ОФАНЗИВНЕ САЈБЕР АКТИВНОСТИ

Потпуковник *Горан* Калаузовић

Улогу постојећих информационих технологија (ИТ) у заштити и прикупљању података карактерише пораст примене у широком спектру свих друштвених активности, па и војних. У том смислу развијени су дефанзивни и офанзивни сајбер капацитети, односно сајбер одбрана и напад, с тим што, последњих десет година, сајбер напади имају све већу улогу у области познатој као извиђање рачунара. Ове активности подразумевају неовлашћено приступање циљаном рачунару или рачунарској мрежи, са којих се без знања власника информације и подаци преузимају и прослеђују на жељену меморијску локацију (рачунар).

*Аутор ради у Војнообавештајној агенцији

Последња деценија, а посебно последњих неколико година, општеприхваћен термин сајбер *(cyber)* доживео је своју експанзију у условима нарастајућих опасности, усмерених на комуникационо-информационе системе (КИС). Нарочито од потпуне блокаде КИС у Естонији 2007. године, ова претња се прихвата све мање као случај, а све више као нарастајућа неконвенционална опасност, која за релатив-

но кратко време може да дестабилизује државу или регион. С обзиром на то да постоји могућност заметања трагова сајбер напада и немогућности да се нападач идентификује, офанзивне сајбер мере се све чешће примењују у покушају да се дође до информације или да се она деградира.

Реч *cyber* је део грчке речи *cybernetics (*Κυβερήτης) или кибернетика*,* тј. наука о комуникацији и повратној контроли бића и система или остваривање сигурне ефикасности у току неке активности. Она је уско повезана са терминима *computer* и *internet.* Један од кључних појмова који се доводе у везу са овим термином је и сајбер претња (*cyber threat*) због чега је потребно објаснити шта у ствари сајбер претња подразумева.

Термин сајбер се, у ширем смислу, односи на активност којом се нарушава рад рачунара и рачунарске мрежне инфраструктуре. Међутим, у суштини, сајбер претња у примарном значењу представља могућност неовлашћеног приступа подацима и информацијама на рачунару и рачунарској мрежи, односно нарушавање функционисања комуникационо-информационе инфраструктуре у секундарном смислу.[1] Наиме, рачунарска мрежа представља два и више рачунара који се „виде", тј. који међусобно комуницирају, те се сајбер претња односи на приступ похрањеном материјалу у тим рачунарима без знања власника. Због тога, када постоји сајбер угроженост или могућност сајбер напада, мисли се искључиво на активност којом се на нелегалан начин обезбеђује приступ подацима смештеним на рачунар или више њих, употребом интернета и других доступних метода и техника.

У овом раду обрађена је примарна страна овог питања, позната као *извиђање рачунара* (*computer surveillance)*, једна од подобласти укупних обавештајних активности.[2] То је офанзивна сајбер активност, за разлику од пасивне сајбер активности, које се односе углавном на регистровање, односно праћење активности на интернету, праћење активности појединих корисника, заштиту информација и приступа појединим датотекама, постављањем корисничких шифри и лозинки. За реализацију офанзивних сајбер активности, извиђање рачунара се реализује:

– прикупљањем података помоћу интернета (извиђање употребом хакерских, злоћудних програма и хакерске технике) и
– прикупљањем података регистровањем електромагнетне енергије (ЕМЕ) коју емитују рачунарске компоненте (пасивно извиђање уз помоћ опреме за примену електронске подршке, односно извиђање радио-веза).

[1] У ситуацији отвореног сукоба, када сајбер нападач нема потребу заметања трагова о присуству циљаним рачунарима, циљ сајбер напада може да буде и уништење датотека са информацијама.

