MINISTERUL EDUCAŢIEI, CULTURII ŞI CERCETĂRII
Universitatea Tehnică a Moldovei
Facultatea Calculatoare Informatică şi Microelectronică
Departamentul Ingineria Software și Automatică

ELABORAREA LABORATORULUI DE ANALIZĂ A FIȘIERELOR MALIȚIOASE

ELABORATION OF MALWARE ANALYSIS LAB

Student: **Munteanu Dmitri**

Conducător: **Bulai Rodica**
lect. univ.

Chişinău, 2020

MINISTERUL EDUCAŢIEI, CULTURII ŞI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

Departamentul Ingineria Software și Automatică

Admis la susținere, Șef departament: conf. univ., dr. Ion FIODOROV

_____

"__" _____ 2020

Elaborarea laboratorului de analiză a fișierelor malițioase

Teză de master

Student: **Munteanu Dmitri**

Conducător: **Bulai Rodica**
lect. univ.

Chișinău, 2020

ADNOTARE

Prezenta teză de master a fost întocmită pe baza surselor bibliografice studiate și practicii de examinare a fișierelor malițioase de-a lungul ultimilor 5 ani în calitate de specialist și expert judiciar în domeniul mijloacelor și tehnologiilor informaționale.

Mai întâi de toate, este redată prin introducere o luare de cunoștință de cauză cu privire la situația actuală în lumea Cyber global cât și în Republica Moldova, a amenințărilor căror sunt expuși utilizatorii sistemelor informatice, entitățile economice cât și instituțiile de stat, necesității dezvoltării segmentului de examinare și analiză a produselor malițioase. Ulterior, în capitolul ”CONSIDERAȚII TEORETICE” sunt expuse definițiile/abrevierele care vor fi întâlnite în prezenta lucrare de master, precum și descrierea și reprezentarea virușilor.

În capitolul 3 este descris cum se configurează unui mediu de laborator izolat, căci este crucială înainte de a analiza programele rău intenționate și va preveni răspândirea accidentală a virusului în sistemul și rețeaua gazdă. Capitolele 4 și 5 sunt destinate descrierii modalităților și etapelor de analize a fișierelor malițioase, și anume statică și dinamică.

Sunt expuse o mare parte din surse bibliografice necesare cu tematica de analize malware, ce au servit drept sursă de inspirație la examinarea sistemelor informatice infectate și fișierelor malițioase.

Ca surse pentru întocmirea a două rapoarte de examinare, au fost selectate:

- un sistem informatic (bloc de sistem) infectat la începutul anului 2015 cu un malware de tip *ransomware* denumit ”Zeus”;
- două dispozitive de stocare a informației de tip optic cu un fișier de tip Excel malițios și copii de rezervă a două site-uri WEB compromise, ce constituie dintr-o campanie de atac cibernetic de tip ”Phishing Email”.

ADNOTATION

This master's thesis was prepared based on the bibliographic sources studied and the practice of examining malicious files over the past 5 years as a specialist and forensic expert in the field of information technologies.

First of all, it introduces an awareness of the current situation in the global cyber world and in the Republic of Moldova, the threats to which users of information systems, economic entities and state institutions are exposed, the need to develop the segment in examination and analysis of malicious products. Subsequently, in the chapter "THEORETICAL CONSIDERATIONS" are presented definitions/abbreviations that will be encountered in this master's thesis, as well as the description and representation of viruses.

Chapter 3 describes how to configure an isolated laboratory environment, as it is crucial before analyzing malicious programs and will prevent the accidental spread of the virus to the host system and network. Chapters 4 and 5 are intended to describe the ways and stages of analysis of malicious files, namely static and dynamic.

A large part of the necessary bibliographic sources on the subject of malware analysis are exposed, which served as a source of inspiration when examining infected computer systems and malicious files.

As sources for the preparation of two analysis reports, the following were selected:

- a computer system infected in early of 2015 with a ransomware malware called "Zeus";
- two optical storage devices with a malicious Excel file and backup copies of two compromised WEB sites, consisting of a "Phishing Email" cyber attack campaign.

CUPRINS

INTRODUCERE

În zilele noastre, tehnologiile informaționale se dezvoltă foarte rapid, ce vin în primul rând în folosul societății, facilitând și îmbunătățind viața de zi cu zi a omului în activitățile de comunicare, lucru, divertisment și multor altor necesități. Bunăoară, în lumea cyber concomitent s-a creat și cealaltă latură cu obiective rău intenționate, bazându-se pe neglijența utilizatorului și vulnerabilităților existente în mediile sistemelor informatice. În ultimii ani, peisajul *Malware* a evoluat dramatic, de la botneturi IRC până la amenințări persistente avansate (APT) și viruși sponsorizate de stat care vizează activiști, fură planuri și documente altor companii precum și state, sau chiar atacă centrale electrice, reactoare nucleare și alte entități critice de furnizare a resurselor necesare societății.

Paralel, mai evidențiat s-a dezvoltat și criminalitatea informatică, care a evoluat pentru a deveni o afacere de milioane de dolari, de la furturi de date de carduri bancare până la deturnarea rețelei bancare SWIFT, de la spam-uri până la blocarea sistemului informatic.

Practic orice limbaj de programare poate fi folosit pentru a scrie o bucată de cod care va fi folosit ulterior în scopuri rău intenționate. Deoarece Windows este încă cel mai utilizabil și răspândit sistem de operare predominant în lume, nu este de mirare că marea majoritate a fișierelor malițioase sunt create pentru acesta. Evident că au fost creați și viruși predestinate pentru celelalte sisteme de operare, cum ar fi: Linux, MacOS, Android, etc.

