REDSOCKS
malicious threat detection

RedSocks Malicious Threat Detection

When it comes to Malware and Advanced Persistent Threat (APT) protection, many organizations have a false sense of security. They believe they have secured their key services against these threats simply by deploying AV devices or firewalls in front of their infrastructure. However, current generation malware has become sophisticated and widespread enough to bypass many, if not all, of these security measures. Infections typically go undetected for a long time, causing serious damage.

Against this background, many security experts argue 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 for controlling risk is to strike the right balance between 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 breach occurs or when a dormant threat that has previously infiltrated your network becomes active.

Unique concept

The Dutch company RedSocks has invented a unique concept for detecting and fighting malware and over the past three years, has built an innovative new hardware and network appliance to exploit it. Traditional network security monitoring uses only inbound Internet traffic. In contrast, the RedSocks Malicious Threat Detection (MTD) monitors outbound traffic.

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 appliance raises an alert and informs the user on which end-point devices are probably infected and which ones are certainly infected. It verifies the "probably infected" devices and alerts to any suspected malware activity to keep an eye on.

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 behaviour and outgoing connections. All this information is continuously fed to every MTD appliance in the field, resulting in your organization being optimally protected against the latest threats. Once malware is detected, the organization will immediately receive a report with all the necessary technical information, enabling them to counteract the infection. If a Service Level Agreement (SLA) is in place, RedSocks specialists will also be able to provide a solution in that respect.

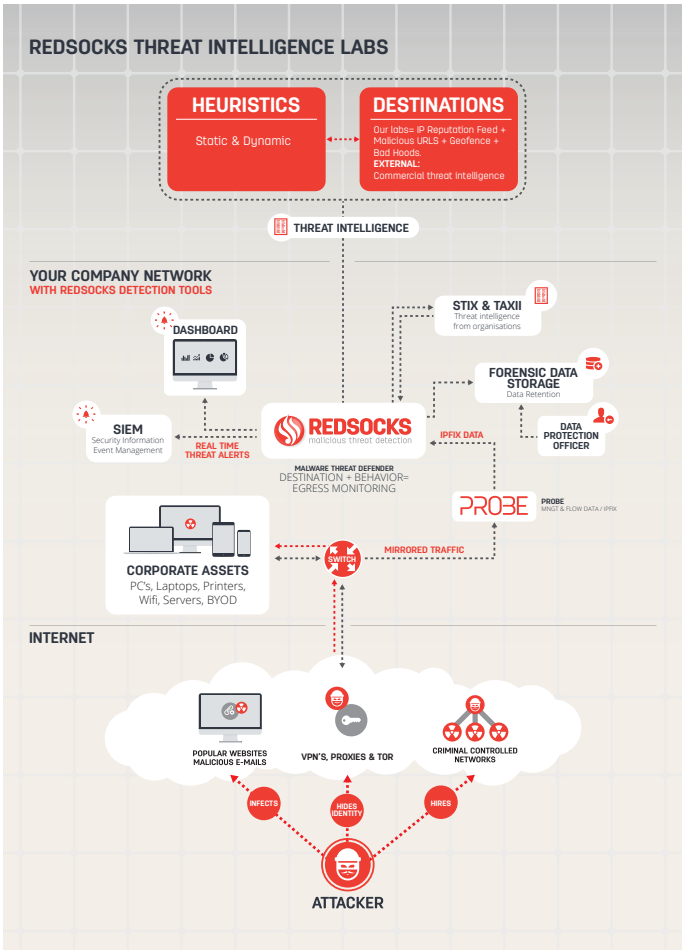
Highlights:

- Detect advanced threats, **plug-and-play** solution that detects malware by checking network traffic in near real-time
- **Forensic security** tool for upcoming EU and Dutch GDPR regulations
- **Non-intrusive** to privacy due to the inspection of meta-data only
- Integrate with existing security systems through syslogs
- No impact on network performance or operation due to **passive monitoring**
- **Scalable** due to the use of NetFlow and IPFIX
- Operating system independent
- **Future proof** - latest security standards STIX/TAXII

How does it work?

The RedSocks Probe/MTD architecture is plug-and-play and detects malware by checking network traffic in real-time for all malicious communication to the Internet.

For RedSocks, the security and privacy of our customers' data is our primary concern. Our systems, the MTD and the flow monitoring setups are designed with that principle in mind.



The @RedSocks-Probe - a device that has access to full packet streams - is designed for point-to-point connectivity to a RedSocks Malicious Threat Detection (MTD), e.g., for time synchronization, requires no dedicated Internet connectivity and has no on-board data storage. It is not possible for captured data to be leaked to the Internet, or to be stolen in the event of a breach. The @Redsocks MTD, acting both as flow collector and as analysis application, provides encrypted (forensic) data storage. In addition, the MTD supports transport over encrypted channels using (D)TLS, therefore 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 analysis over longer periods of time. This enables detection of the most sophisticated malware and APTs. 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 setup as a MitM. Using the appliance has no impact whatsoever on the performance and reliability of the IT-infrastructure. These features make the RedSocks portfolio a unique combination of devices for a security and privacy-aware network.

RedSocks as a compliancy tool under the new GDPR regulations

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 the RedSocks Malicious Threat Detection, data breaches in the technical information infrastructure can be traced and it provides proof of the effective operation of the measures in the network. RedSocks worked together with SBR Powerhouse and have developed a classification, making it possible to include the findings and the proof of proper operation of RedSocks Malicious Threat Detection in the management system. This will enable companies and institutions to take an important step in controlling the risks in terms of liability and expenses resulting from the duty to report data breaches.

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

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.nl • **Website** www.redsocks.nl