



Consulting

bsk consulting

[BSK Consulting GmbH](#) Security

## What We Do

Security Consulting, Projektmanagement, Sicherheitsaudits, Risikoanalysen, Planung, Umsetzung, Betriebseinführung von Sicherheitslösungen

## Unser Team

- Unternehmen »
- Dienstleistungen »
- Produkte »
- Blog
- Downloads »
- Partner
- Kontakt

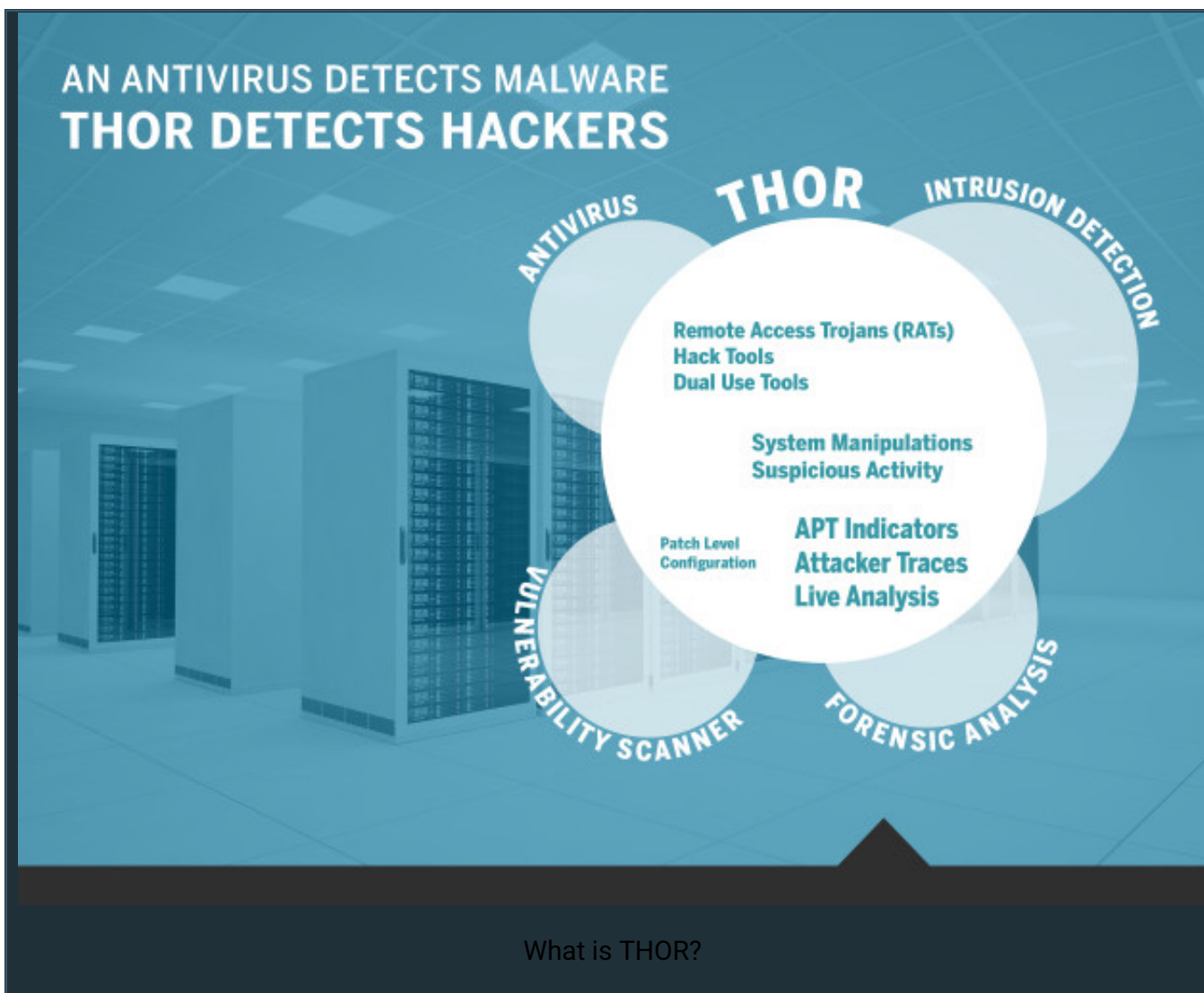


# APT Scanner THOR (EN)



Our APT Scanner THOR is the only flexible tool on the market that is able to evaluate the full extend of security incidents within your corporate networks in order to treat them appropriately.

In contrast to common Antivirus solutions THOR focuses on the detection of attacker activity. While well-known Antivirus solutions are configured to detect malware like trojans, worms and some types of exploit code, THOR performs a deep system analysis using more than 20 modules to reveal hidden attacker activity in log files, typical attacker tools, anomalies within the user accounts, sessions, error reports, dump files, network connections and many other check items.



In contrast to other incident response solutions THOR needs no installation as an agent, it can be configured to use only a small amount of system's resources and works fully compliant with German data privacy regulations (German Data Protection Act, European privacy policy).

The basic features of THOR

- Scans for hacking tools and adversary activities (Triage Tool)
- Portable – no installation needed
- No special requirements. (no Runtime Environment, .NET Framework needed)
- Adjustable to react on adversaries tactics, techniques and procedures
- Several ways to export information
- Throttling the scanning process possible

We frequently update our signature database and heuristic algorithms based on analyses from different sources.

These sources include:

- Forensic Analyses of compromised systems in customer APTs (mainly German DAX and MDAX companies)
- Investigation results of public authorities

- Public Malware and APT reports from different sources in the private sector: Mandiant Reports (like the [APT1 Report](#)), Kaspersky Labs Report („[MiniDuke](#)“, „[Red October](#)“), McAfee Reports („[Operation ShadyRAT](#)“), RSA, CrowdStrike („[Shell\\_Crew](#)“), Trendmicro usw. Full Overview: [APT Reports](#)
- Big collection of hack tools, scanners, password dumpers, web shells and other leaked chinese underground tool sets

```
#####
#####
###   ###  /-----\ /-----\ /-----\ /-----\
###   ###  /-----\ /-----\ /-----\ /-----\
#####
##### The Portable Incident Response Scanner
```

```
F. Roth, March 2014
(C) BSK Consulting GmbH / HvS Consulting AG
Version 6.1.2
```

```
Licensed for: Florian Roth
License valid until: 2014/12/31
```

```
Info: Thor Version: 6.1.2
Info: Run on system: PROMETHEUS
Info: Running as user: neo
Info: User has admin rights: yes
Info: Start Time: 2014-03-21 10:59:13
Info: Sensitive Time Frame: the last 0 hours
Info: Writing Report file to: PROMETHEUS_thor_2014-03-21.html
Info: Argument list: thor.py --nohotfixes --nofirewall --noeventlog -d
Info: CPU count: 2
Info: Memory in Megabyte: 1535
Info: Syslog Export: off
Info: Signature Database: 2014/03/20
Info: License valid until: 2014/12/31
```

```
=> Reading signature and hash files ...
```