Cu toate acestea, a apărut și o creștere a cererii de cercetători malware foarte calificați pentru a face față acestui val și nivel de amenințări și să poată crea următoarea generație de tehnologii de protecție a securității.

Nu rămâne neafectată nici Republica Moldova, ținte ale atacatorilor sunt atât utilizatorii sistemelor informatice, entitățile economice cât și instituțiile de stat. Conform statisticii celor de la ”Kaspersky Lab”, în ultima perioada de timp, Republica Moldova este ținta celor mai fecvente atacuri pe segmentul WEB cu diferite malware-uri de tip Trojan. Bunăoara, pe percursul ultimului deceniu Republica Moldova a fost ținta diferitor tipuri de atacuri malware, cum ar fi: viruși, trojeni, viermi, ransomware, adware, etc, și majoritatea din ele nefiind examinate de către entitățile de stat specializate pe investigații a infracțiunilor.

Scopul principal al acestei lucrări este de a crea punctul de reper pentru elaborarea unui laborator de analize fișiere malițioase în cadrul Centrului tehnico-criminalistic și expertize judicare al Inspectoratului General al Poliției pentru analiza practic a oricărui tip de virus și raportarea rezultatelor obținute în Raport de constare tehnico-științifică și Raport de expertiză judiciară/extrajudiciară.

CONCLUZII

Avansarea tehnologiilor informaționale a schimbat viața omenirii într-o direcție evident pozitivă și a revoluționat modul în care organizațiile conduc afacerile. Cu toate acestea, evoluția tehnologiei și digitalizarea au dat naștere activităților cibernetice cu caracter criminal. Amenințarea crescândă a atacurilor cibernetice asupra infrastructurilor critice, centrelor de date, sectorului privat / public, apărării, energiei, statului și sectoarelor financiare reprezintă o provocare unică pentru toată lumea, de la un individ la corporații mari. Aceste atacuri cibernetice folosesc programe malițioase (cunoscute și sub numele de viruși) pentru furt financiar, spionaj, sabotaj, furt de proprietăți intelectuale și războiuri hibride.

Odată ce atacatorii devin mai numeroși și efectuează atacuri malițioase avansate, detectarea și răspunsul la astfel de intruziuni este esențială pentru specialiștii în securitatea cibernetică și măsurilor de investigație. Analiza virusului a devenit o necesitate indispensabilă pentru combaterea atacurilor cibernetice. Bunăoară, pentru o analiză de succes este necesar de a dispune de un mediu cu instrumente specializate și cunoștințe în domeniul respectiv.

În această teză de master s-a pus accent pe redarea compartimentelor necesare în eleborararea unui laborator, metodelor și instrumentelor la examinarea fișierelor malițioase, care cu siguranță vor servi punctul de reper pentru elaborarea unui laborator de analize malițioase în cadrul Centrului tehnico-criminalistic și expertize judiciare al Inspectoratului General al Poliției pentru analiza practic a oricărui tip de virus și raportarea rezultatelor obținute în Raport de constare tehnico-științifică și Raport de expertiză judiciară/extrajudiciară.

BIBLIOGRAFIE

1. Monnappa K A. Learning Malware Analysis. Birmingham: Packt Publishing Ltd., 2018. ISBN 978-1-78839-250-1;
2. Alexey Kleymenov, Amr Thabet. Mastering Malware Analysis. Birmingham: Packt Publishing Ltd., 2019. ISBN 978-1-78961-078-9;
3. Валентин Холмогоров. PRO Вирусы (2-е издание). Санкт-Петербург: ООО <<Страта>>, 2017. ISBN 978-5-9909788-0-5;
4. Christopher C. Elison. MALWARE, ROOTKITS &BOTNENTS (a beginer's guide). The McGraw-Hill Companies, 2013. ISBN: 978-0-07-179205-9;
5. Wenke Lee. Malware Knowledge Area (issue 1.0). Crown Copyright, The National Cyber Security Center, 2019;
6. .Abhijit Mohanta, Anoop Saldanha. Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware. Apress, 2020. ISBN: 978-1-4842-6193-4;
7. Michael Hale Ligh, Steven Adair, Blake Harstein, Matthew Richard. Malware Analyst's Cookbook and DVD. Indianapolis: Wiley Publishing Inc., 2011. ISBN: 978-0-470-61303-0;
8. Allan Liska, Timothy Gallo. Ransomware. Sebastopol: O'Reilyy Media Inc., 2017. ISBN: 978-1-491-96788-1;
9. Yonas Leguesse, Christos Sidiropoulos, Kaarel Jõgi, Lauri Palkmets. Andvanced Artefact Analysis: advanced static analysis. European Union Agency for Network and Information Security (ENISA), 2015;
10. Yonas Leguesse, Christos Sidiropoulos, Kaarel Jõgi, Lauri Palkmets. Andvanced Artefact Analysis: introduction to advanced dynamic analysis. European Union Agency for Network and Information Security (ENISA), 2015;
11. Yonas Leguesse, Christos Sidiropoulos, Kaarel Jõgi, Lauri Palkmets. Andvanced Artefact Analysis: advanced dynamic analysis, European Union Agency for Network and Information Security (ENISA), 2015;
12. Гайд по работе с вирусными файлами для новичков, ©2020 [citat 07.10.2020]. Disponibil: https://telegra.ph/Gajd-po-rabote-s-virusnymi-fajlami-dlya-novichkov-09-26;
13. Wich countries have the worst (and best) cybersecurity, ©2020 [citat 05.10.2020]. Disponibil: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/.