Raw_Cyber_Threat_Intelligence

by https://intelbyarvind.weebly.com/

Make use of "Ajna" - Google Powered Search Engine to Explore your R&A

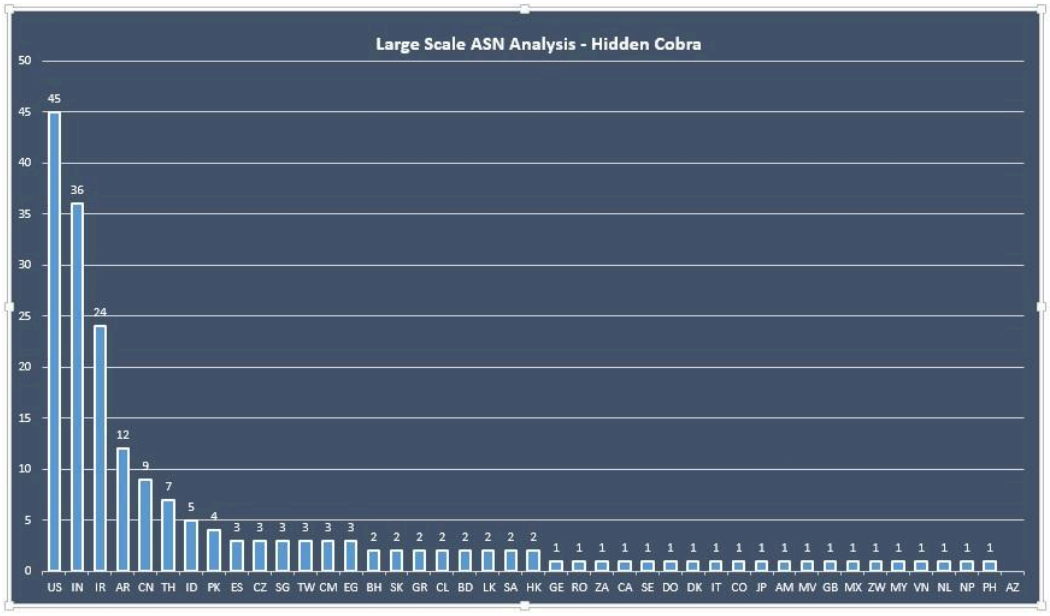
Make use of "CERT_Alerts_Advisories_News" to search real time Global CERT alerts

