Security strategies of hosting companies

WM0824TU Economics of Cyber Security

Group 10 – Facebook threats

Arnoud Toering - 4380061 Valentijn Grapperhaus - 4250338

Yorick de Boer - 4287304 Martine Romer - 4248759

Introduction

From the Facebook Threat exchange dataset that was obtained we decided to focus on the security issue concerning compromised websites. In this scenario, a malicious actor takes over a website or part of a website and uses it to spread malware to its users. A website can be compromised in multiple ways, such as exploit kits and DDos. Websites are often hosted on virtual machines or even shared web hosting solutions, ran by specialized firms using big data centers. This means that the actual website owners do not have to manage the infrastructure themselves. The hoster is therefore responsible for updating its software, so that it includes the latest patches for potential security vulnerabilities, that in turn could lead to the websites being compromised.

The ***problem owner*** of this security issue, are hosting companies. The hosting companies are responsible for security of their hosted websites. Therefore they play a crucial role in the security issue. They have instruments to implement security measures in order to avoid successful attacks. There are various hosting companies offering different services and using different measures, leading to differences in price and quality. When one of their hosted websites is attacked, the website owner will hold the hosting company accountable. This could lead to damage repayment, as well as negative reviews and bad publicity. Moreover, the hosting company will have to tackle the security problems revealed by successful cyber attacks, before more websites become victim of it.

Dataset

The dataset identifies several categories of attacks on a multitude of urls. There's only a security issue when a websites indicates to be compromised, because those attacks were successful. This resulted in about 350 compromised urls per day. Since the website owner is not the problem owner but the victim, those urls are traced back to their hosting company.

In this report describes differences in security performance of three hosting companies. We choose these companies based on the metric of the amount of reported compromised websites over the course of half a year. This metric was normalized by dividing this number by the total amount of IPv4 addresses[1] assigned under the company's AS number. We are aware that this is not a perfect normalization, given that a hoster can also use these IP addresses for other purposes than hosting individual websites, but chose to accept this limitation. We only looked at hosters hosting full websites, so companies hosting redirection and load balancing only like Cloudflare are discarded.

Structure of this report

The structure of the report will be as follows. First, the risk strategy of the main problem owner GoDaddy will be analysed. Then, the other involved actors and their influence on the security issue are discussed. This is followed by a comparison of alternative risk strategies used by other hosting

[1] Assigned IPv4 blocks were obtained from "https://ipinfo.io/"

companies. In this chapter, the differences between security strategies will be indicated. After that, a cost indication of GoDaddy is given using the ROSI method. In the last paragraph, a conclusion of the report is given.

Differences in security performance

We decided to assess the difference between three different hosters. The difference we can see from our metric is that some hosts IP addresses appear to be up to 15 times as less likely to be compromised. This large difference provides an indication that some webhosts may be doing something different in terms of security than others, causing their sites to be less compromised. In table 1 the metric for three hosters are displayed, two of these besides the problem owner we discussed as other actors below. We chose a webhost that has relatively high compromised to ip ratio, one hoster that has a relatively low ratio and one that lies in between these two. The hosting company GoDaddy we picked as our as our problem owner, because it lies in between the extremes.

AS	Name	# Reported sites	# Assigned IPv4s	Ratio
AS20013	CYRUSONE - CyrusOne LLC	2627	221102	0.011881
AS26496	GoDaddy.com, LLC	10604	1852194	0.005725
AS16276	OVH, FR	2109	2734384	0.000771

Table. 1

Risk strategy of the problem owner GoDaddy

GoDaddy offers services such as website hosting. For website owners, this can be economically viable. GoDaddy is a popular hosting company, with about 17 million customers worldwide. n 2017, Godaddy won for the sixth consecutive year at the 2017 Stevie® Awards, for Exceptional Customer Service. According to the data, there are 10604 compromised websites, meaning that about 6% of their hosted websites are being compromised. When a website owner enters into an agreement with a hosting company like GoDaddy, reliable hosting is guaranteed (99.99% uptime), as well as a certain level of cyber security.

GoDaddy offers a range of packages, that differs in the amount and strength of controls. This immediately creates awareness for the website owner, who has to choose between alternatives. The better the package, the higher the cyber security, according to the hosting company. However, with regards to the activities of the hosting company, a successful risk strategy is required to offer these services.

