THOR Log Analysis

Nextron Systems

Feb 05, 2026

CONTENTS:

CHAPTER

ONE

INTRODUCTION

THOR log files are designed to provide as much information on a detected object as possible. However, the THOR scanner is designed to evaluate an object offline without any further data sources aside from the local signature sets. Many log messages must be evaluated by an analyst that has access to other data sources and platforms.

This document is meant for analysts with the task to analyze THOR log files. Each chapter contains guidelines to process messages of a certain module. Please see chapter *Tools for Event Analysis* for an overview of tools to evaluate the events generated by THOR. This is not an exhaustive list and some tools might be outdate/non-existent at some point. It is important to keep up to date with the latest tools.

CHAPTER

TWO

ANALYST PROFILE

The analyst profiles help you to understand which skills are recommended and required to complete a successful log analysis. The THOR scanner actually performs a live forensic analysis on the end systems and highlights elements using the internal signature database. The best possible analyst for these events is someone with experience in digital forensics, incident response or malware analysis.

The expert in digital forensics knows how to spot and qualify suspicious elements.

The incident responder understands adversary tactics, hack tools, lateral movement methods and the many different ways to achieve persistence on an end system.

And the malware analyst has the right mindset and experience to evaluate at least the elements that involve backdoors and persistence methods.

We recommend a two-tiered analysis process in which a second level analyst, with the skill set described above, processes log lines that have been pre-qualified by first level analysts.

2.1 Recommended / 2nd Level

- Forensic Analysis
- Incident Response Specialist
- Malware Analyst

2.2 Required / 1st Level

- Professional with security background
- Knowledge of Microsoft Windows internals (Administration, Development)
- Security analyst with Antivirus log analysis background

CHAPTER

THREE

GENERAL RECOMMENDATIONS

This chapter contains general approaches that apply to all findings regardless of the module that reported it. For a deeper understanding of our products (e.g. ASGARD Management Center or Analysis Cockpit), we recommend our online Training Platform. Please contact us for more information.

3.1 High Quantity Reduces Relevance

In contrast to firewall log analysis, the high number of a particular event doesn't increase, but rather decrease the relevance of that event. In a nutshell, if a suspicious file has been detected on a high number of endpoints within a given network, it is most likely a false positive. Experience showed that the most relevant findings were reported from 1-5 and sometimes up to 30 endpoints, but suspicious elements reported from 100 endpoints and higher are most likely false positives, if no strong indicators suggest the opposite.

3.2 Analysis by Module or Score

Our analysts prefer two types of approaches that are often combined to analyze big amounts of log data.

First, we recommend using our Analysis Cockpit or the free Splunk App / Add-on to sort the log data by score (descending).

This way, analysts are able to see top scoring elements that are often the most urgent ones. It is recommended to process the top scoring events top down to a score of 80 and then switch over to an analysis by module. After selecting a certain module, we recommend selecting the columns (fields) with the most characteristic features. (e.g. `FileScan` module > selected fields **FILE**, **MAIN_REASON**)

1) Sort by score and analyze events top down to a score of 80
2) Analyze events by module and process the remaining events with an appropriate set of columns

3.3 Filter Clear the View

It is crucial to provide a quick and easy way to filter events based on keywords, especially when analyzing events of hundreds or thousands of endpoints. Log analysis or SIEM systems that do not offer easy and fast ways to filter information from a view, make it substantially more difficult to process large amounts of log data.

Typically, false positives are found in great quantities. By providing tools and log management solutions that allow easy filtering, the time to complete the analysis of large amounts of log data can be reduced from days to a few hours.

3.4 Attribute Evaluation

Many evaluation steps that can be automated have already been implemented in the scanners. This document aims at giving an analyst the best possible support to complete the remaining evaluations.

There is no easy step by step guide to analyze the logs of our forensic scanners. The tables named "Attribute Evaluation", which are part of the following chapters, just support this evaluation process. They do not represent all necessary steps to complete an analysis.

CHAPTER

FOUR

FILESCAN

Events reported by the `FileScan` module typically originate from the file system scan. But due to the "Message Enrichment" feature, other modules that include events with full "file path" strings may also produce events of this type (e.g. module `SHIMCache`, `Eventlog`).

Filescan events are rich in attributes and extra information.

4.1 Sample

```
Dec 2 19:29:43 PROMETHEUS/10.0.2.4
THOR: Notice: MODULE: Filescan
MESSAGE: Suspicious file found
FILE: C:\Program Files (x86)\HaoZip\HaoZipExt64.dll
SCORE: 54
MD5: 60873d6560b29bdb30235e05eda97539
SHA1: d312157d7c890a68eed85c5a2fd17fdfe6defa87
OWNER: BUILTIN\Administrators
SIZE: 513800
TYPE: EXE
FIRSTBYTES: 4d5a900003000000040000000ffff0000b8000000 / MZ
COMPANY: ACME
DESC: 2345-Windows
CREATED: Thu Jul 26 05:20:04 2012
MODIFIED: Thu Jul 26 05:20:04 2012
ACCESSED: Fri Sep 20 12:47:39 2013
REASON_1: Haozip_SFX / Haozip SFX Compressed Executable
  Score: +50
  Trigger: Specific Rule Value:
    Str1: release\pdb\HaoZip
```

4.2 Typical False Positives

- Legitimate files matching a filename regular expression IOC
- YARA rules matching THOR reports or clear-text signatures from former scans have been left on the system
- Dual use tools used by administration (e.g. `nmap.exe`, `ncat.exe`)
- Legitimate tools moved to the Recycle Bin and therefore detected with wrong name (e.g. `Psexec` as `$IR4HB6A.exe`)
- Legitimate but very old files that trigger the file size anomaly

- Old and rare versions of legitimate programs that trigger the file signature anomalies (that often happens with `javaw.exe` / `java.exe`)

4.3 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
FILE	See chapter *File Path Checks*			
MD5/SHA1/SHA256	See chapter *Hash Checks* for generic checks on hashes			
SIZE	Is the file size 0 bytes? (Probably reset by AV due to a detected infection)	Yes	Good	High
FIRSTBYTES	Do the fist bytes contain words in native language - e.g. `@ECHO OFFECHO "Übertragung`	Yes	Good	High
FIRSTBYTES	Do the first 20 bytes already contain executables or command line tools - e.g. `@echo off net user /domain >`	Yes	Bad	Medium
OWNER	Is the owner of the file a typical user account - e.g. `DOM\user123`	Yes	Good	Low
OWNER	Is the owner of the file `BULTIN\Administrators`	Yes		
OWNER	Does the owner string of the file contain `IIS` or another service name - e.g. `IIS_USRS`, `tomcat`, `apache`	Yes	Bad	Medium
TYPE	Does the type match the extension?	No	Bad	Low
TYPE	Is the type EXE and the extension a benign looking one - e.g. `.txt` or `.pdf`	Yes	Bad	Medium
COMPANY	Does the company string from the PE header match the expected values - e.g. `cmd.exe` contains `Microsoft`	No	Bad	Medium
DESC	Does the description string from the PE header match the expected values - e.g. `sapgui.exe` contains `SAP GUI for Windows`	No	Bad	Low
CREATED/MODIFIED	Has the file been created very far in the past - e.g. time stamp shows 2021 and older	Yes	Good	Low
CREATED/MODIFIED	Has the file been modified on a Sunday (does not apply to regions were admins work on a Sunday for example)	Yes	Bad	Medium

