FORTINET
High Performance Network Security

FortiSIEM – Fixing Parsers

Prepared by: Rolando Anton – Systems Engineer

Date: 03/10/2017

Table of Contents

1.1 Version History

Version	Date	Revision History	Author
1.0	03/10/2017	First Version	Rolando Antón

2 Introduction

2.1 Issue Identification

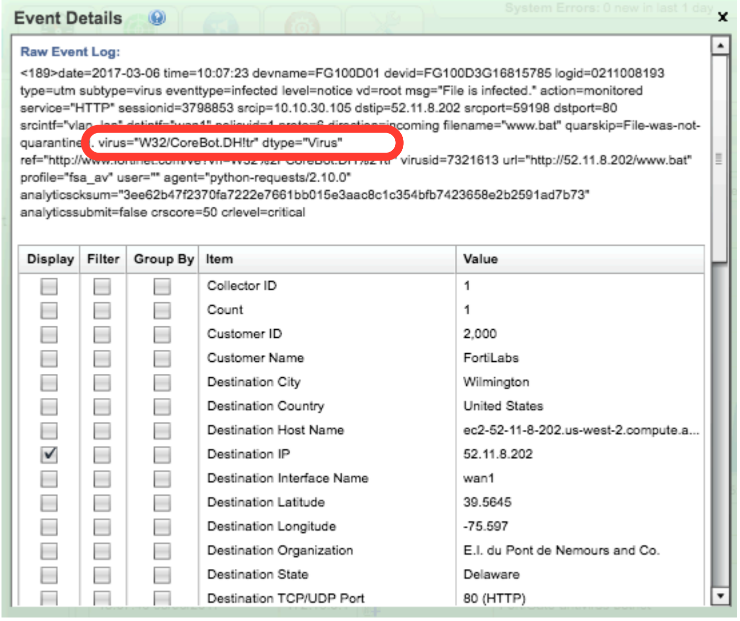
While investigating FortiGate events on the FortiSIEM and trying to create new reports based on the malware name and type found by FortiGate, we were not able to do it. We double check and found that those details are available on the log sent by FortiGate, however this info wasn't identified by the parser. The evidence bellow:

Go to: **Analytics > Historical Search:**

Structured Search:

Event Type = FortiGate-antivirus-infected-file-detect

When we select one of the records matched:



Raw Event Log:

```
<189>date=2017-03-06 time=10:07:23 devname=FG100D01 devid=FG100D3G16815785 logid=0211008193
type=utm subtype=virus eventtype=infected level=notice vd=root msg="File is infected." action=monitored
service="HTTP" sessionid=3798853 srcip=10.10.30.105 dstip=52.11.8.202 srcport=59198 dstport=80
srcintf="vlan_lan" dstintf="wan1" policyid=1 proto=6 direction=incoming filename="www.bat" quarskip=File-was-not-
quarantined. virus="W32/CoreBot.DH!tr" dtype="Virus"
ref="http://www.fortinet.com/ve?vn=W32%2FCoreBot.DH%21tr" virusid=7321613 url="http://52.11.8.202/www.bat"
profile="fsa_av" user="" agent="python-requests/2.10.0"
analyticscksum="3ee62b47f2370fa7222e7661bb015e3aac8c1c354bfb7423658e2b2591ad7b73"
analyticssubmit=false crscore=50 crlevel=critical
```

Display	Filter	Group By	Item	Value
☐	☐	☐	Collector ID	1
☐	☐	☐	Count	1
☐	☐	☐	Customer ID	2,000
☐	☐	☐	Customer Name	FortiLabs
☐	☐	☐	Destination City	Wilmington
☐	☐	☐	Destination Country	United States
☐	☐	☐	Destination Host Name	ec2-52-11-8-202.us-west-2.compute.a...
☑	☐	☐	Destination IP	52.11.8.202
☐	☐	☐	Destination Interface Name	wan1
☐	☐	☐	Destination Latitude	39.5645
☐	☐	☐	Destination Longitude	-75.597
☐	☐	☐	Destination Organization	E.I. du Pont de Nemours and Co.
☐	☐	☐	Destination State	Delaware
☐	☐	☐	Destination TCP/UDP Port	80 (HTTP)

Even when we review all the parsed fields of the event, we can't find a field with the virus name or type as provided by the raw log.

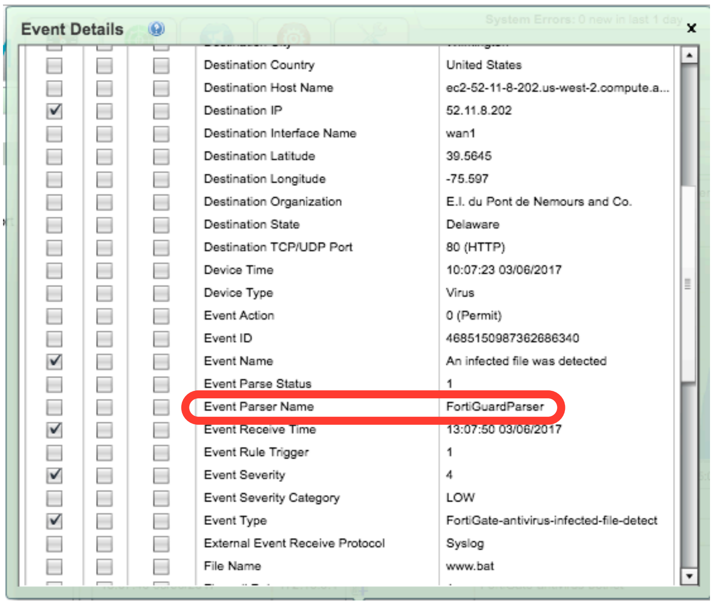
2.2 Impact

Because of this we can't create detailed reports like by example, top malware and with the information of source and destination IP.

3 Solution

3.1 Identify the parser

From the event details if you scroll the details you will find a field related to it labeled as “Event Parser Name”:



Event Details

□	□	□	Destination Country	United States
□	□	□	Destination Host Name	ec2-52-11-8-202.us-west-2.compute.a...
☑	□	□	Destination IP	52.11.8.202
□	□	□	Destination Interface Name	wan1
□	□	□	Destination Latitude	39.5645
□	□	□	Destination Longitude	-75.597
□	□	□	Destination Organization	E.I. du Pont de Nemours and Co.
□	□	□	Destination State	Delaware
□	□	□	Destination TCP/UDP Port	80 (HTTP)
□	□	□	Device Time	10:07:23 03/06/2017
□	□	□	Device Type	Virus
□	□	□	Event Action	0 (Permit)
□	□	□	Event ID	4685150987362686340
☑	□	□	Event Name	An infected file was detected
□	□	□	Event Parse Status	1
□	□	□	Event Parser Name	FortiGuardParser
☑	□	□	Event Receive Time	13:07:50 03/06/2017
□	□	□	Event Rule Trigger	1
☑	□	□	Event Severity	4
□	□	□	Event Severity Category	LOW
☑	□	□	Event Type	FortiGate-antivirus-infected-file-detect
□	□	□	External Event Receive Protocol	Syslog
□	□	□	File Name	www.bat

We are going to also keep a copy of the raw event:

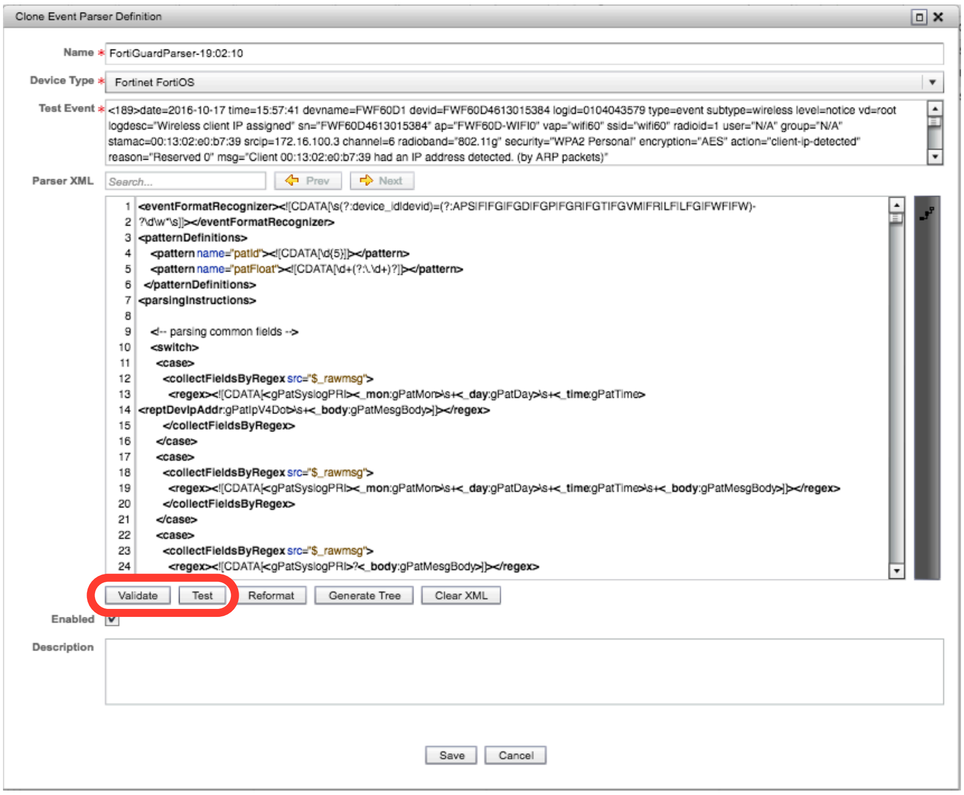
```
<189>date=2017-03-06 time=10:07:23 devname=FG100D01 devid=FG100D3G16815785
logid=0211008193 type=utm subtype=virus eventtype=infected level=notice vd=root msg="File is infected."
action=monitored service="HTTP" sessionid=3798853 srcip=10.10.30.105 dstip=52.11.8.202
srcport=59198 dstport=80 srcintf="vlan_lan" dstintf="wan1" policyid=1 proto=6 direction=incoming
filename="www.bat" quarskip=File-was-not-quarantined. virus="W32/CoreBot.DH!tr" dtype="Virus"
ref="http://www.fortinet.com/ve?vn=W32%2FCoreBot.DH%21tr" virusid=7321613
url="http://52.11.8.202/www.bat" profile="fsa_av" user="" agent="python-requests/2.10.0"
analyticscksum="3ee62b47f2370fa7222e7661bb015e3aac8c1c354bfb7423658e2b2591ad7b73"
analyticssubmit=false crscore=50 crlevel=critical
```

3.2 Parser Modification

3.2.1 Clone Current Parser

Go to: **Admin > Device Support > Parsers**

Use the find box for find “FortiGuardParser”. Before clone it, we must first disable it, just select the ítem and use the “disable” option, after that selcet the “Clone” option, you will get the following window:



Name * FortiGuardParser-19:02:10

Device Type * Fortinet FortiOS

Test Event * <189>date=2016-10-17 time=15:57:41 devname=FWF60D1 devid=FWF60D4613015384 logid=0104043579 type=event subtype=wireless level=notice vd=root logdesc="Wireless client IP assigned" sn="FWF60D4613015384" ap="FWF60D-WIFI0" vap="wifi60" ssid="wifi60" radioid=1 user="N/A" group="N/A" stamac=00:13:02:e0:b7:39 srcip=172.16.100.3 channel=6 radioband="802.11g" security="WPA2 Personal" encryption="AES" action="client-ip-detected" reason="Reserved 0" msg="Client 00:13:02:e0:b7:39 had an IP address detected. (by ARP packets)"

Parser XML

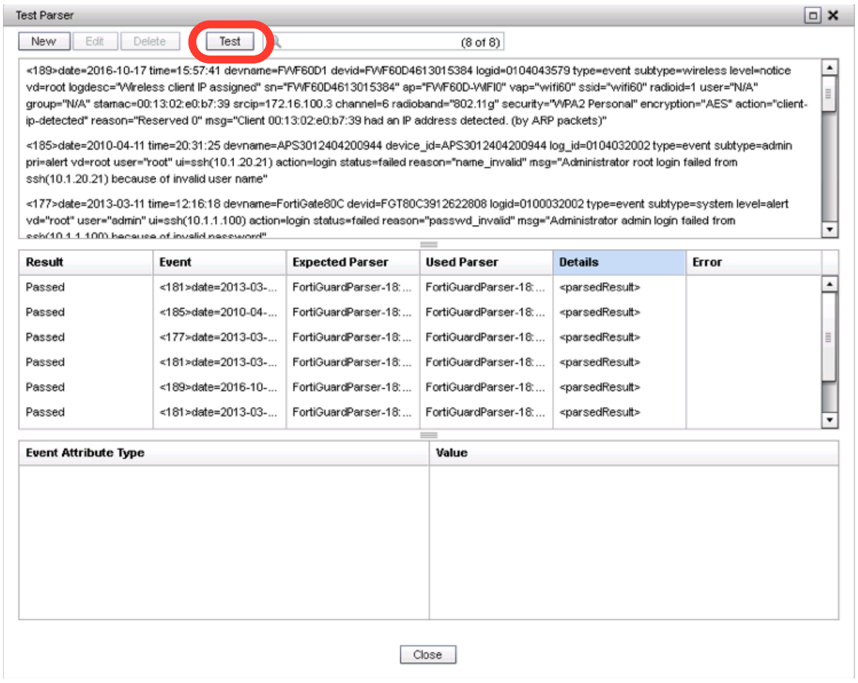
```
<eventFormatRecognizer><![CDATA[\s(?:device_id|devid)=(?:APS|FI|FG|FGD|FGP|FGR|FGT|FGVM|FRL|FL|FG|FWF|FW)-
?\d\w"\s]]></eventFormatRecognizer>
<patternDefinitions>
   <pattern name="patId"><![CDATA[\d{5}]]></pattern>
   <pattern name="patFloat"><![CDATA[\d+(?:\.\d+)?]]></pattern>
 </patternDefinitions>
<parsingInstructions>

   <!-- parsing common fields -->
   <switch>
    <case>
      <collectFieldsByRegex src="$_rawmsg">
       <regex><![CDATA[<gPatSyslogPRI><_mon:gPatMon>\s+<_day:gPatDay>\s+<_time:gPatTime>
<reptDevIpAddr:gPatIpV4Dot>\s+<_body:gPatMesgBody>]]></regex>
      </collectFieldsByRegex>
    </case>
    <case>
      <collectFieldsByRegex src="$_rawmsg">
       <regex><![CDATA[<gPatSyslogPRI><_mon:gPatMon>\s+<_day:gPatDay>\s+<_time:gPatTime>\s+<_body:gPatMesgBody>]]></regex>
      </collectFieldsByRegex>
    </case>
    <case>
      <collectFieldsByRegex src="$_rawmsg">
       <regex><![CDATA[<gPatSyslogPRI>?<_body:gPatMesgBody>]]></regex>
```

Enabled ☑

Description

Before start anything, we are going to save the cloned parser so it can continue working with new events. For do that we must first select the following options:

1. Select the "Validate" option and wait for confirmation that there is no error.
2. Select the "Test" option, and then "Test" again, you will get this window:



<189>date=2016-10-17 time=15:57:41 devname=FWF60D1 devid=FWF60D4613015384 logid=0104043579 type=event subtype=wireless level=notice vd=root logdesc="Wireless client IP assigned" sn="FWF60D4613015384" ap="FWF60D-WIFI0" vap="wifi60" ssid="wifi60" radioid=1 user="N/A" group="N/A" stamac=00:13:02:e0:b7:39 srcip=172.16.100.3 channel=6 radioband="802.11g" security="WPA2 Personal" encryption="AES" action="client-ip-detected" reason="Reserved 0" msg="Client 00:13:02:e0:b7:39 had an IP address detected. (by ARP packets)"

<185>date=2010-04-11 time=20:31:25 devname=APS3012404200944 device_id=APS3012404200944 log_id=0104032002 type=event subtype=admin pri=alert vd=root user="root" ui=ssh(10.1.20.21) action=login status=failed reason="name_invalid" msg="Administrator root login failed from ssh(10.1.20.21) because of invalid user name"

