Economics of Security Assignment 2

Group 11: Malware domains

Niels Gijsen, Noah Goldsmid, Samiksha, Jeroen Weener

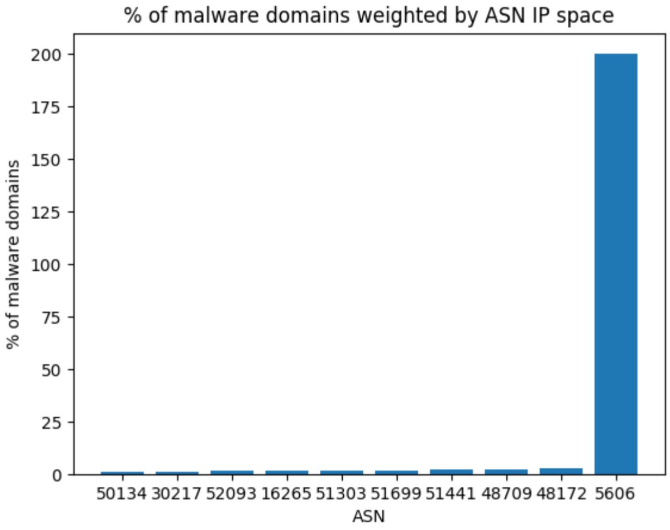
1. Problem Owner

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.

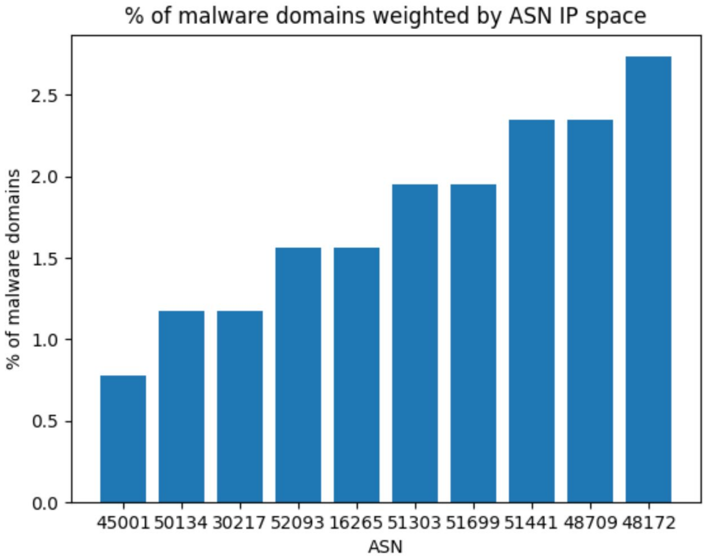
2. Relevant Differences in Security Performance

Evaluating the security performance of hosting providers can be a difficult task, there are a lot of variable at play. One metric that could be useful for this is the percentage of malicious domains hosted by the hosting provider. However this metric can be considered an ideal metric, while no perfect information exists on this topic.

With the dataset provided one can create an estimation of this metric. The Autonomous System Number (ASN) of each incident is reported, combining this with public records such as IP space per ASN we can create some useful metrics. We assume a hosting provider uses one ASN and do not take into account that multiple domains can be hosted on a single IP. This resulted in the graph below:



The metric shows that we have one extremity at 200%, upon further investigation this was caused by the fact that the ASN of 5606 has only one IP address registered. On this address, two malicious domains were hosted, therefore we excluded ASN 5606 from the graph, resulting in the following graph:



In the graph the top 10 ASNs are displayed this shows us the highest percentage of malicious domains is 2.6%, furthermore apart from the top 9, all ASNs have a malicious percentage of <1%. Most hosting providers want to avoid hosting malicious content on their servers for various reasons. Our metric shows the differences in the amount of malicious domains hosted on ASN, it has some limitations, however it gives a good indication in the performance of a single ASN and thus hosting provider.

3. Possible Risk Strategies of the Problem Owner

[7]“Web hosting providers are in the position to play a key role in the security of the Web. In fact, they host millions of websites that are often poorly managed by unexperienced users, and that are likely to be compromised to spread malware and host phishing kits”. 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. A fine balance between techniques and security has to be established, so that all sites function properly without being exposed to any damage or danger. [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.[9] Integrity checks to detect changes on files and directory systems is mandatory in the light of the major threat of website defacement. Another way to mitigate malware risks is to install host-based firewalls for defending a set of hosts.

In order to strengthen controls of network peripheral, a hosting provider would prefer to mitigate the risk. There are certain policies where hosting providers are liable to its customers for cyber crime or malicious activities and here risk mitigation can reduce the induced risk impact. This leads to another reason for preferring mitigating risk, that is, vulnerability management. It could help the hosting providers to regain the trust of its customers and encourage them continue buying the services.

