Economics of Cyber Security Botnet Tracker

M. Kesteloo - 4291158 & R.D. Meeuwissen - 4287150 & P. Remeijsen - 4286243

September 23, 2018

1
INTRODUCTION

In this report we will be discussing the importance of measuring cyber-security, as it relates to a specific domain. To determine the budget available for security, decision makers should be aware of what the current situation is and be able to compare this with past situations. This will help decision makers with communicating about security performance, diagnosing problems and helps with providing a better insight into effective resource allocation. However, because security can not be measured directly, proxies have to be used that can indicate whether security is being handled correctly. In order to do this, appropriate security metrics are needed. The difference between security metrics and measurements is that the metrics take the context into account and produces some insight of value to the observer of the metric. The analyst should be able to reliably monitor these metrics, as well as be able to use them in order to contribute to the security goals.

The particular domain that will be the focus of this report will be botnets. A botnet often sends malicious code to other computers and it does so automatically and autonomously. This way, it creates an even bigger network by infecting victim's computers which will then send the malicious code automatically to others. The data that will be used comes from trackers. These trackers monitor the behavior of the malware, such as the status, infected domains/IP-addresses, botnet Command & Control (C & C) servers and the trackers often provide blocklists to allow firms to block malicious network traffic.

For example, one of the trackers concerns Ransomware. This particular type of malware serves to hold data for ransom in order to coerce the victims into paying the spreaders of the ransomware. Like with a lot of types of malware, ransomware often spreads with Trojans. These are files that seem legitimate, but are actually the malicious software. Victims download the malware through either a malevolent source or some other type of scheme. Once the ransomware is on the computer of the victim, it activates and consequently encrypts data on that computer. Next, the ransomware notifies the victim that only the attackers have the ability to decrypt the data in order to recover it [1, 2]. Sometimes the victim can decrypt the data themselves, but as these types of criminals have become more advanced, the level of encryption has also improved. The result is that the victims are left with the choice to pay, or consider the data to be lost. Ransomware is a significant problem with a very large number of victims and is certainly at the forefront of cybercrime. This particular tracker differentiates between three types of threats. The first type is C & C servers. These are arguably the most interesting as these are the servers that send commands to other nodes in a botnet. The second type are payment sites and the third are distribution sites. These are distinctions that other trackers often make as well. Zeus and Feodo are also financial malware for which datasets are available, but these will not be used in this report. It should be noted that multiple versions of the malware are being tracked and are contained in the dataset.

In Section 2, a further analysis will be given regarding the security issue that will be the focus of this report, as well as which parties are involved. In Section 3, the ideal metrics will be discussed. In Section 4, the metrics that are achievable in practice will be examined. Finally, the metrics defined in Section 4 will be evaluated in Section 5. For this iteration of the project we will only do some analysis on the Ransomware dataset due to it being the most readily available. Considering the other two datasets are very similar and multiple factors smaller, doing the same analysis on them will not be much added value.

2
Security Issue

As we have explained in Section 3, we will examine the data generated by botnet trackers. The problem with botnets is that the malware which is originally spread by the cyber criminal's C & C server is hard to detect: anti-virus programs often do not detect it because the creators of malware are trying to make the malicious code look like standard code. Furthermore, victims may not notice the effects until the malware is used to encrypt the user's files (ransomware). This ensures that the malware is spread to many computers before detection. According to Damballa (now Core Security), an information security company, there were 3.6 million computers infected with ZeuS malware in 2009 [1]. This demonstrates how rapidly such networks can grow.

In order to define the security issue properly, there are a number of factors that have to be considered. Namely:

- Who are the parties involved?
- What are the threats?
- What is at stake?

In this assignment, the focus lies on financial malware. We will use data from ZeuS, Feodo and Ransomware trackers. The malware that these trackers monitor can for example be used to steal credentials or credit card information, committing fraud or encrypting the victim's files. There are a number of parties involved that could be considered the victims. They can be big firms, banks, insurance companies and individuals. Even when the direct target is an individual, banks and insurers can still be affected when the direct target makes a claim on them. Other parties can include the companies selling anti-virus software who also have a stake in this problem as they can earn money if their software helps with detection of malware. The security issue here is the active botnet C & C. The threat that they pose to the parties described earlier include both financial and operational risks. A research paper by Tajalizadehkhoob et al. [3] elaborates on three strategies:

- Access providers taking down the C & C
- Clean up infected machines
- Hosting providers taking down the C & C

It should be noted that the products of trackers such as blacklists can be very valuable in the execution of all three strategies. Similarly, all parties except the attackers and maybe the unknowing users would benefit when the trackers are as successful as possible.

