Defining metrics for hosting providers to measure their security level based on hacked URLs.

WM0824TU Economics of Cybersecurity - Assignment 1: Security Metrics

Charalambous Georgia (4627121), Knippenberg Kjell (4228324), Linssen Barbara (4211995), Moraal, Wouter (4748042)
Delft University of Technology, September 2017

Abstract. This study, performed within the context of the course WM0824TU Economics of Cybersecurity TU Delft, describes an analysis on how to measure the security level of hosting providers. To do this, several metrics are indicated through analysing a dataset from the spamtrap tool CleanMX. The results show that metrics on specific or country domains, and AS with many different IP addresses can help indicating attacker behaviours. The number of internet users is considered not to affect the number of URLs. It is therefore recommended for hosting to focus on the Top-Level Domain (TLD) country domains and Autonomous Systems (AS) per country as indications for attacker behaviour when measuring the security of their services based on hacked URLs; rather than counting the amount of hacked URLs.

1 Introduction

Hosting providers are companies that host technologies and services on the web for both individuals and businesses, which basically means they are providers of websites. Websites are vulnerable to hackers, who have malicious intentions. A hacker can, for example, use websites for phishing and defacement, or infect it with malware. Hacked websites can be bad for the hosting providers' business (Ganan, 2017). As hosting providers want to compete with other hosting providers, they aim to provide as secure services as possible, which means they dont want to be associated with hacked websites. The hosting providers would therefore want to know how well they are performing related to their competition (1), and how they are able to improve their competitive position by improving the security of their services while keeping their costs as low as possible (2). Also, from a more societal point of view, hacked websites can have a large cost on society and are therefore considered highly undesirable (Ganan, 2017). Hosting providers have been shown to be in a good position to avert websites being hacked (Fryer, Stalla-Bourdillon, & Chown, 2015).

This paper is focused on the security issue from the perspective of the hosting providers on how to measure their security performance related to their competition. Therefore, in this paper a metric is provided to enable this comparison between the several hosting providers. Research into the ways to improve the security levels of the hosting providers to improve their competitive position is regarded out-of-scope. The dataset which will be used, is part of a spamtrap database. It consists of the links that have been received by a spamtrap for a period of three years, and their respective date- and time-stamps. From this dataset, we can analyse the scope of hacked websites and the particular incidents of hacked websites further. To the end to be able to form metrics, we will first formulate the ideal metrics from the perspective of hosting providers. Then we will put these metrics in the context of both the academic information security metrics, and the existing metrics used already by the hosting and security industry to grasp and assess hacked websites. In the following section processing of the data will be discussed, and the metrics are operationalised with respect to the dataset at our disposal. Thereafter, the results of these metrics are outlined and explained. We will conclude with a discussion of the resulting metrics, and possible recommendations to hosting providers.

2 Literature Review

In literature, several studies are conducted on ways to measure the performance of security and strategies to improve the returns on security investments. To guide hosting providers in decision-making between the several options to improve security, the ideal metric would, as described by Bohme, enable decision makers to compare multiple security measures associated with a certain security level (Böhme, 2010):

ROSI (Return on Security Investment) = (benefit of security - cost of security) / cost of security.

Cost of security is defined by several decompositions in literature. Anderson et al. decompose the cost of cybercrime into three categories: direct losses, indirect losses and defence costs (Anderson et al., 2012). Direct cost are the monetary equivalent of losses, damage, or other suffering felt by the victim as a consequence of cybercrime (Anderson et al., 2012, p. 5). Indirect losses are the monetary equivalent of the losses and opportunity costs imposed on society by the fact that certain cybercrime is carried out (Anderson et al., 2012, p. 5). Defence costs are the monetary equivalent of prevention efforts, which includes the direct defence costs (development, deployment, and maintenance) as well as the indirect defence costs (inconvenience and opportunity costs caused by the prevention measures (Anderson et al., 2012, p. 6).

Benefits of security are, as explained by Carlos Ganan, determined by the prevented accidents and dependent on the value of the assets at risk (Ganan, 2017). However, fewer accidents can either be due to more attacks failing (better security) or due to fewer attacks (change in attacker behavior) (Ganan, 2017). To determine whether a decrease in attacks is due to change in attacker behavior or due to better security, there should therefore, ideally, be controlled for the attacker behaviour and for the differences unrelated to security (Van Eeten, 2017). Moreover, Noroozian et al. mention that there should be controlled for the level of exposure, which they define as the degree to which a provider, or another class of defenders being studied is exposed to a certain threat (Noroozian, Ciere, Korczynski, Tajalizadehkhoob, & van Eeten, 2017, p. 4). Controlling for the level of exposure includes controlling for the size of the provider, as larger hosting providers have more customers and hence a higher probability of one of those customers being compromised (Noroozian et al., 2017, p.4), and controlling for the business model of the hosting service, as customers of cheap hosting services running popular content management systems are more likely

to be compromised than professional hosting customers with their own security staff(Noroozian et al., 2017, p. 4).

