

Detecting Angler in the Wild



Dr. Jared DeMott

SECURITY RESEARCHER AND ENGINEER

@jareddemott www.vdalabs.com



Overview



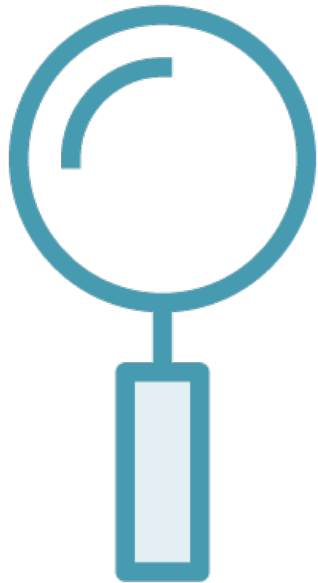
Traffic Examples

Detection

- YARA and friends

Search Rules





How to look?

- Private mode?
 - Watch cookies
- IP address?
 - TOR?

Comments tagged as #angler



#Angler EK from 195.128.125.223

Referer: hxxp://extendoffice.com/

Posted 2 days, 3 hours ago by [anandaherkar](#) <url:f12bb3872af167c8e05ae3ea82f7bab463f306bbb8d0069902fbf0d78868968c>



#Exploitkit

#angler

Posted 2 weeks, 1 day ago by [salawank](#) <url:7e276ad48aaf3a22e04f3d984ed62adaaad043628042762fdb578334be8482a5> [L](#)



#ExploitKit

#Angler



No.	Info	Time
389	GET http://img.ogromnuesosochki.info/megaadvertize/?BVJaGuESzoBulmlRxw=WKRQXeZIVY&aqfHHBuBzZig=zniJVmwdAHR&oiqPJtGGpjqaLR0le=...	220.12
520	GET http://img.ogromnuesosochki.info/favicon.ico HTTP/1.1	221.06
646	POST http://img.ogromnuesosochki.info/megaadvertize/reading/?keyword=11937 HTTP/1.1 (application/x-www-form-urlencoded)	221.09
885	GET http://sound.autodebone.com/boards/viewtopic.php?t=moi&f=b1e2nspnnyz0ktt09z39sn-ln16w5w447ify3xty_a1xsfky9_1h8zi7jzxygtt6...	222.24
1128	GET http://sound.autodebone.com/upon.esproj?pattern=&another=gwdJKt&course=u02&win=Tsjdc&apply=0sqZ-ncen&enemy=hUY5EmdML&ever...	225.77
1171	GET http://sound.autodebone.com/table.muse?lady=cmr&hit=&deal=j6tdTE&in=hSR3UNd1z2&election=xFVX&higher=uIZTJecZo4tfa1AoG5xji...	226.71
1505	GET http://sound.autodebone.com/favicon.ico HTTP/1.1	231.47
1528	GET http://sound.autodebone.com/court.wbs?receive=&strong=h8bMF5&concern=tN3XUgX&why=&faith=gyS6l35Kr&good=&mile=Q-V4IH&cut=o...	235.83
2112	POST http://dustywinslow.com/csys.php HTTP/1.1 (application/x-www-form-urlencoded)	295.72



No.	Info	Time
389	GET http://img.ogromnuesosochki.info/megaadvertize/?BVJaGuESzoBulmlRxw=WKRQXeZIVY&aqfHHBuBzZig=zniJVmwdAHR&oiqPJtGGpjqaLR0le=...	220.12
520	GET http://img.ogromnuesosochki.info/favicon.ico HTTP/1.1	221.06
646	POST http://img.ogromnuesosochki.info/megaadvertize/reading/?keyword=11937 HTTP/1.1 (application/x-www-form-urlencoded)	221.09
885	GET http://sound.autodebone.com/boards/viewtopic.php?t=moi&f=b1e2nspnnyz0ktt09z39sn-ln16w5w447ify3xty_a1xsfky9_1h8zi7jzxygtt6...	222.24
1128	GET http://sound.autodebone.com/upon.esproj?pattern=&another=gwdJKt&course=u02&win=Tsjdc&apply=0sqZ-ncen&enemy=hUY5EmdML&ever...	225.77
1171	GET http://sound.autodebone.com/table.muse?lady=cmr&hit=&deal=j6tdTE&in=hSR3UNd1z2&election=xFVX&higher=uIZTJecZo4tfa1AoG5xji...	226.71
1505	GET http://sound.autodebone.com/favicon.ico HTTP/1.1	231.47
1528	GET http://sound.autodebone.com/court.wbs?receive=&strong=h8bMF5&concern=tN3XUgX&why=&faith=gyS6l35Kr&good=&mile=Q-V4IH&cut=o...	235.83
2112	POST http://dustywinslow.com/csys.php HTTP/1.1 (application/x-www-form-urlencoded)	295.72



