Economics of Security — Measuring Cybersecurity

Tycho Teesselink (s1560506)
Tariq Bontekoe (s1451278)
Æde Symen Hoekstra (s1479679)
Ramon Houtsma (s1245228)
Group 13 — Phishing

September 2018

1 What security issue does the data speak to?

There are two ways to look at the security issue of the data:

1. Companies lose money and reputation, since their customers are being targeted.
2. Domains are being misused.

The first viewpoint is mainly about social engineering, so getting people to do something they normally would not do willingly, i.e. give up their password or transfer money to an adversary such as a "Nigerian prince". Phishing attacks usually appear in two forms, either untargeted bulk attacks or targeted spear phishing [1]. These attacks might to lead to great repercussions for users or customers of a certain service or company such as infected computers, installation of ransomware or compromised credentials to ones bank account or digital identification. For the companies and service providers this has quite a negative turnout. Sometimes they have to compensate their clients with money and they will definitely lose reputation, when a lot of phishing mails are being sent 'on their behalf'.

This implies that the companies and service providers should want to mitigate the phishing problem, due to the negative effects it has for their business. Moreover, they are also in the position to try and do something about this, hence they are the main actors when looking at the phishing problem this way.

According to the 2018 phishing trends & intelligence report [2], there were roughly 16000 known phishing attacks per month in 2017. Contrary to previous years the main target shifted from financial institutions (21%) to email and online services (26%).

Popular attack vectors for phishing are listed below:

- SMS/mobile messages
- Social media
- E-mail
- URL padding (fake login pages)

The number of phishing attacks and the wide variety of attack vectors put into perspective the relevance of this security issue.

The second part of the phishing problem is that of domain name abuse. The actors that are affected by this are the top-level domains, since phishing might affect their reputation badly. In the current world of the internet each top-level domain is responsible for everything that happens underneath it and can be held responsible by ICANN [1]. This implies that a top-level domains reputation will decrease when the amount of phishing sites within its domain increases. This also implies that these TLDs will try to eradicate phishing sites in their domain, hence it is interesting to look into the abuse within their domain. In an article of Moore and Edelman [3] observed that a big proportion of URLs containing typos can be found on a relatively small amount of name servers. [4]

These two viewpoints together provide a good look into the security problem of phishing. On the one hand there are companies and service providers that do not want their reputation to be scathed or lose money and the TLDs do not want to lose reputation, which might result in an outflux of 'proper' users. It is also not unlikely to think that companies and

service providers will actually pressure TLDs to attack the phishing problem more rigorously and hence both groups of actors somewhat share the same problems and are likely to be interested in, at least partly, the same security metrics.

2 What would be the ideal metrics for security decision makers?

Expected damage to reputation.

Companies and TLDs experience damage to their reputation when their business is used, or their companies are targeted by phishing mails. When these companies are associated with many phishing campaigns, general trust might decrease, which could lead to reputation damage. It is therefore of interest for these companies to know what the expected reputation damage can be when, for example, deciding on counter measures.

Occurrence of companies in phishing attacks relative to size.

This metric shows which companies are targeted more than others, this is of course with respect to their relative sizes, for the amount of phishing attacks is dependent on the size of a company. This metric gives insight in popularity and will help companies in deciding how much they should invest in anti-phishing measures.

Return on investment (ROI) of awareness campaigns.

Knowing the return on investment is a very good metric, although very hard to measure. It helps on making decisions on how often campaigns need to be done, and whether other investments might be better [5]. This metric is useful for both companies and the TLDs as they both benefit from investing in counter measures.

Occurence of abused domains in TLD with respect to size.

This metric helps on improving control measures. If certain TLDs are used often, it might be a good idea to handle websites listed under this TLD with caution. This also implies that TLDs that have a high score on this metric could compare their practices with TLDs that have a lower score.[1]

Persistence of abused domains in TLD.

