**Extracting Insights from OSINT Feeds**

Valentin Todorov

**Objective**

The objective of this project is to analyze OSINT feeds from Bambenek Consulting.

**Methodology**

For the purposes of the analysis I decided to use the master feed of known and active C2 domains. Specifically, I’ll be working with the logs from https://osint.bambenekconsulting.com/feeds/c2-masterlist.txt

The link to the manual for the feeds is broken (http://osint.bambenekconsulting.com/manual/c2-masterlist.txt), and I made some assumptions what the data in the feeds is. The C2 feeds are comma-delimited, in some fields, the value is a list of pipe-delimited values. The comma-delimited values are the following (with examples in the parenthesis):

- domain name ([aakamen.com](http://aakamen.com/))

- domain IP (78.24.9.52)

- FQDNs of the ISP hosting the domain, often times a pipe-delimited list ([ns2.vshosting.cz](http://ns2.vshosting.cz/)|[poski.vshosting.cz](http://poski.vshosting.cz/))

- IPs of the FQDNs, often times a pipe-delimited list (78.24.9.52|89.235.0.2)

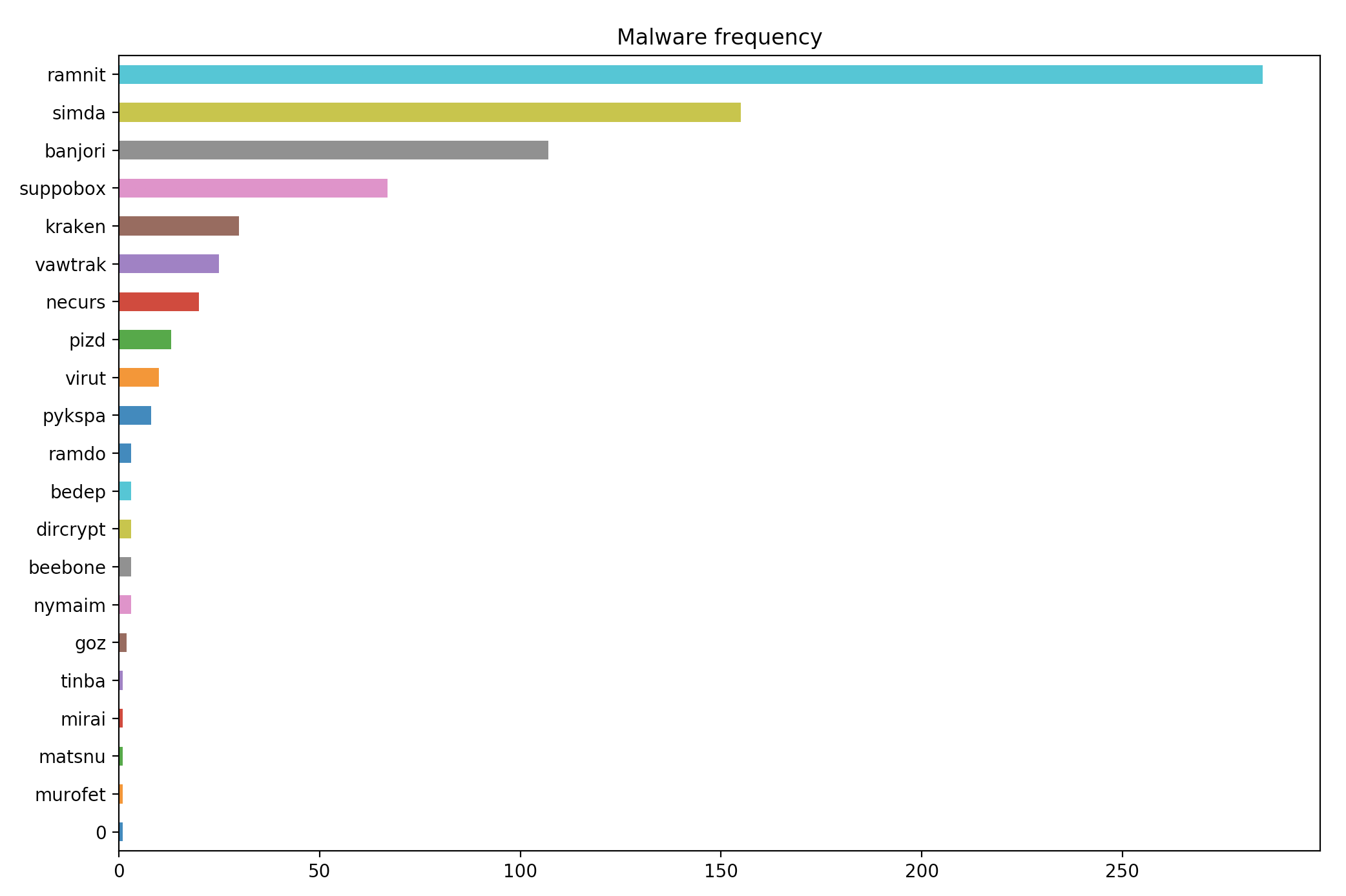
- Description that contains the name of the malware (e.g. Master Indicator Feed for **banjori** non-sinkholed domains)

