Final Deliverable 2 - Security Investment

Group 2 - TelnetScans

Ivan Lukman - S1967754

Metin A. Açıkalın - S1984853

Valentine Legoy - S2178192

Economics of Security

University of Twente

October 8, 2018

1 Introduction

Telnet, a protocol allowing the communication in-between terminals or processes, has been widely used since its creation in 1969. However its lack of encryption and its use over the Internet create a security concern [1].

During the first assignment of Economics of Cyber Security, we detailed, based on our dataset and the study of the existing literature, a security issue, security metrics already existing, ideal metrics for the related actors and metrics evaluated based on the received dataset. In order to fully understand this paper, please read this previous assignment [2].

In this assignment, we will explore the different actors and owner that can be related to the security issue, and explain the different risk strategies that each of them can apply. The security performances of the different owners of the problem will be expressed and compared based on the dataset. Finally, the Return on Security Investment (ROSI) will be defined, based on one of the explained strategy and our dataset.

1.a What has been changed according to the feedback of final report of block 2?

The peer reviews and feedback from the first assignment encouraged us to review our metrics. The metric which was mainly criticized was the "number of telnet sessions that are accessible, grouped by each type of industry", as we were not able to normalize it. As a reminder, the four other metrics evaluated during the previous assignment gave us the following information:

1. 77% of the telnet sessions requested log in.
2. 9% of the attempts of connection to telnet port were rejected.
3. 17% of the banners grabbed during the scan were giving information about the service.
4. 1% of the banners gave information about white-listed IP.

The metrics defined during the first assignment might not have been enough to answer the questions of the present assignment, thus we worked again on the definition and evaluation of metrics present in the dataset.

If all the IP from the dataset have been scanned on port 23 or 2323, which are usually used for the telnet protocol, some banners gave us information as to which another protocol the scanned port was assigned. 0.5% are used for FTP. 0.05% is used for SMTP. 5% is used for SSH.

If we did consider evaluating metrics regarding security measure, such as login forms and connection rejection, we did not consider until now the banner giving a warning message, which can be included as a preventive measure. In the overall scan, over 5% of the banners give out a warning message to the person trying to access the service.

For the purpose of the second question of this assignment and as a replacement of our previous grouping of telnet sessions by NAICS and SIC, we decided to group the session by domain name, based on our definition of the problem owner. The obtained grouping will allow us to normalize the difference between security performance at the second question of this assignment.

Several other metrics, which have been found not being relevant to this assignment, have also been evaluated. The previously mentioned metrics will be developed in the following paper.

2 Who is the problem owner of the security issue as measured in your first assignment?

In this report, "problem owner" is referred to any person, or instances, or organizations, that is responsible of preventing or handling the problems [3]. When dealing with telnetscan data, the problem owners can be said as the executives and the SysAdmins of the company's or individual devices that open the telnet port.

As it was mentioned in the first assignment, there are two security issues that are raised from the given dataset, which is about the telnet scan result.

- Firstly, this dataset gives an example of leakage of systems' critical information. In the given dataset, this is can be seen directly by inspecting the telnet banners. Some records reveal the system's information, such as the Operating System (OS) name and its version, using the telnet sessions' banners. Taking the security perspective, this leakage of information is very useful for the attackers to find available vulnerabilities, but on the other hand, this is not what the system owners want.

- Secondly, and the more important security problem, is the fact that many computers and networking devices allow remote access from anywhere via telnet. This problem is actually the reason why the dataset was created. There are still a lot number of devices that allow telnet communications from anywhere in the world.

The problem owner of both of the two issues are the executives related to the information security, such as Chief Information Security Officers (CISOs), in the case where the devices belong to a company. If the system that open a telnet port is owned individually, the owner of that device can be said to be the problem owner. SysAdmins, one of the actors that can be related in both cases, can also be blamed, because technically, they are the ones responsible for configuring the devices. If they can enable the telnet services, they should also be able to change the login banners.

These CISOs and SysAdmins should have implemented policies about what should be published into the telnet banners (for the first problem) and from where should the device be accessible (for the second problem). Opening telnet port, to be accessible from anywhere, could be a double-edged sword for the problem owners. On one hand, this may increase the convenience of the SysAdmins because they can configure the device from anywhere. On the other hand, attackers from all around the world can also access the system.

3 What relevant differences in security performance does your metric reveal?

The analysis of the whole dataset shows that some security measures were taken. One of those is the presence of a login form when the port is access, before being able to use the service. Logging in is required in 77% of the case presented in the dataset. However, the use of the telnet protocol to send a password to a server could make the service less secure, as the credentials will not be encrypted and might be sniffed. The dataset doesn't allow us to know if the credentials required are the default ones or not, which could be an additional security issue, as it had been exploited during the Mirai attacks [4].

