

Important Note

This project is only inactively maintained. This means that I merge pull request for bug fixes and issues that can be easily integrated but I don't have the time to add new features or extend existing ones. For years, I've been working on a much more sophisticated scanner called THOR. There is a free version of THOR Lite available. THOR Lite is faster, more stable, tested in our CI environments and simply the better solution. You can find a comparison of the open source, free and commercial scanner [here](#). I've also started working on a Rust-based version of LOKI called LOKI 2 but I have no idea when it's in a state that reflects the current feature set of LOKI. A while ago I made a flow chart to help you with the decision which scanner to use.



Loki - Simple IOC and YARA Scanner

Scanner for Simple Indicators of Compromise

Detection is based on four detection methods:

- 1 1. File Name IOC
- 2 Regex match on full file path/name
- 3
- 4 2. Yara Rule Check
- 5 Yara signature match on file data and process memory
- 6
- 7 3. Hash Check
- 8 Compares known malicious hashes (MD5, SHA1, SHA256) with scanned
- 9 files
- 10
- 10 4. C2 Back Connect Check
- 11 Compares process connection endpoints with C2 IOCs (**new** since
- version v.10)

Additional Checks:

- 1 1. Regid filesystem check (via --reginfs)
- 2 2. Process anomaly check (based on [Sysforensics](<http://goo.gl/P99QZQ>))
- 3 3. SWF decompressed scan (**new** since version v0.8)

The Windows binary is compiled with PyInstaller and should run as x86 application on both x86 and x64 based systems.

How-To Run LOKI and Analyse the Reports

Run

- Download the newest version of LOKI from the releases section
- Extract the program package
- Run loki-upgrader.exe on system with Internet access to retrieve the newest signatures
- Bring the program folder to a target system that should be scanned: removable media, network share, folder on target system
- Open a command line “cmd.exe” as Administrator and run it from there (you can also run LOKI without administrative privileges but some checks will be disabled and relevant objects on disk will not be accessible)

Reports

- The resulting report will show a GREEN, YELLOW or RED result line.
- Please analyse the findings yourself by:
 1. uploading non-confidential samples to Virustotal.com
 2. Search the web for the filename
 3. Search the web for keywords from the rule name (e.g. EQUATIONGroupMalware_1 > search for “Equation Group”)
 4. Search the web for the MD5 hash of the sample
- Please report back false positives via the “Issues” section, which is accessible via the right sidebar (mention the false positive indicator like a hash and/or filename and the rule name that triggered)

Requirements

No requirements if you use the compiled EXE.

If you want to build it yourself:

- yara : It's recommended to use the most recent version of the compiled packages for Windows (x86) - Download it from here: <https://github.com/VirusTotal/yara-python/releases>
- colorama : to color it up
- psutil : process checks
- pywin32 : path conversions (PyInstaller issue; Windows only)

Usage

```

1  usage: loki.py [-h] [-p path] [-s kilobyte] [-l log-file] [-r remote-
   loghost]
2                  [-t remote-syslog-port] [-a alert-level] [-w warning-
   level]
3                  [-n notice-level] [--allhds] [--alldrives] [--printall]
4                  [--allreasons] [--noprocsan] [--nofilescan] [--
   vulnchecks]
5                  [--nolevcheck] [--scriptanalysis] [--rootkit] [--
   noindicator]
6                  [--dontwait] [--intense] [--csv] [--onlyrelevant] [--
   nolog]
7                  [--update] [--debug] [--maxworkingset MAXWORKINGSET]
8                  [--syslogtcp] [--logfolder log-folder] [--nopesieve]
9                  [--pesieveshellc] [--nolisten]
10                 [--excludeprocess EXCLUDEPROCESS] [--force]
11
12  Loki - Simple IOC Scanner
13
14  optional arguments:
15  -h, --help            show this help message and exit
16  -p path                Path to scan
17  -s kilobyte            Maximum file size to check in KB (default 5000
   KB)
18  -l log-file            Log file
19  -r remote-loghost      Remote syslog system
20  -t remote-syslog-port  Remote syslog port
21
22  -a alert-level          Alert score
23  -w warning-level        Warning score
24  -n notice-level         Notice score
25  --allhds                Scan all local hard drives (Windows only)
26  --alldrives             Scan all drives (including network drives and
   removable media)
27
28  --printall              Print all files that are scanned
29  --allreasons            Print all reasons that caused the score
30  --noprocsan             Skip the process scan
31  --nofilescan            Skip the file scan
32  --vulnchecks            Run the vulnerability checks
33  --nolevcheck            Skip the Levenshtein distance check

