

Ev Tipi Tehdit İstihbaratı

written by Mert SARICA | 1 October 2019

If you are looking for an English version of this article, please visit [here](#).

Yazılarımı okuyanlarınız, Esaretten Kaçış başlıklı yazımda güvenliğini kendinizin sağlayabildiği, güvenlik özellikleri ile dopdolu bir yönlendirici (router) kullanmanın avantajlarından büyük bir mutlulukla bahsettiğimi hatırlayacaklardır. Yazıda da bahsettiğim üzere DNS trafiğini şifreli (Dns over HTTPS – DoH) hale getirmek için dnscrypt-proxy aracını kullanmaya başlamıştım.

Termostatların akıllandığı (smart), akıllı televizyonların kameralarla donatıldığı, elektrikli su ısıtıcılarının, ütülerin casuslaştırıldığı günümüzde, ev ağımıza bağlı olup internete bağlanan güvensiz nesneler (IoT), enfekte olmuş, zararlı yazılım barındıran sistemler, cihazlar güvenliğimiz, mahremiyetimiz için büyük risk teşkil ediyorlar. Hacklenmiş, enfekte olmuş, arka kapı içeren ev ağımızdaki sistemleri nasıl tespit edebileceğim üzerine düşünürken dnscrypt-proxy aracı sayesinde ev ağına bağlı tüm sistemler, cihazlar, aygıtlar tarafından gerçekleştirilen DNS isteklerini de kayıt altına alabileceğimi hatırladım.

DNS isteklerini kayıt altına alabildiğim noktada Open Threat Exchange (OTX), Critical Stack gibi siber tehdit istihbaratı servislerinden faydalanarak bu DNS isteklerinde yer alan, alan adlarını ve ip adreslerini bu servislere sorarak ev ağımızdaki zararlı sistemleri tespit edebilirdim. Vakit kaybetmeden bu fikrimi hayata geçirmek için ihtiyaç listesi üzerine düşünmeye başladım.

İlk olarak elimin altında bulunup bu gibi durumlarda her daim yardımına koşan Mini-PC'imde çalışan Ubuntu işletim sistemi üzerine syslog-ng paketini kurmaya karar verdim. Paketi kurduktan sonra gelen dns isteklerini /var/log/dns-sys/gönderenin-ip-adresi klasörü altındaki tarih.log dosyasına kayıt edecek şekilde ayarladım ve /etc/syslog-ng/conf.d/dns-sys.conf dosyasına kayıt ettim.

```

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

```

Sonraki adımda dnscrypt-proxy aracının dns isteklerini yönlendiricinin syslog'una kayıt etmesi için /jffs/configs/dnsmasq.conf.add dosyasına log-queries satırını ekledim. Ardından yönlendiricinin bu istekleri syslog sayfasında göstermesini sağlamak için Default message log level ve Log only messages more urgent than değerlerini debug olarak ayarladım ve bu mesajları Ubuntu üzerinde çalışan syslog-ng uygulamasına yönlendirmek için Remote Log Server değerini Ubuntu'nun ip adresi olarak tanımladım.

```

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# █

```

ASUS RT-AC1900U

Powered by
Asuswrt-Merlin

Logout

Reboot

English

Quick Internet Setup

Operation Mode: **Wireless router** Firmware Version: **384.9** SSID:

General Log Wireless Log DHCP leases IPv6 Routing Table Port Forwarding Connections

System Log - General Log

This page shows the detailed system's activities.

System Time	Wed, Mar 27 21:07:46 2019
Uptime	17 days 9 hours 34 minute(s) 20 seconds
Remote Log Server	192.168.1. Port: 514
Default message log level	debug
Log only messages more urgent than	debug

