

# Home-based Threat Intelligence

written by Mert SARICA | 1 October 2019

Those of you who read my articles will recall that in my post titled “Escape from Imprisonment”, I enthusiastically discussed the advantages of using a router packed with security features. As I mentioned in the article, I had started using the dnscrypt-proxy tool to encrypt DNS traffic (Dns over HTTPS – DoH).

In today’s world where thermostats are getting smarter, smart TVs are equipped with cameras, and electric water heaters and irons are being turned into spy devices, insecure Internet of Things (IoT) devices connected to our home network pose a great risk to our security and privacy. As I was thinking about how to detect systems in our home network that have been hacked, infected, or contain backdoors, I remembered that thanks to the dnscrypt-proxy tool, I could also record DNS requests made by all systems, devices, and gadgets connected to the home network.

At the point where I could record DNS requests, I realized I could detect malicious systems in my home network by querying the domain names and IP addresses found in these DNS requests through cyber threat intelligence services like Open Threat Exchange (OTX) and Critical Stack. Without wasting time, I started thinking about the list of requirements to bring this idea to life.

First, I decided to install the syslog-ng package on the Ubuntu operating system running on my Mini-PC, which is always at hand and always comes to my aid in such situations. After installing the package, I configured it to record incoming DNS requests in the date.log file under the /var/log/dns-sys/sender’s-ip-address directory and saved this configuration in the /etc/syslog-ng/conf.d/dns-sys.conf file.

```

root@ubuntu:/etc/syslog-ng/conf.d# ls
dns-sys.conf
root@ubuntu:/etc/syslog-ng/conf.d# cat dns-sys.conf
#####
options {
    create_dirs(yes);
    perm(0640);
    dir_perm(0750);
};

#####
source s_net {
    tcp(ip(0.0.0.0) port(514));
    udp(ip(0.0.0.0) port(514));
};

#####
destination d_host-specific {
    file("/var/log/dns-sys/$HOST/$DAY-$MONTH-$YEAR.log");
};

filter f_cached { match("cached"); };           # Filter regex keyword cached
filter f_query { match("query"); };             # Filter regex keyword query
filter f_reply { match("reply"); };             # Filter regex keyword reply

log {
    source(s_net);
    filter(f_cached);
    destination(d_host-specific);
};

log {
    source(s_net);
    filter(f_query);
    destination(d_host-specific);
};

log {
    source(s_net);
    filter(f_reply);
    destination(d_host-specific);
};

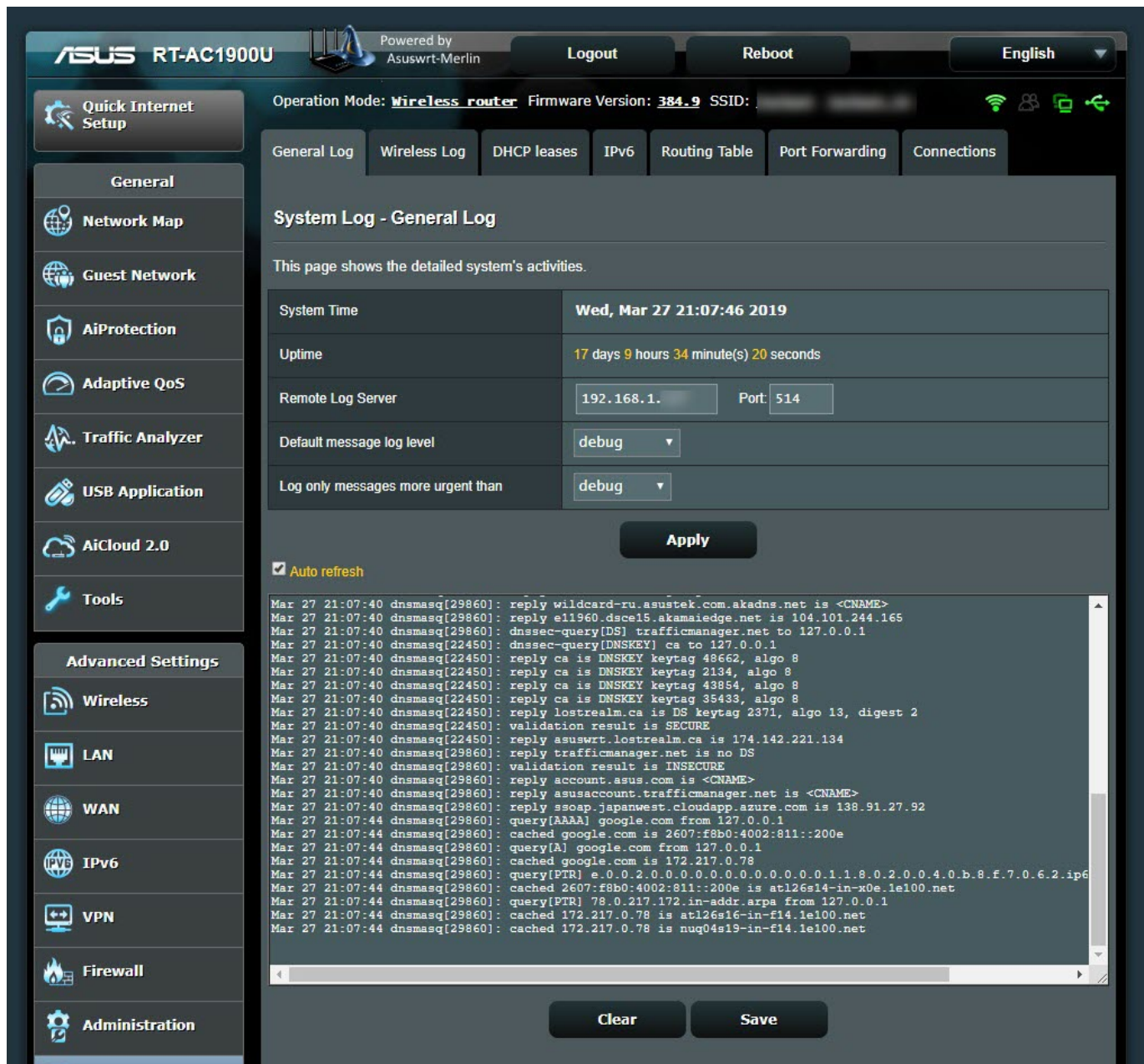
```

