REDSOCKS
malicious threat detection

RedSocks Security
Malicious Threat Detection Solutions

When it comes to Malware and Advanced Persistent Threat (APT) protection, many organizations have a false sense of security. Many believe they have secured their key services against these threats simply by deploying anti-virus solutions or firewalls in their infrastructure. However, today's malware has become sophisticated and widespread enough to bypass many, if not all, of these defensive security measures. Infections typically go undetected for an average of 187 days, causing serious damage to organizational health.

Many security experts argue that the days of preventing the compromising of your network are over. Modern day heterogeneous networks with wireless protocols, VPN connections, BYOD, tablets, smart phones and many more externally accessible services, contain so many entry points into your business systems and data that protecting them all is futile. Of course this doesn't mean we should give up and let the cyber criminals run free but it does mean that we must focus our efforts and investments differently than in the past.

The trick to controlling risk is to strike the right balance between awareness, prevention and detection.

Experience has shown that fighting malware efficiently using traditional detection methods is no longer feasible, as malware is specifically crafted to bypass firewall and anti-virus software. An effective intrusion detection solution should allow you to react quickly and minimize damage when a malicious activity occurs or when a dormant threat that has previously infiltrated your network becomes active.

Unique concept

As partner of The Hague Security Delta, the proudly Dutch cyber security solution provider RedSocks Security has invented a unique concept for detecting and fighting malware and since 2012, has engineered innovative malicious threat detection solutions to facilitate business continuity. What RedSocks Security offers is passive, continuous network monitoring solutions based on AI, machine learning and (actionable) cyber threat intelligence. These security solutions provide real-time, alerts to enable instant threat response.

Future Proof - Respond to Advanced Persistent Attacks

Detection by design without alert overload, the RedSocks solution is built with APTs in mind. The behavior of endpoints dramatically changes once it is infected by an APT. The RedSocks MTD raises an alert and informs the user on which end-point devices are likely to be infected and which ones are in fact infected. It verifies the "likely infected" devices and alerts to any suspected malicious activity to closely monitor.

RedSocks Malware Intelligence Team

The RedSocks Malware Intelligence Team consists of a group of highly experienced specialists who develop algorithms based on both known and emerging patterns. Thousands of botnets are continuously monitored and over 350,000 pieces of malware are automatically analyzed in terms of behavior and outgoing connections (destination). This information is continuously fed to MTD appliances in the field, resulting in your organization being optimally protected against the latest threats. Once malware is detected, the organization is immediately alerted with all necessary technical information, enabling them to counteract the infection. If a Service Level Agreement (SLA) is in place, RedSocks Security specialists are able to provide a tailored solution (on site).

Why RedSocks Security?

- **Non-Intrusive** network monitoring that protects privacy and information security from both ends.
- **Non-Stop** Network Monitoring that alerts your organization the instant malicious activities take place.
- **Limitless** Data Retention opportunities to retrace potentially malicious network activity and used in forensic analyses.
- **Overview of blind spots** in an organization's network infrastructure and the (potential) malicious activity therein.

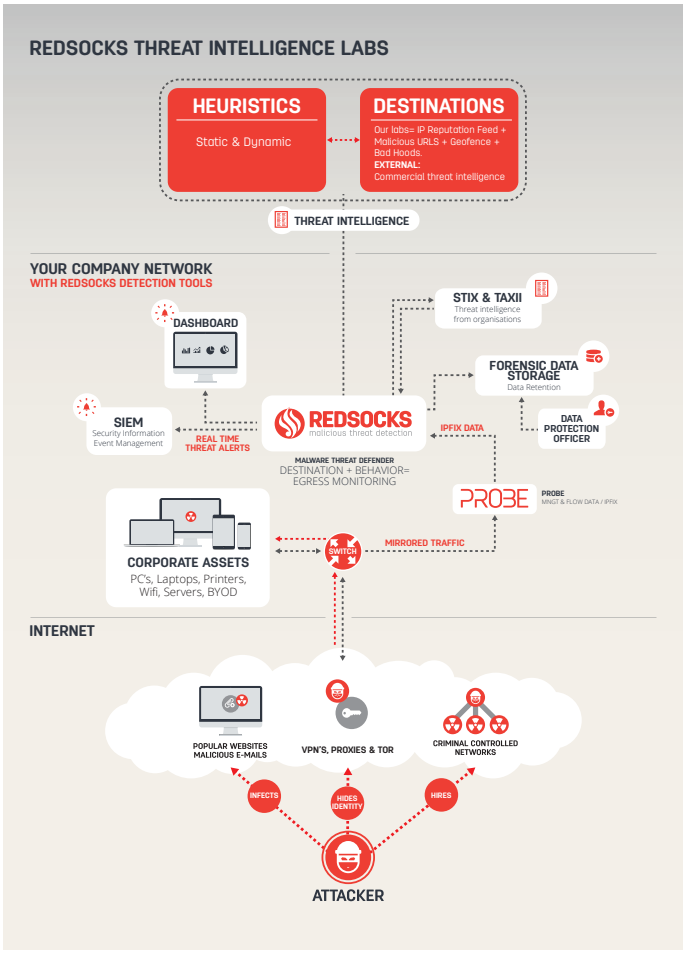
How does it work?

The RedSocks Security solution architecture is plug-and-play and detects malicious threats by monitoring network traffic in real-time for all (potentially) malicious outbound communication.

At RedSocks Security, our clients' data security and data privacy is our primary concern. Our systems, the MTD and the flow monitoring set ups are designed with that principle in mind.

The RedSocks Security Probe - a device that has access to full packet streams - is designed for point-to-point connectivity to a RedSocks Malicious Threat Detector (MTD), e.g., for time synchronization, requires no dedicated Internet connectivity and has no on-board data storage. The Redsocks MTD, both a flow collector and analysis application, provides forensic data storage. In addition, the MTD supports transport over encrypted channels using (D)TLS, which ensures transport is secure when third-party flow exporters are used.

By exclusively focusing on traffic meta-data (so-called flow data) it becomes possible to perform faster analyses over longer periods of time. This enables detection of the most sophisticated malware, APTs and other malicious activities. The MTD only monitors traffic meta-data and not the content itself, thus preventing compromise of confidential corporate information. There is no additional network burden either as the Probe/MTD architecture does not send additional traffic over the network and is not set-up as a Man-in-the-Middle. Using the appliance has no impact on the performance and reliability of the IT-infrastructure. These features make the RedSocks Security solution portfolio a unique asset for a secure and privacy-aware network.



RedSocks Security Solutions and GDPR

The GDPR will impact how organizations gather, process and store personal data. It will affect any business operating from, doing business within, or storing its data in the EU. The penalties for non-compliance will be harsh. Exact terms are being debated but it could be up to 5% of worldwide turnover. In other words, non-compliance is not an option.

The GDPR not only imposes requirements to implement appropriate security measures, but also makes it a mandatory requirement to report a data breach to the relevant data protection authority.

Ascertaining the effective operation of control and security measures taken for privacy protection is not an easy task. When using RedSocks Malicious Threat Detection, data breaches in the technical information infrastructure can be traced and provides proof of the effective operation of the security measures within the network.

FOR MORE INFORMATION PLEASE CONTACT US VIA INFO@REDSOCKS.EU

REDSOCKS
malicious threat detection

www.redsocks.eu

Laan van Nieuw-Oost Indië 133f, 2593 BM Den Haag, The Netherlands • **Tel** +31 (0)88 13 33 333 • **E-mail** info@redsocks.eu • **Website** www.redsocks.eu