Apply

☒ Auto refresh

Mar 27 21:07:40 dnsmasq[29860]: reply wildcard-ru.asustek.com.akadns.net is <CNAME>
Mar 27 21:07:40 dnsmasq[29860]: reply e11960.dscl15.akamaiedge.net is 104.101.244.165
Mar 27 21:07:40 dnsmasq[29860]: dnssec-query[DS] trafficmanager.net to 127.0.0.1
Mar 27 21:07:40 dnsmasq[22450]: dnssec-query[DNSKEY] ca to 127.0.0.1
Mar 27 21:07:40 dnsmasq[22450]: reply ca is DNSKEY keytag 48662, algo 8
Mar 27 21:07:40 dnsmasq[22450]: reply ca is DNSKEY keytag 2134, algo 8
Mar 27 21:07:40 dnsmasq[22450]: reply ca is DNSKEY keytag 43854, algo 8
Mar 27 21:07:40 dnsmasq[22450]: reply ca is DNSKEY keytag 35433, algo 8
Mar 27 21:07:40 dnsmasq[22450]: reply lostrealm.ca is DS keytag 2371, algo 13, digest 2
Mar 27 21:07:40 dnsmasq[22450]: validation result is SECURE
Mar 27 21:07:40 dnsmasq[22450]: reply asuswrt.lostrealm.ca is 174.142.221.134
Mar 27 21:07:40 dnsmasq[29860]: reply trafficmanager.net is no DS
Mar 27 21:07:40 dnsmasq[29860]: validation result is INSECURE
Mar 27 21:07:40 dnsmasq[29860]: reply account.asus.com is <CNAME>
Mar 27 21:07:40 dnsmasq[29860]: reply asusaccount.trafficmanager.net is <CNAME>
Mar 27 21:07:40 dnsmasq[29860]: reply ssoap.japanwest.cloudapp.azure.com is 138.91.27.92
Mar 27 21:07:44 dnsmasq[29860]: query[A] google.com from 127.0.0.1
Mar 27 21:07:44 dnsmasq[29860]: cached google.com is 2607:f8b0:4002:811::200e
Mar 27 21:07:44 dnsmasq[29860]: query[A] google.com from 127.0.0.1
Mar 27 21:07:44 dnsmasq[29860]: cached google.com is 172.217.0.78
Mar 27 21:07:44 dnsmasq[29860]: query[PTR] e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.1.1.8.0.2.0.0.4.0.b.8.f.7.0.6.2.ip6
Mar 27 21:07:44 dnsmasq[29860]: cached 2607:f8b0:4002:811::200e is at126s14-in-x0e.1e100.net
Mar 27 21:07:44 dnsmasq[29860]: query[PTR] 78.0.217.172.in-addr.arpa from 127.0.0.1
Mar 27 21:07:44 dnsmasq[29860]: cached 172.217.0.78 is at126s16-in-f14.1e100.net
Mar 27 21:07:44 dnsmasq[29860]: cached 172.217.0.78 is nuq04s19-in-f14.1e100.net

Clear Save

General

Network Map

Guest Network

AiProtection

Adaptive QoS

Traffic Analyzer

USB Application

AiCloud 2.0

Tools

Advanced Settings

Wireless

LAN

WAN

IPv6

VPN

Firewall

Administration

Syslog-ng kayıtlarını teker teker incelemeye ve tehdit istihbaratı adına hangi tür kayıtlara odaklanmam gerektiğine bakmaya başladım. Kayıtlarda yer alan query[A], cached ve reply bilgilerden faydalanabileceğimi öğrendikten sonra bu kayıtları OTX ile entegre çalışabilen Security Onion'a gönderebileceğimi düşündüm. Security Onion'un 16.04.5.6 işletim sistemini kurup çalıştırdıktan sonra logstash servisinin (so-logstash) bir türlü çalışmadığını farkettilim. Üzerinde debelenmeme rağmen başarılı olamadıktan sonra alternatif yollar üzerine araştırma yapmaya başladım.

```

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
dnssec-query[DNSKEY]
dnssec-query[DS]
forwarded
query[A]
query[AAAA]
query[PTR]
query[SRV]
reply
root@ubuntu:/etc/syslog-ng/conf.d#

```

Twitter üzerinden ELK kurmam gerektiği ile ilgili bir mesaj paylaştığımda bulut ve hazır ELK sistemlerinden faydalanabileceğime dair mesajlar aldım. Ubuntu işletim sistemine ELK mı kursam yoksa bulut bir sistemden mi faydalansam derken Grok filter ve Translate filter eklentilerine sahip Logstash'in bu iş için biçilmiş kaftan olduğunu öğrendim.



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 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



2



Security Onion – OTX entegrasyonu için geliştirilmiş olan securityonion-otx betik dosyasını kendi ihtiyaçlarım doğrultusunda düzenlemeye başladım. bro-otx dosyası saat başı OTX'ten tehdit istihbaratı bilgisini /etc/logstash/ls-otx/otx.dat dosyasına kaydetmek için ayarladım. OTX.py dosyasını da her saatin 5. dakikasında otx.dat dosyasındaki zararlı URL ve DOMAIN kayıtlarından sadece alan adı bilgilerini alıp Translate filter tarafından