4.4 Typical REASONs

Attribute	Question	Answer	Indication	Weight
REASON_1	Is the only REASON a file name pattern match (prone to false positives)	Yes	Good	Low
REASON_2	Is the file located in a personal user folder and does it look like that the user changed the extensiopn to avoid certain filter mechanisms - e.g. `Chrome-Portable.exe.txt`)	Yes	Good	Medium
...	Does the Reason field report a file anomaly and the file is located in a backup folder from a very old version of Windows (or maybe a outdated version of the original program) - e.g. `F:\WinNT35\...` or `C:\Program Files\NextGen Software\bin\javaw.exe`	Yes	Good	Medium
	Does the REASON report a suspicious, unsigned javaw.exe and is that file located in a folder of a software product (Rule: Javaws_Not_Verisign) - e.g. `C:\Program Files\IBM Backup Manager\bin\javaw.exe`	Yes	Good	Medium
	Rule starts with `VUL_` reporting a vulnerability	Yes	Good	Medium
	Does the rule match on a hack tool, which is installed in a typical location on disk or in a backup location - e.g. `ncat` in `/usr/bin/ncat` or `/backups/sys1/20171113/bin/ncat`	Yes	Good	Medium

CHAPTER

FIVE

SHIMCACHE

The `SHIM Cache` or **AppCompatCache** (Application Compatibility Cache) is a special Registry cache containing valuable information, because the cache tracks metadata for binary files that were executed.

It includes the full path to the executable file image and a timestamp, which could be the date of the last execution or the creation time stamp of the file, depending on the Windows version.

In cases where the executed file is still present on disk, THOR calculates hashes and includes them in the log message (message enrichment). If you can't find a hash in the log line, this means that THOR wasn't able to find the file on disk anymore.

5.1 References

- Count Upon Security

5.2 Samples

```
Aug 26 13:10:21 SRV2345/10.2.0.22
THOR: Warning: MODULE: SHIMCache
MESSAGE: Suspicious file name in Shim Cache Entry detected
ELEMENT: SYSVOL\Temp\1.exe
PATTERN: \ [01]\.exe AND \[A-Za-z0-9]\.(exe|com|dll|bat|scr|vbs)$ AND \[Tt]emp\[0-9a-zA-
↪Z]\.(exe|dll)
SCORE: 60
DESC: Typical attacker scheme
FILE: SYSVOL\Temp\1.exe
DATE: 02/21/17 15:44:32
TYPE: system
HIVEFILE: None
EXTRAS: N/A N/A True
MD5: -
SHA1: -
SHA256: -
```

```
Aug 26 12:02:59 SRV1123.internal.net/10.0.0.112
THOR: Warning: MODULE: SHIMCache
MESSAGE: Suspicious file name in Shim Cache Entry detected
ELEMENT: D:\Temp\test\ client.exe
PATTERN: \client.exe
SCORE: 60
```

(continues on next page)

(continued from previous page)

```
DESC: Typical Malware Names
FILE: D:\Temp\test\ client.exe
DATE: 01/23/17 08:03:37
TYPE: system
HIVEFILE: None
EXTRAS: N/A N/A False
MD5: 099120aca1c34e7a529b3b390cfdbc1e
SHA1: 4ece72b9fa13019a4ce8b4229ca7b6aee09d6982
SHA256: c3c336a23021b68b026bdf1642b220d88037039aa6d7f8e7d4d576cc38063088
```

5.3 Typical False Positives

- Legitimate software that uses strange executable locations
- THOR's own scans if administrators chose a suspicious working directory (e.g. `C:\Temp\`, `C:\thor\`)

5.4 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
ELEMENT	See chapter *File Path Checks*			
MD5/SHA1/SHA256	Is the hash field empty (this means: File was not found during the scan)	Yes		
MD5/SHA1/SHA256	See chapter *Hash Checks* for generic checks on hashes			

CHAPTER

SIX

AUTORUNS

The `Autoruns` module makes use of the command line version of SysInternals Autoruns. It parses the tools output and integrates the output in each log message.

6.1 References

- Microsoft Sysinternals

6.2 Issues

The hash generation for the SHA1 hash in Autorunsc.exe is not reliable. The reason for this is unknown. The issue has been reported but hasn't been fixed so far. The value is therefore suppressed.

6.3 Samples

```
Aug 26 18:48:28 system.internal.net/10.1.2.50
THOR: Warning: MODULE: Autoruns
MESSAGE: New or changed autoruns element
LOCATION: HKLM\System\CurrentControlSet\Services
ENTRY: SymELAM
ENABLED: enabled
CATEGORY: Drivers
PROFILE: System-wide
DESC: Symantec
ELAM PUBLISHER: Symantec Corporation
IMAGE_PATH: c:\windows\system32\drivers\sep\0c011b95\19c8.105\x64\symelam.sys
LAUNCH_STRING: system32\Drivers\SEP\0C011B95\19C8.105\x64\SymELAM.sys
MD5: 20f758e6339a16f97dd83389d582e09a
SHA1: -
SHA256: 837016154b7952b645b5545aeb8e2a8878efa8674e6b96471c3db5e458b06960
SCORE: 60
```

```
Aug 26 13:00:55 system.internal.net/10.1.2.50
THOR: Warning: MODULE: Autoruns
MESSAGE: Autoruns element located in a suspicious location
MATCH_STRING: \temp\
LOCATION: HKLM\System\CurrentControlSet\Services
ENTRY: inject3526
ENABLED: enabled
```

(continues on next page)

(continued from previous page)

```
CATEGORY: Services
PROFILE: System-wide
DESC: -
PUBLISHER: -
IMAGE_PATH: c:\users\markschmitt\appdata\local\temp\inject23.exe
LAUNCH_STRING: C:\Users\markschmitt\AppData\Local\Temp\inject23.exe
MD5: 7f9a4835a7a237d2873901bb73d00e7b
SHA1: -
SHA256: d21d4ad73b848488890bf7f846daff7455062801d0d86238d99591219878f36a
SCORE: 75
```

6.4 Typical False Positives

- New entries that are legitimate
- Legitimate software that uses strange autorun locations

6.5 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
MESSAGE	Does it contain "New or changed autoruns element" (Note: This is just a change notice and can be relevant on critical systems or under certain circumstances)	Yes	Good	Low
IMAGE_PATH	See chapter *File Path Checks*			
PUBLISHER	Is the field empty	Yes	Bad	Low
DESC	Is the field empty	Yes	Bad	Low
MD5/SHA1/SHA256	Is the hash field empty (this means: File was not found during the scan)	Yes		
MD5/SHA1/SHA256	See chapter *Hash Checks* for generic checks on hashes			

CHAPTER

SEVEN

LOGSCAN

The `LogScan` module processes `*.log` files found on disk line by line (It performs some checks to avoid scanning files that are not ASCII log files, but something else that uses the `*.log` extension). Each log line is checked with all file name and keyword IOCs and scanned with the "keyword" and "log" type YARA rules.

