

Name: Ramya Ajay

Roll No: CB.EN.P2CYS22004

Yara

Yara

Introduction to Yara rules (Task 4)

yara myrule.yar somefile
where

yara - Command

myrule.yar - File that contains yara rule

somefile - Name of file, directory, or process ID to use the rule for.

Using LOKI and its YARA rule set (Task 8)

Scan file 1. Does Loki detect this file as suspicious/malicious or benign?

Suspicious

```
cmnatic@thm:~/suspicious-files/pe-sieve$ python ../../tools/Loki/loki.py -p .
cmnatic@thm-yara:~/suspicious-files/file1$ python ../../tools/Loki/loki.py -p .

LOKI
LOKIRENNER

Copyright by Florian Roth, Released under the GNU General Public License
Version 0.32.1

DISCLAIMER - USE AT YOUR OWN RISK
Please report false positives via https://github.com/Neo23x0/Loki/issues

[NOTICE] Starting Loki Scan VERSION: 0.32.1 SYSTEM: thm-yara TIME: 20230606T16:17:30Z PLATFORM: PROC: x86_64 ARCH: 64bit
[NOTICE] Registered plugin PluginWMI
[NOTICE] Loaded plugin /home/cmnatic/tools/Loki/plugins/loki-plugin-wmi.py
[NOTICE] PE-Sieve successfully initialized BINARY: /home/cmnatic/tools/Loki/tools/pe-sieve64.exe SOURCE: https://github.com/hasherezade/pe-sieve
[INFO] File Name Characteristics initialized with 2841 regex patterns
[INFO] C2 server indicators initialized with 1541 elements
[INFO] Malicious MD5 Hashes initialized with 19034 hashes
```

```

[NOTICE] Starting Loki Scan VERSION: 0.32.1 SYSTEM: thm-yara TIME: 20230606T16:17:30Z PLATFORM: PROC: x86_64 ARCH: 64bit
[NOTICE] Registered plugin PluginWMI
[NOTICE] Loaded plugin /home/cmnatic/tools/Loki/plugins/Loki-plugin-wmi.py
[NOTICE] PE-Sieve successfully initialized BINARY: /home/cmnatic/tools/Loki/tools/pe-sieve64.exe SOURCE: https://github.com/hasherezade/pe-sieve
[INFO] File Name Characteristics initialized with 2841 regex patterns
[INFO] C2 server indicators initialized with 1541 elements
[INFO] Malicious MD5 Hashes initialized with 19034 hashes
[INFO] Malicious SHA1 Hashes initialized with 7159 hashes
[INFO] Malicious SHA256 Hashes initialized with 22841 hashes
[INFO] False Positive Hashes initialized with 30 hashes
[INFO] Processing YARA rules folder /home/cmnatic/tools/Loki/signature-base/yara
[INFO] Initializing all YARA rules at once (composed string of all rule files)
[INFO] Initialized 653 Yara rules
[INFO] Reading private rules from binary ...
[NOTICE] Program should be run as 'root' to ensure all access rights to process memory and file objects.
[NOTICE] Running plugin PluginWMI
[NOTICE] Finished running plugin PluginWMI
[INFO] Scanning ...
[WARNING]
FILE: ~/ind3k.php SCORE: 70 TYPE: PHP SIZE: 80992
FIRST BYTES: 3e3f7068700a2f2a0a0962337346b20322e320a / <?php/*b374k 2.2
MD5: 1606bdac2cb613bf0b08a22690364fbc5
SHA1: 9383ed4ee7df17193f7a034c3190ecabc9000f9f
SHA256: 5479f8cd1375364770df36e5a18262480a8f9d311e8eedb2c2390ecb233852ad CREATED: Mon Nov 9 15:15:32 2020 MODIFIED: Mon Nov 9 13:06:56 2020 ACCESSED: Tue Ju
n 6 16:15:52 2023
REASON 1: Yara Rule MATCH: webshell metasoft SUBSCORE: 70
DESCRIPTION: Web Shell - file metasoft.php REF: -
MATCHES: Str1: $buff .= "<tr><td><a href=\\\"?d=\\\". $pwd.\\\"\\\">[ $folder ]</a></td><td>LINK</t
[NOTICE] Results: 0 alerts, 1 warnings, 7 notices
[RESULT] Suspicious objects detected!
[RESULT] Loki recommends a deeper analysis of the suspicious objects.
[INFO] Please report false positives via https://github.com/Neo23x0/signature-base
[NOTICE] Finished LOKI Scan SYSTEM: thm-yara TIME: 20230606T16:17:34Z

```

What Yara rule did it match on?

webshell_metasoft

What does Loki classify this file as?