This metric helps on improving control measures. If certain TLDs are really quick in mitigating a phishing site when it comes up and others do not, this is interesting for companies in order to decide which TLDS have high risk. Moreover, TLDs can compare themselves with others and compare their methods in order to try and get a grasp of which methods work and which do not.[1, 4]

Reuse of attacks under different domain names.

Attacks that are being reused on different domain names show that there is still a lack of awareness. People apparently do not notice the body of the attack, only the domain name. This shows that there is still room for improvement in the awareness campaigns [1, 4]. This metric is very beneficial for companies that create and test awareness campaigns.

Type of phishing (banking/social media/...), so trends.

This metric helps companies understand what the current phishing landscape looks like, e.g. which type of companies are being targeted. This can help in deciding what awareness campaigns should look like, as well as what to look out for when attempting to prevent the creation of these sites. For example, TLDs will know that they have to be extra observant when sites that are similar to banking sites are being registered. [2]

3 What are the metrics that exist in practice?

We have decided to divide the metrics in practice in four different categories; controls, vulnerabilities, incidents and prevented losses.

Controls

Awareness program click rate. This metric provides an estimate of how security aware customers and users are. It may also show light on the effectiveness of the awareness programs that have been used in the past and if the click rate is decreasing over time. [6, 7]

Change in behavior of click rate. The change is very important as this shows whether customers or users are learning. If the overall click rate does not change, but every time a different person is affected, at least you can infer that the program is working. However, if the same person is affected each time, the program might not be effective. Companies can use this information to determine if change is needed and if so why these phishing attacks are still present. [6, 7]

Vulnerabilities

Time until detection and response. This metric can be used to determine how vulnerable a TLD is, and how fast a company or TLD detects a phishing site. The lower the response time, the better your chances of preventing an attack. Especially TLDs should find this interesting, since it tells them whether they should improve the time in which they take phishing sites down.[6, 8]

Incidents

Amount of successful attacks over time. This metric provides insight in possible compliance issues due to incidents. It shows whether there are any improvements since a certain point in time. This is interesting for companies in order to determine whether they should really invest into mitigating phishing sites. It is also helpful in determining whether past investments have improved the security. [7]

Occurrence of Abuse. Difference in amount of abused domain names in different top-level domains, in order to see which TLD has the biggest abuse issues. This metric should of course be used relative to the size of a TLD. [1, 4]

(Prevented) losses

Report time of phishing sites. Reporting phishing sites an important step. This helps to prevent customers and users to get tricked. Therefore the time it takes to report a phishing site should be measured, this gives an insight in whether companies, services providers and TLDs should put more effort into finding these sites.[6]

Persistence of Abuse. This measure will describe how quick TLDs and intermediate registrars are in removing a known abused domain.[1, 4]

4 Metrics designed from the dataset

Share of known phishing sites per country. Knowledge of phishing sites per country can help companies understand where high security risks may present itself. If one country is constantly the victim of phishing campaigns it might be beneficial to obtain countermeasures for that specific country.

Uptime (per virus / per TLD). This metric is incredibly powerful as it shows many companies what the 'health' of this TLD is. If the majority of all phishing sites are being hosted under a single TLD, it might be more attractive to pick a different TLD. It might also show that a TLD is actively working against phishing and therefore it might be attractive.

Ratio of attacks targeting specific companies. Companies can use this metric to review their own involvement in phishing websites. This may help them in deciding what actions might be needed to take, as well as how to improve their awareness campaigns, if any exist. This metric basically shows an overview of what the thread landscape looks like for phishing, which might also be interesting for TLDs.

Ratio of phishing sites per specific TLD. This metric can be regarded as a popularity measure for TLDs. If certain TLDs are used often relative to their sizes, it might be a good idea to handle websites listed under this TLD with caution. This also implies that TLDs that have a high score on this metric could and maybe should compare their practices with TLDs that have a lower score, since it might be that they have better measures in place to detect phishing sites prematurely. Of course, this might also have different causes but it might be worth it to take a look.

