Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorarbeit

Felix Karl Franz Uelsmann

Cyber Threat Intelligence - An economic analysis of how to handle security incidents

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Felix Karl Franz Uelsmann

Cyber Threat Intelligence - An economic analysis of how to handle security incidents

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung

im Studiengang Bachelor of Science Wirtschaftsinformatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Klaus-Peter Kossakowski
Zweitgutachter: Prof. Dr. Klaus-Peter Schöneberg

Eingereicht am: 20. Februar 2016

Felix Karl Franz Uelsmann

Thema der Arbeit

Cyber Threat Intelligence - An economic analysis of how to handle security incidents

Stichworte

Cyber Threat Intelligenge, Sicherheit

Kurzzusammenfassung

Dieses Dokument befasst sich mit der Fragestellung, welchen Mehrwert eine funktionierende Cyber Threat Intelligence liefern würde. Im Speziellen werden die verschiedenen Angreifergruppen, deren Methodiken und wie man durch präventive Maßnahmen monetäre Mittel einsparen kann, betrachtet.

Felix Karl Franz Uelsmann

Title of the paper

Keywords

Cyber Threat Intelligenge, Security

Abstract

This document analyzes the question what the main benefits of Cyber Threat Intelligence are. A functional CTI could work in a preventiv way to defend against threats before they occur on a system. Futhermore, threatening groups and their corresponding attack patterns .

Contents

List of Tables

List of Figures

1 The era of Cyber Threat Intelligence

With the rise of new technologies in our society, Cyber Security is getting more important by the day. People tend to think antivirus software and windows built in firewalls are enough to secure them properly. These kind of software is only reactive, which means, something has to happen to your systems before these programs are able to react. To act in a proactive way, we need a tool that not only aggregates information but also provides strategies before something occurs. Cyber Threat Intelligence not only collects information, it is able to provide the right strategy for each individual case. One program, trying to achieve the goal of not only reacting before an attack occurs but going further and analyzes user and device behavior is Microsoft Advanced Threat Analytics[1] for example. The program analyzes log files, which are storing data about every single step that occurs in an it environment. For example the number of authentication tries or which IP address is currently occupied by which user. If the system detects unusual or dangerous behavior, it automatically informs the security officer in charge and gives advice of how to handle this incident. But what the program does not do, is sharing this information with other users of the software.

Cyber Threat Intelligence does only work if all the informations are shared. If a new incident is successfully handled by one user, the others are saving up the time to learn how to handle the incident. Therefore the time which need to be invested by cyber security officers and their staff in order to handle this incident can be used elsewhere. The amount of time and money which is saved by using the best practice way of another company, who handled the incident successfully is called the learning effect.

The idea of using information as an advantage in case of an upcoming attack is very old. To quote the art of war "If you are not stronger than your enemy, be smarter." Let us take a look at a real world example to get a better idea of what this quote means.

You are a medium sized company and a situation occurs in which 100,000 bots [2] are attacking your network with a distributed Denial-of-Service attack (dDoS) [3]. Your web-service is crashing, users are not able to log into their accounts anymore. You lose money every minute. Most

[1] Microsoft (2015)

[2] remotely controlled PCs

[3] Chang (2002)

businesses that size are not able to run their own Computer Emergency Response Team (CERT) to handle such complex attacks.

And now imagine you are able to rely on global database, which can tell you how this attack works. You would know you could redirect the traffic from the bots via a service called anti-dDoS Server and still be able maintain your service.

The attacker is stronger in case of soldiers he owns, in order to attack you but you know that these soldiers are mindless. This leads to other part of the quote be smarter. Since these soldiers are not able to think, they are only following commands, in our case send the same request to the server over and over again. If the company now setups a anti-dDoS service before the main server of the company, it will recongnize this behaviour and redirect the traffic to a dead end. Therefore the main server will not be affected at all.

Cyber Threat Intelligence is all about using information to make smart decisions and this thesis will explain how information can be extracted and used in order to make our cyber environment a much securer place.

1.1 Motivation

Why do you think, establishing a secure cyber environment to work and to live in, is important? People tend to think its not their job to establish it. There is a certain community, they assume, which handles all kinds of incidents and vulnerabilities. Their digital environment is protected by the manufactures and third party software like Avira or McAffee, but is this enough? Do you know what kind of damage an attacker could do if he infiltrates your system? More importantly, do you really think attackers who perform attacks against governments and agencies like the Federal Bureau of Investigation (FBI) are not able to hide themselves? Classic security software is only able to react, if the software recognizes a certain signature inside the malicious application. These programs are only able to react if the manufacturer already has this specific signature in his database.

As a CIO or CEO of a company you not only have to account for your competition, but you also have to be concerned with those actively working against your business. These come in various shapes, those employing information technology to harm your business and who will be discussed in this thesis are known as black and grey hat hackers. Black hats are using illegal methods to seriously cause financial, image or identity theft damage to people or companies in order to enrich themselves. Grey hats on the other side are hacking into systems using illegal methods either to prove the lack of security inside certain companies or for internet fame.

Weather you are company , a political party, a manufacturer or a financial institution, all of

them have individual enemies. We will further look into the motivations for their activities in chapter three. Since companies need to rely on their information systems, databases, and cloud collaboration, intelligent cyber criminals are able to cause considerable damage to them. While an in-depth analysis of the current situation is provided in chapter four, my key assumption is that without adjusting the way we handle security now, we could be facing serious threats in the future.
Cyber Threat Intelligence is able to change how security incidents are handled. Furthermore it is able to save a lot of money due to the fact that incidents need to be handled only once in the optimal case.

1.2 Aim of the thesis

The aim of this thesis is to serve as a practical guide for decision-makers in upper management, to help them decide what kind of security level is needed for their business to establish a secure cyber work environment. Furthermore, it is intended to support employees from the field of IT-security by providing an overview of Cyber Threat Intelligence in general. Sharing information about different threats and incidents regarding your IT infrastructure is a critical point of Cyber Threat Intelligence. Through sharing of knowledge of incidents and exploits, a database can be established, which will guide your decision on what kind of protection is required for your company.

It is important to understand that not only security staff needs to be well informed about current cyber threats. Some vulnerabilities could be exploited because an employee, who has not installed the latest update of the flash player for example. There are attack patterns in which old software releases are used to execute arbitrary code with user rights in order to copy his password for example or steal sensitive data. The technical understanding of each vulnerability is not necessary to provide a secure IT-environment but it is indeed important to teach your employees the importance of cyber security.
Your cyber security staff would always be informed about the latest vulnerabilities, specific attack patterns or a rise of attacks in your field of operation. They would have a plan at hand to know as much as possible about upcoming attacks or how to handle attacks they did not experience before.

1.3 Target audience for this thesis

This thesis is intended for people who are interested in developing smarter responses to upcoming threats, such as CISOs (Chief Information Security Officer), CEOs (Chief Executive Officer), managerial staff, companies cooperating with the military or governments. Sensitive information like constructual drawings, military grade secrets or bank account data need to be protected under any circumstancs. Even if there are contracts between two countries to not perform cyber attacks against each other like in the event of the USA and China it does not guarantee protection. A recent example are the chinese black hat hacker group *"deep panda"*. It attacked technology and pharma companies in the USA shows that even a contract between two of the mightiest nations does not prevent such espionage attacks [4].

This document is meant to function as an introduction for people, who are not particularly informed about information security issues. It aims at providing solutions to common issues and introducing ways for improving defense strategies through Cyber Threat Intelligence. It gives insights into the ways in which companies can save financial resources by implementing a Cyber Threat Intelligence database in order to prevent cost-intensive damage.
Furthermore, it is important to me to write a thesis which can be used by non-specialists. It is important to me to interest and inform a broad audience about the threats present in a technologically advanced society. The best way to prevent damage through cyber threats, is to inform the broader public of its dangers.

1.4 Differentiation

In order to keep this bachelor-thesis in a regular scale, there a some aspects which will not be discussed in detail.
Technical details of certain attacks are not a part of this thesis in order to keep it understandable for a broad audience.
Several business terminologies like costumer acquisition costs or revenue will not be discussed. The implementation of a Cyber Threat Intelligence database is not part of this thesis as well. The goal is to provide sufficient information in order to understand the benefits of global database for threat prevention. A detailed introduction into Cyber Security is out of scope as well. A good introduction can be found on https://www.futurelearn.com/courses/introduction-to-cyber-security

[4] Kharpal (2015)

1.5 Structure

At first I will explain the basic principles of Cyber Security 2, especially the difference between Information Security and Cyber Security. These fields are related but they both need to fulfill different tasks in order to work. Afterwards we are looking at the term Cyber Threats because there are threats who could influence our security status but are not predictable like floods or fire. These physical threats are not of interest for Cyber Threat Intelligence. In order to understand how these threats are fought against at the moment, we need to take look at the current handling of security incidents. Furthermore we will take a look at the costs of incident handling to show that there is room for improvement in this sector. At last we will show the current state of the art regarding Cyber Threat Intelligence to show what is possible at the moment.

The chapter "Analysis of threats and the threatening groups" is about the different attacker groups and their attack models. In order to be prepared in the best possible way, you need to understand your enemies. Different groups are targeting different kinds of companies or organizations to achieve certain goals.

Afterwards the improvement of our current Cyber Security is the focus of chapter "Improvement oof Cyber Security trough Cyber Threat Intelligence" to show based on an example how we are able to retrieve information to use it for our own defense. The attack is divided in three phases to show the process of this particular attack and to analyze it step by step. The last part of the thesis shows how much financial damage such an attack could cause and how much it would have cost to prevent an attack like this.

In the end further research topics based on this thesis will be presented as well as the conclusion and outlook.

2 Introduction to Cyber Threat Intelligence

Cyber Threat Intelligence is compared to established concepts like cyber security and information security relatively new ellusive concept. The wikipedia page for this topic was created in August 2015, which indicates the majority of people is not aware of its existence. The concept of using intelligence in order to analyze certain trends is not completely new. Business intelligence, which is analyzing trends on the stock market works in a similiar way with the difference that threat intelligence analyzes cyber crimes, activism and espionage rather than stock prices.

2.1 Cyber Security vs. Information Security

To get an idea how Cyber Threat Intelligence is preferable to add an important dimension to classic security, there are two major topics which need to be explained. Information Security (InfoSec) and Cyber Security are defined, standardized, established ISO norms to provide a global standard. Information Security as defined in the 44 U.S. Code 3542:

(1) The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:
(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity
(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
(C) availability, which means ensuring timely and reliable access to and use of information.
[1]

If we look at this definition from the view point of a company, the main purpose is to protect important assets. These include the company's unique selling propositions, employee data, and – one of the most important aspects – data about the cash-flows. If able to obtain this information, attackers have leverage against the company. This could be used in order to

[1] https://www.law.cornell.edu/uscode/text/44/3542

achieve a certain goal like money or other information which can be selled.