[1] See https://en.wikipedia.org/wiki/Zeus_(malware)

3

Ideal Metrics

As we already mentioned in Section , it is very important that security decision makers have knowledge about the security issue, which means a set of metrics should be available to them. However, there is often a gap between the ideal metrics that security researchers are looking for and what is actually available in practice. In this section, the ideal metrics will be discussed, as well as what are the key characteristics of these metrics.

The ideal metrics are dictated by the security issue at hand. Because metrics gain their value from the context in which they are defined, the metrics that will be discussed are specific to the security issue explained in Section 2. In order to deal with the security issue presented by the botnets, it would be ideal to have metrics that inform us of some key characteristics of these networks. Examples would be whether the nodes of the network are clustered around certain regions of the world. Similarly, knowing when a certain domain is related to malicious behaviour would also be useful. One of the challenges with botnet trackers is that it is not a perfectly accurate system. Supplementary information such as the accuracy, scope and false positive rates of the trackers would be very valuable to the decision makers using the tool. Similarly, information from hosting providers about the digital landscape of countries would be useful. For example, the Netherlands are one of the worlds largest hosting providers, so it would be wrong to assume that the Netherlands is "the worst" hosting provider. This is an example of distinguishing between metrics and measurements. These metrics would not give insight into control or the losses, but would instead help to hinder the expansion of the botnet by giving insights into the incidents aspect. Furthermore, we have to keep in mind that we have multiple stakeholders involved like we explained in Section 2. Each of these will want other sets of metrics. We will provide a list of ideal metrics which are useful for all stakeholders, but some will be more useful to for example companies which provide anti-virus software then for banks.

- The speed at which new malware versions are developed. The potential losses can then be estimated more accurately as new versions are often not detected immediately.
- The time needed to detect a new version of malware.
- Distribution of C & C servers across geo-locations.
- Which users will get infected in the future.
- Time till malware removal
- Accuracy of detection: are we certain that all malware gets detected someday and how often is normal software branded malware.
- The up-time of a malicious domain.
- The financial costs (from the past and future) caused by the financial malware (insurance money, lost clients due to reputational damage, etc.)
- Which hosting provider is preferred by the criminals at any time.

4

Metrics in Practice

4.1. CVSS/CCSS/CMSS

A way to measure cyber security is by evaluating the principal characteristics of a vulnerability, produce a numerical score reflecting its severity and by explaining why it has that particular score. Three different ways of scoring are defined in the following frameworks:

- Common Vulnerability Scoring System (CVSS)
- Common Configuration Scoring System (CCSS)
- Common Misuse Scoring System (CMSS)

A detailed explanation of these frameworks can be found below.

4.1.1. Common Vulnerability Scoring System

The CVSS is the most famous scoring system of the three mentioned before. The benefit of this scoring system is that there is a standard for the scoring of vulnerabilities and users can easily identify whether a certain vulnerability has a higher risk than other vulnerabilities [4]. Therefore identifying the financial gain of solving a vulnerability is easier.

The framework is composed of three metric groups: the base, temporal and environmental. They are described by Mell (2007) in the following way: The base represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments. The temporal represents the characteristics of vulnerability that change over time but not among user environments. The environmental metric group represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment.[4]

The score is a number ranging from 0 to 10, where 0 is the lowest risk posed and 10 is the highest risk posed. The calculation is shown in Figure 4.1. When calculating the CVSS score the base metric is a requirement and the temporal and environmental metrics are not required but give a more accurate reflection of the risk posed by a vulnerability to user's environment. The base equation is derived from two sub equation: the exploitability sub score and the impact sub score. The CVSS metrics produce besides the numerical scoring also a textual representation of the metric values used to score the vulnerability. It contains each value assigned to each metric and is always displayed with the vulnerability score to add more detail.[5]

