Spamhaus

Externalities

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

Group number
6

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

1 Introduction

In this report, the previously-described Spamhaus dataset will be used to identify which externalities can be expected when mitigating the risk imposed by the Gamut botnet. Externalities are costs or benefits that affect an external party which does not participate directly in the transaction[citation needed]. For example, when a production company chooses to dump its waste in a nearby river, the health issues this causes for citizens living downstream can be seen as a (negative) externality. These externalities can cause a lack of incentives for actors to take action and mitigate harm they are causing. In the case of the production company, the company does not bear the costs of the health issues and therefore has no incentive to mitigate risk it imposes for citizens living downstream.

Moreover, the analysis of the security performance for different countries has shown a significant variance in the infection rate among the countries. The second part of this report will be aimed at defining factors that cause this variance and will provide a statistical analysis showing the variance that be can be explained by a subset of these factors.

2 Externalities

In this section, the externalities that occur when certain actors invest in the treatment of the risk caused by the Gamut botnet will be assessed. First, three focal actors are chosen. Then, a countermeasure is discussed for each of these actors. Moreover, the distribution of costs and benefits for each actor and the respective countermeasure is evaluated. Finally, the lack of incentives to take the countermeasures as well as the externalities that occur are presented.

2.1 Actors

The first actor we will focus on is the Vietnamese governmental **cybersecurity agency**, which was also the problem owner in our previous report. This agency is responsible for

assessing the country’s cybersecurity and it reports its findings to and gives advice to the Vietnamese government. The government may, in turn, impose certain security standards on the country’s companies and may create regulations and legislation.
The choice for Vietnam is based on the country’s disproportionate amount of infections by the Gamut malware. This makes it an interesting point of focus when it comes to analyzing the underlying reasons behind the existence of this problem.

A Vietnamese **IT company** such as VNPT[1] provides a large variety of services, ranging from telecommunications to consultancy. The Gamut botnet poses a threat to VNPT by sending extremely large volumes of spam, which may clog the network and reduce the available bandwidth for legitimate users. If users are significantly affected they may blame VNPT and switch to another provider. Therefore, VNPT should be interested in countermeasures even though Gamut does not directly attack the company.

The machines of **citizens** are interesting targets for malware such as Gamut because these machines are often poorly protected—they use default passwords and vulnerabilities are not often patched. On the other hand, citizens are not directly affected by malware such as Gamut other than slightly reduced performance. Therefore, citizens are an interesting actor to analyse because they can potentially solve the problem but do not have a vested interest in doing so.

2.2 Countermeasures

As the **cybersecurity agency** in Vietnam has general incentives for amplifying the defences of the country’s network, one countermeasure that the cybersecurity agency could take to mitigate the security issue is to set up a collaboration network for ISPs. In general, most companies have not been adept at collaborating to defend against cyber attacks, and cybercriminals have exploited the fact that the defenders have not been coordinated. By exchanging information through this new information channel set up by the cybersecurity agency, the companies can to a larger extent coordinate responses and share experiences. This will lead to a more efficient security performance.

IT companies could set up spam filters. These will prevent spam emails from entering the network, thus protecting the network from further infections. Spam filters generally have a very high precision and recall, and, as analysed in our previous report are a cost-effective method against spam.

In order to respond to the botnet threat, **citizens** could properly secure the machines they own. One specific countermeasure they could take against the botnet threat is installing antivirus software. In some cases, the antivirus software will be able to detect and remove the malware from a device. However, in other cases, the complexity of the malware and creativity of the attacker disables the antivirus software from solving the issue.[2] To illustrate this, many malicious programs present on infected machines are able to interfere with the

[1] http://vnpt.vn/en
[2] http://clico.pl/services/practical-defense-in-depth-protection-against-botnets

antivirus software and disable it (Hachem, Mustapha, Granadillo & Debar, 2011). In these cases, prevention in the form of e.g. better passwords may be a better alternative.

2.3 Cost distribution

(0.5 point) Analyze the distribution of costs and benefits among the different actors that the deployment of the countermeasure would entail.
`// TODO`

2.4 Incentives

The incentive for the **cybersecurity agency** is the lost efficiency and productivity in the country due to domains being on blocklists. The reputation of its national servers.