In the next step, to make the dnscrypt-proxy tool log DNS requests to the router's syslog, I added the line 'log-queries' to the /jffs/configs/dnsmasq.conf.add file. Then, to make the router display these requests on its syslog page, I set the 'Default message log level' and 'Log only messages more urgent than' values to 'debug', and to redirect these messages to the syslog-ng application running on Ubuntu, I defined the 'Remote Log Server' value as the IP address of Ubuntu.

```

mert@RT-AC1900U-6610:/jffs/configs# cat dnsmasq.conf.add
no-resolv
log-queries
server=127.0.0.1#65053
mert@RT-AC1900U-6610:/jffs/configs# █

```



I started examining the syslog-ng records one by one and looking into which types of records I needed to focus on for threat intelligence. After learning that I could use the query[A], cached, and reply information in the records, I thought I could send these records to Security Onion, which integrates with OTX. After installing and running Security Onion's 16.04.5.6 operating system, I noticed that the logstash service (so-logstash) wasn't working at all. Despite my struggle, I was unsuccessful and started researching alternative methods.

```

root@ubuntu:/etc/syslog-ng/conf.d# tail -n 20 /var/log/dns-sys/192.168.1.1/09-04-2019.log
Apr 9 21:09:25 192.168.1.1 dnsmasq[29860]: reply partnerad.l.doubleclick.net is 74.125.21.156
Apr 9 21:09:25 192.168.1.1 dnsmasq[29860]: reply partnerad.l.doubleclick.net is 74.125.21.157
Apr 9 21:09:25 192.168.1.1 dnsmasq[29860]: reply partnerad.l.doubleclick.net is 74.125.21.154
Apr 9 21:09:25 192.168.1.1 dnsmasq[29860]: reply partnerad.l.doubleclick.net is 74.125.21.155
Apr 9 21:09:25 192.168.1.1 dnsmasq[29860]: query[A] s.w.org from 192.168.1.225
Apr 9 21:09:25 192.168.1.1 dnsmasq[29860]: query[A] widget.engageya.com from 192.168.1.225
Apr 9 21:09:25 192.168.1.1 dnsmasq[29860]: reply s.w.org is 192.0.77.48
Apr 9 21:09:25 192.168.1.1 dnsmasq[29860]: reply widget.engageya.com is <CNAME>
Apr 9 21:09:25 192.168.1.1 dnsmasq[29860]: reply widget-engageya.edgekey.net is <CNAME>
Apr 9 21:09:25 192.168.1.1 dnsmasq[29860]: reply e15247.dscg.akamaiedge.net is 104.96.141.105
Apr 9 21:09:25 192.168.1.1 dnsmasq[29860]: query[A] www.googletagservices.com from 192.168.1.225
Apr 9 21:09:25 192.168.1.1 dnsmasq[29860]: reply www.googletagservices.com is <CNAME>
Apr 9 21:09:25 192.168.1.1 dnsmasq[29860]: reply pagead46.l.doubleclick.net is 172.217.3.226
Apr 9 21:09:27 192.168.1.1 dnsmasq[29860]: query[A] gatr.hit.gemius.pl from 192.168.1.225
Apr 9 21:09:27 192.168.1.1 dnsmasq[29860]: reply gatr.hit.gemius.pl is 5.135.121.144
Apr 9 21:09:27 192.168.1.1 dnsmasq[29860]: reply gatr.hit.gemius.pl is 37.59.195.0
Apr 9 21:09:27 192.168.1.1 dnsmasq[29860]: reply gatr.hit.gemius.pl is 37.187.168.211
Apr 9 21:09:27 192.168.1.1 dnsmasq[29860]: reply gatr.hit.gemius.pl is 149.202.193.219
Apr 9 21:09:27 192.168.1.1 dnsmasq[29860]: reply gatr.hit.gemius.pl is 149.202.204.241
Apr 9 21:09:27 192.168.1.1 dnsmasq[29860]: reply gatr.hit.gemius.pl is 188.165.145.88
root@ubuntu:/etc/syslog-ng/conf.d# cat /var/log/dns-sys/192.168.1.1/08-04-2019.log | cut -d " " -f 7 | sort | uniq -i
cached
dnsssec-query[DNSKEY]
dnsssec-query[DS]
forwarded
query[A]
query[AAAA]
query[PTR]
query[SRV]
reply
root@ubuntu:/etc/syslog-ng/conf.d#

```

When I shared a message on Twitter about needing to install ELK, I received messages suggesting that I could use cloud and ready-made ELK systems. As I was considering whether to install ELK on Ubuntu or use a cloud system, I learned that Logstash, which has Grok filter and Translate filter plugins, was tailor-made for this job.





**Mert SARICA** @MertSARICA · 7 Mar

Yapılacaklar listem kabardıkça kabanyor, eve gidince ELK kurmam lazım. Beni bu kadar çok çalıştıran kendimi, şikayet edecek bir merci bulmam lazım. :)

3



11



**Furkan ÇALIŞKAN**

@caliskanfurkan\_

Takip ediliyor

@MertSARICA adlı kullanıcıya yanıt olarak

[cloud.elastic.co](https://cloud.elastic.co) 14 gün ücretsiz hazır cloud ELK :)

22:47 - 7 Mar 2019

5 Beğeni



1



5



Yanıtını Tweetle



**Mert SARICA** @MertSARICA · 7 Mar

@caliskanfurkan\_ adlı kullanıcıya yanıt olarak

Eyv.

1



**Samet** @belleveben · 8 Mar

Bu da docker elk. [elk-docker.readthedocs.io](https://elk-docker.readthedocs.io)



2



I started modifying the securityonion-otx script file, which was developed for Security Onion – OTX integration, according to my needs. I set the bro-otx file to save threat intelligence information from OTX to the /etc/logstash/ls-otx/otx.dat file every hour. I also configured the OTX.py file to extract only domain name information from the malicious URL and DOMAIN entries in the otx.dat file and save it as the

