March 2019

Empirical Analysis of a Cybersecurity Scoring System

Jaleel Ahmed
University of South Florida, ahmed.jaleel.aj7@gmail.com

Empirical Analysis of a Cybersecurity Scoring System

by

Jaleel Ahmed

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Computer Science
Department of Computer Science and Engineering
College of Engineering
University of South Florida

Major Professor: Xinming Ou, Ph.D.
Paul Rosen, Ph.D.
Jarred Ligatti, Ph.D.

Date of Approval:
March 8, 2019

Keywords: Metrics, Botnet, BitSight, Sinkhole

DEDICATION

To my family

ACKNOWLEDGMENTS

I would like to thank my advisor Xinming Ou for having patience with me and providing me with guidance. I was lucky to have him as an advisor. His insights at times helped me whenever I faced a road block. He has helped me to become more intrigued with research and I am venerated to have worked with him.

I want to thank the members of the Argus Lab for their invaluable guidance. Especially, Anwesh Tuladhar for providing me with apprehension regarding the subject. I would also like to thank Arshad Jamal for his insights regarding the subject.

TABLE OF CONTENTS

LIST OF FIGURES iii

ABSTRACT iv

CHAPTER 1: INTRODUCTION 1
- 1.1 Motivation 1
- 1.2 Contribution 1

CHAPTER 2: BACKGROUND 3
- 2.1 Metrics of Security 3
- 2.2 Economics of Security 5
- 2.3 Co-relation Between Metrics and Economics 8

CHAPTER 3: SECURITY SCORE 10
- 3.1 Limitations 10
- 3.2 Use Cases 11
- 3.3 Fair and Accurate Rating 12

CHAPTER 4: BITSIGHT 15
- 4.1 Rating 15
- 4.2 Network Mapping and Scaling 16
- 4.3 Botnet Infection 18
  - 4.3.1 Adversary Scenario 19

CHAPTER 5: SINKHOLING 21
- 5.1 Process 23
- 5.2 Information Gathered 23
- 5.3 Use Cases 25
- 5.4 Bitsight Sinkhole 25

CHAPTER 6: UNDERSTANDING DATA 27
- 6.1 BitSight Data 27
- 6.2 Data Collection 27
  - 6.2.1 Sinkhole IP from NAT Logs 28
  - 6.2.2 Identifying Infected Machines from DHCP Database 29
  - 6.2.3 Identifying User from RADIUS Database 29
  - 6.2.4 Data from Logs 30

CHAPTER 7: DATA ANALYSIS 34
7.1 VirusTotal 34
7.1.1 Knowledge Discovery 34

CHAPTER 8: CONCLUDING REMARKS 37
8.1 Future Work 39

REFERENCES 40

LIST OF FIGURES

Figure 2.1	Security level as described by Rainer	5
Figure 2.2	Security expenditure VS Security benefits	9
Figure 3.1	Uses of security score	13
Figure 4.1	BitSight security score	17
Figure 4.2	Capturing botnet infection scenarios	20
Figure 5.1	Sinkholing process	24
Figure 6.1	Unmasking the C&C IP	29
Figure 6.2	Figure out the internal IP from NAT logs	30
Figure 6.3	Identifying the infected machine from DHCP database	31
Figure 6.4	Identifying the user from RADIUS database	32
Figure 6.5	Complete workflow	33
Figure 7.1	Monthly tickets handled by analysts	35
Figure 7.2	Guests having an effect on the score	36

ABSTRACT

In the field of cybersecurity, the top-level management make use of metrics to decide if the organization is doing well to protect itself from cyber attacks or is in tatters leaving itself susceptible against the vast threats looming around. Not only that but metrics are even used to measure the performance of the security team. The aim of this thesis is to show how economics is closely related to cybersecurity and how metrics play an important role in policy making of an organization. Furthermore, I scrutinize one of the leading security score providers for the way they detect botnet infection. Botnet infection is a part of compromised system group in their score card categories that amounts to 55% of the total security score. So, it becomes essential for the security score providers to have the right method of grading a company since it will have an impact on how they use their resources to protect itself from outside threat and the insurance premium they pay to cover any successful cyber attacks. I have found out that the data on which the botnet infection vector is graded has false positives. I shed light on security analyst and security team on a whole in their role in making decisions according to the security score. It is even the duty of the security team to work ethically, that is, the aim should not be to improve the security score rather the aim should be to protect the organization from outside attacks and if it happens to increase the security rating then be it so.

CHAPTER 1: INTRODUCTION

With the rapid growth in the field of cybersecurity, it has become essential to measure the cybersecurity through some metrics which not only gives an organizations security posture in regards to the industry standards followed but also provides information regarding the operational efficiency of the organization.

1.1 Motivation

The motivation to pursue this topic for my thesis had come during the group discussions carried out. It was during these discussions and the ongoing work at security operation center at the University of South Florida which made me wonder about the standard operational procedures and the importance of cybersecurity score for an organization.

1.2 Contribution

My contribution with the help of this thesis it to study the cybersecurity metrics and its relation with the economics factor associated with the security field. I further study the cybersecurity score published by BitSight and scrutinize the way the security score published by them is calculated. I narrow down to the way the botnet infection vector is ranked, which is a part of the compromised system part of the security score which makes up the fifty five percent of the total security score. Chapter two comprehensively describes the cybersecurity metrics in use and how there has been a shift in paradigm in the measurement of the security of the firm. It further co-relates the importance of metrics with the economic factor associated with the security of the firm. Chapter three shed light on what a security score is and what is it contained of. It further explores the limitations of the security score, its use

cases and the need to have fair security score reporting. Chapter four elucidates BitSight, which is a security score provider with focus on how it ranks it botnet activity vector while calculating the security score. Chapter five discusses the sinkholing infrastructure widely used by the research community in the fight against the botnet. Chapter six unravels the data collected for crosschecking purpose in the chapter seven. Chapter seven lays out information regarding the virus total results and the set up used. Finally, Chapter eight concludes the thesis while highlighting the future areas of work.

CHAPTER 2: BACKGROUND

The motive of this section is to get familiar with how metrics effect the functioning of the cybersecurity team in an organization and the importance of metrics to measure the performance of the team.

2.1 Metrics of Security

Metrics as defined by National Institute of Science and Technology (NIST) are tools that are designed to facilitate decision-making and improve performance and accountability through collection, analysis and reporting of relevant performance related data [1].

A Security Operation Center (SOC) is a team generally in an organization who is responsible for defending the organization's network from various threats and attacks. This team comprises of top level managers and security analysts. To evaluate the performance of the team and have a measure of the security of their network, top level managers prefer to have a numeric value representation as compared to an abstract representation of the organizations defense against outside threat vectors. An abstract representation will include time being spent on patching something up or defending and closing security related event tickets. Whereas, the numerical value would present the managers with answers to questions like, if the network was more secure yesterday compared to today? Most top level managers are not very technical compared to the security analysts and it becomes difficult on the part of the security analysts to convey information to them. So, a numeric representation bridges this gap.

Traditionally, Metrics in cybersecurity were based on the Risk Analysis. CIO used to measure the security level of the company by making sure if they were compliant with

international standards and the industry frameworks in use. With the evolving time and age, many complex algorithms and models have been developed. All of them keeping the Risk Analysis as the base for their work. Now the paradigm had shifted to much more of daily functioning metrics. The metrics the industry started to care was based on quantitative value, like time to detect the malware in the network and the time it took to eradicate it. This showed the responsiveness and alertness of the analysts working for the organization. Rainer Bohme studied the metrics of security as levels of security [2]. He developed a security metrics framework which quantified the security cost and as well as the benefits obtained by the security cost applied. The benefits were measured in terms of levels of security applied. He suggested in his paper [2] that for the cost of the security and the benefits obtained for it can be measured using four types of security metrics,

- Controls: Controls could be material like having proper alarms, institutional in the sense of not having under staffed team, procedural controls make sure that proper steps are taken by the security incident response team if an attack takes place, and technical controls would include the firewall and encryption mechanisms in place [3]. These controls are compared with the industry standard frameworks and checked for their implementation by the organization

- Vulnerabilities: It checks if the controls in place actually worked or not and its the measure of the controls fared with respect to the attack on the network. They are the gaping holes in the security which the attacker can exploit. An organization should think of a speculative attack or an actual attack which had happened in some other organization while checking for vulnerabilities within their own network

- Incidents: If the present vulnerability is abused then an incident takes place. This happens if the controls placed is breached, this will create an event in the organization at risk. Detecting incidents is a cumbersome task due to the high magnitude of events taking

place in the system combined with the false positive rate in the controls placed. In the end, incidents give a good picture of the controls in place by the organization

- Losses: This depicts the losses which could have happened by the incident due to the exploitation of the vulnerability. This is the risk analysis part tied to the metrics. This metrics looks at the possible loss an organization could face if its security is successfully breached

Most of the traditional metrics used fall into one of these metrics described in the framework.