Figure 1 shows the relationship between the level of security, the number of incidents, the number of prevented losses and the benefits of security. A negative relationship means that an increase of the one factor leads to a decrease of the other factor, and vice versa. For example, an increase of the level of security should lead to a decrease of the number of incidents. A positive relationship means that an increase of the one factor leads also to an increase of the other factor, and vice versa. For example, an increase of the level of security is associated with an increase in the number of prevented losses. The dotted arrow between prevented losses and incidents indicate that the number of prevented losses is dependent on the number of incidents. As it is not possible to directly measure the level of security, the decision maker would like to measure indicators that reflect different aspects of the security level. One metric to measure the security level of the hosting providers is to measure the occurred incidents and prevented losses. However, ideally, the decision maker would like to know the factors influencing the incident rate, so he could try to prevent an incident from occurring. Besides, when an incident does happen, the hosting providers would ideally want to know how the trace the attackers to know who hacked the domains and to eliminate them. By knowing which hacked domains belong to which hosting providers, the hosting providers would be possible to compare their security performance with the performance of the competition. Moreover, the hosting providers would ideally like to know how their security performance (and the performance of the competitive providers) changes over time.

However, as explained by Noroozian, using abuse data to measure security performance suffers from the problem that abuse data is driven by a multitude of causal factors that are hard to disentangle (Noroozian et al., 2017, p. 1). Besides, abuse data is notoriously noisy; highly hetero-

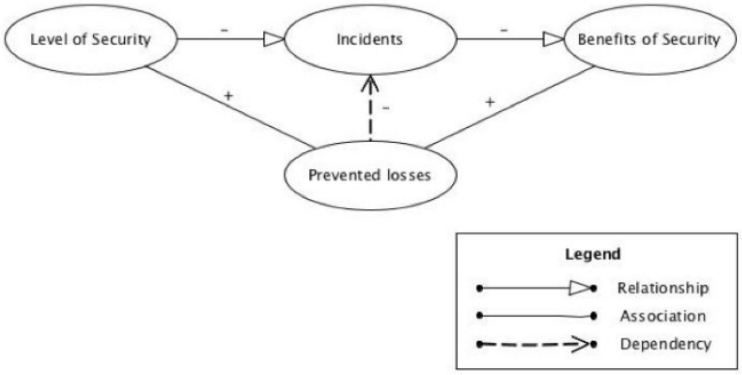


Fig 1 Relationship between the level of security, incidents and the benefits of security

geneously; often incomplete, as not all abuse events are observed; and biased, as providers without incidents were not observed (Noroozian et al., 2017, p. 2). Taking into account these problems with incident data, Nooroozian et al. created a statistical model which could quite significantly predict a variable that they called ”security performance” among different hosting providers (Noroozian et al., 2017). Simplified, the model they use, takes an aggregate of different factors of exposure of the subjects (the hosting providers), a random error variable for number of attacks, and an input variable of incident count, to output the security performance (Noroozian et al., 2017). Testing their model they are able to show that using this model the security performance explains most of the variance in the incident count (Noroozian et al., 2017). Following Nooroozian, for each dataset the number of observed events per provider is counted. This metric is defined as the number of unique pairs (domain-IP-address) recorded per abuse feed and uses Autonomous Systems (AS) as unit of analysis (Noroozian et al., 2017). Even better is to, if possible, use the organization from to which the IP-addresses are assigned. Important is to note the observation bias in the data, especially with one dataset. The following events per dataset can for example be noted: Alloctated IPs, Domains, Hosting IPs, Shared IPs and Shared Domains. These events can be translated into a latent variable, which defines the level of exposure of the dataset. Nooroozian argues that if we

can control for a random variable, then the main driving factor in the abuse data is the security performance (Noroozian et al., 2017).

Another problem is stated by Carlos Ganan, who argues it is attractive to capture impact of cybercrime in a monetary amount, making it comparable and amenable for decision making, but states it is actually impossible to generate trustworthy monetary estimates (Carlos Ganan & van Eeten, 2017). Ganan et al. argue cybercrime has different impacts to individual agents (Carlos Ganan & van Eeten, 2017). A client would have direct costs on for example buying the product and assessing the security by a managing board.But also indirect costs can be indicated when using a spamfilter, such as productivity losses due to inconvenience of using the software. For example, spam filters possibly need to be updated every once in awhile, which will cost time. It is therefore difficult to capture all aspects in a monetary value and prevents using ideal metrics for the estimating of the level of security.

Next to the advised metrics in literature, the actual metrics used in practise can be elaborated upon. Hosting providers, additional plug-ins and programs are explored to get an overview of possible metrics that are currently used on the internet. Five random hosting providers were chosen to indicate metrics from, being Bluehost, iPage, Hostgator, Siteground, and Sitebuilder. Among these five providers, comparable notions about security are given on their websites. These mainly focus on providing back-ups, password protections, expert teams, and penetration testing (Bluehost, n.d.; HostGator, n.d.; Hosting, n.d.; Siteground, n.d.; iPage, n.d.). Furthermore, most providers make use of an external security entity, for example SiteLock (Bluehost, iPage, Hostgator). SiteLock argues to fix threats, prevent future attacks, accelerate website speed, and meet PCl standards. To do this, they scan for malware, delete old applications, execute penetration tests, and mitigate backdoor activities (SiteLock., n.d.). In addition to these security preventions, one could install a

plug-in, when using for example WordPress, to protect its website more intensively. Two plug-ins are explored, to see what kind of metrics are used. First, Wordfence Security focuses on identifying malicious traffic and scans, and blocks known attackers. It is even possible to block certain countries or schedule scans on specific times. iThemes Security scans and reports mainly on file exchange and 404-errors. Also, it enables the client to make back-ups.