The following list of norms are of particular interest for information security professionals.

- ISO 15443: "Information technology - Security techniques - A framework for IT security assurance"
- ISO/IEC 27002: "Information technology - Security techniques - Code of practice for information security management"
- ISO-20000: "Information technology - Service management"
- ISO/IEC 27001: "Information technology - Security techniques - Information security management systems - Requirements"

Cyber Security or IT Security in comparison is meant to secure your whole environment. Hardware, software and information everything related to a company environment.
According to the Department of Homeland Security, 'Cyber Security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access' [2]. Furthermore it has 5 main tasks to fulfill.

- *Application Security*
  The process of eliminating vulnerabilities inside of applications which can be exploited. You should perform penetration testing to your application in order to test a variety of scenarios. These tests are helping to achieve a higher state of security for your application.
- *Information Security*
  Protecting your information assets are a key task in every company. Several different ISO norms were established to achieve this particular goal like the ISO 15443 which was mentioned above.
- *Network Security*
  Establishing a protected network not accessible by unauthorized people and preventing unwanted communications to the internet from our protected network.

[2] http://whatis.techtarget.com/definition/cybersecurity

- *Disaster recovery / business continuity planning*
  Describes how an organization should deal with potential disasters. A disaster is an event that makes the continuation of normal functions impossible. A disaster recovery plan, therefore, consists of the precautions taken so that the effects of a disaster will be minimized and the organization will be able to either maintain or quickly resume mission-critical functions. Typically, disaster recovery planning involves an analysis of business processes and continuity needs; it may also include a significant focus on disaster prevention.[3]

- *End-User Education*
  However, it should be noted that security precautions are not effective if users are uninformed about information security issues. Password security can prove to be quite dangerous, for instance if passwords such as "123456" are used by accountants. Ensuring users understand the importance of password strength, thus, is one of the crucial steps in the process. As we see, information security is part of cyber security but it is specialized in securing data. Securing information about critical fields inside a company weather it is personal data of employees or companys is a very important task in every kind of instituition.

2.2 Cyber Threats

The United States CERT[4] provides a general definition of Cyber Threats: "Cyber threats to a control system refer to persons who attempt unauthorized access to a control system device and/or network using a data communications pathway. This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the internet. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders. To protect against these threats, it is necessary to create a secure cyber-barrier around the Industrial Control System (ICS). Though other threats exist, including natural disasters, environmental, mechanical failure, and inadvertent actions of an authorized user, this discussion will focus on the deliberate threats mentioned above." [5]
The German agency for informaton security “Bundesamt für Sicherheit in der Information-technik “ (BSI) provides a catalog on how to ensure the ISO 27001 certification in a company.

[3] http://searchenterprisewan.techtarget.com/definition/disaster-recovery-plan
[4] Computer Emergency Response Team
[5] https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions

They do provide information on how to deal with physical threats like natural disasters, access control and cyber threats to achieve a certain standart of a secure cyber environment. [6]
Cyber Threat Intelligence now uses any kind of information about Cyber Threats. But not only responsive actions against a known threat are important. Significant questions are:
How is an attacker able to use different kinds of vulnerabilities? What is he able to achieve if he exploits these? Is there more than one way to exploit it? All those questions and many more could be used to build an enormous knowledge database. This database could include information about attack statistics like already known bots which are attacking my network or which time is most common to start attacks. Signatures of viruses, worms or trojans which have not been registred in the antivirus software database. Furthermore unusual behavior of users could be saved to identify certain attack patterns. The regular download volume for example is around 100 megabyte per day and it suddenly rises to 10 gigabytes. This could be an indicator for a potential data theft. These kind of information could allow an investigation unit to identify a potential spy for example.
The issue of Cyber Threats is a very broad topic within Cyber Security. It has been discussed in many works before[7]. Due to its nature of different complexities, it is difficult to estimate a standard price of handling security incidents when vulnerabilities are exploited. To provide a better overview about security incident handling, the next section will provide a shortened version on how to handle individual incidents.

[6] https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Zertifizierung27001/GS_Zertifizierung_node.html

[7] in Network Security Imperial College UK; MEng in Electrical Engineering und Greece. (2015) Choo (2011) MITRE

2.3 Handling Security Incidents

In the event of an update, vendors commonly publish a description of the vulnerabilities, they are about to close with the update. Most of the more known vendors use generic descriptions of what an exploitation of the vulnerability could cause. These are pretty dificult to interpret for users who have no technical background sometimes.
The following description of the heartbleed vulnerability by US CERT shows how such a vulnerability descriptions looks like:

OpenSSL versions 1.0.1 through 1.0.1f and 1.0.2 beta through 1.0.2-beta1 contain a flaw in its implementation of the TLS/DTLS heartbeat functionality (RFC6520). This flaw allows an attacker to retrieve private memory of an application that uses the vulnerable OpenSSL libssl library in chunks of up to 64k at a time. Note that an attacker can repeatedly leverage the vulnerability to increase the chances that a leaked chunk contains the intended secrets. The sensitive information that may be retrieved using this vulnerability include:

- Primary key material (secret keys)
- Secondary key material (user names and passwords used by vulnerable services)
- Protected content (sensitive data used by vulnerable services)
- Collateral (memory addresses and content that can be leveraged to bypass exploit mitigations)

Solution

This issue is addressed in OpenSSL 1.0.1g. Please contact your software vendor to check for availability of updates. Any system that may have exposed this vulnerability should regenerate any sensitive information (secret keys, passwords, etc.) with the assumption that an attacker has already used this vulnerability to obtain those items. Old keys should be revoked. Reports indicate that the use of mod spdy can prevent the updated OpenSSL library from being utilized, as mod spdy uses its own copy of OpenSSL. Please see https://code.google.com/p/mod-spdy/issues/detail?id=85 for more details.[8]
Regular users of computer systems probably do not understand the impact of such a vulnerability. Heartbleed was one of the most discussed bugs in the year 2014 since it showed how

[8] http://www.kb.cert.org/vuls/id/720951

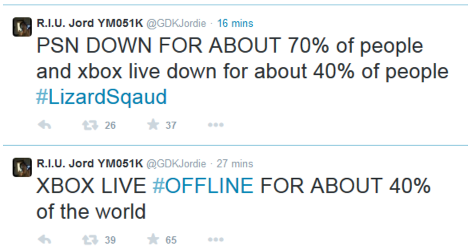
insecure a very trusted encryption software like the Open Secure Socket Layer (OpenSSL) was. Personal experience in the field of handling security incidents often followed the scheme below.

- A problem occurs and is penetrating one the following vectors.
  - Availability
  - Confidentially
  - Integrity
- The exact damage/ kind of attack is determined
  - Which vulnerability has been exploited?
  - How did the attack work?
  - What kind of data has been compromised/stolen/ made unavailable?
  - Did the attacker get any kind of unauthenticated access to the system?
  - Was the attacker able to execute any kind of code?
- Counter actions are being initiated to prevent further damage
- Repairing the system to its pre-attack state.

That is more or less the scheme used by vendors to describe security incidents. A more detailed way is described in the Computer Security Incident handling guide from the National Instute of Standards and Technology (NIST)[9] The problem which occurs is, that an attack has to be performed by an attacker to make them react against it. The attacks on the PlayStation Network and Xbox live around December 2014, are two examples of such attacks. More specifically, both fell victim to a considerable Denial-of-Service-Attack and were unable to regain control.

[9] Grance u. a. (2004)

As a result, the game servers of the two biggest console gaming companies were unreachable for seven days. The infamous hacker squad – *Lizard Squad* – took responsibility for these attacks on Twitter shown in figure 2.1.



R.I.U. Jord YM051K @GDKJordie · 16 mins

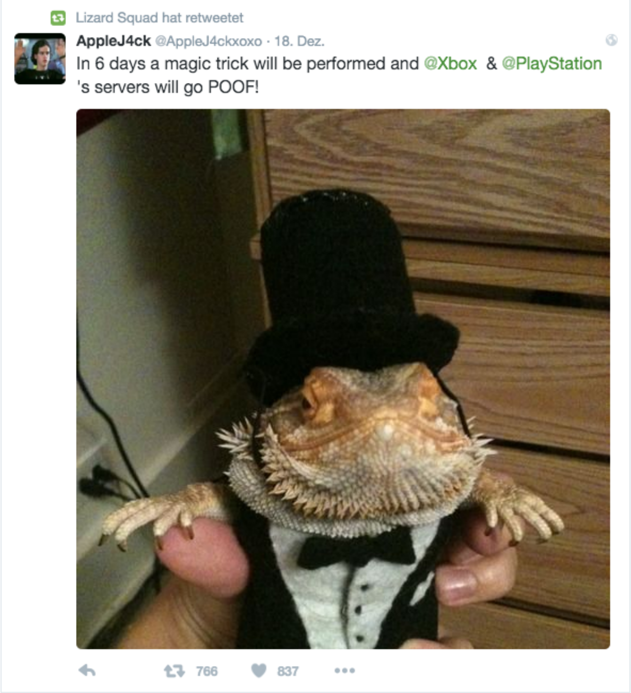
PSN DOWN FOR ABOUT 70% of people and xbox live down for about 40% of people #LizardSqaud

R.I.U. Jord YM051K @GDKJordie · 27 mins

XBOX LIVE #OFFLINE FOR ABOUT 40% of the world

Figure 2.1: Tweet about PSN and XBOX Live attack

To announce upcoming attacks from certain groups has been some kind of standard procedure. In figure 2.2 Lizard Squad announces the upcoming attack in December 2014 to the Playstation Network and Xbox Live. Other examples are oftenly seen by the group Anonymous who are announcing attacks against ISIS for example.



Lizard Squad hat retweetet

AppleJ4ck @AppleJ4ckxoxo · 18. Dez.

In 6 days a magic trick will be performed and @Xbox & @PlayStation 's servers will go POOF!

Figure 2.2: Announcement to attack PSN and XBOX Live on Christmas Eve

The Lizard Squad is only one example of a group of hackers intending to gain attention from the media and the broader public. Furthermore they are looking for some kind of fame or recognition from other groups.
There are many more groups on the darknet, forums and websites, such as 4chan, posting announcements in order to get the recognition for their attacks. More attacks, especially spectectular like the botnet attack on Sony and Microsoft (December 2014) are examples for it. Website-crawlers are automated programms to look for specific keywords on websites. They could be used to look for upcoming attacks. Companies could be prepared for the impact of an attack and at the same time other companies could also adapt these mechanisms against the same attacks.

