REDSOCKS
malicious threat detection

Operational White Paper

June 2016

REDSOCKS
malicious threat detection

Table of Contents

REDSOCKS
malicious threat detection

Introduction

This document introduces some key concepts about malware and how the RedSocks Malicious Threat Detection (MTD) solution can effectively address the dangers inherent in malware attacks.

What is Malware?

Malware is software with a malicious intent — it compromises hardware & software in your network by executing tasks designed solely to undermine their functionality.

Malware often installs itself unnoticeable on laptops, computers, servers and other devices. The list of at-risk equipment is extensive: tablets, smart phones, phone systems, printers, network switches, webcams and network routers; in fact, any connected device can be infected by malware. Equipment that is prone to malware infection also includes off-premise virtualised hosted services (e.g., cloud services).

Malware is particularly dangerous due to its unpredictability. Like a chameleon, on any given moment malware has the ability to change its functionality (the pay-load) and behaviour. This can be remotely modified on a day-to-day or hour-by-hour basis. The ability of malware to change its pay-load renders it impossible to use classical digital fingerprint methods or static analysis to determine its functionality and activities. When malware is detected on a device on which it has been active for some time, damage assessment becomes more difficult. To mitigate this risk, malware must be detected and removed as soon as possible.

How RedSocks MTD works

Security products generally attempt to prevent malware infections by inspecting incoming code, scripts and other content. RedSocks, however, uses a different approach: RedSocks Malicious Threat Detection (MTD) focuses on the communication characteristics of malware that has installed itself on your devices. This method provides instant notification whenever a device becomes infected. The RedSocks MTD Solution placed in a new environment will effortlessly detect malware that has been present for days, weeks or even months.

To detect malware, RedSocks monitors all connections to the Internet. In order to implement this RedSocks MTD delivers an appliance; that is, a custom-built server that is placed on the outer edge of your network. Specifically, the unit is positioned adjacent to the edge router that is responsible for supplying traffic meta-data (called flow data). This unit's sole task is to detect malware by analysing all flow data. This configuration enables the MTD to act practically instantly.

For the detection of malicious behaviour over a longer period of time, the MTD uses heuristic analysis of traffic data history statistics. This feature enables the MTD to utilise a more fine-grained detection method designed to capture malware that slips through security product implementations that are limited to real-time detection.

Blind Spot in Security

A differentiating aspect of the RedSocks approach is that the MTD monitors outbound network traffic for malicious characteristics. This approach differs from the traditional security, which typically only checks inbound network traffic. A firewall, for instance, approves inbound traffic by

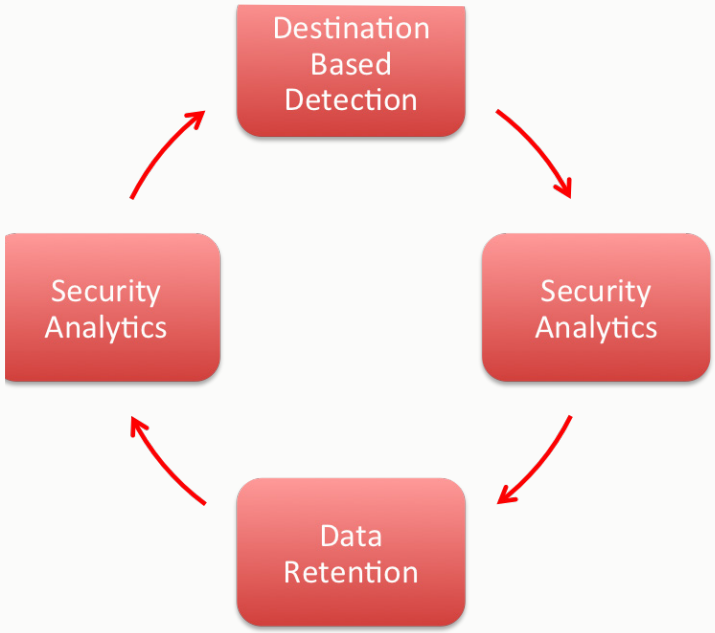
matching it with an earlier outbound request. An anti-virus product approves inbound traffic on content. Both of these methods, however, have blind spots due to their sole reliance on inbound traffic monitoring.

Outbound network traffic will always reveal in what way, by what volume, to what country and how frequent client devices are in contact with destinations on the Internet (i.e., always detect malware activity).

RedSocks MTD is meant to act alongside your existing security measures and acts as a complementary safeguard that is capable of covering the blind spots that traditional tools do not monitor. When traditional solutions fail, RedSocks MTD will be there to defend your system.