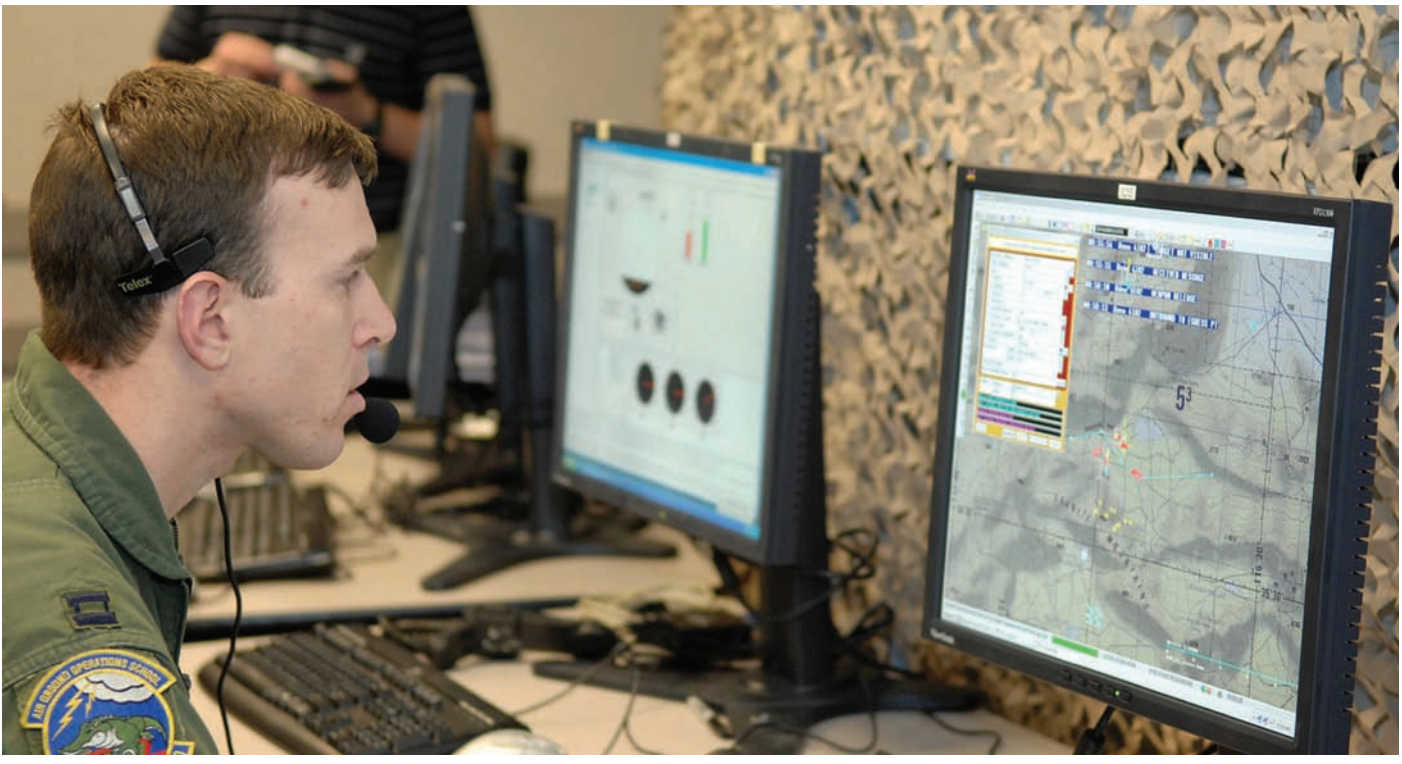
[2] *Intelligence Surveillance and Reconnissance – ISR.* Сајбер активности по својој природи, у односу на објекат ангажовања, могу бити активне и пасивне.

Прикупљање података помоћу интернета

Познато је да је интернет јавни медиј, који подједнако могу користити државни и недржавни актери под одређеним условима, које диктирају провајдери. У том смислу, највише пажње заинтересованих лица привлаче сајтови државних и приватних агенција и компанија, у очекивању да се дође до одређене информације. Наравно да се не очекује да се на њима нађу критичне информације, јер се оне архивирају на одвојеним мрежама и рачунарима, којима је врло тешко приступити, с обзиром на то да су физички одвојени и заштићени. Такође, ради квалитетније заштите података, формирају се приступне лозинке и шифре са што већим бројем карактера и њиховом честом променом.

Међутим, данас се, нарочито за комерцијалне потребе, све више уводи у праксу електронско пословање и комуникација између кореспондената, односно размена информација, докумената, поднесака, али и плаћање услуга, трговина и остале финансијске трансакције. С обзиром на то да је овај начин комуникације уведен најпре из практичних разлога, због удаљености учесника и корисника, у првом моменту се није водило рачуна о заштити података. Да би се обезбедила приватност, односно безбедност таквог начина размене информација, уведена је потреба регистровања корисника и посетиоца одређених сајтова, где се додељују одређене корисничке шифре и приступни кодови.

