Bots over wireless networks

Prof Emeritus Sureswaran Ramadass

Nelaka Priyankara

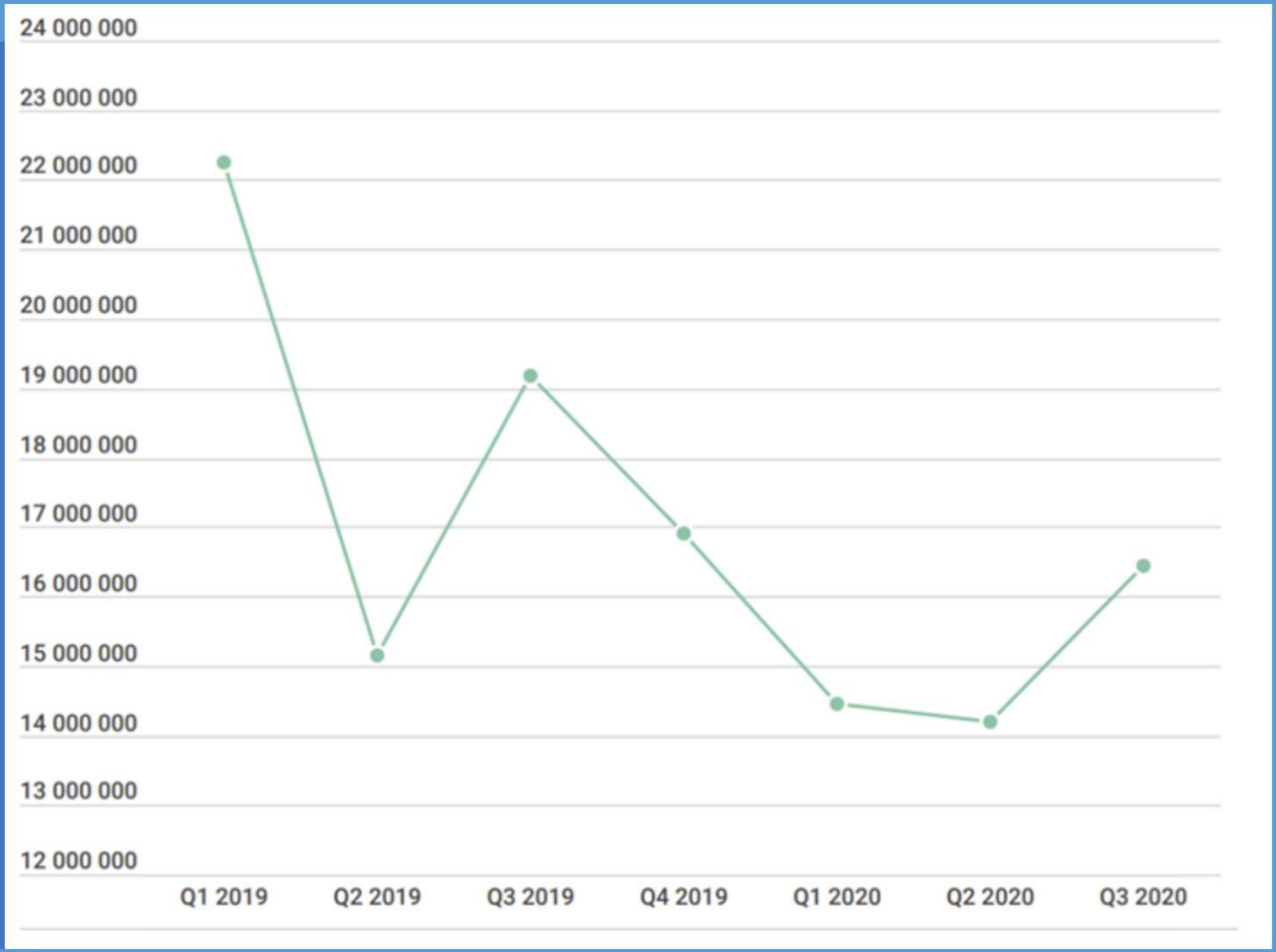
Malaysia University of Science and Technology

Content

- Introduction
- Bots
- Vulnerabilities in Mobile Network
- Life cycle of Bot
- Bots control architectures
  - Type of Bots
- Types of attacks
- Detecting Mobile Botnet techniques
- Conclusion