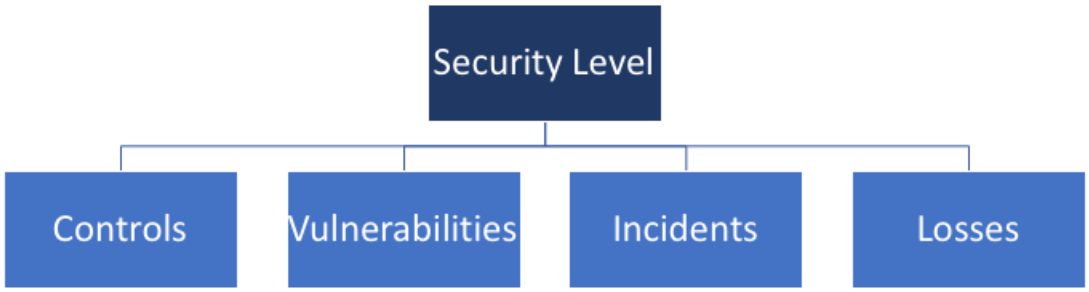

Figure 2.1: Security level as described by Rainer

2.2 Economics of Security

Cybersecurity off late has become one of the most talked about topics in the field of research. It is necessary to look at security from an economics perspective. A company should realize what they are protecting and against who are they protecting ? Once this is done a risk statement needs to be formed for the security analysts to have a clear vision. It

does not make any sense for a company to spend a lot on it's security which includes paying analysts, buying high end firewalls and anti-viruses if the value of what they are protecting is less than what they are spending on securing them. This is the cost of security which includes buying security tools, hiring staff to abstract costs such as the training time of the staff , time to recover from a breach, having a strong password and time to patch a software. Abstract costs more or less remains the same for most of the organizations whereas the other observable costs vary a lot depending on the size of the organization and the incentive they have to protect the organization from a breach. Apart from the observable and abstract costs we have certain hard and periodic costs. Hard cost will include the cost of implementing a policy whereas the periodic cost will have the maintenance of the hardware and software updates.

Expenditure on a company's security is not a binary decision. One has to formulate the risk associated with asset being protected. This too has another problem of its own, that is, what may be risk to one person might not be to another. While formulating the risk statement, an important factor pops up which is the base of the economics study of the cybersecurity, "incentive". If given a proper thought on why a company is being attacked by hackers, it is because of the incentive the company has to offer. No one would want to attack a company which has nothing to offer and then waste not only their resources but also valuable time. For this very reason a company should know the importance of the information or asset they are protecting. Carl Landwehr in an NRC report of his mentioned that regardless of the fact of how much money the Pentagon spent they were not able to convince the standard organizations like the Microsoft and IBM to create and ship more secure software and products. The main cause for this was due to the network effect and the market monopoly due to the lock-in of users [4]. Network effect in simple terms can be explained as, "The more the merrier". It states that every user adds to the value of the network. This theory is not just locked down to the network like telephone network, but it

expands into a much broader horizon of the internet, emails, applications and much more. Once the value of the company increases due to the number of users it has, it gets difficult for the users to shift from one technology to another. It not only takes time but also an extra effort and training for the users. So the probability of users letting go of the service gets down even if the service is not up to the standard. This gives birth to another challenge, since the market gets occupied by a monopoly, the hackers tend to write malware for the very specific product even if it is harder to break the security of the product because once the security is bypassed the incentive is higher here compared to attacking a company which has far less to offer, hence, here more number of machines get effected by the malware and become a part of the botnet network.

To counter such effect the market needs to be healthy and needs to have a competition rather than a monopoly [4]. Right now Microsoft is being challenged by Apple, giving the users an option to shift to another service provider. Hence, giving Microsoft an incentive to create and ship products with better security features for them to retain the user share. There is a divided opinion in security researchers as to how to view the cybersecurity problem. One group believes that the problem should be viewed as a technical problem and solved using technical measures while the other group looks at it as a problem of economics.

Getting an answer to the " why should a company spend on its security ?", by formulating a right risk statement, the other important decision a company has to make is how much to spend on their security and what part of their security needs spending? These two are very important and critical questions which does not have a definitive answer. For this to be answered precisely there needs to be certain quantitative metrics rather than qualitative beliefs for the chief security officer to decide that a component needs spending in order to be properly secured and what proof does the CIO have that even after spending money his company is more secure?

2.3 Co-relation Between Metrics and Economics

An organization has a specified limited budget for its IT operations and a part of that budget is allocated for the security of the organization. Since, the funds are scarce there is an important need to figure out where to use them so that it actually impacts the security of the organization. To solve this problem the upper management who hold the strings to the purse rely on the right security metrics. The security metrics guide them in allocating right funds to specific area and give grounds for the expenditure they are making. Rainer Bohme in his research introduced a graph which links the amount of money spent on security and the benefits reaped from it [2]. He showed that after a certain amount of expenditure there is not much improvement to the security. He calls the point point at which we see the improvements to level out as risk mitigation. This is the point at which the company has to spend bare minimum to not be at a risk from a vulnerability, beyond the risk mitigation point it is up to the organization if they want to spend more to accept marginal improvements or not.

With cybersecurity score there comes and additional economic incentive of cyber insurance. The insurance providers look at the cybersecurity score of an organization to underwrite the cybersecurity insurance premium a company has to pay [5]. This provides the organizations with an additional incentive and an important one too, since this directly involves monetary expenditure of the firm to insure it for any successful attack. This cybersecurity score even points at the area which should be improved, so that the upper management can decide the budget funding necessary for it. In case of third party vendors cybersecurity score even plays an important role in deciding if they are successful or not.

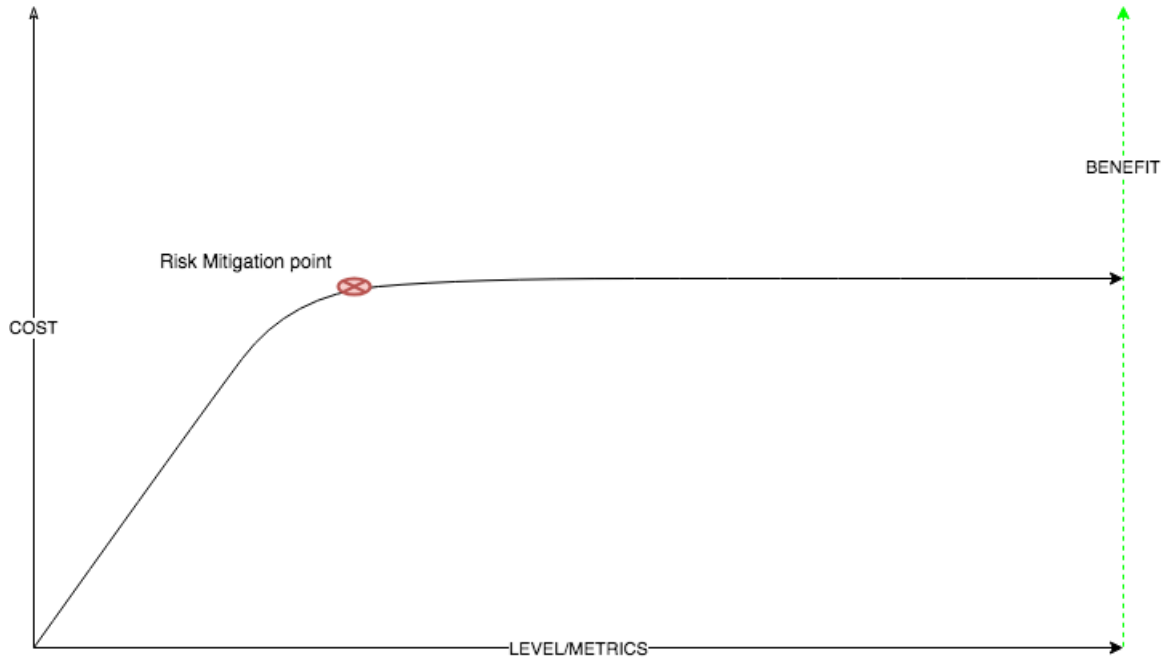

Figure 2.2: Security expenditure VS Security benefits

CHAPTER 3: SECURITY SCORE

A security score is a quantitative metric of the security of an organization. Compared to the qualitative measure this quantitative metric can help answer very important questions raised in Chapter 2. Usually, higher the score the better a company's security but it may vary based on the organization which is providing the metric. You can think of this security score as a FICO score, FICO score gives an idea about an individuals financial condition whereas the security score will rate an organization's security posture. Security score providers only analyze a company's security posture using externally accessible data that they do not need permission to acquire [6]. A security score usually consists of the three important things [6]:

- External Data: This will include open ports, spam propagation, patching frequency, file sharing practices and other externally observable events
- Public Intel: This category will look on for leaked credentials on the internet, Dark web and hacker groups
- Proprietary Algorithm: This part combines the above two to finally output a security score based on the algorithm the security score provider is using.

