THOR

THOR is a portable scanner that detects hack tools, backdoors and traces of hacker activity on end points.

While everyday Anti-virus scanners recognize malware such as viruses, trojans and exploit codes, THOR uses more than 4500 special signatures and a series of more than 20 different checks to examine systems for typical attacker tools, activities in logs, system manipulations, and other elements that can expose attacker activities.

Security analysts, forensic experts and security monitoring specialists at HvS and BSK Consulting regularly update THOR with information from various sources on attack patterns and hack tools. These sources include:

- Threat Intel Reports and Threat Feeds
- Ongoing monitoring of attackers tool sets
  (e.g. disclosed tools, hack tools from underground forums)
- Forensic analyses of compromised systems in customer APTs

THOR can be easily extended to handle individual, client-specific attack patterns (e.g. the detection of specific malware files or certain log entries on the basis of a forensic analysis).

THOR generates different output types: text log, HTML report and SYSLOG. The well-known CEF format as used by ArcSight is also supported. Therefore it is an easy task to integrate THOR‘s logs into any major SIEM system.

THOR can operate completely offline. The scope of application is therefore very flexible. You can easily scan separated network segments like DMZs, collect and merge the log data afterwards.

Focus on APTs

Signatures maintained by security analysts

Specific indicator and signature sources

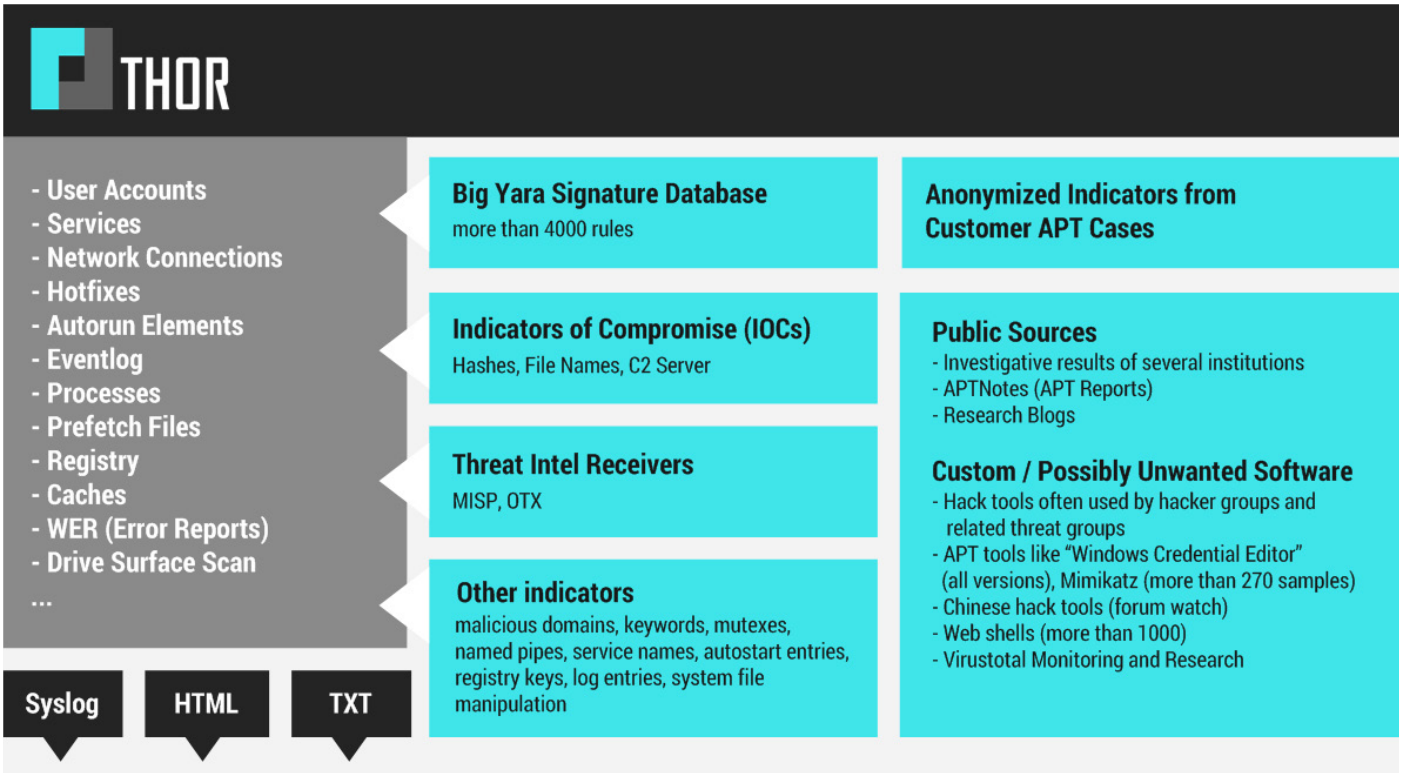
Custom case-related attack patterns

Multiple output formats

High flexibility due to offline scan

AN ANTIVIRUS DETECTS MALWARE
THOR DETECTS HACKERS

THOR



Beside the hard indicators THOR uses a scoring-system that evaluates a score for files based on attributes, contents and meta data. It allows THOR to report suspicious files and detect malware that is yet unknown.

There are three major use cases for THOR:

- **Triage Sweep**
  Scan run on all systems in a system einvironment, reporting to a central SIEM to identify compromised systems
- **Single System Live Forensics**
  Scan run on a single running system reported as suspicious to falsify or verify a possible threat
- **Image Scan im Lab**
  Scan run on a mounted drive image in the Lab to identify known indicators of compromise and speed up forensic analysis

Further advantages / features are:

- Central scan control via ASGARD appliance
- Free Splunk App / Add-on
- Quarantine samples via network (Bifrost)
- Disk surface scan to detect already deleted elements (DeepDive)
- Resource control feature provides high stability and ensures low CPU load during the scan
- Encrypted signatures
- Data protection option to remove personal information from the scan results
- Quick scan mode for fast analysis of the most important elements within minutes
- Golden ticket and skeleton key detection
- Direct contact to the developers / quick feature integration / security made in Germany