The use of a warning message in the banner has been in 5% of the case. It is part of the recommendation to make a secure banner [5]. However, this preventive measure might not be discouraging the malicious individuals to attack the service.

Among these five millions of sessions created, only 9% of the IP scanned have rejected the telnet connection. In some cases, because of the number of telnet sessions connected were over the limit. In other cases, the IP address from which the scan was done was not whitelisted by the system. The use of SSH on 5% of the ports scanned is the strongest security measure observed, as it is often recommended instead of telnet [6].

The fact that 17% of the scanned ports gave information about the sys-

tem in their banner is proof of a low-security level. Banner grabbing is one of the issues related to open telnet services. Information gathered from the banners can be used to find vulnerabilities on the system which could be exploited in an attack.

Additionally, the fact that these services are accessible from the Internet is, in itself, proof of a low-security level. The Shadowserver, which is the author of this scan, affirmed on their website, that these addresses are not firewall-ed from the Internet [7]. Thus they did not have to do much effort to have access to the services, proving that any attackers could potentially benefit from the low-security performance.

All these different observations, that were made on the overall dataset, impact the security. The given data have been grouped by domain name, based on the hostname provided in the set, so it can be linked to the previously defined problem owner, but also, so the security performance can be compared [8].

As the dataset contains over 1830 different owners, it is difficult to compare in a graph the security performance for all of them. The following graphs represents the frequency of the different security measures mentioned before. Figure 1 shows how frequency of the proportions of Telnet ports used for SSH varies per domain name. Figure 2 shows the frequency of the rejected telnet requests per domain name. Figure 3 shows the frequency per domain name of the banners that warns the unauthorized accesses and Figure 4 shows the frequency of the Telnet communications that require username - password combination per domain name.

Based on the figure 1,2,3,4, it can be observed for each of the security measure, that an important part of the owners do not implement it. While, at the same time, it can be observed that a majority of the owners do not give any information about there system, there is still a significant part of them giving out information which could be used to exploit there system, as can be seen at Figure 5.

Based on all of these metrics, we tried to define which owner has a satisfying security performance. We evaluated this performance based on the number of security measure taken and on the system information found in the banner.

Figure 6 shows that 41.78% of the defined owners have configured their telnet ports in a way to make it more secure. They have adopted at least one of the mitigation measures presented before and they do not give any information on their system in the banner. Among those owners, 3.6% are using two different mitigation systems. It is important to note that half of the owners do not have a satisfying security performance, thus making them

more vulnerable to attacks relying on Telnet scans.

4 What risk strategies can the problem owner follow to reduce the security issue as measured in your first assignment?

When discussing about the strategies to manage the security risk, there are 4 major methods that problem owners can follow. These methods can be explained as follows.

- Risk reduction is one way of tackling the problem. For this phase, problem owners should follow a risk mitigation strategy. For the data that had spoken to, some mitigation methods can be followed to prevent the attackers getting valuable information from the leakage of information about critical running systems. According to Gunderson [9], a company should have a policy on the banners they put to openly accessible ports from internet. Agreeing to this, according to Akin (2002) [10], a banner message has four goals:

  - Be legally sufficient for prosecution of intruders.
  - Shield administrators from liability.
  - Warn users about monitoring or recording of system use.
  - Not leak information that could be useful to an attacker.

  By following these guidelines, problem owners can minimize the security threats, at least preventing the attackers from getting the information from the banners.
  Another way problem owners could consider to increase the security of the telnet system can be using kerberos to authenticate the users over non-secure networks [11]. If there must be a port that must be accessible from the internet, moving from unsecured telnet ports to secure SSH ports can also be considered. Besides, mitigation and prevented losses should be calculated for this purpose to see if the cost of mitigation are worth investing in it. This brings us to second strategy.

- On the other hand, in Risk Acceptance phase, if risk owners' calculations on risk mitigation makes investment infeasible because the mitigation costs are higher than expected losses, the risk is generally accepted and no mitigation strategy is followed.

- Another strategy that can be followed is the risk avoidance strategy. For the discussed situation, risk owners can choose to shut down the Telnet ports that they are using to access some of their critical systems from the internet if it is too risky for them to keep it on.

- Last strategy that can be used to handle the risk is the Risk Transfer. For the risk transfer phase risk owners transfer the cost of risks to third parties, such as the insurance companies. Even though an exploit can cause loss of reputation for problem owners, sometimes it is the cheaper and more feasible than investing in the risk mitigation strategies.

5 What other actors can influence the security issue as measured in your first assignment?

Following the definition of actors from the previous report, "actors" can be categorized into three groups, namely:

- Local, which includes SysAdmins and organizational decision makers.

