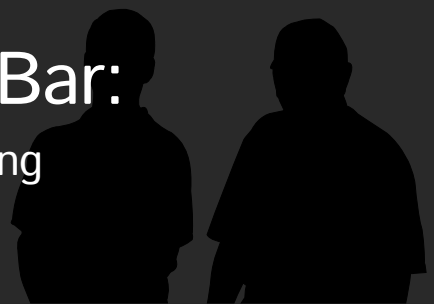
Two Shady Men Walk Into a Bar:

Detecting Suspected Malicious Infrastructure Using Hidden Link Analysis



Summary

› We show how hidden link analysis of malware and IP address mentions on the open and dark Web can be used to detect suspicious IP addresses and infrastructure.

› This method complements traditional blacklists created from intrusion detection systems, honeypots, honeynets, etc.

› 92% of the suspicious IP addresses identified with this method were not identified by current blacklists.

› Requiring co-occurrence of a suspicious IP address with several malware can increase the precision of this analysis.

› The method can also be used to identify target addresses, useful in itself, but can also be used as an indication of potential future malicious addresses if an attack is successful and a system is taken over.

Overview

The purpose of this threat intelligence research is to identify new methods for identifying malicious infrastructure. Today, multiple sources on the Web provide blacklists with IP addresses and URLs suspected of being used in malicious activity[1]. Typically these lists are populated with information from honeypots and intrusion detection systems, for example.

This work was inspired in part by the MLSec project[2], which shows that different blacklists typically contain significant overlap. This inspired us to find methods to detect new, potentially malicious IP addresses that can be found in ways that are complementary to the methods used to populate these lists.

We believe that new information can be derived and additional suspected malicious infrastructure can be identified by analyzing open and dark Web sources that relate malware of various kinds to IP addresses and URLs. In this study, we use the Recorded Future Web index to identify IP address candidates mentioned in suspicious contexts, such as known malware. One might think of this as similar to deciding the shadiness of a bar: if you see one criminal walk in it might be just chance, but if you see two or more this is likely not a place you should visit!

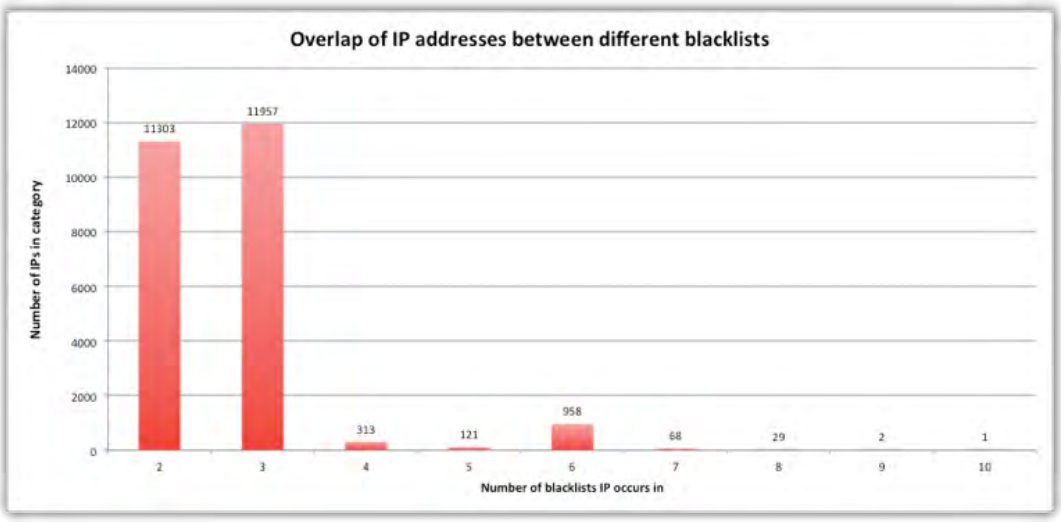
For this project, Recorded Future analyzed 890,000 documents that mention malware (including Web pages, tweets, and pastes) from nearly 700,000 Web sources that Recorded Future tracks, for the time period from January 1, 2014 to August 2, 2015. Sources span from big media to cyber security blogs, social media, forums, and paste sites. A total of 1,408 different malware were mentioned in these documents, and of these, we chose to analyze only 322 that have a defined category in the Recorded Future Cyber Ontology[3] and were not categorized as Adware (which we see as not being truly malicious). This restriction improves the meaningfulness of our analysis.

[1] See https://zeltser.com/malicious-ip-blocklists/ for a set of such lists
[2] https://github.com/mlsecproject, http://www.slidesearch.org/slide/defcon-22-measuring-the-iq-of-your-threat-intelligence-feeds-tiqtest
[3] http://info.recordedfuture.com/Portals/252628/resources/cyber-anatomy-white-paper.pdf

For each document, we selected the primary malware (i.e., malware with the highest Recorded Future Relevance Score) being discussed in the document. We then associated that primary malware with all IP addresses mentioned in the document. This yielded a set of 67,563 IP addresses that were associated with some type of malware in some document.

To narrow our analysis down to a smaller set of particularly suspicious IP addresses, we then selected only those IP addresses that had at least two different malware associated with it (think again of the two shady guys in the bar). We also removed a number of known "whitelisted" IP addresses, such as Google's DNS servers 8.8.8.8, 8.8.4.4, Comcast's DNS servers 75.75.75.75 and 75.76.76.76, and other special addresses such as 127.0.0.1, and the private address ranges - RFC 1918 (10.*.*.*, 172.16.*.*, 192.168.*.*). This gave us a final working set of 1,521 IP addresses and 198 different malware.