2.3.1 Cost of Security Incidents

One of the key questions relating to information security for companies is: "What does it cost to prevent and fight attacks?". Equally important question is: ""What does it cost to repair the damage caused?"
However, providing even a rough estimate is difficult, without all companies providing their estimates. In 2015 Microsoft held its tech conference in Hamburg. The conference introduced their new tool, focusing on advanced threat analysis. Microsoft estimated annual cost of security incidents worldwide at around *3 Billion $*.[10]
This, however, only covers the costs of handling incidents once they occurred. In this estimation the aspect for which Cyber Threat Intelligence could really make a difference is missing: the learning effect.
Currently, every single company has to learn how to defend their assets against every new threat individually. If the information about potential threats would be a commonly available, the cost to learn about the correct measures against the threat would decrease significantly and quickly.

Lizard Squad's attack on Microsoft and Sony is a case in point. The PlayStation Network experienced a substantial dDoS-Attack in December 2014; resulting in 70% of user accounts unable to connect to the network. As a result, Sony suffered considerable losses. The human capital needed to restore services was immense. Hundreds of employees thoroughly focused on this single task for days, until they were able to regain control. Simultaneously, Microsoft was faced with the same attack on its Xbox live system. Had both companies shared the information they gathered on these attacks, costs for both would have been minimized. On the other hand Sony would damage itself by handing out beneficial information to Microsoft:

[10] citeMicrosoft2015

Microsoft would receive something like a heads up in form of better information about the attack and minimized loss of reputation from their costumers. This is a great disadvantage for Sony. Since they are competitors on the same market, it is unlikely for companies like them to share their information on attacks like that.

Nevertheless the process of mutual exchange and learning is a key aspect of Cyber Threat Intelligence. It entails that companies and organizations would no longer go through the same learning processes over and over again to defend themselves against attacks. Every company participating in this system would profit from the very beginning. Systems could be checked for previously exploited vulnerabilities to make sure others cannot be threatened with the same exploit. IP-blockers from known bots or proxy-servers, used to hide their traces by using an in-between server, could be established.
Signatures of backdoor-programs like Trojans, viruses and worms could be saved for an even better blocking table than from well-known anti-virus-software. Triggers who provoke hackers to attack certain companies or organization, like political statements or business decisions, could be identified. This could help to not only build something like an early warning system but furthermore to help them with their public relation strategies.
Public organizations like the German Parliament could benefit from such an information sharing system as well.

2.4 Cyber Threat Intelligence

Cyber Threat Intelligence is a relatively new sub-field of Cyber Security. Thus, there is no commonly agreed definition for the term yet [11]. The most fitting for this thesis is provided by the Mitre cooperation:

Cyber threat intelligence itself poses a challenge in that no organization in and of itself has access to an adequate scope of relevant information for accurate situational awareness of the threat landscape. The way to overcome this limitation is via sharing of relevant cyber threat information among trusted partners and communities. Through information sharing, each sharing partner can potentially achieve a more complete understanding of the threat landscape not only in the abstract but also at the instantial level of what specifics they can look for to find the attacker. MITRE Information is gathered and categorized to find solutions for attacks before they occure. The core functionality of CTI is the sharing of information about attacks, vulnerabilities and threats to build a network for finding solutions as a unit for IT-security. From an economic point of view this a very interesting field for secure environments. The situation at the moment consists of many companies who have their own security centers to provide such an environment for themselves. This means that every single attack against the companies has to be solved and afterwards repaired over and over again. Now imagine, you, as a company, have access to a global knowledge network, providing information about attacks, threats, vulnerabilities, threatening groups, attack patterns and much more. You could use this information to build a secure and up-to-date environment.
An easy example:
In 2014 the PlayStation Network (PSN) was attacked by the infamous hacker association Lizard Squad. They probably used a huge network out of hacked computers to generate so much traffic that the PSN servers where not reachable for the community. Before they attacked the PSN, Lizard Squad infected a lot of systems with malware to remotely execute arbitrary code. This kind of network is called Bot-Net and it is basically an army of zombie computers. Sony was not able to shield its servers against this distributed Denial of Service attack and the PSN was not reachable for several days after Christmas. Economically, this was a disaster. A few days after the attack against Sony, Xbox Live – the counterpart of PSN from Microsoft – was also attacked with the same method. If Microsoft and Sony would have worked together against the same "enemy", they would probably have found a solution against the attack in a significantly shorter period of time. Sony could have provided intell about what they already

[11] Mcallister und Ludwick (2015)

tried, where the attack was coming from, warning signs and other important information. Microsoft could have been much better prepared and could already have looked for other ways of building a defense.

2.5 State of the Art

According to the CERT-UK cyber security vendors define Cyber Threat Intelligence based upon their procedural viewpoints and competitive imperatives. To define this term for thesis, the combination of two definitions will be used.

The Software Engineering Institute of the Carnegie Melon University defines Cyber Intelligence as follows:

The acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions, and activities to offer courses of action that enhance decision making.[12]

It underlines the importance of gathering as much information as possible to built a knowledge base which is capable of not only analyzing vulnerabilites but in addition activities. The activities which could be interesting range from political decisions to the leak of confidential information. It is also important to understand the intentions of the attacker. Gartner defines Threat Intelligence:

It is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.[13]

The most influencing organization regarding Cyber Threat Intelligence is the MITRE cooperation. They are a not-for-profit organization that operates research and development centers sponsored by the federal government (United States of America). They are responsible for developing the data format Structured Threat Information Expression (STIX). This format is able to provide sufficient information for everyone who is involved in defending networks and system against cyber threats. This structured format which uses a common language to describe cyber threat information allows easy sharing within the same community using this format.

Microsoft with its advanced threat analysis programm is also on its approach but without sharing their experiences with other users of the same software. This is not compliant with the idea of Cyber Threat Intelligence to share information about experiences with certain incidents.

[12] Mcallister und Ludwick (2015)

[13] Definition: Threat Intelligence https://www.gartner.com/doc/2487216/definition-threat-intelligence

A whitepaper published by the SANS organization also shows the trend of Cyber Threat Intelligence and has been really helpful for generell understanding of the idea.[14]

[14] urlhttp://www.sans.org/reading-room/whitepapers/analyst/cyberthreat-intelligence-how-35767

3 Analysis of threats and the threatening groups

To get an idea about the current threats, we need to take a look at the different groups and their methods of attacking. These groups goals are different, highly variable and based on their underlying motivations for the attacks on different people and organizations. These groups can be driven by a variety of motivations ranging from political purpose to gain information or public recognition.

Groups like Anonymous, Pro-ISIS or Lizard Squad are all called hacker groups, but their motivation to attack governments and organizations are completely different. The general pattern of an attacker is shown in figure **??** .

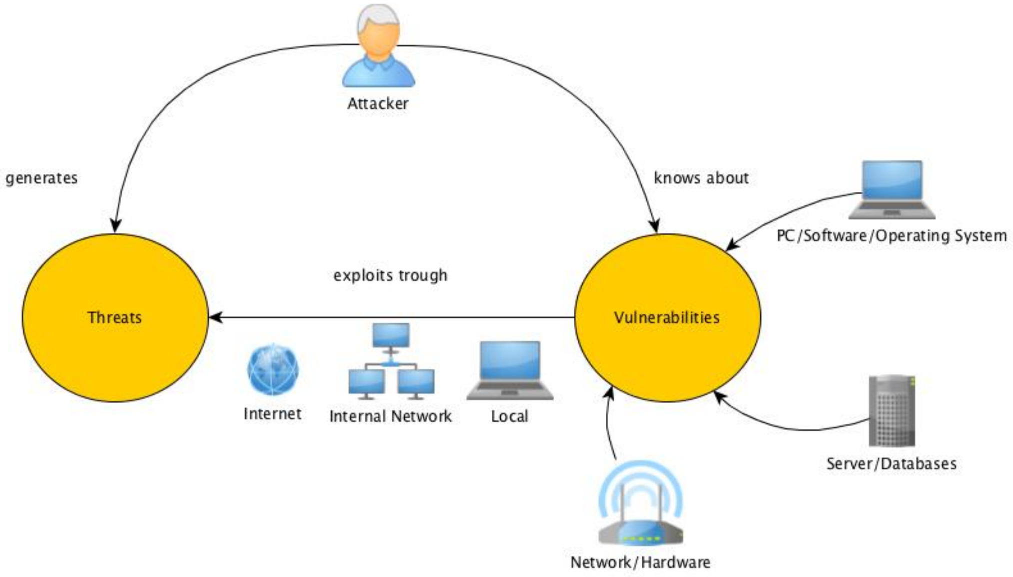


Figure 3.1: generell attack

3.1 Hacktivists

According to Manion und Goodrum (2000) Hacktivists use their skill of computer hacking to help advance political causes. A recentliy very famous group will give you an idea about their motivation to attack certain parties.
The ICS-CERT [1]Hacktivists are described as follows:
Hacktivists form a small, foreign population of politically active hackers that includes individuals and groups with anti U.S. motives. They pose a medium level threat of carrying out an isolated but damaging attack. Most international hacktivist groups appear bent on propaganda rather than damage to critical infrastructures. Their goal is to support their political agenda. Their subgoals are propaganda and causing damage to achieve notoriety for their cause. [2] Anonymous is famous for spreading news about topics like politics, cyber security, environment, rights and intelligence. The idea behind Anonymous is not to become a group or an organization. It is to become the idea itself of a free world where everybody is equally treated. Their own words from the website are:[3]
This article is not about becoming an Anonymous member. Anonymous is not an organization nor a group. Anonymous is an idea, and ideas are bulletproof. If you want to be Anonymous, you are already "in." EVERYONE and ANYONE can be Anonymous: spread truth, share any post, video or tweet regarding Anonymous or its operations, or write & submit your own article to AnonHQ! Just remember, always stay anonymous, do not show your face or reveal your identity, for this is the power of Anonymous.
The group is well known in public due to the considerable media coverage their actions have received. Back in 2008, Anonymous started attacking Scientology because of their try to take down a video interview from Tom Cruise. They used a simple method to start one of the biggest DoS-attacks in the history of the organization. Thousands of people called the support-hotline to ask general or stupid questions just to block their ability to receive calls [4]. Anonymous overall intention as hackers is to work for justice, following their statements on twitter.[5] Their goal is neither money, nor whistle blowing like for example Edward Snowden and the NSA incident, instead their goal is to spread the word about actions against free speech on the internet. A few examples:

The hack of the Zimbabwean government for censoring WikiLeaks documents or against

[1] United States Computer Emergency Response Team
[2] cert.us cert.gov (2014)
[3] http://anonhq.com/be-anonymous/
[4] Cosh (2015)
[5] https://twitter.com/youranonnews?lang=de

Visa, MasterCard, PayPal for blocking their services to WikiLeaks in 2010. A more recent example would be operation “Ice ISIS”, motivated by the act of terror against Charlie Hebdo, Anonymous released the following statement on their social media accounts.

