POWERFUL EFFECT OF COMPUTER FORENSIC SCIENCE

Ivan CRISTIUC

Modern Languages, TI-2110, Faculty of Computers, Informatics and Microelectronics, UTM, Chișinău, Republic of Moldova

Autorul corespondent: Puscasu Ala, e-mail: ala.puscasu@lm.utm.md

Summary. *The research was conducted on basis of open sourced information. The analysis was carried out according to the following criteria: importance, usage, real incidents, danger. I investigated complexion of the procedures and significance. I analyzed different parts of computer forensics and found out how investigations are conducted, how to work with incidents and what steps are taken.*

Keywords*: investigation, incident, security, hacker, compromise, data.*

Introduction

By the 1980, personal computers had become widespread, causing rise of criminal activity leaded by machines (frauds, cracks). Then, the discipline of cyber forensics had come as method of investigation and recovery of different digital evidences. With advancing of availability and number of devices, virtual crime has grown. The Computer Emergency Response Team (CERT) Coordination Center reported over 135,000 occurrences in 2003, a 67% boost from 2001 [1]. Image 1. That is when cyber forensics had come to fix situation with rising offensive. Computer Emergency Response Team (CERT) — department that collects information about incidents or stopped attacks, then information is summarized and distributed by the companies which cooperate with CERT. Digital forensics is the application of investigation and analysis techniques to gather and preserve proof from particular machines in a way that is suitable for presentation in a court of law. The goal of forensics is to perform structured researches and maintain a documented chain of evidence to find out exactly what happened on a machine and who was responsible [2]. Forensic techniques are used to explain the current state of hard disk or CD-ROM.

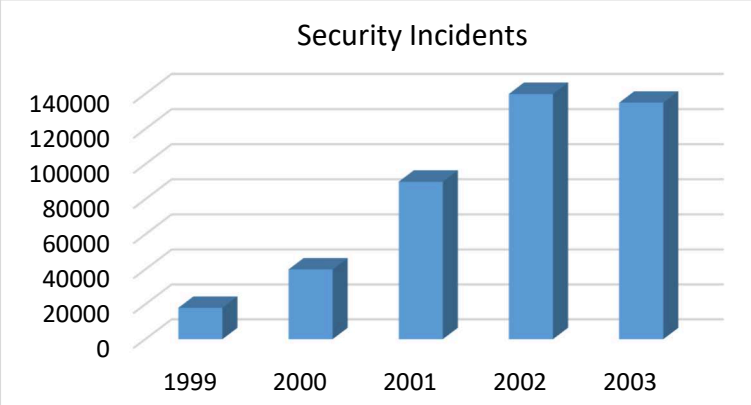

Image 1. Incidents report to CERT

Why is computer forensics important?

Nowadays, technologies surround us everywhere. Each company has hundreds of computers on which work depends future business fate. May be cases when corporation asks cyber detectives for help in protecting system, not suspecting them to be compromised by a group of hackers for years. This squad could have stolen information, money, or even they wait interesting data to appear.

Application areas of computer forensics

There are three most identified forensic fields:

1) Disclosure and investigation of criminal offences — working with data and machines as the instrument of the crime;
2) Collection and investigation of evidence — research case of infringement of intellectual property rights (trademark or domain name thieves);
3) Internal corporate investigations of security incidents — preventing information leakage, information systems protection.

How does it work inside?

The first department — investigates incidents and helps customers to respond to them. Very often, the ability to react correctly to an incident before the investigation begins helps to notice an attacker on the way to theft. At this moment, experts start thinking how to stop the criminal.For effective counteraction, it is necessary to possess the skills of Threat Intelligence, which allows to understand who is attacking, how he does it, applied tools and exact interests of offender. For example, someone may be interested in data, others in money and group of forensic specialists chooses style of behavior depending on the problem. Threat intelligence (cyber threat data) — is information about current threats and groups of cybercriminals, which allows organizations to study the goals, tactics and tools of attackers and build an effective strategy to protect against attacks. Companies can collect data on cyber threats themselves or order information from third-party suppliers [3]. Computer incident — the fact of violation or termination of the functioning of the object of the key information structure and (or) violation of the security of the information processed by the object, which occurred as a result of a computer attack [4].