It is interesting to compare our results against a set of industry standard blacklists. For a specific day, these lists contained 325,106 entries with 258,288 unique IP addresses, so there was 21% overlap within the blacklists. A total of 24,752 IPs occurred on more than one blacklist, and as can be seen in the following diagram most of those occurred on two or three blacklists:



We also looked at the distribution of IPs categorized as inbound and outbound, and found that 256,253 (99%) were categorized as inbound and only 1,953 (1%) as outbound. 82 addresses were categorized as both inbound and outbound.

We then compared the 1,521 IP addresses against the 258,288 IP addresses currently occurring on the blacklists, and found that only 117 of them were on those list, whereas the rest were unknown and not included on the blacklists. In other words, 92% of the suspicious IP addresses identified with this method were not identified by current blacklists. Of the 117 addresses, 67 were classified as inbound and 50 as outbound, and 12 of the 117 addresses occurred on multiple blacklists.

The small overlap between our set of suspicious IP addresses and those from blacklists is an indication that the overlap in original sources is small — i.e. that few of the sources used to create blacklists are published to the Web in other forms, and few of the sources harvested by Recorded Future are taken into account when creating blacklists. Another reason for the low overlap between our approach and traditional blacklists is that though the focus is on malware co-occurrence we tend to get a larger proportion of suspicious outbound IP addresses than the blacklists, which to a large extent are based on honeypots and therefore focus more on inbound malicious addresses. The fairly even distribution of inbound/outbound addresses in the small set of addresses overlapping our method and the blacklists supports this.

We then relaxed the criteria to include IP addresses mentioned together with only one malware; this expanded the set to 67,209 suspicious IP addresses (again, removing a set of whitelisted addresses from the starting set), of which only 1,420 were on our set of blacklists and 65,789 (98%) were unknown. The lower percentage of overlap with blacklists probably validates our hypothesis that the relaxed approach increases the volume of suspicious addresses at the expense of introducing more noise.

Using GeoIP and Whois services we can enrich the set of suspicious addresses by adding information about owner, geographic location, and ASN association for each IP address.

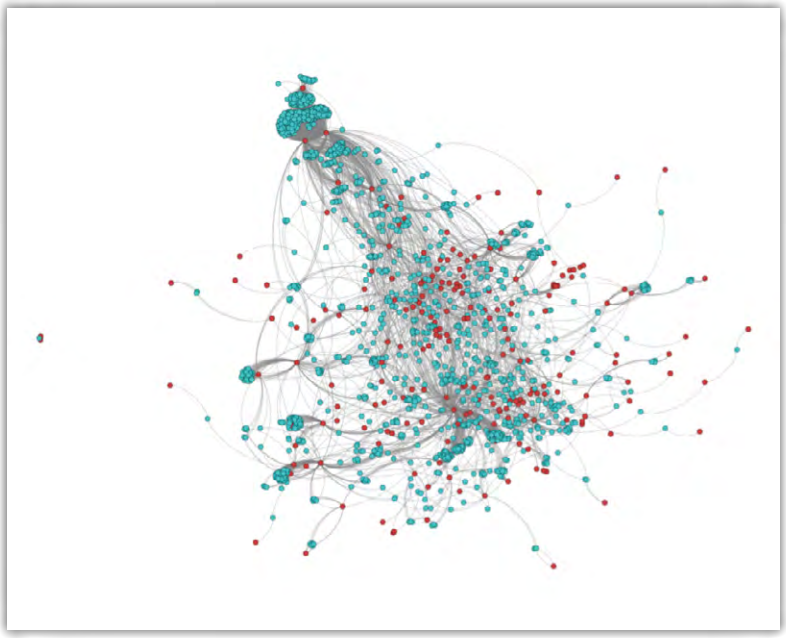
It can be argued that in some cases the implicated IP addresses belong to hosting providers that use massive shared hosting on a single IP address, and therefore the suspicious address is related to only a small subset of the servers and services hidden behind that address. We argue that such a hosting provider should still be investigated, since malware might spread within the site, and the fact that many unaffected services originate from an address does not mean the problematic ones can be ignored.

Based on this exercise, we believe any organization wanting to keep its cyber defenses up to date needs to not only subscribe to an extensive set of blacklists, but also complement these with IP risk scoring using hidden link analysis based on Web intelligence from both open and dark Web sources.

Detailed Examples

The restricted set of 1,521 IP addresses and 198 malware can be illustrated by the following co-occurrence graph (where malware are red nodes and IP addresses blue nodes). Even though pictures like these are helpful in identifying interesting structures and regions of a malware-IP-graph, we prefer algorithmic link analysis based on this co-occurrence graph.

The analysis we suggest is best understood by a few examples.