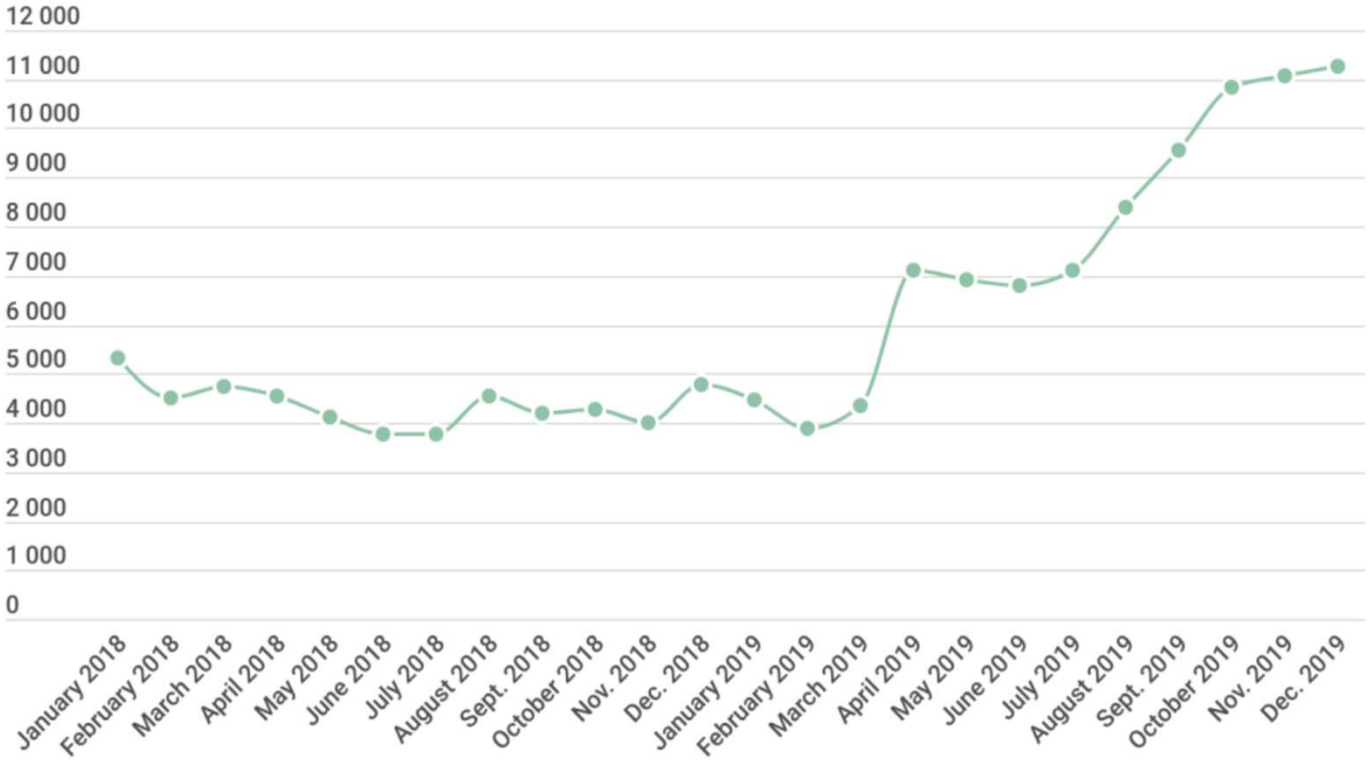
Introduction (1/3)

- In Q3 2020, Kaspersky mobile protective solutions blocked 16,440,264 attacks on mobile devices, an increase of 2.2 million from Q2 2020.



Introduction (2/3)

Over the past year, the number of attacks on the personal data of mobile device users increased by 50%: from 40,386 unique users in 2018 to 67,500 in 2019.



