proofpoint

ET Intelligence BRO Support Tech Brief

Tech Brief

Overview:

The ET Intelligence now supports exporting the acclaimed Emerging Threats reputation list which can be seamlessly integrated directly into BRO to help identify suspicious activity on your network. This document will outline how to install, configure, and operate the ET Intelligence reputation list in BRO IDS.

Installing ET Intelligence in BRO

Prerequisite Steps:

1. We will assume that you have already built your BRO IDS sensor, and it is using the default directory /usr/local/bro.
2. We will assume that it has a monitor network interface as well as a management network interface which can be used to connect to the ET Intelligence server for updates.
3. You must already be an ET Intelligence customer with a valid Authorization Code.

Installing ET Intelligence in Bro

1. Make a new directory for the ET bro iprep files to live in

   ```
   [rsh@sensor1 opt]$ mkdir /opt/etpro_bro
   [rsh@sensor1 opt]$ cd /opt/etpro_bro
   ```

2. Create the following config files in the folder you just created. These files can also be downloaded from the EmergingThreats github at https://github.com/EmergingThreats/bro

   ```
   [rsh@sensor1 etpro_bro]$ __load__.bro
   ```

   That's two underscores on each side. This is a file that bro requires to know which .bro script in this directory to load.

   ```
   [rsh@sensor1 etpro_bro]$ cat __load__.bro

   #this file exists to load the below referenced bro file
   @load ./etpro_intel.bro
   ```

3. Define which reputation list categories you would like to use on your sensors. Simply uncomment the categories that you want to use. Take care with the commas and quotes. Make sure that the last file listed does not have a comma after it.

```
[rsh@sensor1 etpro_bro]$ cat etpro_intel.bro


#ETPRO IPREP for BRO

@load base/frameworks/intel
@load frameworks/intel/seen
@load frameworks/intel/do_notice

redef Intel::read_files += {

#       @DIR + "/etpro-AbusedTLD-domainrepdata.intel",
#       @DIR + "/etpro-AbusedTLD-iprepdata.intel",
#       @DIR + "/etpro-Bitcoin_Related-domainrepdata.intel",
#       @DIR + "/etpro-Bitcoin_Related-iprepdata.intel",
#       @DIR + "/etpro-Blackhole-domainrepdata.intel",
#       @DIR + "/etpro-Blackhole-iprepdata.intel",
        @DIR + "/etpro-Bot-domainrepdata.intel",
        @DIR + "/etpro-Bot-iprepdata.intel",
#       @DIR + "/etpro-Brute_Forcer-domainrepdata.intel",
#       @DIR + "/etpro-Brute_Forcer-iprepdata.intel",
#       @DIR + "/etpro-ChatServer-domainrepdata.intel",
#       @DIR + "/etpro-ChatServer-iprepdata.intel",
        @DIR + "/etpro-CnC-domainrepdata.intel",
        @DIR + "/etpro-CnC-iprepdata.intel",
        @DIR + "/etpro-Compromised-domainrepdata.intel",
        @DIR + "/etpro-Compromised-iprepdata.intel",
#       @DIR + "/etpro-DDoSAttacker-domainrepdata.intel",
#       @DIR + "/etpro-DDoSAttacker-iprepdata.intel",
#       @DIR + "/etpro-DDoSTarget-domainrepdata.intel",
#       @DIR + "/etpro-DDoSTarget-iprepdata.intel",
        @DIR + "/etpro-DriveBySrc-domainrepdata.intel",
        @DIR + "/etpro-DriveBySrc-iprepdata.intel",
#       @DIR + "/etpro-Drop-domainrepdata.intel",
#       @DIR + "/etpro-Drop-iprepdata.intel",
#       @DIR + "/etpro-DynDNS-domainrepdata.intel",
#       @DIR + "/etpro-DynDNS-iprepdata.intel",
#       @DIR + "/etpro-EXE_Source-domainrepdata.intel",
#       @DIR + "/etpro-EXE_Source-iprepdata.intel",
#       @DIR + "/etpro-FakeAV-domainrepdata.intel",
#       @DIR + "/etpro-FakeAV-iprepdata.intel",
#       @DIR + "/etpro-IPCheck-domainrepdata.intel",
#       @DIR + "/etpro-IPCheck-iprepdata.intel",
#       @DIR + "/etpro-Mobile_CnC-domainrepdata.intel",
#       @DIR + "/etpro-Mobile_CnC-iprepdata.intel",
#       @DIR + "/etpro-Mobile_Spyware_CnC-domainrepdata.intel",
#       @DIR + "/etpro-Mobile_Spyware_CnC-iprepdata.intel",
#       @DIR + "/etpro-OnlineGaming-domainrepdata.intel",
#       @DIR + "/etpro-OnlineGaming-iprepdata.intel",
#       @DIR + "/etpro-P2P-domainrepdata.intel",
#       @DIR + "/etpro-P2P-iprepdata.intel",
```

```
#       @DIR + "/etpro-P2PCnC-domainrepdata.intel",
#       @DIR + "/etpro-P2PCnC-iprepdata.intel",
#       @DIR + "/etpro-Parking-domainrepdata.intel",
#       @DIR + "/etpro-Parking-iprepdata.intel",
#       @DIR + "/etpro-Proxy-domainrepdata.intel",
#       @DIR + "/etpro-Proxy-iprepdata.intel",
#       @DIR + "/etpro-RemoteAccessService-domainrepdata.intel",
#       @DIR + "/etpro-RemoteAccessService-iprepdata.intel",
#       @DIR + "/etpro-Scanner-domainrepdata.intel",
#       @DIR + "/etpro-Scanner-iprepdata.intel",
#       @DIR + "/etpro-SelfSignedSSL-domainrepdata.intel",
#       @DIR + "/etpro-SelfSignedSSL-iprepdata.intel",
#       @DIR + "/etpro-Skype_SuperNode-domainrepdata.intel",
#       @DIR + "/etpro-Skype_SuperNode-iprepdata.intel",
#       @DIR + "/etpro-Spam-domainrepdata.intel",
#       @DIR + "/etpro-Spam-iprepdata.intel",
        @DIR + "/etpro-SpywareCnC-domainrepdata.intel",
        @DIR + "/etpro-SpywareCnC-iprepdata.intel"
#       @DIR + "/etpro-TorNode-domainrepdata.intel",
#       @DIR + "/etpro-TorNode-iprepdata.intel",
#       @DIR + "/etpro-Undesirable-domainrepdata.intel",
#       @DIR + "/etpro-Undesirable-iprepdata.intel",
#       @DIR + "/etpro-Utility-domainrepdata.intel",
#       @DIR + "/etpro-Utility-iprepdata.intel",
#       @DIR + "/etpro-VPN-domainrepdata.intel",
#       @DIR + "/etpro-VPN-iprepdata.intel"

};
```