Packet	Hostname	Content Type	Size	Filename
3	img.ogromnuesosochki.info	text/html	4060 bytes	?BVJaGuESzoBulmlRxw=WKRQXeZIVY&aqfHHBuBzZig=zniJVmwdAHR&oiqPjtGGpjqaLROle=TxPMsoY
7	img.ogromnuesosochki.info	application/x-www-form-urlencoded	54 bytes	?keyword=11937
24	img.ogromnuesosochki.info	text/html	570 bytes	favicon.ico
28	img.ogromnuesosochki.info	text/html	947 bytes	?keyword=11937
81	sound.autodebone.com	text/html	71 kB	viewtopic.php?t=moi&f=b1e2nspnnyz0ktt09z39sn-lN16w5w447ify3xty_a1xsfky9_1h8zi7jzxygtt6d0nv-2z
109	sound.autodebone.com	application/x-shockwave-flash	65 kB	upon.esproj?pattern=&another=gwdJKt&course=uO2&win=Tsjdc&apply=OsqZ-ncen&enemy=hUY5E
221	sound.autodebone.com	application/octet-stream	376 kB	table.muse?lady=cmr&hit=&deal=j6tdTE&in=hSR3UNd1z2&election=xFVX&higher=uIZTJecZo4tfa1A
223	sound.autodebone.com	text/html	0 bytes	favicon.ico
349	sound.autodebone.com	application/octet-stream	376 kB	court.wbs?receive=&strong=h8bMF5&concern=tN3XUgX&why=&faith=gyS6l35Kr&good=&mile=Q-V
350	dustywinslow.com	application/x-www-form-urlencoded	645 bytes	csys.php
351	dustywinslow.com	text/html	20 bytes	csys.php



MALWARE-TRAFFIC-ANALYSIS.NET



OR

This is an overview of the most popular exploit kits that we have caught in our honeypots in the past few weeks and have tested against [Malwarebytes Anti-Exploit](#).

For those interested in studying or replaying those captures (at your own risk!!), the corresponding Fiddler saz files can be downloaded [here](#) and opened with the usual password.

Angler EK

#	Result	Protocol	Host	URL	Body
1	200	HTTP	cuttlefi.hawaiiinbak.com	/boards/viewforum.php?f=1n0&sid=o6v87x61hi53a030737668m9	152,753
2	200	HTTP	cuttlefi.hawaiiinbak.com	/basic.jsf?unit=&direction=focstFF&require=&county=NSFxp-4&read=&cover=94CZ&...	64,285
3	200	HTTP	cuttlefi.hawaiiinbak.com	/service.web?settle=&foot=TH4JId8Oi&grow=x98w&indicate=kMI-xp4Ms&right=3KU...	389,140
4	200	HTTP	cuttlefi.hawaiiinbak.com	/strength.aspx?social=&audience=aPT411MzSx&month=IOqDzpl&stock=4KvjbmIpm8...	101,449
5	200	HTTP	cuttlefi.hawaiiinbak.com	/every.p7?moral=juma&facility=QKaG4mPs&indicate=rB_ontq6&ago=KTQF_9mC&acro...	389,140
6	200	HTTP	cuttlefi.hawaiiinbak.com	/attend.asax?we=VtBzdbVdjJ&free=Zh53UAHi&themselves=iHJWtHigX&religious=xfy...	389,140

Fiddler Session #1 - http://cuttlefi.hawaiiinbak.com/boards/viewforum.php?f=1n0&sid=o6v87x61hi53a030737668m9