5 Evaluation of defined metrics

All metrics mentioned in the previous section have been evaluated using Tableau, the results and interpretation hereof will described below one security measure at a time.

Share of known phishing sites per country. In Figure 1 we see a ranking of the top countries, ranked in descending order of amount of phishing sites that is hosted in that country. We see that the United States is by far the most popular in comparison to other countries. Even we we consider their relative sizes, population sizes and technological position. It is also noticeable that for example the Netherlands is quite high up in this list, considering the small size of the country.

TLDs that host a lot in these countries should maybe try and discover the reason why this is the case in order to tackle this problem.

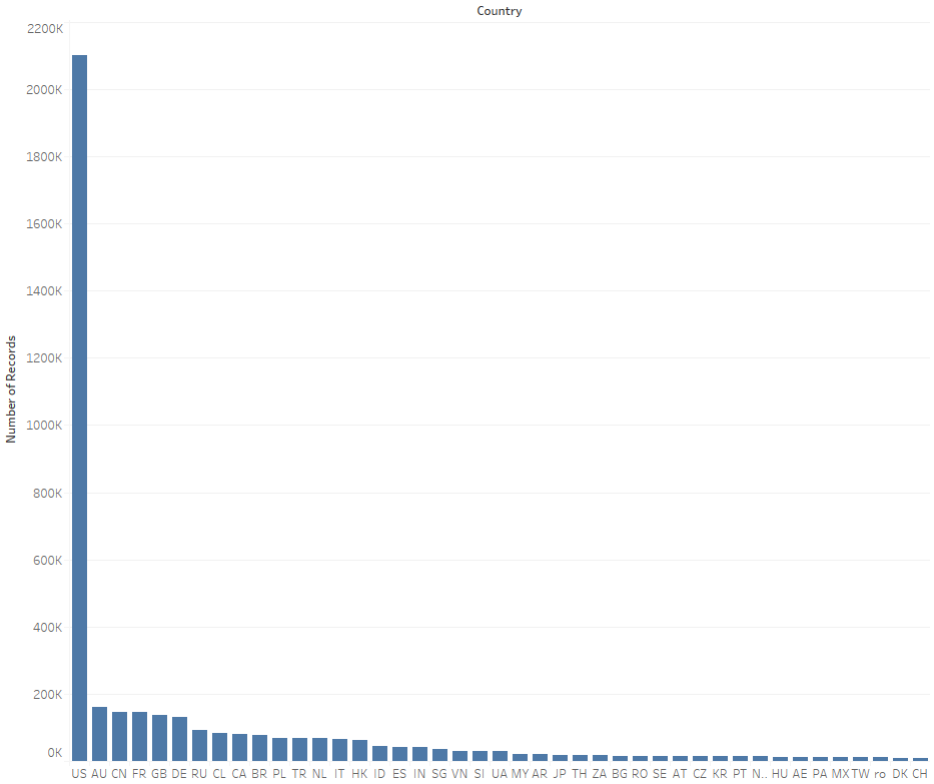

Figure 1: Number of known phishing sites per country (only top countries).

Uptime (per virus / per TLD). In Figure 2 we see a ranking of the different virus types in our dataset in descending order of average uptime. Please note, that only the ones with the highest uptime are included in the picture, due to the page size. The uptime is the time it takes to take down a phishing site. If this uptime is high this means that the site is probably more succesful for the criminals.

Companies that are scathed by this virus should think about investing more in detecting phishing sites of this type. The companies should of course also take into account how many phishing sites of this type there are, since this also gives a view on the size of the problem. Examples of these companies are Yahoo, the IRS and Deutsche bank, which can be seen in the figure below.

