Spamhaus

Security Investments

Felix W. Dekker, Nick Ho Sam Sooi, Jorai Rijsdijk, Jakob S. Kok

Group number
6

GitHub
https://github.com/Erackron/EoC/

Introduction/background

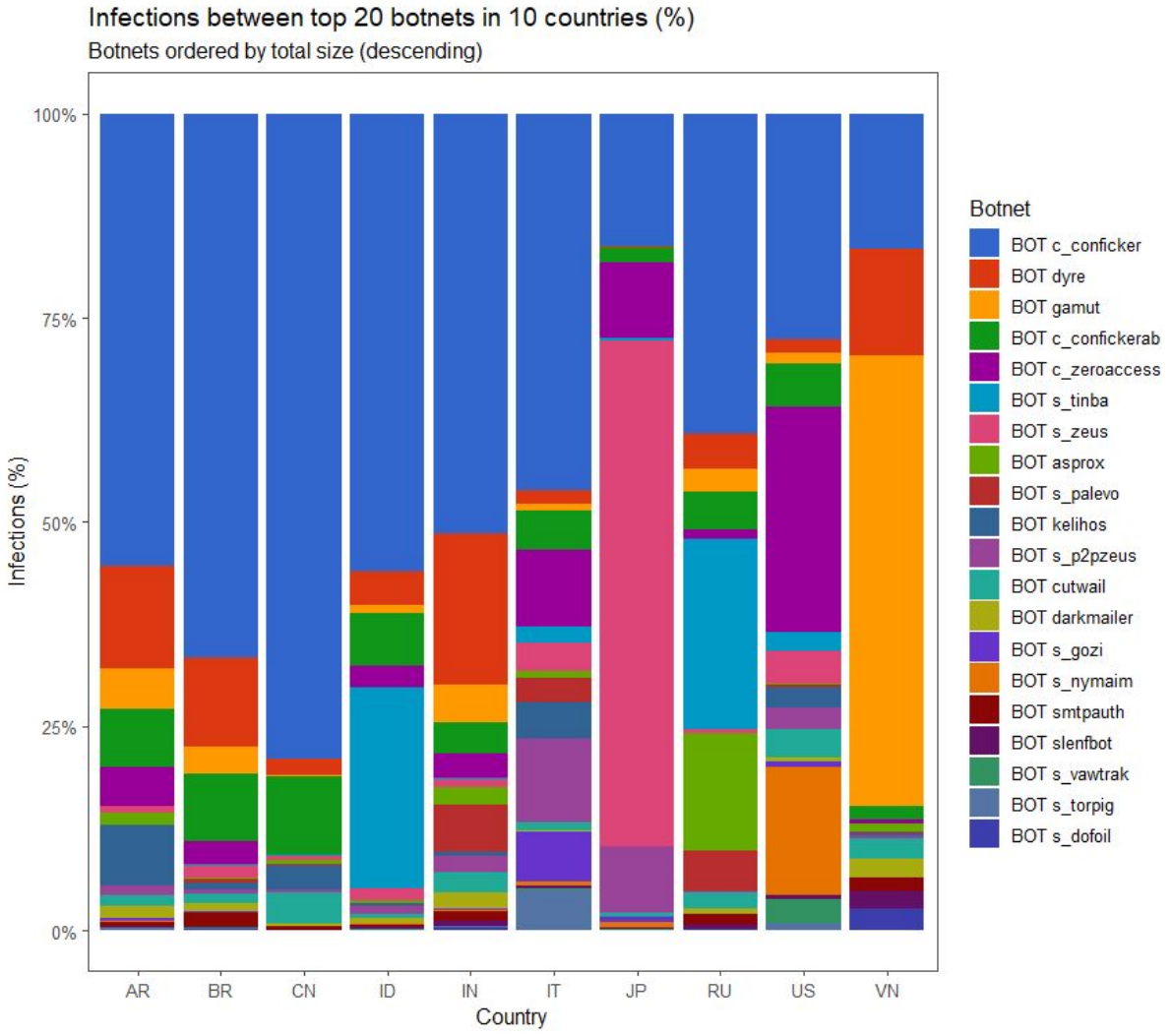
1. Who is the problem owner of the security issue as measured in your first assignment? (0.5 points)
    - Cybersecurity agency in a country. For the purpose of this analysis, we choose the country of Vietnam as they have a disproportionate amount of infections of the Gamut botnet.
    - Core “business”: Advising central government regarding cybersecurity issues
    - Goals: Prevention/Detection/Mitigation of cyber risks/losses

Gamut Botnet

According to the McAfee Labs Threats report of September 2018, the Gamut botnet was responsible for sending 86% of all spam in Q2 of 2018[1], which makes it an interesting target for our analysis, especially with Vietnam having a larger than average proportion infections by the Gamut botnet.

