UDC: 681.518:343.983 ИНФО М: стр. 40-43

ОПШТИ АСПЕКТИ ДИГИТАЛНЕ АНТИ-ФОРЕНЗИКЕ
GENERAL ASPECTS OF DIGITAL ANTI-FORENSICS

Петар Чисар, Криминалистичко-полицијска академија

РЕЗИМЕ: Дигитална форензика је суштинска област за успешно супротстављање компјутерском криминалу. Она је повезана са много изазова, укључујући и брзе промене у компјутерским и дигиталним уређајима, као и све софистицираније нападе на рачунарске системе и мреже и брз пораст злоупотреба информационо-комуникационих система. Иако постојеће одбрамбене технике могу поуздано детектовати многе уобичајене облике угрожавања, недавна истраживања су показала да оне могу да се избегну коришћењем анти-форензичких активности, планираних тако да сакрију доказе о злонамерним активностима. Зато су као одговор на то, развијене нове форензичке технике у циљу детекције употребе анти-форензичких средстава. У светлу овога, постоји изражена потреба за теоријским разумевањем интеракције између анти-форензичког акта и форензичког испитивања.

КЉУЧНЕ РЕЧИ: дигитална форензика, анти-форензика, скривање података, форензички алати

ABSTRACT: Digital forensics is essential for the successful opposition of computer crime. It is associated with many challenges, including rapid changes in computer and digital devices, and more sophisticated attacks on computer systems and networks and the rapid increase in abuse of ICT systems. Though many of existing defensive techniques can reliably detect traditional forgeries, recent research has shown that they can be bypassed by anti-forensic operations designed to hide evidence of such activity. In response, new forensic techniques have been developed to detect the use of anti-forensics. In light of this, there is a need to develop a theoretical understanding of the interactions between anti-forensic act and a forensic investigator.

KEY WORDS: digital forensics, anti-forensics, data hiding, forensic tools

УВОД

Дигитално доба се може окарактерисати широком употребом компјутерске технологије као начином за унапређење претходних могућности и садашњих потреба. Примена компјутерских система као средства у личне, комерцијалне, образовне, управне и друге сфере модерног живота, учинило је бољим многе сегменте ових ентитета. У исто време, примена информационих технологија као криминалног средства увећала је могућност за извршење, прикривање или подршку незаконитим или неетичким активностима. У основи, њихова масовна употреба од стране најшире популације, удружена са покушајем анонимности, подстиче криминалне активности које користе рачунарске системе. Овај тзв. "сајбер криминал" није нужно нова форма криминала, већ знатно више класична криминална активност која користи широке могућности рачунара и приступ информацијама. Он се може сматрати последицом растуће доступности нових технологија и корисничких способности за употребу рачунара у злонамерне сврхе. Са циљем лоцирања, хватања и осуђивања актера укључених у компјутерски криминал, надлежни истражитељи морају имплементирати конзистентне и прецизно дефинисане дигиталне форензичке процедуре.

Дигитална форензика је наука о опоравку и испитивању дигиталних уређаја, са циљем обезбеђења доказа у вези са компјутерским криминалом. Форензички истражитељи прикупљају дигиталне уређаје/доказе, извлаче потенцијалне доказе и анализирају их, како би утврдили могуће везе између извршеног криминала и починиоца. У судским процесима, истражитељи презентују своје резултате и извештавају о испитивањима како би помогли тужиоцима да формирају оптужнице против извршилаца. Ово је идеалан сценарио, али нажалост ситуација се у реалности мења, а сајбер криминал временом постаје све више софистициран. Основна идеја је да напад не мора обавезно да буде савршено изведен, већ је потребно да се посао истражитеља учини што сложенијим и отежа проналажење нападача и могућих доказа о повезаности напада и нападача. Ово правило и овај приступ се односи на идеју анти-форензике. Анти-форензика (АФ) се може дефинисати као различитост софтверских алата и техника дизајнираних са циљем да се компјутерском форензичком истражитељу отежа проналажење сумњивих података или да се потенцијални докази учине неприхватљивим на суду.