Web Shell

```

cmnatic@thm-yara:~/tools/Loki/signature-base/yara$ ls | grep webshell
apt_laudanum_webshells.yar
apt_webshell_chinachopper.yar
cn_pentestset_webshells.yar
gen_cn_webshells.yar
thor-webshells.yar
cmnatic@thm-yara:~/tools/Loki/signature-base/yara$

```

```

rule webshell_metasoft {
    meta:
        description = "Web Shell - file metasoft.php"
        license = "https://creativecommons.org/licenses/by-nc/4.0/"
        author = "Florian Roth"
        date = "2014/01/28"
        score = 70
        hash = "aa328ed1476f4a10c0bcc2dde4461789"

    strings:
        $s7 = "$buff .= \"<tr><td><a href=\\\"?d=\\\". $pwd.\\\"\\\">[ $folder ]</a></td><td>LINK</t"

    condition:
        all of them
}

```

Based on the output, what string within the Yara rule did it match on?

Str1

What is the name and version of this hack tool?

b374k 2.2

Inspect the actual Yara file that flagged file 1. Within this rule, how many strings are there to flag this file?

1

Scan file 2. Does Loki detect this file as suspicious/malicious or benign?

benign

```

    _____
   /_____/_____
  /_____/_____
 /_____/_____
/_____/_____

Copyright by Florian Roth, Released under the GNU General Public License
Version 0.32.1

DISCLAIMER - USE AT YOUR OWN RISK
Please report false positives via https://github.com/Neo23x0/Loki/issues


[NOTICE] Starting Loki Scan VERSION: 0.32.1 SYSTEM: thm-yara TIME: 20230606T17:00:23Z PLATFORM: PROC: x86_64 ARCH: 64bit
[NOTICE] Registered plugin PluginWMI
[NOTICE] Loaded plugin /home/cmnatic/tools/Loki/plugins/loki-plugin-wmi.py
[NOTICE] PE-Sieve successfully initialized BINARY: /home/cmnatic/tools/Loki/tools/pe-sieve64.exe SOURCE: https://github.com/hasherezade/pe-sieve
[INFO] File Name Characteristics initialized with 2841 regex patterns
[INFO] C2 server indicators initialized with 1541 elements
[INFO] Malicious MD5 Hashes initialized with 19034 hashes
[INFO] Malicious SHA1 Hashes initialized with 7159 hashes
[INFO] Malicious SHA256 Hashes initialized with 22841 hashes
[INFO] False Positive Hashes initialized with 30 hashes
[INFO] Processing YARA rules folder /home/cmnatic/tools/Loki/signature-base/yara
[INFO] Initializing all YARA rules at once (composed string of all rule files)
[INFO] Initialized 653 Yara rules
[INFO] Reading private rules from binary ...
[NOTICE] Program should be run as 'root' to ensure all access rights to process memory and file objects.
[NOTICE] Running plugin PluginWMI
[NOTICE] Finished running plugin PluginWMI
[INFO] Scanning ...
[NOTICE] Results: 0 alerts, 0 warnings, 7 notices
[RESULT] SYSTEM SEEMS TO BE CLEAN.
[INFO] Please report false positives via https://github.com/Neo23x0/signature-base
[NOTICE] Finished LOKI Scan SYSTEM: thm-yara TIME: 20230606T17:00:26Z

Press Enter to exit ...