> *ISIS: We will hunt you, Take down your sites, accounts, emails, and expose you.*
> *From now on, no safe place for you online*
> *You will be treated like a virus, and we are the cure*
> *We own the internet*
> *We are Anonymous; we are Legion; we do not forgive, we do not forget, Expect us.*
> Cosh (2015)

3.2 Cyber Criminals

Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam[6], phishing[7] and spyware/malware [8] to commit identity theft and online fraud. Office (2009) When you take a look at the FBI most wanted cyber criminals list, the most frequent crimes committed by those people are money laundering, wired fraud and financial crimes like credit card fraud. One of the most well known criminal organization on the internet was the group behind the “silk road”. Back in 2013 Ross Ulbricht aka "Dread Pirate Roberts" was captured by the FBI [9]. They did not only distribute illegal goods like drugs, weapons, credit card numbers and hacking services in addition they laundered money trough the service bitcoin wallet to cover their illegal activities even more. [10] One darknet service became infamous in 2013 trough their spectacular take down by the FBI. The illegal marketplace was called silk road and besides drug trafficking and illegal gun offers, some market salesmen offered hacking services and stolen credit card numbers. The “silk road” and “silk road” 2.0 were taken down by the authorities but it did not stop them. “Silk road” 3.0 is still offering hacked accounts and other services. [11]

Figure 3.3shows how other users, who bought hacked accounts validate the usefulness of those. The system from silk road works similar to web shops like amazon or ebay. Users with very good ratings are often offering more than one service or hacked account. As seen in

[6] unsolicited messages

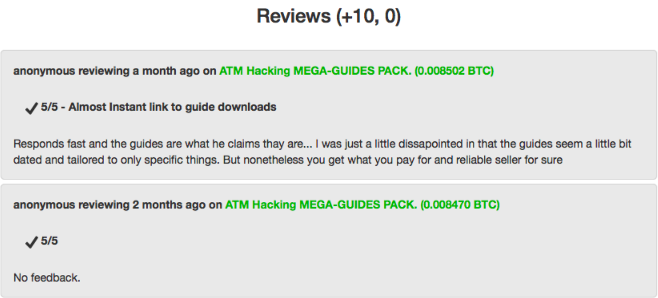
[7] The attempt to steal sensitive information such as usernames, passwords and credit card data

[8] software that aims to gather information about a person/organization without their knowledge

[9] http://www.theguardian.com/technology/2013/oct/02/alleged-silk-road-website-founder-arrested-bitcoin

[10] Bad (2015)

[11] The Screenshots were taken at 03.11.2015 with my personal account.



Reviews (+10, 0)

anonymous reviewing a month ago on ATM Hacking MEGA-GUIDES PACK. (0.008502 BTC)

✓ 5/5 - Almost Instant link to guide downloads

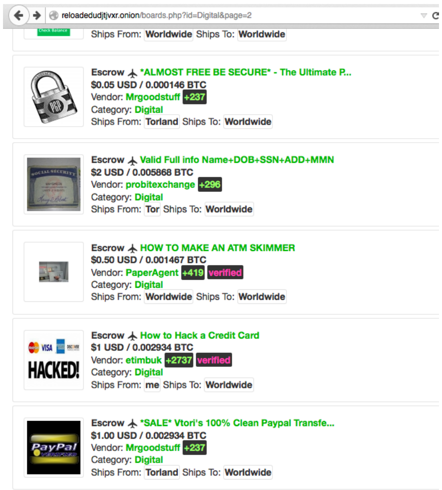
Responds fast and the guides are what he claims thay are... I was just a little dissapointed in that the guides seem a little bit dated and tailored to only specific things. But nonetheless you get what you pay for and reliable seller for sure

anonymous reviewing 2 months ago on ATM Hacking MEGA-GUIDES PACK. (0.008470 BTC)

✓ 5/5

No feedback.

Figure 3.2: Offered services from Silkroad 3.0



reloadedudjtjvxr.onion/boards.php?id=Digital&page=2

Ships From: Worldwide Ships To: Worldwide

Escrow *ALMOST FREE BE SECURE* - The Ultimate P...
$0.05 USD / 0.000146 BTC
Vendor: Mrgoodstuff +237
Category: Digital
Ships From: Torland Ships To: Worldwide

Escrow Valid Full info Name+DOB+SSN+ADD+MMN
$2 USD / 0.005868 BTC
Vendor: probitexchange +296
Category: Digital
Ships From: Tor Ships To: Worldwide

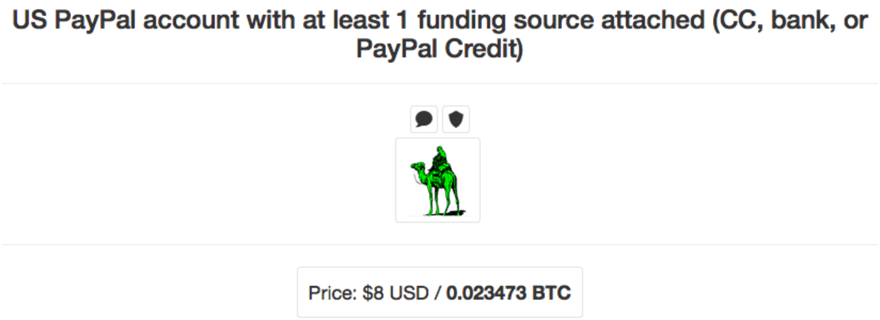
Escrow HOW TO MAKE AN ATM SKIMMER
$0.50 USD / 0.001467 BTC
Vendor: PaperAgent +419 verified
Category: Digital
Ships From: Worldwide Ships To: Worldwide

Escrow How to Hack a Credit Card
$1 USD / 0.002934 BTC
Vendor: etimbuk +2737 verified
Category: Digital
Ships From: me Ships To: Worldwide

Escrow *SALE* Vtori's 100% Clean Paypal Transfe...
$1.00 USD / 0.002934 BTC
Vendor: Mrgoodstuff +237
Category: Digital
Ships From: Torland Ships To: Worldwide

Figure 3.3: Reviewsystem similar to Amazon

Figure 3.4 the price of a PayPal account with at least one funding source like a bank account or a credit card costs about 8$. Valid credit card numbers range from 1$ to 5$.



US PayPal account with at least 1 funding source attached (CC, bank, or PayPal Credit)

Price: $8 USD / **0.023473 BTC**

Figure 3.4: The price of one valid PayPal Account

3.3 Cyber Spies

Cyber spies as the last threatening group needs to be classified in two different groups. They are working in an industrial environment to obtain data about products, machinery, not patented methods or other critical information about a company. A recent example for those kind of spies comes from the U.S.A. where six Chinese stole information from the companies Avago Technologies and Skyworks Solutions Inc. relating to how to filter out unwanted signals in wireless devices(Technologies, 2015). The other group are spies, who are working for governments or agencies like the NSA, BND, MI6. They employ professional hackers or using software build by them to spy on other governments. "The Hacking Team" from Italy used a zero-day-exploit from the plug-in Flash to build a spying tool for agencies all around the world. The software gave the agents the ability to practically read and record everything a user does on his computer.

3.4 The Methods of threatening groups

As seen above, the groups are interested in different kind of data and files. Different aims need different methods to obtain sensitive data. Some attacks just require packet sniffing, where the attackers listen to the outgoing packets of a victim. Others need a trojan which observes and saves all the keyboard commands of a victim.

Hacktivist groups are using attack models to disturb their victims like previous mentioned DoS attacks or hacking into their social media accounts in order to make them unuseable, e.g. in the case of the anti ISIS attacks from Anynomous. Furthermore they do not have financial interests. They say they want to be the modern vigilantes in order to help the people and protect the freedom of the internet.

Hacker associations like Lizard Squad are more interested in fame and proving no system is secure point. They are announcing their attacks in order to generate as much attention as possible. Financial gain is not their interest either but they are not trying to help people as well. They do it to proof, information and cyber security of companies like Sony and Microsoft is too fragile for modern standarts. Their methods of choice are hacking into certain systems, disturbing web services and stealing data like unreleased movies e.g. in the event of the sony hack in November 2014 by the group "Guardians of Peace", who claimed responsibility.

Cyber criminals are mostly targeting private users in order to install unwanted software on their personal computers. These backdoor programms allow this group to collect sensitive data like credit card number plus security number. They use large scale attacks in order infect as many users as possible to collect valid data for mostly financial purposes. Credit card fraud and money laundering are still are still most common cyber crimes commited these days according to to the federal bureau of investigation cyber crimes most wanted list. [12].

Cyber spies are a very complex category of attackers. Some attackers who violate the information security status from the inside are called whistleblowers. They are stealing sensitive and confidential information in order to make it publicly available. They are performing these thefts to serve a higher purpose, to educate the people and to inform the public. One of the most well known cyber spies is Edward Snowden. He gave up a very comfortable life to live on in embassies of states who are not poli

Industrial and military spies on the other hand are stealing data ether for money or for military advantages. Their thefts will mostly never be revealed.

The information indicates different methods are used by these groups to achieve their individual goals. Once you set the profile of potential attackers against your cyber environment, you are able to develop specific defense strategies. That makes it much more difficult to execute a successful attack against your cyber environment.

3.5 Attack patterns

Understanding and knowing the specific attacks used by different groups is a key discipline of Cyber Threat Intelligence. Each of the formerly mentioned groups has specific attack patterns to reach a certain goal. The table3.1 shows attacks, how they work and which group is typically using it. The table is based on the Office (2009) paper and a collection of whitepapers published by the company blue coat. [15] There are several reasons behind vulnerabilites. It is not always

[12] https://www.fbi.gov/wanted/cyber

Attack	*Description*	*Corresponding group*
Denial-of-Service (DoS)	An attack designed to make a system, network or cyber environment unavailable for its legit users. This can be done by sending more requests to a server than it is able to handle or blocking the in and output peripheral devices (keyboard or mouse). The only aim of this attack is to make sure, users are not able to connect to the attacked objectives.	Hacktivists and Terrorists
Distributed Denial-of-Service (dDoS)	A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.	Botnet operators and Hacktivists
Zero-Day-Exploits	These are vulnerabilities which are discovered but not reported. A famous example was the vulnerability of the "Flash Plugin" which was exploited by the "Hacking Team" from Italy to build a spyware tool around it. They selled this software to different agencies, law enforcements and governments around the world[13]. The "Hacking Team" is not a criminal group but their case demonstrates in detail how these exploits can be used and selled.	Cyber Criminals and Cyber Spies.
Credit card fraud	In the event of paying with a credit card in a store or webshop, the data from a card should just pass trough to the corresponding bank. In 2005 more than 40 million credit card files have been compromissed. An unknown group of cyber criminals was able to steal these files by using penetration attacks to the stores and webshops[14]. The reason why the attackers were able to steal the data was because the vendors stored the data on their insecure systems for research purposes. They did not attack the credit card companies because of their highly secured cyber environment. The reason the attacker was able to commit an attack like this was simply because of the not compliant status of the vendors.	Cyber criminals

Table 3.1: Attack patterns and their corresponding groups

software or hardware. Human interaction is still one of most critical vulnerabilites in cyber environments worldwide. In the event of the credit card data theft several humans decided to keep these very sensitive data for research purposes rather than sticking to the guideline of just transferring the data to the corresponding bank. An outbalanced security system between humans and machines is the key to a safe cyber environment.
To point out the importance of balance, the next section gives some examples on how to deal with certain insecurities and how someone is able to protect against them.

