RECONSENTINEL
ONLINE SECURITY, ALWAYS ON DUTY

March 16, 2018

Product Overview

The Recon Sentinel™ is a small, inconspicuous cyber security device designed to add a layer of detection and protection above and beyond traditional anti-virus, anti-malware and firewall solutions. Designed for ease of use, the Recon Sentinel works with all routers, firewalls and wireless access points, compliments your existing antivirus and anti-malware solutions, will automatically update its firmware and detects malicious behaviors rather than relying on signatures. Need to manage multiple Recon Sentinels for multiple locations or businesses? No problem. Our cloud based management or mobile application will allow you to manage all of your registered Recon Sentinels, no matter where you are!

Functions Overview

Recon Sentinel was developed to complement your current security solutions, focusing on the first link in the Cyber Attack Cycle; Reconnaissance. Using our ethical hacking backgrounds we designed the Recon Sentinel to detect reconnaissance activity that malware and attackers exhibit when breaking into networks. With this in mind, the Recon Sentinel was developed to work with all devices, and all existing security solutions (anti-virus/anti-malware, firewalls, etc), adding a critical layer of technically advanced detection and protection that is essentially plug-and-play.

There are currently five major functions that the Recon Sentinel provides, and these are detailed below:

Real Time Network Inventory

You can't defend what you don't know. The Recon Sentinel will take an initial "snapshot" of the current network upon first installation. All devices, manufacturers, IP addresses, MAC addresses and Network Services are inventoried and baselined. If anything deviates from this baseline, the Recon Sentinel will detect the change and if the change is significant, i.e. a new device on the network, or a new network service the user will be alerted.

This function fills a very important gap in current cybersecurity solutions that exists today; not knowing what is on the network or if someone has compromised the network with a malicious device. Business customers that do not have the expertise, time or budget to implement a full Network Access Controller solution can implement the Recon Sentinel to keep tabs of authorized or "trusted" devices on the network, and be alerted to any new devices that connect.

Lastly, Information Technology (IT) teams can take advantage of the Network Inventory functions to keep tabs on "Shadow IT" which is when users put unknown or unwanted devices and services on a network without IT staff knowledge or approval. Shadow IT makes the network vulnerable to attacks and difficult to defend and Recon Sentinel helps to eliminate this threat.

Network Reconnaissance Scanning Detection

Most networks cannot detect the presence of a stealthy network scanner. Many malware programs and attackers use network scanning as a way of performing reconnaissance to determine what other devices on a network are vulnerable to attack. While sometimes network scanning is not hostile, often times it can be an early warning indicator of an attacker trying to breach a network and steal information or destroy systems.

The Recon Sentinel has a Scan Detection engine that will detect these scans, even if they are very slow, which is a method used by attackers and malware to avoid detection. Once scanning is detected, the Recon Sentinel will alert the user and show the user which device initiated the scan, giving the user the option to block the device.

Cyber-Deception Traps

“All Warfare Is Based on Deception… Sun Tzu” The Recon Sentinel utilizes a cyber deception engine to present itself as a valuable target on the network. By looking like a device that offers valuable network services, but having no real production value, the Recon Sentinel can offer a low to no false positive intrusion detection capabilities usually only offered on devices costing many orders of magnitude more. Malware, intruders, and other advanced attackers will try and interact with the Recon Sentinel, but once they do, the Recon Sentinel has already detected their presence and can start its defenses.

Once an attack is detected, the user is alerted immediately about the attacking device, and that device can be automatically blocked using the Recon Sentinel’s Active Defense Countermeasures.

Active Defense Countermeasures (ADC)

The Recon Sentinel has the ability to run Active Defense Countermeasures (ADC) against a device that has exhibited reconnaissance activity, a new, “unknown” device on the network, or a device attacking a deception service on the Recon Sentinel. ADC will disrupt the communications of the device, not allowing it to communicate over the Internet.