- National, for example each countries' ministry of information security.

- Global, for example, the Internet Society (ISOC).

In this report, the term "other actors" refers to any person or instances besides the attackers. These actors can influence the security issues positively (preventing/reducing the damages) or negatively (causing worse damages).

Based on the aforementioned security problems, there are other actors that can influence the security issues, such as:

1. Non-profit organizations, for instance ISOC, Regional Internet Registry (RIR) Communities, and ShadowServer. There are several ways that these organizations can influence, for example:

    - Arranging a large meeting periodically, together with governments, research institutes, or individuals, to develop new policies to make the Internet more secure. For instance, the discussions held by RIR Communities [12]. During these discussions, basically, all three categories of actors can contribute to make the internet more secure by understanding the latest security threats and technologies. Therefore, these events can impact the security issues positively.

- Like ShadowServer [7], the organization can just scan for every kinds of security flaws and report the problems to the corresponding SysAdmins or companies. By doing this, external actors that initially have no relations with the devices owners can affect the security issues positively.
- Holding a training session about what threats can happen and how to mitigate these vulnerabilities. This can be a positive influence, because more people are aware about how to protect their devices. On the other hand, this can also be a negative influence, as they could also apply the attacks for other active devices in real-world.
- Publishing information about cybersecurity, such as the issue about "Building Trust in the Internet" raised by ISOC [13]. This method can bring positive influence to handle the security issues by increasing the awareness of the people regarding the vulnerabilities that present in the internet.

2. Governments. In general, governments usually bring positive impacts about the security issues. The information security minister will obviously try to protect the country from cyber attacks. Thus, they will create policies that can improve the security of the devices connected to the internet in their respective regions. The problem is, that these policies are deployed in a different paces. Some countries that are aware of technology threats can impose the laws quicker and more efficiently than other countries.

3. Educational institutions. In general, educational instances, such as universities [14], could also bring positive impacts in reducing security issues. Introducing the threats and mitigation could increase the awareness of SysAdmins and network configuration staffs. This means, indirectly, external institutions could bring positive influence positively about the security issues.

4. Attackers. Attackers are the directly-related actors when talking about security issues. They basically create the security issues that introduce problems for other instances, such as individuals or organizations. They have different goals of exploiting the existing vulnerabilities in the internet. For instance, as also explained in [15], economic motivations, whereby attackers can gain access to valuable assets of a person and force the victims to pay their ransom. When doing their duties, they do not want to get caught by cyber agencies, such as the police, because of

doing illegal things. Therefore, the attackers bring negative influences regarding the security issues.

6 Identify the risk strategies that the actors can adopt to tackle the problem.

In this section, the four strategies to mitigate the risk, as mentioned in previous sections, will be explained in depth based on the actors.

6.a Non-profit Organizations

6.a.1 Risk Reduction.

To reduce the risk, organizations can arrange periodic conferences about cyber security matters. The aim of these conferences is to increase the awareness of the people about existing cyber threats, for example when related to openly-accessible telnet ports. In addition, state-of-the-art mitigation strategies could also be introduced during these conferences, so that people can deploy these security measures to reduce the risks. Therefore, the impact of the risk could be reduced.

6.a.2 Risk Acceptance.

Another way to tackle the problem is by accepting the risk, which in this case, non-profit organizations could just simply ignore the openly-accessible telnet ports because some companies do need to use the telnet ports.

For example, educational institutions could conduct experiments by introducing some systems, running one of the Telnet, that can be accessible from anywhere in the internet, or SSH, for some period of time. The goal of the experiments is to teach the students why SSH is preferred over Telnet.

Based on this scenario, non-profit organizations should just accept that there are systems that are openly accessible using Telnet because the educational institutions are aware that Telnet is not secure. Furthermore, the risk is relatively minor, compared to the positive impacts on the future.

6.a.3 Risk Avoidance.

Non-profit organizations could also avoid using Telnet in their systems. By not using Telnet, hopefully, the problem could be mitigated because the underlying architecture is not used anymore.

6.a.4 Risk Transfer.

One other way to tackle the problem is by transferring the risks to external parties. For example, these organizations could recommend users to use configuration services provided by a company using their own protocols. By transferring the risk to this company, the problem could be minimized.

6.b Governments

6.b.1 Risk Reduction.

Governments could give incentives for organizations or educational institutions to teach the people or the student about the security related to Telnet ports. By doing this, the government could reduce the risk because more people are aware of the security vulnerabilities in systems that enable openly-accessible Telnet ports. This measure could be conducted once or periodically.

6.b.2 Risk Acceptance.

Taking the same case as in the previous actor, which is about the research in an educational institutions, government should also accept the risk, because the main goal of the research is for the good of the Internet. In fact, by allowing these institutions to conduct the research, the country will produce more security-aware SysAdmins, which is beneficial for the country.