7.1 Samples

```
Aug 26 18:58:32 System23.local.net/10.2.2.14
THOR: Warning: MODULE: LogScan
MESSAGE: Suspicious file name in Log Entry detected
ELEMENT: Deleted file - E:\TEAM-TRANSFER\4Helmut\Tools\PortScan.exe
PATTERN: \PortScan.exe
SCORE: 65
DESC: PortScanner Names
FILE: D:\ scripts\log\TEAM-TRANSFER.CLEANUP.cmd.2015-09-27.log
LINE: 320
```

```
Aug 27 10:40:30 System23.local.net/10.2.2.14
THOR: Warning: MODULE: LogScan
MESSAGE: Suspicious file name in Log Entry detected
ELEMENT: /EN/cmd.exe /c+dir "C:\data\inetpub\wwwroot\EN\cmd.exe" 404 "SW0123" - -
↪2147024864 - - 0 10.10.9.24 443 - "gi.webshop.com" - 09:48:18.024 "HTTP/1.1" "https"␣
↪1405 102
PATTERN: ([C-Zc-z]:|\\).{1,40}\
```

7.2 Typical False Positives

- Web vulnerability scans trying to access files that do not exist (HTTP Error 404)
- RoboCopy logs that list hack tools like `nmap.exe` or `ncat.exe`

7.3 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
FILE	Does the path include a timestamp that indicates very old data? (e.g. `C:\wwwroot\logs\2003-04-17-access.log`)	Yes	Good	Medium
ELEMENT	Does an investigation for the remote IP address return negative or suspicious results?	Yes	Bad	High
ELEMENT	Does the web server access log line include a response code 404? (404: file not found, see the example above)	Yes	Good	Medium
ELEMENT	Does the element show an Antivirus alert? Antivirus alerts often go unnoticed / it is recommended to include them in the reports	Yes	Bad	Medium
ELEMENT	See chapter *File Path Checks*			

CHAPTER

EIGHT

GROUPSXML

The `GroupsXML` module is a module that reports on critical security issues related to decryptable passwords in group policy files, that are readable for anyone within a Windows Domain.

8.1 References

- Active Directory Security
- SentinelOne

8.2 Samples

```
Aug 28 11:07:24 System32.local.net/10.2.0.7
THOR: Warning: MODULE: GroupsXML
MESSAGE: Found decryptable password in Groups.xml
FILE: D:\SYSVOL_DFSR\sysvol\win55.local.net\Policies\{FFABF4BC-8A98-4B3F-AD7D-
↪D65A5F4C26C1}\Machine\Preferences\Groups\Groups.xml
USER: Administrator (built-in)
PASSWORD: win***removed***
SCORE: 75
```

8.3 Typical False Positives

- Old `groups.xml` files in backup locations that are not active anymore

8.4 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
PASSWORD	Does the password start with 3 digits that could indicate password that is easy to guess? (e.g. `pas*******`, `win******`, `Def*****`)	Yes	Bad	Medium
USER	Is the user name a default user account that attackers could easily use without attracting attention? (e.g. Administrator, Admin)	Yes	Bad	Medium

CHAPTER

NINE

REGISTRY

`Registry` matches can be caused by different signature types: File name IOCs, keywords or YARA signatures matches.

9.1 Samples

```
Aug 29 08:13:37 system123.local.net/10.6.2.10
THOR: Warning: MODULE: Registry
MESSAGE: YARA Rule Match
KEY: Registry Key CMI-CreateHive{D43B12C1-09B5-40DB-AFF6-F6DFEB78DAEC}\Software\
↪Microsoft\Windows\CurrentVersion\Run with 1 values and 0 subkeys
NAME: Suspicious_Startup_Loc_RegistryKey
SCORE: 70
DESCRIPTION: Detects suspicious registry values often used by malware
REF: -
MATCHED_STRINGS:
        Str1: CurrentVersion\Run;Google Update;"C:\Users\MSchmitz\AppData\Local\Google\
↪Update\GoogleUpdate.exe
```

```
Aug 28 08:17:46 system123.local.net/10.10.1.8
THOR: Warning: MODULE: Registry
MESSAGE: YARA Rule Match
KEY: Registry Key CMI-CreateHive{6A1C4018-97AB-4291-A7DC-7AED1C76667C}\Keyboard Layout\
↪Preload with 3 values and 0 subkeys
NAME: Chinese_Keyboard_Layout_RDP_Preload
SCORE: 70
DESCRIPTION: Chinese Keyboard Layout settings detected - this hive's user used the␣
↪chinese keyboard layout
REF: http://www.welivesecurity.com/2014/05/20/miniduke-still-duking/
MATCHED_STRINGS:
        Str1: Keyboard Layout\Preload;2;00000804
```

9.2 Typical False Positives

- Values with system files in rare locations (e.g. backup locations: `\\backupserv\sysbackup20171119\Windows\system32`)
- Keyboard layout preloads that are typical for the region of the system (e.g. "Chinese keyboard layout" on a system in Shanghai)
- Values that start with `4d5a` by pure chance

9.3 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
MATCHED_STRIN	Do the strings match on a suspicious program location and is that location legitimate?	Yes	Good	Medium
MATCHED_STRIN		No	Bad	Medium
NAME	Does the rule name include the string `RDP_Preload` and the respective keyboard layout is completely implausible on that end system? (e.g. Chinese keyboard layout on system in Italy with Italian admins only)	Yes	Bad	Medium
NAME	Does the rule name include the string `RDP_Preload` and the respective keyboard layout is plausible on that end system? (e.g. Chinese keyboard layout on system in Shanghai)	Yes	Good	Medium

CHAPTER

TEN

WMIPERSISTENCE

It is difficult to detect malicious `WMIPersistence` objects. The detection methods are based on whitelists and a blacklist with keywords from APT reports. The whitelists are extended every time our analysts detect false positives in a customer's environment. The black lists are extended every time an APT report states a certain WMI persistence method with specific event filer or event file name.

10.1 References

- Github

10.2 Samples

```
Aug 26 23:16:41 server44.local.net/10.23.3.1
THOR: Warning: MODULE: WMIPersistence
MESSAGE: Suspicious WMI element
KEY: Binding 91
FILTERTYPE: HealthDriverEventConsumer
EVENTFILTERNAME: HP_TempSensorFailureEvent
EVENTCONSUMER: Health Event Consumer
EVENTFILTER: select * from HP_TempSensorFailureEvent
EVENTCONSUMER: -
SCORE: 75
```

```
Aug 26 23:16:41 server44.local.net/1.253.103.134
THOR: Warning: MODULE: WMIPersistence
MESSAGE: Suspicious WMI element
KEY: Binding 93
FILTERTYPE: HealthDriverEventConsumer
EVENTFILTERNAME: HP_ASRStateChangeEvent
EVENTCONSUMER: Health Event Consumer
EVENTFILTER: select * from HP_ASRStateChangeEvent
EVENTCONSUMER: -
SCORE: 75
```

10.3 Typical False Positives

- Legitimate entries caused by system management software (e.g. HP services)

10.4 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
EVENTFILTER	Does the Eventfilter content related to the EventFilterName? (e.g. `HP_TempSensorFailureEvent` and `select * from HP_TempSensorFailureEvent`)	Yes	Good	Medium
		No	Bad	Medium
EVENTFILTER-NAME	Does a google search on the EventFilerName show no result at all?	Yes	Bad	Medium
EVENTFILTER-NAME	Does a google search on the EventFilterName result in results that seem legitimate?	Yes	Good	Medium

CHAPTER

ELEVEN

VULNERABILITYCHECK

The `VulnerabilityCheck` module is limited to a few vulnerabilities that are known to be exploited by various threat groups. The vulnerability checks focus on vulnerabilities that are used for lateral movement or weaknesses which allow an attacker to easily achieve persistence without using any kind of software as backdoor. Note: There are vulnerabilities covered by YARA rules and reported in other modules. The YARA rules that detect vulnerabilities start with `VUL_`.

