Actors and Security Strategies in Malware Domains

EoS Assignment 3, Group 11

1. Countermeasures

For this report, we take a look at three of the actors involved in the security issue of malware domains and what countermeasures they could take to mitigate the problem. The actors we consider are the hosting providers, customers of hosting providers (we assume only customers with good intents. In this report we refer to them as 'customers' for the sake of brevity) and domain registrars since we believe that these actors are either close to the problem or, in the case of the customers, are needed for a complete picture of what is happening.

1.1 Concrete countermeasures per actor

In this section, we will discuss concrete countermeasures the actors could take to mitigate the security issue of malware domains. These countermeasures, while concrete, might not necessarily be the best and should often be combined with other countermeasures.

Hosting providers

As stated in [1]: "*...although hosting providers are a key actor in fighting website compromises, their ability to prevent abuse is constrained by the security practices of their own customers*". Therefore, it might be more effective for hosting providers to direct their security efforts towards the security of their customers. A measure to take would be to recommend customers to update their software as soon as an update becomes available. This can be communicated on a regular basis via channels such as email or can be stated when the customer opens an account at the hosting provider.

Customers of hosting providers

Customers can mitigate the security issue by applying software patches as soon as they become available. They should also only use software that is considered safe by the industry. By downloading the latest updates, the systems the customer is hosting are not vulnerable to known exploits.

Domain registrars

Domain registrars can mitigate the security issue by scanning for malicious use of domains, using a detection system. Multiple of such systems have been proposed [2, 3, 4]. These systems aim to detect malware domain either by analysing URLs with linguistic tools or by analysing other domains to derive new malware domains. The benefit is that malware domains are actively being found, rather than being reactively found, as with standard blacklists.

1.2 Distribution of costs and benefits

In this section, we look at both the costs and the benefits of the defined actors with respect to the suggested countermeasures.

Convincing customers to update their software

Hosting providers convincing their customers to update their software would lead to a decrease in the vulnerabilities cybercriminals can exploit to place malware. This would mean that there will be less malware in the domains hosted by the hosting provider.

This would be a benefit for the hosting provider in question and the domain registrars, as they pay a cost for removing malware. We expect that convincing the customers will take some time and therefore the benefit for these parties will increase as time goes on until a certain saturation is achieved in which all customers that can be persuaded in updating their software have done so. The benefit for customers depends on both the threat frequency and the threat capability that is applied to their application. The distribution can be assumed to have a high benefit after the first patch cycle if it has been a long time since the customer has updated its software. Then, for every next patch cycle, there will be some benefit for the customers, as it is applying the latest security updates. Then the benefit will lower over time because new vulnerabilities will be found in the software that is used. This effect will repeat itself after every software update.

The cost for this countermeasure is low for the hosting provider, as communicating with customers is a trivial task. We expect some initial costs on researching techniques to persuade customers or implementing a solid reminder policy, but after that, the costs should be negligible. One could argue that reminding customers to update security could be seen as annoying by customers, or it might create a feeling of safety because the hosting provider is perceived responsible with concerns to security. We do not consider these factors. Domain registrars do not have any cost associated with this countermeasure. The actor that has the highest cost is the customer if he chooses to listen to his hosting provider. Not only the updating itself takes time, but systems also often break because of software updates, causing extra costs for making the system function correctly again. The cost distribution has peaks corresponding to update periods. The costs will be a bit lower after, but they will not be negligible because the update might have introduced bugs that need to be fixed. After this, the cost is zero until the next patch cycle.

Updating the software

Here, the customer is the actor that decides on updating the software, regardless of whether the hosting provider stimulates this. The situation is almost the same as described before, with an exception to the cost of the hosting provider, as this cost will be zero.

Deploying detection systems

When domain registrars deploy detection systems, they are the only ones that pay a cost. The technology has to be bought first (cost in the beginning). Then, the staff of the registrar needs to be trained in order to use the technology, as there is always some manual handling needed. These are sunk costs. Last but not least, the technology will need to be maintained. In this case, it is logical to assume that the system has to be updated from time to time since cybercriminals will find ways to bypass the detection system. The benefits for the domain registrar and the hosting providers is that they can respond earlier to infections. The customers do not have any benefit from this countermeasure.

1.3 The incentive to take the countermeasure

One question one could ask is whether an actor has the incentive to take the countermeasure. In the cybersecurity world, the entities that are in the position to mitigate a problem are often not the people that experience the problem [5].

