Economics of Security Assignment 2

Group 11: Malware domains

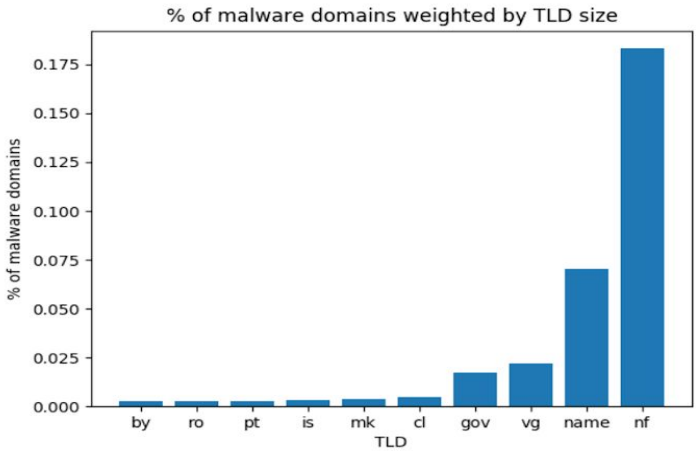
Niels Gijsen, Noah Goldsmid, Samiksha, Jeroen Weener

Problem owner

A problem owner is the one responsible for a problem. It is his duty to handle it. In the case of malware domains, the problem owners are the hosting providers. To avoid attracting attention to themselves, cyber criminals do not often run their business on their own servers. They either get a server from a hosting provider, or they hack a website of someone else (which is probably also located on the server of a hosting provider). While hosting providers cannot be held accountable for the malware they host [1], it is in their best interest to uphold their reputation. Besides, they exert the most influence on the problem since the malware is on their servers. Therefore, hosting providers should strive to detect and remove malware from their servers as soon as possible.

Relevant differences in security performance

One of the most significant differences in security performance of domain names can be found based on the Top Level Domain (TLD). When looking at the TLD of the malicious domains and weighing them by the size of the TLD, we see that four TLD's are obviously more represented in the dataset as the others, as can be seen in figure below.



The differences shown by this metric can be hypothesised in multiple ways, for example the TLD's might be easier for attackers to hack or register. Or it can be the case that these malicious domains are skewed because of the irregularity in user reports. Nevertheless this metric can be considered valuable for our actor, the hosting provider.

Most hosting providers want to avoid hosting malicious content on their servers for various reasons. Our metric can support hosting providers, the metric shows that certain domains might be more susceptible to being malicious than others. Hosting providers can implement security measures based on the TLD of the domain thus reducing the chance of hosting malicious content or increasing the speed at which is detected.

Risk strategies the problem owner follows to reduce security issues:

It is essential to know how to prioritize risk before choosing any risk management strategy. The hosting providers who are the problem owners must follow a plan. A plan that may involve risk mitigation, risk transfer, risk acceptance or risk avoidance. Any of the following four strategies can be chosen depending on the severity of the attack that is imposed on the customers (also visitors) and credential information.

Mitigation: The hosting providers must start with prevention techniques. [2]The log in to data center space access must be limited to trained technicians with security clearance in order to avoid the unwanted access to the web page and source code manipulation. The hosting

providers must monitor the internal networking frequently and once a malicious activity is detected , they can take down the website temporarily as it may deter the visitors.

Transfer: Digital information and it's availability are vulnerable targets of cyber crimes. Also data breach can cost enough to withdraw from the market. Cyber liabilities insurance works for such IT businesses. The hosting providers invest in purchasing cyber insurance because they might not want to lose their reputation and customers as well. They want a third party to work for them and help them at an affordable cost. The insurance covers the defacement websites. This risk transfer strategy can cover the basic cost of the loss and make the hosting providers survive in the marketing business. [3]But it will not reduce the extra work that would be needed to fix the security flaws. [4]SLAs typically cover server-based resources rather than server performance levels. The provider as well as the client can be liable for not following the agreement. [5]There are situations when hosting providers are not responsible for the content that has been added in the website by the customers. The hosting providers cannot keep a check on the all the content but can rely on the visitor's reviews. This may also attract the cyber criminals to play with website. Thus the hosting providers can clearly state it's terms and conditions while creating a customer's account and the customer can become liable for not following them. The hosting provider can suspend or limit the access of the defaulter's (customer) account. For instance, the account holder finds out about unknown intrusions, or a hint of SQL injection, reviews of getting phishing emails by the visitors, and still takes no action which later bring catastrophic damages.

Acceptance: A hosting provider has to accept some level of risk. The question is how much risk the provider allows. It includes investing little higher on the security issues or sharing the host with other servers. If the dedicated team fails to fight against the malware cyber attack and the cost structure to handle the security issues gets disbalanced, the host providers are unable to mitigate the risk. The host providers come across several threats, but they need to assess which threats are minor or major. Risk acceptance is to ignore those minor risks. But this could lead to the withdrawal from the market as this little intrusion might just be a warning of major threat.