It is apparent that hosting providers mainly outsource their protection to experts. Also it can be concluded that, different, probably more usable metrics are indicated than proposed in the literature. A possible explanation can be because in real-life, metrics should also be easy to use, focus on effort and risks are directed to the buyer (anybody know the source? its in the lecture also.).

3 Methodology

3.1 The Data

The data methodology that is used in this research was based on techniques described by (Han, Pei, & Kamber, 2011). This section is used to discuss the data collection, data investigation and data-processing processes.

3.1.1 Data Collection

The main dataset used in this research is provided by CleanMX [1] , and contains hacked URLs, from a period of three years (2014 - 2016). Besides the compromised url, the dataset contains the timestamp. Additional datasets have been collected and used in this research for normalization purposes: (1) The total number of Internet users for the period 2014-2016 was obtained from internetlivestats[2]; (2) the population of countries for the period 2014-2016 was obtained from

[1] http://support.clean-mx.com/clean-mx/viruses.php
[2] http://www.internetlivestats.com/internet-users/

Worldbank [3]; (3) The total number of Internet users for the period 2014-2016 was obtained from internetlivestats [4] . The tld code for each country obtained from the Github repository: tld-list [5].

3.1.2 Data Investigation

Using R, an initial investigation of the dataset obtained from CleanMX was conducted based on the number of hacked URLs per year. The results showed the existence of records happening in 2013. The difference between 2013 (Fig. 2) and the other years was massive. Therefore, the values from 2013 were removed from the dataset since they can be considered as noise or outliers. After that, the dataset contained 3.624.831 rows. For the conduction of this research, only a sample (1%) of the dataset was used. This means, the data is reduced significantly to 36000 rows. An advantage of a smaller dataset is that it saves time. A reduced dataset may have implications on the viability and reliability of the results. First, the certainty that the dataset represents the population decreases, as a smaller dataset provides less information about the population than a bigger one. Furthermore, a smaller set gives less power to indicate differences and may therefore be less precise (Marley., 2017).

3.1.3 Data Preprocessing

The information provided from the initial dataset cannot be considered sufficient for the purposes of this research, since insight into the hacked URLs alone cannot answer the indicated questions completely. Therefore, additional information should be used and added in order to find answers regarding the security issue, as described in detail in section 3.2 - The metrics. Using the URLs, additional information was extracted. The attributes added to the initial dataset are the following:

[3] http://databank.worldbank.org/data/reports.aspx?source=2
[4] http://www.internetlivestats.com/internet-users-by-country/
[5] https://github.com/umpirsky/tld-list

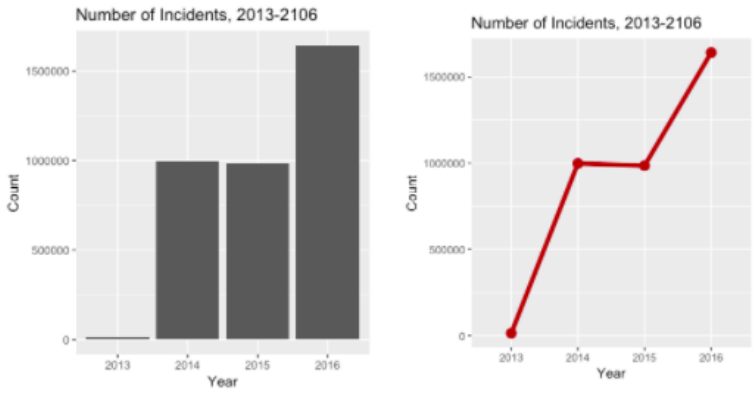


Fig 2 Total number of hacked URLs per year

- Domain of URL - Using urltools package
- TLD of URL - Using urltools package
- IP (Internet Protocol) address of URL - Using iptools package
- AS - Using cymruservices package

3.2 The metrics

The purpose of this paper is to identify patterns, trends over the three years time period and to give insights to hosting providers. These trends and insights can help hosting providers to evaluate their security level, regarding the websites they host. The developed metrics are based on different attributes extracted from the URLs. Aim is to try identify if attackers have some patterns when they are hacking websites. Possible questions are for example: Do hackers prefer some domains more than others? Are specific countries considered to be more vulnerable by hackers, which means they focus on specific TLD country domains or AS? However, it should be noted that those metrics are not ideal for hosting providers, since they can only give general indications for a hosting provider. An overview of the metrics and their definition is presented in Table 1.