/etc/logstash/translate/OTX.yaml file to be read by the Translate filter at the 5th minute of every hour.

```
root@ubuntu:/etc/cron.d# cat bro-otx
# /etc/cron.d/bro-otx
#
# crontab entry to manage Bro OTX pulse updates

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

0 * * * * root python /etc/logstash/ls-otx/bro-otx.py >> /var/log/bro-otx.log 2>&1
root@ubuntu:/etc/cron.d# cat ls-otx
# /etc/cron.d/bro-otx
#
# crontab entry to create Logstash dictionary from OTX file

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

*/5 *1 *1 * * root python /etc/logstash/ls-otx/OTX.py >> /var/log/ls-otx.log 2>&1
root@ubuntu:/etc/cron.d#
```

GNU nano 2.9.3		otx.dat	
#fields indicator	indicator_type meta.source meta.url	meta.do_notice	
34bad798c01b452d708c1409590ea30	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
4601e75267d0dcf4256c43f45ec470a	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
76c173d469c7a73a13ac303214256c	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
805bf50655ab736f4c018d15739e352	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
F547e6ff4376eb0873023f02b911e0230	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
827bd892b43d13c0ab33e82ce37735d178b02e85d3623181e97efe02df	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
www.uscni11ers.com/r1n/images/01/js/index.php	Intel::URL	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
www.lunw.com/wp-includes/images/wlw/img/site.php	Intel::URL	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
db909c50b4f7263ef76902d89680a37f	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
0ce010a8b0525ba10245b877406e36	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
224652a0a0683215e6f143ff70e20c	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
50ed86b6c5cf9a4bf97345935725f20f	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
6b5ce7fb6dd1e588fdd1c344720f7c7a	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
C7323e35841980e3812903a5a000da	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
73c79f84361f8d74ec53c36067b39e6	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
7246a752864933dc640b3e46d84c9f0	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
181d4f01d6dd1aba0e847ce74e24268	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
955a2287f560b1b9f98a1c1313558b	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
patane.myonlinereport.org	Intel::DOMAIN	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
tszakali.sakura.ne.jp/p1c1/index.php	Intel::URL	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
patane.myonlinereport.org	Intel::URL	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
www.wco-kyouai.com/ex-engine/modules/comment/queries/deletecomment.php	Intel::URL	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
www.sics.net.zy/images/patterns/preview/deletecomment.php	Intel::URL	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
c411bf01ee6a31d9f0863c41a1393	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
537d16b7ad05af9d9e0e99346bb9e5	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
f92f8dddb98442c2deb3a36e88cc755	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
a287d48e7eed8f4ce4ba1ca5470b8f3	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
ec0ef96943300ef5030245b420bc706	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
67b2d7b0f6b0e6ba6f0f0c16b93b0e7	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
59a23b229724c2e72a94b0a2f8f8c1	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
15898db0761637094007305de4d238b	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
ed4234b2304341e4a20ed01c0284044	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
ea4f61f03de8ced007fb38e4485883e	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
0ed9e723fdaef595dc1c5d774f8b9b37	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
0ffdd2bdc5f506661cf4d05f9fcb9e61	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
50de060f1689863317eb97c5c1da03	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
25d0cb6204045c992128be2a5211599	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
9e8113a89571904acdb1c714f00689	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