<177>date=2013-03-11 time=12:16:18 devname=FortiGate80C devid=FGT80C3912622808 logid=0100032002 type=event subtype=system level=alert vd="root" user="admin" ui=ssh(10.1.1.100) action=login status=failed reason="passwd_invalid" msg="Administrator admin login failed from ssh(10.1.1.100) because of invalid password"

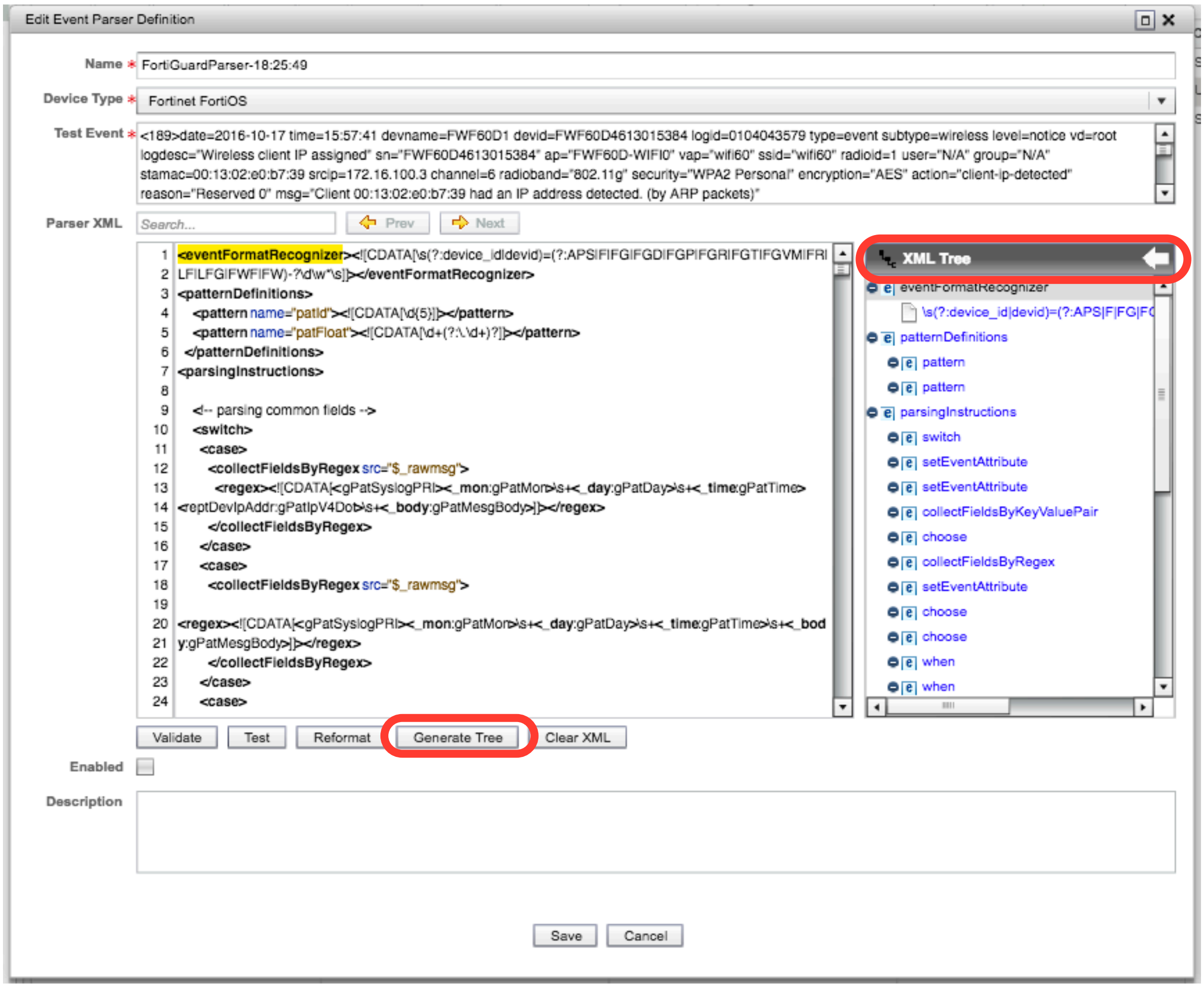
Result	Event	Expected Parser	Used Parser	Details	Error
Passed	<181>date=2013-03-...	FortiGuardParser-18:...	FortiGuardParser-18:...	<parsedResult>	
Passed	<185>date=2010-04-...	FortiGuardParser-18:...	FortiGuardParser-18:...	<parsedResult>	
Passed	<177>date=2013-03-...	FortiGuardParser-18:...	FortiGuardParser-18:...	<parsedResult>	
Passed	<181>date=2013-03-...	FortiGuardParser-18:...	FortiGuardParser-18:...	<parsedResult>	
Passed	<189>date=2016-10-...	FortiGuardParser-18:...	FortiGuardParser-18:...	<parsedResult>	
Passed	<181>date=2013-03-...	FortiGuardParser-18:...	FortiGuardParser-18:...	<parsedResult>	

Event Attribute Type	Value

Once you are back to the Parser Definition window, don’t forget to leave the “Enabled” checkbox selected, then save.

3.2.2 Edit Cloned Parser

Select the new cloned parser, and then select “Edit”. On the right of the XML code there is a grey bar, just click on it for see the “XML Tree”. Now select the option “Generate Tree” and then “Show XML Tree”, you will get this screen:



Name * FortiGuardParser-18:25:49

Device Type * Fortinet FortiOS

Test Event * <189>date=2016-10-17 time=15:57:41 devname=FWF60D1 devid=FWF60D4613015384 logid=0104043579 type=event subtype=wireless level=notice vd=root logdesc="Wireless client IP assigned" sn="FWF60D4613015384" ap="FWF60D-WIFI0" vap="wifi60" ssid="wifi60" radioid=1 user="N/A" group="N/A" stamac=00:13:02:e0:b7:39 srcip=172.16.100.3 channel=6 radioband="802.11g" security="WPA2 Personal" encryption="AES" action="client-ip-detected" reason="Reserved 0" msg="Client 00:13:02:e0:b7:39 had an IP address detected. (by ARP packets)"

Parser XML Search...

```
<eventFormatRecognizer><![CDATA[\s(?:device_id|devid)=(?:APS|F|FG|FGD|FGP|FGR|FGT|FGVM|FR|
LF|LFG|FWF|FW)-?\d\w*\s]]></eventFormatRecognizer>
<patternDefinitions>
   <pattern name="patId"><![CDATA[\d{5}]]></pattern>
   <pattern name="patFloat"><![CDATA[\d+(?:\.\d+)?]]></pattern>
 </patternDefinitions>
<parsingInstructions>

   <!-- parsing common fields -->
   <switch>
     <case>
       <collectFieldsByRegex src="$_rawmsg">
         <regex><![CDATA[<gPatSyslogPRI><_mon:gPatMon>\s+<_day:gPatDay>\s+<_time:gPatTime>
<reptDevIpAddr:gPatIpV4Dot>\s+<_body:gPatMesgBody>]]></regex>
       </collectFieldsByRegex>
     </case>
     <case>
       <collectFieldsByRegex src="$_rawmsg">

<regex><![CDATA[<gPatSyslogPRI><_mon:gPatMon>\s+<_day:gPatDay>\s+<_time:gPatTime>\s+<_bod
y:gPatMesgBody>]]></regex>
       </collectFieldsByRegex>
     </case>
     <case>
```

Enabled □

Description

For understand the structure of the XML is better to reference this document:

https://accelops.atlassian.net/wiki/display/docdev/Event+Parser+XML+Specification