11.1 Samples

```
Aug 29 10:06:58 server44.local.net/10.23.3.1
THOR: Warning: MODULE: VulnerabilityCheck
MESSAGE: Tomcat credential weakness
REASON: Password equals the user name
USER: tomcat
FILE: F:\\apache\\tomcat\\conf\\tomcat-users.xml
SCORE: 75
```

11.2 Typical False Positives

- Weaknesses in inactive `tomcat-users.xml` files, e.g. in backup locations or tomcats that are only accessible on localhost

11.3 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
REASON	Password equals the user name	Yes	Bad	Medium
REASON	Password is a default password	Yes	Bad	Medium
FILE	Tomcat Vulnerability: Does the folder look like a backup location or an inactive location, not used by a running tomcat process? (e.g. `H:\Backup\test_23\conf\tomcat-users.xml`) Background: The vulnerability is only relevant if used by an active tomcat process. Local development installations or backups of a default config are not relevant.	Yes	Good	High
MESSAGE	Does the message state `Domain Controller is running since before 11/17/2014`	Yes	Bad	High

CHAPTER

TWELVE

LOGGEDIN

The `LoggedIn` module analyses all currently logged in users and analyses their names.

12.1 Samples

```
Aug 26 12:28:07 server44.local.net/10.7.1.100
THOR: Warning: MODULE: LoggedIn
MESSAGE: Suspicious logged in user name
KEYWORD: ^[0-9a-z]{1,3}$
USER: abc
SCORE: 75
```

12.2 Typical False Positives

- Legitimate user account with three or less characters

12.3 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
USER	Does the user name look suspicious to a human eye? (e.g. `abc`, `123`, `adm123`, `suser`, `bckdr`, `master`, `access`)	Yes	Good	Medium
		No	Bad	Medium

CHAPTER

THIRTEEN

PROCESSCHECK

Different checks are performed in the `ProcessCheck` module. Some of them check the process characteristics such as parent/child relations, process priorities and executable file locations for anomalies. Other checks evaluate the processes network connections and YARA checks match on the process memory.

13.1 References

- nasbench.medium.com

13.2 Samples

```
Aug 26 13:02:27 server22.local.net/10.6.19.8
THOR: Warning: MODULE: ProcessCheck
MESSAGE: Process started from a typical attacker / malware location
PID: 8336
PPID: 5796
PARENT: C:\temp\ProcessMonitor\Procmon.exe
NAME: Procmon64.exe
OWNER: server-ABC123
COMMAND: "C:\Users\SERVER~4\AppData\Local\Temp\2\Procmon64.exe" /originalpath "C:\temp\
↪ProcessMonitor\Procmon.exe"
PATH: C:\Users\SERVER~4\AppData\Local\Temp\2\Procmon64.exe
CREATED: 24.08.2017
```

```
Aug 26 13:02:55 server.local.net/10.1.19.2
THOR: Warning: MODULE: ProcessCheck
MESSAGE: Yara rule match on process
PID: 32980
PPID: 4104
PARENT: C:\Program Files\Internet Explorer\iexplore.exe
NAME: iexplore.exe
OWNER: SYSTEM
COMMAND: "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE"
PATH: C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE
CREATED: 24.08.2017 05:00:02
MD5: e3da77b534d7dff8a2ae6a577a44703b
CONNECTION_COUNT: 0
LISTEN_PORTS: -
RULE: CN_C2_Domain_HvS_Client_A3
```

(continues on next page)

(continued from previous page)

```
DESCRIPTION: THOR HvS Client A3 - C2 domain in file
REFERENCE: -
SCORE: 75
STRINGS:
        Str1: .lookipv6.com
```

13.3 Typical False Positives

- Legitimate software started from strange locations
- Old Windows versions (XP, 2003) show abnormal parent/child relation and process priority warnings
- Process end points in suspicious GEO IP regions of the world (e.g. system in China with process connections to other systems in China)
- Process memory scan alerts in processes that may contain clear-text signatures (AV process memory, VMWare tools (copied THOR to the system), GRR, SearchIndexer)

13.4 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
COMMAND	Is the executable a well-known SysInternals tool?	Yes	Good	Medium
PATH	See chapter *File Path Checks*			
PARENT	Is the parent of the suspicious process a Microsoft Office program?	Yes	Bad	High
OWNER	If the owner of the suspicious process starts with `IWAM_`, `IUSR_` or `IIS_`?	Yes	Bad	Medium
MESSAGE	Did the YARA rule match on `IEXPLORE.EXE`, `VMWARE tools process memory`? (Note: the Internet Explorer and VMWare tools process memory is prone to false positives)	Yes	Good	Low
MESSAGE	Did the YARA rule match on Antivirus or Security tool process memory? (e.g. CarbonBlack, GRR)	Yes	Good	High

CHAPTER

FOURTEEN

HOTFIXCHECK

The `HotFixCheck` module analyses the installed hotfixes on the end system.

14.1 Samples

```
Sep 4 16:33:27 server11.local/192.168.2.2
THOR: Warning: MODULE: HotfixCheck
MESSAGE: Outdated System - No hotfixes installed for the last 90 days. Last hotfix
DATE: 2015/01/09
SCORE: 75
```

14.2 Typical False Positives

- THOR failed to evaluate the modules on the system and didn't return a single hotfix. In these cases, THOR reports *No Hotfixes installed or no hotfix information available*.

CHAPTER

FIFTEEN

RUNKEYCHECK

The RunKeyCheck module processes entries in the RUN Key.

15.1 Samples

```
Aug 6 11:22:11 server11.local/10.252.8.237
THOR: Warning: MODULE: RunKeyCheck
MESSAGE: Suspicious file name in value detected
ELEMENT: "C:\Program Files\Microsoft Security Client\msseces.exe" -hide -runkey
PATTERN: (?i)\msseces\.exe
SCORE: 60
DESC: Executable used by PlugX DLL side-loading in non-standard location Run Key Entry
NAME: MSC
VALUE: "C:\Program Files\Microsoft Security Client\msseces.exe" -hide -runkey
FILE: C:\Program Files\Microsoft Security Client\msseces.exe
FIRSTBYTES: 4d5a90000300000004000000ffff0000b8000000 / MZ
SHA1: 71fac169a5f04af634d06c367e7d832e72c1cdf2
```

15.2 Typical False Positives

- Elements matching known system files in suspicious locations (see example with `msseces.exe`)

15.3 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
VALUE	Does the value attribute point to a suspicious location such as `C:\Users\Public\` or `%temp%`? name look suspicious to a human eye?	Yes	Bad	Medium
SHA1	Does the SHA1 value gets flagged by AV scanner on website such as VirusTotal?	Yes	Bad	Medium

CHAPTER

SIXTEEN

AMCACHE

The `AmCache` module processes entries in the AmCache of the system. In contrast to the SHIMCache entries, AmCache entries contain a SHA1 hash value that can be used to determine the exact program that was executed on the end system.

