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 9000 special signatures and a set of more than 20 different modules to examine systems for typical attacker tools, activities in logs, system manipulations, and other elements that tend to expose malicious activities.

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

- Threat intel reports and threat exchanges
- 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

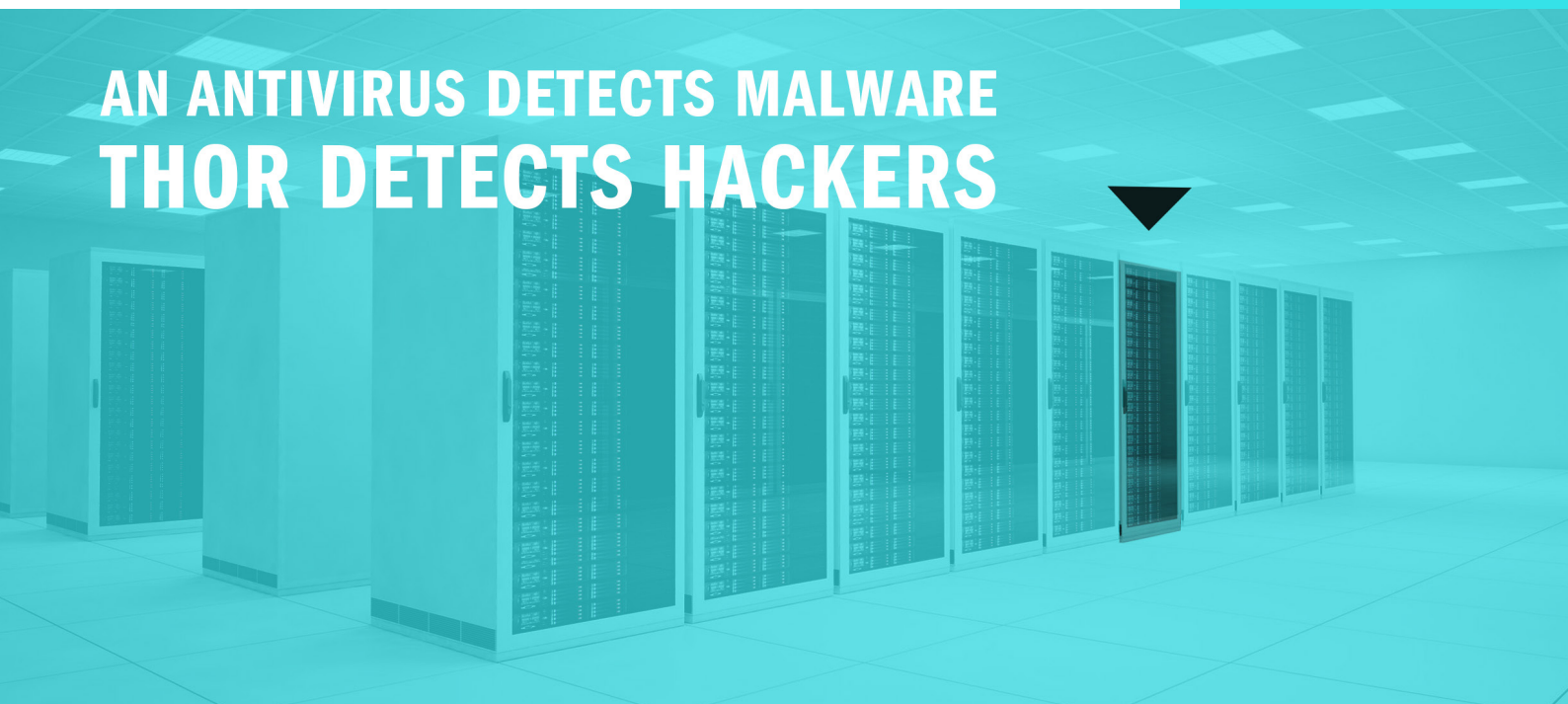**Signatures maintained by security analysts**

