THOR CHEAT SHEET

Components		
thor-upgrade.exe		Update tool (usage with --help)
thor-util.exe		Used with ASGARD: License generation and on-premise update tool
/docs/		THOR manual and cheat sheet
/custom-signatures/		Custom Hash, C2, Filename IOCs ("hash", "c2", "filename" keywords in file name)
/custom-signatures/yara/		Custom YARA Rules ("log", "registy", "process" kewords in filename or default)
/signatures/		Encrypted signature set (sigrev contains version info)
/tools/		Tools; add Sysinternals 'autorunsc.exe' and 'handle.exe'
/config/	thor.cfg	General: Max file size to check, CEF field mapping, Actions on trigger
	directory-excludes.cfg	Exclude directories or files based on regex pattern per line
	false_positive_filters.cfg	Suppress messages that match on regex patterns in this file
/threat-intel/		Receiver scripts for OTX and MISP
changes.log		Information on signatures, features and bug fixes

User Manual

Custom Sigs

Configuration

Excludes

False Positive Filters

Signature Info

Most Important Parameters	
--quick	Skips 'Eventlog' & scans only most important locations
--intense	Do an intense scan (no skips on unknown file types)
-e *output-path*	Write all output files to the given target path
-s *target[:port[:type:[prot]]]*	Syslog target, port, type (DEFAULT/CEF), protocol (UDP/TCP)
--nolog / --nohtml / --nocsv	Disable output files
--fsonly -p *path [path2 ...]*	Scan only a given target path (useful in testing)
--noresume	Disable the automatic resume on the last scan position
--allhds	Scan all local hard drives (no removable / network drives)
-e *number-of-days*	Do only scan the last X days of the Windows Eventlog
-d	Debug output

Syslog Output

Lab Scan

Custom YARA Rule Condition Extensions					
filename	**filepath**	**extension**	**filetype**	**md5**	**id (Eventlog)**
pdump.exe	C:\temp	vbs	EXE	a56df ...	1102

Custom YARA Meta Data Extensions			
nodeepdive = 1	**falsepositive = 1**	**type = "file"**	**type = "memory"**
Don't apply rule in DeepDive	Reduce total score by score defined in this rule	Don't trigger in ProcessCheck	Don't trigger in FileScan

Custom YARA Rules

Automatic Adjustment (detection / mode)			Implicit	
Windows Client	**Windows DC**	**1 CPU / <1024 MB RAM**	**--fsonly**	**--intense**
fast	soft	auto-throttle	no-fast	no-soft

Automatic Adjustments