6.b.3 Risk Avoidance.

Government could also impose laws that strictly saying that Telnet port must not be accessible from anywhere in the Internet. The government could also suggest some devices as the alternatives of the vulnerable devices. Thus, the risk could be avoided.

6.b.4 Risk Transfer.

One possible way to transfer the risk is by encouraging people to register insurances on the systems that are accessible openly via Telnet. This means that since the risk is transferred to the insurance company, the overall problem that the governments are responsible for is minimized.

6.c Educational Institutions

6.c.1 Risk Reduction.

To tackle the problem, educational institutions could give (mandatory) course about securing the internet, which also discusses about minimizing the usage of Telnet when configuring some devices. This might not have a direct impact on the risk, but in the future, the risk will be reduced.

6.c.2 Risk Acceptance.

Continuing the case when an educational institution gives course about securing the internet, they could also give a practical assignment on Telnet communications, such as brute-forcing the credentials or sniffing the communications. Noted that by introducing this exercises, real attackers could also gain access to these devices. However, since the risk of an attacker could really control the device is too small compared to the knowledge that the students gain, the universities could also accept that risk.

6.c.3 Risk Avoidance.

Educational institutions could also just encourage the students to avoid using Telnet. This way, the risk introduced in the previous sections will be avoided.

6.c.4 Risk Transfer.

One of the methods to transfer the risk out from individual students is by encouraging them to subscribe to a internet providers. In this case, the students do not have to configure all the home (wireless) routers and network devices that might use Telnet by themselves. Instead, the company is the one that are responsible for the risk. In this strategy, the risk is transferred from the students to the internet provider companies.

6.d Actors with Different Strategies: End Users of openly accessible Telnet ports

End-users that are defined here is the users who use the Telnet services, which could be configured by the SysAdmins. The end-users basically have no rights either to configure the devices or influence the problem. On the other hand they can act from another angle to be able to reduce risks to tackle the problems.

6.d.1 Risk Reduction.

As Telnet uses an unencrypted communication between server and client. This poses lots of risks regarding confidential information disclosure. Using virtual private networks (VPNs) can create a secure tunnel in a non-secure network which can reduce risk.

6.d.2 Risk Acceptance.

End users can accept the risk of the probability of their confidential information reveal in the network by connecting to an openly accessible telnet port. If using the telnet port without any mitigation strategies is more important than the important disclosures, that's when nonideal case of using it is accepted.

6.d.3 Risk Avoidance.

End users can deny using these ports without any mitigation strategy implemented when the disclosure of information they are transferring is not something that they can risk.

6.d.4 Risk Transfer.

Transferring the risk is not always a possible case. Also in this case there is no possible way of transferring the risk to another third party.

6.e Have the Strategies Changed Significantly over Time in A Way That Reduces or Increases Risks?

The strategies to tackle our security issue have had little evolutions over time. If the creation of Telnet goes back to 1969, the lack of security due to the protocol being unencrypted became a much more important concern during the Internet expansion of the 1990s [16]. Before that, some mitigations strategies had already been developed. One of them was to encrypt the authentication mechanism using, for example, Kerberos authentication [11]. However, the creation of SSH in 1995 which had for explicit purpose to propose a secure alternative to unencrypted protocol, such as Telnet, change the overall mitigation strategies [17]. It has since been mostly recommended to switch from Telnet to SSH as a risk reduction technique, in case a service had to be accessible from the Internet. The use of SSH is currently prevalent in the Netherlands, Telnet protocol being used for only 6% of the services available from the Internet [18].

7 Return of Security Investment

The risk strategy selected for this approximation is migrating from Telnet to SSH.

7.a Estimation of the costs involved in following that strategy

The costs of conducting the risk strategy cannot be determined precisely as each owners from our data have different number of devices to switch from Telnet to SSH, which cannot be measured from the dataset. The number of devices per owner varies from 1 up to 12100. In the case of the owners with only one device, it is more likely that they will need of a professional service to do this change, because fixing the problems might not always work. Thus, we can estimate this cost to around 100 euros [19]. In the case of the owners with a lot of devices, it is more likely for them to already have a team taking care of this sort of tasks. Therefore, we can estimate the cost based on the time it would take to switch all the device from Telnet to SSH and the hourly rate of the employees. If we consider that a network admin is paid between 25 and 72.5 euros per hour [20], and assume that the migrating process takes around 1 hour, the maximum cost for an owner (with 12100 devices) for this strategy would be 877250 euros.

