Economics of Cyber Security Botnet Tracker

M. Kesteloo & R.D. Meeuwissen & P. Remeijsen

September 17, 2018

1

Introduction

The security issue that will be discussed in this report, as well as the following reports, is the tracking of different types of malware. Trackers are web-services that register the hosts and IP-addresses affiliated with the spread of malware. This serves to keep track of dangerous parties that should be avoided, as well as incidentally gathering some data about these parties. The data comes from three different trackers that slightly differ in the attributes that they track, as well as the types of malware that they track. By using trackers, the cyber security community might learn something about their opponents, as well as produce valuable side-product like blacklists. These could be used to stifle the spread of the malware. Some trackers also link to resources the victim could consult for purposes like identification of the ransomware, or forums for decrypting-solutions. This could lead to an increase in the probability that one could decrypt the data without paying. The trackers often rely on a community to update the tracker database and allows people to submit entries. These will, after verification by the administrators of the tracker, be added.

One of the trackers concerns Ransomware, which 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 and make it recover it [1, 2]. Sometimes the victim could 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 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 3 types of threats. The first type is Command & Control (C & C) servers. These are arguably the most interesting as these are servers that send commands to other nodes in a botnet. The second type are payment sites and the third are distribution sites.

The second tracker we will look at is pertaining specifically to the command and control types of servers, which is called Zeus. It keeps track of these types of threats on a global scale and has been known to receive retaliation from presumably disgruntled criminals[1].

The last tracker pertains to a specific Trojan called Feodo, which is used to commit fraud and steal personal information such as credentials or credit card details.

[1] See https://krebsonsecurity.com/tag/zeustracker/

2 Metrics

To determine the budget available for security, decision makers should be aware of how the current situation is and be able to compare this with past situations. Being able to compare situations also helps decision makers with communicating about security performance, diagnosing problems and helps with providing a better insight into effective resource allocation. However, good security metrics are needed. But what are the ideal metrics for security decision makers? Böhme came up with a *security production function* [3] which maps the cost of security onto the security level. The security level in turn has a stochastic influence on the benefits of security, see Figure 2.1. The security level is split up into four parts: controls, vulnerabilities, incidents and (prevented) losses. Control is considered to be without a threat environment and vulnerabilities are considered to be with little threat environment. The ideal metrics should therefore give in indication on the controls in place and the vulnerabilities in the system. The ideal situation however would be that incidents and prevented losses, which are with a threat environment, are also measured for making security decisions. Unfortunately it is difficult to find metrics for the threat environment, that is for incidents and especially (prevented) losses. The question is why it is so difficult to measure this threat environment. The straightforward answer is that the threat environment is stochastic. It is constantly changing and can be influenced by a great many factors. For example, cyber criminals might design new attacks which makes it easier for them to attack or users become more aware of threats, making them less vulnerable.

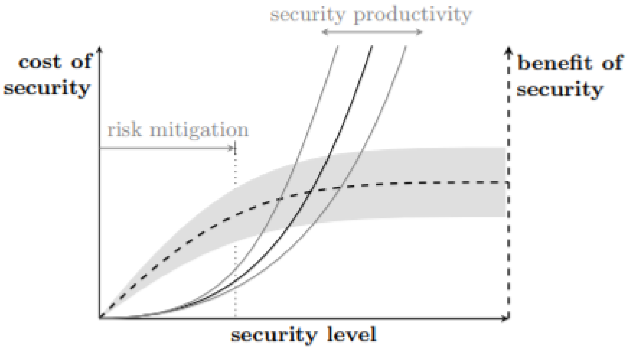

Figure 2.1: The security production function [3]

Summarizing the above, the ideal metrics would have to give an indication of the security level of the controls, vulnerabilities, incidents and (prevented) losses.

3

Ransomware Metrics

As explained in the introduction ransomware is malware that often spreads with Trojans. When ransomware is tracked valueable data can be retrieved. By means of metrics we can visualise this data and use it to explain and prevent the spread of these Trojans.

3.1. The Ransomware Dataset

The dataset of the ransomware contains the following data:

- Firstseen (UTC) → Date malware was first found
- Threat → Three different kinds of threatlevels:
    - 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

3.2. Insights and Corelations

The data could give multiple insights and corelations. For example the most fraudulent top level domains (TLDs) for ransomware could be shown; Which countries are the source of most ransomware; And which malware is used the most in a certain time frame.

3.3. Lack of Data

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] R. Böhme, *Security metrics and security investment models,* in *International Workshop on Security* (Springer, 2010) pp. 10–24.