16.1 References

- www.swiftforensics.com
- windowsir.blogspot.de

16.2 Samples

```
Aug 26 16:14:22 server33.local/10.1.2.31
THOR: Warning: MODULE: Amcache
MESSAGE: Suspicious file name in Amcache entry detected
ELEMENT: C:\temp\1.exe
PATTERN: \(tmp|temp)\[a-zA-Z0-1]\.(exe|com) AND \[01]\.exe AND \[A-Za-z0-9]\.
↪(exe|com|dll|bat|scr|vbs)$ AND (temp|tmp)\[0-9]{1,50}\.exe$ AND \[Tt]emp\[0-9a-zA-Z]\.
↪(exe|dll) SCORE: 60 DESC: Typical attacker scheme
FILE: C:\temp\1.exe
SHA1: 9cf9c57b0927c45d6712387871dd435053d912b6
SIZE: None
DESC: None
FIRST_RUN: 2017-05-22 15:41:00.021779
CREATED: 0001-01-01
```

```
Aug 19 13:08:49 server4448.local.net/10.0.10.1
THOR: Warning: MODULE: Amcache
MESSAGE: Suspicious file name in Amcache entry detected
ELEMENT: C:\Users\blueprism\FPipe.exe
PATTERN: FPipe.exe AND \(Users|Documents and Settings)\[^\]{1,20}\[^\]{1,20}\.
↪(exe|dll|vbs|bat|ps1)
SCORE: 75
DESC: Pattern in Amcache entry
FILE: C:\Users\Public\FPipe.exe
SHA1: 41d57d356098ff55fe0e1f0bcaa9317df5a2a45c
SIZE: 13312
DESC: FPipe
FIRST_RUN: 2017-07-12 14:13:32.823776
CREATED: 2017-07-12 14:13:26.886278
```

(continues on next page)

(continued from previous page)

```
PRODUCT: FPipe
COMPANY: Foundstone
```

16.3 Typical False Positives

- Legitimate files in suspicious locations
- Elements matching known system files in suspicious locations

16.4 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
ELEMENT	See chapter *File Path Checks*			
MD5/SHA1/SHA256	See chapter *Hash Checks* for generic checks on hashes			
FIRST_RUN	Did the file run the first time on a Sunday?	Yes	Bad	Medium
FIRST_RUN	Did the file run the first time at night between 00:00 and 06:00 am in the early morning?	Yes	Bad	Medium

CHAPTER

SEVENTEEN

FIREWALL

The `Firewall` module evaluates all local Windows firewall rules and tries to detect suspicious entries by using white- and blacklists.

17.1 Samples

```
Aug 26 17:51:25 server23.local.net/10.19.2.17
THOR: Warning: MODULE: Firewall
MESSAGE: Zeus Local Port defined in Firewall rule
SIGNATURE: ZEUS
RULE_NAME: Appsense_Input
PORT: 7771
SCORE: 75
```

```
Jul 29 11:19:48 serverx-print/10.255.80.56
THOR: Warning: MODULE: Firewall
MESSAGE: Suspicious Trojan/Backdoor Local Port defined in Firewal rule
SIGNATURE: Strange Value
RULE_NAME: XXXCloudProxy.exe
PORT: 8080
SCORE: 75
```

17.2 Typical False Positives

- Legitimate rules for non-white-listed programs
- Legitimate rules on suspicious ports (e.g. `WinSSHd` on port `60022/tcp`, `Apache` on port `4443/tcp`)

17.3 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
RULE_NAME	Does the name look suspicious?	Yes	Bad	Low
PORT	Does the port relate to the rule name? (e.g. `Port 8080` to `Apache`, `Port 2222` to `Bitvise SSH Daemon`)	Yes	Good	Medium

CHAPTER

EIGHTEEN

SERVICECHECK

The ServiceCheck module evaluates all registered local Windows services. It detects suspicious service entries by different anomaly checks, blacklisted keywords and reports file path anomalies.

18.1 Samples

```
Aug 1 15:14:26 server88.localnet/192.168.2.4
THOR: Warning: MODULE: ServiceCheck
MESSAGE: Service started from typical attacker location
KEY: srvany
SERVICE_NAME: srvany
IMAGE_PATH: c:\srvany.exe
SHA1: 7c5329229042535fe56e74f1f246c6da8cea3be8
START_TYPE: unknown
USER: LocalSystem
SCORE: 75
```

```
Jul 1 11:52:41 server77.local.net/10.10.9.19
THOR: Warning: MODULE: ServiceCheck
MESSAGE: Service started from suspected attacker location
KEY: cpuz139
SERVICE_NAME: cpuz139
IMAGE_PATH: \??\C:\Users\u23491\AppData\Local\Temp\cpuz139\cpuz139_x64.sys
SHA1: 13df48ab4cd412651b2604829ce9b61d39a791bb
START_TYPE: ONDEMAND_START
USER:
SCORE: 75
```

```
Nov 20 11:44:52 PROMETHEUS/10.0.2.4
THOR: Warning: MODULE: ServiceCheck
MESSAGE: YARA Rule Match in service
STRING: loadersvc - {993B4A05-7C9E-4DA7-9052-4192A3B96F21} - C:\Testing\uixvd.exe
NAME: Malicious_Keylogger_Service_Driver
SCORE: 65
DESCRIPTION: Detects malicious keylogger service driver - loadersvc
REF: -
MATCHED_STRINGS:
        Str1: loadersvc
KEY: loadersvc
SERVICE_NAME: {993B4A05-7C9E-4DA7-9052-4192A3B96F21}
```

(continues on next page)

(continued from previous page)

```
IMAGE_PATH: C:\Testing\uixvd.exe
MODIFIED: 2017-03-17T10:53:51.143664
SHA1: -
START_TYPE: ONDEMAND_START
USER: LocalSystem
```

18.2 Typical False Positives

- Legitimate software with service binaries located in suspicious folders (e.g. the user's `%AppData%` folder)
- Services with matching regular expression file name IOCs
- Services registered by administrators in suspicious locations (e.g. `C:\srvany.exe`)

18.3 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
ELEMENT	See chapter *File Path Checks*			
MD5/SHA1/SHA256	See chapter *Hash Checks* for generic checks on hashes			
SERVICE_NAME	Is the service name a random ID? (e.g. `98ncjs87e`, `{993B4A05-7C9E-4DA7-9052-4192A3B96F21}`)	Yes	Bad	Medium
START_TYPE	Is the start-type `ONDEMAND*`?	Yes	Good	Low
MODIFIED	Has the service been modified in a suspicious time frame? (Sunday night between 00:00 am and 06:00 am)	Yes	Bad	Medium
MESSAGE	Does a YARA rule match on the service entry?	Yes	Bad	Medium

CHAPTER

NINETEEN

DNSCACHE

The `DNSCache` module evaluates the entries of the local DNS cache. It compares the entries with known C2 servers and reports suspicious entries based on some regular expression checks.

19.1 Samples

```
Aug 19 11:27:08 system444.local.net/172.27.2.7
THOR: Alert: MODULE: DNSCache
MESSAGE: Malware Domain found in DNS Cache
ENTRY: 60.10.1.183.in-addr.arpa
IP: 10.252.8.5
SIGNATURE: 60.10.1.
DESC: Graphedt Group
SCORE: 100
```

```
Jul 8 11:30:56 system88.local.net/10.10.9.15
THOR: Warning: MODULE: DNSCache
MESSAGE: Entry with dangerous TLD found
TLD: biz
ENTRY: altftp.compsys.biz
IP: 10.11.11.40
SCORE: 75
```

19.2 Typical False Positives

- Legitimate company domains registered with a black-listed Top Level Domain (TLD) (e.g. `vpnaccess.companybranch.info`)
- False positives caused by `in-add.arpa` reversed strings that match on black-listed IP addresses
- Too short domain names from 3rd party IOC sources (e.g. `ipv6.com` matching on `benign-site-ipv6.com`)

19.3 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
IP	Is the IP known for malicious activity? (Check the platforms listed in chapter 33 Tools for Event Analysis)	Yes	Bad	Medium
		No	Good	Medium
ENTRY	Is the FQDN known for malicious activity?	Yes	Bad	Medium
		No	Good	Medium
TLD	Seems the FQDN to be legitimate although it is registered under a suspicious TLD? (e.g. `servftp.companyname.biz`, `www2.companybranch.cn`)	No	Bad	Medium
		Yes	Good	High

CHAPTER

TWENTY

HOSTS

The `Hosts` module evaluates the entries in the local hosts file.