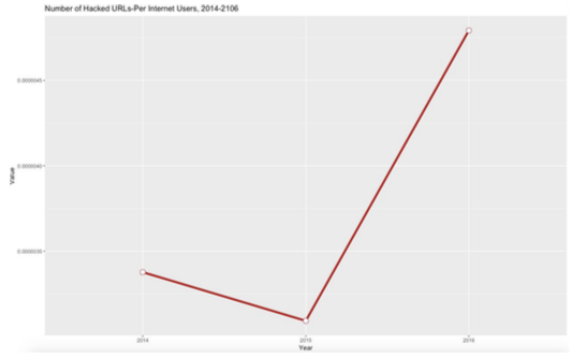
Table 1 Overview of Metrics

Metric	Definition
# Hacked URLs / Total amount of Internet users (2014 - 2016)	Examine if there is a dependency between the #Hacked URLs and the total number of Internet Users. How does the existence of more internet users influence the number of Hacked URLs? Do the two have a positive, negative or no relationship?
# Hacked IPs / AS	Examine which AS has the more #Hacked IPs over time
# Hacked TLD domains per country	Examine how many hacked URL occurred per country using the domain of each country (e.g. .nl, .au) and normalize the value based on the amount of internet users per country.
# AS with host hacked IPs per country / Countrys population	Examine which country has the most AS with hacked URLs and normalize the value based on the population of each country.
# Unique hacked domains / Total number of domains	Examine the number of unique hacked domains compared to the total number of hacked domains.
# Unique hacked domains / Total number of domains	Examine the number of unique hacked domains compared to the total number of hacked domains.
# Unique hacked IP addresses / Total number of IP addresses	Examine the number of unique IPs addresses compared to the total number of IPs addresses.

4 Results

4.1 # Hacked URLs / Total amount of Internet users

Figure 3 presents the change in the number of hacked URLs per Internet user over the time period (2014-2016), as obtained by dividing the amount of hacked URLs by the total amount of Internet users. It shows that in 2016 there were more hacked URLs per user than in the two previous years. However, based on the table showing the amount of Internet users and Figure 3, it can be concluded that in 2015 there were fewer hacks compared to 2014 despite of the growing amount of Internet



Year	Internet Users**
2016*	3,424,971,237
2015*	3,185,996,155
2014	2,956,385,569

Fig 3 # Hacked URLs / Total amount of Internet users

users. It can therefore be concluded that in general the number of Internet users does not give insight in the hacked URLs and the attacker behavior. So, hosting providers are not recommended to use this metric as an indicator to evaluate their security level.

4.2 # Hacked TLD domains per country

Figure 4 shows the value of the amount hacked TLD domains per country, normalized with the Internet users per country for each year. Figure 5 presents the average value of this metric for the three years (2014-2016). It can be observed that this value is steady over time for the most countries, which can indicate that the hosting providers did not consider this behaviour (of domains be hacked) as a vulnerability for their services, as they did not take any action to reduce it. On the other hand, when an extreme case appears, like Gabon in 2015, it is not sure if the hosting providers took action to solve this particular hacked domain, or that it was a random event from the attacker's side. In conclusion, the use of this metric can shed light on how vulnerable a country TLD domain is to attacks. This then can also give an indication on how attackers behavior changed over time.