When dealing with a lot of incoming spam without having a spam filter, the employees of **IT companies** will take much longer to go through their email on a day-to-day basis, leading to decreased efficiency and productivity and the potential of emails being missed in the flood of spam.
The other side of the incentive to install a spam filter is that if your network is perceived to be sending a lot of spam, your network might end up on a blocklist, which means that other companies with spam filters will likely mark all your legitimate email as spam as well, leading to decreased revenue and a loss of clients.

When a **citizen**'s home network or machine is infected with a botnet, the botnet will take up processing power, network bandwidth, and more. In addition, the botnet may install other malware on the machine, further increasing the effect. Finally, the malware may steal payment credentials, personal information or prevent access to personal data unless a fee is paid.

2.5 Externalities

The cooperation network set up by the **cybersecurity agency** can not only be used to fight the Gamut infection, it may also prove useful in defending against other cybersecurity threats. This is a positive externality.
On the other hand, because of all kinds of regulations that new companies will have to comply with, the entry barriers for new companies will be significantly higher. Furthermore, companies not in the network will be targeted worse. All put together, this will lead to more spam and thus more infections in those companies.

As a positive externality, the **IT company**'s spam filter will not only prevent new infections in its own network, it will also prevent currently infected machines from sending spam from the network. That is, the spam filters will indirectly protect other networks from being infected. Furthermore, spam filters are an effective countermeasure for all sorts of malware, not only the Gamut botnet.
The flipside of this is that spammers will turn their attention to worse-protected networks which will as such be infected more.

When a **citizen** increases the security on their own machine, they will no longer contribute to the botnet and the threat the botnet poses will therefore decrease. While it was not the goal of the citizen, the volume of spam will ever so slightly decrease as a result of the improved security.
However, by adopting a specific type of antivirus, you become part of the reason that malware developers will try to circumvent the protection from that specific antivirus vendor.

3 Analysis

(7 points) Identify the type of actor whose security performance is visible in the metric(s) you selected (e.g. ISPs, software vendors, countries). Note that this is not necessarily the problem owner, rather it is the unit of analysis in your metric.

1. Choose a type of actor.
   a. Countries.
2. Identify different factors explaining (causing) the variance in the metric.
   a. *National cybersecurity investment*
   b. *Global Cybersecurity Index*[3]
   Correlation:

Pearson	-0.0851
Kendall	0.0450
Spearman	0.0629

   c. *GDP per capita per country*[4]
   Correlation:

Pearson	0.1144
Kendall	0.1700
Spearman	0.2537

   d. *Population characteristics, e.g. density etc.*[5] [6]
   e. *Government initiatives*
   f. *The ratio of cybersecurity papers published in the country*[7]
   Correlation:

Pearson	0.0126
Kendall	-0.1260
Spearman	-0.1878

   g. *Technology index*[8]
   Correlation:

Pearson	-0.1066
Kendall	-0.0037
Spearman	0.0225

[3] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
[4] https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?view=map
[5] https://population.un.org/wpp/DataQuery/
[6] https://en.wikipedia.org/wiki/List_of_countries_and_dependencies_by_population_density
[7] https://www.scimagojr.com/countryrank.php
[8] http://www.nationmaster.com/country-info/stats/Economy/Technology-index

h. *The ratio of cybersecurity experts in the country*

i. *The ratio of attackers caught in a country = police effectiveness*

j. *Median citizen income*[9]

Correlation:

Pearson	-0.1006
Kendall	0.0854
Spearman	0.1455

k. *IDI*[10]

Correlation:

Pearson	-0.0264
Kendall	0.1399
Spearman	0.2204

l. *The annual turnover of IT companies*

m. *Ratio of cybersecurity firms in a country*

n. *Number of computers per citizen*[11]

Correlation:

Pearson	0.2318
Kendall	0.1326
Spearman	0.2029

3. Collect data for one or several of these factors.
    a. OK
4. Perform a statistical analysis to explore the impact of these factors on the metric.
    a. `// TODO`

References

Hachem, N., Mustapha, Y. B., Granadillo, G. & Debar, H. (2011). Botnets: lifecycle and taxonomy. In *Network and Information Systems Security (SAR-SSI), 2011 Conference on* (pp. 1-8). IEEE.

[9] https://news.gallup.com/poll/166211/worldwide-median-household-income-000.aspx

[10] https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf

[11] http://www.nationmaster.com/country-info/stats/Media/Personal-computers/Per-capita