In 2019, Kaspersky mobile products and technologies detected:

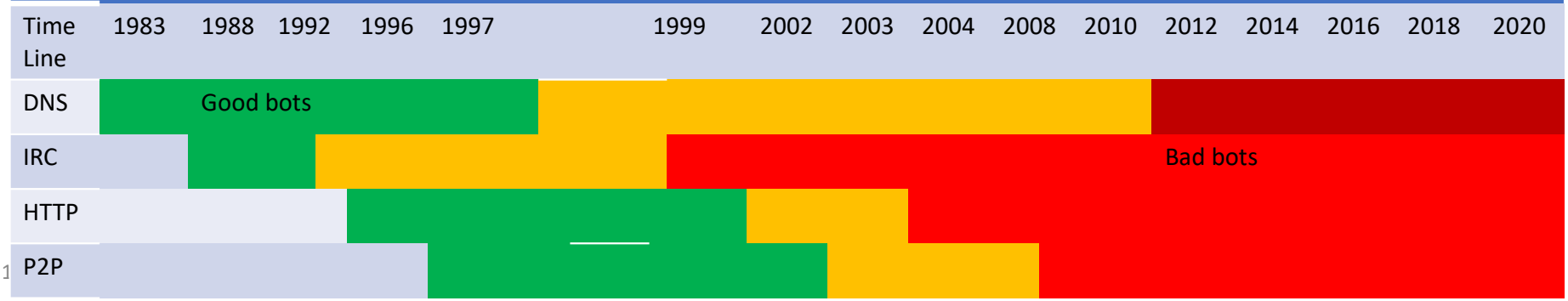
- 3,503,952 malicious installation packages.
- 69,777 new mobile banking Trojans.
- 68,362 new mobile ransomware Trojans

Introduction (3/3)

Evolution of technology

Technology	1G	2G	3G	4G	5G
Development Research ,Standardization & Commercialization	1974/80	1980/90	1990/2002	2000/2010	2014/2020
Core Network	PSTN	PSTN	Packet Network	Internet	Internet
Technology	Analog	Digital (GSM)	Broadband/ CDMA/IP	LTE , WiFi	5G, 4G , LTE, WIFI
Multiplexing	FDMA	TDMA/CDMA	CDMA	CDMA	CDMA
Service	Mobile telephony	Digital : Voice ,SMS	Integrated high quality audio, video and data	Dynamics information access, variable devices	Dynamics information access, variable devices with AI
Bandwidth	2kbps	14-64kbps	2mbps	200mbps	>1gbps

Evolution of Bots and C&C in network



What is a bot?

an autonomous program that use the internet to interact with systems or users to perform certain defined tasks.

Good Bots

- beneficial to businesses
- Individual
  - ex : spider bots, crawler bots GoogleBot, bingbot and Baide spider etc.

Bad Bots

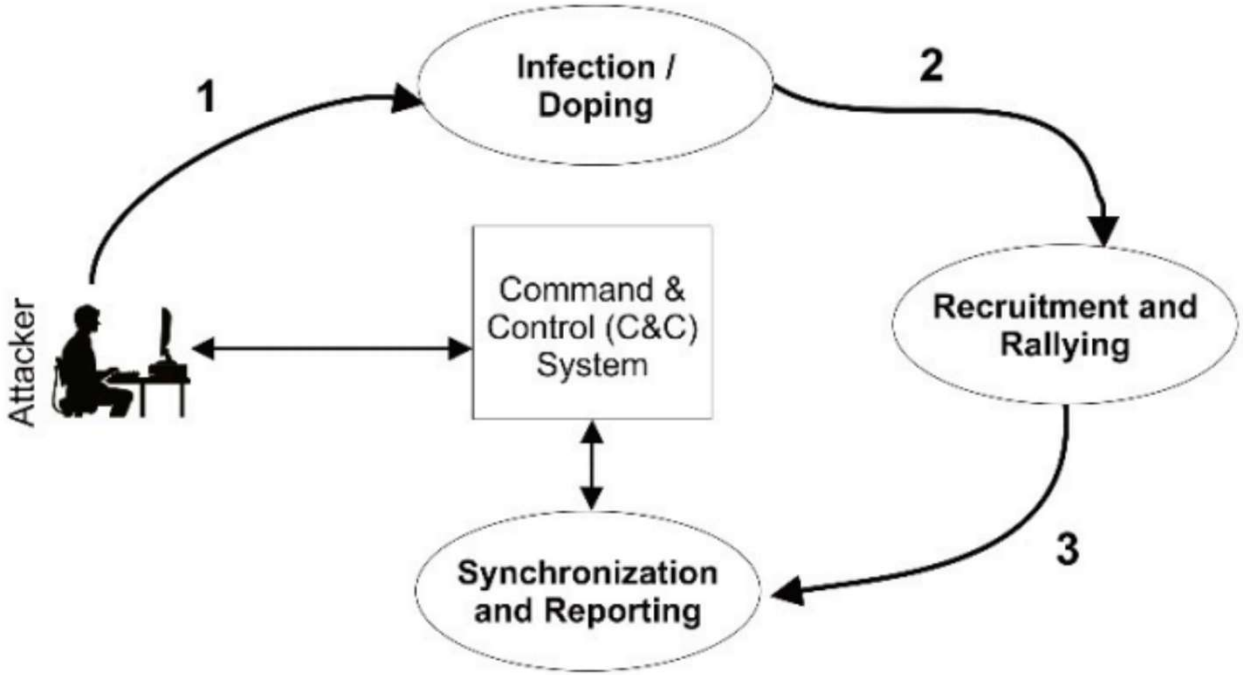
- perform a variety of malicious jobs
- mostly used by fraudsters, cybercriminals, and nefarious parties engaged in various illegal activities