```

Inspect file 2. What is the name and version of this web shell?

b374k 3.2.3

```
cmnatic@thm-yara:~/suspicious-files/file2$ ls
Index.php  loki_thm-yara_2023-06-06_17-00-23.log
cmnatic@thm-yara:~/suspicious-files/file2$
```

```
GNU nano 2.9.3                                     Index.php
$?php
/*
    b374k shell 3.2.3
    Jayalah Indonesiaku
    (c)2014
    https://github.com/b374k/b374k
*/

$GLOBALS['pass'] = "fb621f5060b9f65acf8eb4232e3024140dea2b34"; // sha1(md5(pass))
$GLOBALS['module to load'] = array("explorer", "terminal", "eval", "convert", "database")
```

Creating Yara rules with yarGen (Task 9)

To run yarGen :

```
cmnatic@thm-yara:~/tools/yarGen$ python3 yarGen.py -m /home/cmnatic/suspicious-files/file2 --excludegood -o /home/cmnatic/suspicious-files/file2.yar
-----
  _____
 /  _  _  \  /  _  \  /  _  \  /  _  \  /  _  \  /  _  \  /  _  \  /  _  \
/_  _/_  _/_  _/_  _/_  _/_  _/_  _/_  _/_  _/_  _/_  _/_  _/_  _/_  _/_
  Yara Rule Generator
  Florian Roth, July 2020, Version 0.23.3
-----

Note: Rules have to be post-processed
See this post for details: https://medium.com/@cyb3rops/121d29322282
-----
[+] Using identifier 'file2'
[+] Using reference 'https://github.com/Neo23x0/yarGen'
[+] Using prefix 'file2'
[+] Processing PEStudio strings ...
[+] Reading goodware strings from database 'good-strings.db' ...
    (This could take some time and uses several Gigabytes of RAM depending on your db size)
[+] Loading ./dbs/good-imphashes-part9.db ...
[+] Total: 1 / Added 1 entries

[+] Total: 404321 / Added 22840 entries
[+] Loading ./dbs/good-imphashes-part8.db ...
[+] Total: 17388 / Added 183 entries
[+] Loading ./dbs/good-imphashes-part4.db ...
[+] Total: 19764 / Added 2376 entries
[+] Loading ./dbs/good-strings-part7.db ...
[+] Total: 12284943 / Added 851561 entries
[+] Processing malware files ...
[+] Processing /home/cmnatic/suspicious-files/file2/1index.php ...
[+] Processing /home/cmnatic/suspicious-files/file2/loki_thm-yara_2023-06-06_17-00-23.log ...
[+] Generating statistical data ...
[+] Generating Super Rules ... (a lot of foo magic)
[+] Generating Simple Rules ...
[-] Applying intelligent filters to string findings ...
[-] Filtering string set for /home/cmnatic/suspicious-files/file2/1index.php ...
[-] Filtering string set for /home/cmnatic/suspicious-files/file2/loki_thm-yara_2023-06-06_17-00-23.log ...
[+] Generating Super Rules ...
[+] Generated 2 SIMPLE rules.
[+] Generated 0 SUPER rules.
[+] All rules written to /home/cmnatic/suspicious-files/file2.yar
[+] yarGen run finished
cmnatic@thm-yara:~/tools/yarGen$
```

From within the root of the suspicious files directory, what command would you run to test Yara and your Yara rule against file 2?

```
yara files2.yar file2/1index.php
```

Did Yara rule flag file 2?

Yay

```
cmnatic@thm-yara:~/suspicious-files$ yara file2.yar file2/1index.php
_home_cmnatic_suspicious_files_file2_index file2/1index.php
cmnatic@thm-yara:~/suspicious-files$
```

Copy the Yara rule you created into the Loki signatures directory

```
cp file2.yar ~/tools/Loki/signature-base/yara
cmnatic@thm-yara:~/suspicious-files$ cp file2.yar ~/tools/Loki/signature-base/yara
cmnatic@thm-yara:~/suspicious-files$ cd ~
cmnatic@thm-yara:~$ cd tools
```

Test the Yara rule with Loki, does it flag file 2? (Yay/Nay)