С друге стране, када се говори о сајтовима, а који се тичу одбране и безбедности, укључујући и компаније које су специјализоване за пружање услуга и потреба системима одбране, на таквим сајтовима могу се наћи информације које не нарушавају систем одбране тих земаља. Намена таквих сајтова је да пружи основне информације заинтересованим корисницима по појединим питањима, пре свега због могуће сарадње у одређеним областима са другим системима одбране или другим компанијама, где постоји заједнички интерес. Такође, поједини сајтови имају могућност класификације корисника, односно могућност доделе привилегија за приступ одређеним документима појединим корисницима, по додељеном критеријуму корисника. Примера ради, припадници појединих америчких јединица имају могућност да приступе одређеним сајтовима и документима, док је за друга лица сајт недоступан. Слична ограничења се постављају и пред припаднике комерцијалних компанија ради спречавања неовлашћеног приступа службеним подацима. Истовремено, постоји могућност контроле посећености сајта, у смислу ре-



гистровања интересовања за поједине *web* странице – ко су интересенти, колико учестало посећују поједине интернет адресе, која област их интересује и слично. Због тога и за такве потребе, а као неписано правило, на тим сајтовима се постављају дискретни програми који имају могућност само да региструју наведене податке. Међутим, уколико неки од посетилаца има намеру да по сваку цену приступи одређеном сајту или да предузме неку другу радњу за коју није овлашћен, такви сајтови имају уграђене механизме, програме, који упозоравају власника сајта на покушаје који се могу сматрати нападом на сајт. Зависно од процене колико је сајт угрожен, пружа се адекватан одговор, односно примењују се дефанзивне или офанзивне мере, које спадају у домен сајбер или компјутерскомрежних активности. Оне подразумевају јаче мере заштите и онемогућавање приступа сајту или се, ако се процени да је неопходно, предузимају и мере одговора, односно контранапада.

С обзиром на то да се ради о заштити комуникационо-информационих система (КИС), као изузетно осетљивом и питању од националног значаја, за такву врсту активности, многе земље су, након случаја „Естонија" као првог примера сајбер напада на КИС и институције једне државе, отпочеле са формирањем капацитета за супротстављање таквим претњама.

Познато је да су у сегменту заштите од сајбер напада најдаље отишле ОС САД мада у сајбер активностима и Кина има све већу улогу.[3] Оне су формирале команде и сајбер јединице управо са циљем да прате активности на интернету, како из иностранства тако и у унутрашњости државе, ради благовременог упозорења на могућност напада, пружања заштите, али и предузимања противнапада.[4]

О прикупљању података преко интернета, а с обзиром на карактер делатности, не постоје подаци о посебним специјализованим системима који се користе за реализацију тих задатака. То су одређене технике прикупљања података, које користе поједине хакерске програме и вештине, али и несавршеност и недостатке појединих програма за претраживање,[5] од којих се у пракси најчешће примењују две:

– прикупљање података употребом хакерских (злоћудних) програма и
– прикупљање података помоћу бежичног (*wireless*) интернета.

Наведене технике представљају, заправо, основна сајбер средства, која се користе за сајбер делатности употребом интернета.

Метода прикупљања података употребом програма (software) са интернета

Метода подразумева развој и примену *посебних хакерских програма* или софтвера, који треба да буду у функцији прикупљања података у корист сајбер нападача, а остварује се њиховим дискретним убацивањем на рачунар корисника док је повезан на интернет. Ови злоћудни програми рекламирају се као бесплатни (*free download*) програми за различите намене или рекламе (*advertisement*) на сајтовима различитих провајдера, а најчешће као програми „мамци", који треба наводно да поспеше рад рачунара (интернета) или пруже адекватну услугу кориснику.[6] Када се учитају са сајта и након рестартовања рачунара, њихово присуство се манифестује на различит начин, од нарушавања до блокирања рада рачунара, те се у највећем броју случајева стиче утисак да је рачунар заражен вирусом. У почетку, то и јесте био основни циљ хакера, да се поремети уоби-

[3] Највећи светски претраживач *Google* плаћа годишњу лиценцу да би могао да буде коришћен на простору Кине, што се сматра контролисаном употребом овог претраживача од стране кинеских сајбер институција.

[4] Сајбер команда САД, формирана средином 2009. године, почетком октобра 2010. године достигла је пуну оперативну способност.

[5] *„Microsoft – jedan od krivaca za hakerski napad na Google",* 15. јануар 2010. године.