3.1 Limitations

Security score is a new idea for a lot of analysts. Moreover the way a security score is calculated changes from time to time which hugely impacts the score. To overcome this uncertainty one must understand what a security score stands for. The basic thing a security analyst should understand is that it is not necessary that if the organization has a better score then the chances of them getting attacked is less compared to them having a high score.

This is due to "incentives" that a company has to offer. If a company has a high score still a breach can occur although the chances might be less for a breach to be successful whereas if a company has a low score and has nothing to offer as an incentive for the attacker then what is the point of breaching the company? The other thing a company should know is, the security score is provided by observing the company's network from the outside and it is still their duty to train the workers about maintaining good security practices within the organization. Lastly, the security score does not address the budget a company spends on its security. Therefore, it does not necessarily mean that if an organization spends a lot of money on its security then it will be graded with a good security score.

3.2 Use Cases

- Cyber Insurance: It is well known that the insurance companies look at the cybersecurity score of a company before determining the insurance amount a company has to pay. There is a monetary incentive involved for the companies to maintain a good security score

- Third Party Risk: Companies look at the cybersecurity score of a company before getting in business with them or taking over a company. Earlier to vet this process organizations used to hire an external company and give them the task to find out about the vulnerabilities the third party faces. One of the famous incidents regarding this happened back in 2014 when Target was breached through the HVAC company they were doing business with [7]. The HVAC company had complete access to Target's network. The result of this was huge, credit card details of many customers were hacked following this were repercussion of the CEO stepping down and law suits

- Benchmark: Security score provider companies claim that they help organization by providing them with a benchmark to compare themselves with their peers and other

competition. Earlier this was done with the help of surveys but with the introduction of security score this has become easier

- Higher level reporting: Most of the upper management does not understand the technicality involving cybersecurity. It gets difficult for security analysts to convey the upper management about the security of the network. Security score can act as a bridge of understanding for both the analysts and the management. Management can monitor if the security posture of the company is improving or not

- Security expenditure: The management can decide on how much percent of the IT budget needs to be allocated towards the security based on the security score. They can even realize the area on which the spending needs to be done. The other benefit which comes along with this is that an organization can realize the benefit of spending money on security with the increase or decrease in the security score thereby giving them an idea if the spending was worth it or not

3.3 Fair and Accurate Rating

We need fair and accurate rating providers because the incentive here is very high. It not only involves monetary incentive in the case of cyber insurance but it also impacts the success an organization is going to have in the case of third party vendors. Right now there are few security rating providers, since this is a new concept for the industry. The US Chamber of Commerce along with the industry group which included major banks and organizations in June had adopted six principles which would guide the security rating provider to be fair and accurate in their rating [8][9]. They are as follows:

- Transparency: This principle states that the security score providers should at any time provide the company who they will be grading through their proprietary algorithm the data through which they are graded and the source they got the data from.

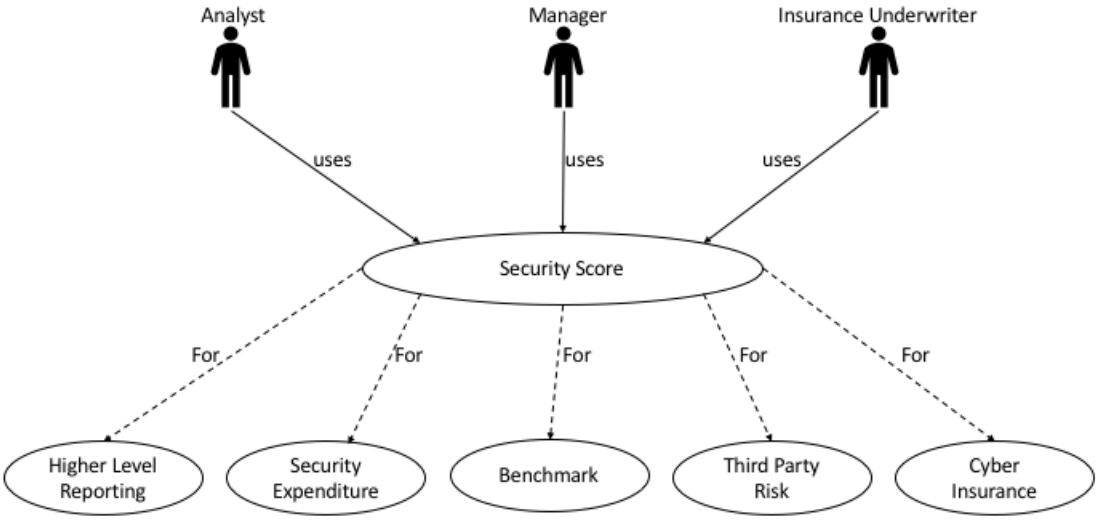

Figure 3.1: Uses of security score

- Dispute, Correction and Appeal: This principle allows the organization who has been rated by the security rating providers, the chance to question the rating they are provided along with the data through which they were rated as such. Every security rating provider should in essence have a process dedicated to this principle.

- Accuracy and validation: The rating provided should not be theoretical but rather observable and verifiable with the data in hand. The security score providers should provide accuracy of the models being used by them in generating the security score for an organization. This model should also be verifiable through the historical data points.

- Model Governance: If the security rating providers are going to change their model on how they calculate the rating then it is their duty to inform the companies about the influence that the change is going to have in the security score which will be provided after the changes are made permanent.

- Independence: This principle asserts that regardless of the fact that if a company is a customer of the security rating provider or not, they can still view the rating they are provided by the security rating provider and have the authority to challenge it like the actual customers of the security rating providers.

- Confidentiality: It is the duty of the security score providers to not disclose any data concerning an organization to a different organization which could ascend to a compromise of the organizations security. Along with this they should take special care to not publicly advertise security rating for an organization. If the organization has challenged the security score providers, during the time of the challenge the rating should not be disclosed to any one.

CHAPTER 4: BITSIGHT

BitSight is an organization which grades the security structure of an organization taking into consideration various fields as inputs. According to BitSight, a company with a higher grade is less likely to get compromised by an attack compared to the company who has been graded low [10]. All of their data inputs are collected from outside observation points. They manage to collect data breach information through public disclosure of the company effected or by filing a Freedom of Information Act (FOIA) requests [11]. Once this data is collected it is then mapped to an organizations known network. This can simply be done with the help of free tools like OPENVAS or the Nessus. The security score generated by them varies from two hundred and fifty to nine hundred. The higher the security score, the chance of data breach occurring is slimmer.

4.1 Rating

The rating generated by BitSight represents an organizations real-time security posture. The externally observable data is given as an input to BitSight's proprietary algorithm which churns out the score. This Algorithm examines the data for its severity, frequency, duration and confidence [12]. We can further break down the externally collected data into three parts [13],

- Compromised Systems: This data gives an idea about the infected devices running with in a network. This part constitutes fifty five percent of the whole security score. Compromised systems can be further divided into five risk vectors:

- Botnet Infection: This vector shows how many devices with in a network is infected with botnet. Bitsight even provides information on the type of botnet.
- Spam: This vector portrays the devices indulging in spam activities and propagation. This can have an adverse effect on the image of an organization.
- Malware Server: If servers are seen indulging in activities like hosting of illegal websites.
- Unsolicited Communication: This happens when a machine is trying to set up a connection with another machine with regards to a process which that machine does not allow. This portrays that the connecting machine is infected and is looking to infect the communicating machine.
- Potentially Exploited: These types of devices are due to newer type of attacks where attackers use the browser to inject ad-ware and meddle with user's interaction over the internet.

- Diligence: This accounts for thirty five percent of the total security score. This provide an overview of how a company maintains its servers. If they run updated software or not. The most important vector which diligence include is the open ports, this makes up thirteen percent out of the thirty five percent of the diligence.

- User Behavior: This adds the remaining ten percent of the security score. This will include how a user is using its network. The only risk vector in this category as of now is file sharing. It constitutes the whole of user behavior. This risk vector monitors the illegal torrent activities over the network.