Yay

```
cmnatic@thm-yara:~/tools/Loki$ python loki.py -p ~/suspicious-files/file2

  L O K I
  _ _ _ _

Copyright by Florian Roth, Released under the GNU General Public License
Version 0.32.1

DISCLAIMER - USE AT YOUR OWN RISK
Please report false positives via https://github.com/Neo23x0/Loki/issues

[NOTICE] Starting Loki Scan VERSION: 0.32.1 SYSTEM: thm-yara TIME: 20230613T17:40:12Z PLATFORM: PROC: x86_64 ARCH: 64bit
[NOTICE] Registered plugin PluginWMI
[NOTICE] Loaded plugin /home/cmnatic/tools/Loki/plugins/loki-plugin-wmi.py
[NOTICE] PE-Sieve successfully initialized BINARY: /home/cmnatic/tools/Loki/tools/pe-sieve64.exe SOURCE: https://github.com/hasherezade/pe-sieve
[INFO] File Name Characteristics initialized with 2841 regex patterns
[INFO] C2 server indicators initialized with 1541 elements

[NOTICE] Starting Loki Scan VERSION: 0.32.1 SYSTEM: thm-yara TIME: 20230613T17:40:12Z PLATFORM: PROC: x86_64 ARCH: 64bit
[NOTICE] Registered plugin PluginWMI
[NOTICE] Loaded plugin /home/cmnatic/tools/Loki/plugins/loki-plugin-wmi.py
[NOTICE] PE-Sieve successfully initialized BINARY: /home/cmnatic/tools/Loki/tools/pe-sieve64.exe SOURCE: https://github.com/hasherezade/pe-sieve
[INFO] File Name Characteristics initialized with 2841 regex patterns
[INFO] C2 server indicators initialized with 1541 elements
[INFO] Malicious MD5 Hashes initialized with 19034 hashes
[INFO] Malicious SHA1 Hashes initialized with 7159 hashes
[INFO] Malicious SHA256 Hashes initialized with 22841 hashes
[INFO] False Positive Hashes initialized with 30 hashes
[INFO] Processing YARA rules folder /home/cmnatic/tools/Loki/signature-base/yara
[INFO] Initializing all YARA rules at once (composed string of all rule files)
[INFO] Initialized 654 Yara rules
[INFO] Reading private rules from binary ...
[NOTICE] Program should be run as 'root' to ensure all access rights to process memory and file objects.
[NOTICE] Running plugin PluginWMI
[NOTICE] Finished running plugin PluginWMI
[INFO] Scanning /home/cmnatic/suspicious-files/file2 ...
[WARNING]
FILE: /home/cmnatic/suspicious-files/file2/index.php SCORE: 70 TYPE: PHP SIZE: 223978
FIRST BYTES: 3c3f7068700a2f2a0a09623337346b207368656c / <?php/*b374k shel
MD5: c6a7ebafdbec239d65248e2b69b670157
SHA1: 3926ab64dcf04e87024011cf39902beac32711da
SHA256: 53fe44b4753874f079a936325d1fdc9b1691956a29c3aaf8643cddb49f5984bf CREATED: Mon Nov 9 15:16:03 2020 MODIFIED: Mon Nov 9 13:09:18 2020 ACCESSED: Tue Ju
n 13 17:06:54 2023
REASON 1: Yara Rule MATCH: home cmnatic suspicious files file2 index SUBSCORE: 70
DESCRIPTION: file2 - file index.php REF: https://github.com/Neo23x0/yarGen
MATCHES: Str1: var Zepto=function(){function G(a){return a==null?String(a):z[A.call(a)]|["object"]}function H(a){return G(a)==="function"}fun Str2: re ... (trun
cated)
[NOTICE] Results: 0 alerts, 1 warnings, 7 notices
[RESULT] Suspicious objects detected!
[RESULT] Loki recommends a deeper analysis of the suspicious objects.
[INFO] Please report false positives via https://github.com/Neo23x0/signature-base
[NOTICE] Finished LOKI Scan SYSTEM: thm-yara TIME: 20230613T17:40:18Z
```

What is the name of the variable for the string that it matched on?

Zepto

Inspect the Yara rule, how many strings were generated?