4.1.2. Common Configuration Scoring System

The CCSS is a framework derived from CVSS. This system can assist organization in making decisions about how security configuration issues should be addressed. A security configuration is a composition of settings of a certain software program which can be altered inside that software. For example turning encryption on or off. A security configuration issue vulnerability is using the configuration settings in way that it negatively affects the security of the program. In principal the scoring system is quite similar to the CVSS and CMSS. The

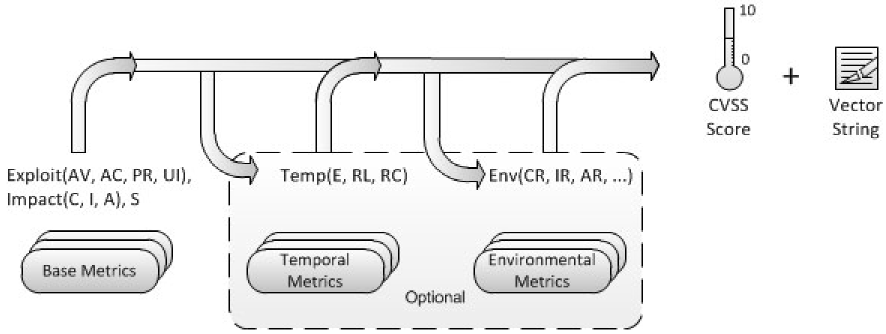


Figure 4.1: CVSS Metrics and Equations[5]. The Base Metric is a requirement for the calculation of the CVSS score. I consists of the exploitability metrics and impact metrics. Together with the optional Temporal Metrics and Environmental Metrics an output score ranging from 0 to 10 and a explanatory textual representation is produced.

most notable difference of the base metrics is that the type of exploitation, active or passive, is also measured. Active exploitation refers to an attacker performing actions to take advantage of a vulnerability, where on the other hand passive exploitation's refers to vulnerabilities that prevent authorized actions from occurring. The temporal and environmental metrics are quite different from CVSS. The temporal metrics focus on the general prevalence of attacks against the vulnerability and the general effectiveness of available remediation measures. Examples are using anti-virus software and conducting awareness activities. The environmental metrics are divided in two metric groups: exploitability and impact. This allows to generate sub-scores for these groups which is not available in CVSS.[6]

4.1.3. COMMON MISUSE SCORING SYSTEM

Like CCSS, CMSS is also derived from CVSS. It has the same common core and the composition is quite similar to that of CCSS. This scoring system focuses on software feature misuse vulnerabilities. A software feature misuse vulnerability is present when the trust assumptions made during the design process can be abused in a way that violates security. These misuse vulnerabilities allow attackers to use the functions of the software, that were intended to be beneficial, for malicious purposes. An example is being able to render HTML in an email, but the hyperlinks in this HTML email are used to send the receiver to a malicious website. The base metrics are the same as CVSS, though the temporal en environmental metrics have some differences and are the same as CCSS. [7]

4.2. OTHER CYBER SECURITY METRICS

There are many other ways to measure the security level. The Center for Internet Security (CIS) has created a document that provides guidelines to help organizations set up their set of measures and metrics more efficiently [8]. The Mission Support Alliance (MSA) for example used this document to set up their set of metrics: the Hanford Cyber Security Metrics. The MSA set a few goals for this set [9]. Firstly, the metrics have to be meaningful. Secondly, the metrics have to be reproducible. Thirdly, the set of metrics should be manageable and last but not least, they should provide an increased level of transparency. They got their inspiration from both NIST publications as well as a paper written by Payne [10] but they eventually used the CIS security metrics as main inspiration. The CIS security metrics can be applied to almost any situation as they are easily adapted to suit ones needs.

In a recent paper, Tajalizadehkhoob proposed some metrics which can be used for financial malware [3]. Some of the metrics they propose are:

- Distribution of malware types over the years.
- Distribution of malware hosting types over the years.
- Number of providers hosting C & C domains per year.
- Amount of new C & C domains per host per year.

- Amount of removed C & C domains per host per year.
- Cumulative percentage of C & C domains for the percentage of hosting providers.