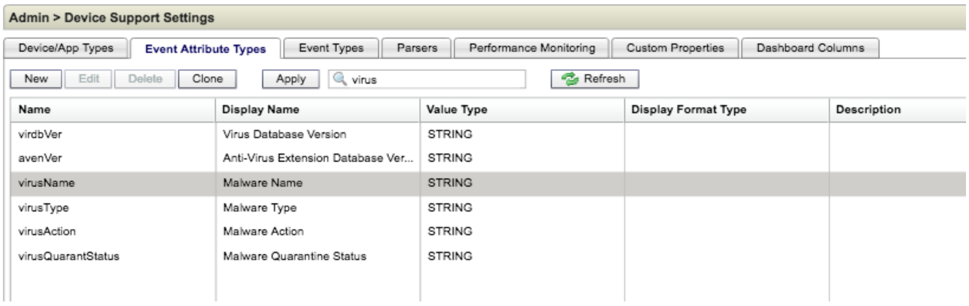
This is also a good read:

https://accelops.atlassian.net/wiki/display/docdev/Creating+a+Custom+Parser

As we are not building a parser from scratch, we need to check if some requirements already exist like:

- Event Types
- Event Attributes Types

Using the keyword “virus” we found that the “Event Attribute Type” already exist:

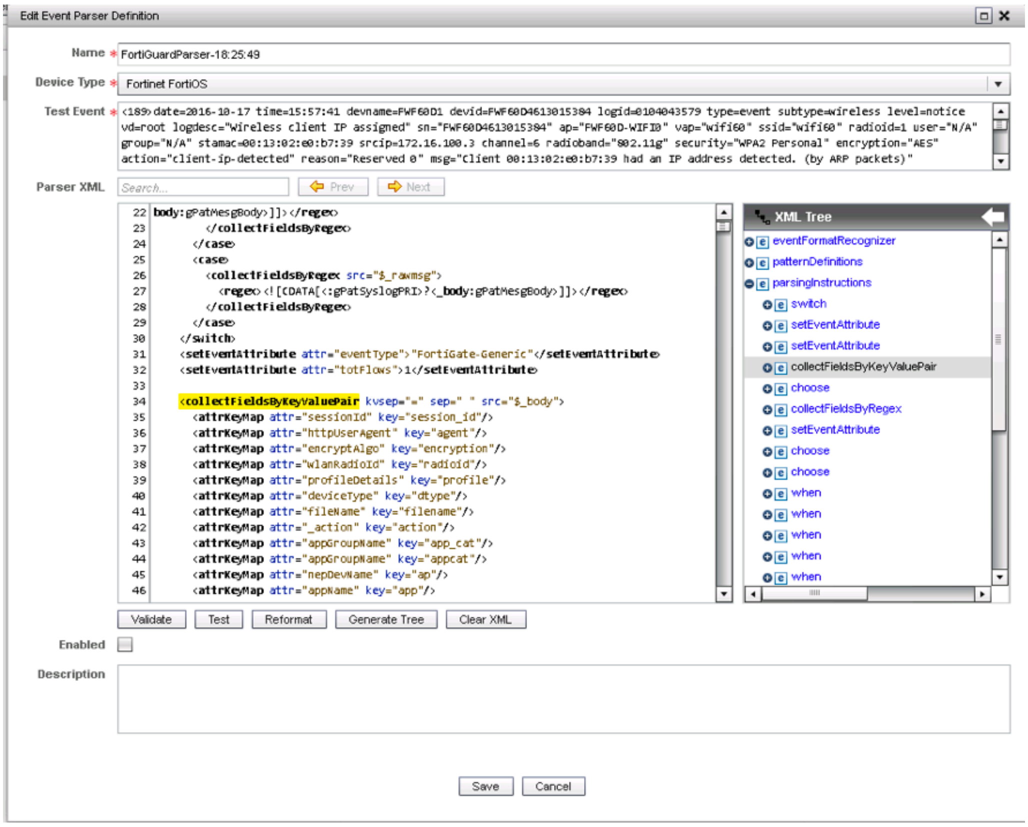


Name	Display Name	Value Type	Display Format Type	Description
virdbVer	Virus Database Version	STRING		
avenVer	Anti-Virus Extension Database Ver...	STRING		
virusName	Malware Name	STRING		
virusType	Malware Type	STRING		
virusAction	Malware Action	STRING		
virusQuarantStatus	Malware Quarantine Status	STRING		

We can define the following info related to the event:

- Event Type:
    - FortiGate-antivirus-infected-file-detect
- Event Attributes Types:
    - virusName
    - virusType

After read and better understand the current parser, we found that the “collectFieldsByKeyValuePair” has a list of the fields processed, and we also found that the virusName and virusType fields doesn’t exist in the list.



Name * FortiGuardParser-18:25:49

Device Type * Fortinet FortiOS

Test Event *

```
<189>date=2016-10-17 time=15:57:41 devname=FWF60D1 devid=FWF60D4613015384 logid=0104043579 type=event subtype=wireless level=notice
vd=root logdesc="Wireless client IP assigned" sn="FWF60D4613015384" ap="FWF60D-WIFI0" vap="wifi60" ssid="wifi60" radioid=1 user="N/A"
group="N/A" stamac=00:13:02:e0:b7:39 srcip=172.16.100.3 channel=6 radioband="802.11g" security="WPA2 Personal" encryption="AES"
action="client-ip-detected" reason="Reserved 0" msg="Client 00:13:02:e0:b7:39 had an IP address detected. (by ARP packets)"
```

```
body:gPatMesgBody>]]></regex>
          </collectFieldsByRegex>
        </case>
        <case>
          <collectFieldsByRegex src="$_rawmsg">
            <regex><![CDATA[<:gPatSyslogPRI>?<_body:gPatMesgBody>]]></regex>
          </collectFieldsByRegex>
        </case>
      </switch>
      <setEventAttribute attr="eventType">"FortiGate-Generic"</setEventAttribute>
      <setEventAttribute attr="totFlows">1</setEventAttribute>

      <collectFieldsByKeyValuePair kvsep="=" sep=" " src="$_body">
        <attrKeyMap attr="sessionId" key="session_id"/>
        <attrKeyMap attr="httpUserAgent" key="agent"/>
        <attrKeyMap attr="encryptAlgo" key="encryption"/>
        <attrKeyMap attr="wlanRadioId" key="radioid"/>
        <attrKeyMap attr="profileDetails" key="profile"/>
        <attrKeyMap attr="deviceType" key="dtype"/>
        <attrKeyMap attr="fileName" key="filename"/>
        <attrKeyMap attr="_action" key="action"/>
        <attrKeyMap attr="appGroupName" key="app_cat"/>
        <attrKeyMap attr="appGroupName" key="appcat"/>
        <attrKeyMap attr="nepDevName" key="ap"/>
        <attrKeyMap attr="appName" key="app"/>
```

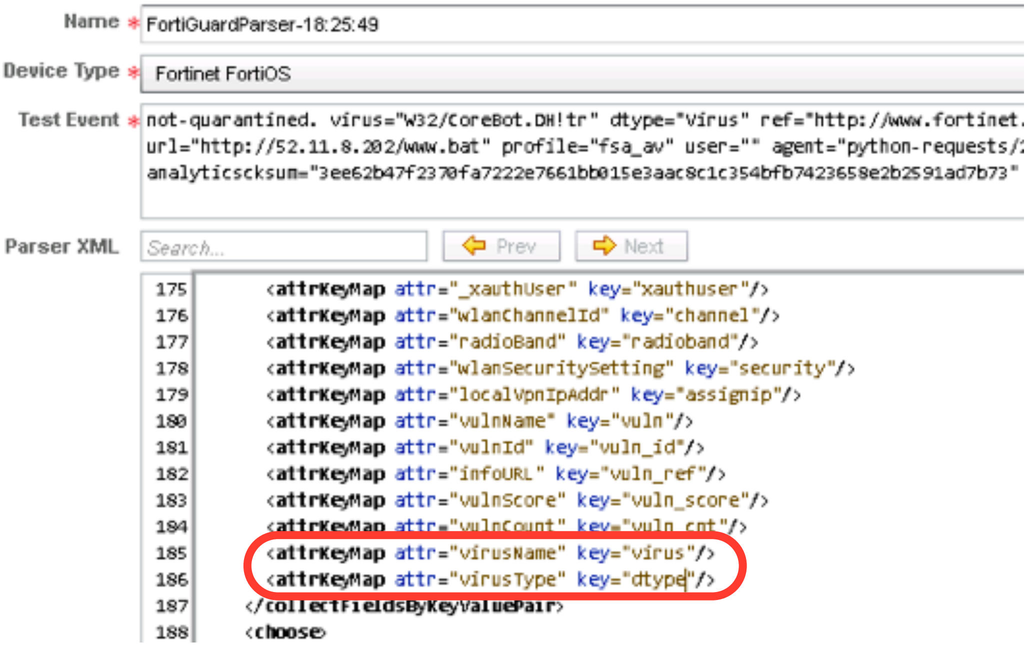
Enabled □

Description

At the end of the section we are going to add the following lines:

```
<attrKeyMap attr="virusName" key="virus"/>
<attrKeyMap attr="virusType" key="dtype"/>
```

