MENA
INFORMATION SECURITY
CONFERENCE 2018

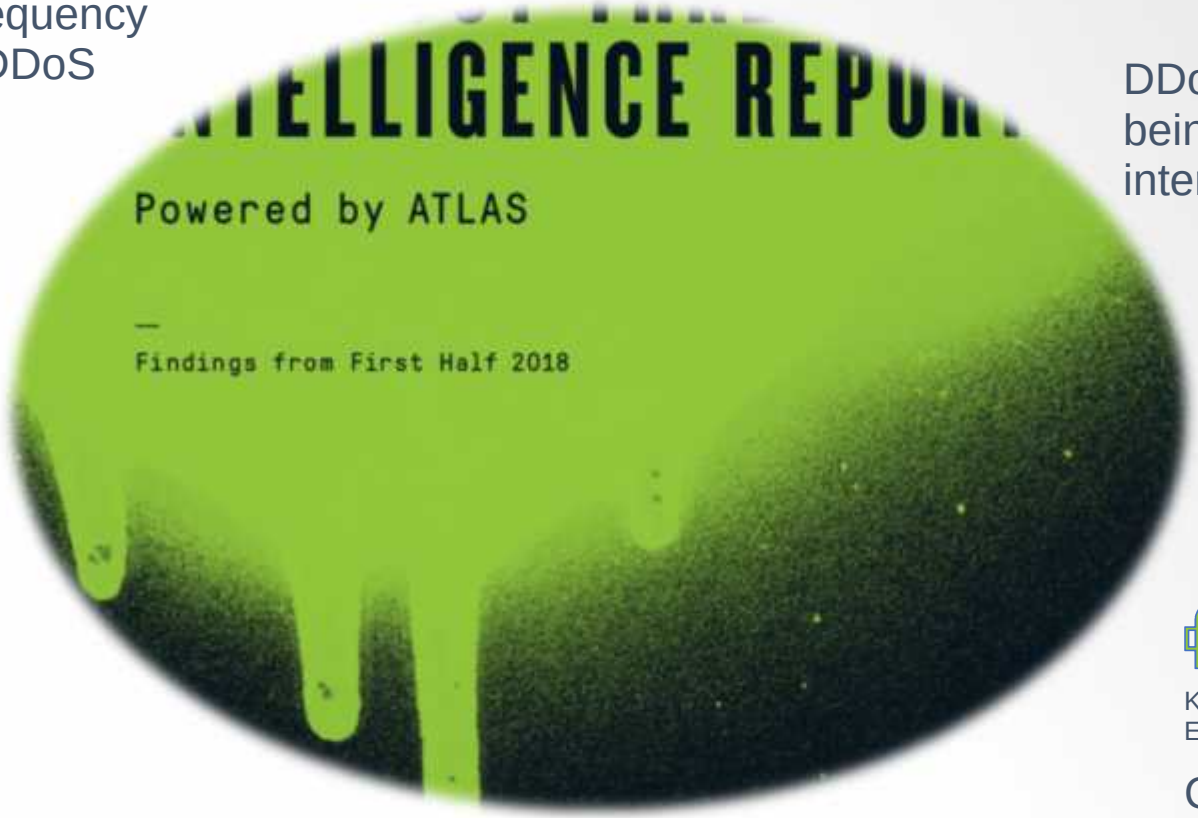
Leveraging Machine Learning &
AI in Cyber Defense

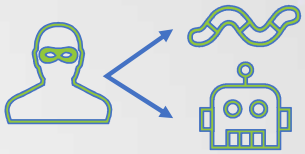
Threat Intelligence – Highlights from 1H 2018

Richard Wray
NETSCOUT|Arbor : Sr. Director, Presales EMEA

VIRTUPORT
@VirtuPortMEA
www.menaisc.com

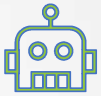
Big jump in frequency of very large DDoS attacks since Memcached.