[6] *Internet Service Provider – ISP.*

чајени начин рада рачунара (мреже). Међутим, временом су захтеви проширени на потребу инсталирања лоших програма на рачунаре корисника, са намером дискретног прикупљања података са меморијских локација и периферије. На тај начин, уколико рачунар не поседује потребну заштиту (антивирусни програм и заштитни зид – *firewall*), може доћи до отицања личних, али и службених података са рачунара. Уз то, провајдери имају могућност да утврде адресе и локације корисника интернета, прегледом сајтова на којима су корисници боравили и могу да утврде њихова интересовања (на дневној основи). Такође, приступом шерованим датотекама (доступне датотеке на рачунарима корисника интернета) и периферији (*CD/DVD ROM, USB,* укључујући и десктоп) могу да прикупе личне и друге корисне податке и на тај начин изврше ближу идентификацију и процену власника рачунара.

Постоји више врста различитих хакерских програма, који су у функцији претходно наведеног (слика 1).

Вирус (*virus*) јесте програм или код који се сам генерише у другим датотекама с којима долази у контакт и извршава штетно дејство без знања корисника и његовог одобравања. Може да се нађе и зарази било који програм, сектор за подизање рачунара, документ који подржава наредбе, тако да промени садржај те датотеке и у њу копира свој код. Рачунарски вирус обично се састоји од два дела. Први је самокопирајући код који омогућава размножавање вируса, сакривен у другом делу или корисној информацији која је на сајту послужила као тзв. програм мамац (постоје и вируси који се састоје само од самокопирајућег кода).

Вирус се генерише покретањем програма који садржи вирус или отварањем неког зараженог линка или датотеке. Постоје злоћудни (малвер) и доброћудни вируси. Разлика је у томе што доброћудни заузимају системску меморију или меморију на хард диску и ништа не предузимају, док злоћудни извршавају одређене радње, које доводе до нежељених последица. Појавом првих рачунарских вируса и њиховим штетним дејством појавила се потреба да се онемогуће, тј. бришу са зараженог компјутера. Први вируси били су програми који су исписивали занимљиве, пропагандне или духовите поруке на монитору (као, на пример, вирус Каменко, који је исписивао поруку на монитору: „Ваш диск је скамењен"), док се вируси новијег времена најчешће убацују дискретно, са намером да обезбеде отицање података.

Слика 1 – Злоћудни програми

Малвер (*malware*) јесте сложеница настала од енглеских речи *malicious* и *software*, што у преводу значи малициозни или злоћудни софтвер (програм). Осим класичних рачунарских вируса обухвата све врсте софтвера који на било који начин могу да угрозе рачунарски систем или рачунарску мрежу, као што су тројанци, рачунарски црви, руткит, задњи улаз и различите врсте спајвера.

Спајвер (*spyware*) јесте сложеница настала од енглеских речи *spying* и *software.* Спајвер или шпијунски програм је врста малициозног софтвера чија је намена да пресреће или преузима делимично контролу рада на рачунару без знања или дозволе корисника. Иако назив сугерише да је реч о програмима који надгледају рад корисника, спајвер означава широк спектар програма који искоришћавају рачунар корисника за стицање користи за трећу страну. Спајвер се разликује од вируса и од црва по томе што се обично не умножава, односно не преноси у друге фолдере и датотеке. Као многи нови вируси, спајвер је креиран да искористи заражене рачунаре за прикупљање осетљивих података, комерцијалне, војне и др. Типичне тактике су приказивање незахтеваних поп-ап реклама, крађа личних информација (укључујући и финансијске информације као што су бројеви кредитних картица и лозинке), праћење активности на интернету за маркетиншке сврхе или преусмеравање нових *HTTP*

захтева на рекламне странице. У неким случајевима спајвер се користи за верификовање придржавања услова лиценце за коришћење програма. Зараза се у највећем броју случајева догађа приликом посете страница са илегалним или порнографским садржајем.

Тројанци (*trojan horses*) имају улогу да са компјутера на којем се налазе, путем интернета или друге везе, проследе другом кориснику податке првог. Обично су то шифре, лични подаци, бројеви кредитних картица и сл. Најпознатији тројанац је *Back Orifice* којег је за само месец дана преузело и користило скоро 100.000 људи на интернету. Он изгледа као обична сервер апликација, с тим што се сервер, тј. сам тројанац, инсталира без питања, као вирус, а када се стартује заражена апликација омогућава кориснику који дође до *IP* броја да преузме контролу над рачунаром.