okunacak olan /etc/logstash/translate/OTX.yaml dosyası olarak kayıt etmesini sağladım.

```
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	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
4601e75267d0dcf6a25434f454c470a	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
76c173d469c7a73a15ac303214256c	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
805bf50655ab736f4c018d15739e352	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
F547eef4376eb0873023f02b911e4230	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
827bd892b43d13c0ab33e87ce37735d178b02e85d3623181e97efe02df	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
www.uscettl.com/wp-includes/images/01/js/index.php	Intell::URL	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
www.lunw.com/wp-includes/images/wlw/index.php	Intell::URL	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
db909c50b4f7263ef79602d9680a37f	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
c0ec10a8b525a10245b87f406e36	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
224652a9a06831215e6f143ff7e20	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
50dec86b6c5fa94bf97345935725f20f	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
6b5ce7fb6dd1e588fdd1c344720f7c	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
C7323e35841980e3812903a5a000da	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
73c79f84361f8d74ec53c36067b39e6	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
7246a752864933dc640b3e46d84c9f0	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
181d4f01d6dd1aba0e847ce74e24268	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
955a2287f560b1b9f98a1c1313558b	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
patane.myonlinereport.org	Intell::DOMAIN	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
tszakali.sakura.ne.jp/p1c1/index.php	Intell::URL	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
patane.myonlinereport.org	Intell::URL	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
www.wco-kyouai.com/ex-engine/modules/comment/queries/deletecomment.php	Intell::URL	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
www.sics.net.zy/images/patterns/preview/deletecomment.php	Intell::URL	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
c411bf01ee6a31d9f0863c41a1393	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
537d16b7ad05af9d9e0e99346b9e65	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
f92f8dd098442c2eb7a36e88cc5755	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
a287d48e7eed8f4ce4b1ca25470b8f3	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
ec0ef96943300ef5030245b420bc706	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
67b2d7b0f6b0e6ba6f0f0c16b93b0e7	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
59a23b229724c2e72a94b0a2f8f8c1	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
15898db0761637094007305de4d3238b	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
ed4234b2304341ea20ed01c028a04d4	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
ea4f61f03de8ced007fb38e4485883c	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
0ed9ef2307dae5f95dc1c5d774f8b9b37	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
0ff42dbcf5f0d66b1cf4d05f9fcb9e61	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
50de060f1689863317eb97c5c1da03	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
25d0cb6204045c59212b8e2a5211599	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
9981131a89571904acdb1c714f06689	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
1f4904dacaf15d97293c6c596303f1	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
8090282a98f035b0778de6884d720c0	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
753ac3700a31f8a68f8e9d9380f72d8	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
1f2ad09430583bb8cf72cd07456370	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
8e604502c823461d0833e33f91c5728	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
ek39969f45cb889a0e443732973a22	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
3dc29291a34b4ef9f29404f5277c04	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
054cfr8c56245c54793379fa1b1c99	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
08d651877d26f49e5d01f08a147ce8	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
ca068126a11e0683f88f68f457f779	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
61654e3eabc22eabaf14ef50b7f1f57	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
dc0ef0b3f1ff4723eead4333ad7f3e8f	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
lbd0c42be04ae1add09ab50bdcd1c9d	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
893f4b3c99c3865db08e1c1ce7980e0	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
da0683bb5e6618051361be772d058	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
1c2b1e6e3e33f01e81be5998d08a38b	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
b108df0bd168684f27b0dded73735e	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
e7106810a5141963305247c03e390d	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
416b22173deb8e6d4a9a8d141a8fdd	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
47ef240746e695ce2a6700725a9f025	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
a438cf073110b03183a34c93169f81	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
a92f17f5cccf378a6a4e8f239acd93	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
068aee098a2f224b45b9f8d5d30109	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
3c6e67f0c08818363b7ddade90757a84	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...
82ec6f2aaf4abb7e05c0c78e9dedc93	Intell::FILE_HASH	Alienvault OTXv2 - Tick group ID: Scald06890ff2a34699adb68	Author: Alienvault http://download.ahnlab.com/kr/site/library/Analysis_Report/Tick...

```

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#

```

Logstash'un ayar dosyası (logstash.conf) üzerinde syslog-ng ile kayıt altına alınan DNS kayıtlarını Grok filtresi ile okuyan ve Translate filtresi ile burada yer alan ip adreslerinden veya alan adlarından herhangi birinin OTX.yaml dosyasında olması durumunda e-posta ile alarm gönderen tanımlamaları yaptım. Ardından Logstash'i yeniden başlatıp OTX.yaml dosyasında yer alan www[.]aucsellors[.]com adresine nslookup yaptığımda alarmın başarıyla

üremesini ve bana e-posta ile gönderilmesini sağlamış kısaca ev tipi tehdit istihbaratı servisini başarıyla hayata geçirmiş oldum. :)

Test grok patterns

Not secure | grokconstructor.appspot.com/do/match#result

Hack 4 Career. Info... | LinkedIn | Mert SARICA (mertsarica@gmail.com) | Inbox - mertsarica@gmail.com

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 ^ \$ 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) %{GREYEDDATA:syslog_iporhost} (is) %{GREYEDDATA: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 avr 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) %{GREYEDDATA:syslog_iporhost} (is) %{GREYEDDATA:syslog_iporhost2}" }
    add_tag => "dnsmasq"
  }
  grok {
    match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp} %{SYSLOGHOST:syslog_hostname} %{DATA:syslog_program}(?:\[%(POSINT:syslog_pid)\])?: (query\[\A\]) %{GREYEDDATA:syslog_iporhost} (from) %{GREYEDDATA: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_iporhost}<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_iporhost}<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" => "omTayqWwXwxyroESsittgGNzLYnxkva",
  "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" => "omTayqWwXwxyroESsittgGNzLYnxkva",
  "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

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.