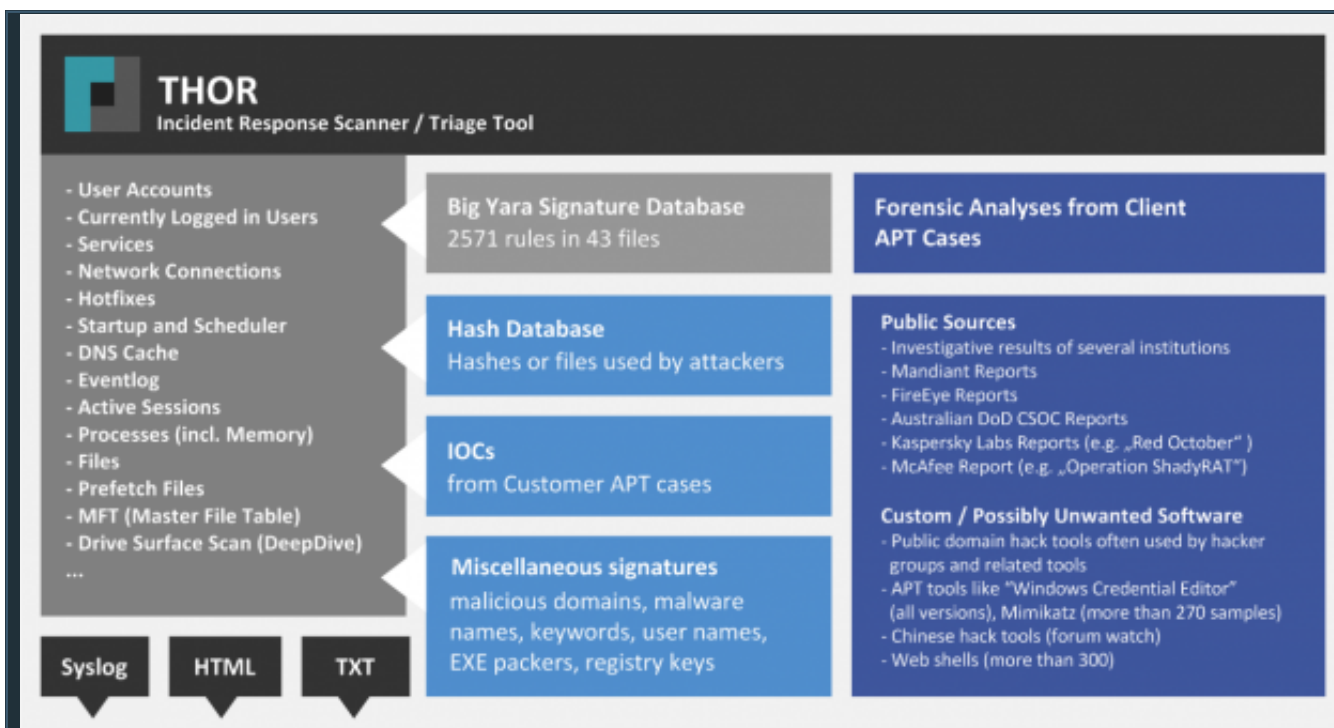
```
Info: > file-type-signatures.cfg initialized with 21 values.
Info: > signatures/filename-characteristics.dat initialized with 799 values.
```

Incident Response Scanner THOR

From these reports and sources we derive numerous „Indicators of Compromise“ (IOC) based on [Yara](#), hash values, file name characteristics, C2 server and other keywords like certain user names, registry values or service names. We the recently implemented support for [STIX](#) (Cybox) and Yara you can easily integrate your own specific signatures.

THOR supports various way to report findings. You may define a output log file in ASCII format, a HTML report or an export via Syslog. The Syslog export function supports the use of UDP, TCP and the CEF format used by the ArcSight SIEM system.























































### Triage Scanner THOR Overview

We also published a free IOC scanner called [LOKI](#) that offers a tiny but relevant subset of THOR's features. This table gives an overview of the various modules and their availability in the different scanners.

Feature	Description	LOKI	THOR
Custom File Hashes	Detect malware or hack tools based on custom file hashes. MD5/SHA1/SHA256		
Custom Filename Characteristics	Detect malware or hack tools based on filename characteristics (Regular Expression)		
Custom Yara Rules	Detect malware or hack tools based on Yara signatures (file and process memory scan)		
Eventlog Analysis	Detect attacker activity and traces of the hack tool usage in the local events written by the Windows event log service		
Registry Analysis	Detect typical keys used in APT groups to maintain persistence on the system		
Profile Directories Check	Checks identifying irregularities in the user profile directories		
SHIM Cache Scan	Detects malicious tools in the SHIM Cache registry section that logs binary executions on Windows systems		
Shell Bags Scan	Analysis of logged shell bags that show which locations of the file systems have been		

	accessed by users		
DNS Cache Analysis	Checking DNS cache entries for suspicious or malicious domain names		
Firewall Configuration Check	Checking the local firewall for suspicious rule definitions		
Active Sessions Check	Checking the current active sessions for suspicious attributes – e.g. length of the user sessions, remote end point		
Process Analysis	Analysis of the current running processes for strange Hooks/File Handles/Mutex definitions, network connections, memory strings, working directories, cloaking attempts		
Active Network Connections	Analysis of all active network connections; users, process ids, end points, strange port numbers		
Network Share Check	Irregularities in the network share definition; user names, share names, permissions		
Open Files Check	Files opened by processes; locations, user, permissions		
LSA Session Analysis	Checking all active LSA sessions for duration or known and typical evil user names from known APT cases		
Services Checks	Analysis of all local services to detect uncommon configurations; service executable location, start type and user account combination, malware names in service image path etc.		
Scheduled Tasks Analysis	Checking the scheduled tasks for malicious entries		
Run Key Contents Analysis	Intensive check of the RUN key entries to determine uncommon code executed at startup		
Startup Element Analysis (WMI)	Analysis of the Startup Elements listed via WMI		
File System Analysis	Analysis of the Master File Table (MFT) and all files on the file system by a specialized scanner that can be equipped with signatures to identify, the attacker's tool set, common backdoor modifications, hash or password dump files, cloaked executables and much		