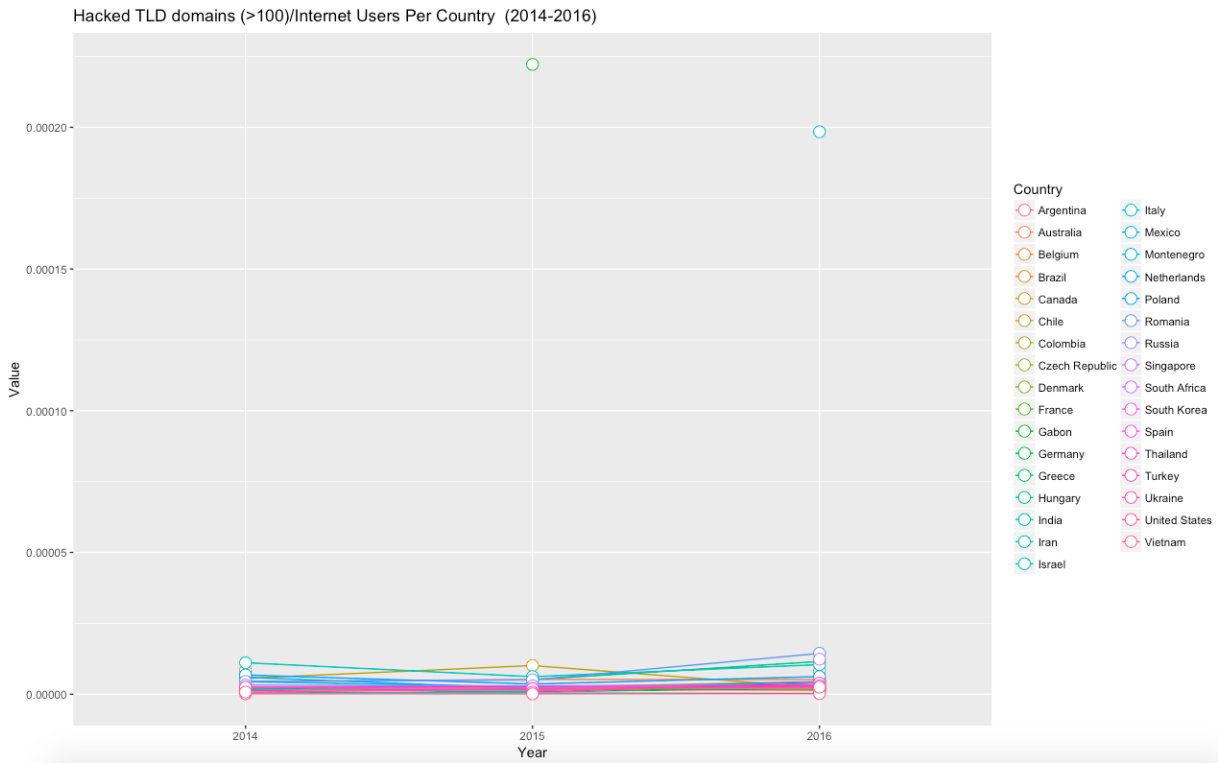


Fig 4 # Hacked TLD countries domains

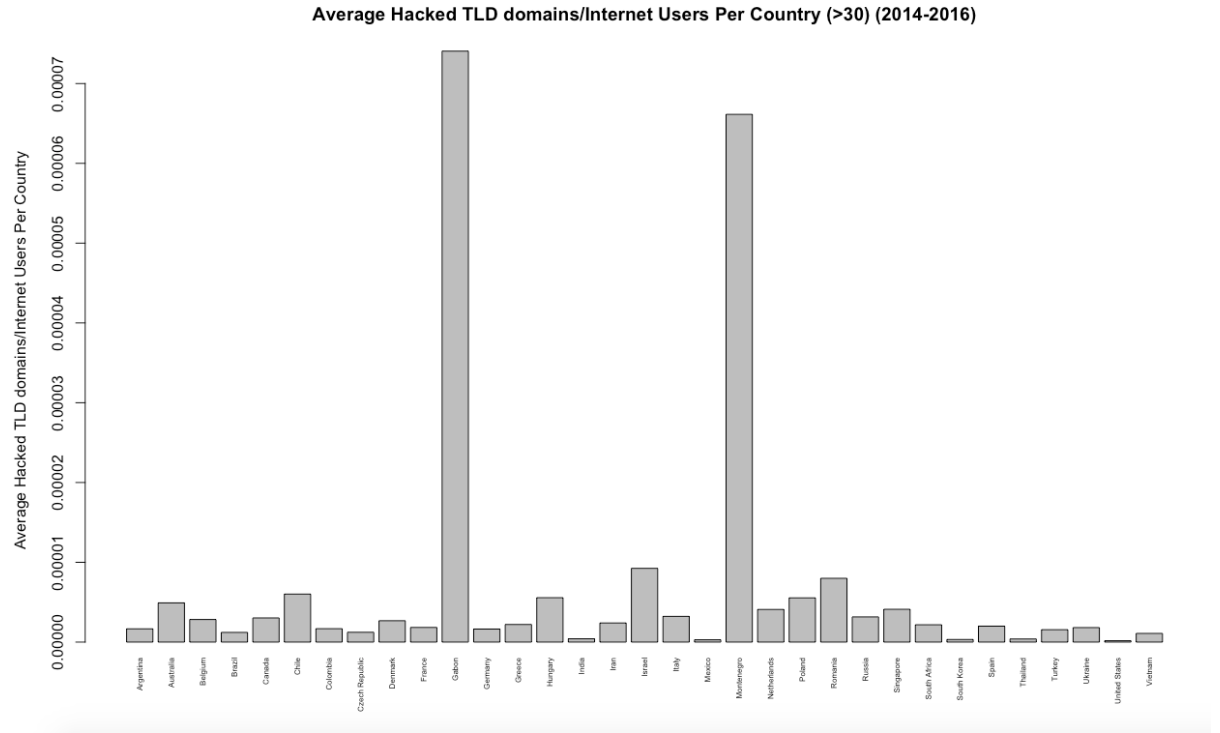


Fig 5 Average value of the hacked TLD domains per Internet user per country

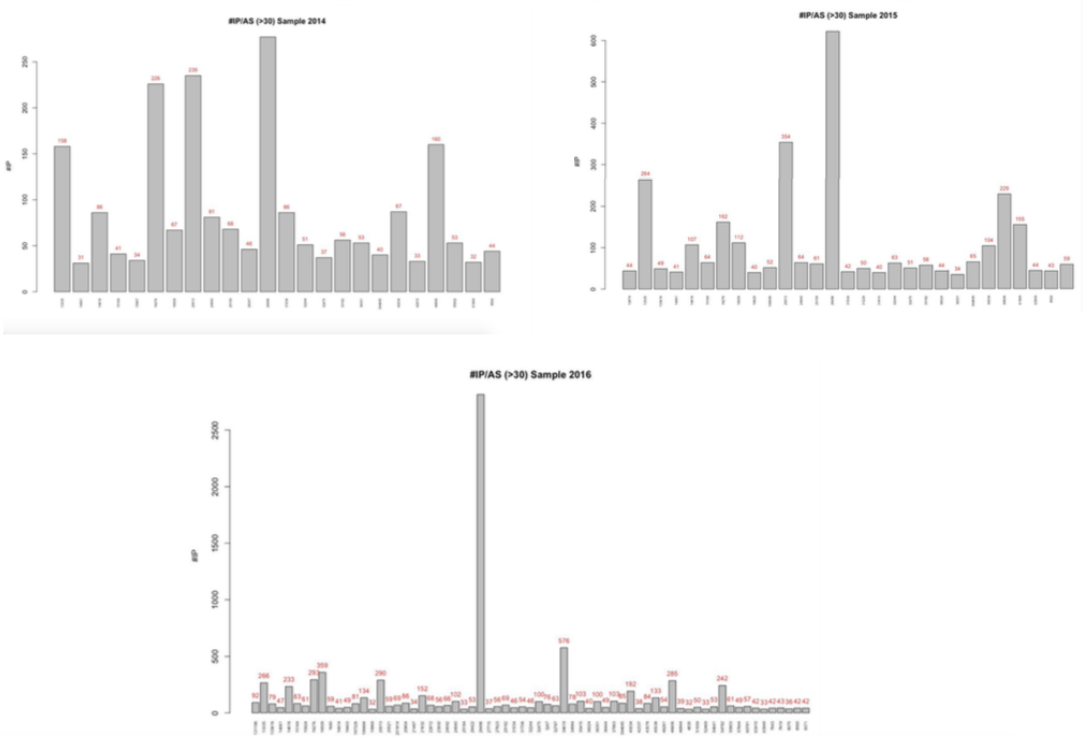


Fig 6 # Hacked IPs / AS

4.3 # Hacked IPs / AS

Figure 6 presents the AS with the highest number of hacked IPs over the three year-time period. Again, the results show that the AS have more or less the same values over the years, which mean that no action has been taken against the hacked IPs. Moreover, in 2016 an extreme number of #Hacked IPs is associated with one particular AS. This AS had the most hacked IPs over the years. In total, this metric can show which AS are associated more with hacked IPs and which countries and organizations are associated with specific IPs.

4.4 # AS with host hacked IPs per country / Countrys population

Figure 7 shows the value of the total number of AS per country normalized with the population per country for each year. Figure 8 presents the average value of this metric for the three years.