- A link to the feed's manual. Often times, the links are broken (<http://osint.bambenekconsulting.com/manual/banjori.txt>)

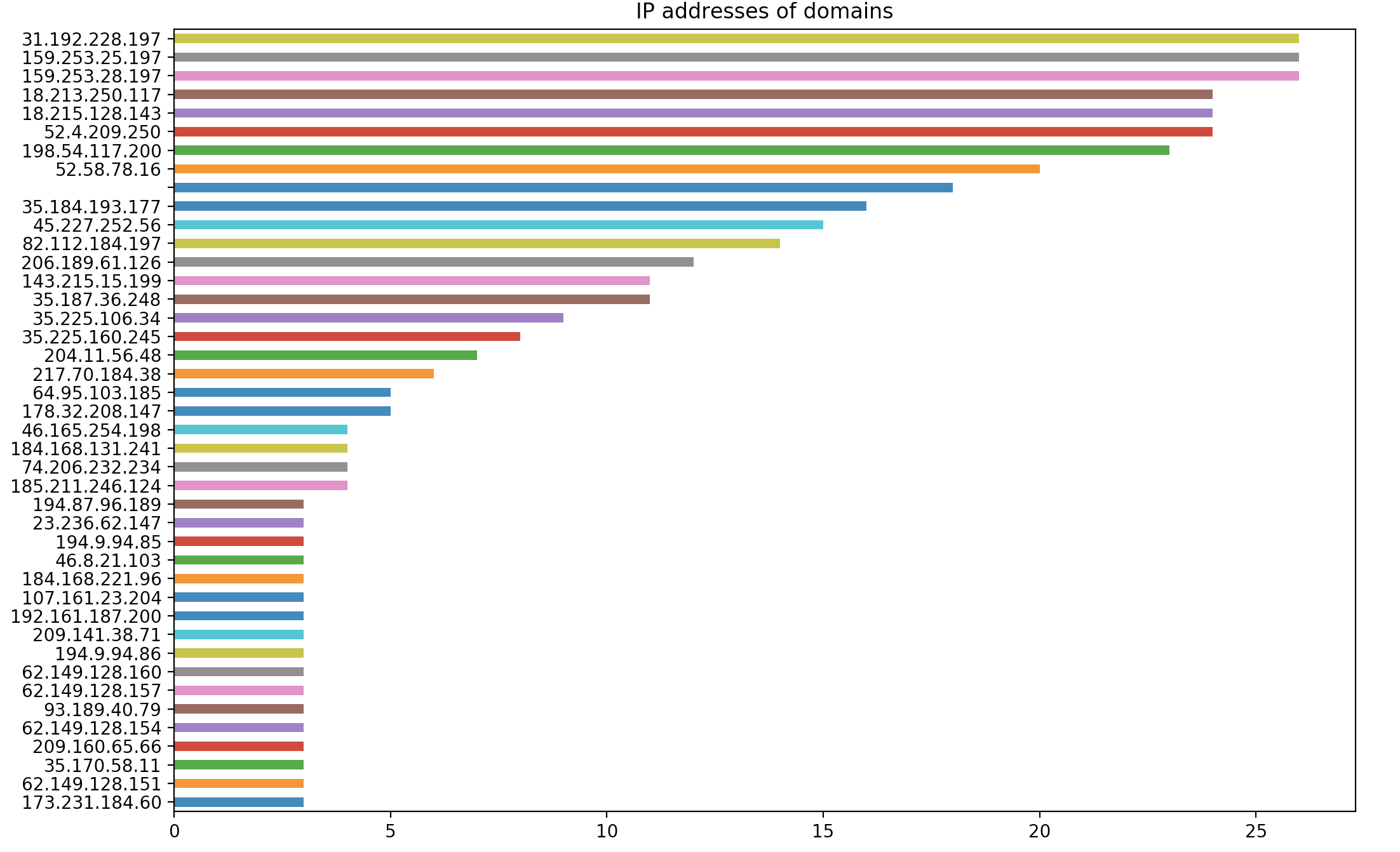
**Analysis**

As of this morning, there were 742 entries in the C2 feed.