GoDaddy's risk strategy can be seen as follows. First, the risks are reduced by means of controls. These controls depend on the package as chosen by the website owner. Second, some risks are simply accepted. The legal agreement that is entered with GoDaddy describes a level of uncertainty

when dealing with cyber threats. Also, some risks are avoided. For example, the premium package mitigates several risks. The first one is protection against attacks that redirect the website's visitors to a malicious website, by using DNSSEC-security. Also, eavesdropping is protected against. Lastly, a certain amount of risks is transferred.

Obviously, GoDaddy doesn't provide full transparency on its activities, for purposes of security. This means that it's difficult to properly analyze the processes surrounding the hosting company. Also, GoDaddy cannot provide its customers perfect security. Its risk management must therefore deal with the possibility of failures.

It could be concluded that GoDaddy is driven by customer service. Part of the security strategy is creating awareness by website owners. The vulnerabilities and threats are explained easily and precautions are offered, some in the basic package and some as possible additions. Because of the clear explanation, it probably will make the customer feel safer and more protected. At the same time, this doesn't mean that GoDaddy is fully protected and doesn't have its own vulnerabilities. The information provided on their website is not fully complete, as they only introduce security issues that could be mitigated by one of their packages.

What other risk strategies can the problem owner follow

The risk strategy for the problem owner should result in bringing down the number of compromised websites it hosts. These strategies can be categorized in four categories, mitigation, transfering, avoiding and accepting.

Mitigating strategy

This strategy aims to reduce the amount of compromised websites to an acceptable level. This could be done by by continuously updating the system. This ensures the latest version of software is implemented. A second strategy would be to create timely backups of the hosted websites, and as soon as a website is noticed as being compromised, put the backup up. A third mitigation strategy would be to instead of putting back the the complete backup, only remove the malicious files, that cause the website to be compromised. For both the second and third strategy the systems would have to be continuously monitored to detect the compromise in time.

Transferring strategy

Creating more awareness with the user about the security of their website, this can be done in the form of newsletters to the website owner, such that the user is more aware of current security vulnerabilities and is pushed to take action. Another transfering strategy in case the hosting company itself is not capable of handling the security of the websites its users host, a possible option would be to outsource this job en let a company specialized in this work handle it.

Avoiding strategy

Hosting can be done in globally two ways, vps hosting in which the website owner has full control and shared hosting in which almost everything is managed by the hoster, if the hoster would stop offering vps hosting it is completely responsible for the security of the website and avoids the customers misconfiguration or not updating their hosted website.

Accepting strategy

Accepting as a strategy is an option if the cost of the solution is higher than the damage. This strategy would not be likely to reduce the amount of compromised websites, only if the attacker would stop compromising websites, the amount of compromised websites would eventually go down.

Other involved actors that can influence the security issue

First of all, there is ***the attacker.*** This actor tries to attack users through hosting companies. The impact of the attack will depend on the strength of the attack. There are different types of attackers such as professionals and script kiddies having different motivations and expertise. For example, the professional attacker arguably makes use of sophisticated methods in order to accomplish a certain goal, while the script kiddie is concerned with spreading havoc for fun. The attackers goal, motivation, resources, skills and so on have direct effect the extent of the security issues of the hosting companies, although it is difficult to determine its exact relationship.

Secondly, ***the website owners***. Within this report, they are considered the victims. The so-called victims suffer damage caused by malware, data loss and more. This actor has few or no instruments available to protect itself due to the great dependency on its hosting company. Although a website owner is responsible for hiring a hosting company and looking at its associated security measures. On that basis, the website owner may identify remaining weaknesses in its cyber security. In the end, the website owner has a reputation to lose and with it, many website users. To conclude, the website owner could influence the security issue by choosing a hosting company with high/ medium or low security standards.

Thirdly, the ***website users***. This actor can also be considered the victim in this report. The user seeks trustworthy websites to use, and keep on using. Therefore, this actor is primarily concerned with preventive measures. Once the damage is done, the user cannot reverse the process by any mean. In fact, it could be that the damage was done a long time ago, and the user remained unaware. It is also up to the user to stay informed and pay attention to potential cyber threats. The actor can be alert and avoid a security issue.