```

34	<code>--scriptanalysis obfuscated</code>	Statistical analysis for scripts to detect code (beta)
35		
36	<code>--rootkit</code>	Skip the rootkit check
37	<code>--noindicator</code>	Do not show a progress indicator
38	<code>--dontwait</code>	Do not wait on exit
39	<code>--intense and</code>	Intense scan mode (also scan unknown file types
40		all extensions)
41	<code>--csv processing)</code>	Write CSV log format to STDOUT (machine
42	<code>--onlyrelevant</code>	Only print warnings or alerts
43	<code>--nolog</code>	Don't write a local log file
44	<code>--update sub</code>	Update the signatures from the "signature-base"
45		repository
46	<code>--debug</code>	Debug output
47	<code>--maxworkingset MAXWORKINGSET</code>	
48		Maximum working set size of processes to scan (in MB,
49		default 100 MB)
50	<code>--syslogtcp</code>	Use TCP instead of UDP for syslog logging
51	<code>--logfolder log-folder</code>	
52		Folder to use for logging when log file is not specified
53		
54	<code>--nopesieve</code>	Do not perform pe-sieve scans
55	<code>--pesieveshellc</code>	Perform pe-sieve shellcode scan
56	<code>--nolisten</code>	Do not show listening connections
57	<code>--excludeprocess EXCLUDEPROCESS</code>	
58		Specify an executable name to exclude from scans, can
59		be used multiple times
60	<code>--force excluded</code>	Force the scan on a certain folder (even if
61		with hard exclude in LOKI's code

Signature and IOCs

Since version 0.15 the Yara signatures reside in the sub-repository signature-base. You will not get the sub-repository by downloading the LOKI as ZIP file. It will be included when you clone the repository.

The IOC files for hashes and filenames are stored in the './signature-base/iocs' folder. All 'yar' files placed in the './signature-base/yara' folder will be initialized together with the rule set that is already included. Use the 'score' value to define the level of the message upon a signature match.

You can add hash, c2 and filename IOCs by adding files to the './signature-base/iocs' subfolder. All hash IOCs and filename IOC files must be in the format used by LOKI (see the default files). The files

must have the strings “hash”, “filename” or “c2” in their name to get pulled during initialization.

For Hash IOCs (divided by newline; hash type is detected automatically)

```
1 Hash;Description [Reference]
```

For Filename IOCs (divided by newline)

```
1 # (optional) Description [Reference]
2 Filename as Regex[;Score as integer[;False-positive as Regex]]
```

User-Defined Scan Excludes

Since version v0.16.2 LOKI supports the definition of user-defined excludes via “excludes.cfg” in the new “./config” folder. Each line represents a regular expression that gets applied to the full file path during the directory walk. This way you can exclude certain directories regardless of their drive name, file extensions in certain folders and all files and directories that belong to a product that is sensitive to antivirus scanning.

The ‘“exclude.cfg”’ looks like this:

```
1 # Excluded directories
2 #
3 # - add directories you want to exclude from the scan
4 # - double escape back slashes
5 # - values are case-insensitive
6 # - remember to use back slashes on Windows and slashes on Linux / Unix
   / OSX
7 # - each line contains a regex that matches somewhere in the full path
   (case insensitive)
8 #   e.g.:
9 #   Regex: \\System32\\
10 #   Matches C:\Windows\System32\cmd.exe
11 #
12 #   Regex: /var/log/[^/]+\..log
13 #   Matches: /var/log/test.log
14 #   Not Matches: /var/log/test.gz
15 #
16
17 # Useful examples
18 \\Ntfrs\\
19 \\Ntds\\
20 \\EDB[^\.]+\..log
21 Sysvol\\Staging\\Ntfrs_cmp
22 \\System Volume Information\\DFSR
```