4.2 Network Mapping and Scaling

One of the important parts of grading an organization's network is to correctly identify the network which belongs to the organization. This should include all its subsidiaries it

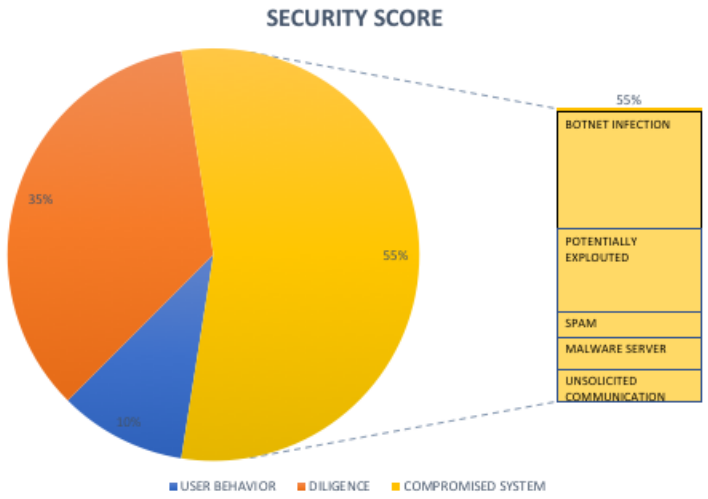

Figure 4.1: BitSight security score

owns completely. Although this may sound a simple task but it is a complex process which involves human interaction for verification. BitSight makes use of automated tools along with human interaction to form a network map of a company's internet footprint. This network map helps in figuring out starting point of the infected devices in a sea full of organizations. To rightly formulate the whole procedure, Bitsight follows these three steps [14],

- Information Gathering: This step involves acquiring important data regarding an organization. This will include the industry it belongs to, its logo and other important characteristics which will assist in differentiating it with an organization having a same name. This information is collected from publicly available sources such as LinkedIn, Wikipedia, Company's own website [14].

- Domain Discovery: Global DNS activity is tracked to find out which domains are owned and maintained by organization.

- CIDR Blocks, ASN and pDNS: Classless Inter-Domain Routing number is assigned to the companies network through publicly available data. ASN stands for Autonomous System Number which is a unique number to a network. In addition to these two Bitsight monitors passive DNS to detect IP addresses belonging to a company [14].

To consider a subsidiary into the mapping process, an organization should completely own the subsidiary and not a part of it. On top of it the subsidiary should not work independently and have its own IP range. After Network Mapping is performed, to set two organizations in comparison to each other, the larger organizations should be scaled in accordance with the smaller organization. Only then to a point will the security score be comparable to one another. Bitsight goes about doing this by assigning weight factors to the risk vectors and then normalizing it based on the number of employees an organization harbours.

4.3 Botnet Infection

A bot is an infected device in a network. A botnet is a collection of infected devices which are controlled by an attacker through Command and Control server. A botnet is used to perform attacks like spam or a denial of service attack. A botnet infection suggests that a network has not only been infested by one or more devices through which data can be leaked but it also uses up network bandwidth which adds to the company's resources. Botnet Infection is a part of compromised systems which is fifty five percent of the security score provided by Bitsight. Bitsight research scientist's have found out that organizations who are not graded 'A', that is, graded 'B' or lower for botnet infections are more than twice as likely to experience a data breach [15] [11]. Bitsight grades botnet infection by the number of events taking place and the duration of each event till the infection was cleared of the network. This is then normalized based on the magnitude of the company. Botnet infection is weighted the most in compromised system category [16]. The longer the botnet infection event lasts the greater the impact it has on the security score of the organization compared to

the events which are shorter in duration. Botnet drains the resources of the company and can be used to perform large-scale attacks. Recently due to the boon of cryptocurrency, botnets are being used to mine bitcoin. BitSight makes use of its sister company called Anubis Networks to identify botnet infections. Bitsight makes use of data from their data providers through sinkholes and honeypots which makes a communication with the bot pretending to be their Command and Control server. Bitsight captures randomly generated domains to figure out botnets which make use of Domain Generation Algorithm (DGA).

4.3.1 Adversary Scenario

To identify a botnet infection within a network infrastructure we can take a look at an adversary scenario. The first step is for the attack to take place. For this the attacker can send a phishing email to the user of the network. If the user is not aware or properly trained then the chances are high that he will open the email and this will put things into motion, that is, downloading of malicious software on the system which is on the network. Once the machine is compromised, it becomes a part of the botnet. The next step for the compromised machine is to try and connect with other machines which are compromised or it will try and reach out to its command and control server for further actions. Once the compromised machine does this, it is possible for the researchers to detect the infected machine. Two possible scenarios of how this can be done is [17],

- Network Monitor: Having prior knowledge of the botnet network and then observing it for any communication. If a communication is taking place, then the IP involved can be traced back to the company it belongs to, this can be done through the network map created.

- Sinkhole: Sinkholes are used by a lot of researchers to detect new and known botnets. When the infected machine tries to communicate with its command and control server

this connection can be intercepted with the help of the sinkholes and the network packets can be captured for further inspection.

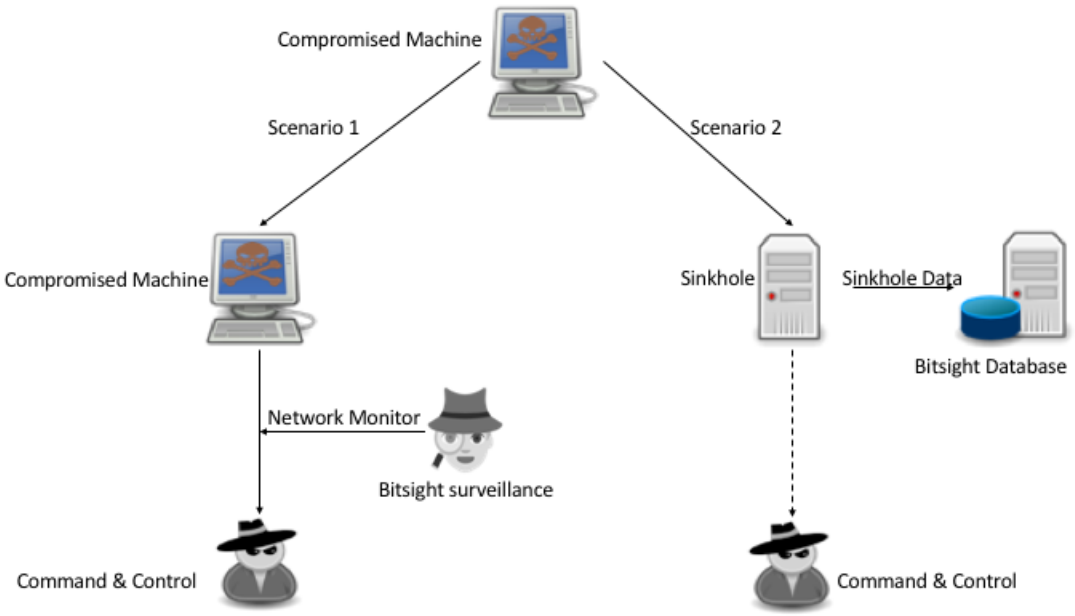

Figure 4.2: Capturing botnet infection scenarios

CHAPTER 5: SINKHOLING

As mentioned in previous chapters about the threat posed by the botnet in a network for a company, there have been many approached to tackle this problem. Most predominantly this botnet problem is studied with the help of a technique called sinkholing. Sinkholes are widely used by the security research community to study the malicious botnet activity going on over the internet. The connection between a machine which is taken over by botnet and its command and control server is intercepted. This communication is further studied to know the features of the malware present. This technique is known as sinkholing because when the infected machine requests for the malicious domains, the DNS server is set up in such a way that it responds with non-routable address to every such query. Usually a known list of malicious domains are set up in the sinkhole list, that is, a list for which the DNS forwarder will not actually resolve the actual website address. The DNS forwarder record which has command and control server address is replaced by a known IP address which acts as a sinkhole. These IP addresses are usually maintained by research industries and even law enforcement. The challenge in replacing the known malicious IP address with a sinkhole IP address is the cooperation with the Internet Service Providers (ISP) which can immediately re-mediate abusive domains [18]. This cooperation is usually not extremely quick, and has an another factor attached to it, which is the relationship an analyst have with the parties involved. This is a cumbersome process also because of the fact that sinkholing mechanism does not provide the internet service providers with any incentive.

When a user tries to visit a website through a domain name, the query is first sent to the domain name resolver to locate the address. If the resolver successfully resolve the address it returns the user with the website it requested for, if not, it forwards the query to

another resolver above in the DNS resolver chain to find the requested domain name by the user. Therefore, the DNS resolver which is placed at higher level get more traffic in contrast to the one at the lower level. Therefore, it makes sense to have a sinkhole placed in higher levels to be more efficient and capture more traffic [19]. Doing this may sound easy but in reality it is more complex than what it looks to the eye. To get this working a researcher or the sinkhole operator will have to work with various law enforcement divisions, internet service providers and in doing so comply with laws and regulations of the different countries involved in the process. The internal sinkholing infrastructure on the other hand is easier to maintain although it will capture less information and traffic. Internal sinkholing refers to influencing of the compromised machine in the company operated network instead of the internet. The internal sinkholing infrastructure is easier to implement because the network is most likely completely controlled by the organization [20].