20

```


/* Rule Set ----- */
rule_home_cmnnatic_suspicious_files_file2_index {
  meta:
    description = "file2 - file index.php"
    author = "yarGen Rule Generator"
    reference = "https://github.com/Neo23x0/yarGen"
    date = "2023-06-13"
    hash1 = "53fe44b4753874f079a936325d1fdc9b1691956a29c3aaf8643cddb49f5984bf"
  strings:
    $s1 = "var Zepto=function(){function G(a){return a==null?String(a):z[A.call(a)]||\"object\"}function H(a){return G(a)==\"function\"}fun" ascii
    $s2 = "return (res = new RegExp('(?:^|; )' + encodeURIComponent(key) + '=[^;]*').exec(document.cookie)) ? (res[1]) : null;" fullword ascii
    $s3 = "$cmd = trim(execute(\"ps -p \". $pid));" fullword ascii
    $s4 = "$cmd = execute(\"taskkill /F /PID \". $pid);" fullword ascii
    $s5 = "$buff = execute(\"wget \". $url.\" -O \". $saveas);" fullword ascii
    $s6 = "(d=\"0\"+d);dt2=y+m+d;return dt1==dt2?dt1<dt2?-1:1);r:function(a,b){for(var c=0,e=a.length-1,g=h;g;){for(var g=j,f=c;f<e;++f)0" ascii
    $s7 = "$buff = execute(\"curl \". $url.\" -o \". $saveas);" fullword ascii
    $s8 = "$cmd = execute(\"tasklist /FI \". $pid eq \". $pid.\" \". $pid);" fullword ascii
    $s9 = "$cmd = execute(\"kill -9 \". $pid);" fullword ascii
    $s10 = "execute(\"tar xzf \". $archive.\" \". $target.\" -C \". $target);" fullword ascii
    $s11 = "execute(\"tar xzf \". $archive.\" \". $target.\" -C \". $target);" fullword ascii
    $s12 = "$body = preg_replace(\"/<a href=\\\"http://\\\"www.zend.com\\\"(.*)</a>/\", \"\", $body);" fullword ascii
    $s13 = "ngs.mimeType|xhr.getResponseHeader(\"content-type\"),result=xhr.responseText;try{dataType=\"script\"?1,eval)(result):dataTyp" ascii
    $s14 = "$check = strtolower(execute(\"node -h\"));" fullword ascii
    $s15 = "$check = strtolower(execute(\"javac -help\"));" fullword ascii
    $s16 = "$check = strtolower(execute(\"python -h\"));" fullword ascii
    $s17 = "$check = strtolower(execute(\"perl -h\"));" fullword ascii
    $s18 = "/* Zepto v1.1.2 - zepto event ajax form ie - zeptojs.com/license */" fullword ascii
    $s19 = "$check = strtolower(execute(\"ruby -h\"));" fullword ascii
    $s20 = "$check = strtolower(execute(\"nodejs -h\"));" fullword ascii
  condition:
    uint16(0) == 0x3f3c and filesize < 700KB and
    1 of ($x*) and 4 of them

```

One of the conditions to match on the Yara rule specifies file size. The file has to be less than what amount?

700kb

Valhalla (Task 10)



currently serving 11634 YARA rules

Query	Keyword, tag, ATT&CK technique, sha256 or rule name	Search
API Key	Your API key or select demo API key	<input type="checkbox"/> JSON <input type="checkbox"/> DEMO <input type="button" value="Get Rules"/>

[Statistics](#)
[API](#)
[Integration](#)
[More Information](#)

Enter the SHA256 hash of file 1 into Valhalla. Is this file attributed to an APT group?

Yay

5479f8cd1375364770df36e5a18262480a8f9d311e8eedb2c2390ecb233852ad

Keyword: 5479f8cd1375364770df36e5a18262480a8f9d311e8eedb2c2390ecb233852ad (Results: 7)


 Query

Search

Type	Rule Name	Description	Date	Reference	Ref	VT	Info
YARA	SUSP_ShellStorm_Shell_Feb23	Detects ShellStorm shells - different short reverse shells	2023-02-04	https://github.com/0bfxgh0st/ShellStorm			
YARA	Webshell_b374k_Jan18_1	Detects hacktool / webshell found in disclosed hack tool set of Chinese APT group	2018-01-10	Internal Research - disclosed toolset web mirror			
YARA	b374k_2_4_poly	Detects Webshell - file b374k-2.4.poly.php	2016-12-09	Webshell Repos			
YARA	b374k_2_3_poly	Detects Webshell - file b374k-2.3.poly.php	2016-12-09	Webshell Repos			
YARA	Operation_Emil_Webshell_b374k	Detects Webshell - file info 2.php	2016-07-25	Operation Emil			
YARA	metasloit	Detects Webshell - rule generated from file metasloit.php	2016-01-11	https://github.com/nikicat/web-malware-collection			
YARA	Webshell_metasloit	Web Shell - file metasloit.php	2014-01-28	-			

Do the same for file 2. What is the name of the first Yara rule to detect file 2?

