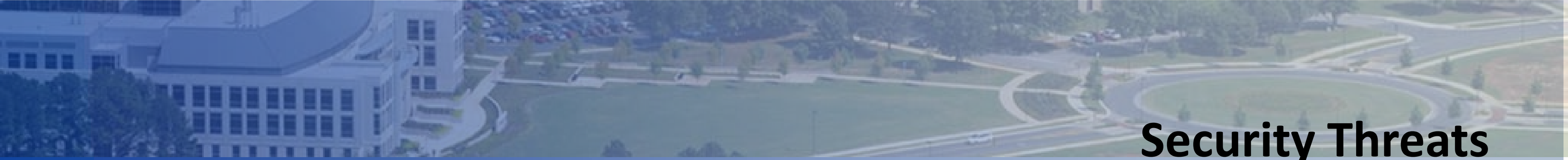


Emerging Security Threats 2011

Security Threats

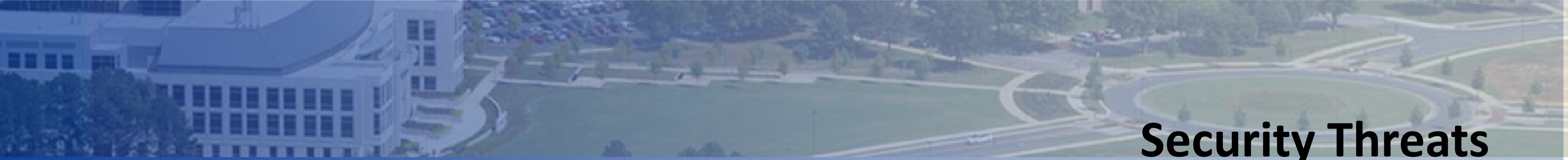
URL-shortening services

- McAfee Labs expects those with URL-shortening services will be at the forefront.
- The use of abbreviated URLs on sites like Twitter makes it easy for cybercriminals to mask and direct users to malicious websites.
- With more than 3,000 shortened URLs per minute being generated, McAfee Labs expects to see a growing number used for spam, scamming and other malicious purposes.

Security Threats

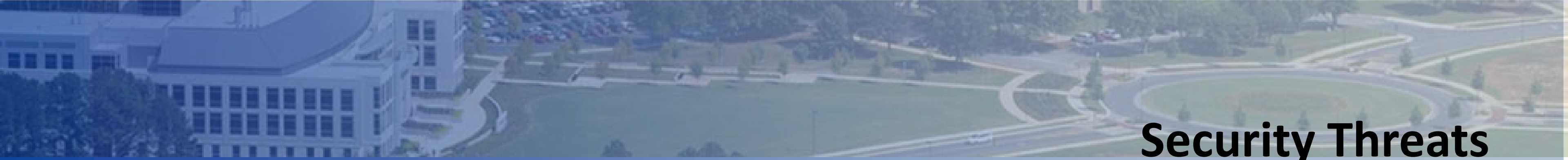
Geolocation services

- Locative services such as foursquare, Gowalla and Facebook Places can easily search, track and plot the whereabouts of friends and strangers.
- Cybercriminals can see in real time
  - who is tweeting
  - where they are located
  - what they are saying
  - what their interests are
  - what operating systems and applications they are using
- This wealth of personal information on individuals enables cybercriminals to craft a targeted attack.



Mobile Malware

- Malware targeting smart phones and tablets is on the rise
- Malware has been discovered in the wild that extracts information from your phone
  - contact information
  - GPS position
  - emails
- Android
  - Malware increased 76% in second quarter of 2011
  - Still lacking tight reviews of apps in Marketplace
- iPhone
  - More review control over apps, but still seeing an increase in malware

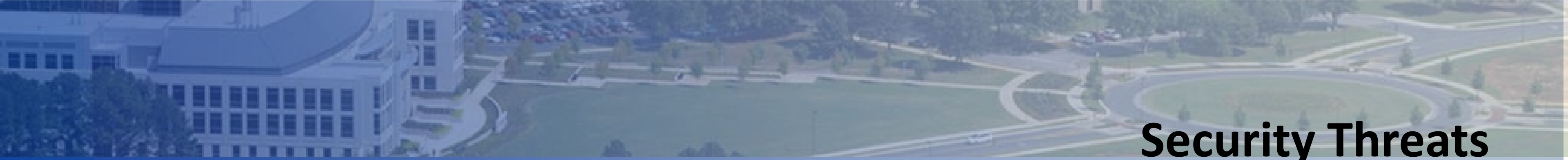


Apple – Mac’s not immune

- The biggest current threat to Mac OS is fake antivirus
  - Mac Defender scam – tricked users into downloading fake AV…which was a virus itself
  - Research before you download anything!
  - There is a growing quantity of web-based malware targeting Mac OS
    - “Drive by downloads” – you visit a site that secretly embeds malicious software on your machine
    - These have typically been “back doors” that allow attackers to access your computer
  - McAfee, Norton, Sophos and ClamXav all offer legitimate antivirus protection for Macs now (just to name a few)

Sophistication Mimics Legitimacy

- Your next computer virus could be from a friend.
  - Malicious content disguised as personal or legitimate emails and files to trick unsuspecting victims are becoming harder to identify
- "Signed" malware that imitates legitimate files will become more prevalent
  - Koobface - spreads primarily through social networking sites as links to videos. When a user visits the website that is hosting the video, they are prompted to download a video codec or other necessary update, which is actually a copy of the worm
- McAfee Labs expects increased abuse of social networks, which will eventually overtake email as a leading attack vector.



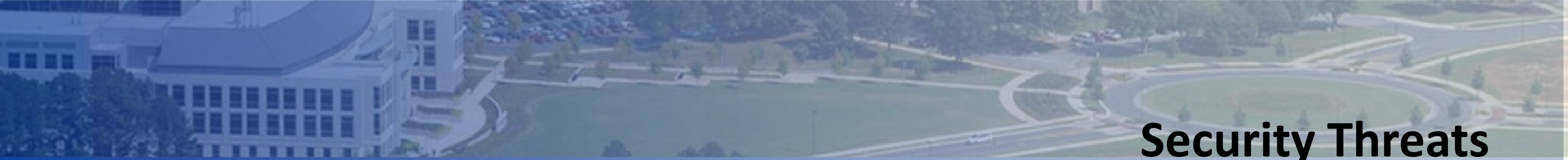
Botnets – Hacker's Zombie Armies

- Botnets continue to use a seemingly infinite supply of stolen computing power and bandwidth around the globe
  - Created by embedding malware on user's machines
  - Malware "phones home" to a control server
  - Now massive amounts of distributed computing power can be used for…
    - Distributed Denial of Service Attacks (DDoS)
    - Spam delivery
    - Serving Porn
    - All without the user's knowledge
  - Bot Herders (hacker's who control them) often offer them "for rent"
  - Mariposa - dismantled on December 23, 2009, it consisted of 8 to 12 million individual computers
  - Zeus botnet – still in existence and it various forms is estimated to include 3.6 million computers. It steals banking information.
- They are becoming more sophisticated

Security Threats

Hacktivism: Following the WikiLeaks path

- Next year marks a time in which politically motivated attacks will proliferate and new sophisticated attacks will appear.
- More groups will repeat the WikiLeaks example, as hacktivism is conducted by people claiming to be independent of any particular government or movement, and will become more organised and strategic by incorporating social networks in the process.
- McAfee Labs believes hacktivism will become the new way to demonstrate political positions in 2011 and beyond.



Security Threats

Questions?