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 provider finds out about offended content, or a hint of SQL injection, reviews of getting phishing emails by the visitors, from one of its user accounts. The provider warns the user to perform necessary amendments but the user does nothing 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, the cost structure to handle the security issues gets disbalanced and host providers fails to reduce such risk impacts. 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: 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, gain access to private user data, eat up web server resources and gain the political incentives. There could be customers who intent to host malware content, send spam mails, host botnet controllers from. To avoid the risk, it is important for hosting providers to lay certain rules. 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. [7] Providers can employ URL blacklists in order to prevent SQL injection attempts and remote file uploads.[8] Both inbound and outbound network traffic should be examined for known malware patterns and signatures using intrusion and/or prevention detection systems.

4. 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.

(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.

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.

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.

5. 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.

Return on Security Investment

In this section we will look at the Return on Security Investment (ROSI) for hosting providers using the mitigation strategy as stated in *Possible Risk Strategies of the Problem Owner*. We do consider the measures discussed in this section with the exception of restricting access to data center space, since the problem stems largely from outside the hosting providers and unwanted access to a web page and source code manipulation are rarely the cause of malware domains.

The Impact

The impact for the hosting provider when a domain gets infected with malware is based largely off of the reputation damage they incur when this happens, since they do not suffer direct losses from the malware being active. Customers of the hosting provider obviously dislike it when their domain gets infected with malware or when control is taken over entirely. The reputation cost the hosting provider suffers depends on the type of customers the hosting provider serves, the size of the hosting provider and factors such as timing, due diligence and the response of the hosting provider when a report of malware is made. It also depends on whether the malware gets detected at all and by whom [6]. We could not find a reliable method for quantifying these factors. Also, since we do not consider a specific hosting provider, it doesn't make sense to accurately estimate these values. We think it is likely that the cost is normal distributed. Our estimates are based on intuition.

Strategy Cost

Determining the cost for the mitigation of the risk is difficult, as the cost is dependent on a lot of variables. For instance is the hosting provider going to buy multiple licences of anti malware software, or is it going to install a hardware device. Furthermore some solutions are dependant on the malicious domain itself, for instance, a domain that handles 500GB of monthly traffic would be more expensive to protect than a domain that handles only 1 GB of traffic.

In order to calculate the ROSI of this strategy, some numbers are needed for the cost. In order to take as much as possible into account, we are going to determine the cost of a low end solution, an average and a high end solution. This band of different prices will be used for further calculations.

Low-end solution
As a low end solution we are going to use an off the shelf anti malware application. The cost of an enterprise licence of Malwarebytes(one of the most popular anti malware applications) is around EUR 35.- yearly per machine. Most of the scanning will be done automatically however some incidents require actions by a employee. We assume these actions will cost 2 hours monthly, with an average hourly rate of EUR 50.-, this comes in a total of EUR 1235.-

High-end solution
Solutions which give more types of protection such as a Web Application Firewall(WAF) can help domains to stay uninfected. For the estimation of this solution we took the monthly price of Cloudflare, as this company has a big market presence and an clear pricing. The enterprise level plan is EUR 200.- monthly. Even when outsourcing the protection, some labour is needed to set up the service, we estimate an initial set-up time of around 4 hours, with maintenance of 0.5 hours monthly. Using the same hourly wage, this results in a total of EUR 2900.- yearly.

The Frequency

In this section we will look into frequency distributions of an incident happening, using the data from malwaredomainlist. As explained in the first section, we look at the amount of incidents per autonomous system, weighted by the size of their IP-space. This is the occurence of malware domains per IP owned by the autonomous system.

From the data we extracted the occurences of 440 autonomous systems. For every AS we have the amount of incidents per IP they own expressed as a percentage. This is the same data as shown in the first section. Using a normal test from scipy [10], it looks to be a normal distribution with a mean of 0.072% and a standard deviation of 0.286. This translates to 291 incidents per year on average.

To prevent outliers from distorting our estimation, we ignore all values that differ more than twice the standard deviation of the mean. This leaves us with 430 results.

We assume that every AS is associated with one hosting provider. Every hosting provider will control it's risk in their own way. As we can only observe the outcome, and not their way of controlling the risk, we assume that the worst performing autonomous systems have put in the least effort of mitigating the risk, and the best performing have put in the most effort. Using this we can estimate what incident frequency we will endure if we chose to invest in security.

In our data the average autonomous system owns 2020470 IPs. Below we will sketch two different scenarios. In these scenarios we will assume the point of view of an averaged sized hosting company.

