NETSCOUT | Arbor

The Evolving Landscape of Threats – Arbor Development Direction

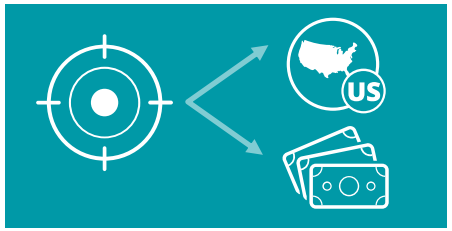
23rd October 2018

Michele Di Dedda – Consulting Engineer Italy, Cyprus, Malta and Albania

Alessandro Bulletti – Consulting Engineer Italy, Cyprus, Malta and Albania

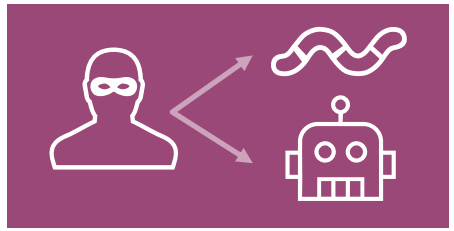
Threats Reported in the Wild

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



- Supply Chain and IoT related Threats (like with Absolute Lojack recovery software)

- More nation states adding APT to their statecraft



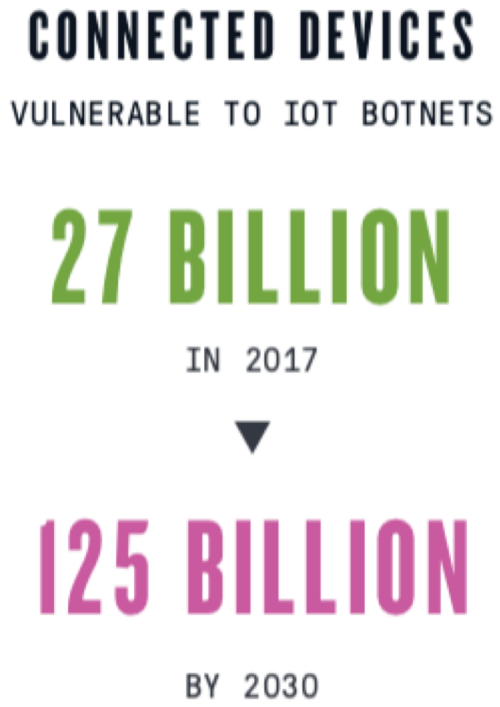
- Crimeware and espionage adding Internet Scale techniques (worms, botnets for mass malware distribution)

Source: NETSCOUT Threat Intelligence Report 1H 2018

Threats Reported in the Wild

- Increased use of auto propagation methods (worms and mass malware distribution like in CCleaner, VPNFilter, WannaCry and NotPetya programs) and cryptocurrency mining in malware
- Crimeware developing new platforms, such as such as Kardon Loader, but well-known malware platforms such as Panda Banker are directed at new targets
- IOT Threats expansion: new generations of Mirai introduce new functionality (i.e. 'Satori' leverages remote code injections exploits for propagation)

Source: NETSCOUT Threat Intelligence Report 1H 2018



Threats Reported in the Wild

IOT, Ransomware and DDoS

- Mid-2016, a variant of Cerber ransomware added DDoS capabilities, which could only DDoS the local network segment..
- Attackers targeting hosts within enterprise networks are now interested in launching DDoS attacks from within – at targets on the same network!
- A single infected Windows computer has the capability to infect and subvert the “innocent” IoT population behind Enterprise firewalls into zombies
- The attacker can then use the zombies to:
  - Infect other IoT devices
  - Launch outbound attacks against external targets
  - Perform reconnaissance on internal networks, followed by targeted attacks against internal targets

© Shutterstock

© Shutterstock

Threats Reported in the Wild

- Network-based ransomware cryptoworms eliminate need for human element in launching campaigns, as well as with wiper malware masquerading as ransomware
- C2 channels relying on legitimate Internet services like Google, Dropbox, and GitHub or on Encryption to evade detection
- Exploit new gaps in security, like with IoT and Cloud services
- IoT Botnets with more advanced DDoS capabilities as IoT and becomes mature and automated
- 53% of attacks resulted in financial damages of more than US$500,000, including lost revenue, customers, opportunities, and out-of-pocket costs

