Malicious Network Activity Visualisation

Aled Mason

Cardiff University

April 22, 2014

Overview

Many large organisations now implement Intrusion Detection Systems (IDSs) to mitigate the increasing Cyber-threat. These IDSs are capable of producing log files, containing information about each Cyber-threat that was prevented. However understanding this data is a difficult task, as a log file typically contains thousands of entries.

Approach

The aim for this project will be to analyse and interpret these log files taken from Cardiff University Information Services (INSRV) IDSs. Specifically, aims to build a visualisation environment tool that can efficiently process, format and communicate this data to the end-user. It also aims to answer some research questions surrounding this data:

- What is the most common type of attack launched towards a given network?
- What time of the day is the busiest with respect to malicious traffic?
- Which country do most Cyber-attacks originate from?
- What time of day are severe attacks launched towards a given network?
- Which sub-networks do most Cyber-attacks target?

Dataset

An example of a raw dataset-

```
Apr  2 00:51:25 picard 1,2014/04/02 00:51:25,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:19,148.251.71.7,131.251.176.35,0.0.0.0,0.0.0.0,In
00:51:25,886669,2,58894,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674773328,0x0,Germany,United
Apr  2 00:51:30 picard 1,2014/04/02 00:51:30,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:25,148.251.71.3,131.251.212.3,0.0.0.0,0.0.0.0,Inb
00:51:30,1038104,2,65145,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674775028,0x0,Germany,Unite
Apr  2 00:51:31 picard 1,2014/04/02 00:51:31,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:25,148.251.71.3,131.251.176.35,0.0.0.0,0.0.0.0,In
00:51:31,855410,1,49343,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674775373,0x0,Germany,United
Apr  2 00:51:31 picard 1,2014/04/02 00:51:31,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:26,2.230.243.35,131.251.176.228,0.0.0.0,0.0.0.0,I
00:51:31,1899270,1,53055,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674775374,0x0,Italy,United
Apr  2 00:51:31 picard 1,2014/04/02 00:51:31,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:26,144.76.178.228,131.251.176.254,0.0.0.0,0.0.0.0
00:51:31,1584006,2,64907,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674775375,0x0,Germany,Unite
Apr  2 00:51:32 picard 1,2014/04/02 00:51:32,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:26,148.251.71.3,131.251.176.212,0.0.0.0,0.0.0.0,I
00:51:32,7423,2,49568,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674775702,0x0,Germany,United
Apr  2 00:51:33 picard 1,2014/04/02 00:51:33,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:28,148.251.71.3,131.251.212.3,0.0.0.0,0.0.0.0,Inb
00:51:33,100741,1,50561,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674776054,0x0,Germany,United
Apr  2 00:51:33 picard 1,2014/04/02 00:51:33,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:28,2.230.243.35,131.251.176.6,0.0.0.0,0.0.0.0,Inb
00:51:33,738943,1,53091,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674776077,0x0,Italy,United
Apr  2 00:51:34 picard 1,2014/04/02 00:51:34,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:29,144.76.178.228,131.251.176.254,0.0.0.0,0.0.0.0
00:51:34,165078,2,50824,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674776368,0x0,Germany,United
Apr  2 00:51:35 picard 1,2014/04/02 00:51:35,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:30,70.63.69.154,131.251.248.133,0.0.0.0,0.0.0.0,I
Threats,2014/04/02 00:51:35,383120,1,28021,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674776726
Apr  2 00:51:36 picard 1,2014/04/02 00:51:36,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:30,148.251.71.3,131.251.176.212,0.0.0.0,0.0.0.0,I
00:51:36,1172724,1,51376,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674777095,0x0,Germany,Unite
Apr  2 00:51:37 picard 1,2014/04/02 00:51:37,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:32,148.251.71.3,131.251.212.3,0.0.0.0,0.0.0.0,Inb
00:51:37,1418830,1,53237,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674777444,0x0,Germany,Unite
Apr  2 00:51:37 picard 1,2014/04/02 00:51:37,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:32,144.76.178.228,131.251.176.254,0.0.0.0,0.0.0.0
00:51:37,2057928,3,51895,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674777445,0x0,Germany,Unite
Apr  2 00:51:38 picard 1,2014/04/02 00:51:38,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:32,148.251.71.7,131.251.176.35,0.0.0.0,0.0.0.0,In
00:51:38,26693,1,65320,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674777768,0x0,Germany,United
Apr  2 00:51:38 picard 1,2014/04/02 00:51:38,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:33,148.251.71.3,131.251.176.35,0.0.0.0,0.0.0.0,In
00:51:38,489312,1,53317,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674777769,0x0,Germany,United
Apr  2 00:51:39 picard 1,2014/04/02 00:51:39,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:33,148.251.71.3,131.251.212.3,0.0.0.0,0.0.0.0,Inb
00:51:39,157972,1,54168,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674778130,0x0,Germany,United
Apr  2 00:51:40 picard 1,2014/04/02 00:51:40,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:34,70.63.69.154,131.251.248.134,0.0.0.0,0.0.0.0,I
Threats,2014/04/02 00:51:40,182999,1,50287,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674778517
Apr  2 00:51:40 picard 1,2014/04/02 00:51:40,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:35,148.251.71.3,131.251.176.212,0.0.0.0,0.0.0.0,I
00:51:40,469450,1,53972,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674778518,0x0,Germany,United
Apr  2 00:51:40 picard 1,2014/04/02 00:51:40,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:34,2.230.243.35,131.251.176.253,0.0.0.0,0.0.0.0,I
00:51:40,1154859,1,53048,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674778544,0x0,Italy,United
Apr  2 00:51:42 picard 1,2014/04/02 00:51:42,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:37,148.251.71.3,131.251.176.212,0.0.0.0,0.0.0.0,I
00:51:42,1793515,3,55718,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674779386,0x0,Germany,Unite
Apr  2 00:51:43 picard 1,2014/04/02 00:51:43,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:38,2.230.243.35,131.251.176.6,0.0.0.0,0.0.0.0,Inb
00:51:43,1147128,1,53269,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674779795,0x0,Italy,United
Apr  2 00:51:44 picard 1,2014/04/02 00:51:44,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:38,148.251.71.7,131.251.176.35,0.0.0.0,0.0.0.0,In
00:51:44,659056,1,52232,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674780228,0x0,Germany,United
Apr  2 00:51:44 picard 1,2014/04/02 00:51:44,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:39,148.251.71.3,131.251.212.3,0.0.0.0,0.0.0.0,Inb
00:51:44,795990,2,56198,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674780229,0x0,Germany,United
Apr  2 00:51:44 picard 1,2014/04/02 00:51:44,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:39,2.230.243.35,131.251.176.228,0.0.0.0,0.0.0.0,I
00:51:44,1692740,1,53237,3389,0,0,0x80000000,tcp,alert,"",MS-RDP Brute-force Attempt(40021),any,high,client-to-server,2674780230,0x0,Italy,United
Apr  2 00:51:45 picard 1,2014/04/02 00:51:45,0009C100858,THREAT,vulnerability,1,2014/04/02 00:51:40,148.251.71.3,131.251.176.35,0.0.0.0,0.0.0.0,In
```