4.3. METRICS OF THE RANSOMWARE DATASET

The dataset of the ransomware contains the following data:

- Firstseen (UTC) → Date malware was first found
- Threat → Three different kinds of threat-levels:
  - Ransomware botnet Command & Control servers (C&Cs)
  - Ransomware Payment Sites
  - Ransomware Distribution Sites
- Malware → Name of the malware
- Host → The IP or domain name used by the ransomware
- URL → The URL where the malware can be found
- Status → The status of the server, eighter online, offline or unknown
- Registrar → The supplier of the domain
- IP address(es) → The IP address used by the ransomware, if the domain name is unavailable, this is the same as the Host
- ASN(s) → autonomous system number
- Country → source country of the host

There are a number of metrics that could be defined from the measurements contained in the dataset. Due to the amount of effort in cleaning the dataset, only a small number of metrics were ready to be included in this report, before the deadline. These are:

- The number of servers per country for the most common countries of origin.
- The number of servers per top level domains for the most common.

The results will be displayed in the next section.

5

Designed Metrics and Evaluation

In this section, an examination will be given concerning the metrics defined in the previous section. This will be a limited analysis considering this deliverable was meant to be a descriptive and exploratory view of the dataset.

5.1. Threats to Validity

After inspection of the dataset it turns out that the data is not clean in the slightest. An example would be numerous different variations of the same names. Sometimes as little as a point or a case difference. We have taken steps to mitigate this, but we can not make guarantees about the quality of the analysis. For example, we are not sure whether a very small deviation like other casing (GoDaddy instead of godaddy) means that we can map these instances to the same group. Additionally, the amount of data available is also not very satisfactory. The hope is that we can make improvements on this aspect of the analysis for the next deliverables.

5.2. Metrics

First we will look at the number of servers for the most common countries of origin, see Figure 5.1. We can see that the majority is actually unknown. We can also see that the U.S is the next most common origin. The value of such a metric lies in the ability to discriminate between traffic from certain countries. For example, extra measures could be taken when the traffic originates from one of the most common countries. When

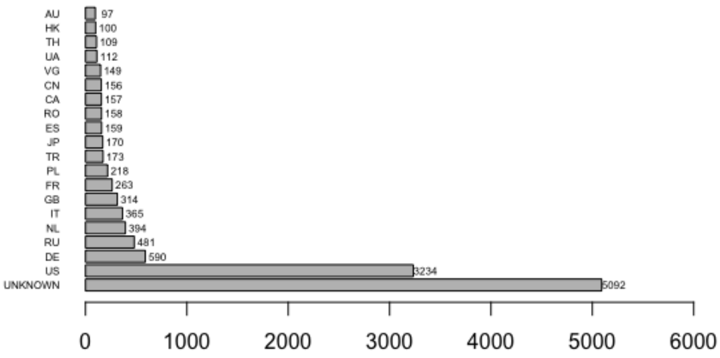


Figure 5.1: Chart of the most common countries of origin.

using such a metric, one must keep in mind that one has to adjust for the size of the country. The fact that the U.S is the most common country could also in part be because it is home to a majority of the traffic in general. Armed with this knowledge, both government as well as the providers could make more informed decisions.

The next metric is the most common registrars, see Figure 5.2. Again we can see that the most common label is unknown. Similar to the metric regarding the countries, the list of most common registrars that are involved with the botnets will enable decision makers to be more aware of the reality of the situation. Similarly, anti-virus software could be more diligent when the software being scanned is originating from a particular registrar.

