THOR

THOR ist ein portabler Scanner, der es ermöglicht, Spuren eines Angriffs auf Endsystemen sichtbar zu machen.

Während übliche Antivirus Produkte ausschließlich Viren und Würmer erkennen, fokussiert THOR auf Werkzeuge und Spuren von „Advanced Persistent Threats“ (APTs). Er prüft mit über 4500 speziellen Signaturen in mehr als 20 verschiedenen Modulen die gescannten Systeme auf typische Angreiferwerkzeuge, Aktivitäten in Logs, Hintertüren und andere Systemmanipulationen.

THOR wird dazu regelmäßig von Security Analysten bei HvS und BSK Consulting mit Informationen zu Angriffsmustern und Hacker-Werkzeugen aus verschiedenen Quellen aktualisiert. Zu den Quellen für die Signaturen zählen unter anderem:

- Threat Intel Reports und Threat Feeds
- Internes Monitoring von Angreiferwerkzeugen
  z.B. Netzwerk Scanner, Passwort Dumper, Pass-the-Hash Tools, Hack Tool Sets, Web Shells, Werkzeuge aus chinesischen und russischen Untergrund-Foren
- Forensische Analysen kompromittierter Systeme im Kundenumfeld (APT)

THOR kann sehr einfach auf kundenspezifische, individuelle Angriffsmuster erweitert werden (z.B. Erkennung spezieller Dateinamen, Hashes, Schlüsselworte).

THOR generiert je nach Bedarf verschiedene Ausgabeformate: Text Log, HTML Report und SYSLOG. Auch das von ArcSight verwendete CEF Format wird unterstützt. Somit ist eine Anbindung an alle bekannten SIEM-Systeme problemlos möglich.

THOR kann vollständig offline eingesetzt werden und somit auch problemlos separierte Netze wie DMZen untersuchen.

Erkennt typische Angreiferaktivitäten

Signaturen von Security Analysten

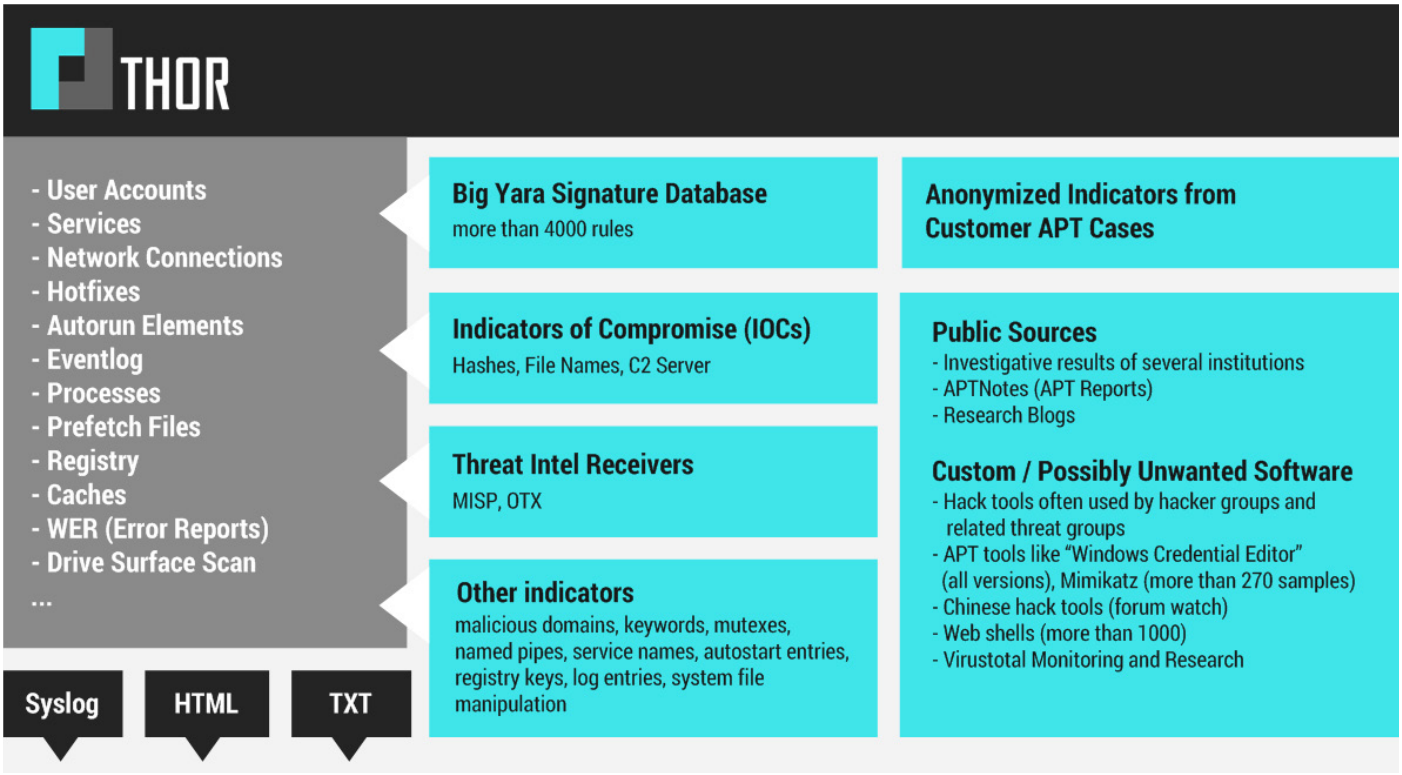
Praxisnahe Quellen

Kundenspezifische Angriffsmuster

Diverse Reporting Möglichkeiten

Hohe Flexibilität durch Offline Scans

THOR



THOR nutzt neben den harten Indikatoren auch ein Scoring-System, bei dem Elemente an Hand verschiedener Kriterien bewertet werden. Dadurch ist es möglich, bisher unbekannte Malware oder Angreifertools zu erkennen.

Es gibt drei wesentliche Anwendungsfälle für THOR:

- **Triage Sweep**
  Scan auf allen Systemen und Lieferung der Logdaten per Syslog an ein zentrales SIEM, um kompromittierte Systeme zu identifizieren
- **Single System Live Forensics**
  Scan eines laufenden und als verdächtig gemeldeten Systems, um Kompromittierung auszuschließen
- **Image Scan im Lab**
  Untersuchung eines montierten Festplatten-Abbildes, um Spuren eines Angriffs zu erkennen und die forensische Analyse zu beschleunigen

Weitere nützliche Features sind:

- Zentrale Scan-Steuerung über ASGARD Appliance
- Kostenlose Splunk App / Add-on
- Zentrale Quarantäne von verdächtigen Dateien (Bifrost)
- Oberflächen-Scan der Festplatte, um von Angreifern gelöschte Spuren erkennen zu können (DeepDive)
- Ressourcenkontrolle für hohe Stabilität und geringe Belastung währen des Scans
- Verschlüsselte Signaturen
- Datenschutz Option, um personenbezogene Informationen aus den Ergebnissen zu filtern
- Quick Scan für eine schnelle Prüfung der wichtigsten Elemente und Ablageorte in wenigen Minuten
- Golden Ticket und Skeleton Key Erkennung
- Deutschsprachiger Support / Kurzer Draht zu den Entwicklern / Security Made in Germany