20.1 References

- blog.malwarebytes.com

20.2 Samples

```
Aug 26 11:46:14 server555.local.net/10.7.1.14
THOR: Warning: MODULE: Hosts
MESSAGE: New hosts entry - not found during the last run
ENTRY: master.comp-a.net
IP: 10.7.10.2
SCORE: 75
```

```
Jul 29 12:16:18 server99.local.net/10.1.1.55
THOR: Warning: MODULE: Hosts
MESSAGE: Suspicious entry found in Hosts file
ENTRY: ctldl.windowsupdate.com
IP: 127.0.0.1
SCORE: 75
```

20.3 Typical False Positives

- Entries on development systems to simulate future DNS resolution (e.g. `www.company-intranet.net 10.0.2.28`)
- Some Antivirus tools insert entries into the hosts file to immunize the system (e.g. `Spybot Search & Destroy`)

20.4 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
MESSAGE	Does a new host file entry look legitimate?	Yes	Good	Medium
ENTRY	Does the FQDN related to a server of a security software like an update server of an Antivirus server? (e.g. `update1.f-secure.com`)	Yes	Bad	Medium
IP	Is the IP address not in a local network? (`10.0.0.0/8`, `192.168.0.0/16`, `172.16.0.0/12`)	No	Bad	Medium

CHAPTER

TWENTYONE

WMISTARTUP

The `WMIStartup` module uses different WMI queries to retrieve information on elements that could be used for persistence. It is very likely that findings by this module also appear in other modules (e.g. `Autoruns`) in a different form, because it just uses a different method to look at the same elements.

21.1 Samples

```
Aug 23 02:03:12 server55.local.net/10.16.1.44
THOR: Warning: MODULE: WMIStartup
MESSAGE: Suspicious startup program WMI Run Key Evaluation
LOCATION: "C:\Users\user1\AppData\Local\Temp\1\RarSFX1\OlympUpgrade.exe"
SCORE: 75
```

```
May 20 11:14:52 wks10021/10.1.7.60
THOR: Warning: MODULE: WMIStartup
MESSAGE: Suspicious startup program WMI Run Key Evaluation
LOCATION: "C:\Users\user1\AppData\Local\Akamai\netsession_win.exe"
SCORE: 75
```

21.2 Typical False Positives

- Legitimate software that uses suspicious startup locations

21.3 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
LOCATION	See chapter *File Path Checks*			

CHAPTER

TWENTYTWO

COMMANDCHECK

The CommandCheck module is a meta module that analyses full command lines (path, executable, parameters) in different modules.

22.1 Samples

```
May 20 12:25:49 server55.local.net/10.1.12.2
THOR: Warning: MODULE: CommandCheck
MESSAGE: Command in suspicious location
PATH: C:\Windows\TEMP\vmw72DE.tmp\guestcustutil.exe
SCORE: 75
```

```
May 6 11:26:59 server88.local.net/10.10.9.33
THOR: Warning: MODULE: CommandCheck
MESSAGE: Command in suspicious location
PATH: d:\temp\aaa.cmd
SCORE: 75
```

22.2 Typical False Positives

- Legitimate administrative activity that looks suspicious

22.3 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
LOCATION	See chapter *File Path Checks*			

CHAPTER

TWENTYTHREE

PROCESSHANDLES

The `ProcessHandles` module is a sub module of the `ProcessCheck` module that analyses the handles of each process. The module makes use of the SysInternals `handle.exe` tool that can be placed in the `./tools` sub folder.

23.1 Samples

```
Jun 24 11:52:08 server77.local.net/10.1.90.18
THOR: Warning: MODULE: ProcessHandles
MESSAGE: Suspicious file name in Process Handle detected
VALUE: D:\Lotus\Domino\data\mail\htrang.nsf
PATTERN: \htran
SCORE: 75
DESC: Diverse
PID: 1068
COMMAND: D:\Lotus\Domino\nserver.exe =D:\Lotus\Domino\notes.ini -j
HANDLEID: EF0
HANDLE: File (RW-)
```

```
Aug 4 11:44:08 serv55123/10.2.47.43
THOR: Alert: MODULE: ProcessHandles
MESSAGE: Malware file name in Process Handle detected
VALUE: G:\Documents\InfoStream\mimikatz-master
PATTERN: \mimikatz AND mimikatz
SCORE: 145
DESC: Allgemein
PID: 4
COMMAND: N/A
HANDLEID: 11698
HANDLE: File (RWD)
```

23.2 Typical False Positives

- Legitimate administrative activity that looks suspicious

23.3 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
VALUE	See chapter *File Path Checks*			
PATTERN	Does it look like a weak pattern matching on legitimate handles?	Yes	Good	Medium

CHAPTER

TWENTYFOUR

PROCESSCONNECTION

The `ProcessConnections` module checks the network connections of a process and generates alerts and warnings based on C2 signature matches and suspicious GEO IP lookups.

24.1 Samples

```
Oct 25 17:33:17 server66.local.net/147.2.20.16
THOR: Notice: MODULE: ProcessConnections
MESSAGE: Established connection
PID: 3012
NAME: dfssvc.exe
COMMAND: C:\Windows\system32\dfssvc.exe
LIP: 147.2.20.16
LPORT: 56513
RIP: 147.2.21.188
RPORT: 53389
```

```
Oct 25 17:33:17 server66.local.net/10.1.30.2
THOR: Notice: MODULE: ProcessConnections
MESSAGE: Relevant remote region GEO IP lookup
PID: 3012
NAME: p.exe
COMMAND: C:\Windows\system32\p.exe
LIP: 10.1.30.2
LPORT: 56513
RIP: 14.102.172.144
RPORT: 6022
COUNTRY: PK
```

24.2 Typical False Positives

- A Legitimate software updater that receive updates directly from 3rd party systems
- OS or AV telemetry services (often related to Microsoft, Google, Symantec, McAfee, etc.)
- Legitimate connections to service providers or branch office servers

24.3 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
COMMAND	See chapter *File Path Checks*			
RIP	Is the remote IP (**RIP**) known for malicious activity? (Check the platforms listed in chapter *Tools for Event Analysis*)	Yes	Bad	Medium
		No	Good	Medium
RIP	Does the remote IP lookup point to a service provider or branch office network? (e.g. stock exchange server range in a banking environment, travel data provider network in an aviation environment)	Yes	Good	High
COUNTRY	Is the endpoint in the given country plausible? (e.g. Web server and endpoint in Pakistan = website visitor)	Yes	Good	Medium
		No	Bad	Medium
RPORT	Does a Google search on the remote port show only suspicious, malware or hacking related results? (e.g. lookup for port `4444`)	Yes	Bad	High
LPORT/RPORT	Does the remote port correspond with the local port and is this form of connection legitimate? (e.g. local port is `22 (ssh)` and remote port is `14560`, local port is `80 (http)` and remote port is `34283`)	Yes	Good	Medium
LPORT/RPORT	Does the remote port correspond with the local port and is this form of connection suspicious? (e.g. remote port is `4444`, remote port is `22/tcp (ssh)` and outgoing SSH is `forbidden`)	Yes	Bad	Medium
LIP/RIP	Is the remote system a system in a public IP range that is not related to the company and is the local system an internal system that shouldn't communicate with the Internet directly?	Yes	Bad	High

CHAPTER

TWENTYFIVE

WER

The WER (Windows Error Reporting) module analyses program crash files and checks for special crashes caused by exploits and filename IOC signature matches in the application path. Software can break, so applications tend to crash, hack tools and exploits crash as well. Even if the attackers completely removed their tools from a system, a crashed exploit code, scanner, password dumper or backdoor will still be visible in the Windows Error Reports.