DDoS tactics being used for internal intrusions

More nation states adding APT to their statecraft.



Kardon Loader, Panda Banker, Emotet, Trickbot;

Crimeware becomes Internet Scale

MENA INFORMATION SECURITY CONFERENCE 2018

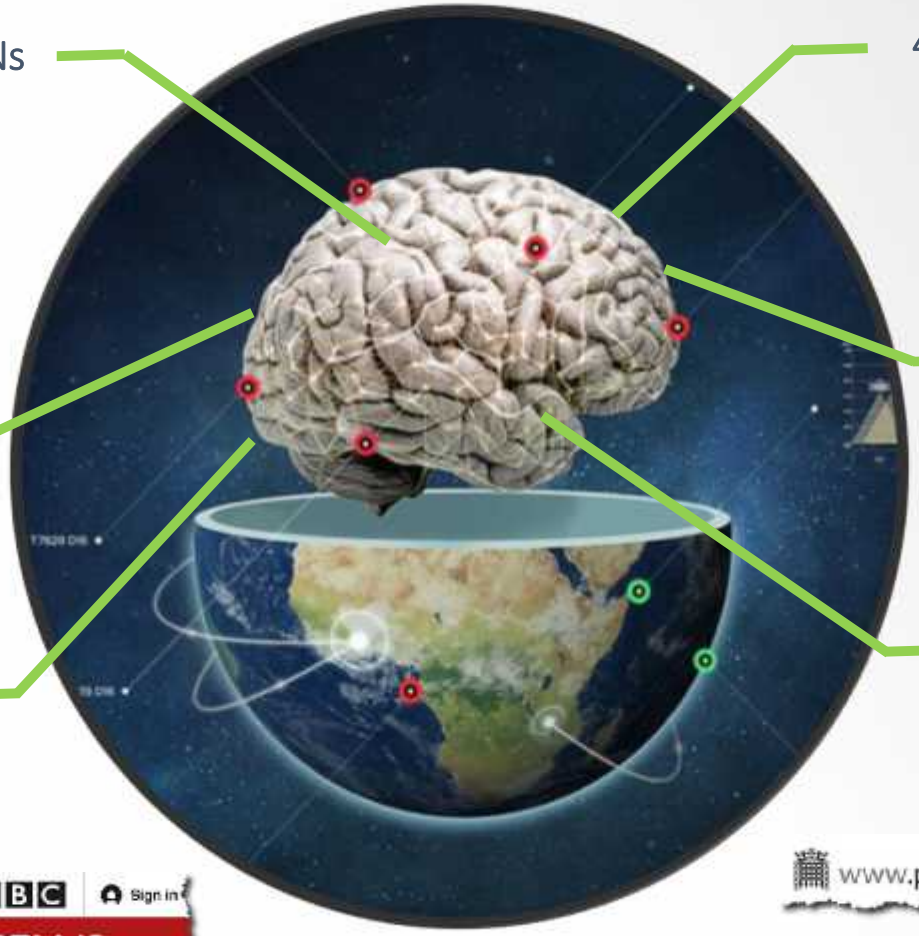
Arbor Threat Level Analysis System - ATLAS

44,570+ ASNs

420+ Active SP Contributors

WIRED

THE WALL STREET JOURNAL.