Risk strategies that other actors can adopt to tackle the security issue

The ***attacker*** takes on a pro-active attitude, and seeks to benefit from discovered IT-vulnerabilities. In this process, the attacker may very well adopt an approach of trial and error. When a successful pathway is found, this can even be used continuously, without the hosting company being aware. With regards to strategy of the attacker, the search for and discovery of vulnerabilities is therefore very dynamic.

The ***website owner*** adopts a budget driven strategy. This actor must make decisions based on trade-offs between financial resources and envisioned level of risks and cyber security. The risks are big, given that the website owner has a reputation to lose. It should be noted that the website owner often does not full control over his website and relies (partly) on the hoster.

The ***website user*** adopts a preventative strategy. More than any other actor, it's interest lies in avoiding involvement in incidents. Once the user is successfully attacked, it becomes impossible to

reverse the process and repair the damage, with regards to lost data for example.
Lastly, other ***hosting companies,*** besides the problem owner, cannot guarantee total cyber security. At the same time, its focus on current and future IT-risks highly influences the degree of cyber security of linked website owners. The hosting companies should therefore play an active role in monitoring and updating its services. Besides the main hosting company GoDaddy there are two other hosting companies evaluated.

First ***CyrusOne,*** which has a relatively high compromised to ip ratio according to the data. CyrusOne owns over 40 data centers worldwide and serves hundreds of customers, more than 185 out of the Fortune 1000 customers worldwide which makes it third-largest data center provider in the US. The hosting company aims to have the highest standards in data center security and comply with standards set by certified organizations and trade groups, which are: **ISO/IEC 27001**, SSAE 16 (SOC 1 Type II), Type 2 AT 101/**SOC 2 & 3**, **PCI DSS,** FISMA-High, HIPAA/HITECH, Business Continuity and Disaster Recovery (BCDR), and TRUSTe (CyrusOne Enterprise Data Centers, 2016). In order to maintain and continually improve certificates there is a compliance management team in place. Furthermore the company has security protocols to protect physical assets containing security guards 27x7, video surveillance and recording of exterior and interior facilities and more.

Second, the risk strategy ***OVH***, this company scores low on the metric of compromised websites. Its was founded in 1999 and has 27 data centers worldwide. OVH does not have any partners with respect to security, from which we conclude it does not outsource any of its security to an external business. OVH's datacenters are physically guarded through fences and security cameras which are monitored by a surveillance team on 24/7 on site. Employees identify themselves by RFID keycard which are checked at a secured two door lock. Certificates ISO/IEC 27001, PCI-DSS certifcates, SOC 1 TYPE II and SOC 2 TYPE II certificates.

To conclude actors do have different strategies because they have different instruments available and different interests. There is no indication of differences related to time based on data. Although security of ICT is becoming increasingly important in society due to the increasing connectivity of IT.

Return on security investment

Chosen strategy
From the possible strategies for the problem owner to solve the security issue, a single issue was chosen. This choice was made based on the requirements that actually tries to solve the problem and thus has a certain cost and that the probabilities can be relatively easily estimated. The solution strategy we chose to calculate the return on investment on is to creation of timely backups, such that websites can be instantly restored after a compromise is detected.

The costs for this solution can be classified in two main components, the direct cost and the indirect cost. For the direct cost is are the expense for new storage servers that create and save the backups. These servers need to be located somewhere bringing cost for to buy and maintain the physical location. These are mostly single-time cost, the maintenance of the servers and keeping the backups up to date are the recurrent costs. We also have sunk cost in the form of employee training, to do the maintenance of the new servers.

Indirect cost occur when current employees suffer productivity loss, because they need to handle the extra responsibilities for the new solution.