Visualisation

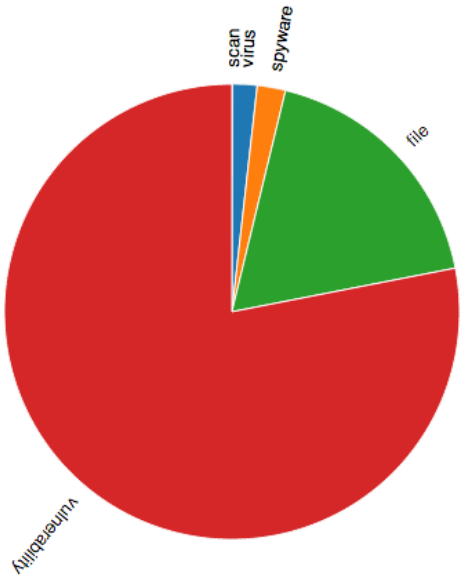
In a TED Talk in 2010, David McCandless, an information designer and author of Information is Beautiful, speaks about data visualisation as a form of knowledge compression[1]. So by using visualisation techniques, we can instantly "make sense" and interpret these large datasets.

[1] McCandless D. *The beauty of data visualization.* 2010. `http://www.ted.com/talks/david_mccandless_the_beauty_of_data_visualization` (accessed 13 Apr 2014).

