****Caution: This lab requires you to work with real malicious domains that serve real and dangerous malware. DO NOT BROWSE TO ANY OF THE DOMAINS associated with this lab and DO NOT CLICK ON ANY DOWNLOAD LINKS.****

Objectives:

- Use online tools to investigate the origin and possible attribution of criminal domains.
- Specific tools to use:
  - ZeusTracker
  - CentralOps
  - MaxMind
  - RobTex

1. Use a Internet browser to go to http://zeustracker.abuse.ch

   a. Take a few minutes to read the FAQ section to familiarize yourself with this site.

   b. Click on the "ZeuSTracker" button. This will show a list of currently known ZueS Command and Control servers .

      i. What is the most common country hosting ZeuS? _____

   c. Choose a host (domain) for further investigation. Click on it.

      i. What domain are you investigating?_____

      ii. What IP address is assigned to your domain?_____

      iii. What are the names of the files that this domain drops on victim systems?

      (DO NOT CLICK ANY DOWNLOAD BUTTONS!!!!!)

      1. **Config File:** _____
      2. **Binary File:** _____
      3. **DropZones:** _____
      4. **FakeURLS:** _____

      iv. If an executable file is dropped, how many antivirus engines in VirusTotal flag it?

      _____

2. Go to http://centralops.net and click on Domain Dossier.
    a. Click on all scans (caution: traceroute and service scan will actually connect to the server you are investigating and may reveal to the suspect that you are investigating them. This may not be your intention.)
    b. Type your ZeuS domain into the text box and click "Go".
        i. What IP address is assigned to this domain? (This may not match the one previously found, they can change frequently.)_____
        ii. When was this domain created?_____
        iii. When does this domain expire?_____
        iv. Who is the registrar?_____
        v. Is there a name and contact information for the registrant? If so, what is it? (Caution, this may or may not be real)_____

            _____

            _____
        vi. Is there a Network WhoIs record? (This is likely the hosting company) _____

            _____
        vii. What services does the Service Scan show the domain is running?_____

            _____

3. Go to www.maxmind.com. Type in your bad domain's IP address into the search bar and click "Get Location".
    a. Where are the ZeuS servers physically located?_____
    _____
    b. What is the ISP listed as?_____
4. Go to www.robtex.com. Type the bad domain's IP address into the search bar and click "lucky".
    a. Click on the "Graph" button. What other domain's link to your ZeuS domain's IP address? (just write a few) _____
    _____
    _____
    b. What AS number is in charge of you domain's IP address? _____
    c. Type the AS number into the RobTex Search bar (syntax: AS10439). What are the upstream providers for this particular hoster?_____
    _____
5. Use the techniques that you just learned to identify any important information about the IP address and the domain that we have identified as malicious thus far in our case. (bankoftatooine.com & 41.71.188.2) ****Do not actually visit 41.71.188.2. It was and may still be dangerous.)****. _____
    _____
    _____