Assuming the worst 20% have little to no security and the best 20% have invested in security, we can estimate the following two scenarios:

Unsecured

In this scenario we do not invest significantly in security. This means we will perform similar to the bottom 20%.
Mean: 50021 incidents per year
Standard deviation: 50099 incidents

Secured

In this scenario we do invest significantly in security. This means we will perform similar to the 20% best performing autonomous systems.
Mean: 47 incidents per year
Standard deviation: 44 incidents

ROSI Distribution

Cost of incident incurs hourly wage of an employ to remove the malicious content and clean up the hacked website. We assume that it takes 2 hours to remove the malware at the cost of EUR 20/ hour. Two hours may seem a little high, but we assume that it takes some work to figure out how and who uploaded malware. Then it needs to be fixed, the rightful domain owner needs to be contacted about the breach. The incident cost can thus estimated to be EUR 40 (2 hours).

To calculate total cost for low-high cost solutions with respect to incident frequency of unsecured-average-high secure scenario, we use total cost cost formula: solution cost + (incident cost * incident frequency).

- For unsecured scenario, there are no solution costs:
  total costs = 0 + (40 * 50021) = EUR 2,000,840
- The average secure scenario with lost cost solution gives:
  total cost = 1235+(40 * 291)= EUR 12,875
- The high secure scenario with high cost solution gives:
  total cost = 2900+(40 * 47)= EUR 4,780

We now calculate the ROSI for highly secure scenario with high cost solution since it produces the best cost structure and high security as well.

$$\text{(1)}\quad ALE_s = Impact \cdot Probability\ (Annual) = 40 * 47 = 1880$$

$$ALE_o = Impact \cdot Probability\ (Annual) = 40 * 12875 = 11640$$

Where ALE_s is Annual Expected Loss for high secure scenario, ALE_o is Annual Expected Loss for low secure scenario. *Impact* is cost per incident and *Probability* is mean of the frequency of respective scenario.

$$\text{(2)}\quad ROSI = \frac{ALE_0 - ALEs - c}{c} = \frac{11649 - 1880 - 1665}{1665} = 4.8$$

C is the difference of solution cost for high and low secure scenario

Conclusion

As seen in the section above, investing in security to prevent as many incidents as possible has a good return on investment. Malicious domains tend to seek out the worst protected hosting providers. This is probably due to the fact that they do not care so much as who is hosting it, and they are too short sighted to care about the quality of the hosting. This means that there are significantly more incidents on providers who have little to no protection.

This means that some investment is absolutely necessary, otherwise the costs would be very high as every incident needs manual cleanup (totalling to EUR 2,000,840) However, the difference between low security or high security is a little less extreme. The difference in solution cost is smaller than the benefits of having even less incidents. This results in a very attractive ROSI value of nearly 5.

However, it should be noted that due to the high variance in the the dataset, it's possible that the actual incident frequency differs. In extreme cases the could mean that the investments are no longer worth it. However since it's a relatively small investment, and the expected result is lucrative, we think it is the best choice to opt for high security.

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 27 Sep. 2018]

[3] url: https://ig.ft.com/sites/special-reports/cyber-attacks/ [Accessed 28 Sep. 2018]

[4] url: http://www.crucialp.com/resources/tutorials/web-hosting/slas-and-web-hosting/ [Accessed 28 Sep. 2018]

[5] url:https://webhostinggeeks.com/blog/can-you-be-held-liable-for-a-website-you-host/ [Accessed 28 Sep. 2018]

[6] Jones, J. (2006). An introduction to factor analysis of information risk (fair). *Norwich Journal of Information Assurance*, *2*(1), 67.

[7] The Role of Web Hosting Providers in Detecting Compromised Websites. Available at: http://s3.eurecom.fr/docs/www13_canali.pdf [Accessed 6 Oct. 2018]

[8] Malware risks and mitigation report. Available at: https://www.nist.gov/sites/default/files/documents/itl/BITS-Malware-Report-Jun2011.pdf [Accessed 6 Oct. 2018]

[9] https://www.giac.org/paper/gsec/2040/cios-guide-managing-security-risk-web-hosting-contracts-managers-w/103521 [Accessed 6 Oct. 2018]

[10] https://docs.scipy.org/doc/scipy/reference/generated/scipy.stats.normaltest.html [Accessed 7 Oct. 2018]

Contributions

All the group members decided the problem owner in chapter-1. Niels Gijsen covered chapter-2 “Relevant differences in security performance”. Samiksha contributed for chapter-3 “Possible Risk Strategies of the Problem Owner”. Noah Goldsmid and Jeroen Weener covered chapter- 4 “Other influencers”. Noah also calculated the frequencies for secured and unsecured scenarios. Noah and Samiksha calculated the ROSI distributions. Niels and Jeroen together contributed for chapter-5 “Risk strategies over time” and its sub sections.