It will look like this:



Name * FortiGuardParser-18:25:49

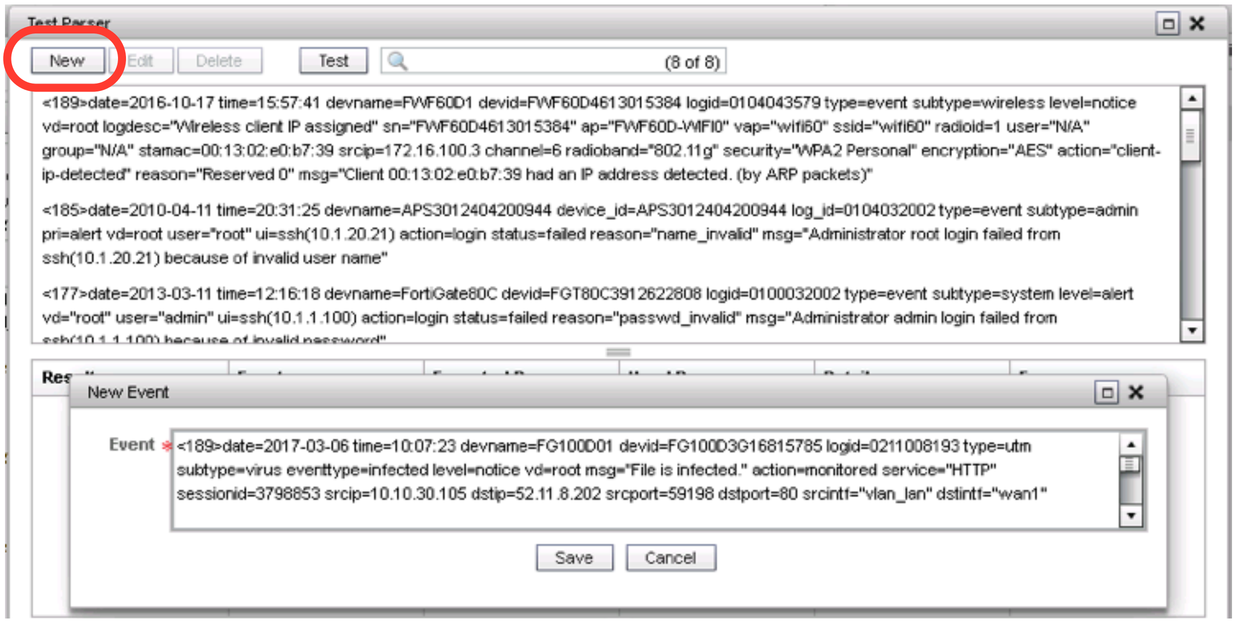
Device Type * Fortinet FortiOS

Test Event *
```
not-quarantined. virus="W32/CoreBot.DH!tr" dtype="Virus" ref="http://www.fortinet.
url="http://52.11.8.202/www.bat" profile="fsa_av" user="" agent="python-requests/2
analyticscksum="3ee62b47f2370fa7222e7661bb015e3aac8c1c354bfb7423658e2b2591ad7b73"
```

```
        <attrKeyMap attr="_xauthUser" key="xauthuser"/>
        <attrKeyMap attr="wlanChannelId" key="channel"/>
        <attrKeyMap attr="radioBand" key="radioband"/>
        <attrKeyMap attr="wlanSecuritySetting" key="security"/>
        <attrKeyMap attr="localVpnIpAddr" key="assignip"/>
        <attrKeyMap attr="vulnName" key="vuln"/>
        <attrKeyMap attr="vulnId" key="vuln_id"/>
        <attrKeyMap attr="infoURL" key="vuln_ref"/>
        <attrKeyMap attr="vulnScore" key="vuln_score"/>
        <attrKeyMap attr="vulnCount" key="vuln_cnt"/>
        <attrKeyMap attr="virusName" key="virus"/>
        <attrKeyMap attr="virusType" key="dtype"/>
      </collectFieldsByKeyValuePair>
      <choose>
```

Now we need to validate and test the parser before use it.

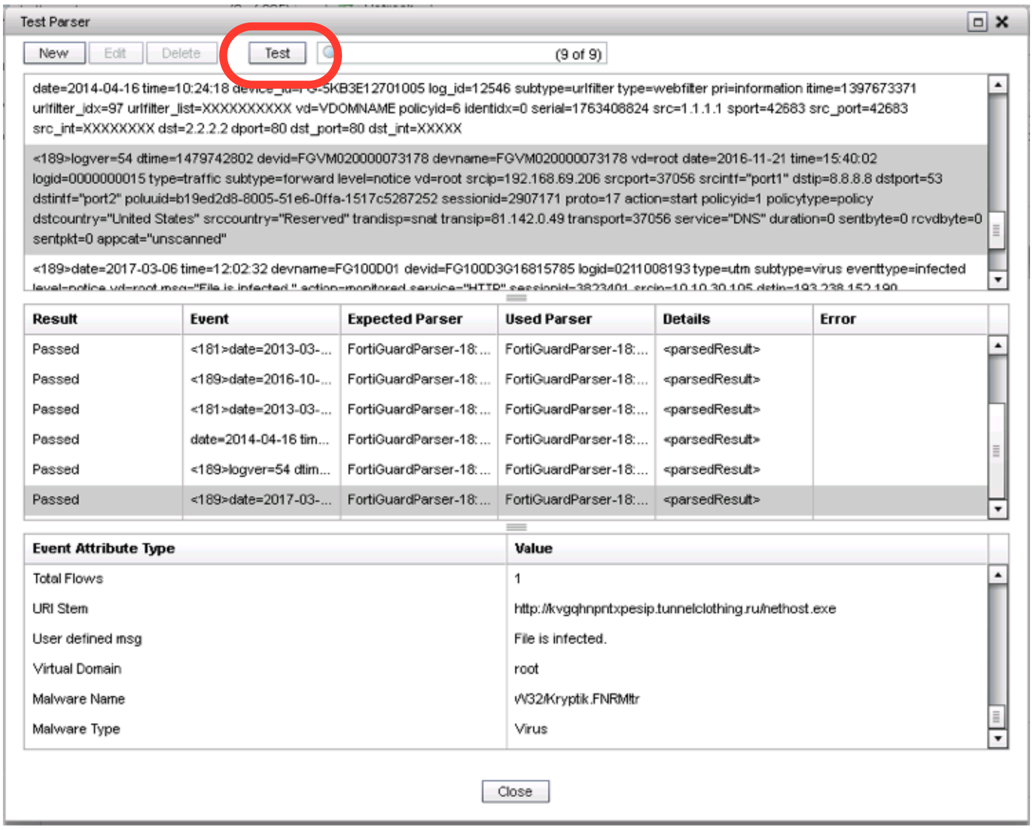
Click on “Test”, and then “New” for add the raw log we previously saved:



```
<189>date=2016-10-17 time=15:57:41 devname=FWF60D1 devid=FWF60D4613015384 logid=0104043579 type=event subtype=wireless level=notice vd=root logdesc="Wireless client IP assigned" sn="FWF60D4613015384" ap="FWF60D-WIFI0" vap="wifi60" ssid="wifi60" radioid=1 user="N/A" group="N/A" stamac=00:13:02:e0:b7:39 srcip=172.16.100.3 channel=6 radioband="802.11g" security="WPA2 Personal" encryption="AES" action="client-ip-detected" reason="Reserved 0" msg="Client 00:13:02:e0:b7:39 had an IP address detected. (by ARP packets)"

<185>date=2010-04-11 time=20:31:25 devname=APS3012404200944 device_id=APS3012404200944 log_id=0104032002 type=event subtype=admin pri=alert vd=root user="root" ui=ssh(10.1.20.21) action=login status=failed reason="name_invalid" msg="Administrator root login failed from ssh(10.1.20.21) because of invalid user name"

<177>date=2013-03-11 time=12:16:18 devname=FortiGate80C devid=FGT80C3912622808 logid=0100032002 type=event subtype=system level=alert vd="root" user="admin" ui=ssh(10.1.1.100) action=login status=failed reason="passwd_invalid" msg="Administrator admin login failed from ssh(10.1.1.100) because of invalid password"
```