The research community tries to maintain their sinkhole IPs publicly but due to the recent boon in cybersecurity industry these IPs are kept secret for proprietary reasons. This brings about another challenge for different research groups since the sinkhole IP which is kept a secret impersonates the actual command and control server it gets difficult to differentiate between the actual command and control server and the sinkhole IP being hosted. Sinkholing mechanism is most efficient when the botnet does not make use of advanced techniques like the domain generation algorithm, in such cases an entire botnet is not captured but only a part of it is recorded [21]. Most commonly used techniques to sinkhole a malicious command and control server include [21]:

- Domain Name: The Internet Service Provider can redirect the domain name query to a sinkhole set up by the researcher.

- Internal IP redirect: The Internet Service Provider can redirect an IP address which is known to be malicious to the sinkhole set up by the researcher only if the sinkhole and malicious IP belong to the same IP range.

- IP redirect: All the internet traffic is redirected towards the sinkhole sinkhole IP set up.

5.1 Process

This subsection aims to go through the attack phase and the use of the sinkhole to mitigate the attack. The sinkhole design consists of (1) a Sinkhole server (2) Sinkhole list which is an updated list of malicious domains for collecting updated information and being influential [22]. The first step would be to infect a machine in a network, this is done by the attacker usually through a phishing email. Second step, once the user opens the email, malicious content is downloaded on to the system and it is compromised. Third step, now the infected machine tries to resolve the malicious domain to try and get in touch with the command and control server. Fourth step, once such a connection is initiated, the sinkhole checks if the address trying to be reached is present in the updated sinkhole list or not, if yes, then the sinkhole set up captures this connection along with the data, else it will allow the connection to go through normally. Lastly, the DNS sinkhole will most likely respond the client trying to make a connection with the local host, hence, abandoning its attempted connection with its command and control server. A modern sinkhole mechanism will even notify the security team about the captured information.

5.2 Information Gathered

The data provided by the sinkholes is used to bring down huge botnets. In its most efficient form, the sinkhole set up can receive all the incoming traffic, that is, all the compromised systems trying to connect to the command and control server. The information

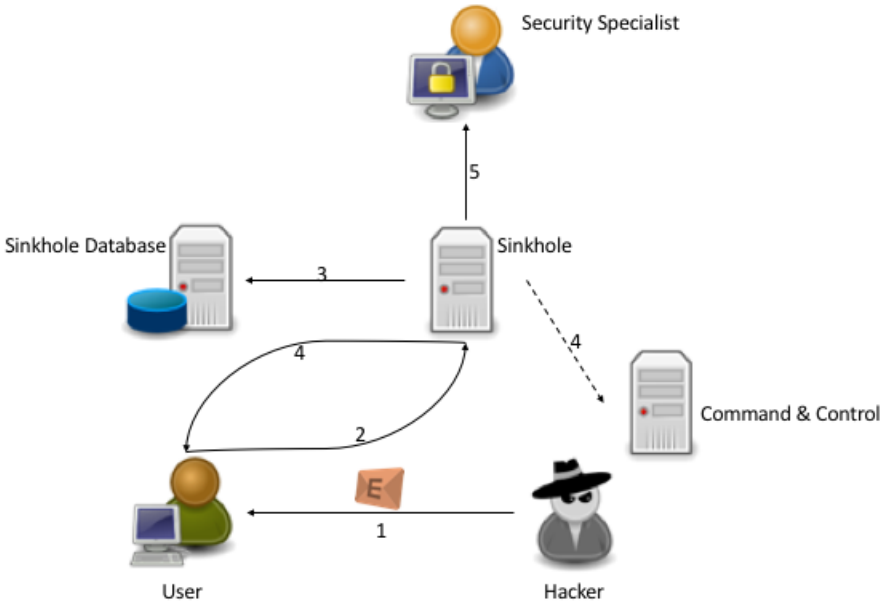

Figure 5.1: Sinkholing process

gathered by sinkholes may vary a lot but at the minimum it gives out five important characteristics about the compromised system [21],

- IP Address: The information gathered provides the sinkhole operators with the IP address of the compromised machine trying to contact the server
- Time: Second important factor provided by the sinkhole information gathered is the time when the compromised system was trying to get in touch with its command and control server
- URL: This gives the sinkhole operators with an idea about the domain name being used along with the path the communication route tried to connect with the address trying to make the communication
- Location: This gives the data about the country the IP address trying to communicate with the Command and control server belong to

- Compromised Machine Data: Usually the data about the infected machine is passed down to the command and control server. This data may include information like the machine name of the infected machine and the operating system running on the machine

This information can be used to track down the infected machine and further know the company network on which the infected machine is sitting on.

5.3 Use Cases

Apart from gathering valuable intelligence threat. These sinkhole infrastructures are mainly used for these two purposes [23]:

- Drive-by Download: Drive-by download refers to the activity of downloading of malicious data on to the user system through a link attached into a legitimate website or source. This type of activity can be prohibited with the use of sinkholes

- Command and Control Channel: The main purpose of setting up sinkhole infrastructure is to block the communication between the command and controller server and the compromised machine

5.4 Bitsight Sinkhole

To detect botnet activity,Bitsight heavily relies on Anubis Networks, a company which was recently acquired by Bitsight in its fight to capture data with wider depth and fields. Anubis Networks claims to has one of the biggest proprietary sinkhole infrastructures in the world, which provides information on botnet infection with zero false positive rate [24]. The claim to be one of the biggest sinkhole infrastructure in the industry is based on the volume of botnet infections it captures and the variety of it, that is, the different malware families it captures. Anubis network makes use of a proprietary real time intelligence mechanism called the cyberfeed. Cyberfeed makes use of several important factors including IP reputation,

sinkholing infrastructure, botnet traffic clustering, malware and website analysis and domain generation algorithm cracking to name a few [24].

CHAPTER 6: UNDERSTANDING DATA

The data being discussed in this chapter relates to the data provided by the bitsight about the botnet infection in an organization. The data provided by the bitsight does not have the complete IP address of the sinkhole which they own due to the proprietary agreement with their data providers. They hide the first octet of the IP address in the information provided. In the further subsections I will be elaborating the data provided by them and the data I collected by performing data analysis and data correlation of the data provided by them and the data logs of the university.

6.1 BitSight Data

BitSight provides forensic information for the security analysts at an organization to work on and improve the security of the organization. This data contains information on all of the security vectors effecting the security score of the organization. This forensic report contains fields like timestamp, risk vector type, IP address of the device which has been effecting the score, source port, destination port, type of infection for botnets, method of detection for botnets and partial command and control IP address of the sinkhole.

6.2 Data Collection

Security operation centers usually follow the standard operating procedures to deal with alerts. Their motive in the case of bitsight or in case of any security score provider is to maintain a good security score. This mainly helps in procuring a good deal with the cyber insurance companies, there by, providing them with an incentive. They look at each botnet infection reported by BitSight as an alert effecting their security score and

deal with it. A further incentive here for them is to detect the botnet infection and get it out of the network before it shows up on the Bitsight report. This is possible if the Sinkhole IP addresses are known to the organization, they can then keep a track of devices in the network trying to reach out for the sinkhole believing it to be their command and control, on detecting such devices, the devices can be quarantined from the network till it is patched up and then brought back on to the network. This is usually the general standard operating procedure followed for such botnet events. Data collection and following the standard operating procedure is a complex task. It involves many components depending on how an organization stores it network logs. For the university, I performed data collection using the BitSight Data Sheet, NAT logs, DHCP database and the RADIUS database.

6.2.1 Sinkhole IP from NAT Logs

The first step here is to identify the complete IP address of the sinkhole having the information provided by the bitsight. This is a complex task of performing correlation of bitsight data with the network logs of the organization. Every organization usually maintains the network logs of every device on the network which contains information on IP address of the device they are trying to communicate with. This type of a log is known as NAT Log where the internal IP address of the machine is natted before making a connection to the outside network. The bitsight data contains partial IP address of the sinkhole and along with it they provide the timestamp information when the compromised machine was trying to reach the command and control server. They even provide the IP address of the infected machine. These three can be used and be correlated with the organizations network log to find out the complete address of the sinkhole. The complexity of this will vary depending on the size of the organization. The bigger the network, that is, the number of users on the network, difficult it gets. Moreover, log analysis is difficult due to incomplete logs.

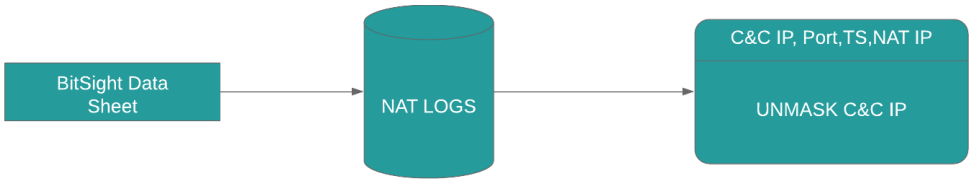

Figure 6.1: Unmasking the C&C IP

6.2.2 Identifying Infected Machines from DHCP Database

On having found out the complete address of the sinkhole being used by the security score provider we can then make use of this information and search the network logs for devices which are trying to reach the sinkhole. From the NAT logs we can get the internal IP address of the machine trying to reach out to the command and control server. We can make use of this information to query the DHCP database which will contain the MAC information of the device which was assigned the IP at that particular timestamp when the event took place.