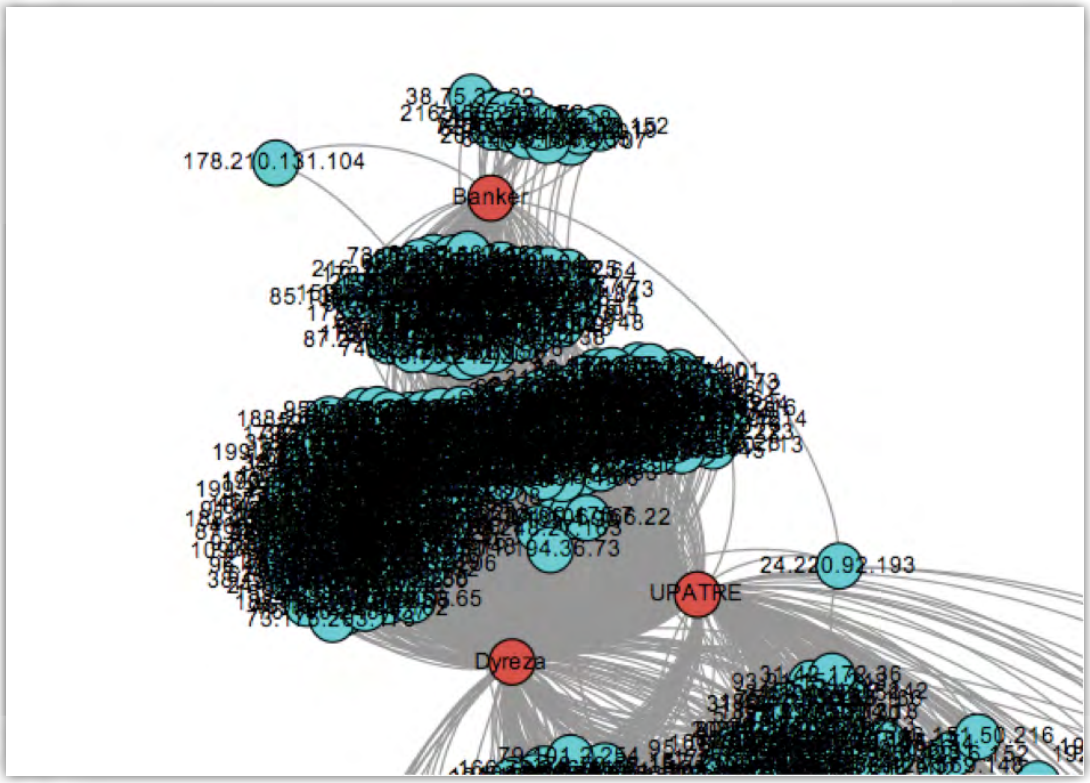
Network graph of 1,521 IP addresses (blue) and 198 Malware (red) shows some major clusters and several smaller structures. At this scale names of nodes are not visible -- see case studies below for labelled subviews of the graph.

To decide which malware and IP clusters are most interesting to explore, we can generate a list of all malware pairs and the number of IP addresses they share as neighbours. We also use the Recorded Future index to calculate the number of text fragments/sentences in which the two malware co-occur, as well as the number of documents where they co-occur (N.B., several fragments can co-occur in the same document, therefore there are in some cases more fragment than document co-occurrences). We also calculate a (somewhat arbitrarily chosen) weighted text overlap index as $\frac{2F+D}{3}$, where F is the number of fragment co-occurrences and D the number of document co-occurrences. Sorting our malware pairs by number of shared IP addresses gives us the following table:

Malware 1 name	Malware 2 name	Shared IP count	Blacklisted IPs	Weighted text overlap
UPATRE	Dyreza	476	41	1214
Banker	UPATRE	100	7	14
Banker	Dyreza	88	7	137
Fareit	Dyreza	61	27	46
Fareit	UPATRE	59	26	17
Citadel	Zeus	48	16	1118
BlackIce	Palevo	44	0	0
EvilBunny	Morto	41	3	0
VAWTRAK	UPATRE	37	4	23
VAWTRAK	Dyreza	37	4	31
Slowloris	Zollard	36	4	0
Dridex	Dyreza	33	3	624
SpyEye	Ramnit	29	2	699
Dridex	UPATRE	26	1	27
Casper	Zeus	26	0	0
Emotet	Zeus	24	0	22
BlackIce	SpyEye	21	0	0
CryptoWall 3.0	CryptoWall	21	0	385
UPATRE	Zeus	21	0	166
SpyEye	Zeus	19	0	3060
Critroni - CTB-Locker	Zeus	18	0	2
Mydoom	Angler Exploit Kit	16	0	0
BlackIce	Dorkbot	15	0	0
Poweliks	Zeroaccess	15	0	9
Sub7 RAT	Lizard Stresser	15	0	4
Fynloski	UPATRE	14	0	0
Crowti	CryptoDefense	14	0	9
Tinba	Dridex	14	4	58
Dridex	Cridex	14	6	555
BlackIce	Zeus	13	1	0

Dyreza and Upatre (and Banker)

The first three lines in the table above correspond to the large cluster of IP addresses in the top left corner of the graph where we find three malware: Dyreza, Upatre, and Banker.



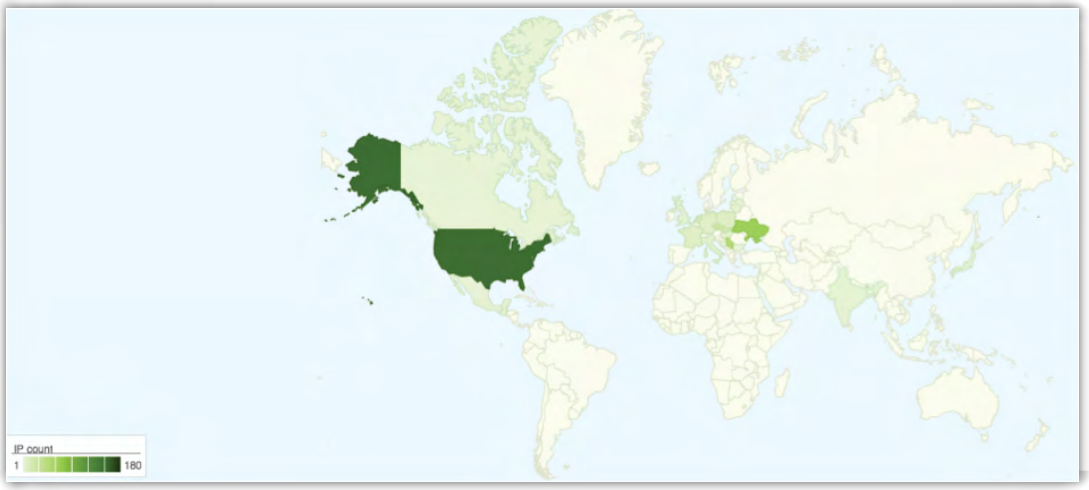
Focusing on Dyreza and UPATRE in particular, the reason for this cluster is that the UPATRE downloader has been used to spread the Dyreza malware, as described in this Threatpost Upatre Downloader[4]. Using our analysis we identify 476 IP addresses associated with both Dyreza and UPATRE. Only 41 of these addresses were known on the blacklists.