У прошлости, анти-форензика је углавном била у домену сајбер криминала – појединаца који познају многе аспекте компјутерских технологија и одлично разумеју концепте рачунарства. Они су дизајнирали најраније врсте алата за извршење основних анти-форензичких активности. Међутим, времена су се променила и ови првобитни алати поново постају актуелни, али у знатно сложенијем облику.

Анти-форензика је прихваћен термин у дигиталној форензичкој дисциплини. Тренутно не постоји једна генерална дефиниција. Да би се јасно артикулисао однос анти-форензике према дисциплини и разликовао од форензике уопште, предложен је појам дигиталне анти-форензике (ДАФ). ДАФ се односи на манипулацију, брисање и заваравање дигиталних података или отежавање испитивања, чинећи га временски захтевним или понекад и немогућим.

ГЕНЕРАЛНЕ КАТЕГОРИЈЕ ДИГИТАЛНЕ АНТИ-ФОРЕНЗИКЕ

ДАФ технике се могу категорисати на основу планираних активности или ефеката које имају на: преписивање

података и метаподатака (брисање), скривање података (стеганографија, криптографија и методе ниског техничког нивоа), брисање артефаката, заваравање трасе, као и напади усмерени на компјутерске форензичке алате (Rogers, 2005).

Преписивање података - Намера ове акције је да се униште сви потенцијални инкриминишући подаци (дигитални докази). Са многим доступним алатима се лако бришу фајлови, директоријуми, партиције и хард драјвови. Истражитељи користе разне алате да форензички очисте хард драјвове пре него што их употребе за аквизицију и анализу података. Већина алата преписује податке помоћу одабраног карактера. Опције алата обично дозвољавају једнократно преписивање (замену) датума у циљу брзог брисања или произвољан број пута за сигурније брисање. Вишеструка преписивања могу учинити опоравак података немогућим. У току анализе није необично да се нађу бројни сектори на осумњиченом хард драјву који сви садрже исте карактере. Ово је добар показатељ да је нешто претходно избрисано са хард драјва.

Скривање података - Иако је стеганографија (скривено писање) позната већ око хиљаду година, она се у данашње време односи на прикривање дигиталних информација у склопу фајла (тзв. фајл носиоц). Стеганографски алати функционишу тако да скривају дигиталне податке на начин да само пошиљалац и прималац знају да су тамо. Често се у пракси користе дигиталне слике као датотеке носиоци. Стеганографски алати могу променити најмање значајне битове у слици и заменити их одговарајућим битовима који потичу од података који се скривају. Када се то уради, jpg-датотека неће бити визуелно различита, иако су њени пиксели промењени. Једини начин да се утврди да ли је слика промењена је да се провери њена величина у бајтовима или упореди hash-вредност у односу на вредност пре измене. Неопходно је да претходне вредности треба да буду познате и негде документоване. Задатак истражитеља је да трагају за присуством стеганографских алата на осумњиченом рачунару. Ако нису пронађени такви алати, могуће је да се њихови артефакти могу пронаћи у регистру. Да би се олашао овај процес, постоје неки комерцијално доступни алати који могу да детектују присуство стеганографских апликација и њихових артефаката.

Брисање артефаката - Алати за брисање артефаката су у употреби већ много година. Програми за брисање (нпр. BC Wipe, Eraser и PGP Wipe) уништавају датотеке са подацима користећи вишеструко преписивање, како би учинили било какво проналажење података практично немогућим (Kessler, 2007).

Софтвер за аутоматско брисање артефаката омогућава кориснику да ослободи простор за складиштење и заштити приватност, уклањањем непотребних привремених датотека које оптерећују хард драјв. Софтвери као што су Evidence Eliminator, Secure Clean и Window Washer, уклањају историју претраживача и кеш фајлове, бришу одређене фајлове оперативног система и бришу slack и неалоцирани простор. Многи од ових програма се испоручују претходно конфигурисани тако да елиминишу последице различитих оперативних система, као и често коришћених алата (Windows, MS Office, Internet Explorer, AOL Instant Messenger и Firefox) и имају додатне plug-in-ове за велики број других апликација (Eudora, Picasa, RealAudio и WinZip). Доступна су многа упутства са детаљним образложењима који фајлови треба да буду очишћени како би анализа била што тежа, а форензика постала спорна.