6.2.3 Identifying User from RADIUS Database

Once the device MAC address is found then the next step would be to identify the user who owns that machine. This is done by querying the RADIUS database which stores information about the owner of the machine based on the MAC addresses. After identifying the user, the user can be notified of a possible compromise of the machine the user owns. Then the necessary steps to make sure that the device does not show up on the security score providers report and effect the security rating of the organization can be undertaken by either temporarily blocking the machine from making any possible outside connection from within the network till it has been patched. To make sure that the organizations are actually getting hold of the devices which are effecting their security rating, they can compare their botnet infection reports before and after following this sort of a standard operating procedure.

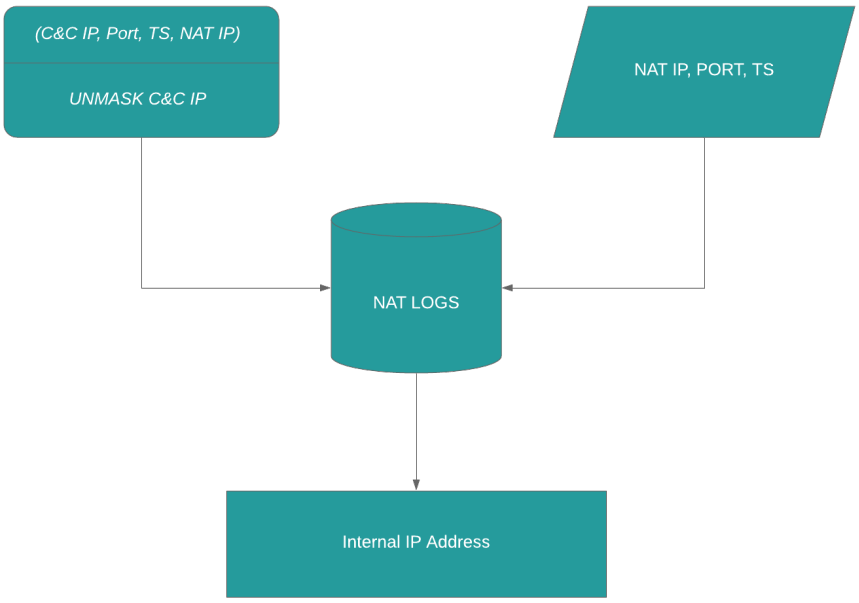

Figure 6.2: Figure out the internal IP from NAT logs

6.2.4 Data from Logs

I have collected data on every such event which took place in the university to further analyze the infected machines and scrutinize the data from the sinkholing infrastructure bitsight set up. I collected information about the supposed infected machines from the network logs. This information has details like the user running the device during the time of infection being detected, the source port used, destination port, destination IP address, size of data sent over during the connection and obviously the timestamp. I further add an extra field to this by looking up for the URLs at the time of the connection made to have more information about the domain names being used. This information is important to check the domain names for malware later on. This will give us an idea about the false positive rates. Further collecting this data is important because it gives us clues and can

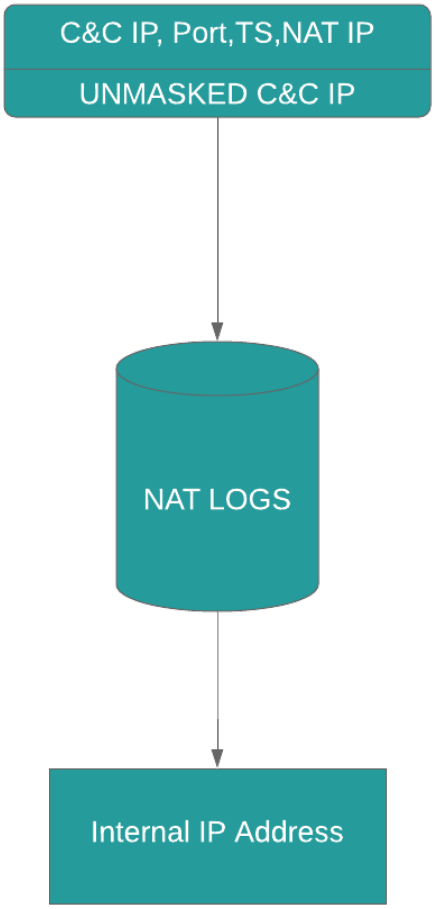

Figure 6.3: Identifying the infected machine from DHCP database

help us in finding patterns the botnets use while trying to connect to the command and control server.