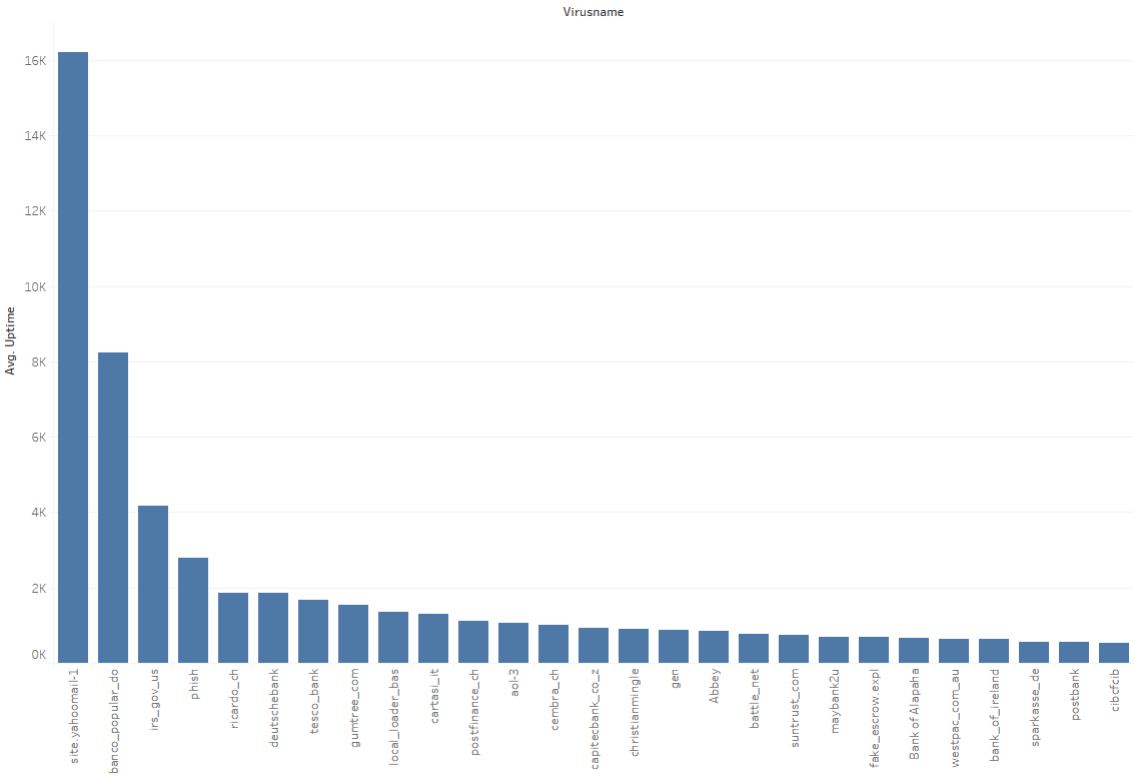

Figure 2: Average uptime per virus (only top averages).

In Figure 3 we see a ranking of the different TLDs in our dataset in descending order of average uptime. Please note, that only the ones with the highest uptime are included in the picture, due to the page size. The uptime is the time it takes to take down a phishing site. If this uptime is high this means that the site is probably more succesful for the criminals.

TLDs with a high average uptime should perhaps compare their practices with those with a low average uptime, to see if they could improve their controls. It is interesting to see that most TLDs that have high uptimes are quite unknown TLDs, such as .hm, .sb and .feedback. The more popular TLDs such as .com, and .uk are much lower in this list.