Note

Microsoft's own Incident Response team makes use of the WER file analysis with their own tool named WOLF

25.1 Samples

```
Jun Oct 25 21:01:51 server44.local.net/10.216.2.186
THOR: Notice: MODULE: WER
MESSAGE: Error Report - Found AppHang
EXE: notepad++.exe
DATE: 2011-08-25 07:37:39
FILE: C:\Users\scadmin\AppData\Local\Microsoft\Windows\WER\ReportArchive\AppHang_
↪notepad++.exe_4eafbb67f1329f8691e382b93f71beb6d0fcb99_cfe6cd59_5da093b9\Report.wer
APPPATH: C:\Program Files (x86)\Notepad++\notepad++.exe
ERROR: - / -
FAULT_IN_MODULE: not set
```

25.2 Typical False Positives

- Software is broken so application tend to crash

25.3 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
APPPATH	See chapter *File Path Checks*			
MESSAGE	Does the message contain a CVE number?	Yes	Bad	Medium

CHAPTER

TWENTYSIX

USERACCOUNTS

The `UserAccounts` module analyses the local user database. It checks for suspicious user names, suspicious members in the `Administrators` group, activated guest accounts, user accounts created on Sundays and reports recently logged in users. It applies the `hot time frame` parameter (`-f`) if given and reports suspicious account activity on a given set of dates.

26.1 Samples

```
Jun Oct 25 21:01:51 server44.local.net/10.216.2.186
THOR: Notice: MODULE: UserAccounts
MESSAGE: Recently logged in
USER: sa_backup
FULL_NAME: sa_backup
PRIV: 2
LAST_LOGON: 24/10/2017 16:08:22
BADPWCOUNT: 0
SERVER: \*
NUM_LOGONS: 9
PASS_AGE: 105.00 days
ACTIVE: True
NO_EXPIRE: True
LOCKED: False
```

```
Oct 23 15:27:12 server44.local.net/10.216.2.186
THOR: Warning: MODULE: UserAccounts
MESSAGE: Last password change of user happened in relevant time frame
USER: Administrator
FULL_NAME:
PRIV: 2
LAST_LOGON: 23/10/2017 08:03:15
BADPWCOUNT: 0
SERVER: \*
NUM_LOGONS: 14
PASS_AGE: 3.00 days
ACTIVE: True
NO_EXPIRE: True
LOCKED: False
SCORE: 75
```

```
Aug 28 12:27:29 PROMETHEUS/10.0.2.4 THOR: Warning: MODULE: UserAccounts
MESSAGE: Suspicious user name in Local Administrators group NAME: Guest SCORE: 75
```

```
Sep 8 12:32:39 PROMETHEUS/10.0.2.4 THOR: Warning: MODULE: UserAccounts
MESSAGE: Suspicious user name KEYWORD: (^[0-9a-z]{1,3}$|^test$|^sa
↪$|hack|exploit|nopw|temp)
USER: neo FULL_NAME: PRIV: 2 LAST_LOGON: 30/08/2017 12:43:41 BADPWCOUNT: 0 SERVER: \*
NUM_LOGONS: 352 PASS_AGE: 930.00 days ACTIVE: True NO_EXPIRE: True LOCKED: False SCORE:␣
↪75
```

26.2 Typical False Positives

- Organizations that use short user names (e.g. `ska`, `mba`, `jmi`)
- User creation on a Sunday creates warning messages in regions in which a Sunday is a normal working day (e.g. Israel)

26.3 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
MESSAGE	Is the user name suspicious but plausible in the organization?	Yes	Good	Medium
MESSAGE	Is the Guest account active although it shouldn't be?	Yes	Bad	High
MESSAGE	Has the Guest account be added to the local Administrators?	Yes	Bad	High
MESSAGE	Does the account activity happen in the given hot time frame?	Yes	Bad	Medium

CHAPTER

TWENTYSEVEN

ATJOBS

The `AtJobs` module analyses the local user jobs and just lists them in "Info" level messages and applies the global string check on the command line.

27.1 Samples

- TBT

27.2 Typical False Positives

- Software updater

27.3 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
LOCATION	See chapter *File Path Checks*			

CHAPTER

TWENTYEIGHT

SCHEDULEDTASKS

The `ScheduledTasks` module analyses the local user at jobs and just lists them in "Info" level messages and applies the global string check on the command line.

28.1 Samples

```
Aug 2 14:37:48 server44/192.168.2.4
THOR: Notice: MODULE: ScheduledTasks
MESSAGE: Noticeable file name in command detected
ELEMENT: C:\start1.bat
PATTERN: \start1\.bat$
SCORE: 50
DESC: Indian Cyber Attack Task
NAME: kpistart1 sabato
COMMAND: C:\start1.bat
USER: Webload
LASTRUN: 15/05/2010 14:02:00
NEXTRUN: 30/11/1999 00:00:00
MD5: 666081523aeff8d40d53b4f6aeedd851
SHA1:
```

28.2 Typical False Positives

- Software updaters
- Administrative jobs

28.3 Attribute Evaluation

Attribute	Question	Answer	Indication	Weight
NAME	Does the name look like a random value? (e.g. `jd8slpk8d8`)	Yes	Bad	High
NAME	Does the name contain words in the local language? (e.g. `Datensicherung`, `copiar-datos-privados`)	Yes	Good	High
LOCATION	See chapter *File Path Checks*			

CHAPTER

TWENTYNINE

RESCONTROL

The `Rescontrol` (Resource Control) module generates "Warning" level messages in cases a resource limit has been reached. In most of the cases, this is caused by very low free main memory levels or false positives that generated many SYSLOG messages. Resource control is active by default and can be deactivated with (`--norescontrol`).

Resource control:

- Stops the THOR scan if the available free main memory drops below 50MB
- Switches to `reduced syslog mode` (Warnings and Alerts only) if more than 5MB of data has been sent via Syslog

29.1 Samples

```
Aug 2 14:37:48 server44/192.168.2.4
THOR: Warning: MODULE: Rescontrol
MESSAGE: Stopping THOR scan in order to avoid a memory outage (use --norescontrol to␣
↪avoid this)
SCORE: 75
```

```
Aug 2 14:37:48 server44/192.168.2.4
THOR: Warning: MODULE: Rescontrol
MESSAGE: Logged more than 5000000 bytes via SYSLOG. This seems odd. Resource control␣
↪activates 'reduced syslog' mode.
SCORE: 75
```

CHAPTER

THIRTY

DEEPDIVE

A `DeepDive` on memory images or disk space cannot be analyzed by THOR events alone. You typically need the memory dumps or restored chunks to evaluate the findings. This typically takes a lot more time, know-how and effort to complete.

We recommend the analysis of DeepDive module events only in case other indicators give a sufficient initial suspicion.