7.b Impact and frequency of an attack based on the security issue

The access to a Telnet port from the Internet as presented in the dataset is not the issue, as much as it is the use made of this access. Since the possible usage are numerous, it is difficult to estimate the impact of our security issue. It can start at the cost of one device, which is privately own. However, in the case of the larger owner of the problem, which are supposedly companies, the financial impact can be the cost of the devices, the cost linked to the loss of time due to the device being inaccessible, and also their reputation. So we can estimate the loss for an owner of only one device touched by the issue to be of an approximative minimum of 200 euros. In the case of the biggest owner of our dataset, we have to consider the prices of the devices (the kind of devices being unknown, they could cost from 50 euros to several thousand), the labor costs of fixing the damages (several ten thousands depending on the issue), the potential loss of client and the loss due to inaccessibility of the devices. This can results to a maximum of 850000 euros per attack [21].

Based on the Fortinet's Threat Landscape Report, there was an average of 153 exploits per firm during the third quarter of 2017 [22]. Based on the fact that our dataset is only related to devices in the Netherlands and that Telnet is not as popular there, as in other countries, we can assume that the maximum number of attacks linked to Telnet per year to 100 [18]. In the case of an individual device owner, the number of incidents will be close to 0.

7.c Impact and frequency of an attack once the strategy has been applied

If the use of SSH do not delete all possible attack on the owner's system, it is supposed to improve it significantly. We cannot exclude the owner of the unique device, which if they are attacked while have for loss probably 200 euros. It is mostly for companies that the SSH transfer will be cut down the losses, with an approximate maximum of 400,000 euros. [21].

Once SSH is installed, the incidents linked to those open services will decrease, which varies around 0, for the individual owners, to a maximum of 50 for the bigger companies.

Based on the slides from the course, the ROSI can then be estimated as follows:

$$\text{ROSI} = \frac{(\text{ALE}_0 - \text{ALE}_s - c)}{c} \tag{1}$$

With Annualized Expected Losses: ALE = Impact (Unit) x Probability (annual). ALE_0 is for before the security strategy (between 40 and 85000000 euros). ALE_s is calculated after the security measure was applied (between 0 and 20000000 euros), and the cost c is between 100 euros and 877250 euros. Based on the defined number written above, in case of the owner of an individual device, the RoSI would be of -0.6%. In the case of a bigger company, the RoSI would be of 73%. Based on this results, it would not make sense for an individual owner to invest in this strategy. However, it would be beneficial for the bigger companies.

8 Limitations and Conclusion

While evaluating change in risk strategies over time section, we looked in detail some IPs in the original dataset which had significant difference between how many times the scan has been done on them and how many times they displayed unique banners to be able to see and analyse the change.

By this way it was planned to gather the information if they were affecting the security. It has been discovered that for some IPs after a specific time period there is no more entry. To be precise, for instance, IP address 145.130.38.249's scan started on 18 February 2018 and ended on 22 April 2018. If the reason of this cut off in the scan (considering the scan was done from 1st of January 2018 until 30th of August 2018) was because telnet port of this IP was turned off, then it means that there was a significant security change in lots of IP addresses. On the other hand, if it is removed from the scan list upon request of the IP address holder then there still may not be any difference. Unfortunately, for this discussion, we need more information about the methods ShadowServer used to collect this data which is not displayed in their website or online.

It was also hard to relate the data in the dataset with ROSI to be able to give a concrete example because the dataset doesn't include any incidents but just poses a risk.

To conclude, different actors and their important roles on how they affect the risk strategies were evaluated and an example on Return On Security Investment (ROSI) was given despite the limitations of the database.

References

[1] Telnet protocol specification. https://www.rfc-editor.org/rfc/pdfrfc/rfc854.txt.pdf. Accessed: October 8, 2018.

[2] Economics-of-security/eos_1-group_2.pdf at master · metinacikalin/economics-of-security · github. https://github.com/metinacikalin/Economics-Of-Security/blob/master/Assignment\%20block\%202/Final/EoS_1-Group_2.pdf. Accessed: October 8, 2018.

[3] Role: Problem owner. https://www.visioline.ee/itup/itup/roles/problem_owner_3556C72.html. Accessed: October 8, 2018.

[4] The mirai botnet: All about the latest malware ddos attack type | corero. https://www.corero.com/resources/ddos-attack-types/mirai-botnet-ddos-attack.html. Accessed: October 8, 2018.

[5] Securing login banners. https://docstore.mik.ua/manuals/hp-ux/en/5992-3387/ch02s10.html. Accessed: October 8, 2018.

[6] Nvd - cve - 1999-0619. https://nvd.nist.gov/vuln/detail/CVE-1999-0619. Accessed: October 8, 2018.

[7] The shadowserver foundation: Telnet scanning project. https://telnetscan.shadowserver.org/. Accessed: October 8, 2018.