A GeoIP lookup provides the geographic distribution of these addresses, a clear dominance of which come from Eastern European countries (following the US, which tends to always be on top due to the large number of Internet/infrastructure providers operating there).

United States	180
Ukraine	77
Serbia	59
Russian Federation	35
Czech Republic	31
Slovakia	19
Netherlands	12
Poland	11
Germany	9
France	8
Hungary	6
Italy	5
Moldova, Republic of	4

[4] https://threatpost.com/upatre-downloader-spreading-dyreza-banking-trojan/109858

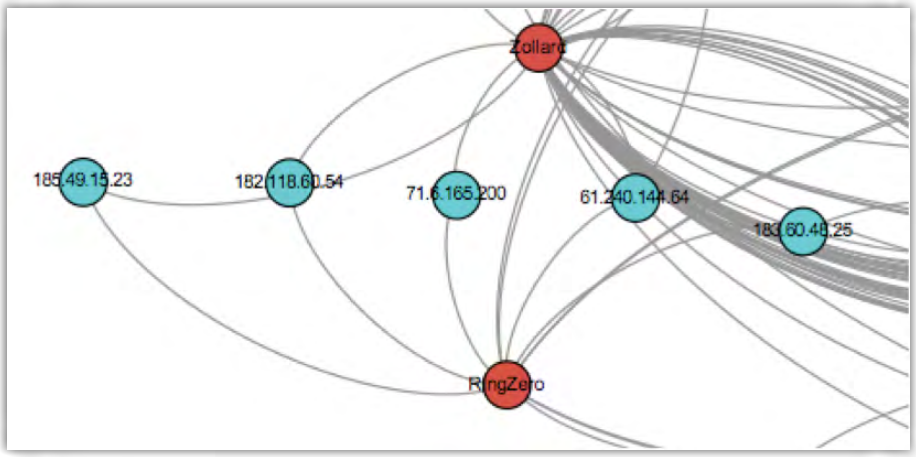
Or, viewed on a world map:



The large text overlap index tells us that these malware are somehow related, and thus the fact that they share a significant number of IP addresses comes as no surprise.

Zollard and RingZero

As a second example, we identify a small set of five IP addresses connecting the Zollard and RingZero malware; three addresses are from China, one from Poland, and one from the US:



IP address	Country	Domain	Owner
61.240.144.64	China	s1.securityresearch.360.cn	China United Network Communications Corporation Limited No.21 Financial Street,Xicheng District, Beijing 100140 ,P.R.China
183.60.48.2	China	N/A	CHINANET Guangdong province network Data Communication Division China Telecom, China Unicom Henan province network China Unicom No.21,Ji-Rong Street, Beijing 100032,China
182.118.60.54	China	hn.kd.ny.adsl	Unicom Henan Province Network
185.49.15.23	Poland	185a49b15c23.greendata.pl	Hosting services,WITRYNA.PL
71.6.165.200	United States	census12.shodan.io	CariNet, Inc.

For example, 182.118.60.54 is mentioned in a tweet:

```
https://twitter.com/HoneyPyLog/status/596020104267051008

"HyPy2: #RingZero Possible RingZero attacks from 182.118.60.54
https://t.co/FoxbjiLmz9 @threatbot"
```

and in a paste on Slexy (now removed from their site):

```
http://slexy.org/view/s21cc4dvcS

\" 500 192 \"-\" \"Mozilla/5.0 (compatible; Zollard; Linux)\".

    …

182.118.60.54 - - [03/May/2015:00:23:11 +0200] \"GET / HTTP/1.1\" 200 1652 \"-\" \"Mozilla/5.0
(Macintosh; Intel Mac OS X 10_10_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2251.0
Safari/537.36\".
```

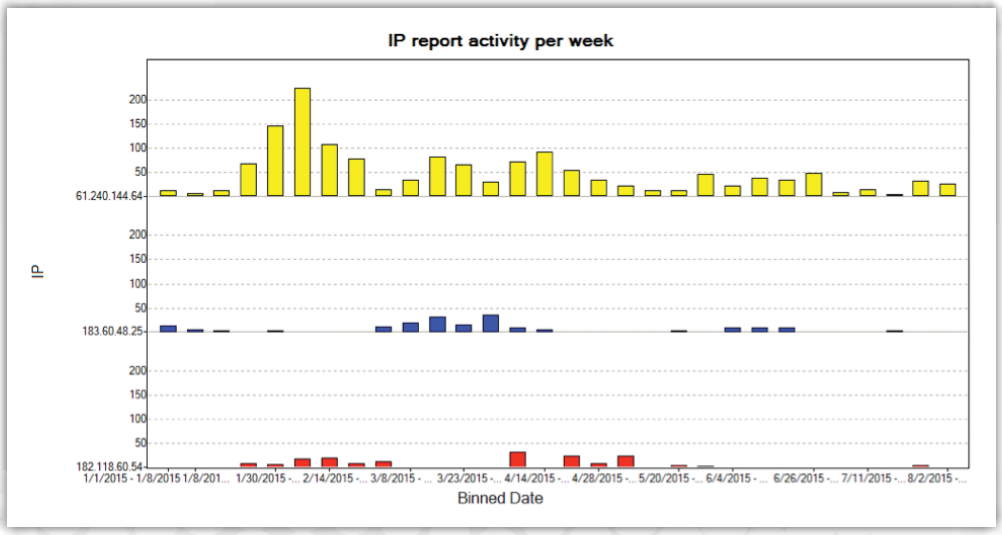
Similarly, 71.6.165.200 (census12.shodan.io) is mentioned together with Zollard on a number of Slexy pastes and in one Pastebin paste, and with RingZero in two tweets. This address has indeed been identified and blacklisted, for example, by AlienVault:

› http://www.alienvault.com/apps/rep_monitor/ip/71.6.165.200/

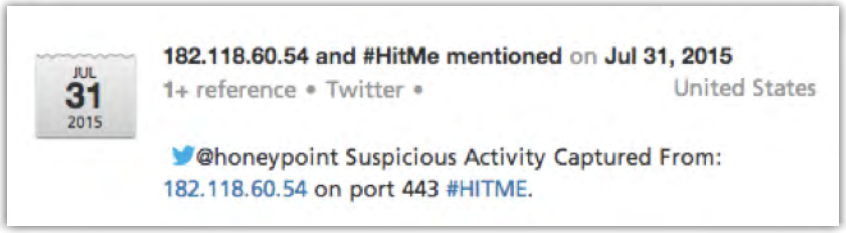
› https://isc.sans.edu/forums/diary/Looking+for+Packets+for+IP+address+716165200/17507/

In this case, the text overlap index is zero – these two malware have never been mentioned together in documents in our index. The hidden links between the malware are through the IP addresses to which they both relate.

The Recorded Future index allows us to plot the number of reports per day during 2015 for each of the three Chinese IP addresses. The complementary report activity level between 183.60.48.2 and 182.118.60.54 stands out in the viualization below, and indicates that they might be alternative infrastructures used by the same actor.

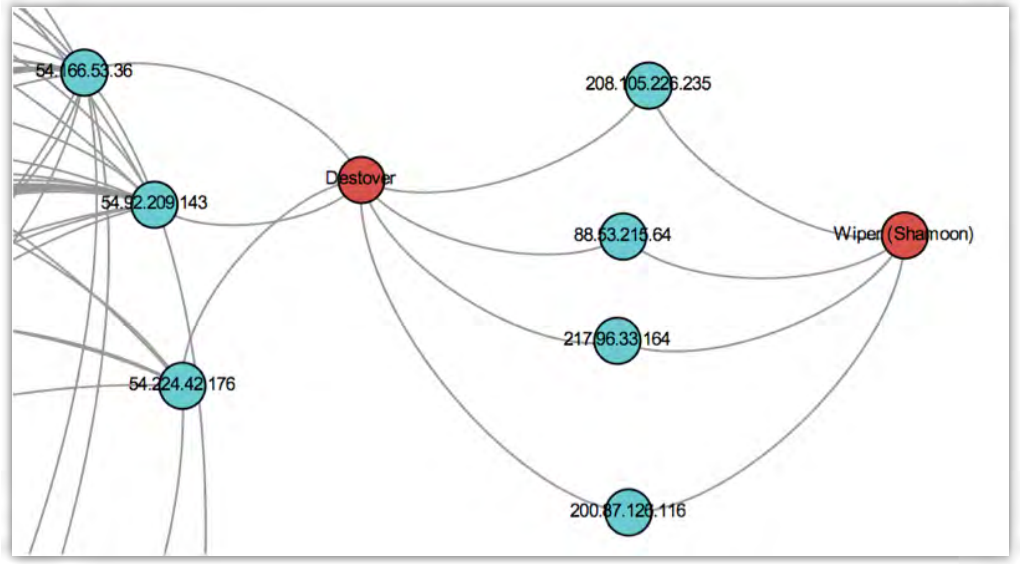


As seen above, report activity peaked for these three addresses during February, March, and April. Reports related to 182.118.60.54 have all but disappeared recently; there might be a small, recent increase in the number of reports related to 61.240.144.64. Interestingly, 182.118.60.54 does not appear on the blacklists any time in the time interval 2015-06-01 – 2015-08-02, despite a honeypot report on 2015-07-31:



Destover and Wiper / Shamoon

The next example involves Destover and Wiper/Shamoon, which we find to be related by four IP addresses:



208.105.226.235 United States
rrcs-208-105-226-235.nys.biz.rr.com
Time Warner Cable Internet LLC

200.87.126.116 Bolivia
NO_REVERSE_DOMAIN
Entel S.A. - EntelNet

88.53.215.64 Italy
88-53-215-64.wdsl.neomedia.it
NEOMEDIA SRL,INTERBUSINESS

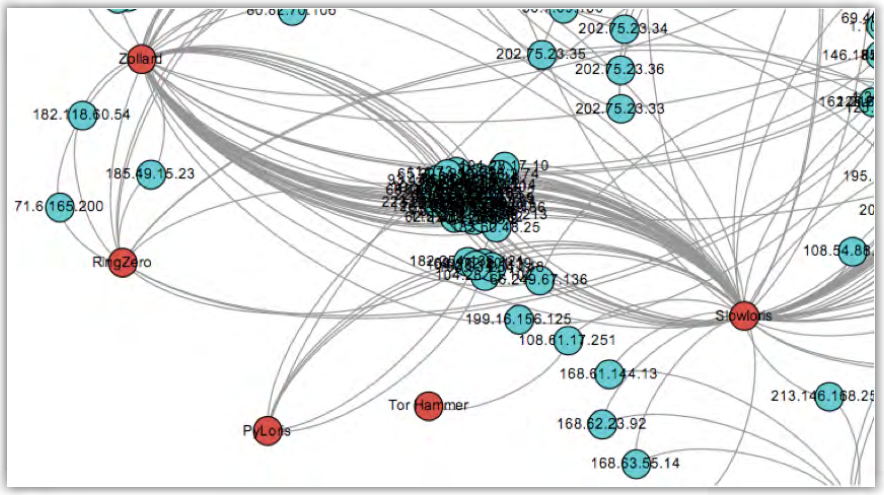
217.96.33.164 Poland
NO_REVERSE_DOMAIN
INTER-PARTS IMPORT EKSPORT WALDEMAR BACLAWSKI UL. JARZEBINOWA
4 11-034 STAWIGUDA,TPNET for abuse: abuse@tpnet.pl

For example, 208.105.226.235 is related to Destover and described as a command and control server by Kaspersky[5], whereas several Facebook posts also relate it to Shamoon.