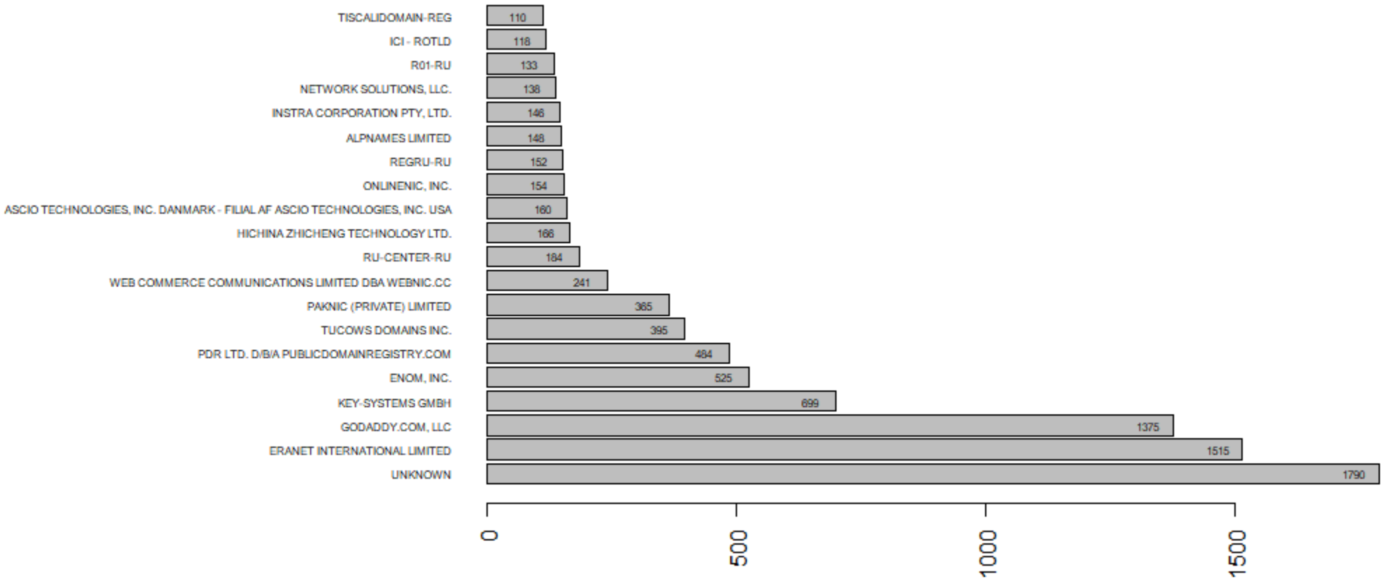


Figure 5.2: Chart of the most common registrars.

Third, the most common top level domains are presented, see Figure 5.3. This statistic is similar to the previous two metrics. For example, when taking into account the relative number of malware-associations per domain, anti-virus software could take extra precautions when scanning software from a certain domain. By using one or more of the three metrics, government could also take extra steps against parties distributing software from high-risk domains according to these metrics.

5.3. CVSS

On the website of first.org [5], the CVSS score can be calculated. In Section 5.3.1, the calculation and reasoning behind it is explained. Furthermore, a vector representation is formed which can be seen in Figure 5.5.

5.3.1. Base Score

- Attack Vector: Network <- Ransomware is remotely exploitable.
- Attack Complexity: High <- The attacker needs to have access to a system to execute the malware.
- Privileges Required: Low <- With basic user access, an attacker can already manage the desired result.
- User Interaction: None <- Whenever the system is infected by the malware, no user interaction is required.

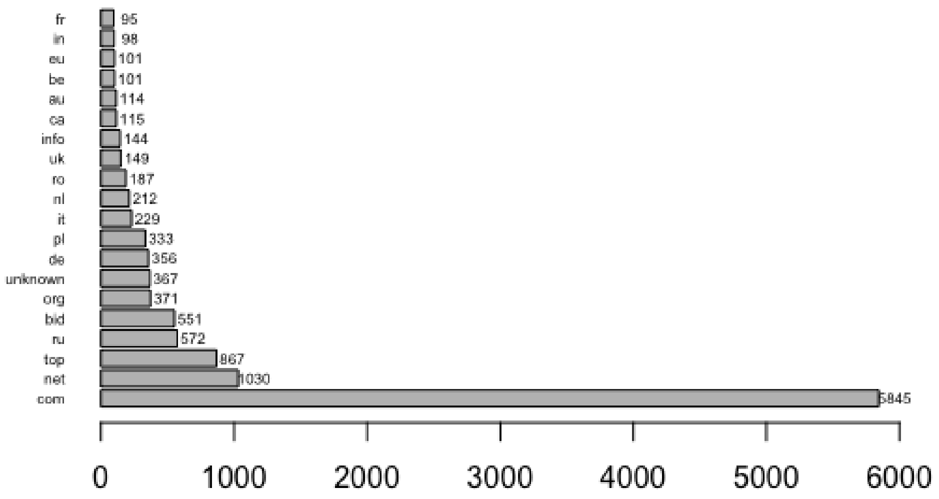


Figure 5.3: Chart of the most common top level domains.

