IP Reputation – Splunk App

BETA 0.61

NO OFFICIAL SPLUNK PRODUCT – NO SUPPORT – USE ON YOUR OWN RISK – TEST FIRST IN PILOT ENVIORNMENT

Presented by:

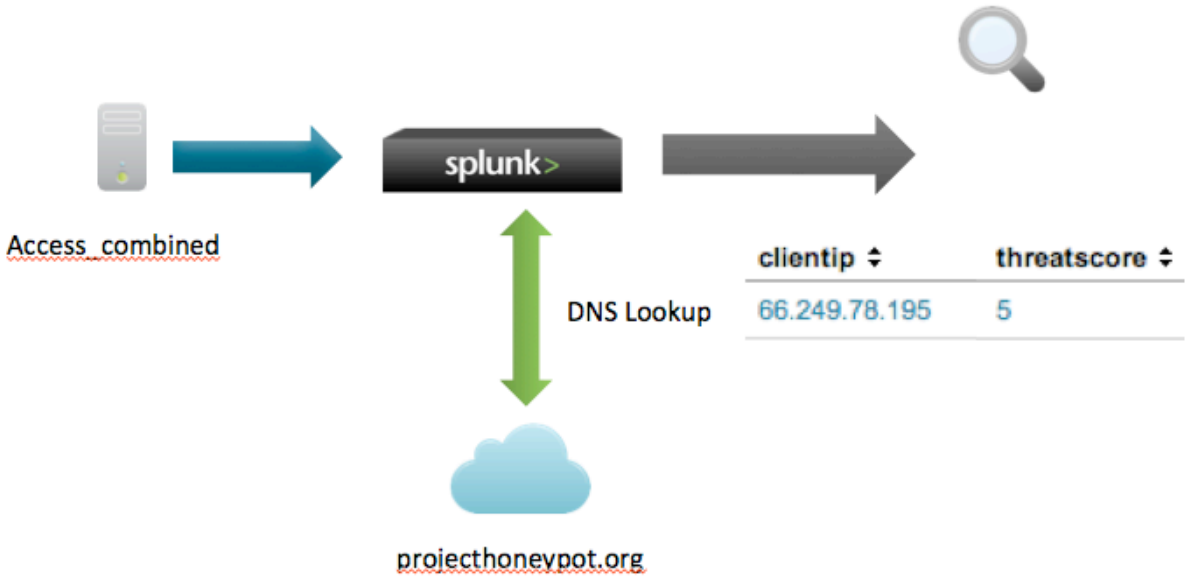
Matthias Maier

Feedback: Matthias@splunk.com

Introduction

This app gives customers the ability to correlate their realtime and historical machine data with threat data from honeypot project database to get a threat scoring of an IP. The script can be modified so that it requests from other databases (http://www.dnsbl.info/dnsbl-list.php)

Architecture



Machine Data is collected from Webservers and processed in Splunk. Splunk will perform via external lookup the score of the IP-Addresses at Project Honey Pot Database. This database monitors over 110 Million IP's, 112 Million Spam Traps and identified Millions of bad Networks and Systems. It has over 3000 harvesters who collect those data currently.

Installation

To install threat score lookup you need the following

- Splunk 5.0.2 installed and configured + Admin Access
- Google Maps App + Maxmind GEO IP
- App: IP Reputation
- http;BL authorization key

- The threat score is pulled down from the project honey pot threat intelligence database. To access this database you'll need to register for free and obtain an access code.
- https://www.projecthoneypot.org/services_overview.php

Configure http:BL Key

To have the authorization to query the Project Honey Pot database you need to add your personalized http:BL Key to the lookup scripts. For this

1. go into <Splunkinstalldir>/etc/apps/ipreputation/bin/
2. open the scorelookup.py script with an editor
3. paste your Code into the "key" value and save the script

```
39  #ip_address = '74.125.129.94'
40  key = '1234567cxccvcv'
41  DNSBL_SUFFIX = 'dnsbl.httpbl.org'
42
43  def scorelookup(clientip):
44      #print
45      #print "----------------------------------
```