Specific indicator and signature sources
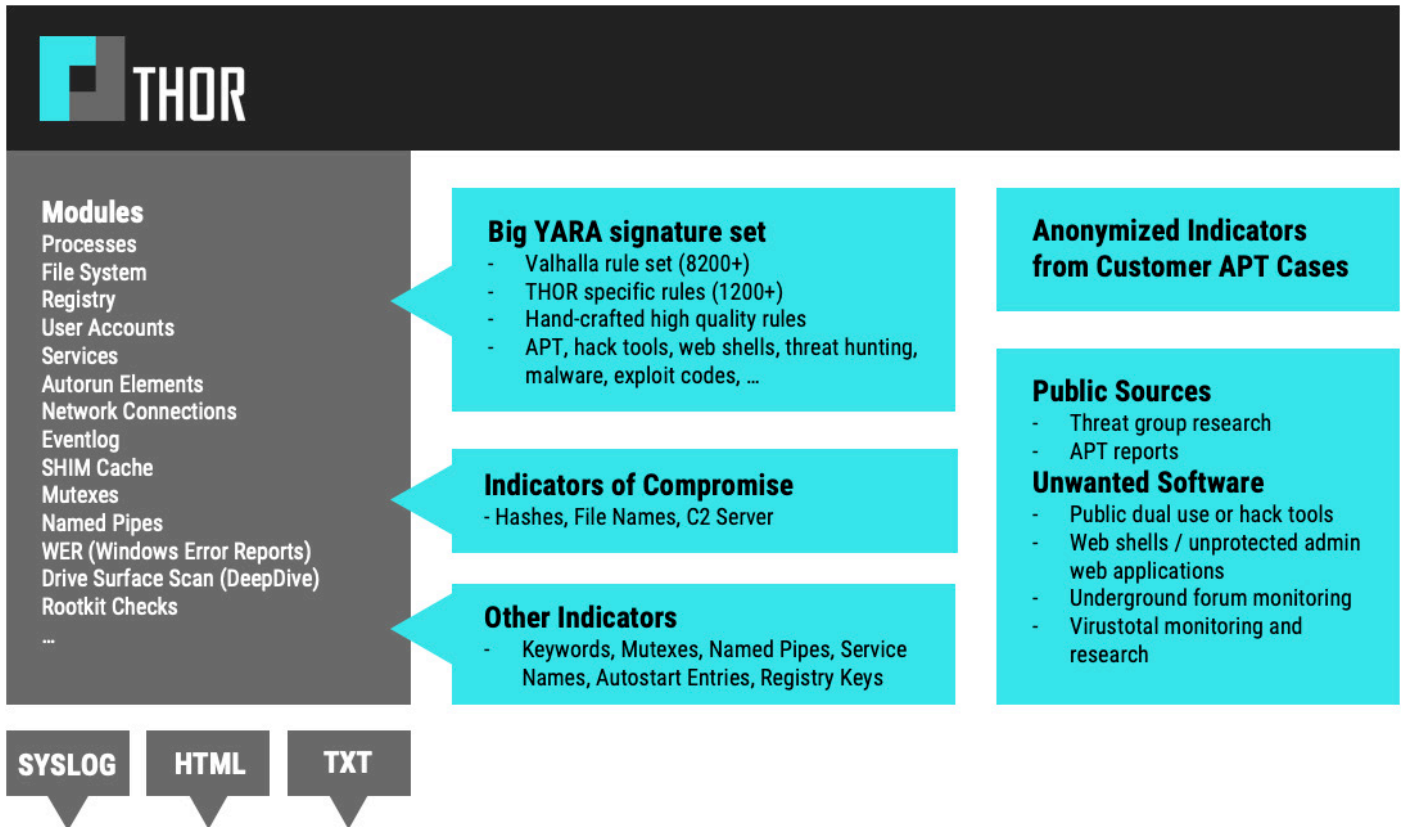
Custom case-related attack patterns

Multiple output formats

High flexibility due to offline scan

AN ANTIVIRUS DETECTS MALWARE
THOR DETECTS HACKERS

THOR

THOR

Modules
Processes
File System
Registry
User Accounts
Services
Autorun Elements
Network Connections
Eventlog
SHIM Cache
Mutexes
Named Pipes
WER (Windows Error Reports)
Drive Surface Scan (DeepDive)
Rootkit Checks
...

Big YARA signature set
- Valhalla rule set (8200+)
- THOR specific rules (1200+)
- Hand-crafted high quality rules
- APT, hack tools, web shells, threat hunting, malware, exploit codes, ...

Indicators of Compromise
- Hashes, File Names, C2 Server

Other Indicators
- Keywords, Mutexes, Named Pipes, Service Names, Autostart Entries, Registry Keys

Anonymized Indicators from Customer APT Cases

Public Sources
- Threat group research
- APT reports

Unwanted Software
- Public dual use or hack tools
- Web shells / unprotected admin web applications
- Underground forum monitoring
- Virustotal monitoring and research

SYSLOG   HTML   TXT

With THOR and it's extensive signature set, you can easily identify compromised systems or suspicious activity.

There are three major use cases for THOR:

- **Triage Sweep**
  Run a scan on all systems in a system einvironment, reporting to a central log management or SIEM system to identify compromised systems

- **Single System Live Forensics**
  Run a scan on a single running system reported as suspicious to verify a possible threat

- **Image Scan in Lab**
  Run a scan 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 previously deleted elements (DeepDive)

- Resource control feature provides high stability and ensures low CPU usage during the scan

- Encrypted signatures

- Public key encrypted output files

- 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