Event *
```
<189>date=2017-03-06 time=10:07:23 devname=FG100D01 devid=FG100D3G16815785 logid=0211008193 type=utm subtype=virus eventtype=infected level=notice vd=root msg="File is infected." action=monitored service="HTTP" sessionid=3798853 srcip=10.10.30.105 dstip=52.11.8.202 srcport=59198 dstport=80 srcintf="vlan_lan" dstintf="wan1"
```

After save the log entry for test, we must select “Test” for start the parser validation. If all went ok you should be able to see that the last record which is the one we added manually now is able to identity the virus name and type as show in the following window:

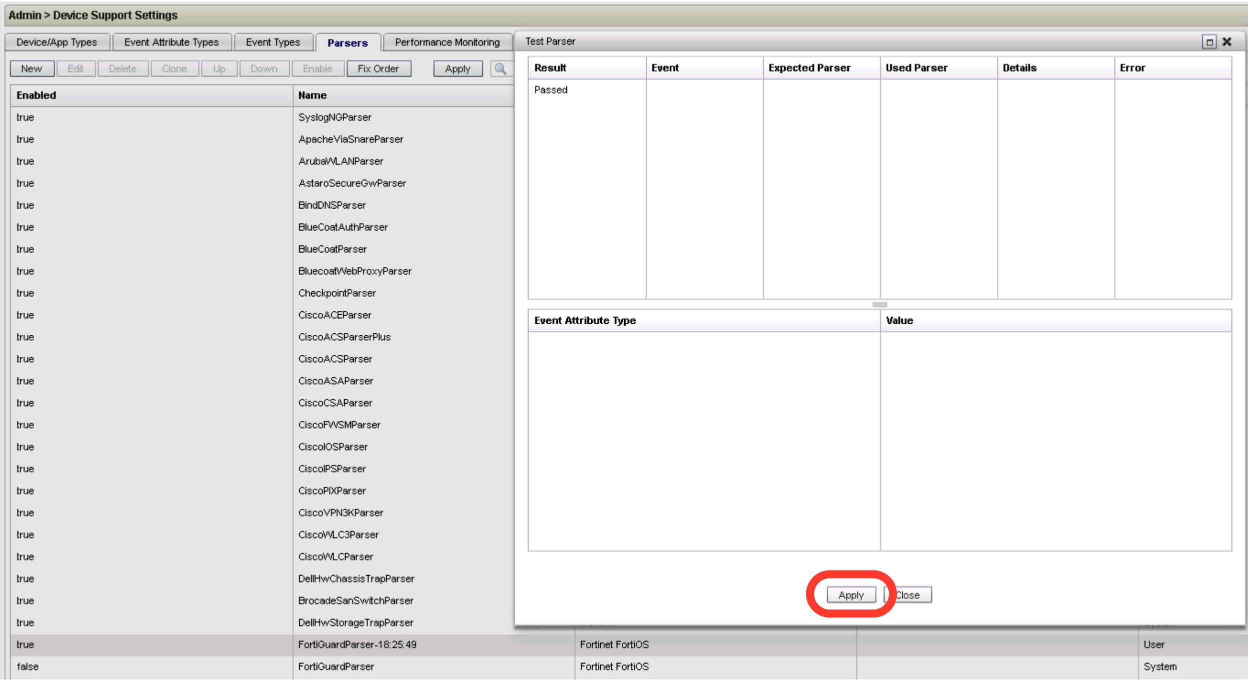


```
date=2014-04-16 time=10:24:18 device_id=FG-5KB3E12701005 log_id=12546 subtype=urlfilter type=webfilter pri=information itime=1397673371
urlfilter_idx=97 urlfilter_list=XXXXXXXXXX vd=VDOMNAME policyid=6 identidx=0 serial=1763408824 src=1.1.1.1 sport=42683 src_port=42683
src_int=XXXXXXXX dst=2.2.2.2 dport=80 dst_port=80 dst_int=XXXXX

<189>logver=54 dtime=1479742802 devid=FGVM020000073178 devname=FGVM020000073178 vd=root date=2016-11-21 time=15:40:02
logid=000000015 type=traffic subtype=forward level=notice vd=root srcip=192.168.69.206 srcport=37056 srcintf="port1" dstip=8.8.8.8 dstport=53
dstintf="port2" poluuid=b19ed2d8-8005-51e6-0ffa-1517c5287252 sessionid=2907171 proto=17 action=start policyid=1 policytype=policy
dstcountry="United States" srccountry="Reserved" trandisp=snat transip=81.142.0.49 transport=37056 service="DNS" duration=0 sentbyte=0 rcvdbyte=0
sentpkt=0 appcat="unscanned"

<189>date=2017-03-06 time=12:02:32 devname=FG100D01 devid=FG100D3G16815785 logid=0211008193 type=utm subtype=virus eventtype=infected
level=notice vd=root msg="File is infected." action=monitored service="HTTP" sessionid=3823401 srcip=10.10.30.105 dstip=193.238.152.190
```

Result	Event	Expected Parser	Used Parser	Details	Error
Passed	<181>date=2013-03-...	FortiGuardParser-18:...	FortiGuardParser-18:...	<parsedResult>	
Passed	<189>date=2016-10-...	FortiGuardParser-18:...	FortiGuardParser-18:...	<parsedResult>	
Passed	<181>date=2013-03-...	FortiGuardParser-18:...	FortiGuardParser-18:...	<parsedResult>	
Passed	date=2014-04-16 tim...	FortiGuardParser-18:...	FortiGuardParser-18:...	<parsedResult>	
Passed	<189>logver=54 dtim...	FortiGuardParser-18:...	FortiGuardParser-18:...	<parsedResult>	
Passed	<189>date=2017-03-...	FortiGuardParser-18:...	FortiGuardParser-18:...	<parsedResult>	

Event Attribute Type	Value
Total Flows	1
URI Stem	http://kvgqhnpntxpesip.tunnelclothing.ru/nethost.exe
User defined msg	File is infected.
Virtual Domain	root
Malware Name	W32/Kryptik.FNRM!tr
Malware Type	Virus

Save it, and don’t forget to click on “Apply” on the Parser panel, that will run an extra test and after confirming the “Passed” result message, we are going to confirm again the “Apply” option.



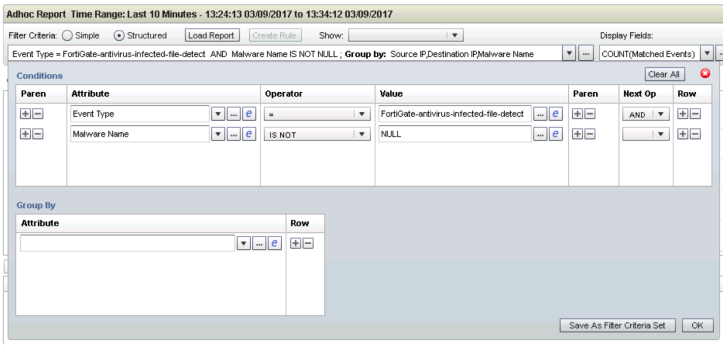
Enabled	Name			
true	SyslogNGParser			
true	ApacheViaSnareParser			
true	ArubaWLANParser			
true	AstaroSecureGwParser			
true	BindDNSParser			
true	BlueCoatAuthParser			
true	BlueCoatParser			
true	BluecoatWebProxyParser			
true	CheckpointParser			
true	CiscoACEParser			
true	CiscoACSParserPlus			
true	CiscoACSParser			
true	CiscoASAParser			
true	CiscoCSAParser			
true	CiscoFWSMParser			
true	CiscoIOSParser			
true	CiscoIPSParser			
true	CiscoPIXParser			
true	CiscoVPN3KParser			
true	CiscoWLC3Parser			
true	CiscoWLCParser			
true	DellHwChassisTrapParser			
true	BrocadeSanSwitchParser			
true	DellHwStorageTrapParser			
true	FortiGuardParser-18:25:49	Fortinet FortiOS		User
false	FortiGuardParser	Fortinet FortiOS		System

