SentryWire
PACKET CAPTURE PLATFORM

Bolster Your Defenses & Hunt Down APTs, How SentryWire Can Help

The threat landscape is ever-changing and organizations need to be prepared to react to breaches like those encountered by SolarWinds and FireEye. Organizations need to be prepared to identify attack tactics, techniques, and Indicators of Compromise (IOCs) relating to Advanced Persistent Threats (APTs) activities.

SentryWire leverages a combination of network detection mechanisms to provide flexible, lightweight, and adaptable Network Security Monitoring capabilities for analysts tasked with hunting for intrusions and monitoring their networks for anomalies. These types of intrusions are often hard to detect with signatures and rules alone.

Recent intrusions attributed to SolarStorm and the threat actor dubbed “UNC2452” by FireEye are challenging to defend against due to their advanced nature, yet-undiscovered methods, and promulgation on critical infrastructure across an enterprise. However, at some point an adversary has to use the network for their attack to have a profound affect, and their options for obfuscation here are finite.

SentryWire was designed to give analysts everything they need to identify and validate threats using network data for efficient and effective threat hunting. The Cybersecurity threat-scape is disproportionately asymmetric. Advanced threat actors often need only one or two vulnerabilities to penetrate a network. From a prevention perspective, that can be rather difficult considering how often new vulnerabilities are published. As mentioned above, attackers have to use the network, and fortunately, it is tough for them to be perfect in a network environment where they must rely on some form of automation for their attack. This is where the importance of having a packet capture system with both an efficient detection and forensic lookback capability comes into play, allowing your threat hunters to establish the techniques and tactics used in an intrusion, turning that information into an identifiable fingerprint.

Previously with traditional IDS systems, a SOC team would most likely spend almost all of their time in passive and reactive mode, passively waiting for an alert to trigger to start an investigation, responding only when notified leads to a constant game of catch up. Organizations using legacy systems that keep their analysts in a reactive-detection pattern will always struggle to have the edge over advanced threat actors or catch a highly targeted campaign before it has time to promulgate. Consider that advanced adversaries will simulate their attacks in labs on equipment similar to that of their target environment -this level of planning largely makes traditional reactive detection ineffective for detecting the type of threats that SolarStorm and UNC2452 present.

Quick Facts

- Full Packet Capture
- Capture Speeds, 1Mbps to +1Tbps
- Powerful & Fast Search
- Extended Capture Timeline
- Intrusion Detection
- NetFlow Analytics
- Easy Integration/RESTfulAPI
- Advanced Filtering

Incident Response

- Unlogged Activity Detection
- Data Exfiltration Detection
- Phishing Preparation Detection
- Malware Infiltration Detection
- Indicators & Signatures Alerting

Network Troubleshooting

- Forensic Traffic Analysis
- Network Access Control Analysis
- User Anomalous Behavior
- Network Behavior Anomaly
- Encryption Visibility

Hewlett Packard
Enterprise

redhat

SentryWire
PACKET CAPTURE PLATFORM

Analysts with access to SentryWire and utilizing active detection techniques to hunt threats will typically not only have a much higher probability of detecting these types of intrusions, but they will also do it much faster. When facing an advanced adversary, the contrast between analysts and those without access to full packet capture with an extended timeline is even sharper; packet data may be the only data source they have. Systems with minimal storage of days will not suffice.

SentryWire provides you with IDS, forensic search back with signatures, rich dataset of correlating metadata, and the ability to offload pcaps and logs to other systems in an efficient and straightforward manner (use what you have!). In addition to these capabilities, SentryWire provides you with the following snapshot of capabilities specific to assisting with finding and identifying the SolarStorm and UNC2452 campaign in environments with SolarWinds Orion:

Using this IDS Lookback capability allows an analyst to identify potential threats even if the executable has been modified and encoded. (MITRE ATT&CK T1132.001 Data Encoding: Standard Encoding)

- SentryWire alerts on known-bad MD5 hashes specific to the SolarWinds exploit. This enables easier detection of executables and other files with known MD5 hashes as they traverse the network.
- SentryWire generates logs for all SMB sessions enabling faster discovery of sessions matching the unique patterns of actions the malware takes.
- Using SMB and other SentryWire logs enables the discovery of files being transferred over the network, even if they are transferred using common protocols. (MITRE ATT&CK T1105 Ingress Tool Transfer)
- SentryWire supports the import of blacklisted IP addresses and domains to alert on hosts and domains that the malware has previously used by known SolarWinds Command and Control (C&C) hosts against live network traffic and retroactive traffic captured in the past.
- If there is known compromised infrastructure, SentryWire will alert on all communications coming from these hosts or domains. (MITRE ATT&CK T1584 Compromise Infrastructure).
- Using statistical baselining, SentryWire identifies historical patterns of Windows Updates among many other applications to identify rogue attempts to pull malware to a host.
- Statistical baselining allows an analyst to identify attempts to pull malware through common file transfer protocols and applications, as well as when pulled through a timed service such as Windows Update and dynamically established C2 connections (MITRE ATT&CK T1105 Ingress Tool Transfer, MITRE ATT&CK T1569.002 System Services: Service Execution, and MITRE ATT&CK T1568.001/1568.002/1568.003 C2 Dynamic Resolution).

A10
AVALON
Check Point SOFTWARE TECHNOLOGIES LTD.
splunk>
Gigamon
MAGNET FORENSICS
RiskVision

ArcSight An HP Company
BLUVECTOR
Hewlett Packard Enterprise
FORTINET
LogRhythm The Security Intelligence Company
paloalto NETWORKS
ThreatSTOP

AVAYA
BlackRidge TECHNOLOGY
Extreme Connect Beyond the Network
FORCEPOINT
lunarline
redhat
virsec

Technology Partners

SentryWire partners with the leading security solution providers to extend the power of our packet capture platform. This ecosystem of partner technologies includes governance, risk compliance management platforms, intrusion detection systems, behavior based solutions, hardware and OS providers, other security & industry solutions.

SentryWire
PACKET CAPTURE PLATFORM

Sentry Series capacities and estimated timelines for the configurations specified above will vary with the network utilization rate, the amount of encrypted traffic and the compression rates achieved with your data. Sentry Series configurations subject to change.