Request

Response

Properties

Headers

TextView

SyntaxView

ImageView

HexView

WebView


Auth

Caching

Cookies

Raw

```
1 <!DOCTYPE html>
2 <html>
3
4 <head>
5
6   <title>
7     you think of nothing but say fine things of "I
8   </title>
9 </head>
10
```

 **Malwarebytes Anti-Exploit has blocked an exploit attempt**

SAZ Files

[Dev](#) » SAZ Files

Background

Session Archive Zip (SAZ) files are used to store HTTP(S) traffic for later examination.

fiddler2pcap

fiddler output to pcap

Example saz file as input `./fiddler2pcap.py -i /home/blah/Downloads/Infinity_2014-03-17.saz -o infinity.pcap --saz`



We have samples, how to
detect?

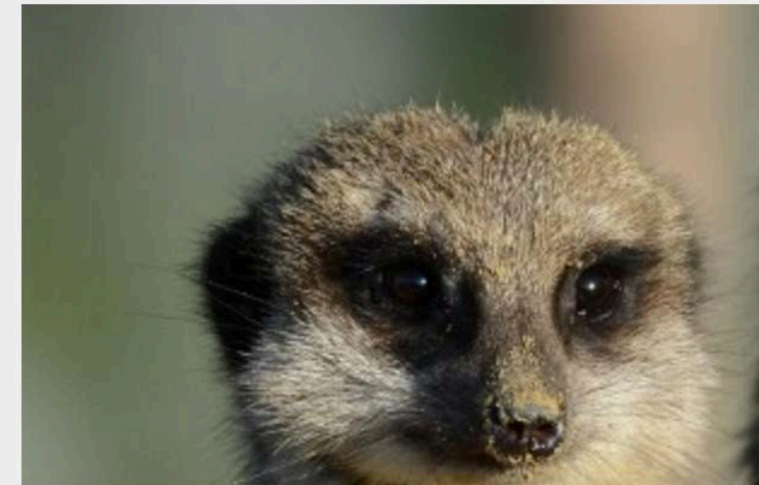
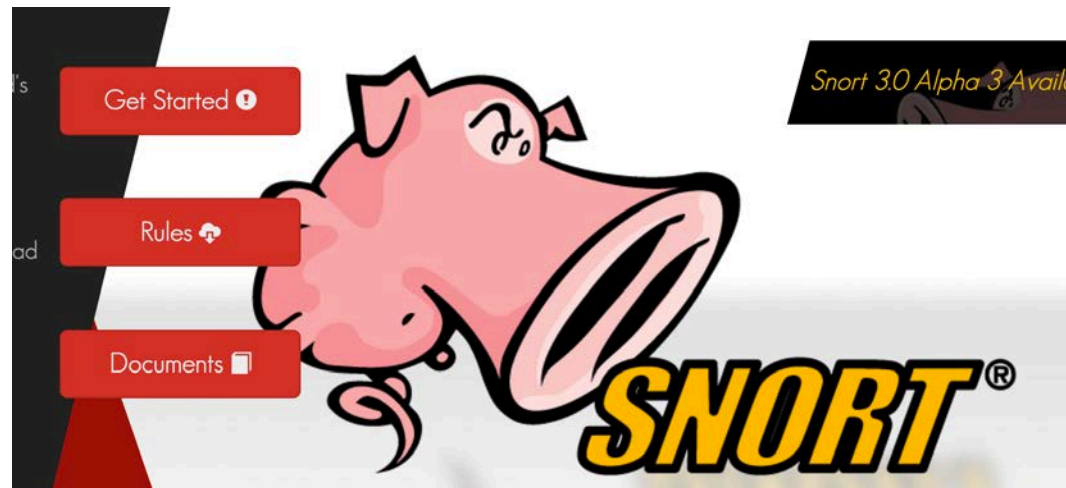


Security nion Solutions

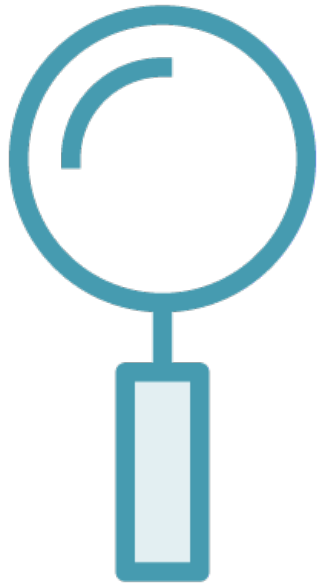
Security Onion Solutions helps you peel back the layers of your network.