Најбољи од ових алата не само да бришу нападачке фајлове, него их и уклањају. Брисање непотребних фајлова је довољно да се опорави простор на диску. Брисање датотеке указује на то да је неко заинтересован за више од простог опоравка простора.

Алати за брисање артефаката чине анализу компликованијом за форензичке истражитеље, али је чињеница и то да нису савршени. Већина програма оставља препознатљиве трагове брисања, а и многи од њих нису комплетни као што се рекламирају, често остављајући за собом остатке који би требало да су избрисани.

Заваравање трасе - Заваравање трасе је појава позната још од 1970-тих година као лажирање пријављивања и касније 1980-тих као лажирање IP и MAC (Medium Access Control) адресе (Kessler, 2007). Напади типа одбијања услуга (Denial-of-Service – DoS) и расподељеног одбијања услуга (distributed DoS - DDoS) зависе од успешног лажирања IP адресе, које је мрежне упаде учинило сложенијим за испитивање. Одбрана од DoS и DDoS напада захтева више превенције, реаговања и опоравка, него детекција нападача, мада су неки методи праћења IP траса управо осмишљени са циљем праћења пакета кроз мрежу све до њиховог извора.

Има много начина да се заварају е-маил истраге. Анонимизатори е-маил-а наводно пружају услуге обезбеђења приватности, спречавајући истражитеље да одреде извор послате поруке. Убацивање лажних заглавља, отворени SMTP (Simple Mail Transfer Protocol) proxy-и и анонимни SSH (Secure Shell) тунелски сервери налазе се међу механизмима који могу учинити сложеним праћење порекла е-маил-а. Веб анонимизатор прикрива идентитет корисника Веб сајта, а скуп алата за анонимност, као што је нпр. Tor, може ефикасно да доведе интернет-базирану истрагу до застоја.

Заваравање трасе се такође може извести брисањем и/или променом серверских лог-фајлова и/или фајлова системских догађаја или мењањем датума различитим фајловима.

Напади усмерени на компјутерске форензичке алате - Директни напади на форензичке процесе рачунара представљају најновији тип АФ и потенцијално најопаснији. Апстрактни модел дигиталне форензике предлаже стандардизовани дигитални форензички процес, који се састоји од следећих шест компоненти (Reith et al., 2007).

Идентификација: препознаје инцидент од индикатора и одређује његов тип.

Припрема: припрема алата, техника, налога за претраживање, праћење овлашћења и управљачка подршка.

Стратегија приступа: развија процедуру са циљем максимирања прикупљања сигурних доказа, уз минимизирање утицаја на жртву.

Очување: подразумева изолацију, обезбеђење и очување стања физичких и дигиталних доказа.

Прикупљање: подразумева снимање физичке сцене и дуплицирање дигиталних доказа, користећи стандардизоване и прихваћене процедуре.

Испитивање: укључује детаљно систематско претраживање доказа који се односе на предметни криминал.

Анализа: утврђивање значаја, реконструкцију фрагмената података и доношење закључака на основу пронађених доказа.

Презентација: укључује преглед и објашњење закључака.

Враћање доказа: обезбеђује да физичка и дигитална имовина буде враћена власнику.

У складу са методологијом дигиталне форензичке анализе (Department of Justice, 2013), три процеса су есенцијална: припрема/екстракција, идентификација и анализа.

Анти-форензичке процедуре могу да учине несигурним поузданост дигиталних доказа. Ако поузданост доказа може да буде доведена у питање, она постаје безвредна на суду.

Мора се истаћи да су забележени успешно реализовани напади на многе познате форензичке алате, као што су EnCase, FTK, iLook, SleuthKit и WinHex (Kessler, 2007).