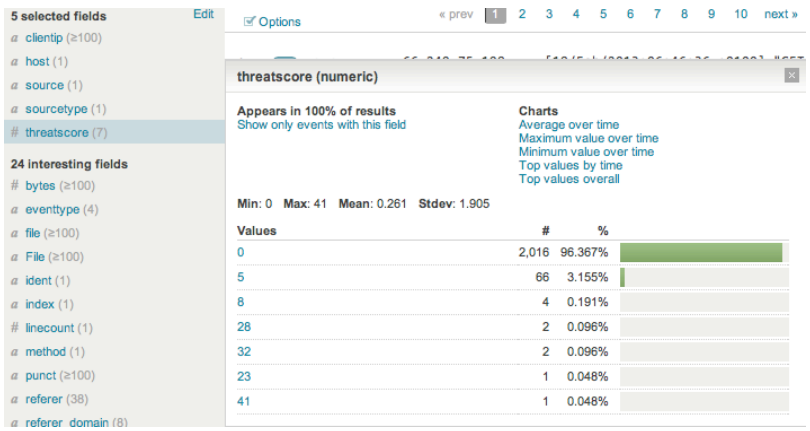
Using threatscore lookup

Go into the **Search** app and test against your webserver logs. It's recommended to group the ip's in front of the lookup to boost performance and avoid multiple lookups of the same IP.

….| lookup threatscore clientip

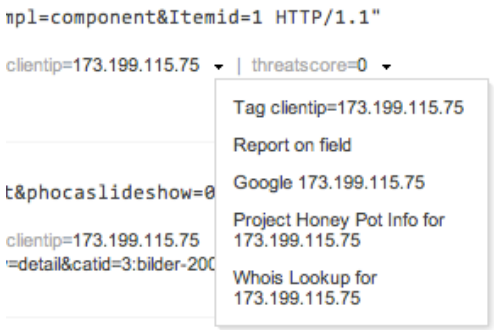
Once executed you should have a additional field called threatscore. 0 means no entry in the database or the IP is okey. A higher number means a more dangerous IP.

You can also rename your lookup field to clientip if it has another name. rename myiptag as clientip



Workflow Actions

During investigation it's possible to jump to the honeypot database to check what activity's this ip performs and gain additional Information. Also a whois lookup is often useful to review for analyses and investigation.



IP from Sweden. Active since 2 weeks, seen from over 30 different honypots. Tries to spam to guestbooks, comment fields on webpages etc.