	more.		
MFT Analysis	Scanning the Master File Table for entries of already deleted files		
Alternate Data Streams (ADS) Check	This check tries to find alternate data streams on NTFS volumes in which attackers may hide their tools and stolen data.		
Host File Analysis	The analysis checks the hosts file for malicious and suspicious entries.		
Windows Error Report (WER) Analysis	This check extracts relevant information from Windows crash reports (Dr. Watson reports) to determine crashes that were caused by exploits targeting known CVE vulnerabilities in browsers, browser plugins and other software.		
Decompressed EXE Scan	Scan a compressed executable in an uncompressed format deflated into memory only.		
Surface Scan (DeepDive)	Analysis of the disks space to find tools that have already been deleted by the attackers.		
TXT Export	Plain text log file of all events reported by THOR.		
HTML Export	Structured HTML Report of all events reported by THOR.		
Syslog Export	Syslog export of the events generated by THOR. This export option is fully flexible. You can define different target ports, multiple target systems, use UDP or TCP and choose between different formats.		
CEF Message Format	Syslog sending messages in Arcsight CEF format to receive warnings and alerts in Arcsight SIEM systems.		
Big Yara Signature Database	THOR includes a huge Yara signature database with more than 2200 rules from different sources. These rules include selected antivirus rules and signatures for hack tools, web shells, networking tools and other software used by attackers on compromised systems. (AES256 encrypted)		
Client APT Signature Database	THOR includes a Yara signature database with more than 240 rules from APT investigations in our client environments. (AES256 encrypted)		



## Custom STIX signatures

Provide your own indicators of compromise via STIX descriptions. The common observables used in STIX will be applied to various check modules.

Especially the „File System Analysis“ and the „Eventlog Analysis“ are time consuming processes with a lot of intensive checks.

## Scoring System

During the „File System Analysis“ every file passes numerous stages in which it receives certain scores according to the check results. THOR checks for certain file name characteristics, the file size, the PE header, extension and the actual file type based on magix header signatures and even decompresses the most common EXE compressor formats like UPX and AsPack. The results of more than 20 checks lead to a total score which is the basis for the different event levels: Notice, Warning and Alert.

We were able to detect previously unknown malware due to this heuristic and characteristics based evaluation

The following picture shows some examples with a reduced set of checks to illustrate the evaluation process.

## Scoring System - Example

Checks	Datei 2: C:\Windows\System32\d.sys	Datei 1: C:\Windows\temp.exe	Datei 3: C:\TEMP\wce.exe
Service Check	is service = +10	-	-
Process Check	-	-	-
Extension	-	.exe = +3    match = -3	.exe = +3    match = -3
Type	EXE = +3	EXE = +3	EXE = +3
File Name Characteristics	[a-z].sys = +15	\temp.exe = +20	wce.(exe dll) = +40
Location	\System32 = +8	\Windows = +8	\TEMP = +15
Size	< 800 kb = +8	< 800 kb = +8	< 800 kb = +8
Owner	-	-	LOCAL_SYSTEM = +5
MAC (Timestamp)	-	-	-
YARA Rules	-	-	WCE Editor = +70
hard IoC	-	-	-
soft IoC	-	String Match = +14	-
	<b>Notice    Score = 44</b>	<b>Warning    Score = 53</b>	<b>Alarm    Score = 141</b>

## Characteristics based Scoring System Examples

### Reporting

Especially the reporting functions are built on practical experiences and are designed to meet the requirements of today's security monitoring infrastructure.

The following output are generated by THOR and can be configured individually via command line parameters:

- **Coloured command line output** gives a quick impression on the severity of the findings. (red=Alert, yellow=Warning, blue=Notice, green=Information, violett=Error, grey=Debug)
- **Text Log:** The format of the Text log is derived from the standard Syslog format, which can be searched via grep very easily and facilitates the process of integrating the Text logs with the logs sent via Syslog in a SIEM system of your choice.
- **HTML Report:** The HTML report provides a quick overview in the header section, alerts and warnings in a special top section and all other events in chronological order below. (recommended output for the analysis of 20 or less systems)
- **Syslog Output:** Sending the events in the Syslog format via UDP or TCP to any port on multiple target systems (ArcSight's CEF Format is also supported)

The following pictures show the different output formats.

```
Warning: Possibly Dangerous file found MODULE: Filescan
FILE: C:\Testing\WinRAR\rarnew.dat SCORE: 62
MD5: ad08fe53a5e484ea568d60544ef3f05c
SHA1: 18629200273779dfa28472d5da28542b69b4dfd2
OWNER: BUILTIN\Administrators SIZE: 20
FIRSTBYTES: 526172211a0700cf9073 / Rar!s COMPANY: N/A DESC: N/A
CREATED: Fri Aug 15 10:23:23 2014 MODIFIED: Fri May 23 17:20:58 2014 ACCESSED: Fri Aug 15 10:23:23 2014
REASON_1: Obfuscated extension - file is RAR Score: +55 Trigger: Extension Value: .dat
Alert: Malware file found MODULE: Filescan
FILE: C:\Testing\xtreme_testing\notepad.exe SCORE: 156
MD5: 8337e178cf7dbcbadd9738316b9027d8
SHA1: 7b4618b152505b81a5965a450f9286aee62eba92
OWNER: BUILTIN\Administrators SIZE: 2871795
FIRSTBYTES: 4d5a90000300000000400 / MZ COMPANY: DESC:
CREATED: Tue Apr 29 09:08:10 2014 MODIFIED: Tue Apr 29 09:14:24 2014 ACCESSED: Tue Apr 29 09:08:10 2014
REASON_1: notepad_ANOMALY / Abnormal notepad.exe - typical strings not found in file Score: +55 Trigger:
le Value: Str1: DC Str2: filename: notepad.exe\n
REASON_2: Xtreme_RAT_Generic Score: +50 Trigger: Generic Match Value: -
REASON_3: File Name Characteristic Score: +50 Trigger: Regex in File Name Value: ^(?!.*SysWOW64|.System
2|.Windows|.winsxs|.WinSxS|.dllcache|.WINXP|.WINNT).*\notepad\.exe$
Warning: Suspicious file name in RAR detected FILE: \creddump.exe PATTERN: creddump SCORE: 70 DESC: Rege
HIVE: C:\Testing\zip\compressed.rar
Alert: Malware name found in RAR FILE: \creddump.exe KEYWORD: creddump ARCHIVE: C:\Testing\zip\compressed
Notice: Suspicious file name in RAR detected FILE: \nbtscan-1.0.35.exe PATTERN: \nbtscan SCORE: 50 DESC:
RCHIVE: C:\Testing\zip\compressed.rar
Notice: Suspicious file found MODULE: Filescan
FILE: C:\Testing\zip\compressed.rar SCORE: 49
MD5: 9844394992e4854e190f3a752f4601d1
SHA1: 87be6bf037bb3febd3b0104de6ca92de346a1773
OWNER: BUILTIN\Administrators SIZE: 30775
FIRSTBYTES: 526172211a0700cf9073 / Rar!s COMPANY: N/A DESC: N/A
CREATED: Fri May 23 18:16:26 2014 MODIFIED: Fri May 23 18:16:26 2014 ACCESSED: Fri May 23 18:16:26 2014
REASON_1: RAR Archive found Score: +30 Trigger: File Type Check Value: RAR
```