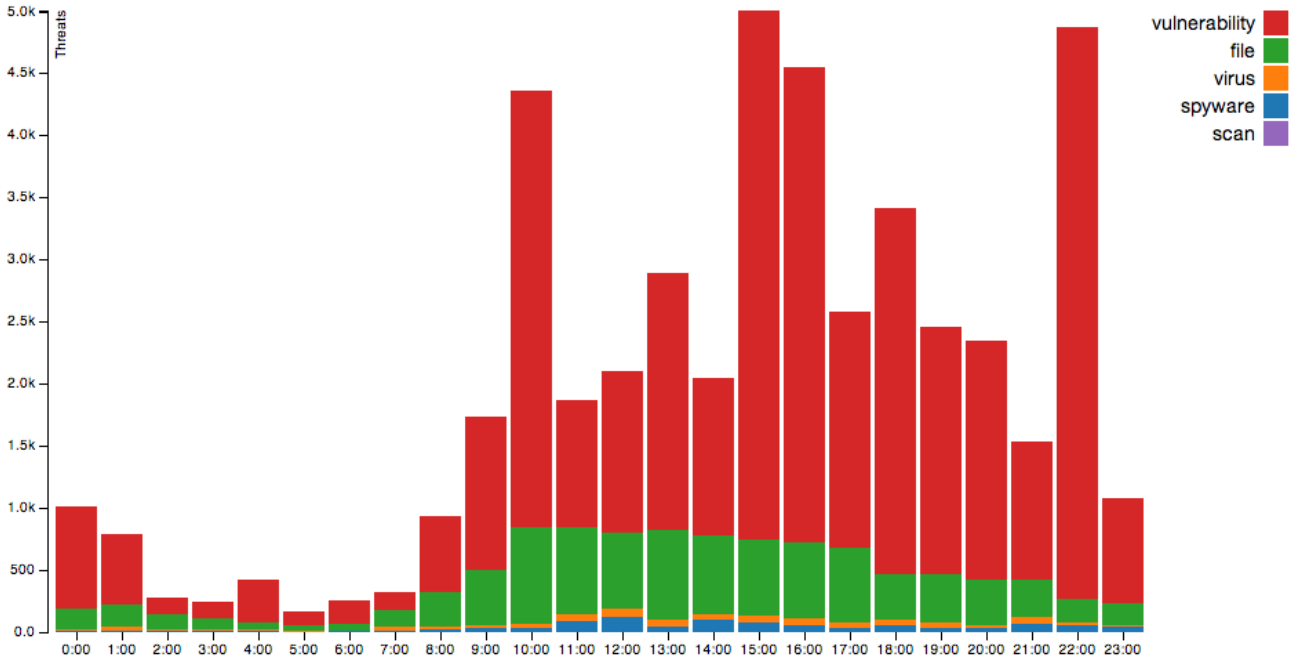
Visualisation

What is the most common type of attack launched towards your network?

We can see that a "vulnerability" attack is the most common type of threat launched towards your system with a total of 36930 entries. Followed by a "file" attack with 8581 entries.



Visualisation



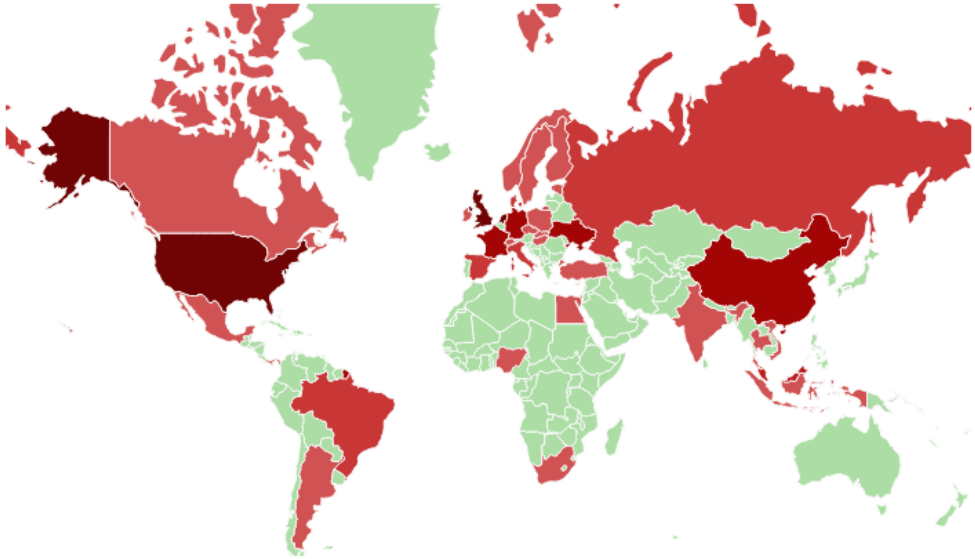
What time of day is the most busy with respect to malicious traffic?