The Bro Network Security Monitor



Suricata



Detect Angler

- Redirect
- Landing page
- Exploit
- Payload

regular expressions 101

>_ regex tester

regex library

irc

regex101

SAVE & SHARE

update regex

fork regex

add to regex library

FLAVOR

pcre (php)

javascript

python

TOOLS

format regex (requi...

code generator

regex debugger

unit tests

REGULAR EXPRESSION — version 1 -

1 MATCH - 19 STEPS

/ state: (on|off) / gmixXsuUAJ ?

TEST STRING

hello

how are you?

lkasjdf

what rule will match this line?

state: off

asdf



“YARA is to files what snort
is to network traffic.”

Victor Alvarez, Yara Creator





The pattern matching swiss knife for malware researchers (and everyone else)



```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        thread_level = 3
        in_the_wild = true

    strings:
        $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
        $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
        $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```



Conditions

Conditions are nothing more than Boolean expressions as those that can be found in all programming languages, for example in an *if* statement. They can contain the typical Boolean operators and, or and not and relational operators `>=`, `<=`, `<`, `>`, `==` and `!=`. Also, the arithmetic operators `+`, `-`, `*`, `\`, `%` and bitwise operators `&`, `|`, `<<`, `>>`, `~`, `^` can be used on numerical expressions.

String identifiers can be also used within a condition, acting as Boolean variables whose value depends on the presence or not of the associated string in the file.

```
rule Example
{
    strings:
        $a = "text1"
        $b = "text2"
        $c = "text3"
        $d = "text4"

    condition:
        ($a or $b) and ($c or $d)
}
```

Counting strings

Sometimes we need to know not only if a certain string is present or not, but how many times the



Code

Issues 43

Pull requests 16

Wiki

Pulse

Graphs

The pattern matching swiss knife <http://plusvic.github.io/yara/>

1,231 commits

4 branches

9 releases

33 contributors

Branch: master

New pull request

New file

Upload files

Find file

HTTPS

<https://github.com/plusvi>



Download ZIP

plusvic Put a limit to the number of fibers while executing a regex

Latest commit 510fc3d 3 hours ago

dist	Update RPM spec	9 months ago
docs	Fix typo	27 days ago
extra	Convert logo to vectorial format	3 months ago
libyara	Put a limit to the number of fibers while executing a regex	3 hours ago
m4	Use ACX_PTHREAD macro for configuring PTHREADS	a year ago
tests	Move tests out of libyara	a month ago
windows	Add support for compiling under cygwin.	10 days ago

[yara-3.3.0-win64.zip](#)

February 10, 2015 3:24:49 PST



[yara-3.4.0-win32.zip](#)

June 18, 2015 12:50:03 PDT

[yara-3.4.0-win64.zip](#)

June 18, 2015 6:50:24 PDT

[yara-python-1.7.1.win-amd64-py2.7.exe](#)

November 26, 2013 3:38:08 PST

[yara-python-1.7.1.win-amd64-py3.3.exe](#)

November 26, 2013 3:40:23 PST

[yara-python-1.7.1.win32-py2.7.exe](#)

November 26, 2013 3:36:07 PST

[yara-python-1.7.1.win32-py3.3.exe](#)

November 26, 2013 3:40:05 PST

[yara-python-1.7.2.win-amd64-py2.7.exe](#)

December 04, 2013 8:18:53 PST

[yara-python-1.7.2.win-amd64-py3.3.exe](#)

December 04, 2013 8:18:45 PST



MINGW32:/c/Users/jared/Desktop/yara

jared@WIN-6FA51D049IN /c/Users/jared/Desktop/yara

\$ yara32.exe test.yar test

silent_banker test\test.bin

jared@WIN-6FA51D049IN /c/Users/jared/Desktop/yara

\$



LOKI

Simple IOC Scanner

<C> Florian Roth - BSK Consulting GmbH
Jan 2015
Version 0.3.0

DISCLAIMER - USE AT YOUR OWN RISK