These malware do co-occur in both fragments and documents, but our analysis confirms that there are also separate reports on their relationships to some IPs.

Zollard and Slowloris

The malware pair Zollard and Slowloris is one such pair with the highest shared IP count (36), but with no fragment or document co-occurrence.



There are 37 shared IPs, with the following geographic distribution:

United States	14
China	6
France	3
Thailand	3
India	2
Taiwan	2
Turkey	1
Brazil	1
Netherlands	1
Singapore	1
Mexico	1
Germany	1
Chile	1

Four of the IPs occur on the blacklists, and 33 are unknown.

As an example, the IP 107.22.163.227 is mentioned together with Slowloris in a PasteBin document[7], and with Zollard in a Slexy paste[8].

[5] https://securelist.com/blog/security-policies/68073/destover-malware-now-digitally-signed-by-sony-certificates/
[6] https://www.facebook.com/1102728606/posts/10205316581289693
[7] http://pastebin.com/K4ecdw8J, now removed.
[8] http://slexy.org/view/s209vfBS8v, also removed.

Below is the entire list of IP addresses involved:

107.22.163.227 United States
ec2-107-22-163-227.compute-1.amazonaws.com
Amazon.com, Inc.

123.151.149.222 China
NO_REVERSE_DOMAIN
HAOWEIGAOKE-LTD TIANJIN CITY

203.158.167.2 Thailand
NO_REVERSE_DOMAIN
Rajamangala Institute of Technology Institute of Information Technology RIT

69.174.245.163 United States
NO_REVERSE_DOMAIN
ServerBeach

65.196.87.161 United States
NO_REVERSE_DOMAIN
CURTIS CIRCULATION COMPANY,MCI Communications Services, Inc.

65.207.23.201 United States
NO_REVERSE_DOMAIN
MCI Communications Services, Inc. d/b/a Verizon Business

128.199.235.176 Singapore
NO_REVERSE_DOMAIN
DigitalOcean Cloud

213.61.149.100 Germany
h-213.61.149.100.host.de.colt.net
SOPRADO GmbH,COLT TECHNOLOGIES

218.56.65.202 China
NO_REVERSE_DOMAIN
China Unicom Shandong province network China Unicom,CNC Group

162.253.66.76 United States
NO_REVERSE_DOMAIN
Garrison Network Solutions LLC,DataWagon LLC

46.105.110.43 France
ns222609.ovh.net
OVH SAS Dedicated servers http://www.ovh.com,OVH ISP Paris, France

115.239.253.11 China
NO_REVERSE_DOMAIN
Ninbo LanZhong Network Co. Ltd.

183.60.48.25 China
NO_REVERSE_DOMAIN
CHINANET Guangdong province network Data Communication Div. China Telecom

67.215.248.8 United States
unassigned.quadranet.com
Secured Private Network

218.108.85.213 China
NO_REVERSE_DOMAIN
WASU TV & Communication Holding Co.,Ltd. 6/F, Jian Gong Building, NO.20 Wen San Road, Hangzhou, Zhejiang province, P.R.China 310012

208.43.71.114 United States
208.43.71.114-static.reverse.softlayer.com
SoftLayer Technologies Inc.

50.22.75.14 United States
test.hostnext.net
SoftLayer Technologies Inc.

62.210.141.58 France
62-210-141-58.rev.poneytelecom.eu
IP Pool for Iliad-Entreprises Business Hosting Customers,Online SAS Paris, France

69.16.238.213 United States
host.acceptprint.com
Liquid Web, Inc.

146.83.216.186 Chile
mece5.inf.uach.cl
Red Universitaria Nacional

185.4.227.194 Turkey
185-4-227-194.turkrdns.com
Istanbul DC Customer,sayfa.NET Istanbul

162.213.24.36 United States
starexserv.com
VolumeDrive

220.128.121.83 Taiwan
220-128-121-83.HINET-IP.hinet.net
CHTD, Chunghwa Telecom Co.,Ltd. Data-Bldg.6F, No.21, Sec.21, Hsin-Yi Rd. Taipei Taiwan 100

223.27.230.174 Thailand
NO_REVERSE_DOMAIN
IDC Beenet

200.98.68.101 Brazil
lojameuauto.com.br
Universo Online S.A.

202.53.8.82 India
mail.report.beamtele.com
Core Infra DNS, Web, Mail, KVM, Database,This route object is for Beam Cable Hyderabad

122.154.46.139 Thailand
NO_REVERSE_DOMAIN
490/1 Petchakaserm Road Hadyai Songkhla 90110 ***send spam abuse to kphariny@cattelecom.co.th***

76.164.201.201 United States
76-164-201.unassigned.userdns.com
Versaweb, LLC

74.63.199.120 United States
mx666.auonline.com.au
Limestone Networks, Inc.

115.254.9.30 India
srap.edst.ibm.com
RCOM-Static-DIA

140.128.85.2 Taiwan
www.rsm.ncut.edu.tw
imported inetnum object for MOEC

93.174.94.137 Netherlands
93-174-94-137.constellationservers.net
ECATEL LTD Dedicated servers http://www.ecatel.net/,AS29073