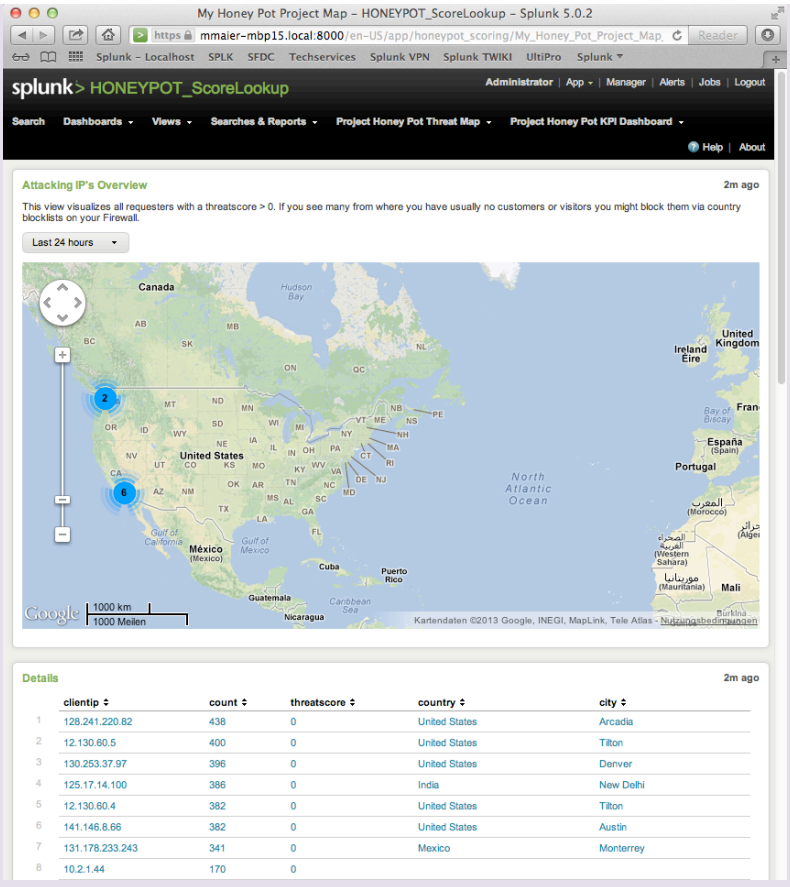
Predefinied Content: IP Reputation App

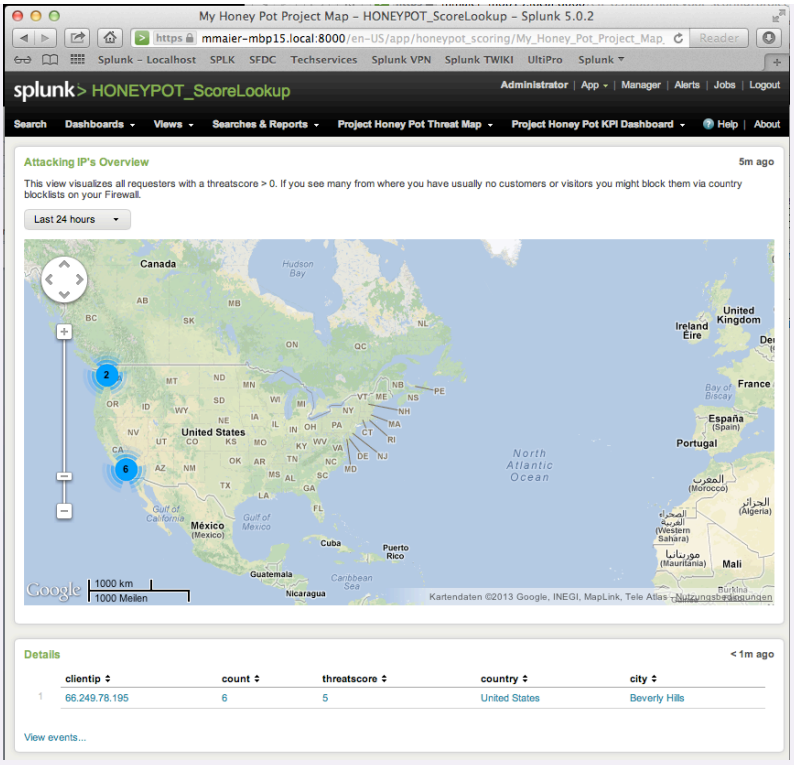
REALTIME Enrichment - App Search

If you search in the Search Window of the Honey Pot App the threat score lookup will be automatically done for every clientip field. You can limit the reports down to specific sources, indexes etc. by editing the event type “honeypot_app_events”. This event type is used in the beginning of every report/dashboard.
Be aware that those searches are a little bit slower and create a lots of DNS requests.

App Dashboard: Project Honey Pot Threat Map

This Dashboard is designed for an overview on your Beamer or Screen within in your floor ;-) and some starting point for investigation workflows

Screenshots	Worflow Step
	1. Overview of your Environment In the Google Map you can see all Events/Page Impressions from Visitors of your Website who have a higher Threat score then 0 on project honeypot database In the Details List you can see a summary of all your visitors by page impressions – you can directly drill into investigation from this to be linked into the search app.

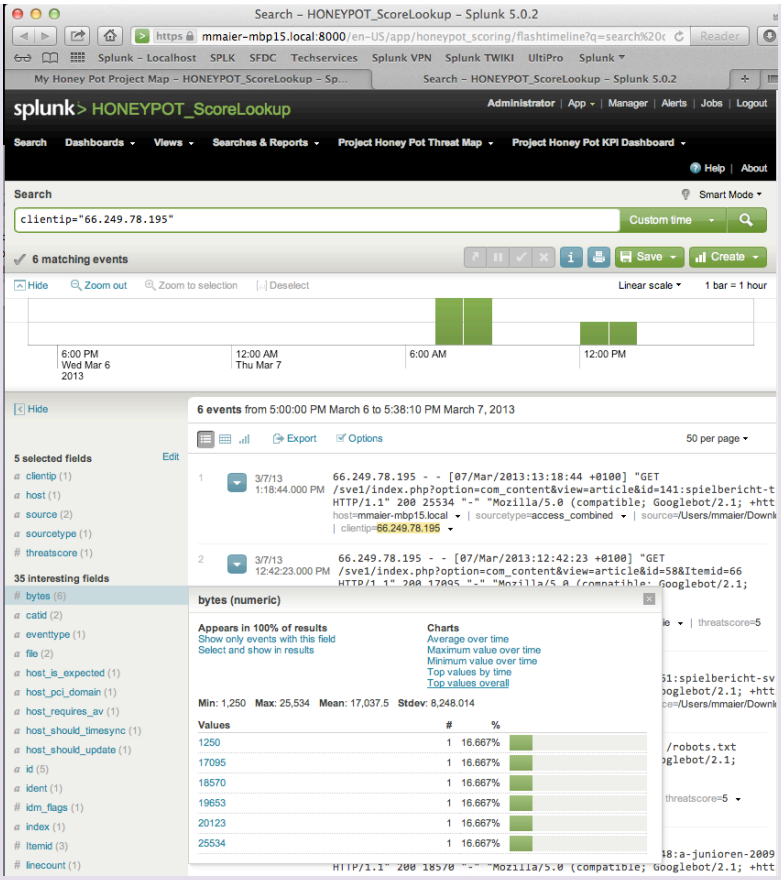


2. Drill down into interesting areas

If you see some areas where multiple events / hits have occurred you might investigate a possible attack. If you click into the Google Maps the results down will be filtered to the IP's with the associated threat score.