Hosting providers

Reputation damage could be a huge loss for a hosting provider and an incentive to opt the countermeasures. A customer chooses a hosting provider by its value in the market. A customer might not want to compromise on choosing a hosting provider with large number of services but low market value. As the market value defines how the hosting provider has sustained in market all this time. The other incentive could be the finances involved. To achieve the financial gains, a hosting provider first has to invest in the security of its customers. For this reason the hosting provider prefers risk mitigation strategy over other strategies because it is cheaper to mitigate risk than to transfer it. Also the risk mitigation is possible at customers' end as well

Customers of hosting providers

In case the application of the customer gets targeted by cybercriminals, there are multiple possible scenarios. The first scenario is that the cybercriminals may choose to take down the website and put up their own one that contains the malware. In this case, the customer's website is no longer available. In the second scenario, the cybercriminals are able to put the malware on the website of the customer. In this case, visitors of the website might download malware, which, if traced back to the website, might affect the reputation of the website owner negatively. Also, services like Google Search will eventually remove the website from the search engine. In both of these cases, the customer of the hosting provider is affected negatively by the security problem. Because of this, he has the incentive to apply the countermeasure as described in section 1.1.

Domain registrars

Domain registrars have the incentive to prevent visitors from visiting infected URLs as it could damage the visitor's computer with malware. It could also lead to severe damages like domain transfer where the visitor unknowingly shares all the credential information. If there is a regular monitoring and scanning on all the URLs in the domain and the detected evil URLs are blacklisted, it would create a safe network for the visitors and account holders.

1.4 The role of externalities

Externalities are the aftereffects that an entity has to bear, though they did not intend to. These externalities could cause good or harm depending upon the outcomes. Negative externalities result in an overuse or overproduction compared to the social optimum whereas positive externalities lead to an underuse or underproduction of the resource afflicted with the externality [6]. In other words, a negative externality is any harm that is imposed on a third party as a consequence of another's actions while a positive externality is a benefit to a third party that is the consequence of another's actions. The role of externalities also defines the need to implement the countermeasures and appropriate solutions to internalise the negative externalities in future.

Hosting providers

Hosting providers can face negative externalities by malware attacks as they have to bear the reputation damage. A higher number of users getting infected by visiting the malicious website can lead to a lesser number of new customers creating an account at the hosting provider. In case of severe damages, where the hosting provider is liable to the customer for the attack, the hosting provider could lose its market value as well. To internalise this, the hosting provider can block the account that is used by the attacker for sending spams, stealing credentials of a visitor or uploading abusive content. This can turn out to be a positive externality for other end users who could not get access to this malicious website.

Customers of hosting providers

The externalities for a customer of hosting provider could be of distinct types. It could be a major or a minor one. The major externalities caused by the malware attacks could be identity theft, monetary damage, political issues or character assassination and minor externalities such as unwanted interruptions or system slow down. Such externalities (both major and minor) influence customers to invest their additional time in cleaning up the infection and fixing the problem. Even when there is no monetary damage or material loss, that is, the infection is benign from the customer point of view, still time is invested to fix flaws to avoid further interruptions by the attacker.

Domain registrars

Domain registrars, like already mentioned, can mitigate the risk by scanning and monitoring the domains. They do this because of the externalities they encounter. An infected domain (or domains) redirect the visitors to a different malicious domains where the visitors might infect their computer with malwares.

2. Variance in the metric

In this section, we aim to understand the variance in the security metric by exploring the impact of different factors.

2.1 Responsible factors

In this section, we will give an overview of factors that might be responsible for variances in the security metric. For every factor, we come up with a hypothesis.