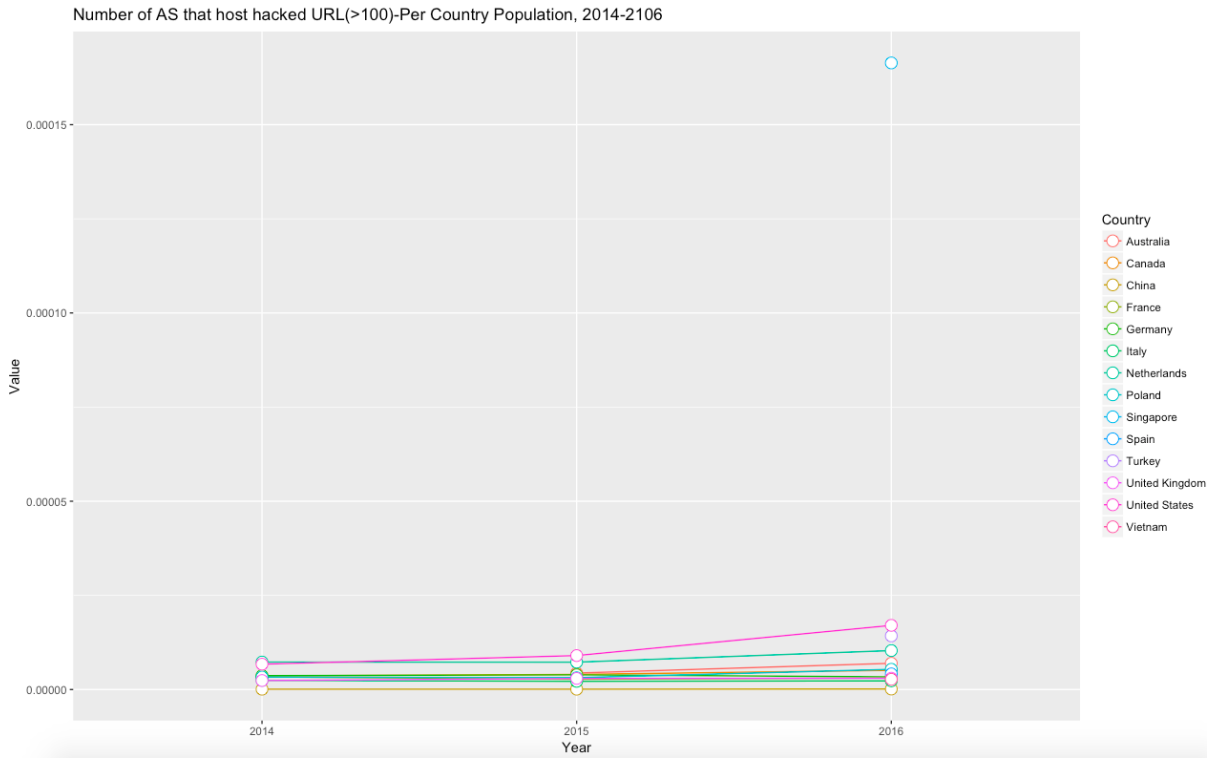


Fig 7 # AS with host hacked IPs per country / Countrys population

It can be observed that this value is steady over time for the most countries, which means that the same AS are having more or less the same number of hacked IPs over the time period examined in this research. Again, this metric can identify extreme or random cases of countries only occurring once during the investigated time period, but having a bigger average value than the rest of the countries. For example, Singapore has a bigger average value than the other countries, but appears only in the list with the countries with the most hacked AS. This metric can help identifying which countries have the AS with the most hacked IPs and could give indications on which countries are used by hackers as target.

4.5 # Unique hacked domains / Total number of domains

This metric examines the number of unique hacked domains compared to the total number of hacked domains over the years. The result, presented in Figure 9, show no linear relationship

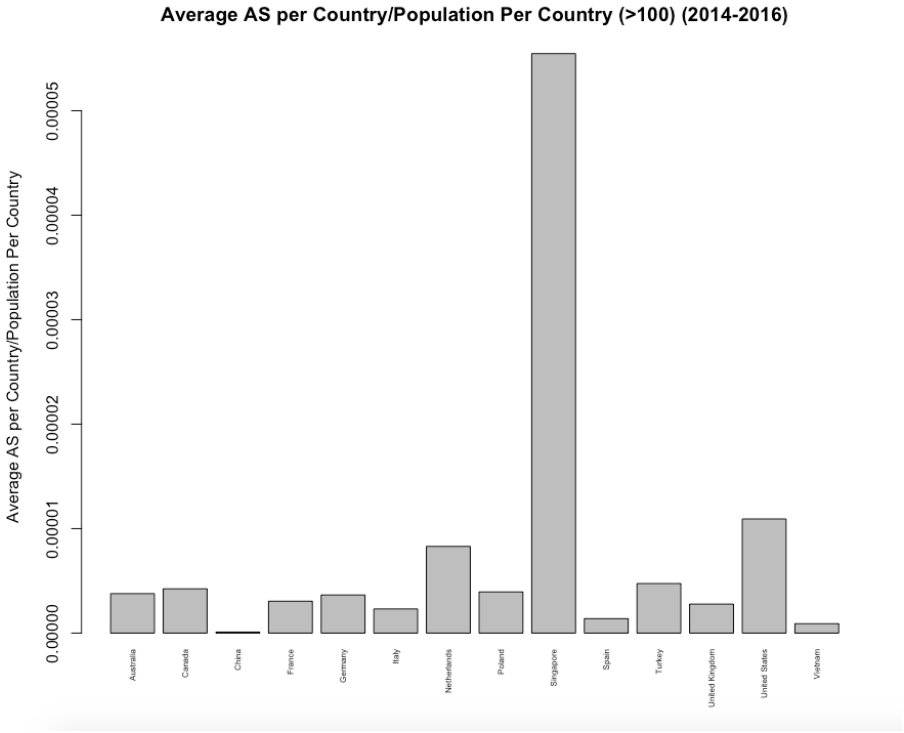


Fig 8 Average Value

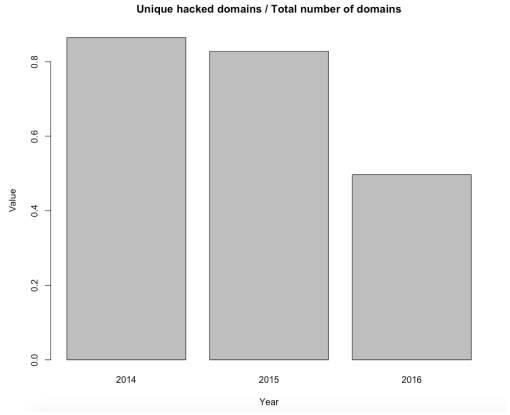


Fig 9 Unique hacked domains / Total number of domains

between both, but that some domains were attacked more often than once. This metric can help hosting providers identify differences in the number of unique domains being hacked every year. Also, it is an indicator that attackers sometimes target the same domain and do not always randomly attack different domains.