Looks like some famous film stars from Beverly Hills are interested in my website, but maybe their systems are infected and previously have been used to sent spam so they got a bad scoring?

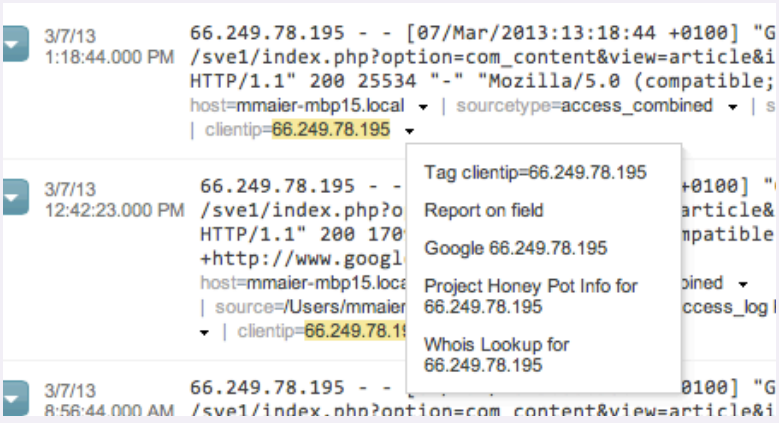
From this view click into the filtered result you want to investigate. You will be moved into the Search App



3. Review Log-Data and activities

Now you can review activities, time flow, other events from this IP-Address to learn more about this behavior.

Maybe you want to investigate how much bandwith or traffic did they use? I'll let this into your hands.



4. Workflow Lookups

Something you might want to do directly:

- Google the IP
- Review Entry Details (First seen etc.) on Honey Pot Website
- Whois Lookup
- Add a tag for "whitelisting" or "ok" after investigation to remove from dashboards