Компјутерски црви (*worms*) користе рачунарску мрежу да би слали сопствене копије на друге рачунаре, обично користећи безбедносне рупе за трансфер са једног рачунара на други, најчешће без интервенције корисника. С обзиром на то да се могу брзо раширити путем мреже, инфицирајући сваки рачунар на свом путу, они представљају један од најпознатијих типова малвер кода, мада их доста корисника меша са вирусима. С обзиром на то да црви често искоришћавају рањивост мреже, они су једина врста малвера која се може делимично спречити постављањем заштитног зида (*firewall*), уз антивирус који треба да буде стално ажуриран.

„Rootkit" или алат за добијање администраторских права над системом представља групу извршних пакета, који дозвољавају хакерима да сакрију било какав доказ или траг да су успели да уђу у систем. Неке од радњи које овај алат обавља су:

– модификација система дневних датотека да би се избрисали докази о хакерским активностима,
– модификација алата система да би се теже открили хакерске радње,
– креирање скривене улазне тачке система,
– коришћење система као почетне тачке напада на остале умрежене системе.

Нарушавање рада сервиса масовном дистрибуцијом порука *(Distributed denial of service, DDoS*) подразумева масовно усмеравање великог броја захтева од стране већег броја *ботнета*[7] према циљаној адреси, односно рачунару – серверу (*URL*), тако да он не може да одговори на упућене поруке довољно брзо, па се његов рад блокира, чиме постаје недоступан и неупотребљив.

Знајући да је у пракси релативно висок ниво заштите који отежава приступ рачунарима који садрже важне податке и информације, поједине институције су отишле корак даље у смислу стварања начина да се дође до информације са обавештајно-безбедоносно интересантних рачунара и рачунарских мрежа. Отуда су развијене и претходно наведене технике прикупљања података приступом шерованим датотекама (фолдерима) рачунара који користе бежични (*wireless* и *wi max*) интернет и регистровањем електромагнетне енергије, коју зраче поједини делови рачунара који се налазе под напоном електричне енергије.

[7] Ботнет (*botnet*) – глобална мрежа већ компромитованих компјутера, од којих се већина налази у САД. Користе се за обарање сервера у важним јавним и приватним установама и институцијама.

Прикупљање података помоћу бежичног интернета

Метод прикупљања података помоћу бежичног (*wireless*) интернета,[8] заснива се на примени хакерских способности појединаца да приступе шерованим (дељивим, доступним) датотекама рачунара, који су у домету заинтересованог лица, најчешће хакера. Успех примене ове методе зависи од квалитета поседоване технике за пријем сигнала и удаљености корисника, као и способности хакера да приступи другим рачунарима. Успостављање комуникације са другим рачунаром врши се почетним испитивањем приступних (незаштићених) места рачунара. Да би се приступило адреси циљаног рачунара користе се стандардни или *USB wireless* модеми (слика 2), који ради јачег сигнала могу бити опремљени квалитетнијом антеном и појачавачем.

Слика 2 – Пример *USB wireless* модема

Регистровањем *wireless* сигнала (мрежа) добијају се подаци о приступу локалним рачунарским мрежама, које могу бити отворене (слободан приступ) или се приступ интернет мрежи условљава шифром. Шифроване мреже подразумевају формирање *WAP* кључева за кориснике у мрежи. За добијање података о *WAP* кључевима у одређеној мрежи, хакери користе кратке програме, који за кратко време обезбеђују преглед свих мрежа са подацима колико која мрежа има учесника, односно корисника и које су њихове адресе. Програми се, углавном, набављају од лиценцираних произвођача, док програми понуђени на различитим сајтовима нису поуздани, јер могу да садрже лоше малвер програме. Када се добије податак о *WAP* кључу шифроване мреже или када се приступа рачунару из отворене мреже, из *command prompta* рачунара који користи нападач (хакер), дају се налози за проверу приступа адресама – рачунарима у мрежи. Када се обезбеди приступ – комуникација са циљаним рачунаром преко адресе у мрежи, отпочиње се са приступом доступних партиција на рачунару. Најчешће је то системска или *C* партиција, мада има случајева да су понекад све партиције и њихови фолдери видљиви (шеровани) за учеснике у мрежи, што зависи од додељених привилегија корисницима. Приступом одређеним партицијама омогућен је и приступ појединим датотекама (најчешће је доступна датотека – фолдер *My Documents*), уколико нису заштићени приступним шифрама, са којих се могу преузимати подаци (фајлови).