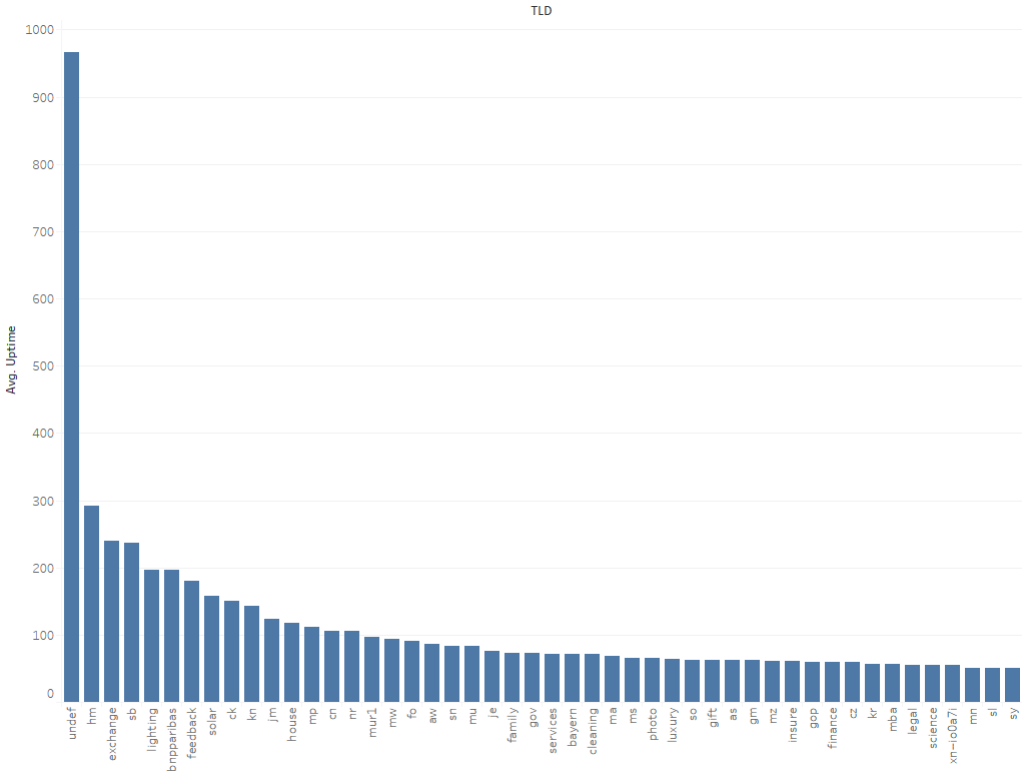

Figure 3: Average uptime per TLD (only top averages).

Ratio of attacks targeting specific companies. Figure 4 shows a ranking of the amount of phishing sites per company, ranked in descending order. The graph has been limited to only show the companies that had at least 25000 phishing sites, to limit the size.

The companies that are ranked really high on amount of phishing sites may need to take precautions, for example to warn their customers, as well as their employees. This metric is also useful when creating awareness campaigns. When creating such a campaign you want it to look as realistic as possible, therefore using one of these companies could result in a better result. Finally TLDs might be able to more actively look for domains that are being registered that resemble the actual domain of the company, which could result in a quicker detection and takedown.

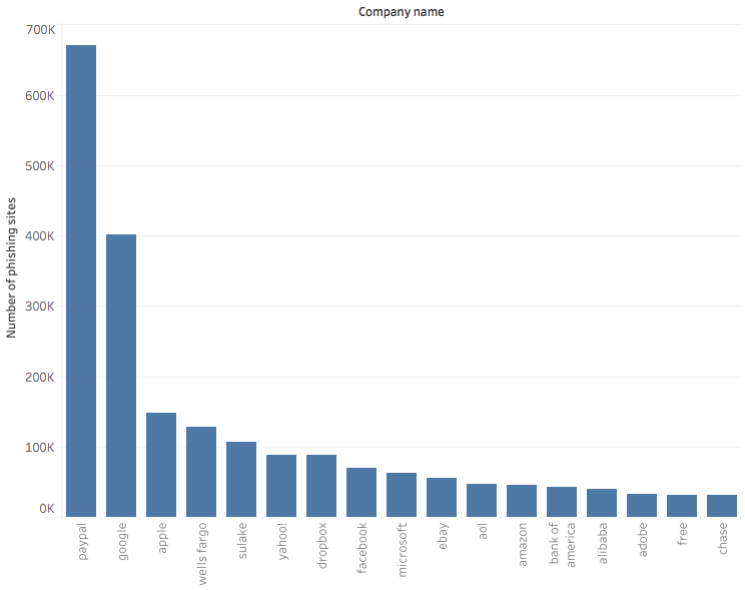

Figure 4: Amount of phishing sites per company with at least 25000 associated phishing sites.