АНТИ-ФОРЕНЗИЧКИ АЛАТИ

Сајбер криминалци детаљно разумеју компјутерску технлологију, до њене веома елементарне форме. Они за остварење својих циљева обично користе неке од најчешћих технологија, али такође могу имати и прилично маштовите идеје.

Неки популарни анти-форензички алати су дизајнирани да се прилагоде метаподацима фајла, са намером да алат који се користи за анализу доведу у забуну. На пример, алати као TimeStomp (Offensive Security Ltd., 2013), омогућавају нападачима да утичу на креирање било ког фајла, његову измену и време приступа. Они такође могу да мењају информације у заглављу фајла. Алати за анализу претражују фајлове по информацији која се налази у заглављу и flag-овима, уколико уоче било какву разлику између података о типу фајла датог у заглављу и типа фајла на основу његове екстензије. Такви алати су способни да модификују заглавља фајлова заједно са екстензијама и на тај начин избегну детекцију.

Други скуп алата, у који се убраја нпр. Sam Juicer (Wright, 2007), је у стању да пронађе лозинке система и системске кључеве за енкрипцију са ограниченим привилегијама, при томе не остављајући никакав траг за собом. Такви алати сами себе смештају у меморију и уз помоћ неких алата (нпр. алата за бинарно паковање или алата за повезивање) се прикључују другим процесима.

Остали алати, као нпр. Slacker (Fifarek, 2008), могу да исеку на делове фајл од интереса, а затим те делове сакрију у slack простор фајла. Ова врста скривања је веома ефикасна, јер форензички алати ову ситуацију тумаче као шум фајла, а не као сам фајл. Чак и у случају да су фајлови означени од стране алата за анализу, веома је тешко поново креирати оригинални фајл без познавања начина на који је претходно растављен. Слични алати могу да смештају податке у фајл и после маркера који означава крај фајла. На тај начин, већина програма неће открити скривене податке у фајлу, пошто су дизајнирани да читају фајл док не наиђу на EOF. Један такав специјалан алат по имену Data Mule FS, сакрива податке у резервисан простор хард диска.

Системска меморија је веома непоуздана јединица за смештај података и дизајнери анти-форензичких алата користе ову чињеницу. Стога алати, као што је MOSDEF, користе ситуацију да данашњи рачунари располажу са великом количином примарне RAM меморије и RAM меморије за видео графику, која се може искористити за покретање неког кода (Berinato, 2007).

Енкрипција је сигуран начин за тајно складиштење података. Особа са тајним кључем може да чита и пише шифровани фајл, док за неког са стране он представља скуп случајних карактера, без неког одређеног значења. Нападач може да изврши партицију фајл система и да репартиционира креирану партицију, са циљем да формира скривену партицију. Сада нападач може да енкриптује скривену партицију и смести податке у њу. Та енкриптована партиција је скуп неразумљивих карактера, коме уз помоћ правог кључа нападач може било када да приступи. Ова техника је веома корисна за нападача, пошто он на овај начин може да стави неке мање осетљиве информације у новоформирану партицију, а осетљиве информације у скривену партицију. Ако нападач буде ухваћен, мала је шанса да истражитељи открију енкриптовану партицију и декриптују је. На тај начин, нападач ће бити одговоран само за крађу мање осетљивих информација.

Стеганографија је још један популаран метод за скривање података. У својој суштини, стеганографија покушава да сакрије осетљиве информације унутар наизглед нормалних информација. Иако овај метод има легитимну намену, он се прилично интензивно користи и од стране нападача. Нападач може да сакрије неку информацију унутар фајла са сликом, звуком или видеом и пошаље је без побуђивања сумње. Ова техника се може проширити убацивањем таквих информација као што је скуп инструкција машинског нивоа у други бинарни фајл, тако да се не промени значење фајла носиоца.

Поред ових алата и техника, постоје и интелигентни алати који генеришу лажне доказе или одводе истрагу у погрешном правцу.