Screenshots

Loki Scan



```
LOKI
Simple IOC Scanner

(C) Florian Roth - BSK Consulting GmbH
Jan 2015
Version 0.2

DISCLAIMER - USE AT YOUR OWN RISK

[INFO] LOKI - Starting Loki Scan on PROMETHEUS
[INFO] File Name Characteristics initialized with 32 regex patterns
[INFO] Malware Hashes initialized with 43 hashes
[INFO] False Positive Hashes initialized with 8 hashes
[INFO] [INFO] Skipping Process - PID: 0 NAME: System Idle Process CMD: N/A
[INFO] [INFO] Skipping Process - PID: 4 NAME: System CMD: N/A
[NOTICE] Scanning Process - PID: 292 NAME: smss.exe CMD: \SystemRoot\System32\smss.exe
[NOTICE] Scanning Process - PID: 380 NAME: csrss.exe CMD: %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
[NOTICE] Scanning Process - PID: 428 NAME: wininit.exe CMD: wininit.exe

[NOTICE] Scanning Process - PID: 436 NAME: csrss.exe CMD: %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
[NOTICE] Scanning Process - PID: 476 NAME: winlogon.exe CMD: winlogon.exe
[NOTICE] Scanning Process - PID: 524 NAME: services.exe CMD: C:\Windows\s
```

Regin Matches

LOKI

Simple IOC Scanner

(C) Florian Roth - BSK Consulting GmbH
Jan 2015
Version 0.2

DISCLAIMER - USE AT YOUR OWN RISK

```
[INFO] LOKI - Starting Loki Scan on PROMETHEUS
[INFO] File Name Characteristics initialized with 32 regex patterns
[INFO] Malware Hashes initialized with 43 hashes
[INFO] False Positive Hashes initialized with 8 hashes
[INFO] Scanning C:\ ...
-[ALERT] Malware Hash TYPE: SHA256 HASH: b12c7d57507286bbbe36d7acf9b34c22
c96606ffd904e3c23008399a4a50c047 FILE: C:\$Recycle.Bin\S-1-5-21-949666807-
3097873-177000209-1000\RC7V2PZ.sys DESC: Regin Malware Sample
[ALERT] Yara Rule MATCH: Regin_APT_KernelDriver_Generic_B FILE: C:\$Recyc
le.Bin\S-1-5-21-949666807-3097873-177000209-1000\RC7V2PZ.sys
```

Regin False Positives

```
X:\Workspace\Loki>python loki.py --noproc -p M:\Regin\falsepositive
```

The logo for LOKI, rendered in a large, green, pixelated font on a black background.

Simple IOC Scanner

(C) Florian Roth - BSK Consulting GmbH
Jan 2015
Version 0.2

DISCLAIMER - USE AT YOUR OWN RISK

```
[INFO] LOKI - Starting Loki Scan on PROMETHEUS
[INFO] File Name Characteristics initialized with 32 regex patterns
[INFO] Malware Hashes initialized with 43 hashes
[INFO] False Positive Hashes initialized with 8 hashes
[INFO] Scanning M:\Regin\falsepositive ...
/[INFO] SYSTEM SEEMS TO BE CLEAN.
```

```
Press Enter to exit ...
```