1f4904dacaf15d97293c6c5963303f	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
8090282a98f035b0778de6884d720c0	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
753ac3700a31f8a68f8ed93850f72d8	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
1f2ad09430583bb9cf72cd07456370	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
8e604502c823461d0833e33f91c5728	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
ek39969f45cb889a0e4437329732a2	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
3dc29291a34b4ef9f29404f5277c04	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
054cfr8c56245c54793379fa17b1c99	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
08d651877d26f49e5d017d8a1747ce8	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
ca068126a11e0683f68f86f473735e	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
61654e3eabc22a6eaf14ef50b7f1f57	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
dc0ef0b3f0f4723eead4333ad7f3e8f	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
lib0cb42be04ae1add09ab50bdcd1c9d	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
893f4b3c99c3865db08e1c1ce7980e0	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
da0683bb5e6618051361be772d058	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
1c2b1e6e3e33f01e81be5998d08a38b	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
b108df0bd168684f27b0dded473735e	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
e7106810a51314963305247c03e390d	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
416b22173deb8e6d4a9a8d141a8fdd	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
47e75d0746e695ce2a6700725a9f025	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
a438cf073110b03183a34c93169f81	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
a9217f5cccf378a6a4e8f239acd93d	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
068aee098a2f224b45b9f8d5d30109	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
3c6e67f0c08818363b7ddade90757a84	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds
82ec6f2aaf4abb7e05c0c78e9dedc93	Intel::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68 Author: Alienvault	http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick_Threat_Group.pds



```

root@ubuntu:/etc/logstash/ls-otx# cat OTX.py
#!/usr/bin/env python
# -*- coding: utf-8 -*-
# OTX to Logstash Dictionary Script
# Author: Mert SARICA
# E-mail: mert [ . ] sarica [ @ ] gmail [ . ] com
# URL: https://www.mertsarica.com
#
# Credit: https://raw.githubusercontent.com/TravisFSmith/MyBroElk/master/maliciousIP.py

import re
debug = 0

def writeYAML():
    fname = "/etc/logstash/ls-otx/otx.dat"
    yamlFile = open('/etc/logstash/translate/OTX.yaml', 'w')
    with open(fname) as html:
        cti = []
        for line in html.readlines():
            line = re.sub('\r|\n', '', line)
            if line.find("Intel::DOMAIN") >= 0:
                try:
                    line = line.split("\t")[0]
                    if line not in cti:
                        cti.append(line)
                        if debug:
                            print line.split("\t")[0]
                    yamlFile.write("\t" + line + "\t: \"YES\" + "\n")
                except:
                    continue
            if line.find("Intel::URL") >= 0:
                try:
                    line = line.split("\t")[0]
                    line = line.split("/")[0]
                except:
                    line = line.split("\t")[0]

                try:
                    line = line.split(":")[0]
                    if line not in cti:
                        cti.append(line)
                        if debug:
                            print line
                    yamlFile.write("\t" + line + "\t: \"YES\" + "\n")
                except:
                    if line not in cti:
                        cti.append(line)
                        if debug:
                            print line
                    yamlFile.write("\t" + line + "\t: \"YES\" + "\n")

    yamlFile.close()

if __name__=="__main__":
    writeYAML()
root@ubuntu:/etc/logstash/ls-otx# █