THOR Command Line Output



```

2014-08-14 08:49:59 PROMETHEUS/10.0.2.4 THOR: Info: MODULE: Init MESSAGE: Reading YARA rule file thor-ye_scada.yat
2014-08-14 08:49:59 PROMETHEUS/10.0.2.4 THOR: Info: MODULE: Init MESSAGE: Reading YARA rule file thor-ye_trojans.yat
2014-08-14 08:49:59 PROMETHEUS/10.0.2.4 THOR: Info: MODULE: Init MESSAGE: Reading YARA rule file yara-brg-portscanner.yat
2014-08-14 08:49:59 PROMETHEUS/10.0.2.4 THOR: Info: MODULE: Init MESSAGE: Reading YARA rule file yara-brg-webshells.yat
2014-08-14 08:50:00 PROMETHEUS/10.0.2.4 THOR: Info: MODULE: YARA MESSAGE: 42 YARA files with 3015 rules initialized.
2014-08-14 08:50:00 PROMETHEUS/10.0.2.4 THOR: MODULE: InitHead MESSAGE: => Reading False Positive Rules ...
2014-08-14 08:50:00 PROMETHEUS/10.0.2.4 THOR: Info: MODULE: YARA MESSAGE: 2 YARA files with 3 rules initialized.
2014-08-14 08:50:00 PROMETHEUS/10.0.2.4 THOR: MODULE: InitHead MESSAGE: => Reading PEID Rules ...
2014-08-14 08:50:00 PROMETHEUS/10.0.2.4 THOR: Info: MODULE: Init MESSAGE: 3519 YARA PEID rules initialized.
2014-08-14 08:50:00 PROMETHEUS/10.0.2.4 THOR: MODULE: InitHead MESSAGE: => Reading STIX Packages
2014-08-14 08:50:00 PROMETHEUS/10.0.2.4 THOR: Info: MODULE: STIX MESSAGE: Parsing: X:\Workspace\Thor\.\signatures\stix\Appendix_D_FQDNs.xml
2014-08-14 08:50:03 PROMETHEUS/10.0.2.4 THOR: Info: MODULE: STIX MESSAGE: Parsing: X:\Workspace\Thor\.\signatures\stix\Appendix_E_MD5s.xml
2014-08-14 08:50:04 PROMETHEUS/10.0.2.4 THOR: MODULE: InitHead MESSAGE: => STARTING CHECKS
2014-08-14 08:50:04 PROMETHEUS/10.0.2.4 THOR: MODULE: Control MESSAGE: 03/24 => Scanning for malicious mutexs ... (< 1 min)
2014-08-14 08:50:04 PROMETHEUS/10.0.2.4 THOR: Info: MODULE: Mutex MESSAGE: Trying method 2 - .NET Mutex enumeration
2014-08-14 08:50:05 PROMETHEUS/10.0.2.4 THOR: Warning: MODULE: Mutex MESSAGE: Malicious Mutex found in handle KEYWORD: _SHuassist.mtx DESC: Unspec
2014-08-14 08:50:05 PROMETHEUS/10.0.2.4 THOR: MODULE: Control MESSAGE: 06/24 => Analyzing Hosts File ... (0 - 2 mins)
2014-08-14 08:50:05 PROMETHEUS/10.0.2.4 THOR: Info: MODULE: Hosts MESSAGE: Hosts entry ENTRY: www.eamtn.com
2014-08-14 08:50:05 PROMETHEUS/10.0.2.4 THOR: Alarm: MODULE: Hosts MESSAGE: Malware Domain found in Hosts file in DOMAIN: www\.\eamtn\.\com LINE: 10
2014-08-14 08:50:05 PROMETHEUS/10.0.2.4 THOR: Info: MODULE: Hosts MESSAGE: Hosts entry ENTRY: update.microsoft.com
2014-08-14 08:50:05 PROMETHEUS/10.0.2.4 THOR: Warning: MODULE: Hosts MESSAGE: Suspicious entry found in Hosts file in LINE: 10.2.2.2 update.mi
2014-08-14 08:50:05 PROMETHEUS/10.0.2.4 THOR: Info: MODULE: Hosts MESSAGE: Hosts entry ENTRY: xxx.360.cn
2014-08-14 08:50:05 PROMETHEUS/10.0.2.4 THOR: Notice: MODULE: Hosts MESSAGE: Entry with dangerous found TLD: cn ENTRY: xxx.360.cn
2014-08-14 08:50:05 PROMETHEUS/10.0.2.4 THOR: Warning: MODULE: Hosts MESSAGE: Suspicious entry found in Hosts file in LINE: 127.0.0.1 xxx.360.cn
2014-08-14 08:50:05 PROMETHEUS/10.0.2.4 THOR: Info: MODULE: Hosts MESSAGE: Hosts entry ENTRY: microsoft.operaa.net
2014-08-14 08:50:05 PROMETHEUS/10.0.2.4 THOR: Alarm: MODULE: Hosts MESSAGE: Keyword found in Hosts file in KEYWORD: operaa\.\net LINE: 255.0.0.0 m
2014-08-14 08:50:05 PROMETHEUS/10.0.2.4 THOR: Alarm: MODULE: Hosts MESSAGE: Malware Domain found in Hosts file in DOMAIN: operaa\.\net LINE: 255.0
2014-08-14 08:50:05 PROMETHEUS/10.0.2.4 THOR: MODULE: Control MESSAGE: 08/24 => Scanning Eventlog for malicious activity ... (1 - 60 mins)
2014-08-14 08:50:05 PROMETHEUS/10.0.2.4 THOR: Info: MODULE: Control MESSAGE: This could take a while - depending on the number of entries
2014-08-14 08:50:05 PROMETHEUS/10.0.2.4 THOR: Info: MODULE: Eventlog MESSAGE: Checking Microsoft-Windows-Sysmon/Operational Eventlog ...
2014-08-14 08:50:27 PROMETHEUS/10.0.2.4 THOR: Warning: MODULE: Eventlog MESSAGE: Suspicious file name in eventlog entry detected ENTRY: \\??\C:\
2014-08-14 08:50:27 PROMETHEUS/10.0.2.4 THOR: Alarm: MODULE: Eventlog MESSAGE: Malware name found in eventlog entry ENTRY: \\??\C:\Testing\gse
2014-08-14 08:50:27 PROMETHEUS/10.0.2.4 THOR: Warning: MODULE: Eventlog MESSAGE: Suspicious file name in eventlog entry detected ENTRY: \\??\C:\
2014-08-14 08:50:27 PROMETHEUS/10.0.2.4 THOR: Alarm: MODULE: Eventlog MESSAGE: Malware name found in eventlog entry ENTRY: \\??\C:\Testing\gse
2014-08-14 08:50:27 PROMETHEUS/10.0.2.4 THOR: Warning: MODULE: Eventlog MESSAGE: Suspicious file name in eventlog entry detected ENTRY: \\??\C:\
2014-08-14 08:50:27 PROMETHEUS/10.0.2.4 THOR: Alarm: MODULE: Eventlog MESSAGE: Malware name found in eventlog entry ENTRY: \\??\C:\Testing\gse
2014-08-14 08:50:27 PROMETHEUS/10.0.2.4 THOR: Warning: MODULE: Eventlog MESSAGE: Suspicious file name in eventlog entry detected ENTRY: \\??\C:\
2014-08-14 08:50:27 PROMETHEUS/10.0.2.4 THOR: Alarm: MODULE: Eventlog MESSAGE: Malware name found in eventlog entry ENTRY: \\??\C:\Testing\gse
2014-08-14 08:50:48 PROMETHEUS/10.0.2.4 THOR: Notice: MODULE: Eventlog MESSAGE: Keyword (Startup) found in eventlog entry ENTRY: .NET Runtime Opt
2014-08-14 08:50:49 PROMETHEUS/10.0.2.4 THOR: Info: MODULE: Eventlog MESSAGE: Eventlog Microsoft-Windows-Sysmon/Operational Entry Count: 9671
2014-08-14 08:50:49 PROMETHEUS/10.0.2.4 THOR: Info: MODULE: Eventlog MESSAGE: Checking System Eventlog ...