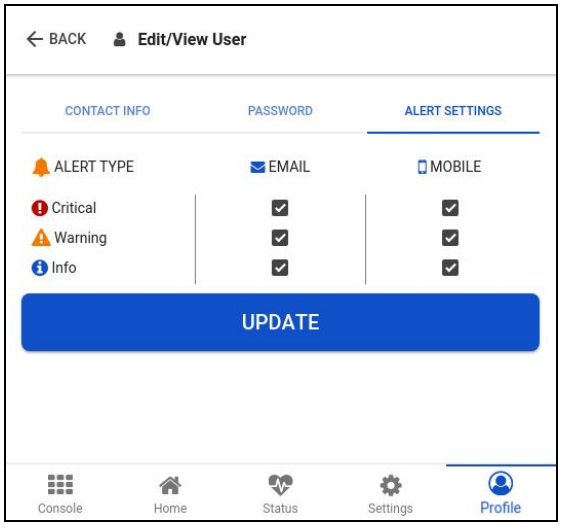
The purpose of ADC is to disrupt the Command and Control (C2) communications of any attacker or malware that has taken control of a device. By interrupting the C2 communications, Recon Sentinel can disrupt a breach or stop the offenders from exfiltrating data via the affected device.

We accomplish ADC by tricking the affected device into believing that it’s path to the Internet is through the Recon Sentinel, where we route that traffic to the ‘bit bucket’. This makes it extremely difficult for the offending device to connect to the Internet (if at all), until the ADC Block has been turned off.

ADC provides a simple, yet very effective way to block Internet communications to affected devices.

Instant Alert Notifications

The Recon Sentinel has the ability to alert a user in multiple ways, all user-configurable via our mobile app.



Users can choose the type of alerts they wish to be notified for, if they want to receive an in-app mobile alert, email or both.

Once an alert is received, the in app wizard will walk the user through the alert, describing what the alert is, the behavior that triggered the alert and what they can do to remedy the alert if applicable.

Other Advantages:

Sideband vs Inline:

A device is considered to be ‘inline’ if it is connected between the internet and the router/modem. This gives the device the ability to scan each packet that travels from the network out to the internet and back. The drawbacks to using an inline device are:

- Difficult setup – this requires the user to reconfigure their existing router connection and is typically above the normal users technical capabilities
- Slower Internet speed – Improperly configured inline devices, because they monitor all packets going in and out of the network, can cause a bandwidth slow down, a common complaint for inline devices

A ‘sideband’ device connection means that the device actually connects after the router/modem much like any other device connected to the network (i.e. printer, laptop, mobile device). The disadvantages of an inline device connection are not present with a sideband connection. Although a sideband device cannot see all packets traversing the network, the sideband connection is perfectly appropriate for monitoring network reconnaissance behavior.

The Recon Sentinel was specifically designed to use a ‘sideband’ connection. This means there is no impact to the network speed and it won’t affect internet download and upload speeds. In addition, it makes setup of the device very easy.

Ease of Setup:

Our cybersecurity experts understand the importance of securing networks but also if cybersecurity is too difficult then users will become frustrated and ignore or bypass procedures. With that in mind we designed Recon Sentinel to be very easy to set up. There are three steps to get the device up and running:

1. plug the power in,

2. plug the ethernet cable into your network (doesn’t matter where),

3. register the device online or via the App

The user doesn't have to re-configure or disable their router or add/replace any of their current network infrastructure. There is no need to find the IP address of the Recon Sentinel to configure and use the device. Everything is done through our mobile application.

The Recon Sentinel even tries to help users identify devices they may not know are on their network using the SONAR.

SONAR

Because there are so many different devices including IoT, there are times when the Recon Sentinel will locate a device on the network and the user doesn't know what it is. To solve this problem we created a 'Find' feature in the Recon Sentinel. SONAR sends communication commands to the device and once started the user can disconnect one unknown device at a time. When the communication signal is lost the Recon Sentinel reports that the device has been found and the user can add the name of the device in the app.

Summary

Hackers want control of your devices.

Cybercriminals want your data.

They are relentless in their pursuit.

It's time to fight back.

Recon Sentinel is your trusted partner in the war against cyber-attacks and cyber-crime. By utilizing behavior analysis to detect anomalous behaviors in the beginning of the attack-cycle, we offer an additional layer in your defense-in-depth strategy. Whether you are a home user, small business or enterprise customer, Recon Sentinel is the right choice for cybersecurity.

RECON SENTINEL - ONLINE SECURITY, ALWAYS ON DUTY