Ratio of phishing sites compared with average uptime of a phishing site per specific TLD. In Figure 5 we can see which TLD are the most common for phishing sites. We can also see the average uptime of a phishing site for that same TLD. When these two are compared a view of how well a certain TLD is handling their phishing problems. For example, we can see that the .com TLD, is very popular for phishing websites, however they also have a very respectable takedown time, whereas the .cn is less poplular but has an insane average takedown time. This metric is also interesting for TLDs, to review what they should look out for.

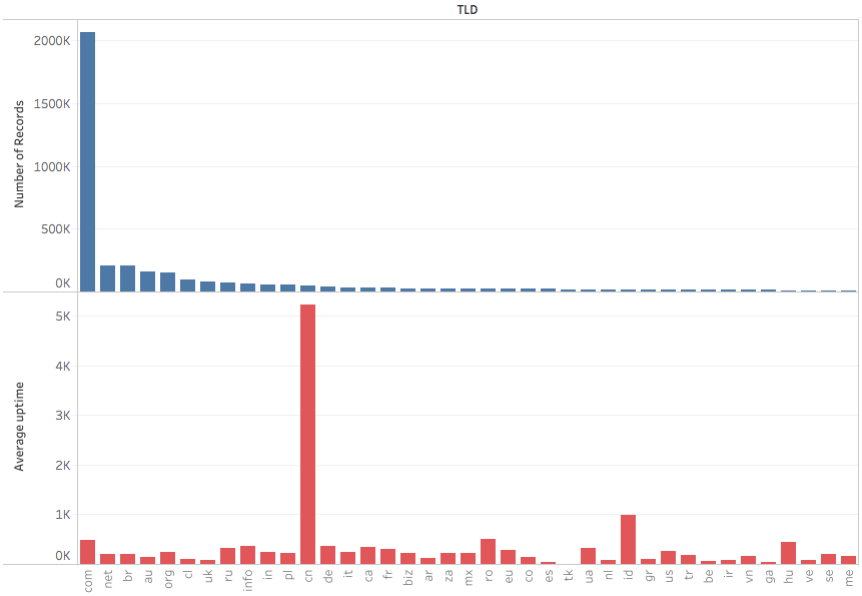

Figure 5: Share of phishing sites per TLD combined with average uptime of phishing sites hosted per TLD.

References

[1] T. Moore and R. Clayton, "Examining the impact of website take-down on phishing," *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, 7 2007.

[2] Phishlabs, "2018 phishing trends & intelligence report," Phishlabs, Tech. Rep., 2018.

[3] T. Moore and B. Edelman, "Measuring the perpetrators and funders of typosquatting," *Proceedings of the 14th International Conference on Financial Cryptography and Data Security*, 2016.

[4] M. Korczyński, S. Tajalizadehkhoob, A. Noroozian, M. Wullink, C. Hesselman, and M. van Eeten, "Reputation metrics design to improve intermediary incentives for security of tlds," *SIDN Labs*, 2017.

[5] Infosecurity-Magazine. Measure ROI of phishing awareness and education training. [Online]. Available: https://www.infosecurity-magazine.com/opinions/measure-phishing-awareness/

[6] Cybeready. (2017) Assessing your phishing risks — what metrics should you rely on? [Online]. Available: https://cybeready.com/assessing-your-phishing-risks-what-metrics-should-you-rely-on/

[7] R. Fahey. Anti-phishing: Measuring phishing awareness training effectiveness. [Online]. Available: https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-countermeasures/anti-phishing-measuring-phishing-awareness-training-effectiveness/

[8] L. Spitzner, "Measuring change in human behavior," RSA Conference, 2 2014, in cooperation with SANS.