```

## THOR Scanner Text Log Output

## THOR Report on ZEUS

### Scan Information

Thor Version	2.6.3b
Run on System	ZEUS
Argument list	D:\Dropbox\Code\gong\thor\thor.exe -t 10
Signature Database	unknown
Start Time	2013-03-10 14:55:49
End Time	2013-03-10 17:00:33
Run as user	neo
Run with admin rights	yes

### Sections

<a href="#">Local user accounts</a>
<a href="#">Profile directories</a>
<a href="#">Installed Hosts</a>
<a href="#">DNS Cache</a>
<a href="#">Eventlog System</a>
<a href="#">Eventlog Application</a>
<a href="#">Eventlog Security</a>
<a href="#">Currently logged in users</a>
<a href="#">Running Processes</a>
<a href="#">Network Connections</a>
<a href="#">Network Shares</a>
<a href="#">Network Sessions</a>
<a href="#">Open Files (Network)</a>
<a href="#">LSA Sessions</a>
<a href="#">Services</a>
<a href="#">Scheduled Tasks</a>
<a href="#">Run Key Contents</a>
<a href="#">Startup Elements (WMI)</a>
<a href="#">File Scan</a>

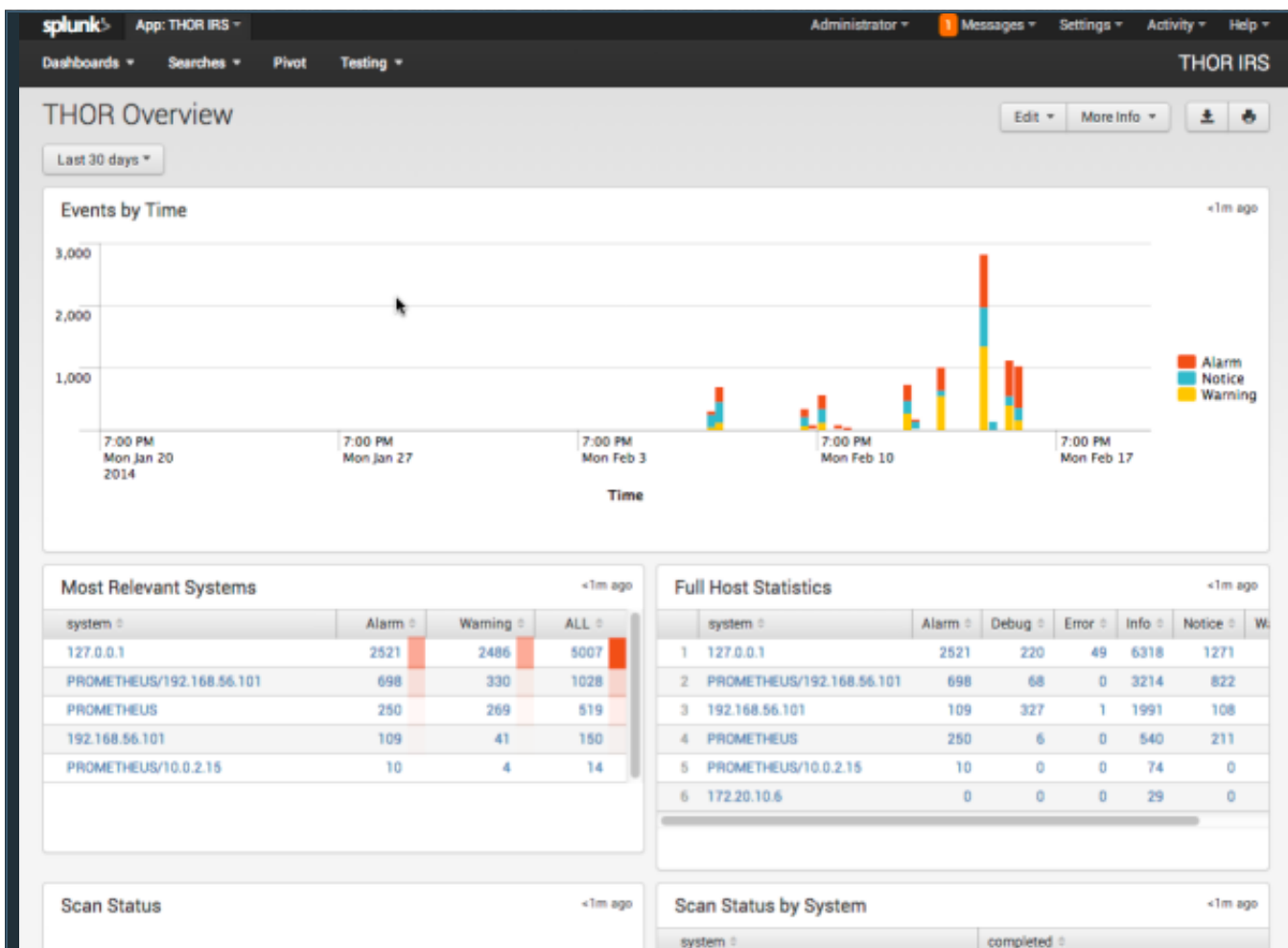
### Statistics

Alarms	27
Warnings	126
Errors	1
Notices	191
Infos	961
Debugs	33

### Alarms

Alarm 1	Malware name detected in Event ID 1073748860 occurred on 03/05/13 17:00:06 MALWARE: psexec USER: None\None ENTRY: Dienst "PsExec" befindet sich jetzt im Status "Been
Alarm 2	Malware name detected in Event ID 1073748860 occurred on 03/05/13 17:00:05 MALWARE: psexec USER: None\None ENTRY: Dienst "PsExec" befindet sich jetzt im Status "Ausg
Alarm 3	Malware name detected in Event ID 1073748869 occurred on 03/05/13 17:00:05 MALWARE: psexec USER: ZEUS\neo ENTRY: Im System wurde ein Dienst installiert. Dienstname: Dienststarttyp: Manuell starten Dienstkonto: LocalSystem
Alarm 4	Malware name detected in Event ID 1073748860 occurred on 03/04/13 20:08:02 MALWARE: psexec USER: None\None ENTRY: Dienst "PsExec" befindet sich jetzt im Status "Been
Alarm 5	Malware name detected in Event ID 1073748860 occurred on 03/04/13 20:08:02 MALWARE: psexec USER: None\None ENTRY: Dienst "PsExec" befindet sich jetzt im Status "Ausg
Alarm 6	Malware name detected in Event ID 1073748869 occurred on 03/04/13 20:08:02 MALWARE: psexec USER: ZEUS\neo ENTRY: Im System wurde ein Dienst installiert. Dienstname: Dienststarttyp: Manuell starten Dienstkonto: LocalSystem
Alarm 7	Malware name detected in Event ID 1073748860 occurred on 03/04/13 13:46:52 MALWARE: psexec USER: None\None ENTRY: Dienst "PsExec" befindet sich jetzt im Status "Been
Alarm 8	Malware name detected in Event ID 1073748860 occurred on 03/04/13 13:46:52 MALWARE: psexec USER: None\None ENTRY: Dienst "PsExec" befindet sich jetzt im Status "Ausg