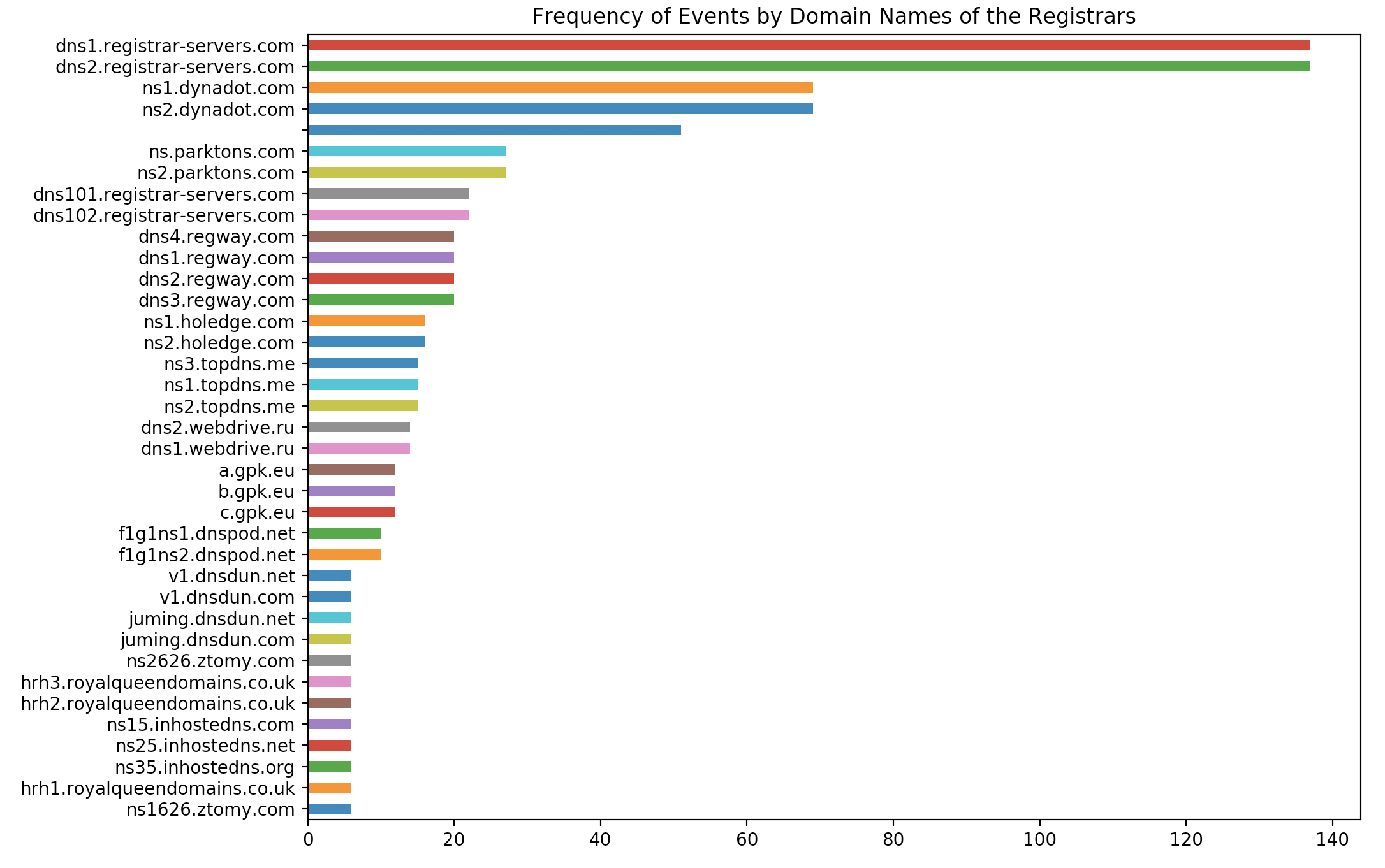
The most common malware attacks were from the malware ramnit, a worm affecting Windows users. The second most common were from the Simda botnet.