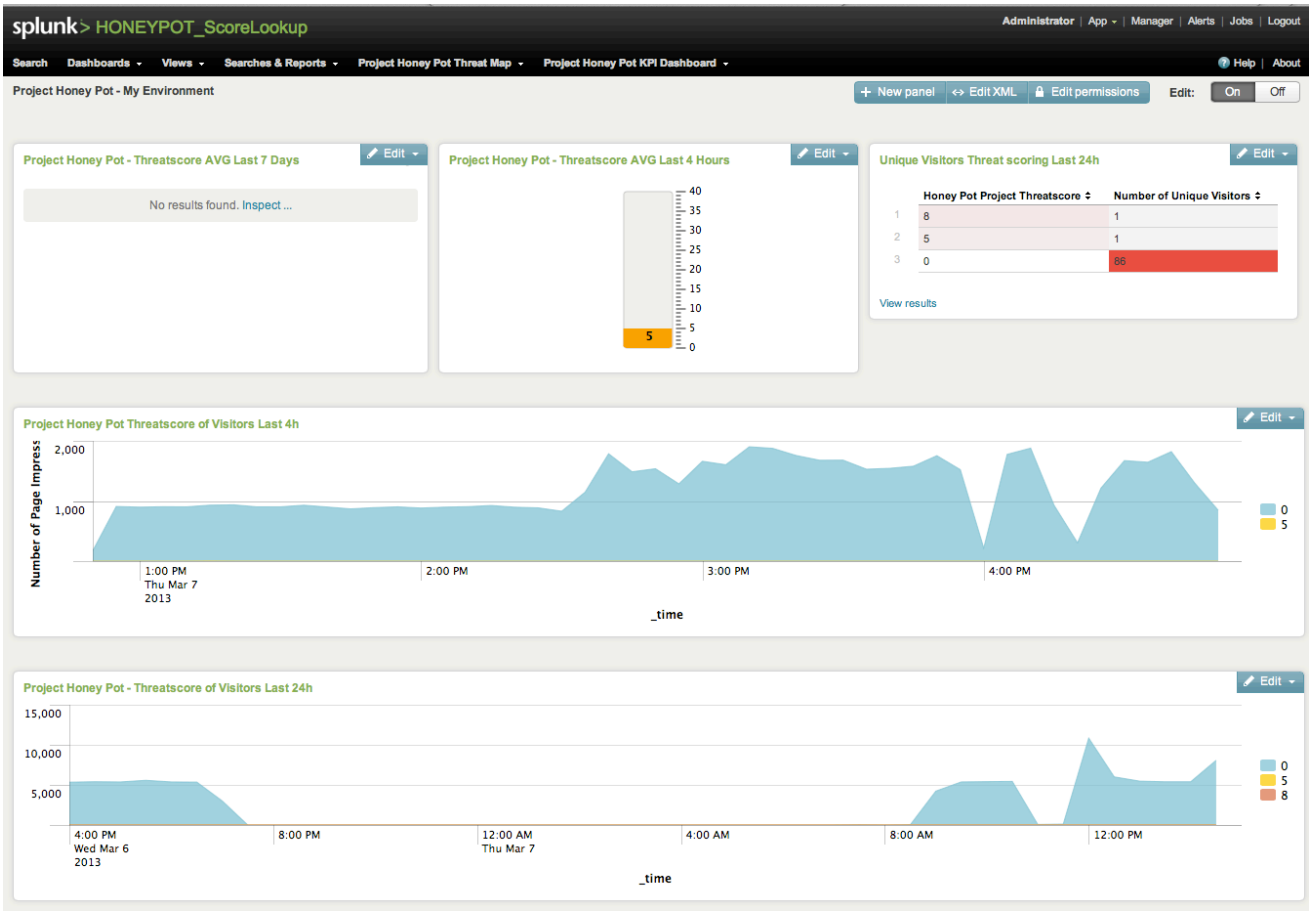
IP Information for 66.249.78.195

IP Location:	United States Mountain View Google Inc.
ASN:	AS15169 GOOGLE - Google Inc. (registered Mar 30, 2000)
Resolve Host:	crawl-66-249-78-195.googlebot.com
IP Address:	66.249.78.195 W R P D T
Whois Server	whois.arin.net

```
NetRange:       66.249.64.0 - 66.249.95.255
CIDR:           66.249.64.0/19
OriginAS:
NetName:        GOOGLE
NetHandle:      NET-66-249-64-0-1
Parent:         NET-66-0-0-0-0
NetType:        Direct Allocation
RegDate:        2004-03-05
Updated:        2012-02-24
Ref:            http://whois.arin.net/rest/net/NET-66-249-64-0-1

OrgName:        Google Inc.
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
RegDate:        2000-03-30
Updated:        2011-09-24
Ref:            http://whois.arin.net/rest/org/GOGL

OrgAbuseHandle: ZG39-ARIN
OrgAbuseName:   Google Inc
OrgAbusePhone:  +1-650-253-0000
OrgAbuseEmail:  arin-contact@google.com
OrgAbuseRef:    http://whois.arin.net/rest/poc/ZG39-ARIN

OrgTechHandle: ZG39-ARIN
OrgTechName:   Google Inc
OrgTechPhone:  +1-650-253-0000
OrgTechEmail:  arin-contact@google.com
OrgTechRef:    http://whois.arin.net/rest/poc/ZG39-ARIN
```

No further actions on this required. It's a google IP-Address which is crawling my website… but usually the search engine IP's have a very good reputation to allow them through firewalls etc. Google should investigate what's going wrong with this one.

App Dashboard: Project Honey Pot Threat Map



Scoring DATA at REST Usage (by default disabled):

If you can't use in your environment real-time enrichment because it would generate too much DNS traffic you can also use the data at rest. All lookups that are done are stored with Timestamp, source_ip and threatscore in the bin directory of the app as score_lookup_log.txt.

2013-03-08 12:47:33 source_ip=94.229.0.20,hist_threatscore=0
2013-03-08 12:47:33 source_ip=94.229.0.21,hist_threatscore=0
2013-03-08 12:47:33 source_ip=212.77.163.111,hist_threatscore=0
2013-03-08 12:47:33 source_ip=66.249.78.195,hist_threatscore=5

During installatio of the app this file will be added to your inputs for monitoring. You can search through those data with sourcetype="Honey_Pot_Scorelookup_Log".

If you schedule a report which performs the lookups once a hour from the past hour or so you can use those data for your reports, scoring etc. as it will be faster than doing a enrichment via dns in real-time. But be aware that reports

might reflect old scores who have changed in the mean time. You can optimize your own reports with commands like first(source_ip) to get the most recent score locally.

To activate remove comments in line 35,89,90,137