- Scope: Unchanged <- Ransomware only targets data which it has access to.
- Confidentiality: High <- There is a total loss of confidentiality, as certain user data can not be accessed anymore by the user.
- Integrity: High <- The data can not be accessed anymore. Only the attacker is able to make the data accessible again.
- Availability: High <- The data is not accessible until the attacker makes it accessible again.

See also Figure 5.4.

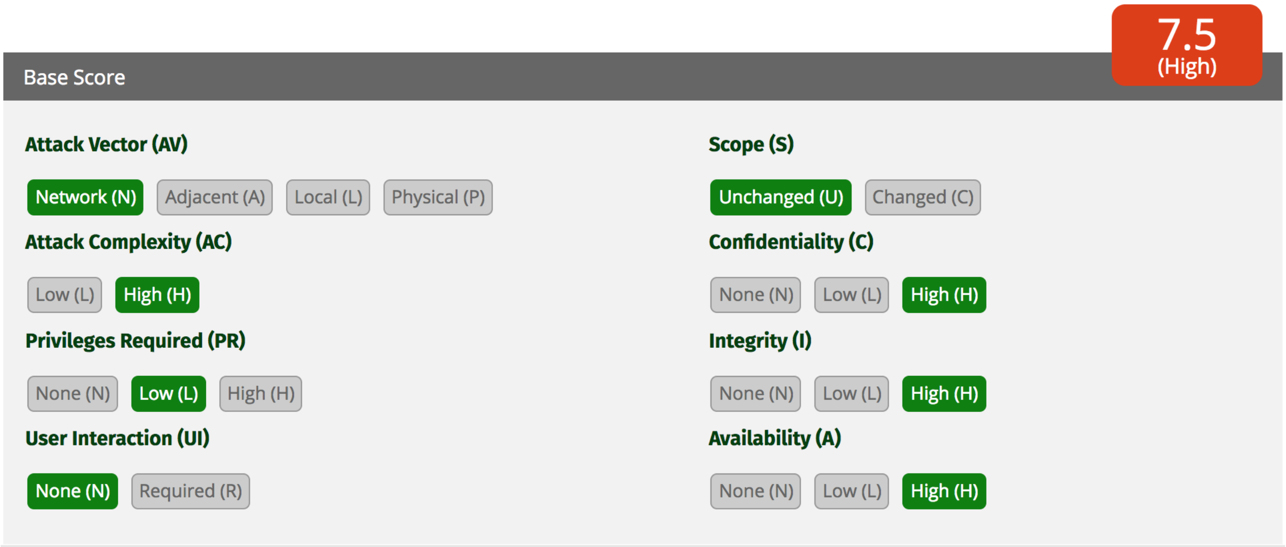
5.3.2. Temporal Score

- Exploit Code Maturity: Not Defined <- There is no information how likely it is that a user will be targeted.
- Remediation Level: Workaround <- By making sure your system has perfect security and the user is aware of security risks and handles correctly, the likelihood of being a target of ransomware is rather small.
- Report Confidence: Confirmed <- The ransomware tracker dataset shows that loads of systems are vulnerable for this malware. As can be seen in Figure 5.1, most of the attacks come from the US.

See also Figure 5.6.

5.3.3. Environmental Score

The environmental score is not evaluated as there is not one single organization analyzed.



Base Score

7.5 (High)

Attack Vector (AV)

[✓ Network (N)] Adjacent (A) Local (L) Physical (P)

Attack Complexity (AC)

Low (L) [✓ High (H)]

Privileges Required (PR)

None (N) [✓ Low (L)] High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

[✓ Unchanged (U)] Changed (C)

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

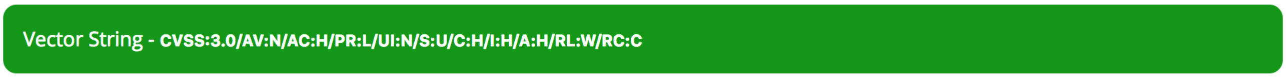
Integrity (I)

None (N) Low (L) [✓ High (H)]

Availability (A)