3.6 Profiling threatening groups and corresponding defense technics

As seen in the table 3.1 from the section “Attack patterns”, there are vulnerabilites based on software, hardware and human behaviour. Each of this vulnerabilities has a corresponding defense technic to secure the cyber environment.

In case of Denial-of-Service attack, the service which is not responding and the attackers method to shut down the specific service need to be identified. A Denial-of-Service attack is not limited to an overload of network requests e.g. in the “lizard squad” attack. If an attacker is able to shut down the authentication service, no user is able to log in into their accounts which results in a Denial-of-Service state as well. This kind of attack has a broad spectrum, of how it can be performed. It is especially dangerous because the attack does not need any kind of authentication to perform this attack. Effectiv ways of preventing attacks like this kind are blacklists who block certain IP-adresses which are sending an irregular amount of requests. Software vulnerabilities which are exploited are preventable if the cyber environment is tested by authorized penetration testers to identify vulnerabilites before an attacker is able to exploit them.
Spyware attacks aim at sensitive data which is worth stealing. Credit card, cashflow, employee and product data files are valuable for different reasons. Certain agencies like the NSA[16] is interested to gather as much information about people and companies as possible. They need this information to identify possible threats and surveilleance of other nations. They use Zero-Day-Exploits to implement spyware tools on target systems to collect these kind of information . Cyber criminals use the same method by infecting but more for monetery

[15] For more information about different attacks I recommend the following page https://en.wikipedia.org/wiki/List_of_cyber-attacks

[16] Natinal Security Agency

reasouns like credit card fraud for example. Victims of such attacks can not tell if they are infected with spyware because its signature has not been registred in the databases of security software vendors. There is still a possibility to identify such attacks. If the spyware software found interesting data, which is worth stealing, it has to transfer these files to the attacker somehow. If an uncommon connection is detected by a firewall like “Sygate”, it shows you the application which is trying to connect to a certain IP-adress which is not autheticated by the user. Even if you are not able to defend against the unwilling installation of spyware, you are maybe still able to prohibit the leakage of sensitive information.

Threating groups are targetting corresponding victim groups. In case of our example from “Lizard Squad”, they are targetting companies, to show the lack of security of their cyber environments. The credit card data theft from 2005 aimed at insecure vendor systems, which stored credit card for research purposes. If companies and end-user would look up former attacks against their category of victim and compare their system with the victims systems, they should be able eliminate certain threats for their systems. There is a service available which already analyzes these incidents and gives advice to the same group of victims. This company is called “Blue Coat” and not only secures a system from already happened attacks but also tries to eliminate as much threatening factors as possible. Email attachments are an excellent example of how malicious files can be transferred to a victims cyber environment. Their security checks every email for malicious files but not only with regular software but detection software specialized in finding malware code.[17] To see how much information you are able to retrieve from an attack, the next chapter will analyze an example attack and show how to use the individual information.

[17] BlueCoatSystemsInc (2013a)BlueCoatSystemsInc (2013c)BlueCoatSystemsInc (2013c)BlueCoatSystemsInc (2013b)BlueCoatSystemsInc (2013d)BlueCoatSystemsInc (2013e)

4 Improvement of Cyber Security through the use of Cyber Threat Intelligence

This chapter analyzes the current state and its potential weak points. We build a model to visualize how the process of developing a threat is performed by an attacker. Figure 4.1 shows the basic model for visualizing the extraction of information.

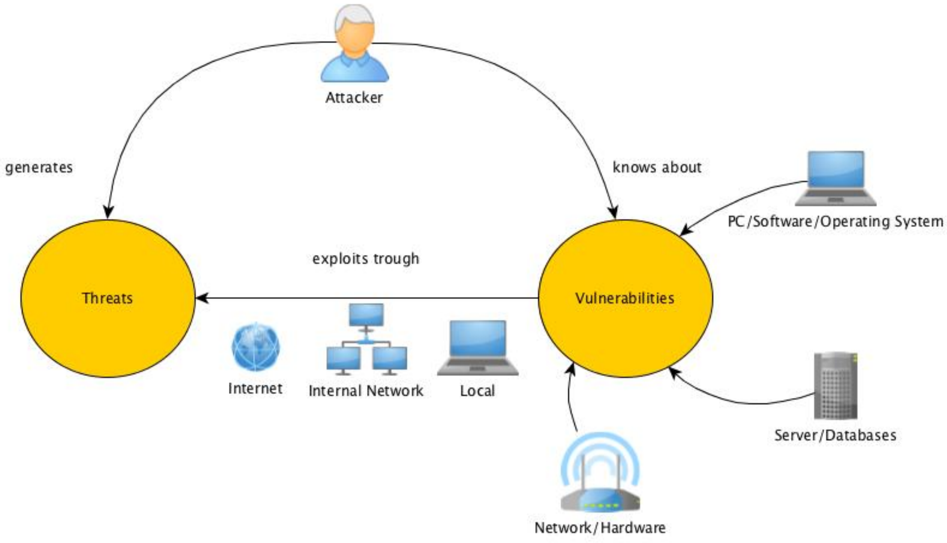


Figure 4.1: Developing a threat

To dig in further we had to split this basic model in 3 phases to show the benefits from every step. A botnet-attack was chosen as an example.[1]

The following table 4.1 provides sources to topics like malicous websites or attacker ip adresses for example. These information can be used for Cyber Threat Intelligence in order to act preventious, for example by blocking all the commonly known attacker ip adresses. Huber (2015)

[1] Baier (2010)

Name of the ressource	*Description of the information*
DNS-BH Malware Domain Blocklist	Shows domains which are known for deploying malicous software without the user knowing
MalwareURL	Malicous websites (Phishing, Drive-by-Downloads and Command and Control Server)
DShield	Firewall logs for attacker IPs
Google Safe Browsing Alerts	Malicous websites
HoneySpider Network	Malicous websites
FIRE (FInding Rouge nEtworks)	Malicous websites
Team Cymru	Malicous websites
EXPOSURE	Malicous websites
Abuse.ch	Adresses of Botnets
Shadowserver Foundation	Information about Botnets, malicious and compromised websites
Darkreadings.net	Information regarding all kinds of Cyber Security topics

Table 4.1: Sources for CTI information

4.1 Phase one “Development”

After an attacker obtained critical information about a vulnerability of a system, an application or hardware, he has to build an exploit around it. In case of our made up botnet-attack, we assume the attacker learnt about a windows operating system vulnerability. He assumes he is able to plant a trojan on the system which automaticlly downloads more parts of a program without the user knowing, to remotely control the system for his own intentions. To reach his goal of controlling as many systems as possible, he needs to programm a trojan which automaticlly downloads more parts to fully takeover the system. The exact steps of what to do next are not relevant for this thesis, so if you are interested in the topic of writing malicous code, you will find ressources regarding it in the last chapter. 4.2 shows the the simplified development of a working trojan. The important question is now what kind of information is obtainable and how to use it against the attacker. In this phase, acquiring information is no easy task at all. Black hats, who are working on a professional level are not likely to share their information publicly.

A possible option to gain information about new vulnerabilites which are not publicly known are “moles”. These “moles” are hackers who were caught by the law enforcement. They agreed to a deal, to work with cyber defense organization in order to not spend time in jail.

Instead of going to jail, they work together with the law against their former colleagues e.g in

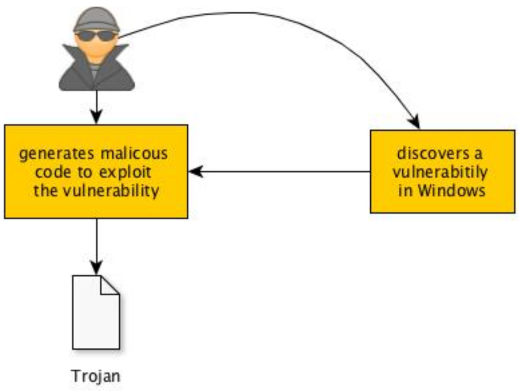

generates malicous code to exploit the vulnerability
discovers a vulnerabitily in Windows
Trojan

Figure 4.2: Visualization of the first phase

the case of the teenage hacker from lizard squad.[2] He did not spend one day in jail but has to work with cyber defense organization to make up for his commited crimes. The court made him work together with a cyber defense department to actually gather as much information as possible of new threats. In conclusion to collect information from this early stage of an attack, you either need a mole inside the inner circle of a "black hat" circle or a "white hat" discovers the same vulnerability on its own.

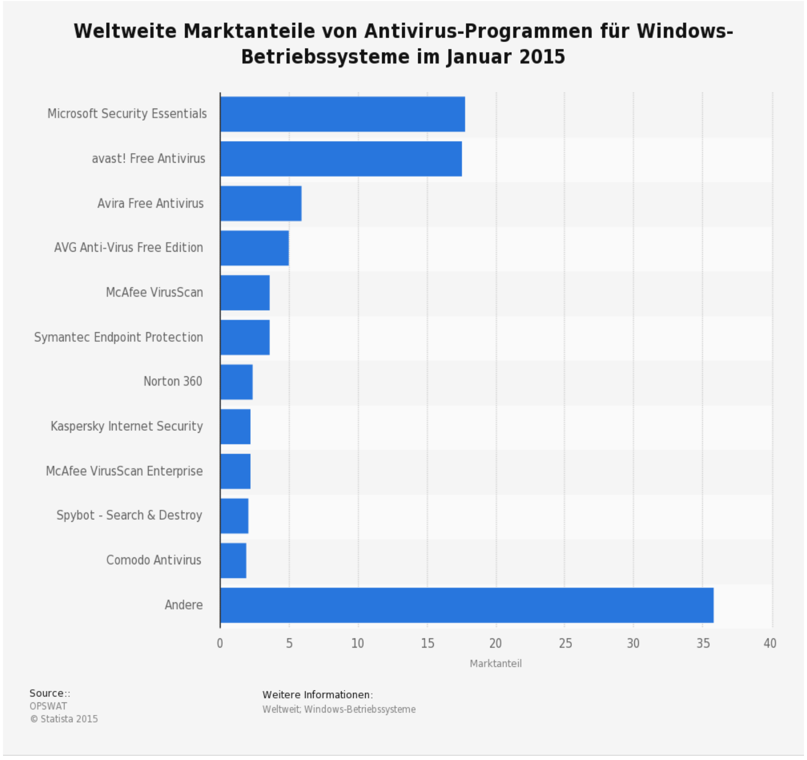
One example for a team of white hat hackers would be Google security team since they are continouisly searching for new vulnerabilities even outside their own products. If they find a vulnerability in another system they alarm the manufacturer and give them 30 days to fix it otherwise it will be published in form of a security report[3]. In addition to it, bounties will be given to a third party white hat, to honor their efforts for a secure environment. In the next section we will look on the attacker and how he spreads the trojan from our example.