53fe44b4753874f079a936325d1fdc9b1691956a29c3aaf8643cdbc49f5984bf

Keyword: 53fe44b4753874f079a936325d1fdc9b1691956a29c3aaf8643cdbc49f5984bf (Results: 4)


 Query

Search

Type	Rule Name	Description	Date	Reference	Ref	VT	Info
YARA	WebshellRepo_convert	Detects Webshell - file convert.php	2016-12-09	Webshell Repos			
YARA	Operation_Emil_Webshell_pluginsphp	Detects an Operation Emil Webshell - file plugins.php	2016-07-29	Operation Emil			
YARA	Webshell_b374k_rule1	Detects b374k webshell	2015-10-16	https://github.com/b374k/b374k			
YARA	Webshell_b374k_rule2	Detects b374k webshell	2015-10-16	https://github.com/b374k/b374k			

Examine the information for file 2 from Virus Total (VT). The Yara Signature Match is from what scanner?

THOR APT Scanner



thor



2 years ago

YARA Signature Match - THOR APT Scanner

RULE: webshell_php_by_string_known_webshell

RULE_SET: Livehunt - Webshells1 Indicators

RULE_TYPE: Community

RULE_LINK: https://github.com/Neo23x0/signature-base/search?q=webshell_php_by_strir

DESCRIPTION: Known PHP Webshells which contain unique strings, lousy rule for low ha

RULE_AUTHOR: Arnim Rupp

Detection Timestamp: 2021-04-17 19:41

AV Detection Ratio: 28 / 59

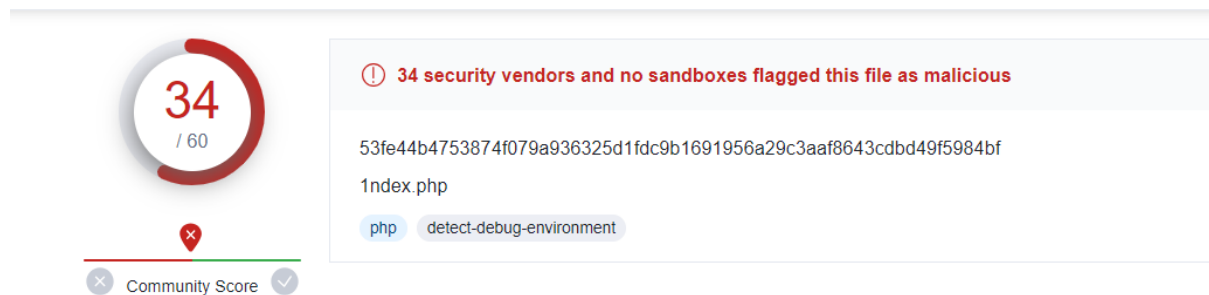
Use these tags to search for similar matches: #webshell #php #known #webshell #livehunt

More information: <https://www.nextron-systems.com/notes-on-virustotal-matches/>

Enter the SHA256 hash of file 2 into Virus Total. Did every AV detect this as malicious?

Nay

53fe44b4753874f079a936325d1fdc9b1691956a29c3aaf8643cddb49f5984bf



Besides .PHP, what other extension is recorded for this file?

.exe




Names ⓘ

1index.php
index2.php
up3.php
b374k-3.2.3.php
3.php
partmgr.sys
f4b3569f68cf9ef1013bc6dc7418077d.txt
c6a7ebafdbe239d65248e2b69b670157.php
file_577.php5
fc9b6386-15bd-11ea-af9f-94f6d6244eb4.php
3926ab64dcf04e87024011cf39902beac32711da.php
001078.php
b374k-3_621.php
ewq1.html
C6A7EBAFDBE239D65248E2B69B670157.exe

^

What JavaScript library is used by file 2?

zepto

YARA	Webshell_b374k_rule1	Detects b374k webshell	2015-10-16	https://github.com/b374k/b374k			
------	----------------------	------------------------	------------	---	---	---	---

```
/* JAVASCRIPT AND CSS FILES START */
$zepto_code = packer_read_file($GLOBALS['packer']['base_dir']."zepto.js");
$js_main_code = "\n\n".packer_read_file($GLOBALS['packer']['base_dir']."main.js");

$js_code = "\n\n".packer_read_file($GLOBALS['packer']['base_dir']."sortable.js").$js_main_code;
$js_code .= "\n\n".packer_read_file($GLOBALS['packer']['base_dir']."base.js");
```