Legislation

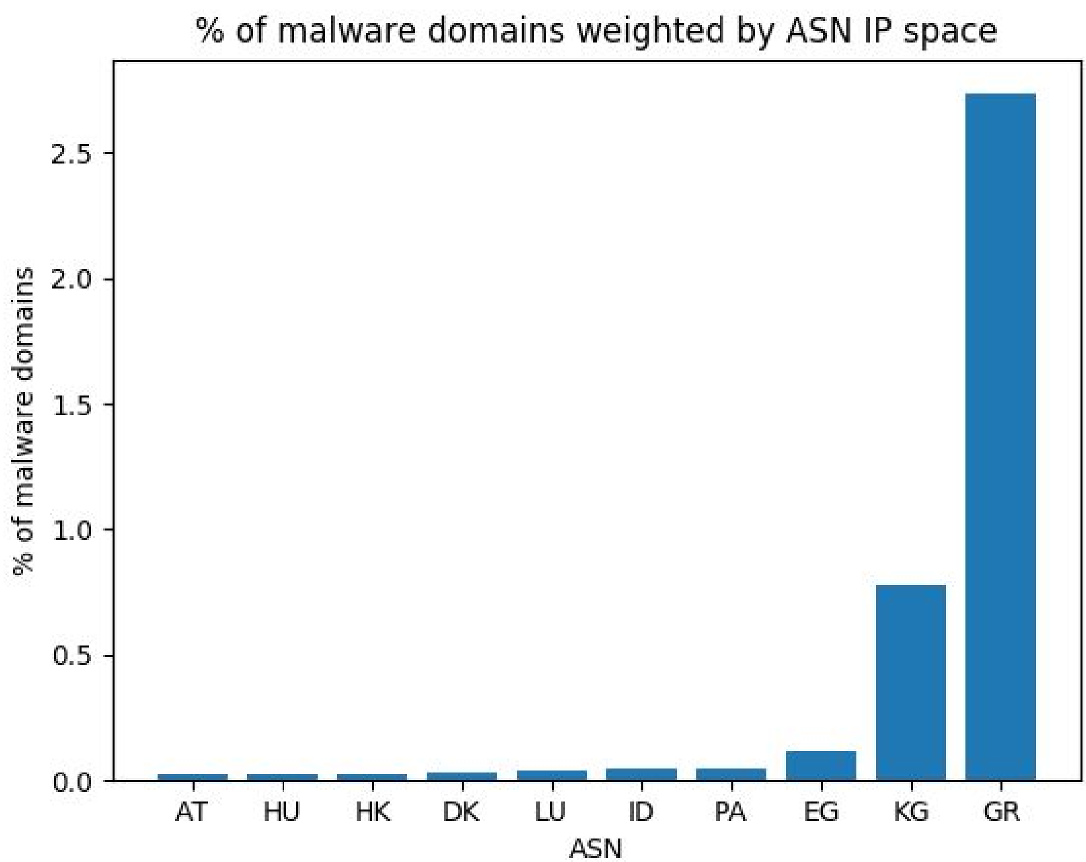
Legislation and local policies can have an impact on the security performance of the hosting providers and other actors. Incentive to improve security comes with liability. The liability can be at the hosting providers, customers of hosting providers or domain registrars depending on the local legislation. In order to test this, we hypothesise a correlation between the infection rate of an ASN and the geographical location. Note that other variables can influence the correlation, however a strong correlation could indicate legislation to be a responsible factor.

Size of the ASN

One explanation of the variances in our security metric could be the influence of the ASN size on the infection percentage. We suspect larger ASNs to have a lower infection rate. Due to the large economies of scale in information security, it should be easier for large hosting providers (and thus ASNs), to mitigate the security risk. Also as we have learned, similar security risks often occur at the same time. Together with information asymmetry, a large hosting provider should be able to perform on our security metric. We therefore hypothesize that the size of the ASN has a negative correlation with the percentage of malware infections in the ASN.

2.2 Data gathering

In the previous assignment we looked at the incident rate per ASN weighted by their IP size. This time we will accumulate all ASNs of a country, that occur in our data.



2.3 Statistical analysis

For our analysis we look at the incident rate of ASNs ordered by country. In total there are 61 countries hosting malicious domains in our dataset. We used Numpy to calculate the statistical values.

Mean: 0.06591
Standard deviation: 0.35863
Variance: 0.12861

Numpy has built in normality tests. One of these tests, based on D'Agostino and Pearson's that combines skew and kurtosis, seems to indicate that our data is not from a normal distribution.

However, we can still try to correlate the country with the found incident rate. As can be seen in the table above there are pretty big differences. To prove they are statistical significant we will use a 2-sample **Kolmogorov–Smirnov test** to compare every countries distribution to the overall distribution. We use a confidence threshold of 90%. The following countries differ significantly from the overall distribution:
BE
ES
CL
This may seem weird looking at the results from above, but these results were not significant since we only had a very small sample size. For example KG and GR only had a single malicious ASN.

References

[1] Tajalizadehkhoob, S. (2018). The Role of Hosting Providers in Web Security: Understanding and Improving Security Incentives and Performance via Analysis of Large-scale Incident Data.

[2] Felegyhazi, M., Kreibich, C., & Paxson, V. (2010). On the Potential of Proactive Domain Blacklisting. *LEET*, *10*, 6-6.

[3] Marchal, S., François, J., & Engel, T. (2012, September). Proactive discovery of phishing related domain names. In International Workshop on Recent Advances in Intrusion Detection (pp. 190-209). Springer, Berlin, Heidelberg.

[4] Hart, M. A., Wilhelm, J. S., & Sundaram, S. (2014). U.S. Patent No. 8,631,498. Washington, DC: U.S. Patent and Trademark Office.

[5] Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, *3*(3-4), 103-117.

[6] van Eeten, M. J. and J. M. Bauer (2008), "Economics of Malware: Security Decisions, Incentives and Externalities", OECD Science, Technology and Industry Working Papers, 2008/1, OECD Publishing.