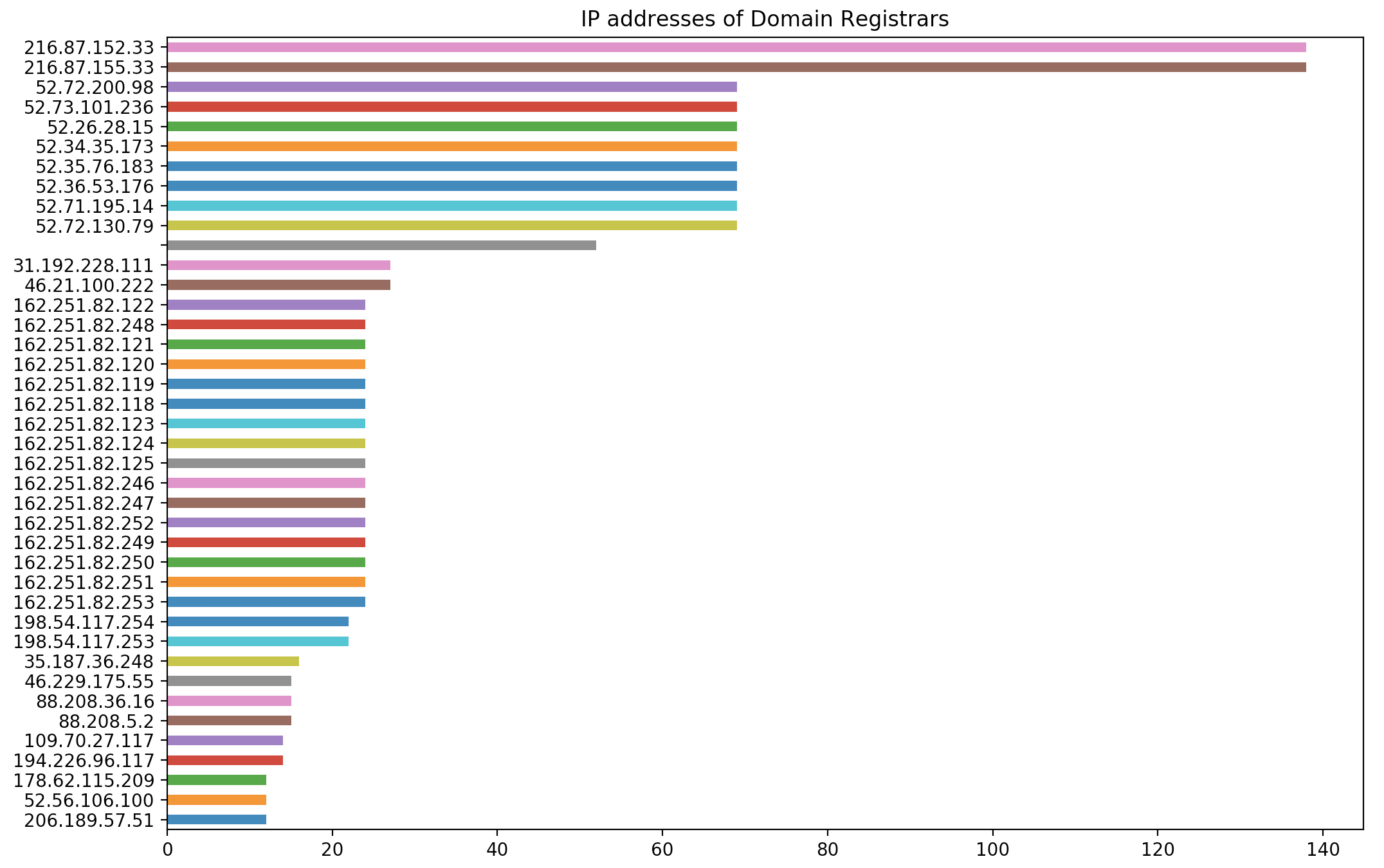
The three domains from which the most malware came were 31.192.228.197, 159.253.25.197 and 159.253.28.197. The graph below shows all the domain IPs from which at least three malware attacks were detected.



The domain registrars used most commonly by malware domains were **registrar-servers.com** with twice as many registrations compared with the second most common **dynadot.com**.



The most common IPs of the registrars are shown below. The top ones are for **registrar-servers.com**



**Next steps**

1. Start aggregating the C2 feed from Bambenek Consulting

Currently, there are only 793 entries in the C2 feed, which are from the last refresh of the feed. The C2 log refreshes at a set frequency and new data is occasionally added. It will be interesting to start aggregating and persisting the information. Over time we’ll collect

1. Augment the data with other sources

Use an RDAP service to get registration information for domains listed in the C2 feed from Bambenek. Similar to the example below, which is from APNIC (the Regional Internet Registry administering IP addresses for the Asia Pacific). It would be relatively straightforward to write a script that loops through the IPs from the list “C2 Masterlist” feed from Bambenek Consulting and searches through RDAP.

By using this information, we can start understanding certain patterns:

* Are there specific ISPs that tend to host more malicious domains than usual? Are there countries that originate a higher percent of domains with malicious content
* Get the information about the ISP that registered a domain. If the information is available, search for that entity in law enforcement databases
  + Are these entities involved in other illegal activities?
  + Can we find the relationship between seeming disparate entities?

https://rdap.apnic.net/ip/47.96.179.127