4.2 Phase two "Deployment"

In this phase the attacker needs to spread its malicous code to as many systems as possible without getting detected. With nowadays security programms sometimes preinstalled on many systems, it should not be that easy of a task. Reality shows another picture in this case. Antivirus programms need specific signatures of malicous software to identify them on their system. A new trojan for example which has never been used before can not be recongnized by such software. In addition to anti virus software you would need a firewall for example

[2] Tassi (2015)
[3] https://googleonlinesecurity.blogspot.com/

which is overwatching your outgoing traffic or Anti Maleware software which is specialized in finding trojans, rootkits and all other sorts of very malicous software that could infect your system.
The real problem is not the availibility of such security-software rather than user behaviour. The majority of people seems to be not interested in building up their cyber defense. If you look at statistics shown in figure 4.6 you will notice the majority relies on free products shipped with their operating system or so called freemium software which gives the basics for free but to unlock all features you need to pay for it. [4]



Source::
OPSWAT
© Statista 2015

Weitere Informationen:
Weltweit; Windows-Betriebssysteme

Figure 4.3: Market share of Security Software worldwide

But the behaviour of people changes probably due to recent events like the Edward Snowden whistleblower case, more media attention to groups like “Anonymous”, “lizard squad” and “the hacker team”. Statistics shown in figure 4.4

[4] http://de.statista.com/statistik/daten/studie/169913/umfrage/marktanteile-antivirus-programme-bei-windows/

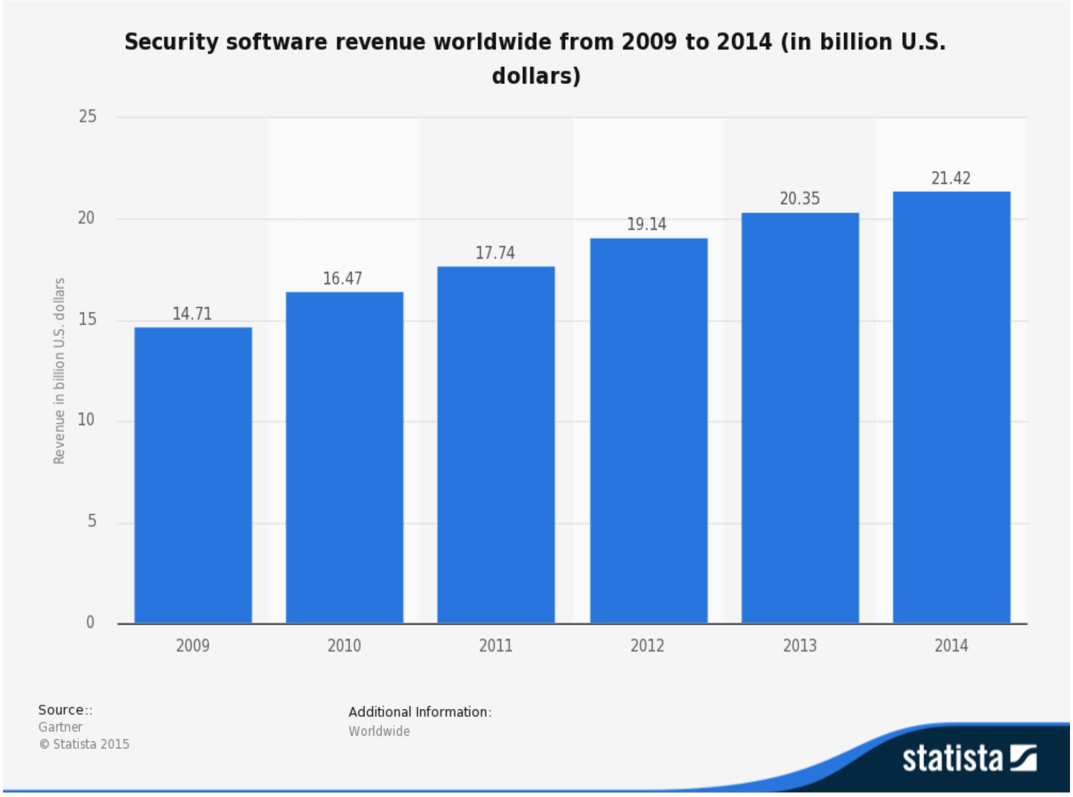


Figure 4.4: Revenue worldwide of Security companies

[5] What information are we able to retrieve from the increasing revenue of security companies worldwide? People are eager to spend money for their security. On the other side it means for attackers it is getting more complicated to infect or hack computers due to improved security.

[5] http://de.statista.com/statistik/daten/studie/189765/umfrage/weltweiter-umsatz-mit-security-software-seit-2009/

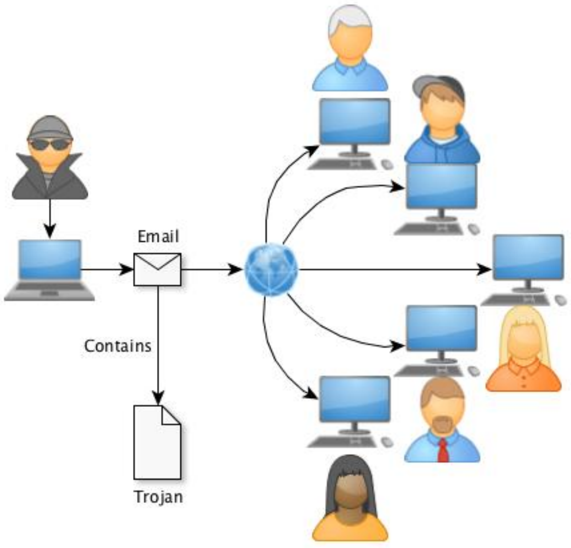


Figure 4.5: Visualization of the second phase

Figure 4.5 shows the attacker from our example and his attempt to deploy his trojan onto as many systems as possible using emails and mailing lists. Furthermore he uses the adress book of his victims to automatically send the malicous email to all other contacts in their adress book. As before we will not further explain how the technical details of this attack work. If you are interested in this topic reference literature will be given in the last chapter.
The information we are able to retrieve from this phase are as shown in table below.

The next section will show what kind of actions the attacker is now able to perform if the deployment succeeds.

Method of Deployment	The attacker could use a single source of deployment like emails or he could hide the malicous apllication in another one which is legitimized. If you know how this application is spreaded you are able to block for example certain email adresses or IPs to prevent further spreading. Other ressources can be found on table **??**of this chapter to block certain websites, IPs and application which are known to be hazardous.
How the trojan works	Its method of self installing through downloading several other parts to complete itself autonomously has the same pote. Not only you could profit from the sharing of information, which is the key to Cyber Threat Intelligence, it is what the society could really benefit from.
How does the remote controll functionality works?	To gethe location of the command & controll server is very useful, what kind of commands is he able to perform without the user knowing or does he use a proxy server to hide its traces? These information could be used for the law enforcement to mark the attackers location and track him down. In the event of arresting him, further threats generated by him are more unlikely to happen

Table 4.2: Example information that can be gathered during the deployment phase

4.3 Phase three “Exploitation”

The last phase of an attack is its exploitation. In the event of a fully performed attack, the attacker in the scenario now has full controll of more than 50.000 PCs. He is now in the position to perform a variety of attacks. Based on his intentions, which leads us back to threatening groups and their different motivations to perform certain kind of attacks. With a Bot-Net as big as this one, he could perform a distributed Denial-of-Service attack for example. In our real example of the “lizard squad” attack on “PSN” and “Xbox live” (See page) this kind of attack is the one what was likely to be performed applied.
Figure 4.6 shows how an attacker sends commands to a command & controll server which afterwards sends this command to every single controlled system. He orders his “zombie-army” to send continous requests to the PSN-Server. This puts the server in a state where he is not able to handle requests any more. This results for example in the http-statuscode 503 “Service unavailable”. In case of our “lizard squad” attack this status remained for nearly a week. To use such an “army” for a dDoS attack is mostly performed by groups like lizard squad. They wanted to show how much the cyber security lacks. The big difference between lizard squad and black hat hackers is the monetary benefit.

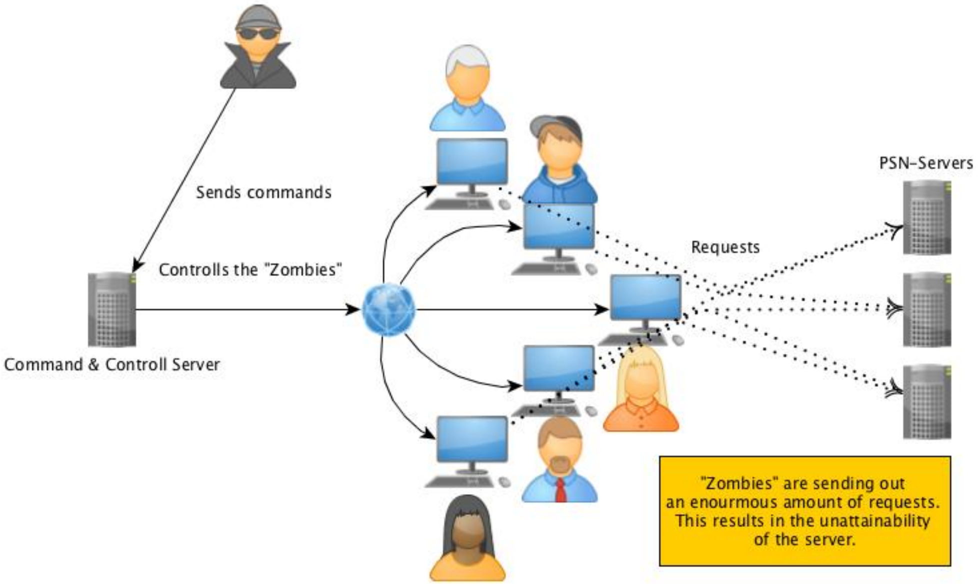

Sends commands
Controlls the "Zombies"
Command & Controll Server
Requests
PSN-Servers
"Zombies" are sending out an enourmous amount of requests. This results in the unattainability of the server.