Alarm 9	Malware name detected in Event ID 1073748869 occurred on 03/04/13 13:46:52 MALWARE: psexec USER: ZEUS\neo ENTRY: Im System wurde ein Dienst installiert. Dienstname: Dienststarttyp: Manuell starten Dienstkonto: LocalSystem

## THOR Scanner HTML Report



THOR Splunk App

## IOC Sharing

Indicators of Compromise (IOCs), which have been derived from forensic analyses in customer APT cases are integrated in an anonymized and encrypted form. The Enterprise License includes all these signatures creating an extraordinary benefit for all participating customers. If you decide to share some of you own IOCs with others you receive an attractive discount on the license price.

## Custom Indicators via Yara and STIX

THOR uses Yara as its main signature format. The way how THOR integrates Yara is fully compatible with normal Yara signatures although THOR extends the standard matching in order to allow certain additional checks.

You are able to extend the integrated database with you own rules matching samples that are confidential. You can add them to the signature database simply by placing these rules in the standard signature folder. The documentation gives you guidance in cases in which you want to utilize the special extensions.

The STIX support is currently based on the defined „Observables“ in form of file names, hashes, c2 server IP or domain names. THOR includes these indicators of compromise by placing the STIX files in the „stix“ subfolder.



```
rule NATEON_Backdoor {
  meta:
    author = "Florian Roth"
    description = "Detects Nateon Malware used in C5 APT SKHack"
    reference = "http://ssvah123.675.tw/e/e7/C5_APT_SKHack.pdf"
    date = "30/04/2014"
    score = 60
  strings:
    $s1 = "SMRACU" fullword
    $s2 = "\\Device\\Floppy"
    $s3 = "SQLNumResultCols"
    $s4 = "SOFTWARE\\CLASSES\\SAFEGUI"
    $s5 = "SYSPREP.EXE" fullword
    $s6 = "PIPE\\RUN_AS_CONSOLE_USER"
    $x1 = "CONFIG-DESTORY!"
    $x2 = "Software\\SafeSvc"
    $x3 = "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;SV1;"
  condition:
    5 of ($s*) or 2 of ($x*)
}

rule Thoper_Sogu_Backdoor {
  meta:
    author = "Florian Roth"
    description = "Detects Backdoor Thoper alias Sogu"
    date = "30/04/2014"
    score = 40
    type = "file"
  strings:
    $s1 = "winsta0\\default" wide fullword
    $s2 = "RUNDLL32.EXE" wide fullword
    $s3 = "RUNAS" wide fullword

    $x2 = "PlgBlt" fullword
    $x3 = "AddAce" fullword
    $x4 = "GetTickCount" fullword
    $x5 = "ADVAPI32.dll" fullword

    $z1 = "SafeSvc.exe" wide fullword
    $z2 = "A3.exe" wide fullword
    $z3 = "A3.exe" wide fullword
    /* $z3 = "SHOPT" wide fullword - too many fps */
    $z4 = "sysprep.exe" wide fullword
```