Прикупљање података регистровањем електромагнетне енергије коју емитују рачунарске компоненте (пасивно извиђање)

Још шездесетих година двадесетог века[9] вршени су покушаји да се прикупе подаци на основу регистровања ЕМЕ коју зраче рачунари и поједине рачунарске компоненте (периферије рачунара).[10] Овај начин добијања података назван је ТЕМПЕСТ[11], а развиле су га, као и интернет, ОС САД и касније НАТО, за шта су дефинисани одређени стандарди и техничке процедуре, које важе у САД, НАТО и државама ЕУ.[12]

[8] Бежични (*wireless*) интернет је систем повезивања рачунара или рачунарске мреже са интернетом без потребе за телефонском линијом, те је иделан за кориснике који немају телефон. Комуникација се обавља бежично, радио-таласима, према међународном стандарду *IEEE 802.11b,* а користи се фреквенција од 2,4 и 5 *GHz.*

[9] Припадник обавештајно-безбедносне службе В. Британије *MI5*, Петер Рајт (*Peter Wright*), 1960. године је за потребе своје владе, која је преговарала за чланство у Европску економску заједницу – ЕЕЗ, са циљем да сазна став француског премијера Де Гола по том питању, регистровао секундарне таласе ЕМЕ које је емитовао заштићени шифарски комуникациони систем, а који је користила француска дипломатска мрежа, *''Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations?", Markus G. Kuhn* и *Ross J. Anderson.*

[10] За разлику од активности СИГИНТ, које подразумевају прикупљање података на основу регистроване електромагнетне енергије комуникацијских и радарских средстава, техника ТЕМПЕСТ почива на детекцији зрачене електромагнетне енергије рачунара и рачунарских средстава.

[11] Амерички акроним *TEMPEST - Transient Electromagnetic Pulse Surveillance Technology* или *Transient Electromagnetic Pulse Emanation Standard.*

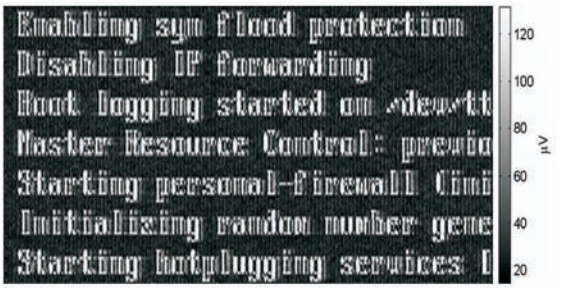
[12] За разлику од НАТО и САД, чије су ознаке ТЕМПЕСТ стандарда јавно доступне, поједине земље ЕУ, попут Немачке, и те податке дефинишу као строго поверљиве.

[13] У међувремену, врло је вероватно да су развијена

ТЕМПЕСТ је, иако позната већ неколико деценија, техника о којој се врло мало података може наћи у јавности.[13] То је технологија која се користи за војне, пре свега обавештајне сврхе, на основу уобичајеног зрачења ЕМЕ рачунарских средстава.[14] Информације прикупљене овом техником, с обзиром на начин на који су прикупљене, најчешће се класификују службеном тајном, по систему *„need-to-know"*, аналогно информацијама добијеним СИГИНТ активностима.

ТЕМПЕСТ технологија бави се и техником *прикупљања информација* са рачунара, али и *заштитом рачунара* од оваквог начина отицања службених информација, јер у супротном могу да настану несагледиве последице, када је у питању национална безбедност државе.

Техника прикупљања информација заснива се на прикупљању података путем регистровања зрачене ЕМЕ, којом се напајају рачунарске јединице, монитор, тастатура, каблови и портови (улаз/излаз) рачунара, као и скенери и принтери који су мање изложени јер се мање користе. Чињеница је да наведене компоненте за напајање користе мрежну електричну енергију, која се ослобађа и зрачи у локалној средини (где се компонента налази), у већој или мањој мери, зависно од снаге уређаја. За исписивање текста на дисплеју лаптопа или монитора потребна је ЕМЕ. Ту функцију обавља графичка картица (*digital video unit – DVU*), која пренети сигнал од тастатуре прослеђује од меморије до дисплеја. Трећа деоница на којој се преноси ЕМЕ и која носи информацију о садржају (тексту) преноси се од рачунара до принтера или од скенера до рачунара. Доказано је у пракси да чак и *RS-232* кабл (за повезивање портова) емитује ВФ фреквенције које носе користан сигнал. Такође, свако притискање типке на тастатури праћено је емитовањем ЕМЕ чије је трајање пропоционално времену колико је потребно за куцање различитих типки. Осим повезаних каблом, за пријем сигнала још су погоднije бежичне тастатуре, које раде на принципу емитовања радио-везе у ВВФ опсегу, чиме поспешују емитовање ЕМЕ и сигнал. Оне су нарочито погодне када је циљ заинтересованог лица (хакера) да се сазна