Sees 1/3rd of All Internet Traffic

2.63B Unique IPv4 Addresses

CNN

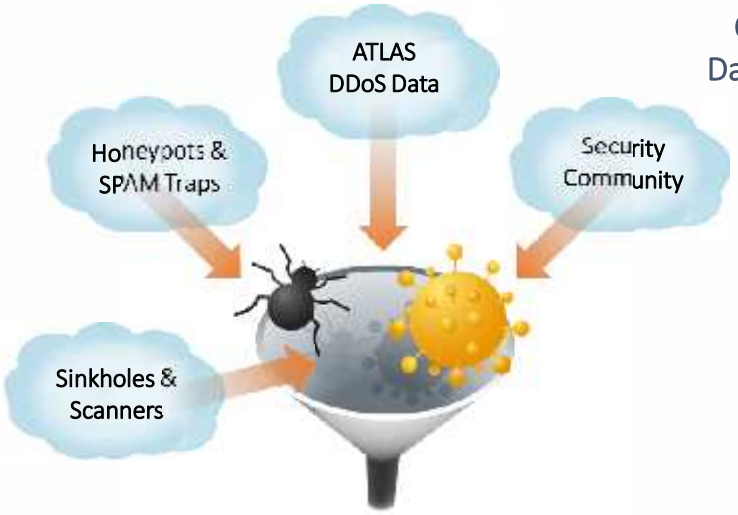
Peak Ingestion of anonymised meta data represents 140Tbps Of Internet Traffic

10 Years of Historical Data

MENA INFORMATION SECURITY CONFERENCE 2018

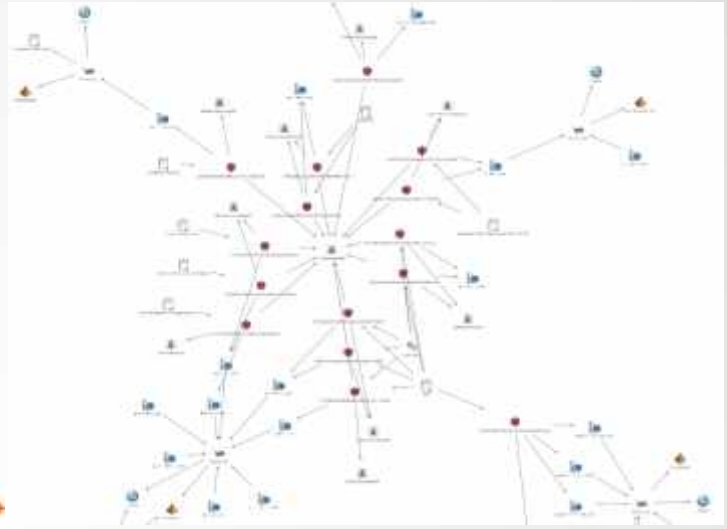
BBC NEWS

www.parliament.uk



Over 20 malware sharing partners
Data Sharing with 70% National CERTs

200,000+
Malware
samples/day



Large scale & highly customized sandbox and analysis suite

Reports and PCAP stored in database

Real time auto-classification and analysis

Hand crafted contextual enrichment of data

Numerous Outputs

Blogs, Twitter, Feeds, Threat Briefs
Threat Reports, 4th Level Support, Consultancy

MENA INFORMATION SECURITY CONFERENCE 2018

APT groups expand beyond traditional arenas

- Campaigns and frameworks are discovered for a broad tier of nations

OilRig (Iran)

Fancy Bear (Russia)
Berserk Bear
Voodoo Bear
Cozy Bear

Hidden Cobra (North Korea)

Ocean Lotus (Vietnam)

Donot Team

Crimeware actors diversify attack methods

- Inspired by large-scale attacks in 2017, many known crimeware families have included auto-propagation (worm) techniques
  - Emotet
  - Trickbot
  - IcedID
- There's an increased focus on cryptocurrency mining
- New platforms/affiliate programs like Kardon Loader continue to emerge
- Banking trojans continually expand to new regions e.g. Panda Banker in Japan

Kardon Loader

Panda Banker

Emotet

Trickbot

Conclusion…

Global threats will require new global interventions

Threat Intelligence is key to informing strategic direction for threat defense

The accelerating internet-scale threat paradigm changes the frontiers for where and how attacks can be launched, observed and interdicted.

https://www.netscout.com/threatreport

Netscout TIR
Verizon DBIR
Symantec ISTR
Kaspersky SA
NCA CT-UK
Netscout WISR

Thank You