Challenge Nineteen

A collection of infected IoT devices and/or other devices can create a large 'NetBot' used to spam or attack other networks. Which one was used to orchestrate the largest DDoS attack with IoT devices?

EarthLink Spammer 2000

- First known to public
- From legitimate websites
- Over 1.25M malicious emails sent
- Earned spammers over $3M USD
- Creators were sued for $25M

Grum 2008

- Pharmaceutical Spammer
- 18B spam emails per day
- 136,000 addresses sending spam on behalf of Grum

Storm 2007

- Most malicious of Botnets
- P2P-controlled by several servers
- Infect through malicious websites
- Botnet was available for rent on Dark Web, not very active today

Cutwail 2007

- Targets Windows OS (Trojan)
- Compromised 1.5 – 2M systems
- 74B spam emails per day!
- 46.5% of global spam distribution
- Remains active today

Mariposa 2008

- 12.7M computers
- Illegal 'Butterfly Flooder'
- 2 years, over 190 countries
- Used malvertising to steal CC #s and passwords from banks

Kraken 2008

- Twice as powerful as Storm
- Command and Control servers
- Over ½M messages per day

Methbot 2016

- Digital ad malware, US based ISPs
- 250K premium URLs
- Malicious videos were added
- Bots 'watched' 30M ads daily

Murai 2016

- Access through default passwords
- Over 6M digital smart devices run on ARC processors infected
- Source code published so others would copy to hide source

3ve 2018

- 3 different sub operations
- 1.7M computers and servers
- Counterfeit 5,000 websites and 60,000 advertising companies
- Sole goal was to seal $$$

Send your answer to: OCIOSecurity@gov.bc.ca Challenge Nineteen