[8] Economics-of-security/domainnamepercentage.csv at master · metinacikalin/economics-of-security · github. https://github.com/metinacikalin/Economics-Of-Security/blob/master/Assignment\%20block\%203/Final/DomainNamePercentage.csv. Accessed: October 8, 2018.

[9] Network security for a communications company. http://minds.wisconsin.edu/bitstream/handle/1793/40423/2002gundersonr.pdf?sequence=1. Accessed: October 8, 2018.

[10] Thomas Akin. *Hardening Cisco Routers: Help for Network Administrators*. " O'Reilly Media, Inc.", 2002.

[11] Telnet authentication: Kerberos version 5. https://tools.ietf.org/html/draft-tso-telnet-krb5-04. Accessed: October 8, 2018.

[12] Regional internet registries | the number resource organization. https://www.nro.net/about-the-nro/regional-internet-registries/. Accessed: October 8, 2018.

[13] Trust | internet society. https://www.internetsociety.org/issues/trust/. Accessed: October 8, 2018.

[14] Top cyber security schools | cyberdegrees.org. https://www.cyberdegrees.org/listings/top-schools/. Accessed: October 8, 2018.

[15] Q&a. what motivates cyber-attackers? | tim review. https://timreview.ca/article/838. Accessed: October 8, 2018.

[16] The network model of the internet explosion. https://www.oreilly.com/library/view/peer-to-peer/059600110X/ch01s02.html. Accessed: October 8, 2018.

[17] Ssh port | ssh.com. https://www.ssh.com/ssh/port. Accessed: October 8, 2018.

[18] National exposure index. https://www.rapid7.com/data/national-exposure/2018.html#NL. Accessed: October 8, 2018.

[19] Stepping up security: Migrating from telnet to ssh. https://www.pragmasys.com/pdfs/pragmawhitepaper_migratessh.pdf. Accessed: October 8, 2018.

[20] Salaries voor systems administrator. https://www.glassdoor.nl/Salarissen/amsterdam-systems-administrator-salarissen-SRCH_IL.0,9_IM1112_KO10,31.htm?countryRedirect=true. Accessed: October 8, 2018.

[21] Cost of cyber crime study. https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf. Accessed: October 8, 2018.

[22] Threat landscape report q3 2017. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/Threat-Report-Q3-2017.pdf. Accessed: October 8, 2018.

9 Annexes

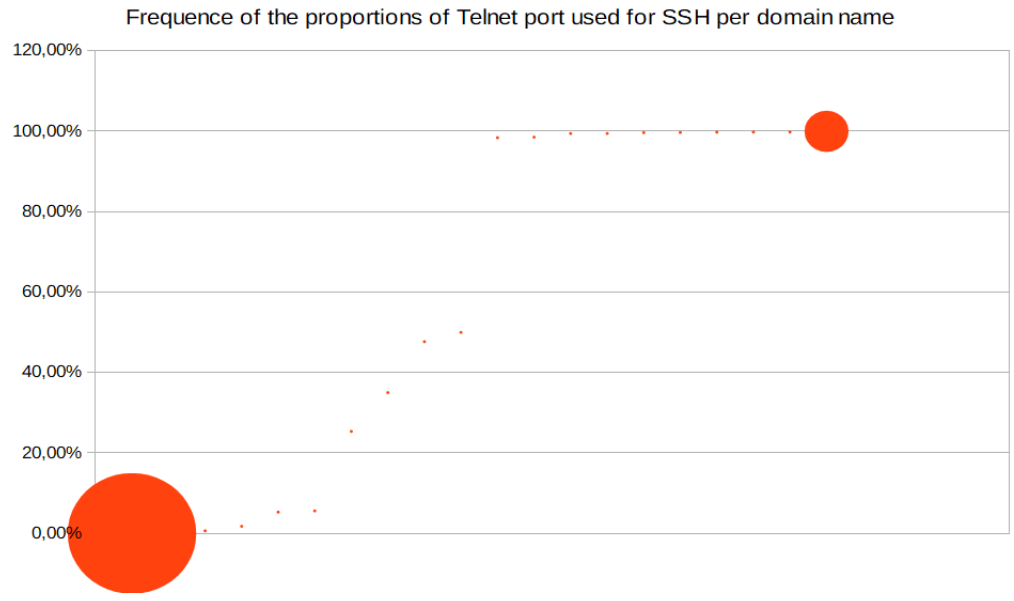

Figure 1: Frequency of the Proportions of Telnet Port Used for SSH per Domain Name.