Applied Threat Intelligence and Security Analytics

The RedSocks Malware Intelligence team uses applied threat intelligence and security analytics to detect malware. In order to detect malware en define Cyber Threat Intelligence, the team analyses over 150 reputable feed sources, over 30 automated labs and uses various engines. Using our Cyber Threat Intelligence, the detection rate of malware is much larger than traditional anti-virus products, for example. Traditional anti-virus solutions were only able to detect 43% of the malware that RedSocks detected in March 2016. annual report 2015



The RedSocks solution uses three main modules, Destination based detection, security analytics and data retention. These three modules are interrelated and complement each other in order to be able to detected newly developed malware and historic malware. Historical data is used to benchmark newly developed malware to detect whether it communicates to a bad Internet neighborhood, for example.

Data Retention

The RedSocks MTD can store more than 12 months' data in a forensic manner, enabling your organization to make large steps towards being compliant to the European legislation, GDPR and the Dutch Legislation "Meldplicht Datalekken". The data is stored forensically sound and authorized users are able to generate historical reports based on rich IPFIX data.

Alerts

The RedSocks appliance is remotely managed using a secure web interface. This interface presents a convenient overview of the MTD detection process:

Lists of alerts are shown in a dashboard screen with listings showing type, source and destination. For additional automated processing, alerts can be sent as syslog messages to an appropriate sys-

tem in your infrastructure (e.g., a Security Information and Event Management (SIEM) system). Any other type of exchange services is easily supported by the solution.

Constant Vigilance against Malware

RedSocks Malware Intelligence Team

The RedSocks Malware Intelligence Team is a group of trained experts who specialise in malware. Their primary task is to develop risk analyses and compile lists of malicious indicators on a 24/7 basis. The results of their enduring malware research is continuously implemented via updates to the RedSocks MTD appliance.

Significant aspects of these malicious indicators are entries that describe certain Internet Destinations; not all malware, however, exhibits behaviour towards Destinations. Such camouflaged malware can still be detected by the MTD via its use of security analytics. This detection method uses heuristics incorporated within the MTD to detect malicious behaviour even when no specific Destinations are targeted. This heuristic analysis adds a critically important layer of protection for devices in your environment.

The Malware Intelligence Team is the backbone in our fight against malware. In addition to malicious indicator compilation, the Intelligence Team writes detection algorithms for malicious behaviour. In other words, the RedSocks MTD can intelligently discover malware even before dangerous code is even developed! By staying abreast of current trends and IT risks, the Malware Intelligence Team is able to keep ahead of the curve while keeping your infrastructure secure 24 hours a day, 7 days a week.

Large-scale Malware Analysis

Automation in research is an important aspect of our overall speed & effectiveness in terms of malware threat research. On a daily basis up to 1 million (time of writing) new unique pieces of malware are automatically analysed in the RedSocks Lab. In this way, RedSocks keeps close track of new malicious trends in the field; for example, new methodologies that are used to compromise specific devices. Due to this effort, new breeds of malware are identified in our own lab, translated into new detection algorithms and then new malicious indicators are integrated into the MTD via updates.

In addition RedSocks commits extra resources, when needed, to address specialised malware that magnifies over time to become a serious threat. Increasingly, criminals and hostile states are targeting specific companies or industry sectors utilizing specialised malware.

To help combat this trend, a large partner network continuously provides RedSocks with malware collections that are harvested in the wild. This collection frequently contains malware that focuses on Dutch and other Western European targets, particularly those that target departments within companies (e.g., R&D, sales, finance), certain data storage, production and research bodies, or government entities.

Consequently, increased activity in this field may temporarily require extra attention. Our lab is

committed to the swift development and implementation of additional algorithms so that the MTD solution is able to effectively deal with these kinds of attacks.

Large-scale Malware Monitoring

RedSocks continuously monitors tens of thousands of botnets in the wild and in real-time, and many more together with partners. Moreover, we monitor millions of infected systems worldwide that are considered a risk. The result of this monitoring is included in the lists of malicious indicators and captured in new detection algorithms.

Beyond Malware Detection

Analysis of Network Traffic History

The appliance is capable of re-evaluating network traffic history to test against new insights supplied by the latest updates. When receiving new malicious indicators containing detection algorithms, the appliance automatically re-runs an analysis on the network traffic history file. For this the appliance stores up to 12 months of condensed network traffic meta-data.

This feature enables the RedSocks MTD to detect active malware in an incredibly short time-span. It also allows you to determine which devices have been at risk due to a particular short-lived malware outbreak caused by a compromised popular website.

In addition, the re-analysis of previous network traffic enables the detection of a specific type of Advanced Persistent Threat (APT) stealth malware that sparsely contacts its creators for new instructions and barely sends out data.