```
[INFO] LOKI - Starting Loki Scan on PROMETHEUS
[INFO] File Name Characteristics initialized with 34 regex patterns
[INFO] File Name Suspicious Characteristics initialized with 51 regex patterns

[INFO] Malware Hashes initialized with 43 hashes
[INFO] False Positive Hashes initialized with 8 hashes
[INFO] Successfully compiled Yara rules from file thor-hacktools.yar
[INFO] Successfully compiled Yara rules from file thor-webshells.yar
[INFO] Successfully compiled Yara rules from file yara_rules.yar
[INFO] Scanning C:\$Recycle.Bin ...
[ALERT] Yara Rule MATCH: Amplia_Security_Tool FILE: C:\$Recycle.Bin\S-1-5-21-949
666807-3097873-177000209-1000\$R04RWGT.zip
[ALERT] Yara Rule MATCH: WindowsCredentialEditor FILE: C:\$Recycle.Bin\S-1-5-21-
949666807-3097873-177000209-1000\$R0WIFVB.raw
[ALERT] Yara Rule MATCH: Amplia_Security_Tool FILE: C:\$Recycle.Bin\S-1-5-21-949
666807-3097873-177000209-1000\$R0WIFVB.raw
[ALERT] Yara Rule MATCH: HackTool_Samples FILE: C:\$Recycle.Bin\S-1-5-21-9496668
07-3097873-177000209-1000\$R0WIFVB.raw
[ALERT] Yara Rule MATCH: HackTool_Producers FILE: C:\$Recycle.Bin\S-1-5-21-94966
6807-3097873-177000209-1000\$R0WIFVB.raw
[ALERT] Yara Rule MATCH: Amplia_Security_Tool FILE: C:\$Recycle.Bin\S-1-5-21-949
666807-3097873-177000209-1000\$R21KENB.zip
[ALERT] Yara Rule MATCH: WindowsCredentialEditor FILE: C:\$Recycle.Bin\S-1-5-21-
949666807-3097873-177000209-1000\$R3BN2BX.raw
```




IDA View-A × simpliFiRE.IDAScope v1.2.1 × Hex View-1 × Structures ×

Semantics Functions WinAPI Crypto YARA



Results for 0 rules loaded from 0 files

Rule Name	Strings Matched	% Matched	Match?
-----------	-----------------	-----------	--------

 No rule selected.

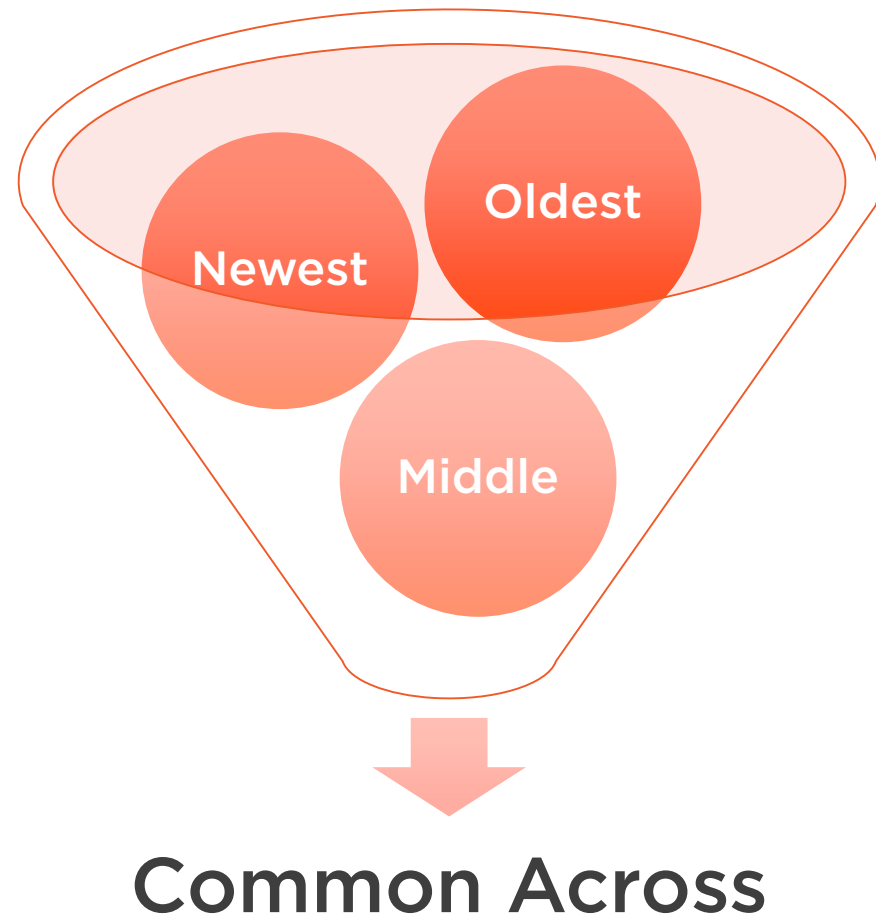
Address / Type	String ID	Value
----------------	-----------	-------



What might an Angler rule
look like?



Data to look for?