Result	Event	Expected Parser	Used Parser	Details	Error
Passed					

Event Attribute Type	Value

3.3 New Parser Validation

Go to: **Analytics > Real-Time Search**, and use the following query:



Adhoc Report Time Range: Last 10 Minutes - 13:24:13 03/09/2017 to 13:34:12 03/09/2017

Filter Criteria: ○ Simple ● Structured

Event Type = FortiGate-antivirus-infected-file-detect AND Malware Name IS NOT NULL ; **Group by:** Source IP,Destination IP,Malware Name

Display Fields: COUNT(Matched Events)

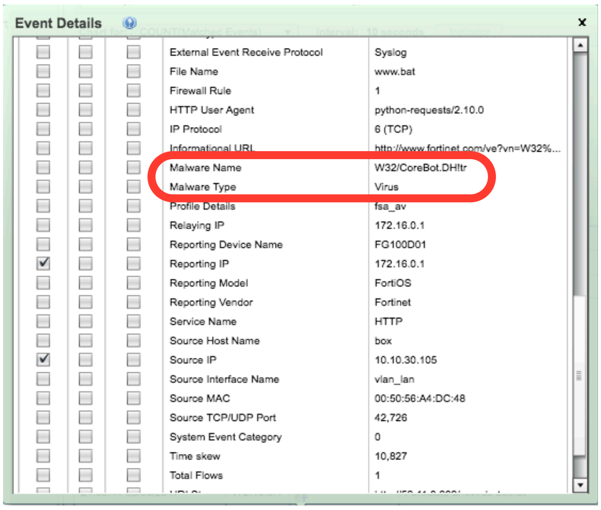
Conditions

Paren	Attribute	Operator	Value	Paren	Next Op	Row
	Event Type	=	FortiGate-antivirus-infected-file-detect		AND	
	Malware Name	IS NOT	NULL			

Group By

Attribute	Row

Then select one of the matched events, you will find that now the Malware Name and Malware fields has the malware details:

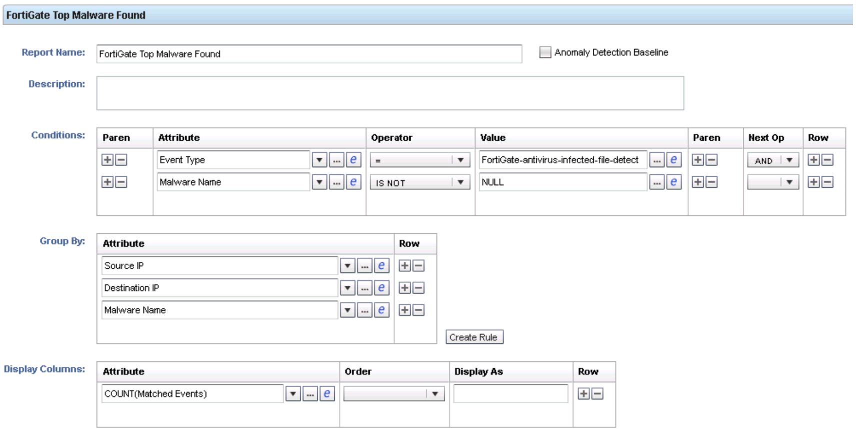


Event Details

☐	☐	☐	External Event Receive Protocol	Syslog
☐	☐	☐	File Name	www.bat
☐	☐	☐	Firewall Rule	1
☐	☐	☐	HTTP User Agent	python-requests/2.10.0
☐	☐	☐	IP Protocol	6 (TCP)
☐	☐	☐	Informational URL	http://www.fortinet.com/ve?vn=W32%...
☐	☐	☐	Malware Name	W32/CoreBot.DH!tr
☐	☐	☐	Malware Type	Virus
☐	☐	☐	Profile Details	fsa_av
☐	☐	☐	Relaying IP	172.16.0.1
☐	☐	☐	Reporting Device Name	FG100D01
☑	☐	☐	Reporting IP	172.16.0.1
☐	☐	☐	Reporting Model	FortiOS
☐	☐	☐	Reporting Vendor	Fortinet
☐	☐	☐	Service Name	HTTP
☐	☐	☐	Source Host Name	box
☑	☐	☐	Source IP	10.10.30.105
☐	☐	☐	Source Interface Name	vlan_lan
☐	☐	☐	Source MAC	00:50:56:A4:DC:48
☐	☐	☐	Source TCP/UDP Port	42,726
☐	☐	☐	System Event Category	0
☐	☐	☐	Time skew	10,827
☐	☐	☐	Total Flows	1

3.3.1 Reports and Dashboards

Now we can create queries like the following example:



FortiGate Top Malware Found

Report Name: FortiGate Top Malware Found ☐ Anomaly Detection Baseline

Description:

Conditions:

Paren	Attribute	Operator	Value	Paren	Next Op	Row
	Event Type	=	FortiGate-antivirus-infected-file-detect		AND	
	Malware Name	IS NOT	NULL			

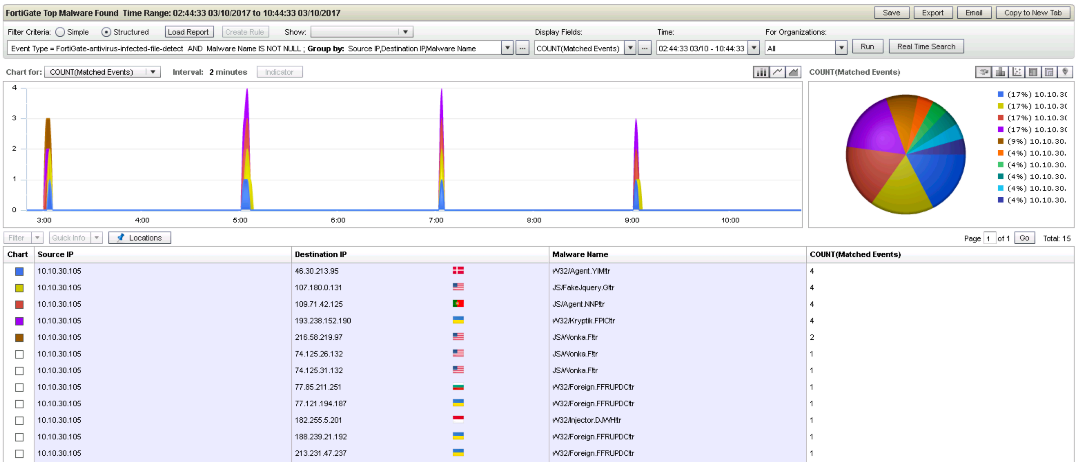
Group By:

Attribute	Row
Source IP	
Destination IP	
Malware Name	

Display Columns:

Attribute	Order	Display As	Row
COUNT(Matched Events)			

After save the report we can execute it and show the result:



FortiGate Top Malware Found Time Range: 02:44:33 03/10/2017 to 10:44:33 03/10/2017

Filter Criteria: ○ Simple ● Structured

Event Type = FortiGate-antivirus-infected-file-detect AND Malware Name IS NOT NULL ; **Group by:** Source IP,Destination IP,Malware Name

Display Fields: COUNT(Matched Events)