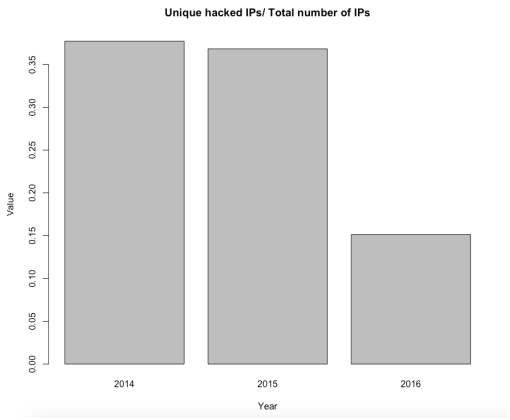


Fig 10 Unique hacked IPs / Total number of IPs

4.6 # Unique hacked IPs / Total number of IPs

Similarly to the metric in 4.5, this metric examines the number of unique hacked IPs compared to the total number of hacked IPs over the years. The results presented in Figure X show that more hacked IPs does not mean that more unique IPs were hacked, but that some URLs have the same IPs and were attacked more than once. This metric can help hosting providers to identify differences in which IPs addresses are more vulnerable and therefore more easy targets of hackers.

5 Conclusion

This paper presents a research that is aimed to define metrics that enable hosting providers to evaluate their security level regarding the security issue of hacked URLs. The dataset used in this research was obtained from CleanMX, which is a spamtrap tool. The following attributes were used: domain, IP address, tld and the AS of the URL. Other datasets, containing information about internet user and the population of different countries, were used for normalization purposes.

Overall, the results have shown that hosting providers did not have any incentives so far to take serious action or measures to prevent hacking of their websites. However, some metrics described in this paper, can provide the hosting providers indications regarding attacker behaviours. For

example when a specific or country domain, or an AS that has many different IPs addresses is targeted. The results have shown that over the years, attackers seem to target their attacks to specific domains and IP addresses. For example, even though there were more hacked URLs in 2016, the number of unique domains and IP addresses were smaller in comparison with 2014 and 2015. The total number of Internet users seems not to affect the number of hacked URLs, which indicates that more Internet users is not a driving force behind the hackers attacks. These metrics can help hosting providers to assess their security level, and give themselves a better position on the market. It is therefore recommended for hosting to focus on the Top-Level Domain (TLD) country domains and Autonomous Systems (AS) per country as indications for attacker behaviour when measuring the security of their services based on hacked URLs; rather than counting the amount of hacked URLs.

There are a number of limitations to the current research. One of them was the fact that a sample was used instead of the whole dataset. As using the whole dataset could lead to very different results, it is very difficult to make generalised conclusions before repeating the research for the complete dataset. Another limitation is that the AS is treated as one organization, while, in reality, an AS can belong to many organizations. It can be the subject of future research to examine what is happening on organizational level. Another subject of future research could be the focus of the file types hackers target more often in the URLs, are those regular .html files or other type. Finally, a research on how hosting providers make money and operate could answer the question why they seem to not care enough about hacked websites on their servers.

References

Anderson, R., Barton, C., ohme R., B., C. R., van Eeten M., M., L., & T., M. (2012). Measuring the cost of cybercrime. WEIS, 1-31.

Bluehost. (n.d.). *Shared hosting done right.* Retrieved 24 September, 2017 from https://www.bluehost.com/shared.

Böhme, R. (2010). Security metrics and security investment models..

Carlos Ganan, M. C., & van Eeten, M. (2017). Beyond the pretty penny: the economic cost of cybercrime. NSPW.

Fryer, H., Stalla-Bourdillon, S., & Chown, T. (2015). Malicious web pages: What if hosting providers could actually do something. *Computer Law & Security Review*, *31*(4), 490–505.

Ganan, C. H. (2017, September). *Tutorial block 2 measuring cybersecurity - wm0824 economics of cybersecurity.* TU Delft.

Han, J., Pei, J., & Kamber, M. (2011). *Data mining: concepts and techniques*. Elsevier.

HostGator. (n.d.). *Hostgator order form.* Retrieved 24 September, 2017 from https://checkout.hostgator.com/signup/shared/4/36/SNAPPY60.

Hosting, S. W. (n.d.). *Web hosting services crafted with care!* Retrieved 24 September, 2017 from https://www.siteground.com/.

iPage. (n.d.). *Get a website that works. it's quick and easy.* Retrieved 24 September, 2017 from https://www.ipage.com/special/start-today.

Marley., S. (2017, September). *The importance and effect of sample size.* Retrieved 24 September, 2017 from https://select-statistics.co.uk/blog/importance-effect-sample-size/.

Noroozian, A., Ciere, M., Korczynski, M., Tajalizadehkhoob, S., & van Eeten, M. (2017). Inferring

the security performance of providers from noisy and heterogenous abuse datasets. In *16th workshop on the economics of information security. http://weis2017. econinfosec. org/wp-content/uploads/sites/3/2017/05/weis_2017_paper_60. pdf.*

Siteground. (n.d.). *Just host web hosting features.* Retrieved 24 September, 2017 from https://www.siteground.com/.

SiteLock. (n.d.). *Cybersecurity solutions — sitelock.* Retrieved 24 September, 2017 from https://www.sitelock.com/products.

Van Eeten, M. (2017, September). *Tutorial block 2 measuring cybersecurity - wm0824 economics of cybersecurity.* TU Delft.

List of Figures

List of Tables