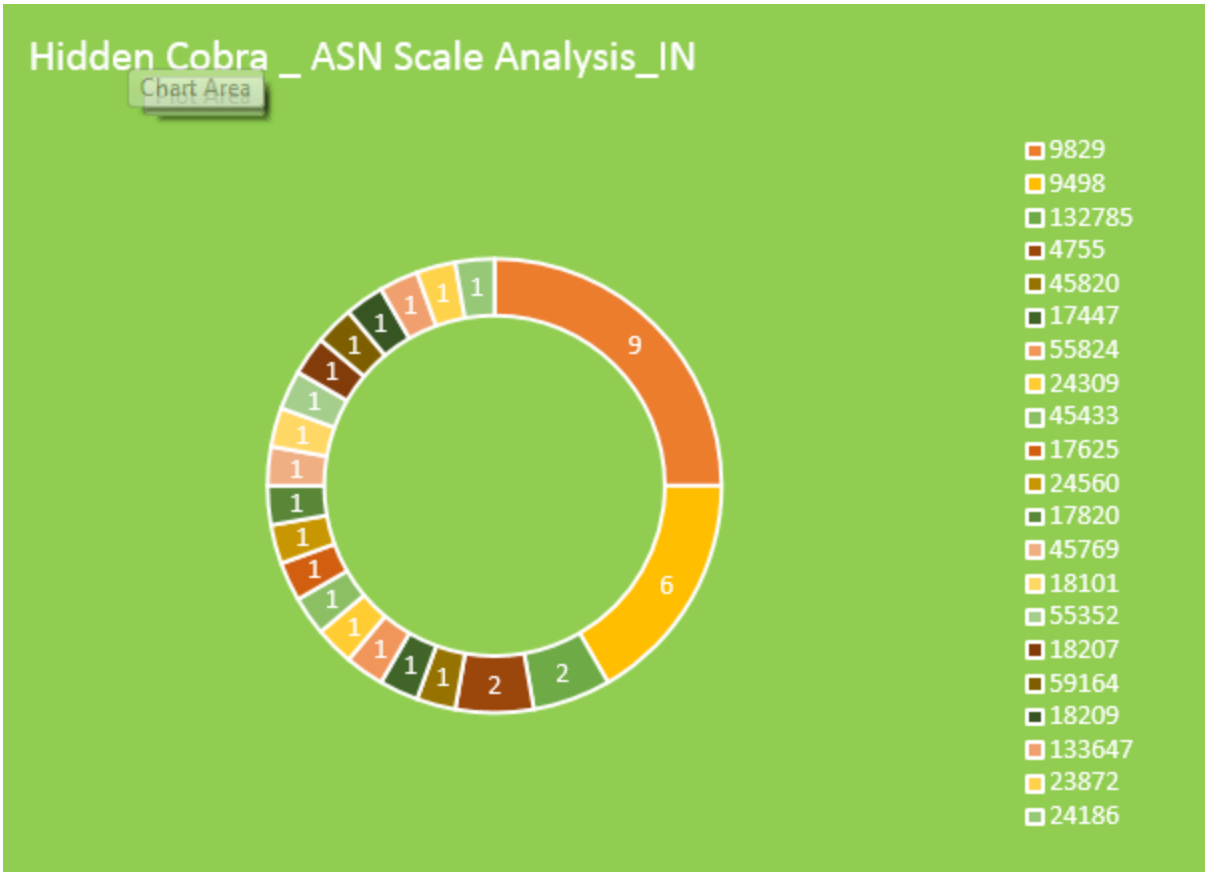
Note*: Please handle with care as the Indicators are potentially riskier by nature.

1. Suspected Campaign : Fin7 campaign (Carbanak)
   IOC_ip : 31.41.41(.)41
   IOC_ssl : 3c1be466ef7af021161f2ce1d714ad4b9417973a
   Ref: https://www.threatminer.org/ssl.php?q=3c1be466ef7af021161f2ce1d714ad4b9417973a
   https://actortrackr.com/report/view/6ac2969d-bab1-451b-946e-bbf9a914db81/
   https://exchange.xforce.ibmcloud.com/ip/31.41.41.41

2. Interesting indicator : BA8C717088A00999F08984408D0C5288
   IOC_Domains : *Static.revenyou(.)com and srv.desk-top-app(.)info*
   Large Scale Infrastructure:
   https://www.virustotal.com/graph/g9ddace6a2551a3813546fe92bac0da80276978c6ea00533a4a6a94b2192389e5

3. Large Scale Analysis of Hidden Cobra Infrastructure :


Large Scale ASN Analysis - Hidden Cobra
50
45
40
35
30
25
20
15
10
5
0
45
36
24
12
9
7
5
4
3 3 3 3 3 3
2 2 2 2 2 2 2 2
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
US IN IR AR CN TH ID PK ES CZ SG TW CM EG BH SK GR CL BD LK SA HK GE RO ZA CA SE DO DK IT CO JP AM MV GB MX ZW MY VN NL NP PH AZ


Hidden Cobra _ ASN Scale Analysis_IN
Chart Area
Plot Area
9
6
2
2
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
9829
9498
132785
4755
45820
17447
55824
24309
45433
17625
24560
17820
45769
18101
55352
18207
59164
18209
133647
23872
24186