```

```

root@ubuntu:/etc/logstash/translate# ls
OTX.yaml
root@ubuntu:/etc/logstash/translate# head -n 10 OTX.yaml
"www.aucsellors.com": "YES"
"www.lunwe.com": "YES"
"patane.myonlineportal.org": "YES"
"isozaki.sakura.ne.jp": "YES"
"www.wco-kyousai.com": "YES"
"www.51cs.net": "YES"
"www6.intarnetservice.com": "YES"
"www.webmailerservices.com": "YES"
"go-trust.webmailerservices.com": "YES"
"www.adobeservice.net": "YES"
root@ubuntu:/etc/logstash/translate#

```

In the configuration file of Logstash (logstash.conf), I defined the rules to read DNS records logged by syslog-ng with the Grok filter and to send an alert via email if any of the IP addresses or domain names in these records match with those in the OTX.yaml file using the Translate filter. Then I restarted Logstash and made an nslookup for the address `www[.]aucsellors[.]com` listed in the OTX.yaml file. With this, the alert was

successfully generated and sent to me by email, and I had successfully implemented the home-based threat intelligence service. :)

Test grok patterns

grokconstructor.appspot.com/do/match#result

Not secure | Hack 4 Career. Infor... | LinkedIn | Mert SARICA (merts... | Inbox - mert.sarica...