Vulnerabilities in Mobile Network

- Vulnerabilities in mobile devices
  - open-source software, thus everybody can develop apps freely
  - download apps for different purposes including social networking

- Vulnerabilities in mobile network
  - IRC chat rooms over remote channels
  - Social Media and Messenger Based Platforms
  - Apps that are free
  - Gaming Apps

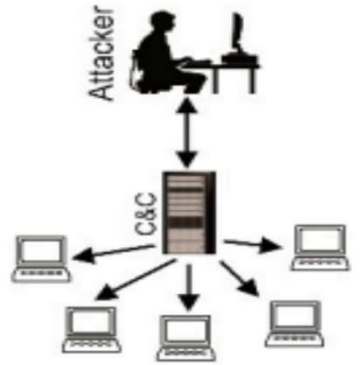
Life cycle of bots



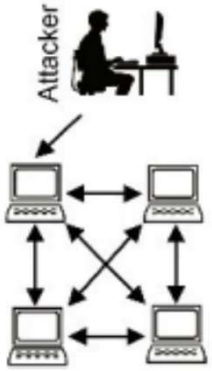
Bots Control Architectures

- Direct

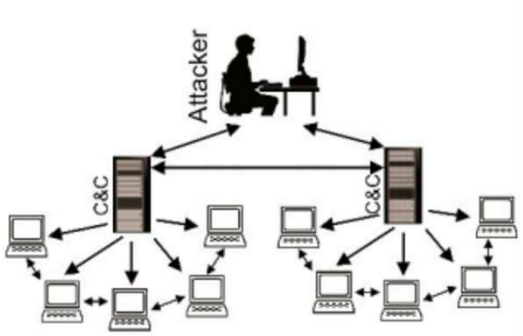
- Centralized



- Decentralized (P2P)



- Hybrid



Type of Mobile Based Bots

- Botnet develop for research activities
  - ex: Andbot, Mobots, PodBots, SMARTbot etc.

- Botnet develops for malicious activities
  - DrainerBot (2019)
  - xHelper (2020)
  - Hiddad (2020)
  - Guerrilla (2020)
  - Mirai malware
  - Phorpiex (First appeared in 2010)

Types of Wireless Bot Attacks

- Packet Sniffing
  - steal your passwords and similar sensitive information
- Rouge Access Point
  - DoS attacks, packet captures, ARP poisoning and more
- Jamming
  - aims to disrupt the network. Due to the wireless features, interference is almost unavoidable
- Evil Twinning
  - ‘evil’ access point cannot be distinguished from actual access points

Detection Mobile Botnet techniques (1/2)

- Signature based approaches
  - Behavioral
  - Hybrid or evolving signatures

- Anomaly based approaches
  - Static
  - Dynamic

Detection Mobile Botnet techniques (2/2)

- Machine learning / Deep learning
  - Neural Network
  - Convolutional Neural Networks (CNN)

- DPI Model Checks for Mobile Botnet Detection
  - Payloadchecking-based method able to detect whether mobile embedded payload contain botnet code

Conclusion

- Wireless network-based attack significantly increases by each year (Kaspersky).
- Wireless and mobile devices are growing at an exponential rate, while Computers have flat lined.
- Due to new vulnerabilities in mobile devices and mobile network as well as the growth opportunity, attackers are now targeting mobile and wireless network.
- To detect bots in wireless networks, signature based, and anomaly detection algorithms are bring developed using Machine learning / Deep learning methods.

Thank You

Prof Emeritus Sureswaran Ramadass <sures@nav6.org>

Nelaka Priyankara <nelakashayamal@gmail.com>