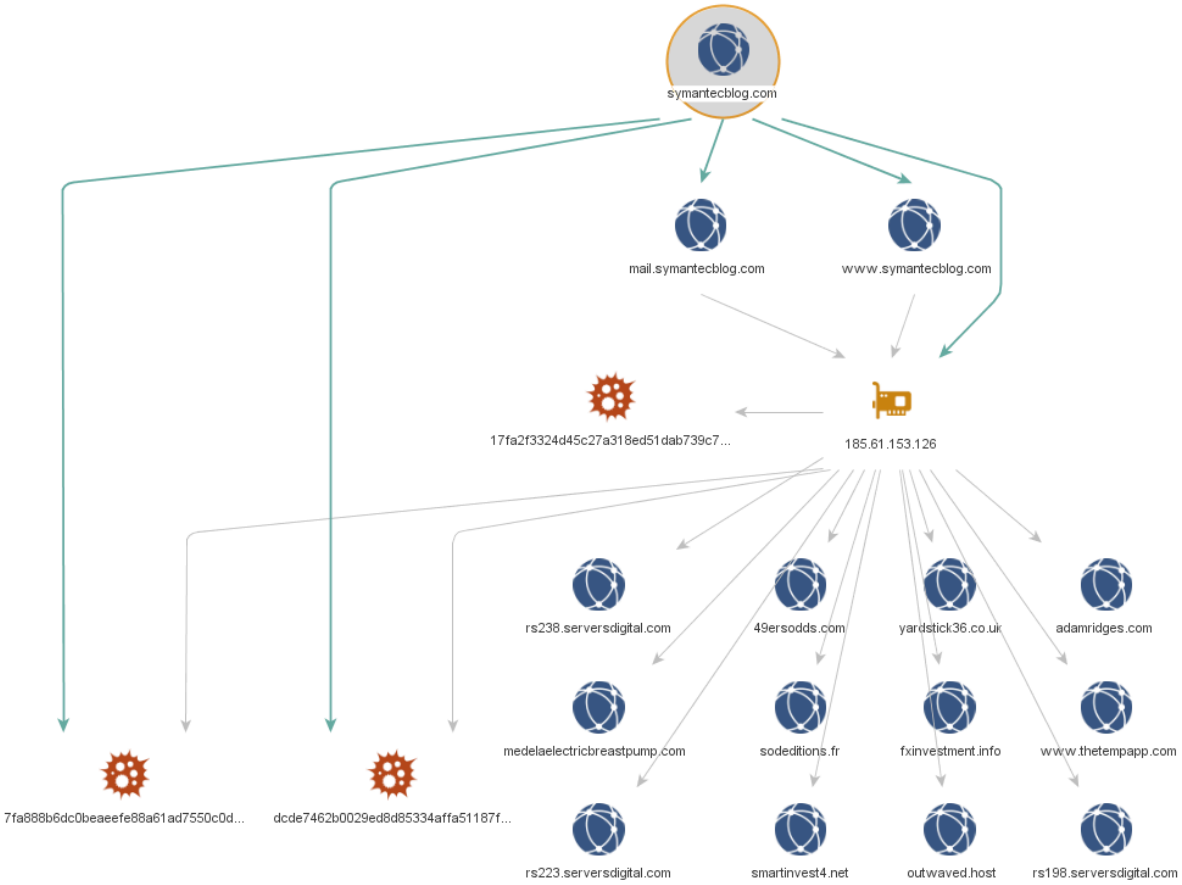
4. Interesting binary:
IOC_Hash : 7a453ad57ab88e0d72fdf7b0366719e8
Embedded Object : d55c71a9fe8065e76f0fc249c33f88d4

5. Fin7:
IOC_Hash :
a1d752f39045f7553300eb010d3ad31d
2fc68005d719e8a25566d05655a22f88
a00ae556a61907d43332449169c88844
768165e0abf16bf3056836d5431a7296
5bb66a5e9a7f6c76325a55b7a4a3128fc8631805676bbd3315ce2ac04ac2937b

IOC_IP:
85.93.2.148
hxtp://185.156.0.74/.update
htXp://185.156.0.74/min2.tar.gz

6. Ioc_Domain : hotmial.com ?

7. Fake Symantec website :
IOC_Domain : symantecblog.com


symantecblog.com
mail.symantecblog.com
www.symantecblog.com
17fa2f3324d45c27a318ed51dab739c7...
185.61.153.126
rs238.serversdigital.com
49ersodds.com
yardstick36.co.uk
adamridges.com
medelaelectricbreastpump.com
sodeditions.fr
fxinvestment.info
www.thetempapp.com
7fa888b6dc0beaeefe88a61ad7550c0d...
dcde7462b0029ed8d85334affa51187f...
rs223.serversdigital.com
smartinvest4.net
outwaved.host
rs198.serversdigital.com