71.86.48.83 United States
71-86-48-83.static.stls.mo.charter.com
Charter Communications

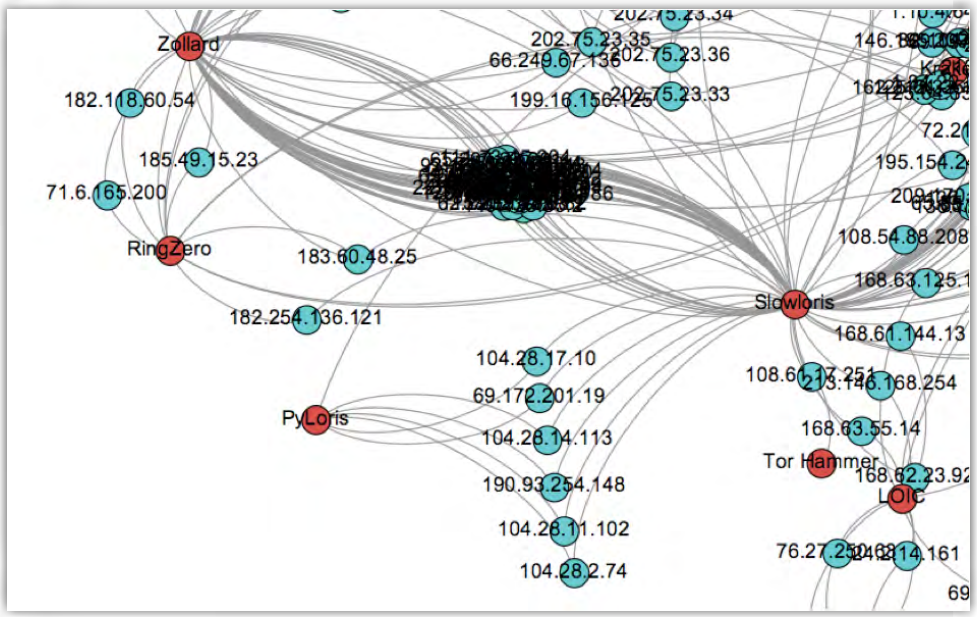
91.121.90.166 France
ns319885.ip-91-121-90.eu
OVH SAS Dedicated Servers http://www.ovh.com,OVH ISP Paris, France

201.161.37.93 Mexico
201-161-37-93.internetmax.maxcom.net.mx
Maxcom Telecomunicaciones, S.A.B. de C.V.

111.73.45.204 China
NO_REVERSE_DOMAIN
CHINANET JIANGXI PROVINCE NETWORK China Telecom No.31

Slowloris and RingZero

These two malware are only related by two IP addresses:



183.60.48.25 B China
NO_REVERSE_DOMAIN
CHINANET Guangdong province network Data Communication Division China Telecom

182.254.136.121 U China
NO_REVERSE_DOMAIN
Tencent cloud computing (Beijing) Co., Ltd. Floor 6, Yinke Building,38 Haidian St, Haidian District Beijing,Tencent Cloud Computing

The first address, 183.60.48.25, is already present on blacklists[9] and is listed by AlienVault[10] as "previously malicious." Note that this address is also associated with the Zollard malware in the graph above.

A honeypot tweet shows that the second IP address, 182.254.136.121, is possibly related to RingZero[11]:

[9] https://www.packetmail.net/iprep.txt
[10] https://www.alienvault.com/open-threat-exchange/ip/183.60.48.25
[11] https://twitter.com/HoneyPyLog/status/553900065417211904

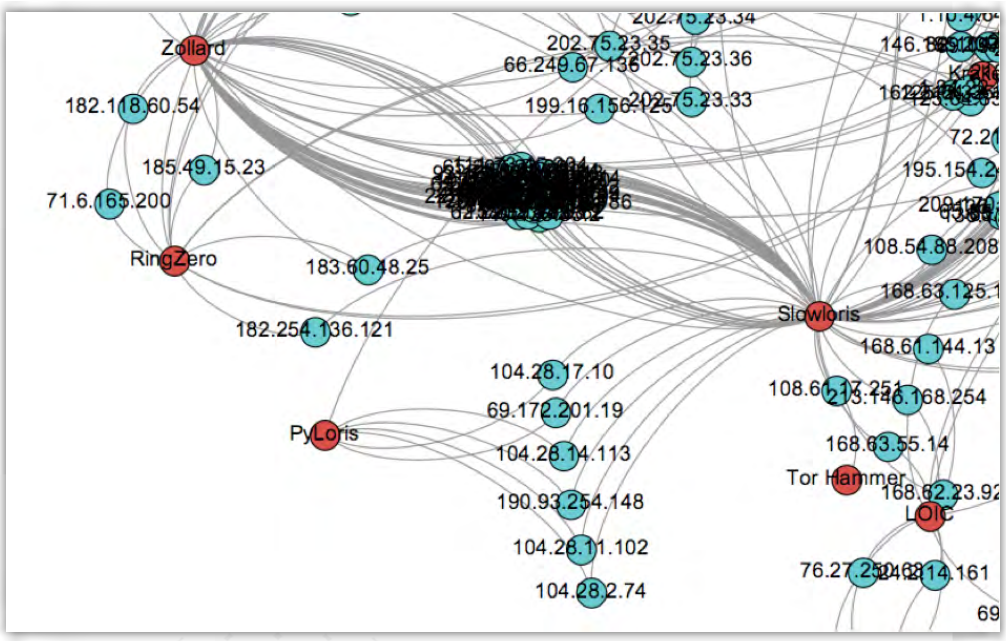
and a Pastebin post, now deleted, shows that it may be related to Slowloris[12] through a paste:

```
"110.164.58.184 /* zologize */" : 1,
"171.211.13.160 /* HNAP1 */" : 1,
"122.195.244.42 /* Serverinfo.jsp */" : 1,
"24.135.54.109 /* SlowLoris */" : 1,
"200.8.99.12 /* zologize */" : 1,
"78.160.1.89 /* wp-login.php */" : 1,
"2.180.21.24 /* wp-login.php */" : 1,
"182.254.136.121 /* SlowLoris */" : 1,
"5.153.130.3 /* wp-login.php */" : 1,
"58.177.86.10 /* zologize */" : 1,
"130.211.186.170 /* SlowLoris */" : 1,
"188.117.151.186 /* wp-login.php */" : 1,
"31.172.30.4 /* wp-login.php */" : 1,
"46.41.199.204 /* wp-login.php */" : 1,
```

Even if it is a small set of only two identified IP addresses, this could be a starting point for looking for a shared, malicious infrastructure.