The most traffic was recorded between 15:00 - 16:00 in the afternoon.

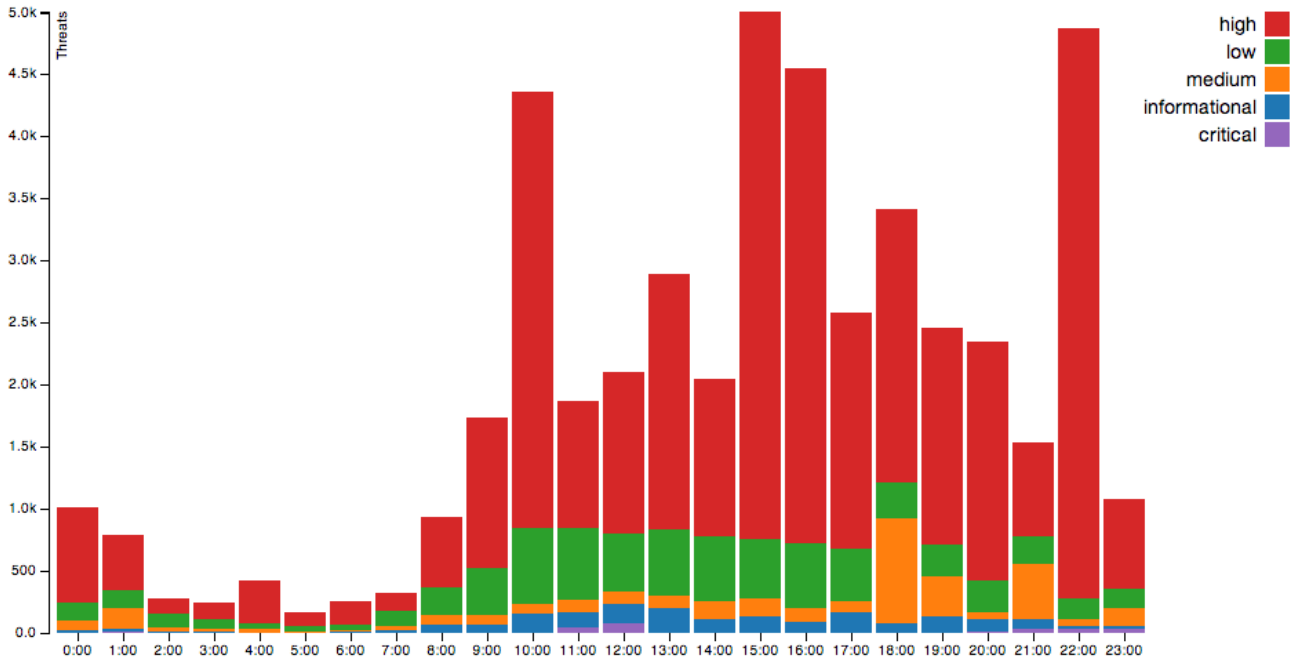
Visualisation

Which country do most threats originate from?

The most threats were recorded to come from United States, with a total of 12364 log entries, followed by United Kingdom with 9319 entries.

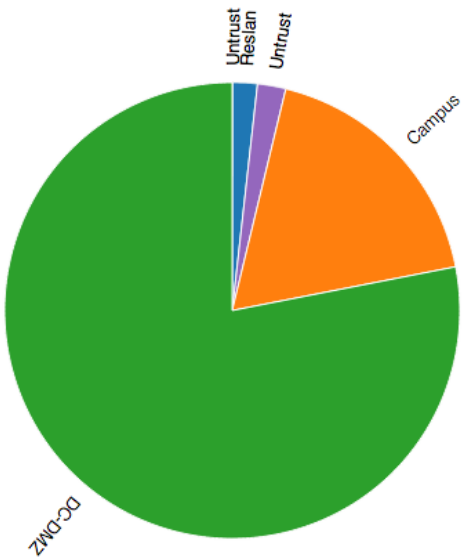


Visualisation



What time of day are high severity attacks launched towards a given network?

Visualisation



What is the most targetted zone in your network?

The most threats were recorded to be targetting DC-DMZ and Campus zones.

Future Work

For future work, there is obviously much scope to continue this project, here are some of my thoughts regarding where this project could lead:-

- Turning this system into a real-time visualisation environment.
- Supporting multiple kinds of log files for analysis.
- Making this project open-source to allow third parties to develop their own visualisations.