Academic Research Projects

In close cooperation with universities the RedSocks Malware Intelligence Team adapts new promising innovative academic analyses and algorithms into practical & effective MTD detection methods for day-to-day use.

Additional detection

The RedSocks appliance also protects against malicious, fraudulent, reckless and risky actions such as undesirable user behaviour, improper use of devices, misconfiguration, hijacked settings, abuse of computing resources and abuse of energy. With these additional detections, the MTD acts as your partner in the enforcement of your company's computer and network usage policy.

Alignment of the MTD with your computer and network usage policies can be accomplished via customisation options within the MTD's web interface. Individual detection categories can be enabled or disabled, giving you the opportunity to enforce company policies from a centralised location.

Additionally, the MTD offers custom black listing and white listing to create exceptions for certain devices on policies. White listing is used to enable exclusions for specific clients while black listing is used to include certain Internet destinations in alerts, such as company-specific sites or services that are not allowed to be used or visited.

Malicious behaviour

The detection of malicious behaviour includes connections to the Tor network, the use of anonymising proxies, utilizing suspect chat protocols, the use of mail servers and DNS servers outside of your company's own network and contact with high-risk countries via geo-fencing. Either users or malware can initiate these behaviours — detection may also assist in identifying users with potentially illegitimate and/or fraudulent intentions. The Malware Intelligence Team works tirelessly to create brand new detection algorithms designed to discover malicious behaviour before the malware code itself is even created.

Data Theft

Transferring files outside of your on-premise managed storage facilities poses a high risk for data leakage, data exposure and data theft. The risk of data theft is significant via the use of cloud storage services, instant messaging and remote access tools. Cloud storage in particular is an attractive and straightforward way to transfer large amounts of information outside of the company.

Users may unintentionally be seduced into high-risk behaviour with extremely accessible cloud services or may deliberately move information outside of the company using these tools. Additionally, malware could use cloud-based tools to transfer seized data.

Abuse of Resources

The abuse of network bandwidth, storage capacity, computing power and even energy might be instituted by users or malware. One example is the support of crypto currencies such as Bit coin. At the time of this writing, the support of crypto currency infrastructures—known as coin mining—requires a considerable amount of processing power and represents a significant portion of current malware.

As mining is done for profit, the abuse of device processing power in your network (resulting in energy abuse) is tempting for maximising earnings. In order to detect this improper behaviour on a network, the MTD appliance checks whether devices in the network are part of crypto currency mining pools and P2P networks.

Implementation

Overview

Implementing RedSocks MTD does not interrupt your network: the appliance simply feeds on flow-data from your router. Flow- data is a concentrated representation of your network traffic and, being a protocol feature, is already present in most network infrastructures; consequently, there is no alteration of existing network equipment when the MTD is implemented.

Flow-data is generated on the fly by your router and is simply fed into the MTD for processing. The processing of this data by the MTD does not require any extraneous resources, does not slow down your company's internal network traffic and has no impact on Internet-related activities. A small configuration change in your router settings is all it takes to provide the MTD with network traffic flow-data for analysis.

The MTD can handle various forms of flow-data, with or without a template. Simply let us know about your network and we can advise with regards to compatibility.

Maximum Privacy

The privacy of your data is of vital importance to RedSocks and the implementation of the MTD reflects this approach. RedSocks MTD is a solution-installed on-premise of your company or organisation. All monitoring, processing and alerting are executed on-premise and with a purpose.

Our malware detection solution offers autonomous operation that facilitates maximum privacy: network traffic analysis, alerts and statistics are kept inside your company network environment. External interaction is restricted to an absolute minimum and is limited to the secure retrieval of updates for new malicious indicators. Of course a client can always choose to have the use of RedSocks outsourced to a managed security operations centre, if desired.

Concerning transparency and insight into the MTD's functionality, it is possible to have the MTD fully audited. To facilitate auditing, every aspect of RedSocks Malicious Threat Detection is developed by RedSocks itself. For us, client privacy and MTD transparency is a key aspect in the MTD development process.

Immediate Effect

Immediately upon implementation, the appliance is operationally effective. This is because the MTD loads the latest malicious indicators when powered on. Relevant alerts are therefore generated instantly pinpointing compromised devices in your network. To give insight into MTD's internal processes, the appliance provides a convenient dashboard homepage within its web interface. This feature facilitates a live overview of the detection process and displays the list of alerts.

For more information
info@redsocks.nl
http://redsocks.eu/

Address: Laan van Nieuw-Oost Indië 133f, 2593 BM Den Haag, The Netherlands | **Tel:** +31 (0)88 13 33 333 | **Email:** info@redsocks.nl