Some log lines you want to match. It's helps much to use several lines, and to choose lines that are as diverse as possible.  
Mar 27 20:15:31 192.168.1.1 dnsmasq[29860]: reply upu.samsungelectronics.com is 54.83.144.140

The (unquoted) pattern that should match all logfile lines.(Please keep in mind that the whole log line / message is searched for this pattern; if you want this to match the whole line, enclose it in ' s or ' A z. This speeds up the search - especially if the pattern is not found.)  
%(SYSLOGTIMESTAMP syslog\_timestamp) %(SYSLOGHOST syslog\_hostname) %(DATA syslog\_program)?(%[POSINT syslog\_pid])? (reply|cached) %  
(GREEDYDATA syslog\_iporhost2) (is) %(GREEDYDATA syslog\_iporhost2)

Please mark the libraries of grok Patterns from logstash v2.4.0 which you want to use. You probably want to use grok-patterns if you use any of the others, since they rely on the basic patterns defined there.  
firewalls avs bro exim bind haproxy linux-syslog squid mcollective-patterns bacula postgresql java maven grok-patterns httpd redis nagios rails mongodb ruby mcollective junos

You can also provide a library of some additional grok patterns in the same format as the pattern files linked above. On each line you give a pattern name, a space and the pattern. For example: WORD %w-%b

If you want to use logstash's multiline filter please specify the used pattern (can include grok Patterns):

☐ negate the multiline regex

Mar 27 20:15:31 192.168.1.1 dnsmasq[29860]: reply upu.samsungelectronics.com is 54.83.144.140

MATCHED	
syslog_program	dnsmasq[29860]
syslog_hostname	192.168.1.1
syslog_iporhost2	54.83.144.140
syslog_iporhost	upu.samsungelectronics.com
syslog_timestamp	Mar-27-20:15:31

root@ubuntu:/etc/logstash# cat logstash.conf

input {  
 # stdin { type => syslog }  
 file {  
 path => "/var/log/dns-sys/192.168.1.1/\*.log"  
 start\_position => "beginning"  
 }  
}

filter {  
 grok {  
 match => { "message" => "%{SYSLOGTIMESTAMP:syslog\_timestamp} %{SYSLOGHOST:syslog\_hostname} %(DATA:syslog\_program)?(%[POSINT:syslog\_pid])?: (reply|cached) %{GREEDYDATA:syslog\_iporhost2} (is) %{GREEDYDATA:syslog\_iporhost2}" }  
 add\_tag => "dnsmasq"  
 }  
 grok {  
 match => { "message" => "%{SYSLOGTIMESTAMP:syslog\_timestamp} %{SYSLOGHOST:syslog\_hostname} %(DATA:syslog\_program)?(%[POSINT:syslog\_pid])?: (query|A|I) %{GREEDYDATA:syslog\_iporhost2} (from) %{GREEDYDATA:syslog\_queryfrom}" }  
 add\_tag => "dnsmasq"  
 }  
 translate {  
 field => "syslog\_iporhost"  
 destination => "malicious"  
 dictionary\_path => "/etc/logstash/translate/OTX.yaml"  
 add\_tag => "malicious"  
 }  
 translate {  
 field => "syslog\_iporhost2"  
 destination => "malicious"  
 dictionary\_path => "/etc/logstash/translate/OTX.yaml"  
 add\_tag => "malicious"  
 }  
 mutate {  
 remove\_tag => ["\_grokparsefailure"]  
 }  
 if "dnsmasq" not in [tags] {  
 drop { }  
 }  
}