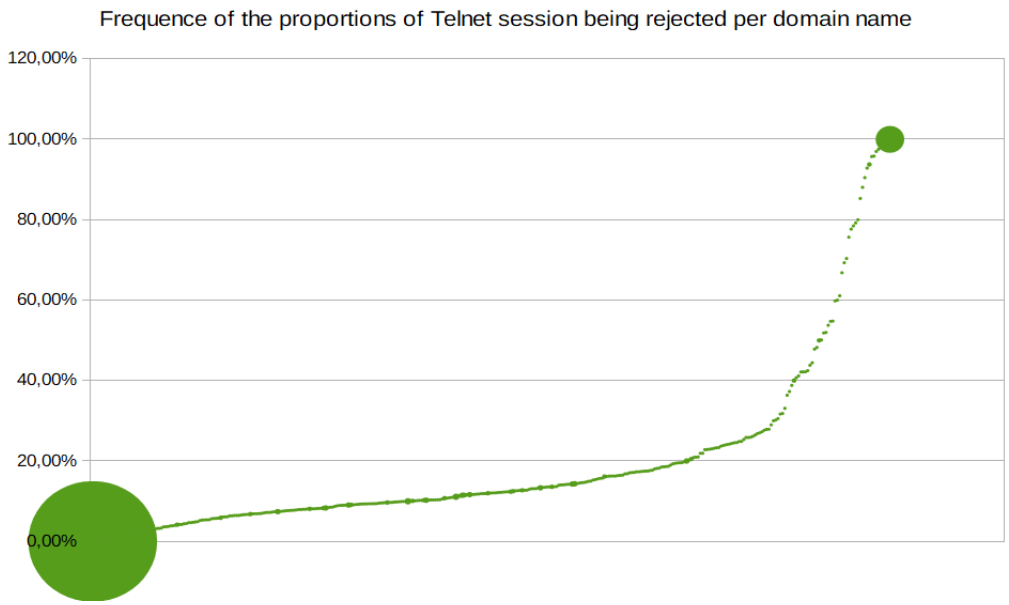

Figure 2: Frequency of Rejected Telnet Sessions per Domain Name.

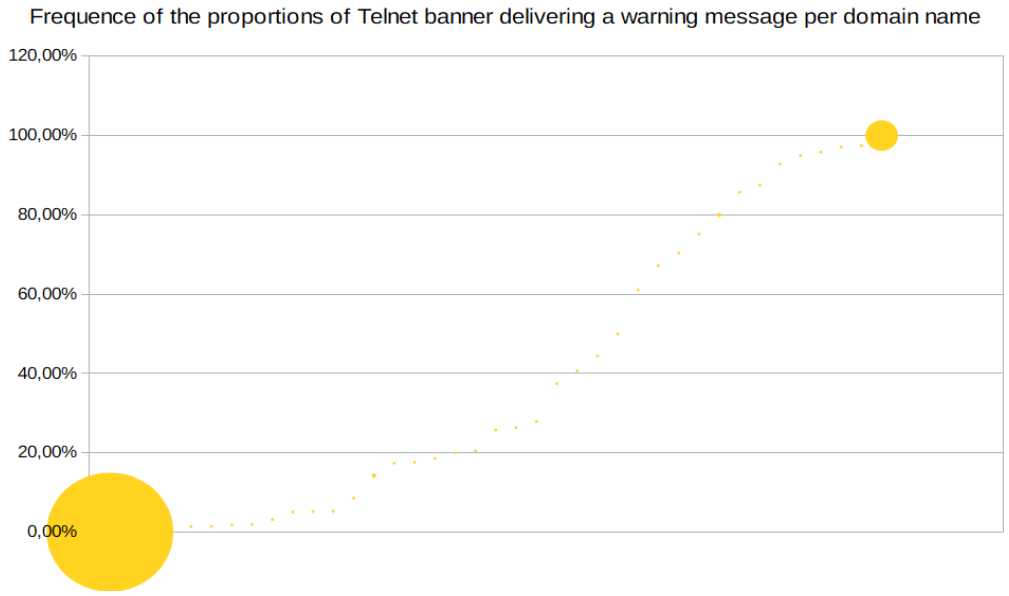

Figure 3: Frequency of Warning Message in the Banners per Domain Name.