Hash based IOCs


```
#
# LOKI CUSTOM EVIL HASHES
# This file contains MD5, SHA1 and SHA256 hashes and a short info like file name
# or hash origin
#
# FORMAT -----
#
# MD5;COMMENT
# SHA1;COMMENT
# SHA256;COMMENT
#
# EXAMPLES -----
#
# 0c2674c3a97c53082187d930efb645c2;DEEP PANDA Sakula Malware - http://goo.gl/R3e6eG
# 000c907d39924de62b5891f8d0e03116;The Darkhotel APT http://goo.gl/DuS7WS
# c03318cb12b827c03d556c8747b1e323225df97bdc4258c2756b0d6a4fd52b47;Operation SMN Hashes http://goo.gl/0K6tW
# 563d1512178cec1f6a73c98d565c98fa;Cygwin nc.exe example

5d853a8de18d844a9ab269f3d51e5072;Five Eyes QUERTY Malware20120.dll.bin
cc8b737edb3f11c9c5dba57035c63103;Five Eyes QUERTY Malware20120.xml
67ac8dc6589a07d950bd12f534dc9789;Five Eyes QUERTY Malware20120_cmdDef.xml
40451f20371329b992fb1b85c754d062;Five Eyes QUERTY Malware20121.dll.bin
ff0afae5c68c5177ed0a3d6339810cae;Five Eyes QUERTY Malware20121.xml
1bc8f4df4551c6efbbb1fe9f965dca49;Five Eyes QUERTY Malware20121_cmdDef.xml
0ed11a73694999bc45d18b4189f41ac2;Five Eyes QUERTY Malware20123.sys.bin
066b6253afc3ad0efe9a15cead4ef7d8;Five Eyes QUERTY Malware20123.xml
790d1b448e97985deb710a94eb927c27;Five Eyes QUERTY Malware20123_cmdDef.xml

ad61e8daeeba43e442514b177a1b41ad4b7c6727;Skeleton Key Malware
5083b17ccc50dd0557dfc544f84e2ab55d6acd92;Skeleton Key Malware

20831e820af5f41353b5afab659f2ad42ec6df5d9692448872f3ed8bbb40ab92;Regin Malware Sample
225e9596de85ca7b1025d6e444f6a01aa6507feef213f4d2e20da9e7d5d8e430;Regin Malware Sample
392f32241cd3448c7a435935f2ff0d2cdc609dda81dd4946b1c977d25134e96e;Regin Malware Sample
40c46bcab9acc0d6d235491c01a66d4c6f35d884c19c6f410901af6d1e33513b;Regin Malware Sample
4139149552b0322f2c5c993abccc0f0d1b38db4476189a9f9901ac0d57a656be;Regin Malware Sample
4e39bc95e35323ab586d740725a1c8cbcde01fe453f7c4cac7cced9a26e42cc9;Regin Malware Sample
5001793790939009355ba841610412e0f8d60ef5461f2ea272ccf4fd4c83b823;Regin Malware Sample
5c81cf8262f9a8b0e100d2a220f7119e54edfc10c4fb906ab7848a015cd12d90;Regin Malware Sample
7553d4a5914af58b23a9e0ce6a262cd230ed8bb2c30da3d42d26b295f9144ab7;Regin Malware Sample
7d38eb24cf5644e090e45d5efa923aff0e69a600fb0ab627e8929bb485243926;Regin Malware Sample
8098938987e2f29e3ee416b71b932651f6430d15d885f2e1056d41163ae57c13;Regin Malware Sample
```

File Name based IOCs

```

#
# LOKI File Name Characteristics
# This file contains regex definitions and a description
#
# APPLICATION -----
#
# Every line is treated as REGEX case sensitive.
# Every line includes a description that gives information about the file name
# based IOC
#
# FORMAT -----
#
# # COMMENT
# REGEX;DESCRIPTION
#
# EXAMPLES -----
#
# # Various examples from APT case X
# \\svcsstat\.exe;Case 1 - infector
# \\(server|services|smrr|srm|svchost|svhost|svshost|taskmgr)\.exe$;Common IOC
# ProgramData\Mail\MailAg\;Case 2
# (Anwendungsdaten|Application Data|APPDATA)\\sydmain\.dll;Malware X Case 3
# (TEMP|Temp)\\[^\\]+\.(xmd|y|ls)$;Case 2
# (LOCAL SETTINGS\\Temp|Local Settings\\Temp|Local\\Temp)\\(word\.exe|winword\.exe);Case 2
#
# Ncat Example
# bin\\nc\.exe;Ncat Demo
#
# Regin
\\usbclass\.sys;File name known from REGIN malware
\\adpu160\.sys;File name known from REGIN malware
\\msrdc64\.dat;File name known from REGIN malware
\\msdcsvc\.dat;File name known from REGIN malware
\\config\\SystemAudit\.Evt;File name known from REGIN malware
\\config\\SecurityAudit\.Evt;File name known from REGIN malware
\\config\\SystemLog\.evt;File name known from REGIN malware
\\config\\ApplicationLog\.evt;File name known from REGIN malware
\\ime\\imesc5\\dicts\\pintlgb\*.imd;File name known from REGIN malware
\\ime\\imesc5\\dicts\\pintlgbp\*.imd;File name known from REGIN malware
ystem32\\winhttpc\.dll;File name known from REGIN malware
ystem32\\wshnetc\.dll;File name known from REGIN malware
\\SysWow64\\wshnetc\.dll;File name known from REGIN malware
ystem32\\svcsstat\.exe;File name known from REGIN malware
ystem32\\svcsstat\.exe;File name known from REGIN malware
IME\\IMESC5\\DICTS\\PINTLGBP\*.IMD;File name known from REGIN malware
ystem32\\wsharp\.dll;File name known from REGIN malware
ystem32\\wshnetc\.dll;File name known from REGIN malware
pchealth\\helpctr\\Database\\cdata\.dat;File name known from REGIN malware
pchealth\\helpctr\\Database\\cdata\.edb;File name known from REGIN malware
Windows\\Panther\\setup\.etl\*.000;File name known from REGIN malware
ystem32\\wbem\\repository\\INDEX2\.DATA;File name known from REGIN malware
ystem32\\wbem\\repository\\OBJECTS2\.DATA;File name known from REGIN malware
ystem32\\dnscache\.dat;File name known from REGIN malware
ystem32\\mregnx\.dat;File name known from REGIN malware
ystem32\\displn32\.dat;File name known from REGIN malware
ystem32\\dmdskwk\.dat;File name known from REGIN malware
ystem32\\nwrsnu\.dat;File name known from REGIN malware
ystem32\\tapiscfg\.dat;File name known from REGIN malware
ystem32\\pciclass\.sys;File name known from REGIN malware