Слика 3 – Пријем видео сигнала са лаптопа *Toshiba Satellite Pro 440CDX,* на којем је инсталиран оперативни систем *Linux*, у резолуцији 800×600@75Hz видео моду, са пријемном антеном смештеној у суседној просторији, на даљини од 3m, без појачивача.

корисничко име, лозинка или e-*mail* адреса корисника. У периоду од 2001. до 2008. године усавршена су четири различита начина да се јасно реконструише текст на основу праћења ЕМЕ емитоване типкама тастатуре, са удаљености од 20 m, укључујући неколико преграда од зидова чврсте градње.

Експерименти су успешно реализовани без обзира на то да ли се ради са жичним или бежичним тастатурама (*PS/2, USB* конекторима, као и са тастатуре лаптопа).[15]

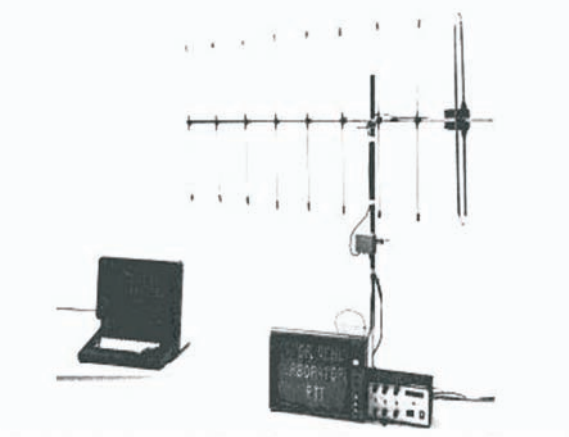
Након дугогодишњег испитивања у пракси, почетком деведесетих година прошлог века, Холанђанин Вим Ван Ек успео је у покушају да региструје емисије ЕМЕ са удаљеног рачунара (слика 3) помоћу једноставне опреме засноване на модификованом ТВ пријемнику са ручно контролисаним осцилатором (или лаптопом опремљеним ТВ картицом), усмереном антеном и појачивача сигнала (слика 4 и 5).

Слика 4 – Пријемник коришћен у експерименту (*DataSafe/ESL Model 400 Tempest Emission Monitor*)

[13] У међувремену, врло је вероватно да су развијена још ефикаснија средства за прикупљање података са рачунара.

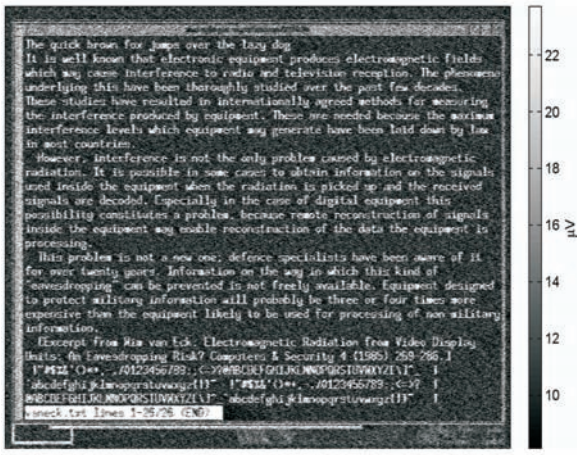
[14] За разлику од ГПС и ГМС техника за одређивање локације објеката и лица, ТЕМПЕСТ се мање користи за комерциијалне потребе.

[15] *''Electromagnetic Eavesdropping Risks of Flat-Panel Displays'' Markus G. Kuhn*, допуна рада из 2008. године.



Слика 5 – Основна опрема за пријем сигнала са дисплеја рачунара

Регистровањем ових сигнала прикупљани су подаци који су уз помоћ технике подешавања вертикалне и хоризонталне рефлектоване фреквенције монитора претварани у текст, односно у корисне информације (слике 3 и 6).



Слика 6 – Резултат експеримента методом Вим Ван Ека - пријем видео сигнала са лаптопа *Toshiba Satellite Pro 440CDX,* на којем је инсталиран оперативни систем *Linux*, са пријемном антеном на даљини од 10m (лаптоп од антене деле две просторије, преграђене са два зида чврсте градње, дебљине 1m) .