Important skills for forensic specialists are:

1) Ability to work in stressful conditions

2) Understanding networks — how the network works, the routing features;

3) Understanding of all operating systems that exist (Windows, macOS, and different LINUX distributives) — to know all the subtleties, nuances and to be able to work with the systems;

4) Working of a large corporative system — working of local network, knowledge of different protocols, user authorization;

5) Understanding of modern IT technologies — everyday many of programs are being updated and to keep up with the progress it is extremely important to leap an eye on them and to test new features.

Company protection

The company that has decided to protect itself, because one way or another, everyone will encounter at least once some of the incidents can use the services of Compromise Assessment. Forensic specialists conduct a research based on information from Threat Intelligence – are there traces of any particular group of hackers, similar behaviors and actions.

After this procedure starts work, throw the stages of protecting:

1) Planning — setting a set of tasks for specialists;
2) Preparing — understanding infrastructure, closing obvious holes, installing information security tools. Also the analysis of information security, security tools, application systems, elements of technological systems should have place during the preparation;
3) Monitoring — monitoring various indicators, identifying acceptable and unacceptable incidents. The monitoring service should work with incidents in real-time mode all the time, because attackers are well aware of possible weaknesses of the system. If the threat is not eliminated in the first hour, then it may be too late. That is the reason why analytics work in 24/7 mode to prevent different incidents;
4) Incident Response — building a response plan for typical incidents (Examples: turn off the machine if the cryptographer hits; if data is compromised, then computer must be

blocked so that the thieves do not begin to move further into the internal infrastructure). After the reaction, it is important to make sure that it was the correct reaction and that the attacker had been eliminated;

5) Neutralization plan — deleting files of compromise and traces of the presence of malicious software, reconfiguration of infected machines and changing user passwords, installing the latest updates and monitoring the absence of repeated network attacks.

However, these stages will not work properly if the company is not following next steps:

1) Company must give the full access to the infrastructure for forensic specialists to provide them the opportunity of investigating all the little things of it;
2) To help quickly understand the infrastructure where the problem was noticed and to understand whether it was an incident related to computer security. For example, broken hard disk can cause difficulties with connecting to the site or sometimes impossibility of it. In this case, issue is not related to Computer Forensics Center.

All this steps they give a good, but not one hundred percent, security guarantee to customers and their database, which will not receive critical damage in case of deviation from the norm.

Final work

After preventing computer incident, a group of forensic specialists draws up a paper report that describes:

1) How attacker got into the infrastructure;
2) Recommendations for eliminating holes (technical and organizational);
3) Where hacker had been
4) What data was spotted, deleted, changed or stolen.

Real cases of using cyber forensics as evidence

Anthony Scott Levandowski, a former executive of both Uber and Google, was charged with 33 counts of trade secret theft in 2019. From 2009 to 2016, Levandowski worked in Google's self-driving car program, where he downloaded thousands of files related to the program from a password-protected corporate server. He departed from Google and created Otto, a self-driving truck company, bought by Uber in 2016. Computer forensics team conducted an investigation and found traces of stealing files. Levandowski plead guilty to one count of trade secrets theft and was sentenced to 18 months in prison and $851,499 in fines and restitution [5]

Conclusion

Computer forensics is an extremely important piece of puzzle that provides security to our progressive society. The fact is – we do not even think of that, in our minds this is something casual, which is how it should be until it reaches us. However, we should be very pleased to forensic companies for global disaster prevention. In technological era, there are plenty of data held on storage devices that can be used for evil purposes. By the help of computer forensic specialists, we cannot worry about occasions of steeling personal evidence. Their work product is not useful only in solving digital-world crimes. It is also used to solve physical-world crime — burglary, attacks, hit-and-run accidents.

References Web:

1. RYAN LEIGLAND, AXEL W. KRINGS. International Journal of Digital Evidence [online]. Available: https://bit.ly/3MasjYZ
2. Wikipedia, the free encyclopedia [online]. Available: https://bit.ly/3HEyxg2
3. Kaspersky IT Encyclopedia [online]. Aviable: https://bit.ly/3tom0bA
4. Security Vision [online]. Aviable: https://bit.ly/3pFis3F
5. Digital Guardian [online]. Aviable: https://bit.ly/3pIpbtB