### THOR Yara APT Signatures

## MFT Analysis

THOR integrates a module for the analysis of the Master File Table of the scanned NTFS partitions. This analysis provides the detection of recently deleted hack tools via their traces in the MFT.



```

> Starting MFT analysis of drive D: ...
> MFT completely read
Info: Small MFT SIZE: 36175872 -> Deep Scan with directory resolution
> MFT completely read
Warning: Malware string in MFT record NAME: \Dropbox\BSK\Kostenabrechnung - Florian\Rechnungen 2013\BurpSuite - Order receipt.pdf DELETED: no
STRING: burpsuite CREATED: 2013-01-28 10:22:08 MODIFIED: 2013-01-28 10:22:02 ACCESSED: 2013-01-28 10:22:01
Warning: Malware string in MFT record NAME: \Dropbox\Prog\burpsuite_pro_v1.3.09.jar DELETED: no STRING: burpsuite CREATED: 2012-12-15 23:46:
18 MODIFIED: 2010-12-09 14:38:26 ACCESSED: 2012-07-07 08:17:39
Warning: Malware string in MFT record NAME: \Dropbox\Prog\ncat.exe DELETED: no STRING: \\ncat\\.exe CREATED: 2012-12-15 23:46:31 MODIFIED: 20
12-05-19 23:11:38 ACCESSED: 2012-07-05 22:06:57
Warning: Suspicious string in MFT record NAME: \Dropbox\Prog\SysinternalsSuite\psgetsid.exe DELETED: no STRING: PsGetsid\\.exe$ CREATED: 2012
-12-15 23:46:40 MODIFIED: 2012-12-15 23:46:40 ACCESSED: 2012-11-20 13:46:33
Warning: Suspicious string in MFT record NAME: \Dropbox\Prog\SysinternalsSuite\pskill.exe DELETED: no STRING: \\pskill\\.exe$ CREATED: 2012-1
2-15 23:46:40 MODIFIED: 2012-12-15 23:46:40 ACCESSED: 2012-11-20 13:46:33
Warning: Suspicious string in MFT record NAME: \Dropbox\Prog\SysinternalsSuite\psloggedon.exe DELETED: no STRING: PsLoggedon\\.exe$ CREATED:
2012-12-15 23:46:40 MODIFIED: 2012-12-15 23:46:40 ACCESSED: 2012-11-20 13:46:17
Warning: Malware string in MFT record NAME: \Dropbox\Prog\SysinternalsSuite\psloglist.exe DELETED: no STRING: \\psloglist\\.exe$ CREATED: 2012
-12-15 23:46:40 MODIFIED: 2012-12-15 23:46:40 ACCESSED: 2012-11-20 13:46:19
Warning: Suspicious string in MFT record NAME: \Dropbox\Prog\SysinternalsSuite\pspasswd.exe DELETED: no STRING: pspasswd\\.exe$ CREATED: 2012
-12-15 23:46:40 MODIFIED: 2012-12-15 23:46:40 ACCESSED: 2012-11-20 13:46:17
Warning: Suspicious string in MFT record NAME: \Dropbox\Prog\SysinternalsSuite\psservice.exe DELETED: no STRING: PsService\\.exe$ CREATED: 20
12-12-15 23:46:41 MODIFIED: 2012-12-15 23:46:41 ACCESSED: 2012-11-20 13:46:17
Warning: Suspicious string in MFT record NAME: \Dropbox\Prog\SysinternalsSuite\psdelete.exe DELETED: no STRING: \\psdelete\\.exe$ CREATED: 2012
-12-15 23:46:42 MODIFIED: 2012-12-15 23:46:42 ACCESSED: 2012-11-20 13:46:30
Warning: Malware string in MFT record NAME: \Dropbox\Prog\SysinternalsSuite\ShareEnum.exe DELETED: no STRING: ShareEnum\\.exe$ CREATED: 2012-1
2-15 23:46:42 MODIFIED: 2012-12-15 23:46:42 ACCESSED: 2012-11-20 13:46:34
Warning: Malware string in MFT record NAME: \Dropbox\Downloads\VMStray.exe DELETED: no STRING: \\VMStray.exe CREATED: 2012-12-15 23:52:26 MODIF
IED: 2012-12-03 18:20:05 ACCESSED: 2012-12-04 23:26:21
Warning: Malware string in MFT record NAME: \Dropbox\BSK\Schulung\hashdump.txt DELETED: no STRING: hashdump CREATED: 2012-12-15 23:57:10 MODI
FIED: 2011-03-01 11:38:05 ACCESSED: 2012-07-05 19:06:14
Warning: Malware string in MFT record NAME: \Dropbox\BSK\Dokumente\meterpreter_payloads.txt DELETED: no STRING: meterpreter CREATED: 2012-12-
15 23:57:54 MODIFIED: 2012-08-11 17:02:54 ACCESSED: 2012-07-05 19:22:38
Warning: Suspicious string in MFT record NAME: \Dropbox\Prog\PeaZipPortable\App\PeaZip\res\upx\upx.exe DELETED: no STRING: \\upx\\.exe$ CREAT
ED: 2013-01-31 22:59:34 MODIFIED: 2013-01-31 22:59:34 ACCESSED: 2013-02-06 09:54:02
Warning: Malware string in MFT record NAME: \Dropbox\Code\gong\mscr.exe DELETED: no STRING: \\mscr\\.exe CREATED: 2013-02-21 11:11:30 MODIFI
ED: 2012-09-28 01:20:22 ACCESSED: 2013-02-21 11:11:30
> Starting surface analysis of drive D: (Deep Dive) ... (this could take hours, skip with STRG+C)

```

## MFT Scan Malware

### „Deep Dive“ – Surface Scan

A module called „Deep Dive“ performs raw data stream analysis of objects like memory dumps, page files (if accessible e.g. on a mounted volume) and whole partitions. „Deep Dive“ reads the input stream in overlapping 3 MB chunks and applies the whole Yara signature database to these chunks. This way THOR is able to detect even deleted attacker tools in the free space of the hard drive.

```

=> STARTING CHECKS

24/24 => Scanning File System ... (1 - 4 hours)
Info: Starting surface analysis of drive C: (Deep Dive) ... (this could take hours, skip with STRG+C)
Scanning \\.\C: (default mode) type: drive
Warning: YARA Score Rule Match NAME: Backdoor_Thoper_Domains_Client8 SCORE: 65 DESCRIPTION: Detects Thoper Malware - Domain names OFFSET: 4194304 MATCHING_STRINGS: S1: .operaa.net IN: 0.cn255.0.0.0microsoft.operaa.net
PROGRESS: 24 MB Warning: YARA Score Rule Match NAME: Gh0st_Service_Generic SCORE: 70 DESCRIPTION: Gh0st service - generic signature based on C2 config string OFFSET: 31457280 MATCHING_STRINGS: S1: GetTickCount IN: ueryPerformanceCounterGetTickCountGetCurrentThreadId S2: GetProcessWindowStation IN: ThuWedTueMonSunGetProcessWindowStationGetUserObjectInformation S3: OpenWindowStationA IN: esktopOpenThreadDesktopOpenWindowStationAOpenWindowStationWPackD S4: AAAAAACEEEEEIIIIIDN00000 IN: ?Ca<?R???23???,1o>????AAAAAAACEEEEEIIIIIDN00000?OUUUUY??aaaaaaaceeeeiiii S5: MZ IN: MZ@
PROGRESS: 104 MB Alarm: YARA Score Rule Match NAME: WindowsCredentialEditor SCORE: 140 DESCRIPTION: Windows Credential Editor OFFSET: 125829120 MATCHING_STRINGS: S1: Windows Credentials Editor IN: wv{{s = "WCE %s (Windows Credentials Editor) - (c) 2010-2013 Ampla
Alarm: YARA Score Rule Match NAME: WindowsCredentialEditor SCORE: 140 DESCRIPTION: Windows Credential Editor OFFSET: 127926272 MATCHING_STRINGS: S1: Windows Credentials Editor IN: wv{{s = "WCE %s (Windows Credentials Editor) - (c) 2010-2013 Ampla
PROGRESS: 224 MB Alarm: YARA Score Rule Match NAME: WindowsCredentialEditor SCORE: 270 DESCRIPTION: Windows Credential Editor OFFSET: 236978176 MATCHING_STRINGS: S1: extract the TGT session key IN: g: I will not be able to extract the TGT session keyDone!Error: Cannot l S2: Windows Credentials Editor IN: for new list! WCE %s (Windows Credentials Editor) - (c) 2010,2011,2012 Am

```

## THOR „Deep Dive“ Hard Disk Surface Scan

Deep Dive is also capable of restoring malware files from the analysed chunks into a given directory. (e.g. network share)