Impact estimation

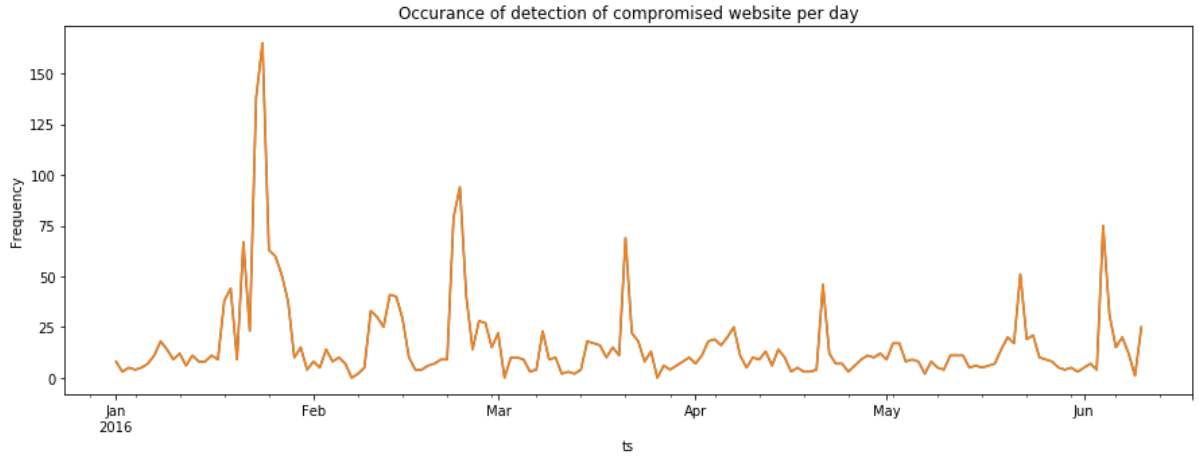
To estimate the impact and create a loss distribution we first got the frequency of a compromised website per day for GoDaddy. In order to quantify the loss a hosting provider occurs the impact cost per customer was calculated using a the cost of reputation function, this function estimates the impact costs that are incurred by the hosting provider based on the reputation loss that it endures.

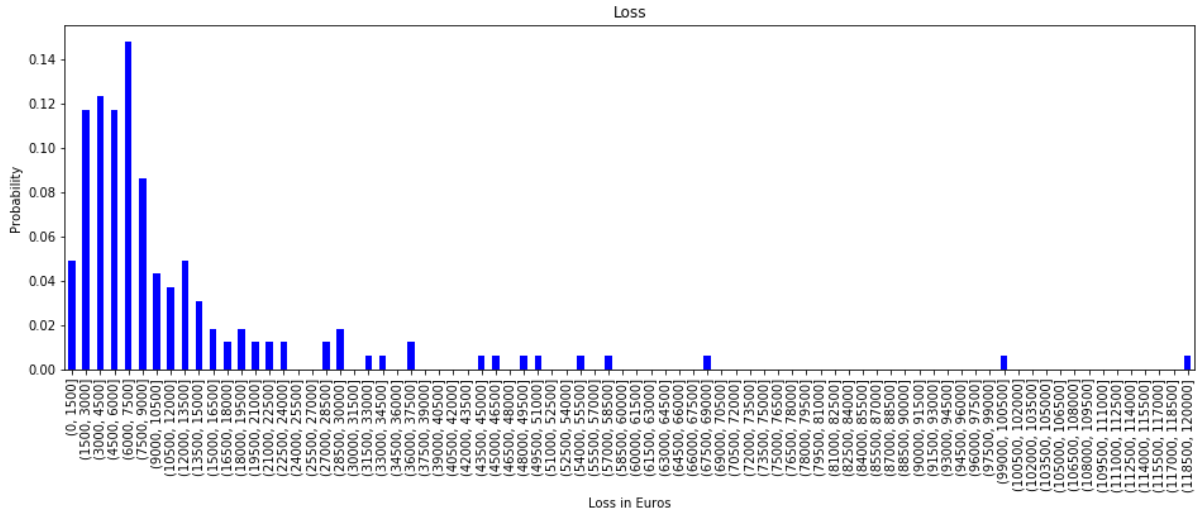
$$CoRL = affected\ customers * (CLV + CtR) + (influenced\ people / 50) * CLV$$

Here the affected customers are the customers experience the compromised website, CLV is the customer lifetime value, CtR is the customer replacement cost, and influenced people are the amount of people.

The customer lifetime value and customer replacement cost can be found in the annual financial report of GoDaddy. The number of influenced people is based on a study that showed that one customer communicates dissatisfaction about the company to eight to sixteen people. The influence these people have reaches to about 250 individuals in total, where 10% being within an organization's primary target audience. Of all those told, 2% (1 in 50) will then avoid an organization upon hearing of the victim's dissatisfaction.