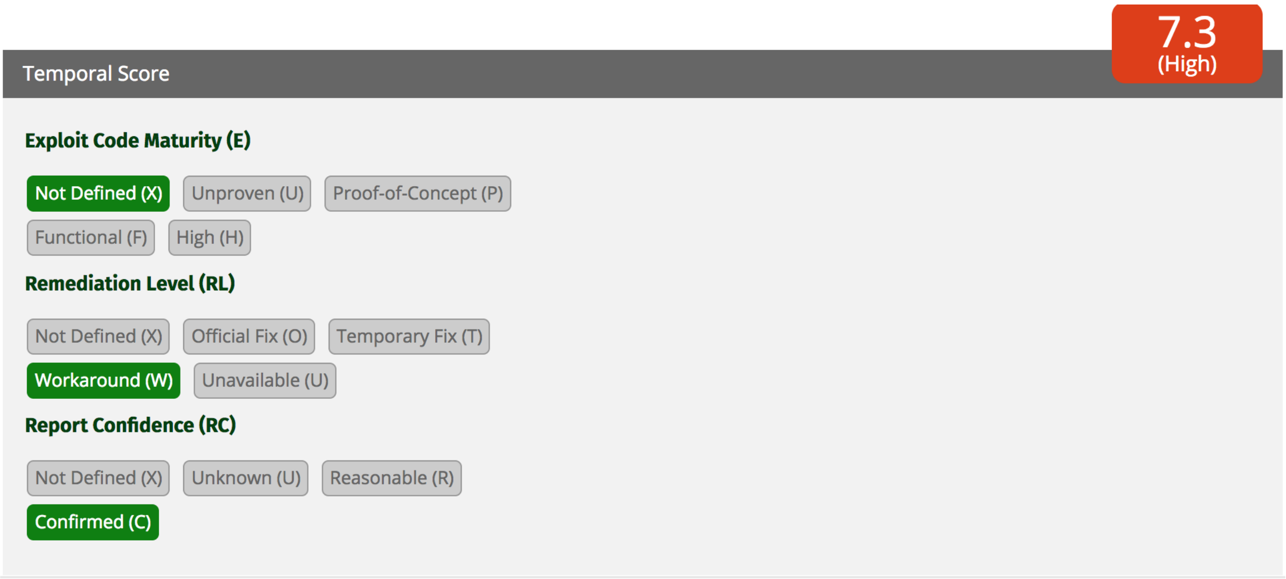
None (N) Low (L) [✓ High (H)]

Figure 5.4: The evaluated base score calculation from first.org[5]



Vector String - CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/RL:W/RC:C

Figure 5.5: The evaluated vector string from first.org[5]



Temporal Score

7.3 (High)

Exploit Code Maturity (E)

[✓ Not Defined (X)] Unproven (U) Proof-of-Concept (P) Functional (F) High (H)

Remediation Level (RL)

Not Defined (X) Official Fix (O) Temporary Fix (T) [✓ Workaround (W)] Unavailable (U)

Report Confidence (RC)

Not Defined (X) Unknown (U) Reasonable (R) [✓ Confirmed (C)]

Figure 5.6: The evaluated temporal score calculation from first.org[5]

Bibliography

[1] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, *Cutting the gordian knot: A look under the hood of ransomware attacks,* in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (Springer, 2015) pp. 3–24.

[2] X. Luo and Q. Liao, *Awareness education as the key to ransomware prevention,* Information Systems Security **16**, 195 (2007).

[3] S. Tajalizadehkhoob, C. Gañán, A. Noroozian, and M. v. Eeten, *The role of hosting providers in fighting command and control infrastructure of financial malware,* in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security* (ACM, 2017) pp. 575–586.

[4] P. Mell, K. Scarfone, and S. Romanosky, *A complete guide to the common vulnerability scoring system version 2.0,* in *Published by FIRST-Forum of Incident Response and Security Teams,* Vol. 1 (2007) p. 23.

[5] First.org, *Cvss v3.0 specification document,* .

[6] K. Scarfone and P. Mell, *The common configuration scoring system (ccss): Metrics for software security configuration vulnerabilities,* NIST interagency report **7502** (2010).

[7] E. Van Ruitenbeek and K. Scarfone, *The common misuse scoring system (cmss): Metrics for software feature misuse vulnerabilities (draft),* (2009).

[8] C. for Internet Security, *The cis security metrics,* .

[9] M. S. Alliance, *A report from the field: Implementing cyber security metrics that work,* .

[10] S. C. Payne, *A guide to security metrics,* SANS Security Essentials GSEC Practical Assignment Version **1** (2001).