output {  
 stdout {  
 codec => rubydebug  
 }  
 if [malicious] == "YES" and [syslog\_iporhost2] {  
 email {  
 address => "127.0.0.1"  
 from => "alert@mertsarica.com"  
 htmlbody => "Malicious traffic has been detected!<br/><br/><b>Destination Domain: </b>%(syslog\_iporhost2)<br/><b>Destination IP: </b>%(syslog\_iporhost2)<br/><b>Raw Log: </b>%(message)"  
 port => 25  
 subject => "Malicious Traffic"  
 to => "mert.sarica@gmail.com"  
 use\_tls => false  
 }  
 }  
 else if [malicious] == "YES" and [syslog\_queryfrom] {  
 email {  
 address => "127.0.0.1"  
 from => "alert@mertsarica.com"  
 htmlbody => "Malicious traffic has been detected!<br/><br/><b>Source IP: </b>%(syslog\_queryfrom)<br/><b>Destination IP or Domain: </b>%(syslog\_iporhost2)<br/><b>Raw Log: </b>%(message)"  
 port => 25  
 subject => "Malicious Traffic"  
 to => "mert.sarica@gmail.com"  
 use\_tls => false  
 }  
 }  
}



```

root@ubuntu:/etc/logstash# /usr/share/logstash/bin/logstash -f logstash.conf
WARNING: could not find logstash.yml which is typically located in $LS_HOME/config or /etc/logstash. You can specify the path using --path.settings. Continuing using the defaults
Could not find log4j2 configuration at path /usr/share/logstash/config/log4j2.properties. Using default config which logs errors to the console
[WARN ] 2019-04-01 21:47:48.681 [Logstash:runner] multi/local - ignoring the 'pipelines.yml' file because modules or command line options are specified
[INFO ] 2019-04-01 21:47:48.747 [Logstash:runner] runner - Starting Logstash {"logstash.version"=>"6.7.0"}
[INFO ] 2019-04-01 21:48:36.336 [Converge PipelineAction::Create<main>] pipeline - Starting pipeline {:pipeline_id=>"main", :pipeline_workers=>4, :pipeline_batch_size=>125, :pipeline_batch_delay=>50}
[INFO ] 2019-04-01 21:48:46.924 [Converge PipelineAction::Create<main>] pipeline - Pipeline started successfully {:pipeline_id=>"main", :thread=>#<Thread:0x4aee8f3b runs>}
The stdin plugin is now waiting for input:
[INFO ] 2019-04-01 21:48:47.157 [Ruby-0-Thread-1: /usr/share/logstash/lib/bootstrap/environment.rb:6] agent - Pipelines running (:count=>1, :running_pipelines=>[:main], :non_running_pipelines=>[])
[INFO ] 2019-04-01 21:48:48.417 [Api webserver] agent - Successfully started Logstash API endpoint {:port=>9600}
Mar 31 19:17:49 192.168.1.1 dnsmasq[29860]: reply test.com is 173.194.219.138
/usr/share/logstash/vendor/bundle/ruby/2.3.0/gems/awesome_print-1.7.0/lib/awesome_print/formatters/base_formatter.rb:31: warning: constant ::Fixnum is deprecated
{
  "syslog_program" => "dnsmasq",
  "message" => "Mar 31 19:17:49 192.168.1.1 dnsmasq[29860]: reply test.com is 173.194.219.138",
  "host" => "0.0.0.0",
  "syslog_iporhost" => "test.com",
  "syslog_pid" => "29860",
  "token" => "omTayqWwXwXwYroESsItgGNzLYnxkva",
  "syslog_iporhost2" => "173.194.219.138",
  "timestamp" => "2019-04-01T18:49:17.281Z",
  "type" => "syslog",
  "syslog_hostname" => "192.168.1.1",
  "syslog_timestamp" => "Mar 31 19:17:49",
  "tags" => [
    [0] "dnsmasq"
  ],
  "version" => "1"
}
Mar 31 19:17:49 192.168.1.1 dnsmasq[29860]: reply www.aucsellors.com is 173.194.219.138
{
  "syslog_program" => "dnsmasq",
  "message" => "Mar 31 19:17:49 192.168.1.1 dnsmasq[29860]: reply www.aucsellors.com is 173.194.219.138",
  "host" => "0.0.0.0",
  "syslog_iporhost" => "www.aucsellors.com",
  "syslog_pid" => "29860",
  "token" => "omTayqWwXwXwYroESsItgGNzLYnxkva",
  "syslog_iporhost2" => "173.194.219.138",
  "timestamp" => "2019-04-01T18:49:27.866Z",
  "type" => "syslog",
  "syslog_hostname" => "192.168.1.1",
  "syslog_timestamp" => "Mar 31 19:17:49",
  "tags" => [
    [0] "dnsmasq",
    [1] "malicious"
  ],
  "version" => "1",
  "malicious" => "YES"
}

```

## Malicious Traffic

Inbox x



**alert@mertsarica.com** via [sandbox.mgsend.net](#)

to me ▾

Malicious traffic has been detected!

Destination Domain: [www.aucsellors.com](#)

Destination IP: 173.194.219.138

Raw Log: Mar 31 19:17:49 192.168.1.1 dnsmasq[29860]: reply [www.aucsellors.com](#) is 173.194.219.138

Reply

Forward

Hope to see you in the following articles.