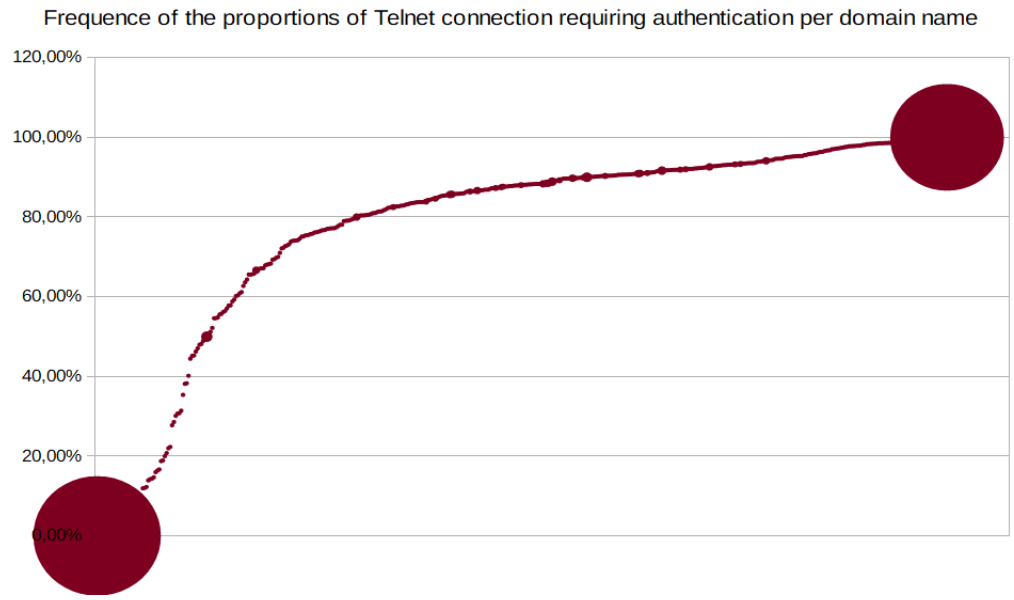

Figure 4: Frequency of Telnet Communications Requiring Authentication per Domain Name.

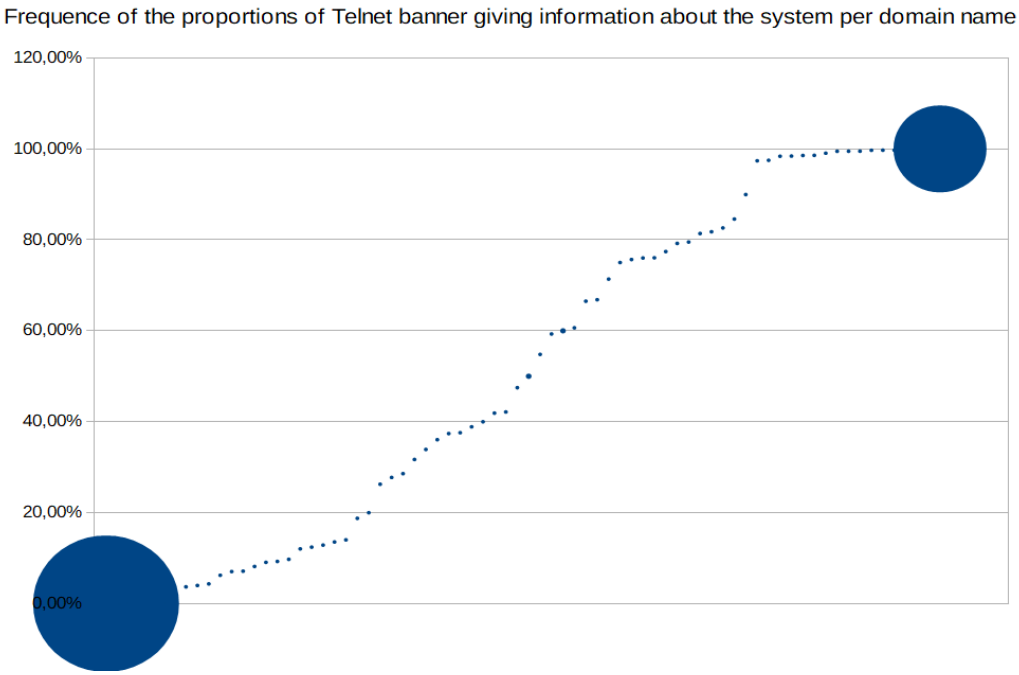

Figure 5: Frequency of Telnet Banners Leaking System Information per Domain Name.

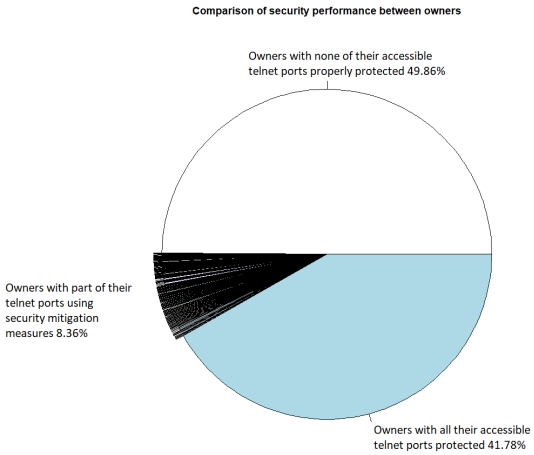

Figure 6: Security Performance Comparison