CoRL per compromised website = 1 * (659 + 67) + 1/50 * 659 = $736 per compromised website





Solution Cost

In the following we will give an estimation of the cost of the solution, first the direct costs can be calculated. Physical Storage Space for extra servers: an average website is estimated at 1GB of which 80% is used, in 2014 8.5 million websites, 17 million customers and 37.000 servers, Growth from 2012-2014 = 70%. Growth from 2014-2016 (data used is from 2016) will be estimated on another 50% = 12.75 million websites, 12.75 million websites = 0.8 *12.750.000 websites = 10.200.000 gigabyte = 9.7 Petabyte per day of backup storage capacity needed: For 7 days = 9,7 petabyte * 7 = 67,9 petabyte

Rough estimate of cost of 5 petabyte storage (including drives, power supply, basic interface and assuming the other infrastructure is already present) = $244.000. For 67,9 petabyte total cost is = 244.000/5 * 67,9 =3.313.520.

$$ROSI = \frac{EBIS - Solution\ Cost}{Solution\ Cost} = \frac{ALE_0 - ALE_S - Solution\ Cost}{Solution\ Cost}$$

ALE_0 = Impact * Probability of Occurrence = Impact Cost * Total #Websites * Probability of Occurrence = 736 * 12.750.000* 0.002 = 18.768.000

The solution will not influence the probability of occurrence because it has no preventive measures. However the solution will significantly lower the impact cost because websites can be rolled back as soon as its compromisation is detected. We assume that reputation loss however still occurs but only takes up 10% of the initial reputation loss costs incurred without the solution implemented: ALE_S = Impact * Probability of Occurrence with Security Solution = Impact Cost * Websites * Probability of Occurrence With Security Solution = (736 * 12.750.000*0.10)* 0.002 = 1.876.800

In this way the Expected benefits can be caclulated with the following formula : EBIS = ALE_0 - ALE_S = 18.768.000 - 1.876.800 = 16.891.000 USD

Finally when the EBIS is obtained the ROSI can be determined with the following formula:

$$ROSI = \frac{EBIS - Solution\ Cost}{Solution\ Cost}$$ = (16.891.000 - 3.313.520) / 3.313.520 = 400%

With a Return On Security Investment of 400% it is concluded that this solution would be highly beneficial for GoDaddy to implement.

Conclusion

The problem of this report is compromised websites and the impact this has on the loss of In this report the problem owner was defined as a webhosting provider, using our metric we chose one of the major players providing this service based on the that had an average ratio of compromised websites. We considered multiple other actors and discussed their risk strategies on the the problem, for the problem owner a couple of different solutions were proposed. From these proposed solutions a single solution was chosen to calculate a return on investment (ROSI) on.

From this ROSI calculation we concluded that the return on investment would be 400%. This can indicates that the solution is economically viable for GoDaddy to implement.

There are a quite a few factors that influence the eventual cost benefit of the proposed solution, some numbers had to be roughly estimated, which affects the eventual benefit calculation outcome. Keeping in mind this uncertainty the strategy does seem to be a reasonable solution, to reduce the loss due to loss of customers.

References

CyrusOne. (z.d.-b). Cyrus One Values - CyrusOne. Geraadpleegd op 8 oktober 2018, van https://cyrusone.com/about/about-us/cyrusone-values/

CyrusOne Enterprise Data Centers. (2016). Data center cetification and audits. Geraadpleegd op 8 oktober 2018, van https://cyrusone.com/wp-content/uploads/2018/01/CyrusOne_PS-004-2016_Compliance_FA3.14.16.pdf

Average hosting space usage: https://kinsta.com/blog/disk-space-wordpress-hosting/

Financial report GoDaddy: https://s21.q4cdn.com/444693267/files/doc_presentations/2017/05/GoDaddy-Overview_May-2017_Site.pdf

Ponemon Institute, & IBM. (July 2018). 2018 Cost of a Data Breach Study: Global Overview (Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC). Geraadpleegd van https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf

Data and source code of metrics: https://github.com/Yzoni/economics-cybsec/tree/master/block_3