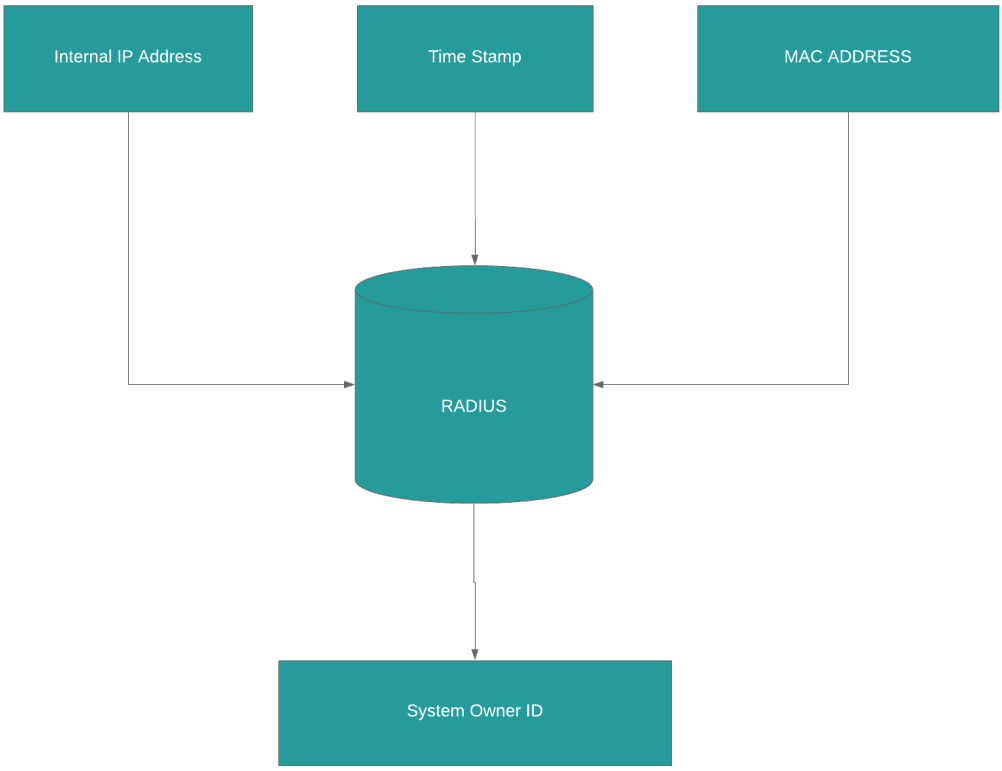

Figure 6.4: Identifying the user from RADIUS database

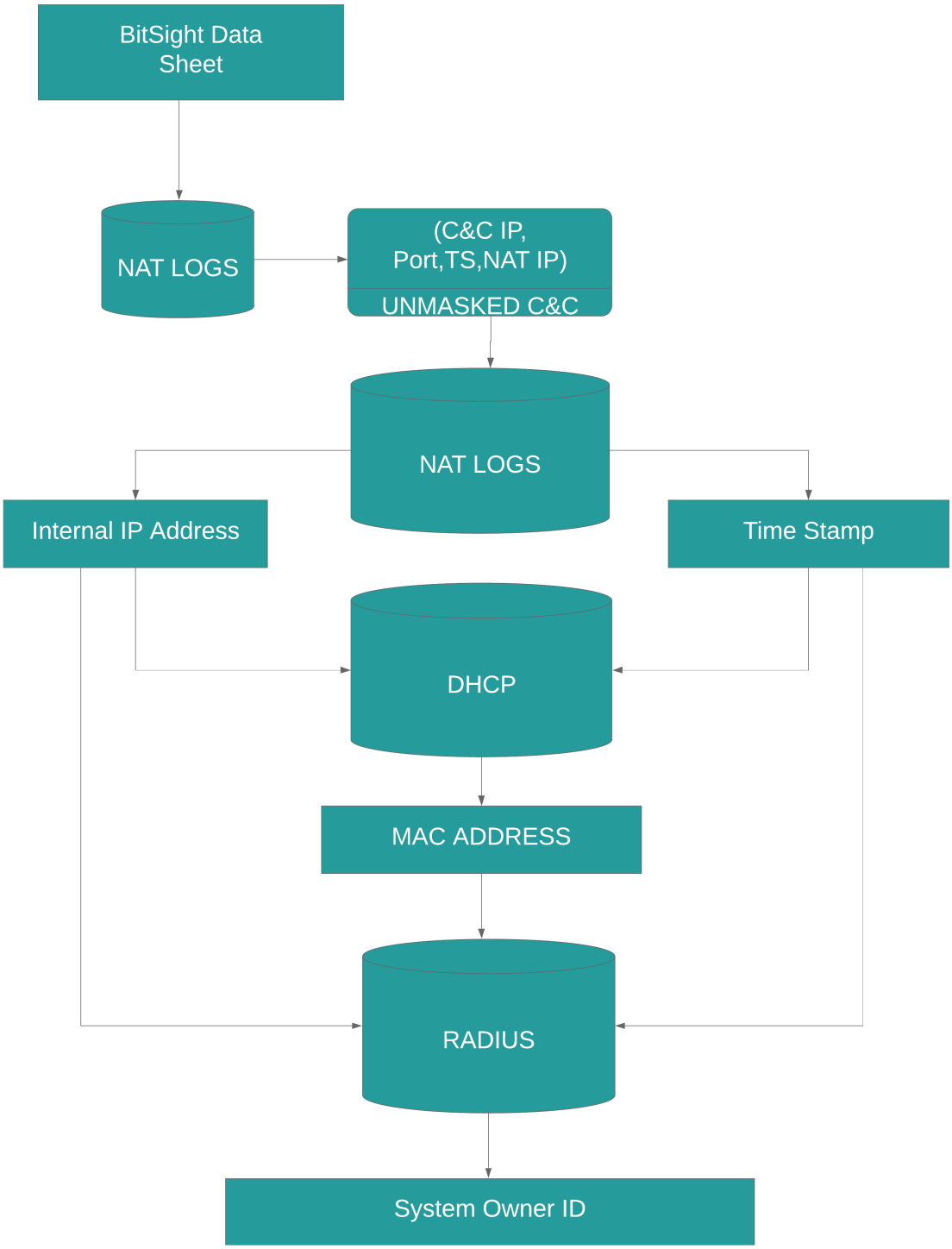

Figure 6.5: Complete workflow

CHAPTER 7: DATA ANALYSIS

Once the data collection part was done, the next step was to to check the gathered URLs for malware detection. For this purpose I made use of VirusTotal. I checked the URLs provided by the bitsight against the VirusTotal to check for any false positives. I further made reports on the data I collected to find insights on how even a small percent of false positives would cost the organization. Moreover, the issues a user would have to face on not being able to access the outside internet is also mentioned. The university along with monitoring the BitSight sinkhole IPs even monitor known sinkhole list available on the internet.

7.1 VirusTotal

VirusTotal scans each URL with approximately 68 antivirus products to check for any infection or compromise. It aggregates these products and scan engines to check for malware and viruses or to verify against false positive [25]. It bestows an API for users to automate scanning of multiple URLs. The free version of the API allows users to check for four events per minute.

7.1.1 Knowledge Discovery

On performing analysis on the data provided by the Bitsight, there were 10 different sinkhole IPs which the Bitsight used. The URLs for these IPs vary. On cross-checking the URLs for malware using VirusTotal, there were 3 false positives from a total of 15 URLs provided in the forensic data sheet which equals to 20%. The data I collected contains events for the BitSight sinkhole list and the list available on the internet. The list available on the internet has a much higher rate of false positives.

In total there were 504 events which took place in about 11 months period which averages up to 45 tickets per month the security analysts have to deal with because of this data. We should keep in mind that number of events does not mean that 504 machines were compromised since the same machine can get multiple events if the user fails to address the issue when the user was initially notified about it. So of the 504 events, there were 212 machines which were actually compromised. Highest number of events for a single machine during this period was 25. This shows how difficult it is to address the actual issue. There are two scenarios to it, First, even if a user is notified of the malware present considering it was not a false positive, the security analysts would have to depend on the user to get rid of the malware from their system and then send them a proof of an anti-virus scan of their machine. There might be a case that the anti-virus product which user is making use of is not able to identify the malware on the system and gives a result to the user which would suggest that their system is free from any malware. Second, another issue would be that if the event is actually a false positive and the anti-virus being used by user is actually giving them the right result of the machine being free of any malware.

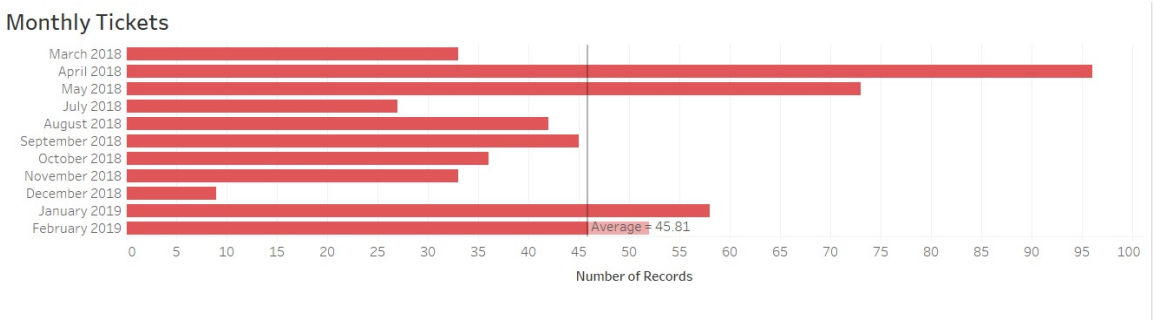

Figure 7.1: Monthly tickets handled by analysts

I was able to collect fully quantified domain name for 404 events. Of these 404 events few IPs were not hosting any URL at the time of performing reverse DNS. The events included students, employees and guests on the network. So a guest can be parents of some students

who would need access to the network. So the SOC would have to take a decision, which is if they are willing to make a compromise to the security for providing better usability. Guests can be blocked access on the network. Security team will always have to make a trade-off between usability and security.

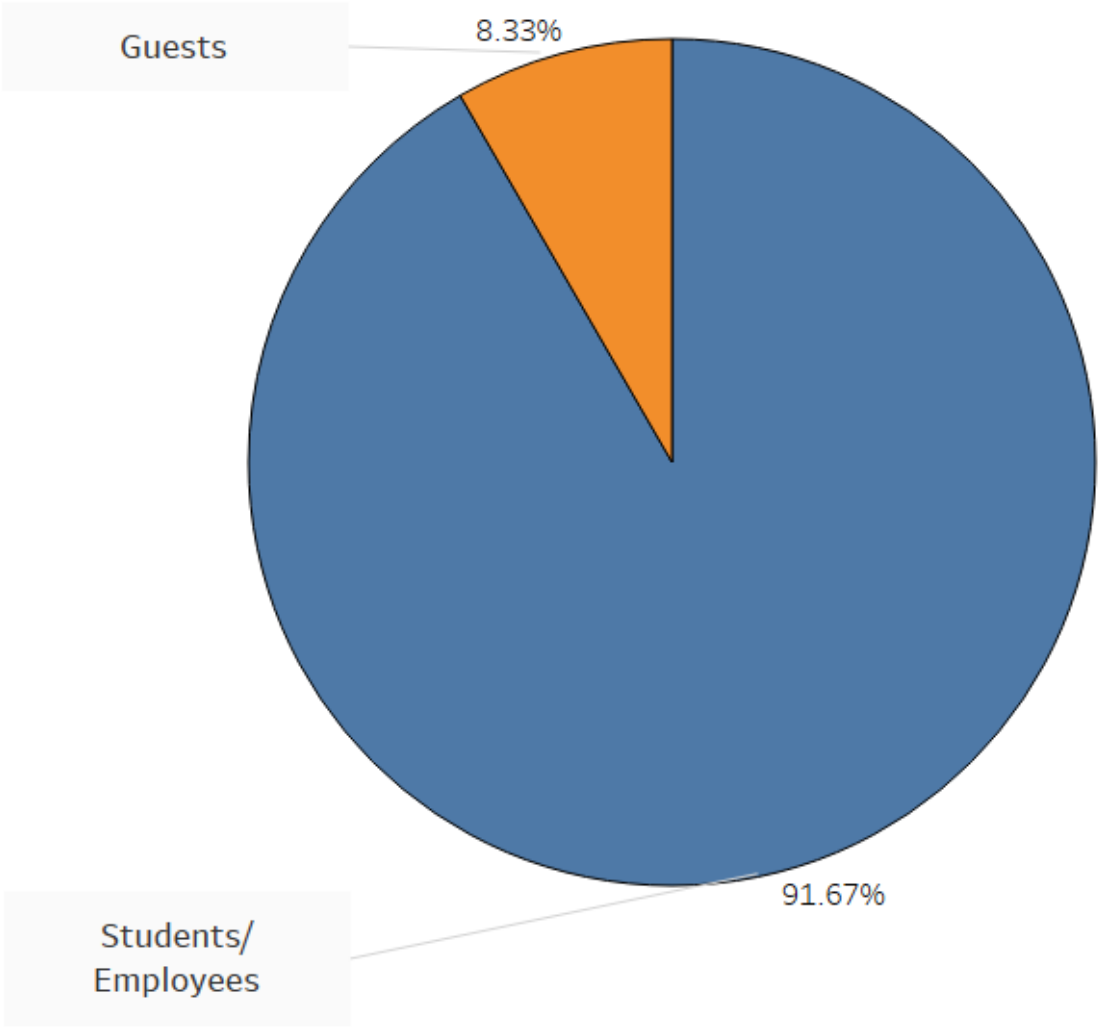

Figure 7.2: Guests having an effect on the score

CHAPTER 8: CONCLUDING REMARKS

With the help of this thesis my aim was to represent how economics is closely related to security compared to the common perception of the people. Secondly, the role cybersecurity score is playing in today's world need to be scrutinized. Security score providers proprietary algorithm should be open sourced for the industry to review and have confidence in regarding what the the security score providers are stating.