[1] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-sep-2018.pdf

Problem definition



2. What relevant differences in security performance does your metric reveal? Evaluate these difference as shown with the metric developed in the 1st assignment. (2 points)
    - Disproportional amounts of infections by particular bots indicate weaknesses relative to other countries, and thus the weakest points. The national agency in Vietnam can learn from other countries approaches on how to deal with the security issue by looking at methodologies, technical implementations, technology, regulations etc.
    - This allows you to see where you need to invest. Since Vietnam has a disproportional amount of Gamut infections, general awareness and technical control mechanisms for this virus should be incorporated on a national level and company level. However, Vietnam has a surprisingly low percentage of the Conficker virus, which is by far the most distributed botnet across the world. This can have many possible explanations, and factors like attacking behaviour might play a role.

3. What risk strategies can the problem owner follow to reduce the security issue as measured in your first assignment? (0.5 point)
    - **Risk mitigation**
      The security risk could be reduced in two ways:
        1. *Attack*
           Since Gamut makes use of command and control centres, these centres could be taken down to prevent infected machines from being informed of what to do. While machines will remain infected, they will become unable to take action. This effectively disables them.
        2. *Defend*
           To defend against Gamut, the Vietnamese government could require mail servers in its country to filter emails that contain the virus, though the ethicality of this approach is questionable.
           The government could also try to raise awareness of the virus in order to prevent more people from being infected, and it could set up contact points that residents could use to ask for help if they are infected or suspect that they are infected.
    - **Risk transfer**
      To transfer risk, Vietnam could set up a national cyber insurance scheme where companies that put more effort into protecting themselves against Gamut have to pay smaller premiums. However, it is not easy to quantify the effort companies put into this, making it hard to decide on concrete numbers for the premiums.
    - **Risk acceptance**
      Vietnam can choose to accept the fact that there will be infections and consider the current risk level tolerable. In this case, they should still keep an eye on risks as they evolve over time, but for now, they can choose to do nothing.
    - **Risk avoidance**
      Vietnam can choose to withdraw entirely from the Internet or spam, though this option is infeasible.

4. What other actors can influence the security issue as measured in your first assignment? (1 point)
    - **Cybercriminals/attackers**
      The attack strategy, motives and capabilities of cybercriminals strongly influence the severity of the security issue. For example, if cybercriminals decide to invest more resources into enlarging their botnet or increasing its complexity, it becomes significantly more difficult to kill it.
    - **Companies**
      Secondly, a diverse set of companies influence the security issue. In order to provide a more in-depth analysis of their influences, a distinction will be made between three types of companies; Security providers, Security consumers and the security industry. Security providers are companies who/which produce IT soft- and hardware. For these companies, security is not a core competence. Examples of such companies are Google, IBM and Apple.

Security providers are able to influence the strength of control measures in machines being used in Vietnam. The security consumers are companies which are mostly involved with mature markets and make use of IT either to innovate or increase their operational efficiency. Security consumers influence the security level by allocating a certain fraction of their budget to security. Finally, The security industry consists of companies which have been able to create a successful business model with security as their core competence. These companies develop security technology which improves the resilience of machines to threats imposed by botnets.

- **Citizens**
  Citizens own machines which can be targeted by attackers. The security of these machines is dependent on their willingness to invest resources into security technology or more secure machines.
- **Law enforcement agencies**
  Law enforcement agencies are responsible for enforcing the legislation regarding threats imposed by botnets and other cyber threats. Increased efforts by law enforcement agencies to such threats enlarge the probability of detection and therefore make it less attractive for cybercriminals to engage in their activities.
- **Regulatory bodies** (EU, national governments)
  Regulatory bodies design the institutional framework in which companies and citizens operate. For example, new regulations might force these actors to invest more resources into security.

5. Identify the risk strategies that the actors can adopt to tackle the problem (1 point)
   - are there actors with different strategies? why?
     1. **Cybercriminals**: The risk for cybercriminals consists of getting caught and having to pay a fine or serve a jail sentence. They can either avoid this risk by not executing any attacks, mitigate it by increasing the complexity of their attack or simply accept it.
     2. **Companies**: Companies can avoid risks by not engaging in risky business activities, accept risks, mitigate them by investing in security or transfer them by buying cyber insurance or incorporating cyber risks in Service Level Agreements.
     3. **Citizens:** Citizens are able to mitigate the risk by making use of secure hard- and software, transfer it by ensuring that the producers of the hard- and software they buy are responsible for losses, accept it, or avoid it by not making use of certain services.
     4. **Law enforcement agencies**: Law enforcement agencies are able to mitigate the risk by investing resources in the detection of botnets
     5. **Regulatory bodies:** Regulatory bodies can mitigate the risk by creating awareness regarding cybersecurity for citizens and providing new, possibly more strict, regulations.

Analysis

6. (5 points) Pick one of the risk strategies identified previously and calculate the Return on Security Investment (ROSI) for that particular strategy. I.e.,
    - Estimate the costs involved in following that strategy
    - Estimate the benefits of following that strategy (assume a particular loss distribution)

Conclusion

// TODO