Figure 4.6: Visualization of the third phase

In figure 4.7the bot-net is used to farm bitcoins [6]. The attacker uses the “zombies” in order to perform pool-mining without the users knowing, their ressources are used to mine new bitcoins. In generell it is a legal method to farm as a collaboration, but only with the permission of the user. In this made up case more than 50.000 PCs are used for the benefit of the attacker. Attackers who perform a pool-mining are only using a small percentage of the total ressources which are available in order to stay hidden as long as possible.

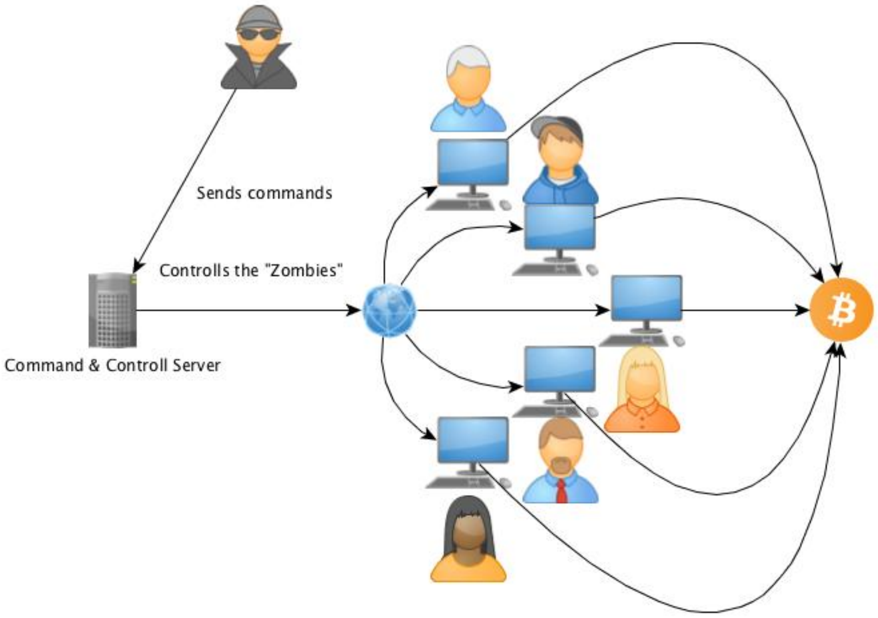


Figure 4.7: bitcoin farming

[6] for more information follow this link https://bitcoin.org/en/developer-guide

What kind of Server was attacked?	Are there similiar services like the server being attacked right now? In our case Xbox live and Steam are also possible victims of this attack. They are able to put an Anti-dDoS-Server before their own in order to protect them from such attacks. [7]
IP adresses of the “zombies”	These can be used to block them in order to prevent further requests from them.
How much damage did this attack cause	We could be able to prioritize certain kind of attacks and would help others to do the same. But how do we measure the financial damage caused by a dDoS attack on a webservice like PSN? The next section tries to give an answer to this question.

Table 4.3: Examples for information that can be extracted from the Exploitation phase

Some information, we are able to retrieve, based on our example case for a dDoS attack are listed in the table 4.3 below.

4.4 Formulas for estimating costs of cyber attacks

The idea to measure the financial damage caused by a Denial-of-Service-attack came with the analysis of use-cases which are used by big companies. They are able to react in a proper way against those attacks but they can not measure the financial damage caused by them.
In order to be able to calculate the damage, you need to consider different variables for measuring profit and sales force for a web shop or web services.

4.4.1 The formula for a Denial-of-Service-Attack on a webservice

The following variables are going to be used for the formula to estimate the costs of a Denial-of-Service attack.

- *Downtime per hour = Dt [t]*
  How long has the server been unreachable for our costumers. This is the basic component to measure the whole damage which was caused. Also indicates what kind of long term damage to expect from the outage.

- *Sales per hour [$]= S*
  How much sales were generated per hour in the last fiscal year? This is important to get a general idea on how much sales were missed during the outage time.

- *Growth of Sales rate[percentage] = Gr*
  Percentage rate of the increased rate of sales during the current fiscal year. How much did our sales increase or decrease this fiscal year? This variable is needed to get a more defined worth of sales based on the average sales from the past year.

- *Seasonal sale = Ss*
  Seasonal up or down in sales in generell measured by the last years statistical average. To be unreachable during christmas for example can be disastrous for an online store like amazon. The decrease or increase in the sales for different seasons helps to define the worth even more.

- *Lost costumers [c] = LT*
  Clicks per hour lost due to the attack. If the regular online store of a costumer is not reachable they change to a competitor in one easy search. The number of the costumers have to be counted to get an idea of much we have to reinvest to receive back the trust of our costumer.

- *Costumer acquisition cost [$] = Cac*
  How much money do I have to invest to get a paying costumer on my website? These investment costs are essential to measure our one time invest to get back on our regular traffic before we were attacked.

All these components lead to the following formula to determine the financial damage caused by a Denial-of-Service-Attack.

$$(((Dt * S) * Gr) * Ss) + (Dt * Lc) * Cac \tag{4.1}$$

In order to put this formula to practical use, we now use our example from the attack of Lizard Squad against the PSN in the next subsection.

Company: Sony Service: PSN	Downtime	170 hours
	Growth of Sales	0%
	Sales per hour	50000 $
	Seasonal Sale	125%
	Lost costumers per hour	200
	Costumer Acquisition Cost	10 $

Table 4.4: Example to calculate a dDoS-attack

4.4.2 Practical example to determine the costs of Denial-of-Service-Attack

The numbers in table 4.4 are fictional, but based on statistics from statista and their annual revenue report
We assume Lizard Squad successfully blocked the PSN services for about a week with their dDoS-attack. Sony earns with its games and services about 4.7 billion dollars annual [8]. We break down this number to their earnings per hour and get around 50.000$. The sales per costumer is by the time of July 2015 is at around 185$ annual, assuming all 25.3 million sold PS4 [9]are buying games for their console. The attack of lizard started around christmas where the sales are going up by approximatelly 25%. The number of sold consoles in 2014 was around 2.3 million pieces and we take the assumption that 70% of these people also buying playstation plus or a game online. This results in around 200 new costumers per hour. To get a new paying costumer a certain amount of money to bind a costumer to their services, we assume 10 $.

$$(((170 * 50.000) * 1) * 1,25) + (170 * 200) * 10\$ \tag{4.2}$$

Damaged caused by dDoS attack: 10.950.000$

Assuming our formula works correct and the numbers are realistic SONY lost nearly 11 million $ in just 7 days. But these are just the costs for the attack period. Long term damage need to be evaluated as well. How many costumers did we lose, how did the reputation of the company suffer, how can we make sure, an attack like this never happens again?
These questions are not ours to answer right now, because it would take a lot more than just one bachelor thesis. Research topics based on this work can be found in the next chapter.

[8] http://de.statista.com/statistik/daten/studie/318279/umfrage/umsatz-von-sony-mit-gaming-software-und-services/

[9] Quartalsbericht von 07.2015 SONY

5 Conclusion and Outlook

Cyber Security is important more than ever in our technology advanced society and to reach the next step of a worldwide equally secure cyber environment, we need to work together as a society rather than working alone. This last chapter summarizes the information obtained and gives an outlook for further research.

5.1 Summary

At first we tried to define the term Cyber Threat Intelligence for ourselfes and the reader to get an idea of what lies behind the term. In order to do that we also had to explain what certain other terms are involved like information or Cyber Security. Furthermore the term of threat needed to be defined for this work because not every threat which could occur is interesting for CTI.

Next on we were looking at different groups which were attacking for different causes. Hackergroups are motivated by different causes. Hacktivists are targeting companies and people who are, in their perspective, bad people and need to be punished. They are modern vigilantes, who try to make a difference through hacking. Cyber criminals on the other hand, are hacking companies, organizations or people for their personal benefit. They try to obtain sensitive information like credit card numbers, production plans or account data. If a company or a person comes in touch with those kind of information, they are endangered for being hacked. Analyzing your enemies, helps you finding the right defense and attack tactics to protect yourself. That is why it is important, to know different threatening groups.

We are taking advantage of all the information obtained previously to sketch a model. We constructed an attack, which happened mostly like the “lizard squad” example and analyzed it, step by step, in order to understand how much information we could obtain and how to use it against the attacker. Our made up attack was split up in three different phases:

- Development
- Deployment
- Exploitation

Each individual phase has its own information which can be gathered. If we use this information, then potential victims are able to use several options for countermeasurments before an attack occures. At last, an example of how to measure the short term damage caused by a dDoS-attack using the formula developed for this thesis was shown. Using financial arguments is the key to persuade most of the management board to invest into cyber security.

5.2 Further work

The next step to further develop the idea of measuring certain kinds of attacks would be to cooperate with companies in order to get real numbers and to prove the formula. Furthermore it is of a certain interest to develop more formulas similiar to the one developed in this thesis. Cryptolock attacks, where hard drives are getting encrypted and therefore made unaccessible for the user, are getting more popular by the day. The attacker is taking your personal files in a hostage situation and to reaccess them, you need to pay a certain amount of money for it. Interesting numbers for Cyber Threat Intelligence would be the rate of a succesful retrival of information and the average price of the decryption key.
Threatening groups need a profiling analysis in order to give companies a more detailed view on their potential attackers. These profiling information can be further used for developing specialized cyber defense systems. Governments who store very sensitive material in their database should permit the use of unchecked USB storage devices for example. According to the german newspaper “Die Zeit” a trojan could infiltrate the Bundestag database trough a USB stick from an employee of the chancelor office[1]. If the threatening group cyber spies are in the position to deposit malicous applications by simply connecting a storage device to a government secured system, there are definitly deficits in their understanding of a secure cyber environment.

[1] http://www.zeit.de/digital/datenschutz/2015-06/bundestag-hacker-trojaner-angriff

Cyber criminals with the intention of monetary goals are getting smarter with their use of insecure private systems. They are constantly testing their own developed spyware in their own environment to make sure their malicous programms are not discovered by the most popular security suits for private users. These users need proper education to know what kind of threats they are facing and that regular security is not enough to protect them properly.

What is missing, is an easy to implement Cyber Threat Intelligence software, which is capable of distributing as well as receiving information about an individual system. This future system could use the already developed STIX format to gather information about existing vulnerabilities, threats and exploits to give their users an overview about potential threats on their individual system. An automaticlly updated blacklist for malicous websites could be displayed and implemented into the users browser by using already existing information like the ones provided in chapter four 4.1. Such a software would be out of scale for a bachelor thesis but would be very suiting as Ph.D. research topic.