Moreover, when two company networks are compared by the security score providers it must be noted that two networks are never the same. Number of users making use of the network also plays an important factor. Each company faces different type of a risk based on what it has to loose. Depending on this a company has an incentive to protect their assets.

Detecting Botnet using sinkhole mechanism has many issues of its own as pointed out by Pierluigi Paganini [22]. He explained why the sinkhole data can contain false positives due to problems like DHCP Churn where the internet service providers assign IP addresses to systems temporarily and it is not feasible to find out or foresee the amount of time a particular IP was assigned to a given system. He even mentioned the problem of many internet devices which are on the internet for various different purposes and these devices may stumble upon sinkholes set up which will add to the data and hence result in a false positive generated.

I scrutinized the botnet infection. I collected the botnet event data provided by bitsight. Almost all of the botnet events triggered by Bitsight are from its malware sinkhole infrastructure. So, it is very important and critical that this infrastructure can be trusted with certainty. On cross checking the data provided by Bitsight against VirusTotal I found few false positives which does not look promising.

The security score even acts as a stimuli for how a security analyst takes steps to protect the system. For the security vector of open ports available on the network, there might be a number of reasons for an accessible open port available from outside the network. For a university one of the reason might be academic where a course instructor might want to set up the environment in such a way that it gets easy for the students to carry out their assignments or another reason might be due to research where there might be outside collaborators who would also want access to the research. The security team will have to make an important decision in these kind of scenarios, they will have to measure how much of an inconvenience will closing these ports be on the user activity compared to the security risk which is due to the available open port. The duty of the security analyst should be to defend the system from external threats and not just find loopholes to increase the security score. For instance it is possible for security engineer to set up the firewall in the network in such a way that it will drop all the connections being made to the outside command and control servers which they have analyzed through the data provided by the security providers to act upon. This does not solve the actual issue of the machine being compromised, it only stops it from making a contact to the command and control server. A machine should be set free of any malicious software it has on its system. Analysts could just be motivated on increasing the security score because that is the only metric they will be judged upon by the top level management. This brings the focus on another issue which is that it is not a good practice to evaluate the performance of security analysts using the security score. The security analyst will be motivated to increase the security score and not protect the network from malicious threats.

8.1 Future Work

I have just scratched the surface with my thesis work by only scrutinizing the botnet detection mechanism. The security score contains other elements which can be further studied and verified based on the claims made by the respective security score providers.

REFERENCES

[1] Yi Cheng, Julia Deng, Jason Li, Scott A. DeLoach, Anoop Singhal, and Xinming Ou. *Metrics of Security*, pages 263–295. Springer International Publishing, Cham, 2014.

[2] Rainer Böhme. Security metrics and security investment models. In Isao Echizen, Noboru Kunihiro, and Ryoichi Sasaki, editors, *Advances in Information and Computer Security*, pages 10–24, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[3] Economics Cybersecurity. Econsec101x - 2b - measuring security levels. https://www.youtube.com/watch?v=jwVNuWi4EwE&feature=youtu.be, Jan 2015.

[4] Economics Cybersecurity. Economics of cybersecurity: The economics of information of goods. https://www.youtube.com/watch?v=TIHUN1weIq0, Feb 2016.

[5] BitSight Technologies. Bitsight security ratings for cyber insurance, 2018. https://www.bitsighttech.com/security-ratings-cyber-insurance, Last accessed on 2018-09-13.

[6] Stacy Collett. Whats in a security score?, 2016. https://www.csoonline.com/article/3103293/security/what-s-in-a-security-score.html, Last accessed on 2018-09-13.

[7] Jaikumar Vijayan. Target attacks shows danger of remotely accessible hvac systems, Feb 2014. https://www.computerworld.com/article/2487452/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html, Last accessed on 2018-09-21.

[8] Russ Bannam. Cyber scorekeepers: A growing number of ratings firms aim to help companies and their insurers assess and manage cybersecurity risks. *Risk Management*, 64(10):26–30, 2017.

[9] Doug Clare. 6 principles for cyber risk scores - and why we need them, Jun 2017. http://www.fico.com/en/blogs/fraud-security/6-principles-for-cyber-risk-scores-and-why-we-need-them/, Last accessed on 2018-09-13.

[10] Bitsight Technologies. Bitsight security ratings, (n.d). https://cdn2.hubspot.net/hub/277648/file-2505376057.pdf, Last accessed on 2018-09-13.

[11] Bitsight Technologies. Beware the botnets: Botnets correlated to a higher likelihood of a significant breach, (n.d.). https://www.bitsighttech.com/hs-fs/hub/277648/file-2726147033-\%20pdf/Insights/BitSight_Insights_Beware_the_Botnets.pdf?t=1513633447234, Last accessed on 2018-09-21.

[12] Jacob Olcott. Input to the commission on enhancing national cybersecurity: The impact of security ratings on national cybersecurity, Sep 2016. https://www.nist.gov/sites/default/files/documents/2016/09/15/bitsight_rfi_response.pdf, Last accessed on 2018-09-20.

[13] BitSight Technologies. How bitsight calculates ratings. Technical report, (n.d.). https://www.bitsighttech.com/hubfs/Non_Public_Collateral/Q117_How_BitSight_Calculates_Ratings.pdf?hsLang=en-us&t=1526668766037.

[14] Ingrid. Network mapping process, (n.d.). https://help.bitsighttech.com/hc/en-us/articles/115014349327-Network-Mapping-Process, Last accessed on 2018-09-21.

[15] BitSight Technologies. Bitsight is the best total solution in security ratings, (n.d.). https://cdn2.hubspot.net/hubfs/277648/Datasheets/Best%20Total%20Solution%20-%20Three%20Pillars%20Data%20Sheet.pdf, Last accessed on 2018-09-21.

[16] Ingrid. How is the compromised systems risk category calculated?, (n.d.). https://help.bitsighttech.com/hc/en-us/articles/360005428073, Last accessed on 2018-09-21.

[17] Bitsight Technologies. Bitsight data, (n.d.). http://cybersel.eu/wp-content/uploads/Bitsight-Technical-Note-on-Data.pdf, Last accessed on 2018-09-21.

[18] Babak Rahbarinia, Roberto Perdisci, Manos Antonakakis, and David Dagon. Sinkminer: Mining botnet sinkholes for fun and profit. In *Presented as part of the 6th USENIX Workshop on Large-Scale Exploits and Emergent Threats*, Washington, D.C., 2013. USENIX.

[19] Wikipedia. Dns sinkhole, Dec 2017. https://en.wikipedia.org/wiki/DNS_sinkhole.

[20] John Bambenek. Principles of malware sinkholing, Jun 2015. https://www.darkreading.com/partner-perspectives/general-dynamics-fidelis/principles-of-malware-sinkholing/a/d-id/1319769, Last accessed on 2018-09-21.

[21] Rainer Link and David Sancho. Lessons learned while sinkholing botnets–not as easy as it looks! In *Proceedings of the 21st Virus Bulletin International Conference,(Barcelona)*, pages 106–110, 2001.

[22] Pierluigi Paganini. Sinkholes: Legal and technical issues in the fight against botnets, May 2014. https://resources.infosecinstitute.com/sinkholes-legal-technical-issues-fight-botnets/, Last accessed on 2018-09-21.

[23] Ryan Mazerik. Understanding dns sinkholes a weapon against malware, Jan 2018. https://resources.infosecinstitute.com/dns-sinkhole/, Last accessed on 2018-09-21.

[24] Nuno Periquito. Tracking botnet activity in real-time with cyberfeed, Apr 2015. https://www.linkedin.com/pulse/tracking-botnet-activity-real-time-cyberfeed-nuno-periquito, Last accessed on 2018-09-21.

[25] Wikipedia. Virustotal, Aug 2018. https://en.wikipedia.org/wiki/VirusTotal, Last accessed on 2018-09-21.