Source: Cisco 2018 Annual Cybersecurity Report

Threats Reported in the Wild

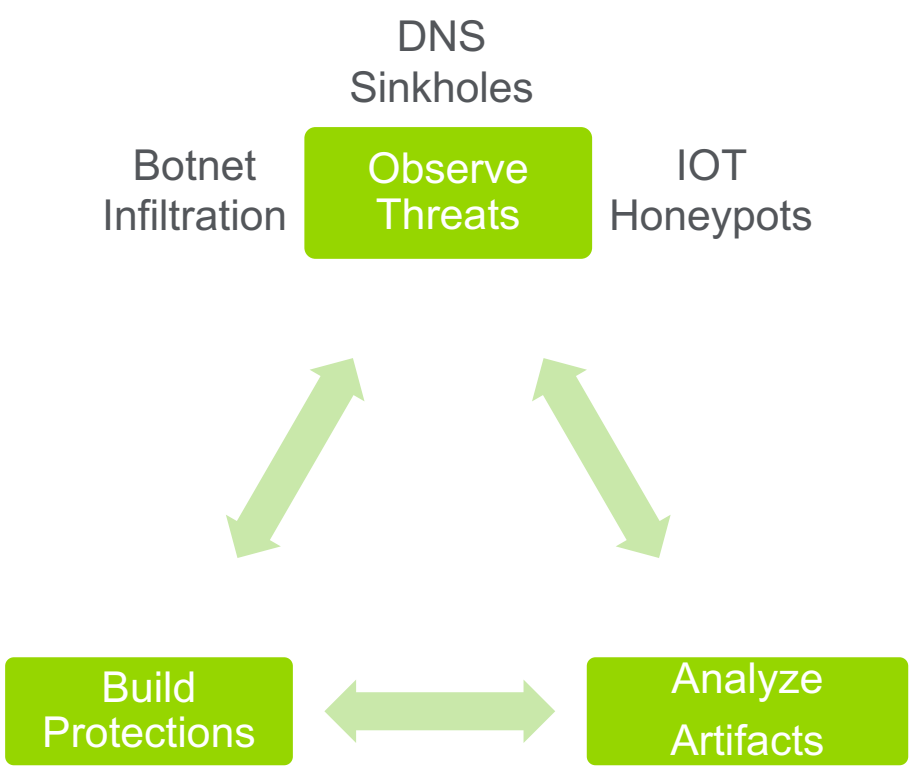
What to expect next..

- Surge in Encrypted Attacks, more sophisticated malware that rely on encrypted traffic to covertly infiltrate organizations
- Proactive IoT Malware, leveraging automated attacks to spread easier and faster
- Malicious Cryptocurrency Mining, malware will force a victim's device resources to mine currency for attackers
- Consumer IoT Attacks, threatening citizens' privacy, information and identities
- Device Control: More and more devices (e.g., cars, refrigerators, thermostats, light bulbs) hyper-connected without much oversight, increasing the scope of locking these devices for ransom and risks for botnets based on consumer IoT devices

Source: 2018 SonicWall Cyber Threat Report

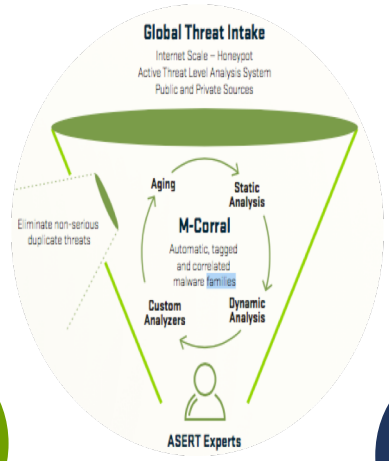
Analyzing Threats – The Big Picture

NETSCOUT | Arbor ASERT – Simplified Malware Research Life Cycle



Streamlined automated collection, analysis, and curation process

Comprehensive contextual information



Scale of Internet

Cross correlation

Stringent scoring and aging criteria

Malware research is an iterative and nonlinear process

Threat Intel and NETSCOUT | Arbor Strategy Update