30.1 Samples

```
Sep 5 17:23:56 server44.local.net/10.16.3.7
THOR: Alert: MODULE: DeepDive
MESSAGE: YARA Score Rule Match
TARGET: C:\WINDOWS\PCHEALTH\ERRORREP\UserDumps\thor.exe.20170904-154909-00.hdmp
TYPE: file
NAME: HurricanePanda_C2_Server
SCORE: 180
DESCRIPTION: Hurricane Panda C2 Server in file http://goo.gl/Fm00Q8
OFFSET: 203423744
MATCHING_STRINGS:
        S1: 203.135.134.243
                IN: 1dns.dubkill.com.in$s2203.135.134.243$s3newss.effers.com$s4
        S2: 202.181.133.237
                IN: upport.proxydns.com$s13202.181.133.237MobileDevicesUsedtoExecu
        S3: 223.29.248.9
                IN: e.authorizeddns.org$s11223.29.248.9$s12googlesupport.proxy
        S4: 61.78.34.179
...
```

```
Aug 26 22:20:18 server44.local.net/10.10.1.4
THOR: Alert: MODULE: DeepDive
MESSAGE: YARA Score Rule Match
TARGET: C:\Program Files (x86)\Common Files\McAfee\TalkBack\Data\RPCSERV(1).dmp
TYPE: file
NAME: WindowsCredentialEditor
SCORE: 140
DESCRIPTION: Windows Credential Editor
OFFSET: 203423744
MATCHING_STRINGS:
        S1: Windows Credentials Editor
                IN: %.2X%.2XttcaWindows Credentials Editor-- by Hernan Ochoa (herna
...
```

30.2 Typical False Positives

- Antivirus signatures in pagefile.sys or in disk surface scans
- Findings in `\McAfee\TalkBack\Data\RPCSERV`
- THOR process dump files

CHAPTER

THIRTYONE

OTHER MODULES

Messages from other modules like `Rootkit`, `SkeletonKey`, `ReginFS` should always be considered relevant and handled with high priority.

31.1 Samples

```
Aug 23 11:26:26 server44.local.net/10.16.22.2
THOR: Notice: MODULE: SkeletonKey
MESSAGE: Domain Controller supports AES type encryption. No SkeletonKey type attack␣
↪detected.
```

CHAPTER

THIRTYTWO

GENERIC CHECKS

32.1 File Path Checks

The checks listed in the following table apply to any file path string in many different modules.

Attribute	Question	Answer	Indication	Weight
FILE	Is the file located in a temporary directory? (e.g. `C:\Temp`, `C:\Users\user1\AppData\Local\Temp`)	Yes	Bad	Medium
FILE	Does the path contain elements in a local language? (e.g. `...\Datensicherung`, `C:\Progs\Zeiterfassung\ze.exe`)	Yes	Good	Medium
FILE	Does the file have matches on other systems as well?	Yes, more than **1**		
		Yes, on more than **10**	Good	Medium
		Yes, on more than **100**	Good	High
FILE	Is the file name known on Google? (results point to goodware or known Windows file names)	Yes	Good	Medium
FILE	Is the file name known on Google and results point to malware or hack tools?	Yes	Bad	Medium
FILE	Does an exact Google search for the program path return no results?	Yes	Bad	Low
FILE	Do sandbox reports and antivirus scan reports show up, when you google the filename or specific path name (e.g. `GoogleMasterUpdate\gm.exe`)	Yes	Bad	Medium
FILE	Does the path look like a "backup" directory or user's "home folder" on a server drive (e.g. `G:\Backup2007\...` or `N:\Home-Folders\user2345\AppData\Local\Temp`)	Yes	Good	Medium
FILE	Is the file located in an `%AppData%` folder in the user profile?	Yes	Bad	Low
FILE	Is the file located in a folder that should not contain executable files? (e.g. `C:\Windows\Fonts`, `C:\PerfLogs`, `C:\Users\x123\AppData\Roaming\Microsoft\certs`, `C:\Windows\inf`, `C:\Users\Public\Documents`)	Yes	Bad	Medium
FILE	Does the file name look like a tool used for administration purposes? (e.g. `C:\robocopy-migration.exe`)	Yes	Good	Low
FILE	Is the path a mounted / shared network drive? (e.g. `\\tsclient\C$`, `\\server1\C$\temp\m.exe`)	Yes	Bad	Medium
FILE	Does the path look like the product is a strange custom software? (e.g. `C:\Temp\Arbeitszeitnachweis\AZN-service.exe`)	Yes	Good	Medium
FILE	Is the program located directly in a folder that is typically empty and only contains sub directories? (e.g. `C:\ProgramData\1.exe`, `C:\Users\user\AppData\Roaming\1.exe`)	Yes	Bad	Medium
FILE	Does the file look as if it has been modified by a user to circumvent security filters? (e.g. Text file reported as executable: `Weihnachsgrüße.txt`, `ChromePortable.txt`)	Yes	Good	Low

32.2 Hash Checks

We recommend using Virustotal for the analysis of Hash values.

- www.virustotal.com

The checks listed in the following table apply to any hash value reported in many different modules.

Attribute	Question	Answer	Indication	Weight
MD5/SHA1/SHA256	What does the Virustotal.com check show?	Unknown		
		Suspicious (> 2 matches)	Bad	High
		Malicious (> 10 matches)	Bad	High
MD5/SHA1/SHA256	Does Virustotal show other suspicious names in the `Additional Information` tab – e.g. file names with `.vir` or `.virobj` extension, or file names that are hashes	Yes	Bad	Low
MD5/SHA1/SHA256	Is `first submission` on Virustotal very far in the past? (>7 years)	Yes	Good	Low
MD5/SHA1/SHA256	Are there any negative votes or comments on Virustotal?	Yes	Bad	Medium
MD5/SHA1/SHA256	Does at least one matching AV signature on Virustotal contain one of the following keywords: `Hack`, `Scan`, `Dump`, `Password`, `Webshell`	Yes	Bad	High
MD5/SHA1/SHA256	Is the file part of the Microsoft software catalogue? (Virustotal shows that on a green bar above the analysis)	Yes	Good	High
MD5/SHA1/SHA256	Does Virustotal show the bar "probably harmless"?	Yes	Good	High
MD5/SHA1/SHA256	Does the file has a valid software signature from a trusted vendor?	Yes	Good	Medium
MD5/SHA1/SHA256	Does the listed `File names` contain only legitimate names? (e.g. `javaw.exe`, `java.exe`)	Yes	Good	Low
MD5/SHA1/SHA256	Does the listed `File names` contain hash values?	Yes	Bad	Low
MD5/SHA1/SHA256	Does the Portable Executable (PE, EXE) file have a very old compilation time stamp? (> 10 years)	Yes	Good	Low

CHAPTER

THIRTYTHREE

TOOLS FOR EVENT ANALYSIS

This list of tools will help you with your event analysis.

33.1 VirusTotal

Used for: File Hashes, Domains, IPs, File Names
www.virustotal.com

Also search for IPs and Domain Names – Examples:
`https://www.virustotal.com/en/domain/DOMAIN/information/`
`https://www.virustotal.com/en/ip-address/58.158.177.102/information/`

File Name Search – via Google Search:
`inurl:virustotal.com filename`

33.2 PEStudio

Windows tool that helps in the initial and static assessment of a file Sample (if available)
www.winitor.com

33.3 APT Custom Search

Custom Search Engine for APT related Sites
cse.google.com

33.4 Hybrid Analysis

Used for: Samples Upload, search for methods and keywords
hybrid-analysis.com

33.5 any.run

Used for Sample Upload and more
any.run

33.6 Automatic Hash Checks

You can use the Python script `munin.py` to batch process lists of Hash values or even complete THOR log files as the script automatically extracts the relevant values from each line. The best option is to use the `*.csv` files produced after a THOR run and use them as input for the script.

```
user@unix~:$ cat *.csv >> all-hashes.csv
user@unix~:$ python munin.py -i config.ini -f all-hashes.csv
```

github.com/Neo23x0/munin

CHAPTER

THIRTYFOUR

INDICES AND TABLES

- search