Time: 02:44:33 03/10 - 10:44:33

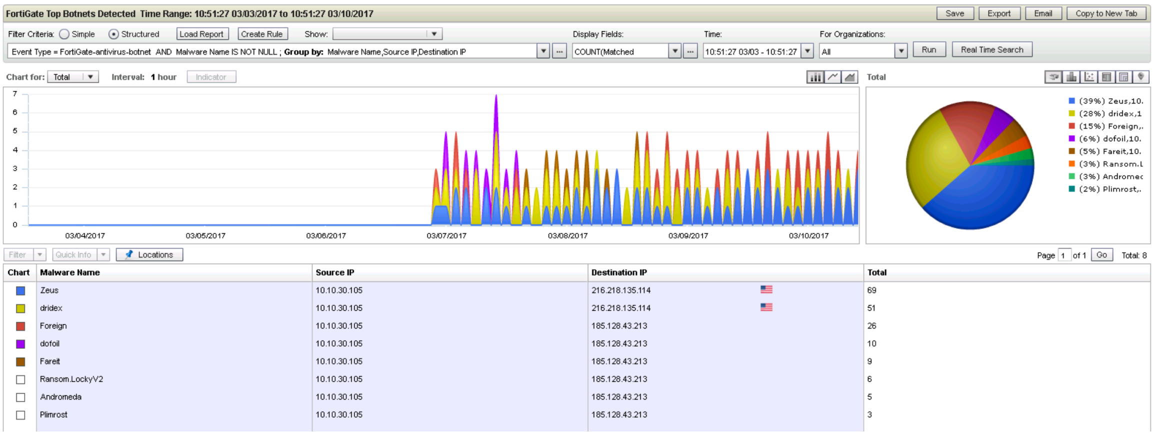
For Organizations: All

Chart for: COUNT(Matched Events)   Interval: 2 minutes

Page 1 of 1   Total: 15

Chart	Source IP	Destination IP	Malware Name	COUNT(Matched Events)
🟦	10.10.30.105	46.30.213.95	W32/Agent.YIMtr	4
🟨	10.10.30.105	107.180.0.131	JS/FakeJquery.Gltr	4
🟥	10.10.30.105	109.71.42.125	JS/Agent.NNPltr	4
🟪	10.10.30.105	193.238.152.190	W32/Kryptik.FPICltr	4
🟫	10.10.30.105	216.58.219.97	JS/Wonka.Fltr	2
□	10.10.30.105	74.125.26.132	JS/Wonka.Fltr	1
□	10.10.30.105	74.125.31.132	JS/Wonka.Fltr	1
□	10.10.30.105	77.85.211.251	W32/Foreign.FFRUPDCltr	1
□	10.10.30.105	77.121.194.187	W32/Foreign.FFRUPDCltr	1
□	10.10.30.105	182.255.5.201	W32/Injector.DJWHltr	1
□	10.10.30.105	188.239.21.192	W32/Foreign.FFRUPDCltr	1
□	10.10.30.105	213.231.47.237	W32/Foreign.FFRUPDCltr	1

The parser correction enabled also to identify other “Event Types” like “FortiGate-Antivirus-Botnet” which will help us to identify botnet connections/callbacks like the following example:



FortiGate Top Botnets Detected Time Range: 10:51:27 03/03/2017 to 10:51:27 03/10/2017

Filter Criteria: ○ Simple ● Structured

Event Type = FortiGate-antivirus-botnet AND Malware Name IS NOT NULL ; **Group by:** Malware Name,Source IP,Destination IP

Display Fields: COUNT(Matched

Time: 10:51:27 03/03 - 10:51:27

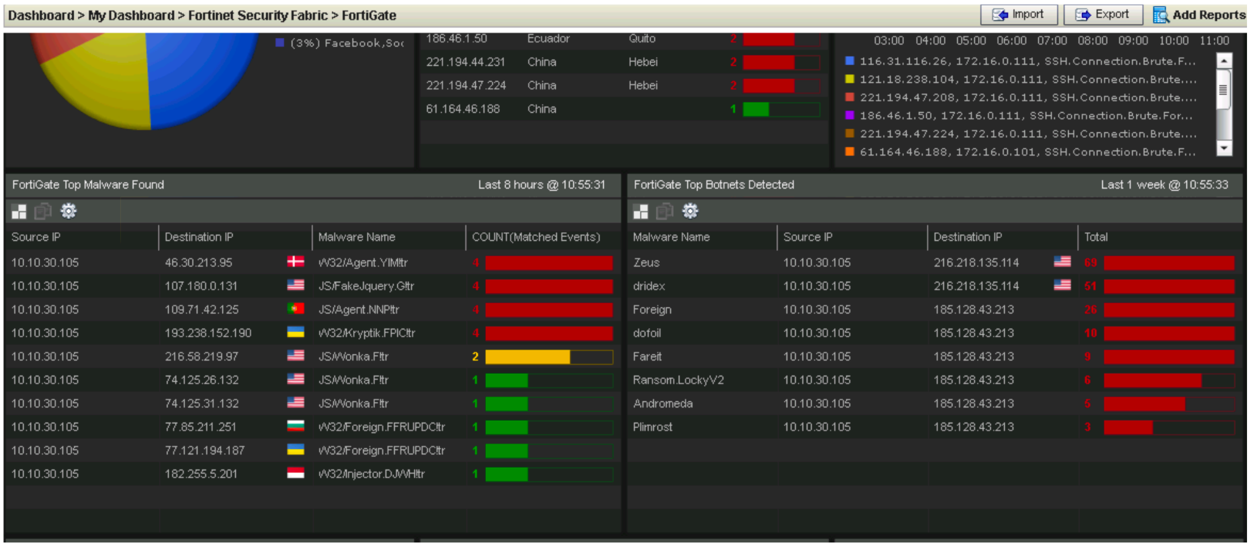
For Organizations: All

Chart for: Total   Interval: 1 hour

Page 1 of 1   Total: 8

Chart	Malware Name	Source IP	Destination IP	Total
🟦	Zeus	10.10.30.105	216.218.135.114	69
🟨	dridex	10.10.30.105	216.218.135.114	51
🟥	Foreign	10.10.30.105	185.128.43.213	26
🟪	dofoil	10.10.30.105	185.128.43.213	10
🟫	Fareit	10.10.30.105	185.128.43.213	9
□	Ransom.LockyV2	10.10.30.105	185.128.43.213	6
□	Andromeda	10.10.30.105	185.128.43.213	5
□	Plimrost	10.10.30.105	185.128.43.213	3

We can also add those reports as widgets to create new Dashboards:



Dashboard > My Dashboard > Fortinet Security Fabric > FortiGate

186.46.1.50	Ecuador	Quito	2
221.194.44.231	China	Hebei	2
221.194.47.224	China	Hebei	2
61.164.46.188	China		1

```
116.31.116.26, 172.16.0.111, SSH.Connection.Brute.F...
121.18.238.104, 172.16.0.111, SSH.Connection.Brute....
221.194.47.208, 172.16.0.111, SSH.Connection.Brute....
186.46.1.50, 172.16.0.111, SSH.Connection.Brute.For...
221.194.47.224, 172.16.0.111, SSH.Connection.Brute....
61.164.46.188, 172.16.0.101, SSH.Connection.Brute.F...
```

FortiGate Top Malware Found   Last 8 hours @ 10:55:31

Source IP	Destination IP	Malware Name	COUNT(Matched Events)
10.10.30.105	46.30.213.95	W32/Agent.YIMltr	4
10.10.30.105	107.180.0.131	JS/FakeJquery.Gltr	4
10.10.30.105	109.71.42.125	JS/Agent.NNPltr	4
10.10.30.105	193.238.152.190	W32/Kryptik.FPICltr	4
10.10.30.105	216.58.219.97	JS/Wonka.Fltr	2
10.10.30.105	74.125.26.132	JS/Wonka.Fltr	1
10.10.30.105	74.125.31.132	JS/Wonka.Fltr	1
10.10.30.105	77.85.211.251	W32/Foreign.FFRUPDCltr	1
10.10.30.105	77.121.194.187	W32/Foreign.FFRUPDCltr	1
10.10.30.105	182.255.5.201	W32/Injector.DJWHltr	1

FortiGate Top Botnets Detected   Last 1 week @ 10:55:33

Malware Name	Source IP	Destination IP	Total
Zeus	10.10.30.105	216.218.135.114	69
dridex	10.10.30.105	216.218.135.114	51
Foreign	10.10.30.105	185.128.43.213	26
dofoil	10.10.30.105	185.128.43.213	10
Fareit	10.10.30.105	185.128.43.213	9
Ransom.LockyV2	10.10.30.105	185.128.43.213	6
Andromeda	10.10.30.105	185.128.43.213	5
Plimrost	10.10.30.105	185.128.43.213	3