THOR APT Scanner Upgrade-Info Version 8.1

Renewed technical base ++ New functional features ++ Additional detection features & signatures

Basic Code Refactoring

THOR code has been refactored to gain more flexibility for future needs and higher performance:

- Up to 20% faster than THOR v7 on Servers
- Up to 40% faster than THOR v7 on Clients

Local THORDB - persistent information over several scans. This allows new features.

Log Caching

- Allows scheduled THOR-Run on "offline" systems, e.g. Clients in Home-Office
- Saves results of local THOR-Scans in local THOR-DB (e.g. for offline clients)
- Transfers THOR-results to central SYSLOG-Server or THOR Center

Resume Scan

- Allows THOR to resume an interrupted scan (e.g. due to client shutdown or server patching)
- THORDB stores list of finished modules
- Skips finished modules until scan completes

Delta Scan

- Allows automatic comparison of selected THOR results (e.g. monthly scan of DCs → where are the differences)
- THORDB allows storing previous module results
- THOR analyses changes to previous scan runs and reports changes

Additional detection features & signatures

- Rare Process Starts - Statistics during "Security" Eventlog scan, Which process started how often
- Service Privilege Escalation - Checks system services for privilege escalation vulnerabilities
- AV exclusion - Automatic analysis of elements that have been excluded from Antivirus scanning
- Automatic C2 IOC YARA rule generation - Automatically generates YARA rules from all C2 IOC input on runtime

If you want to see every THOR upgrade including new signatures immediately:

Follow THOR on Twitter: https://twitter.com/thor_scanner/
Visit our website: https://www.apt-detection.com
Read our THOR-Blog: https://www.apt-detection.com/blog/

The THOR APT Scanner is a development of the IT security companies BSK Consulting GmbH and HvS-Consulting AG.
If you wish to cancel your subscription to this newsletter, please send an E-Mail to: info@apt-detection.com