```

Generated log file

```

Jan 18 13:26:43 PROMETHEUS LOKI: LOKI - Starting Loki Scan on PROMETHEUS
Jan 18 13:26:43 PROMETHEUS LOKI: File Name Characteristics initialized with 32 hashes
Jan 18 13:26:43 PROMETHEUS LOKI: Malware Hashes initialized with 43 hashes
Jan 18 13:26:43 PROMETHEUS LOKI: False Positive Hashes initialized with 8 hashes
Jan 18 13:26:43 PROMETHEUS LOKI: Scanning M:\FiveEyes ...
Jan 18 13:26:43 PROMETHEUS LOKI: File Name PATTERN: \\20120\\.dll DESC: Five Eyes QUERTY Malware Name MATCH: M:\FiveEyes\qwerty\20
Jan 18 13:26:43 PROMETHEUS LOKI: Malware Hash TYPE: MD5 HASH: 5d853a8de18d844a9ab269f3d51e5072 FILE: M:\FiveEyes\qwerty\20120.dll
Jan 18 13:26:43 PROMETHEUS LOKI: Yara Rule MATCH: FiveEyes_QUERTY_Malwaresig_20120_dll FILE: M:\FiveEyes\qwerty\20120.dll.bin
Jan 18 13:26:43 PROMETHEUS LOKI: Malware Hash TYPE: MD5 HASH: cc8b737edb3f11c9c5dba57035c63103 FILE: M:\FiveEyes\qwerty\20120.xml
Jan 18 13:26:43 PROMETHEUS LOKI: Yara Rule MATCH: FiveEyes_QUERTY_Malwareqwerty_20121 FILE: M:\FiveEyes\qwerty\20120.xml
Jan 18 13:26:43 PROMETHEUS LOKI: Yara Rule MATCH: FiveEyes_QUERTY_Malwareqwerty_20120 FILE: M:\FiveEyes\qwerty\20120.xml
Jan 18 13:26:43 PROMETHEUS LOKI: Malware Hash TYPE: MD5 HASH: 67ac8dc6589a07d950bd12f534dc9789 FILE: M:\FiveEyes\qwerty\20120_cmd
Jan 18 13:26:43 PROMETHEUS LOKI: Yara Rule MATCH: FiveEyes_QUERTY_Malwaresig_20120_cmdDef FILE: M:\FiveEyes\qwerty\20120_cmdDef.x
Jan 18 13:26:43 PROMETHEUS LOKI: File Name PATTERN: \\20121\\.dll DESC: Five Eyes QUERTY Malware Name MATCH: M:\FiveEyes\qwerty\20
Jan 18 13:26:43 PROMETHEUS LOKI: Malware Hash TYPE: MD5 HASH: 40451f20371329b992fb1b85c754d062 FILE: M:\FiveEyes\qwerty\20121.dll
Jan 18 13:26:43 PROMETHEUS LOKI: Yara Rule MATCH: FiveEyes_QUERTY_Malwaresig_20121_dll FILE: M:\FiveEyes\qwerty\20121.dll.bin
Jan 18 13:26:43 PROMETHEUS LOKI: Malware Hash TYPE: MD5 HASH: ff0afae5c68c5177ed0a3d6339810cae FILE: M:\FiveEyes\qwerty\20121.xml
Jan 18 13:26:43 PROMETHEUS LOKI: Yara Rule MATCH: FiveEyes_QUERTY_Malwareqwerty_20121 FILE: M:\FiveEyes\qwerty\20121.xml
Jan 18 13:26:43 PROMETHEUS LOKI: Malware Hash TYPE: MD5 HASH: 1bc8f4df4551c6efbbb1fe9f965dca49 FILE: M:\FiveEyes\qwerty\20121_cmd
Jan 18 13:26:43 PROMETHEUS LOKI: Yara Rule MATCH: FiveEyes_QUERTY_Malwaresig_20121_cmdDef FILE: M:\FiveEyes\qwerty\20121_cmdDef.x
Jan 18 13:26:43 PROMETHEUS LOKI: File Name PATTERN: \\20123\\.sys DESC: Five Eyes QUERTY Malware Name MATCH: M:\FiveEyes\qwerty\20
Jan 18 13:26:43 PROMETHEUS LOKI: Malware Hash TYPE: MD5 HASH: 0ed11a73694999bc45d18b4189f41ac2 FILE: M:\FiveEyes\qwerty\20123.sys
Jan 18 13:26:43 PROMETHEUS LOKI: Yara Rule MATCH: FiveEyes_QUERTY_Malwaresig_20123_sys FILE: M:\FiveEyes\qwerty\20123.sys.bin
Jan 18 13:26:43 PROMETHEUS LOKI: Malware Hash TYPE: MD5 HASH: 066b6253afc3ad0efe9a15cead4ef7d8 FILE: M:\FiveEyes\qwerty\20123.xml
Jan 18 13:26:43 PROMETHEUS LOKI: Yara Rule MATCH: FiveEyes_QUERTY_Malwareqwerty_20123 FILE: M:\FiveEyes\qwerty\20123.xml
Jan 18 13:26:43 PROMETHEUS LOKI: Malware Hash TYPE: MD5 HASH: 790d1b448e97985deb710a94eb927c27 FILE: M:\FiveEyes\qwerty\20123_cmd
Jan 18 13:26:43 PROMETHEUS LOKI: Yara Rule MATCH: FiveEyes_QUERTY_Malwaresig_20123_cmdDef FILE: M:\FiveEyes\qwerty\20123_cmdDef.x
Jan 18 13:26:43 PROMETHEUS LOKI: INDICATORS DETECTED!