↑ [-]		<DIR>	15.06.13 20:10
Hitran1_score_90_219	exe	24.064	26.06.13 15:00
Autolt_Script_score_35_21831	exe	422.400	15.06.13 20:10
Autolt_Script_score_35_21038	exe	422.400	15.06.13 20:02
PWDump_String_score_50_17436	dll	505.344	15.06.13 19:46
Amplia_Security_Tool_score_80_17368	exe	216.576	15.06.13 19:46
GSecDump_String_score_70_17328	dll	430.592	15.06.13 19:46
GSecDump_String_score_70_17326	dll	285.184	15.06.13 19:46
GSecDump_String_score_70_17138	dll	669.696	15.06.13 19:45
Honkers_score_40_15059	exe	131.712	15.06.13 19:29
PWDump_String_score_50_14994	dll	110.080	15.06.13 19:28
Honkers_score_40_14955	dll	389.632	15.06.13 19:28
Autolt_Script_score_35_14950	dll	1.894.912	15.06.13 19:28
Mimikatz_String_score_90_14938	dll	465.408	15.06.13 19:28
HackTool_Samples_score_50_14924	dll	65.536	15.06.13 19:27
HackTool_Samples_score_50_14921	dll	68.608	15.06.13 19:27
PWDump_String_score_50_14920	exe	393.216	15.06.13 19:27
HackTool_Samples_score_50_14875	dll	72.192	15.06.13 19:27
PWDump_String_score_50_14706	dll	55.296	15.06.13 19:26
PWDump_String_score_50_14684	exe	974.848	15.06.13 19:26
HangOver_Keylogger_VB_score_50_14467	dll	1.228.800	15.06.13 19:25

Malware Restored from Free Space

## Workshop und Trial

We recommend a one-day workshop to explain the different modes of operation. We demonstrate how attackers work and show how THOR is able to detect this activity, explain all the command line options and explain the most common use cases. We discuss ways in which THOR could be deployed in your environment and how to collect and analyse the log data in an appropriate way.

The workshop includes a 21-day TRIAL license, which enables you to get a quick impression on your network and identify hidden threats.

The price for the one-day workshop is 4,500.- Eur.

## Blog Content

We published numerous posts on our Blog about THOR and its new features. You can find all the THOR related posts [here](#).

## Development

THOR is a joint product of a development partnership between BSK Consulting GmbH and HvS Consulting AG and completely „Made in Germany“. The source code is retained on encrypted storage in our data center near Munich, Germany. Developers access the servers via VPN and authenticate themselves by 2-Factor-Authentication.



## Contact

Get certainty about the integrity of your systems and contact us today.

The contact form can be found [here](#).

Our [APT Scanner THOR](#) on the website of HvS Consulting.

## Kontakt

### Adresse

BSK Consulting GmbH  
Bruchstraße 8  
63128 Dietzenbach  
Deutschland  
Telefon +49 6074 - 728 42 36 [Map](#)

## Request a THOR Trial



Request a THOR Trial

## White Papers



APT Scanner THOR  
Datenblatt (DE)  
(PDF 1.3 MB)



APT Scanner THOR Slides (EN)  
(PDF 1.3 MB)



Splunk Übersicht  
(PDF 0.4 MB)



Flyer der Hackerabwehr  
Schulung  
(PDF 0,5 MB)

## THOR Updates



## Tweets

**THOR APT Scanner**

@thor\_scanner

3 Dec

Update 7.39.1 available / Sig: Patator password brute force tool (Win Exe) Sig: Phishing SPAM Wave December 2015 Bug: Directory exclude...

Expand

**THOR APT Scanner**

@thor\_scanner

30 Nov

Update 7.39.0 available / Chg: New ArcSight CEF message format - msg field now contains full log line (please ask for the new thor.cfg ...

**THOR APT Scanner**

@thor\_scanner

24 Nov

Detect preinstalled eDellRoot root level CA certificate with THOR

#Dell #SSL [pic.twitter.com/iJBpN6gGfh](http://pic.twitter.com/iJBpN6gGfh)

```
Warning: YARA Rule Match KEY: Registry Key CHI-CreateHive{04301200-0905-4000-0000-000000000000}\Software\Microsoft\SystemCertificates\Root\Certificates\98A0A4E4163357790C4A79E6D713FF0AF51FE6927 with 1 values and 0 subkeys NAME: EDellRoot_Reg
Key SCORE: 75 DESCRIPTION: Detects eDellRoot certificate in Windows registry - s
ystem's SSL connections can be intercepted REF: https://goo.gl/CAF3Cw MATCHED_ST
RINGS: Str1: \Root\Certificates\98A0A4E4163357790C4A79E6D713FF0AF51FE6927
```

Expand

**THOR APT Scanner**

@thor\_scanner

19 Nov

Schrödinger's Domain Controller - it remains both clean AND compromised until you check it with THOR

Expand

**THOR APT Scanner**

@thor\_scanner

14 Nov

An Antivirus detects Viruses.

Tweet to @thor\_scanner

## Letzte Blog Einträge

- [Synergetic Effects of Network and Host Based APT Detection](#)
- [How to Write Simple but Sound Yara Rules – Part 2](#)
- [Splunk Threat Intel IOC Integration via Lookups](#)
- [Detect System File Manipulations with SysInternals Sysmon](#)
- [APT Detection is About Metadata](#)
- [How to Write Simple but Sound Yara Rules](#)

## Kategorien

- [Alert](#) (10)
- [APT](#) (4)
- [Check Point](#) (1)
- [Command Line](#) (9)
- [LOKI](#) (1)
- [Presse](#) (1)
- [Security Fix](#) (5)
- [Security Monitoring](#) (3)
- [Splunk](#) (2)
- [THOR](#) (4)
- [Tool](#) (13)

- [Tutorial](#) (11)
- [Unsere Arbeit](#) (11)

## Themen-Wolke

[Oday](#) [analysis](#) [anomaly](#) [AppSense](#) [apt](#) [checkpoint](#) [Citrix](#) [command](#) [data](#) [detect](#)  
[detection](#) [eigene produkte](#) [erkennen](#) [firewall](#) [fix](#) [fremdprodukte](#) [Hacker](#)  
[Hardening](#) [ids](#) [intrusion detection](#) [intrusion prevention](#) [ips](#) [line](#) [linux](#) [log](#) [malware](#) [monitoring](#) [nids](#)  
[Plesk](#) [Proxy](#) [response](#) [scan](#) [Scanner](#) [Schwachstelle](#) [security](#) [security](#)  
[monitoring](#) [splunk](#) [system](#) [thor](#) [tool](#) [vdi](#) [werkzeug](#) [windows](#)  
[workaround](#) [yara](#)

## Weitere Sektionen

- [Impressum](#)
- [Verschlüsselungs-Zertifikate](#)

## SSL Protection



BSK Consulting GmbH © 2015. All Rights Reserved.