresses that can potentially overwhelm organizational networks with spam, malicious files, and even DDoS attacks. IP Reputation Intelligence leverages GlobalView to detect new high-risk IP addresses allowing security teams to block them and prevent network issues.
- **Accelerate threat detection & incident response:** With attackers leveraging botnets to continually attack enterprises and overwhelm their networks – timely, actionable threat intelligence empowers security teams to make smart, rapid, and meaningful decisions against high-risk IP addresses. This allows security teams to ensure business integrity and productivity.

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