```

Contact

LOKI scanner on our company homepage <https://www.nextron-systems.com/loki/>

Twitter @cyb3rOps @thor_scanner

If you are interested in a corporate solution for APT scanning, check out Loki's big brother THOR.

Compile the Scanner

Download PyInstaller, switch to the pyinstaller program directory and execute:

```
1 python ./pyinstaller.py -F C:\path\to\loki.py
```

This will create a `loki.exe` in the subfolder `./loki/dist`.

Pro Tip (optional)

To include the `msvcr100.dll` to improve the target os compatibility change the line in the file `./loki/loki.spec` that contains `a.binaries`, to the following:

```
1 a.binaries + [('msvcr100.dll', 'C:\Windows\System32\msvcr100.dll', 'BINARY')],
```

Use LOKI on Mac OS X (Or later) or Linux

- Install libraries `sudo pip install colorama yara-python psutil rfc5424-logging-handler netaddr`
- Run loki-upgrader.py `sudo python loki-upgrader.py`
- Run loki `sudo python loki.py`

Yara sources

Download Yara sources from [here](#)

Antivirus - False Positives

The compiled scanner may be detected by antivirus engines. This is caused by the fact that the scanner is a compiled python script that implement some file system and process scanning features that are also used in compiled malware code.

If you don't trust the compiled executable, please compile it yourself.

License

Loki - Simple IOC Scanner Copyright (c) 2015 Florian Roth

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see <http://www.gnu.org/licenses/>