Slowloris and PyLoris

PyLoris is a Python implementation of Slowloris, and one might have expected them to share some IP addresses, but actually there are only six addresses they have in common, five of which are owned by CloudFlare:



[12] http://pastebin.com/K4ecdw8J, now deleted.

104.28.2.74	United States
NO_REVERSE_DOMAIN	CloudFlare, Inc.
190.93.254.148	Costa Rica
NO_REVERSE_DOMAIN	CloudFlare Latin America S.R.L
69.172.201.19	United States
NO_REVERSE_DOMAIN	DosArrest,Peer 1 Network (USA) Inc.
104.28.17.10	United States
NO_REVERSE_DOMAIN	CloudFlare, Inc.
104.28.11.102	United States
NO_REVERSE_DOMAIN	CloudFlare, Inc.
104.28.14.113	United States
NO_REVERSE_DOMAIN	CloudFlare, Inc.

The last of these addresses has been related to malicious activity, but not as malicious but identified as a target -- another useful piece of information obtainable by our methodology:

#Target http://www.shahamat-urdu.com 104.28.14.113 #TangoDown.

(from the tweet https://twitter.com/LadyPatriot777/status/554391656317734912 , now remowed from Twitter)

Other reported activities on this IP address can be seen on https://www.virustotal.com/en/ip-address/104.28.14.113/information/

The address 104.28.14.113 was identified as a target in the #OpCharlieHebdo, and listed in http://pastebin.com/tv7AxP5b :

1. TARGETS
2. =======
3. Don't dos these targets. Dump their databases, and deface it.
4.
5. http://www.cyberislamicnews.co.vu/
6. http://alfaransy.olympe.in/
7. http://www.chechensinsyria.com/
8. https://ansarukhilafah.wordpress.com/
9. http://aljileni.blogspot.de/2015/01/blog-post_10.html
10. http://www.anjemchoudary.co.uk/ Apache Server
11. https://www.dawla-is.cf cloudflare - find real ip
12. http://khelafa.org/
13. http://www.uicforce.co.vu/
14. http://issdarat.appspot.com/
15. http://shahamat-arabic.com/ 104.28.17.10
    http://pastebin.com/4GwJUq6x

16. http://shahamat-urdu.com 104.28.14.113
    http://pastebin.com/nFTaat5b
17. http://shahamat-farsi.com 104.28.11.102
    http://pastebin.com/NNcndY8v
18. http://shahamat-english.com/ 104.28.2.74
    http://pastebin.com/4YW9JMT1
19. http://www.profetensummah.com/
20. http://www.atahadii.com/
21. http://www.dawatehaq.info
22. https://isdarat-tube.com

The Pastebin document[13] referenced above (now deleted from Pastebin but cached by Recorded Future) shows us that address was scanned:

NMAP SCAN : http://shahamat-urdu.com
Starting Nmap 6.47 (http://nmap.org) at 2015-01-10 14:05 West-Europa (standaardtijd)
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 14:05
Scanning 104.28.14.113 [4 ports]
Completed Ping Scan at 14:05, 0.29s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:05
Completed Parallel DNS resolution of 1 host. at 14:05, 0.02s elapsed
Initiating SYN Stealth Scan at 14:05
Scanning 104.28.14.113 [1000 ports]
Discovered open port 8080/tcp on 104.28.14.113
Discovered open port 80/tcp on 104.28.14.113
Discovered open port 443/tcp on 104.28.14.113

This example illustrates how Recorded Future can be used to first identify IP addresses related to malicious activity, and then explore who is planning to exploit it and what tools they use. Of course, any IP address identified as a target can later become part of a malicious infrastructure if the attack is successful and the system is taken over. As an example, another address mentioned above, 104.28.17.10 (related to http://shahamat-arabic.com/) is identified as an #OpCharlieHebdo target in Pastebin[14]. This exact address is not present on the blacklists, but two other CloudFlare addresses on the same subnet are listed by AlienVault as actively malicious: 104.28.17.109 and 104.28.17.222

[13] http://pastebin.com/nFTaat5b
[14] http://pastebin.com/RniQXzqx

Conclusion

Through a set of examples we have shown how our new method of hidden link analysis can be used to identify suspicious IP addresses and associated infrastructure. This method complements blacklists generated from intrusion detection systems, honeypots, honeynets etc. By combining information from security experts and analyst reports with information obtained from social media, hacker forums, and paste sites we are able to observe the continuously ongoing cyber battle from the perspective of both attackers and defenders, and draw conclusions about maliciousness of infrastructure that was hitherto unavailable. By incorporating this information into the Recorded Future index we can provide it to threat intelligence analysts and also feed it into SIEM systems for improved risk scoring of IP addresses. This novel approach enables threats to be detected faster and more accurately.

About Recorded Future

We arm you with real-time threat intelligence so you can proactively defend your organization against cyber attacks. With billions of indexed facts, and more added every day, our patented Web Intelligence Engine continuously analyzes the entire Web to give you unmatched insight into emerging threats. Recorded Future helps protect four of the top five companies in the world.

Recorded Future, 363 Highland Avenue, Somerville, MA 02144 USA |