Developing guidelines for the most common attacks like network overload based Denial-of-Service attacks or spyware attacks to steal sensitive data is a logical next step. Users who do not have the technical background to understand these kind of attacks, do need help in form of a guideline to keep their businesses or private cyber environments running and secure.

5.3 Conclusion

CTI could be beneficial to every single computer user worldwide. Weather it is a company cyber work environment or a private user. The challenge of Cyber Threat Intelligence though is to convince every single user of sharing their experience with incidents and vulnerabilites in order to build a safe cyber environment. Blue chip companies [2] are not willing to share their experience because they could be used against them. Competitive thinking when it comes to security will not be of any help when the goal is security. Cyber Threat Intelligence is able to change the security industry on a level never seen before but only with the help of everyone participating in it.

I see a lot of oppurtunities by using financial arguments to the management board in order to establish a Cyber Threat Intelligence participation. This is because the people who are responsible for financial decisions are mostly not the ones who know the technical details from their own company cyber environment. Financial arguments are hard to fight especially in the case of the formula I developed. A protection against dDoS attacks for consumer grade servers is around 5$ a month. Compared to the damage the attack of 2014 caused against Sony

[2] A nationally recognized, well-established and financially sound company.

alone of nearly 11.000.000$ is a fact that stands for itself. Would they have been listening to the information that have been released on twitter from lizard squad before the attack, the instant damage and the loss of trust from their costumers would have minimized or even extinguished.
My analyzes regarding the threatening groups need to be more defined. After reading several articles about the categorisation of attackers, I realized, their motivation often changes from group to group. This part needs a more refined analysis concerning topics like history, development and structure of these groups.
The section “Attack Patterns” could probably fill a whole book. The technical details behind attacks like dDoS or spyware could use a makeover to make them more understandable for people, who are lacking the technical background to understand complex attacks like multi-stage malware attacks. In my humble opinion, the more people understand, how these attacks works, the better are the chances of detecting these kind of attacks.
In generell this thesis should be further worked on by myself to refine its content. The more information and new developments regarding Cyber Threat Intelligence are packed in a scientific work, the more likely is the idea of sharing it. The scientific writing part could probably improved as well to get acknowledgement from different scientific instiute, but my intention was always to write a paper, which is understandle by a broad audience and not by little circle of chosen researchers.
I think, I managed to show how a theoretical concept like Cyber Threat Intelligence is able to make a difference within our society and how it is able to safe money for companies if they work together.
In a nutshell Cyber Threat Intelligence works but only if everyone involved is sharing their information. Companies who are afraid of losing certain positions on the market need to rethink their point of view. If different enterprises work together against common enemies, it will be much harder for threatening groups to find vulnerabilites inside their systems.

Bibliography

[Bad 2015] Bad, Breaking: like Amazon run by cartels. In: *The Guardian* (2015)

[Baier 2010] Baier, Daniel: Botnetze -Funktion, Erkennung und Entfernung von Botnetzen / Hochschule Bonn-Rhein-Sieg. 2010. – Forschungsbericht. – 35 S

[Ball u. a. 2015] Ball, James ; Arthurand, Charles ; Gabbatt, Adam: FBI claims largest Bitcoin seizure after arrest of alleged Silk Road founder. In: *The Guardian* (2015)

[Blockupy-proteste 2015] Blockupy-proteste, Die: Wackersdorf - Heiligendamm - Frankfurt. In: *Frankfurter Allgmeine Zeitung* (2015)

[BlueCoatSystemsInc 2013a] BlueCoatSystemsInc: 5 STEPS FOR STRONGER ADVANCED THREAT PROTECTION HOW TO DEEPEN YOUR DEFENSES AGAINST EXPLORING OPPORTUNITIES TO CLOSE GAPS / Blue Coat. 2013. – Forschungsbericht

[BlueCoatSystemsInc 2013b] BlueCoatSystemsInc: BEST PRACTICES FOR ADVANCED THREAT PROTECTION Advanced Threat Protection Part 3 / Blue Coat. 2013. – Forschungsbericht

[BlueCoatSystemsInc 2013c] BlueCoatSystemsInc: EXPLORING ADVANCED THREATS Advanced Threat Protection Essentials Part 1 / Blue Coat. 2013. – Forschungsbericht. – 1–8 S

[BlueCoatSystemsInc 2013d] BlueCoatSystemsInc: Next Generation Security Analytics : Real World Use Cases Key Features and New Uses for the / Blue Coat. 2013. – Forschungsbericht

[BlueCoatSystemsInc 2013e] BlueCoatSystemsInc: SECURITY ANALYTICS REAL-TIME PROTECTION / Blue Coat. 2013. – Forschungsbericht

[cert.us cert.gov 2014] cert.gov, Ics cert.us: Cyber Threat Source Descriptions. In: *US-CERT* (2014), S. 10–12. – URL https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions

[Chang 2002] Chang, Rocky K.: Defending against flooding-based distributed denial-of-service attacks: a tutorial. In: *Communications Magazine, IEEE* 40 (2002), Nr. 10, S. 42–51

[Chismon und Ruks 2015] Chismon, David ; Ruks, Martyn: Threat Intelligence: Collecting, Analysing, Evaluating. In: *NIST* (2015)

[Choo 2011] Choo, Kim-Kwang R.: The cyber threat landscape: Challenges and future research directions. In: *Computers & Security* 30 (2011), Nr. 8, S. 719–731. – URL http://dblp.uni-trier.de/db/journals/compsec/compsec30.html#Choo11

[Cosh 2015] Cosh, David G.: Online group declares war on Scientology. In: *National Post* (2015)

[Demott u. a. 2011] Demott, Jared D. ; Sotirov, Alexander ; Long, Johnny: *Gray Hat Hacking , Third Edition Reviews.* McGraw HI, 2011. – 721 S. – URL http://books.google.com/books?id=jMmpLwe2ezoC{&}pgis=1. – ISBN 9780071742566

[in Network Security Imperial College UK; MEng in Electrical Engineering und Greece. 2015] Electrical Engineering, George Loukas P. in Network Security Imperial College UK; MEng in ; Greece., Computer Science N.: *Cyber-Physical Attacks: A Growing Invisible Threat.* 1. Butterworth-Heinemann, 6 2015. – URL http://amazon.com/o/ASIN/0128012900/. – ISBN 9780128012901

[Grance u. a. 2004] Grance, Tim ; Grance, Tim ; Kent, Karen ; Kent, Karen ; Kim, Brian ; Kim, Brian: Computer Security Incident Handling Guide. In: *Nist Special Publication* (2004), S. 148. ISBN NIST Special Publication 800-61 Rev. 1

[Hornyak u. a. 2015] Hornyak, Tim ; Squad, Lizard ; Twitter, Lizard S. ; Squad, Lizard ; Espoo, The ; Court, District: Lizard Squad hacker draws suspended sentence for online attacks. In: *PCWorld* (2015)

[Huber 2015] Huber, Edith: *Sicherheit in Cyber-Netzwerken.* Springer, 2015. – 163 S. – ISBN 978-3-658-09057-9

[Kharpal 2015] Kharpal, Arjun: *Is China still hacking US? This cyber firm says yes.* 2015. – URL http://www.cnbc.com/2015/10/19/china-hacking-us-companies-for-secrets-despite-cyber-pact-.html

[Klipper 2015] Klipper, Sebastian: Was ist Cyber Security? In: *Springer* (2015), S. 9–27. – URL http://link.springer.com/chapter/10.1007/978-3-658-11577-7{_}2. ISBN 9783658115777

[LLC 2009] LLC, Francis G.: Glossary about short terms used in Cyber Security. In: *Whitepaper Glossary* (2009)

[Manion und Goodrum 2000] Manion, Mark ; Goodrum, Abby: Terrorism or civil disobedience: toward a hacktivist ethic. In: *ACM SIGCAS Computers and Society* 30 (2000), Nr. 2, S. 14–19

[Mcallister und Ludwick 2015] Mcallister, Jay ; Ludwick, Melissa K.: Advancing Cyber Intelligence Practices Through the SEI a s Consortium SEI Emerging Technology Center / Carnegie Mellon University. URL https://resources.sei.cmu.edu/asset{_}files/Webinar/2015{_}018{_}101{_}434583.pdf, 2015. – Forschungsbericht. – 22 S

[Microsoft 2015] Microsoft: Microsoft Advanced Threat Analytics / Microsoft. 2015. – Forschungsbericht. – 3 S

[Mimoso u. a. 2010] Mimoso, By Michael S. ; Editor, News ; Hichert, Jan: Security News :. In: *Security News* (2010), S. 1–2

[MITRE] MITRE. – URL http://stixproject.github.io/about/. – Structured Threat Information Expression (STIX™) is a structured language for describing cyber threat information so it can be shared, stored, and analyzed in a consistent manner. The STIX whitepaper describes the motivation and architecture behind STIX. At a high level the STIX language consists of 9 key constructs and the relationships between them.

[Office 2009] Office, United States Government A.: Critical infrastructure protection. In: *Report to Congressional Requesters* (2009)

[Personal u. a. 2006] Personal, Munich ; Archive, Repec ; Linck, K ; Pousttchi, Key ; Wiedemann, Dietmar G.: Security issues in mobile payment from the customer viewpoint. In: *Proceedings of the 14th European Conference on Information Systems (ECIS 2006)* (2006), Nr. 2923, S. 1–11

[Picture 2015] Picture, The B.: Eco N ˜ T ˜ on. In: *WhatIs.com* (2015), S. 1–4

[Stein 2002] Stein, Lincoln: The World Wide Web Security FAQ 8 . Securing against Denial of Service attacks. In: *W3C* (2002), S. 1–11. – URL http://www.w3.org/Security/Faq/wwwsf6.html

[Tassi 2015] Tassi, Paul: Lizard Squad Hacker Who Shut Down PSN, Xbox Live, And An Airplane Will Face No Jail Time. In:

Forbes (2015), S. 2015. – URL $\delimiter"026E30F$url{\protect\T1\textbraceleft}http://www.forbes.com/sites/insertcoin/2015/07/09/lizard-squad-hacker-who-shut-down-psn-xbox-live-and-an-airplane-will-face-no-jail-time/{\protect\T1\textbraceright}

[Technologies 2015] Technologies, Avago: U . S . Charges Six Chinese Citizens With Economic Espionage. In: *WSJ* (2015), S. 1–4. ISBN 1432046527

[Work und Shows 2015] Work, Sales ; Shows, Leak: HACKING TEAM LEAK SHOWS HOW SECRETIVE ZERO-DAY EXPLOIT SALES WORK. In: *Wired* (2015), S. 1–7

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, 20. Februar 2016 Felix Karl Franz Uelsmann