ЗАКЉУЧАК

Веома је тешко парирати анти-форензици само уз помоћ форензике. Истражитељи би требало да прошире подручје своје истраге интегрисањем аспеката физичке истраге са дигиталном истрагом. На пример, ако није могуће утврдити нападачку активност са радне станице жртве, истражитељ би требало да користи алате за мрежни мониторинг, лог агрегаторе итд. да пронађе и сакупи информације из више извора. На тај начин се на основу корелације различитих информација из више извора може добити идеја о криминалним активностима.

За сваку форензичку технику постоји одговарајућа анти-форензичка техника. На жалост, обрнуто не важи. Због тога, како се појављују нови алати и анти-форензичке технологије, тако стручњаци из ове области би требало да прате актуелне трендове развијањем нових методологија и техника. Истовремено, примена и стално прилагођавање дубинског сигурносног модела рачунарских система може помоћи у континуираној борби против анти-форензике.

ЛИТЕРАТУРА

[1] Kessler, G.C., (2007). *Anti-forensics and the digital investigator*, In C. Valli & A. Woodward (Ed.), Proceedings of the 5th Australian Digital Forensics Conference. Mt. Lawley, Western Australia: Edith Cowan University

[2] Reith, M., Carr, C., Gunsch, G., (2002). *An Examination of Digital Forensic Models*, International Journal of Digital Evidence, Volume 1, Issue 3.

[3] Rogers, D.M., (2005). *Anti-Forensic Presentation given to Lockheed Martin*, San Diego, http://www2.tech.purdue.edu/cit/Courses/cit556/Lectures/lecture17%20Email.pdf, dostupan 15.4.2013.

[4] Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), Cybercrime Lab, http://www.cybercrime.gov, dostupan 31.8.2013.

[5] "TimeStomp," Offensive Security Ltd., http://www.offensive-security.com/metasploit-unleashed/TimeStomp, dostupan 31.08.2013.

[6] Wright, C., (2007). *SAM Juicer does not need SYSTEM Privileges*, http://gse-compliance.blogspot.com/2007/12/sam-juicer-does-not-need-system.html, dostupan 31.08.2013.

[7] Fifarek, R.H., (2008). *Metasploit Anti-Forensics Project (MAFIA) – Slacker.exe*, http://synfulpacket.blogspot.com/2008/11/metasploit-anti-forensics-project-mafia.html, dostupan 31.08.2013.

[8] Berinato, S., (2007). *How Online Criminals Make Themselves Tough to Find, Near Impossible to Nab*, CXO Media Inc., http://www.cio.com/article/114550/, dostupan 31.08.2013.

доц. др Петар Чисар – Криминалистичко-полицијска академија, Земун
Контакт: petar.cisar@kpa.edu.rs
Области интересовања: дигитална форензика, сигурност информационих система, мобилне технологије, рачунарске мреже, fuzzy-теорија.

infoM

UPUTSTVO ZA PRIPREMU RADA

1. Tekst pripremiti kao Word dokument, A4, u kodnom rasporedu 1250 latinica ili 1251 ćirilica, na srpskom jeziku, bez slika. Preporučen obim – oko 10 strana, single prored, font 11.
2. Naslov, abstakt (100-250 reči) i ključne reči (3-10) dati na srpskom i engleskom jeziku.
3. Jedino formatiranje teksta je normal, bold, italic i bolditalic, VELIKA i mala slova (tekst se naknadno prelama).
4. Mesta gde treba ubaciti slike, naglasiti u tekstu (Slika1...)
5. Slike pripremiti odvojeno, VAN teksta, imenovati ih kao u tekstu, radi identifikacije, u sledećim formatima: rasterske slike: jpg, tif, psd, u rezoluciji 300 dpi 1:1 (fotografije, ekranski prikazi i sl.), vektorske slike – cdr, ai, fh,eps (šeme i grafikoni).
6. Autor(i) treba da obavezno priloži svoju fotografiju (jpg oko 50 Kb), navede instituciju u kojoj radi, kontakt i 2-4 oblasti kojima se bavi.
7. Maksimalni broj autora po jednom radu je 5.

Redakcija časopisa Info M