Avoidance: To avoid the risk, it is important for hosting providers to lay certain rules. End users and their information are prone to cyber attacks. Cyber crime master minds try every possible thing to either get that information from the website or bring that website down permanently in order to deteriorate the business reputation of the hosting provider, make money from the customers and gain the political incentives. There could be customers who intent to host malware content, send spam mails, host botnet controllers from. Thus the hosting providers must screen its customers before creating an account. This could be done by keeping a check on the IP address used to sign up, browser(user agent) and checking the blacklisted customers if they are trying to sign up again.

Other influencers

In this section, we will take a look at other actors that can influence the problem of malware domains. Besides hosting providers there are three other influences: the potential victim, application owners and domain registrars. We will discuss their possible risk strategies below.

(1) (Potential) victim of online cyber crime

Maybe the most obvious actor is the victim. The victim is the actor that visits the malicious site unintended and/or unknowingly and has his credentials stolen. Even though the victim is mostly unaware at the time of visiting the malicious website, he is aware of the global problem, and has strategies to control his risk.

Risk Strategies

Mitigation

Internet users can use two-factor authentication. This way it is harder for attackers to abuse potential data gathered from phishing. They should also use unique passwords per website, that way a single phishing attack can not breach the security of all of the victim's accounts.

Avoidance

Internet users can avoid using more obscure websites or even the internet altogether. Of course this is not a black and white strategy. The victim could decide to do all of his banking business offline, completely avoiding the risk of getting his bank account phished.

Transfer

Transferring the risk is not always possible. However, in some cases a service might offer a refund in case of a hack.

Acceptance

Internet users could accept the risk of getting phished. While not ideal, for many users their account security is not that important. Combined with partial avoidance for the few accounts the victim deems important, this is probably the way the regular internet user controls his or hers risk.

(2)Owner of online application

As stated in ‘Problem Owner’, cyber criminals are known for hacking domains to take over their control. They can then use these domains to host malware. This has the advantage that they do

not need to host the malicious website themselves, which makes it easier to hide his or her trails. Furthermore it has the additional benefit of already driving traffic to the malicious website. To reduce the risk of their domain getting stolen, online application owners should strive to protect their applications from being vulnerable.

Risk Strategies

Mitigation

The owner makes sure to apply software patches when they become available. Additionally, he can hire an entity to pentest his application, to make sure that there exist no known critical vulnerabilities. make use of existing software that is considered safe. Pick a hosting provider that is considered ‘safe’ and ‘secure’ (next to no malware, good detection, fast removal).

Avoidance

Have less of an attack surface. This could be achieved by reducing website functionality for example. Another way to avoid risk is to make use of software that is considered safe by the industry and by picking a hosting provider that is considered safe and secure in terms of malware detection and removal.

Transfer

Application owners can outsource the task of patching and defending their online applications. This way they could insure by opting for a SLA or different method of risk transfer.

Acceptance

If the availability of the online application is not important to the actor, or if the cost of protecting the application transcends the benefit of having the application online, they can choose to accept the risk. This might be the case when the application is a proof of concept rather than a business making service.

(3)Domain Registrar

Most domain registrars are not happy to host malicious domains. Mostly because it impacts their reputation. Furthermore, law enforcement can force a registrar to take down malicious sites, which means it generates additional work for them.

Risk Strategies

Mitigation

A registrar could combat malicious domains by actively searching and blocking them. Developing automated detection or hiring people who manually validate websites are two examples of this.

Avoidance

The register could partly avoid the risk by screening potential customers beforehand, or stop distributing domains to unknown parties altogether

Transfer

Just like the application owner, the register can outsource the mitigation strategy and consider a SLA to transfer the risk to a third party.

Acceptance

The register can also accept malicious domains. After all, asides from reputation losses, its not a huge problem for a register.

Risk strategies over time

Even though the internet has grown a lot over time, these risk strategies have not fundamentally changed. With the rise of SaaS businesses, the possibilities of transferring risk through a SLA have increased. DNS has not changed much in this aspect since the early ages of the internet, and as such, the strategies for registrars or hosting providers have not significantly changed.

References

[1] Web Hosting Provider Liability for Malicious content. (2011). [ebook] StopBadware Inc. Available at: https://www.nist.gov/sites/default/files/documents/itl/StopBadware_Web-Hosting-Provider-Liability-for-Malicious-Content.pdf [Accessed 28 Sep. 2018].

[2]url: https://www.hostingadvice.com/how-to/web-hosting-security-best-practices/ (accessed on 27/09/2018)

[3]url: https://ig.ft.com/sites/special-reports/cyber-attacks/ (accessed on 28/09/2018)

[4]url: http://www.crucialp.com/resources/tutorials/web-hosting/slas-and-web-hosting/ (accessed on 28/09/2018)

[5]url:https://webhostinggeeks.com/blog/can-you-be-held-liable-for-a-website-you-host/ (accessed on 28/09/2018)