```
1 rule mine
2 ▼ {
3 ▼   meta:
4     description = "Detect Angular EK?"
5     author = "Jared DeMott"
6   strings:
7     $a = "malware.dontneedcoffee.com"
8   condition:
9     all of them
10  }
```



```
1 rule AnglerEKredirector072015
2 {
3   meta:
4     description = "Angler Exploit Kit Redirector (July 2015)"
5     ref = "http://blog.xanda.org/2015/08/28/yara-rule-for-angler-ek-redirector-js/"
6     author = "adnan.shukor@gmail.com"
7     impact = "5"
8     version = "1"
9   strings:
10     $ekr1 = "<script>var date = new Date(new Date().getTime() + 60*60*24*7*1000);" fullword
11     $ekr2 = "document.cookie=\"PHP_SESSION_PHP=\""
12     $ekr3 = "path=/; expires=\"+date.toUTCString();</script>" fullword
13     $ekr4 = "<iframe src=\"" fullword
14     $ekr5 = "</iframe></div>" fullword
15   condition:
16     all of them
17 }
```



```
1 rule admedia_js_inject_comment
2 {
3     meta:
4         description = "Detect Admedia Angular EK infected javascript with two identical md5sum comments"
5         reference = "https://blog.sucuri.net/2016/02/massive-admedia-iframe-javascript-infection.html; http://www.malware-
6         traffic-analysis.net/2016/02/15/index.html"
7         author = "James Thompson"
8     strings:
9         $a = /\[/\*[a-f0-9]{32}\*\//
10    condition:
11        for any i in (0..#a):
12            (
13                for all x in (0..8):
14                    (
15                        uint32(@a[i]+(x*4)) == uint32(@a[i+1]+(x*4))
16                    )
17            )
18 }
```



```
# alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"EXPLOIT-KIT Angler exploit kit  
payload download attempt"; flow:to_server,established; urilen:15; content:"/1"; depth:2; fast_pattern;  
http_uri; pcre:"/^\/1[a-z]{0,13}[0-9]{0,12}[a-z][a-z0-9]{1,11}$/U"; content:!"Referer"; http_header;  
content:!"Host|3A| fb.me|OD 0A|"; http_header; metadata:service http; reference:cve,2013-0074;  
reference:cve,2013-0634; reference:cve,2013-3896;  
reference:url,malware.dontneedcoffee.com/2013/10/paunch-arrestationthe-end-of-era.html;  
classtype:trojan-activity; sid:28616; rev:3;)
```

20160203 PCRE:

```
^http:\/\/(?:my[mu][on])[^\x2f]+\/(?!banner)[a-  
z]+\.\php\?s?id=[A-F0-9]{48,}$
```

20151115 PCRE:

^

```
http:\/\/(?:www|forums?)(?:[^\.]+\.[^\.\x2f]+|^[^\.]  
+\.[^\.]+\.(?:[^\.\x2f]+?|^[^\.]+\.[^\.]++))\/[^\x3f]+\/  
(?:index\.\php\?PHPSESSID=[^&]+?&action=(?!dlatt  
ach)[^&]+?&?|view(?:forum|topic)\.\php\?[a-  
z]=[^&]{1,5}&[a-z]{1,3}=(?=[^\n]{0,30}[a-  
z])[^&]{1,31})&?&?&?$
```



Summary



Find more Angler

Create Rules