4. Modify your local.bro file to include this newly created script at the bottom of the file. By default this file exists at /usr/local/bro/share/bro/site/local.bro.

   ```
   [rsh@sensor1 etpro_bro]$ cat /usr/local/bro/share/bro/local.bro

   #ETPRO IP and Domain Reputation Intel
   @load /opt/etpro_bro
   ```

5. Create an hourly Cron job to update the reputation data. Make sure to include your Authorization Code provided to you in your ET Intelligence subscription. You don't have to worry about telling Bro about the new files, it will see them when the date of the file changes.

   This will wget the archive of all the files which is ~1.9M compressed. It will then decompress the files to the directory our script expects them to be in.

   ```
   0 * * * *    wget -q https://rules.emergingthreats.net/<authorization_code>/reputation/bro-repdata.tar.gz && tar -xzf bro-repdata.tar.gz -C /opt/etpro_bro && rm -rf bro-repdata.tar.gz > /dev/null 2>&1
   ```

6. Restart Bro: After Bro knows the intel file exists and loads it, updates of the intel files will be processed by bro automatically. Execute the following commands:

   ```
   [rsh@sensor1 etpro_bro]$ /usr/local/bro/bin/broctl

   [BroControl] > stop
   ```

```
stopping worker-1-1 ...
stopping worker-1-2 ...
stopping worker-1-3 ...
stopping worker-1-4 ...
stopping proxy-1 ...
stopping manager ...
[BroControl] > install
removing old policies in /opt/bro/spool/installed-scripts-do-not-touch/site ...
removing old policies in /opt/bro/spool/installed-scripts-do-not-touch/auto ...
creating policy directories ...
installing site policies ...
generating cluster-layout.bro ...
generating local-networks.bro ...
generating broctl-config.bro ...
generating broctl-config.sh ...
updating nodes ...
[BroControl] > check
manager scripts are ok.
proxy-1 scripts are ok.
worker-1-1 scripts are ok.
worker-1-2 scripts are ok.
worker-1-3 scripts are ok.
worker-1-4 scripts are ok.
[BroControl] > start
starting manager ...
starting proxy-1 ...
starting worker-1-1 ...
starting worker-1-2 ...
starting worker-1-3 ...
starting worker-1-4 ...
[BroControl] > netstats
 worker-1-1: 1444998097.745909 recvd=11 dropped=0 link=11
 worker-1-2: 1444998097.945996 recvd=11 dropped=0 link=11
 worker-1-3: 1444998098.146930 recvd=11 dropped=0 link=11
 worker-1-4: 1444998098.346975 recvd=11 dropped=0 link=11
[BroControl] > exit
```

7. Installation Complete

   You should now see events coming into the intel.log once you start getting hits on ET intelligence data.

   The alert will give you the category and score of that particular indicator.

```
1443106773.411865     CGEsYb3jQDXusALSYi   x.x.x.x  44319   202.108.23.29   80      -
        -       -       202.108.23.29   Intel::ADDR     Conn::IN_RESP ETPRO Rep:
SpywareCnC Score: 107
```

Troubleshooting

While installing ET Intelligence should work as described in this article, issues could arise. If you are running larger intel files on a sensor that is underpowered or overwhelmed, you should refer to Bro's stats.log to

see how your sensor is running. If Bro is dropping packets you will see that there. The more intel files you have active (uncommented) in etpro_intel.bro, the more memory Bro will use. While there was not a noticeable impact on the sensors we tested, everyone has a different setup. If there are any formatting issues with the intel files as they are downloaded every hour, bro will continue to run even if it were to get a badly formatted file. As the intel bro file generation is automated, this should not occur. If bro is unable to load a .intel file for any reason, this will be reflected in bro's reporter.log.

If you require additional assistance, feel free to communicate via the EmergingThreats mailing list.

https://lists.emergingthreats.net/mailman/listinfo/emerging-sigs

Summary

BRO is a very powerful network profiling IDS which can help to identify suspicious activity and behavior on your network. The main challenge with BRO and any IDS is how to extract the actionable events from the noise. ET Intelligence integration empowers you to do exactly that in just a few quick steps.