Почетне процене биле су у правцу да су емисије ЕМЕ изражене због монитора рађених на принципу катодних цеви и да ће се увођењем равних (*flat* или *TFT*) монитора и лаптопова такве емисије смањити. Међутим, испитивања су показала да је потребна много већа енергија за напајање кристала дисплеја, како би графичка картица рачунара (*DVU*) омогућила квалитетан приказ текста. На основу тога, у пракси је потврђено да много веће зрачење долази управо од равних монитора или лаптопова и да је, сходно томе, једноставније и ефикасније прикупљање информација регистровањем ЕМЕ са такве врсте дисплеја. Увођењем на отворено тржиште и употребу јефтиних лаптопова и масовном заменом стандардних, равним мониторима, који су у највећој мери незаштићени према ТЕМПЕСТ стандардима, омогућен је олакшан приступ информацијама на широкој основи, на шта је потребно скренути пажњу и предузети адекватне мере заштите.

Такозвана ненамерна зрачења (*unintentional emissions*), иако мале снаге, могу да буду детектована и претворена у одређену информацију, употребом адекватних антена и осетљивих пријемника за регистровање радио-сигнала у различитим фреквентним опсезима (ФО), са мање или веће удаљености.[16] Ослобођена ЕМЕ је највећа са монитора рачунара, а креће се у ФО од 55 до 245 MHz и може да буде регистрована са удаљености од једног метра до преко једног километра, у складу са опремом и условима у окружењу (препреке) у којем се рачунар налази.

Регистровање ЕМЕ може да се реализује и у ванрадно време, јер врло често рачунари остају укључени у радним просторијама (с обзиром на техничке карактеристике). Чак и ако су само монитори укључени, на основу зрачења кабла монитора повезаног на рачунар, могу се регистровати емисије које могу да дају информацију о физичком присуству лица у просторији где се налази рачунар. И обратно, када је монитор искључен, а рачунар укључен, кабл монитора може да представља антену са које се може детектовати користан сигнал графичке картице рачунара.[17]

Техника заштите рачунара подразумева спречавање или смањење зрачења рачунара (*emission security, EMSEC*), као дела заштите или спречавања отицања службених података путем комуникационих средстава (*communication security, COMSEC*). Наравно, у свакој комерцијалној или војној организацији, у банкарском

[16] *"Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?", Computers & Security, Neher Laboratories of the Netherlands PTT, Wim van Eck*, Холандија, децембар 1985. године.

[17] *''Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations?", Markus G. Kuhn* и *Ross J. Anderson.*

сектору и наменској индустрији нарочито, постоји потреба да се изради процена броја рачунара са најосетљивијим информацијама, који треба да поседују ТЕМПЕСТ стандарде заштите.

Убачени злоћудни или малвер програми (о којима је било речи приликом описивања прве методе) могу бити убачени у рачунар, са улогом да поспеше сигнал који се емитује из рачунара, због чега треба имати ажуриране комерцијалне антивирусне програме.

За потребе заштите рачунара дефинисани су стандард *NATO SDIP* (стара ознака *AMSG 720B*) и стандарди Агенције за националну безбедност САД, *NSA NACSIM 5100A* (слике 7 и 8):

– стандард *NATO SDIP-27 Level A* (стара ознака *AMSG 720B*) и америчка ознака *NSTISSAM Level I - "Compromising Emanations Laboratory Test Standard",* највиши је стандард заштите по питању зрачења ЕМЕ, који подразумева да рачунар има квалитетну заштиту од зрачења ЕМЕ и да заинтересовано лице (нападач) мора да буде на удаљености до 1 m да би регистровао податке са циљаног рачунара,
– стандард *NATO SDIP-27 Level B* (стара ознака *AMSG 788A*) и америчка ознака *NSTISSAM Level II - "Laboratory Test Standard for Protected Facility Equipment",* јесте стандард заштите по питању зрачења ЕМЕ, који подразумева да заинтересовано лице (нападач) може са удаљености од 20 m (укључујући и умањење квалитета сигнала због зидова просторија) да региструје податке са циљаног рачунара,
– стандард *NATO SDIP-27 Level C* (стара ознака *AMSG 784*) и америчка ознака *NSTISSAM Level III - "Laboratory Test Standard for Tactical Mobile Equipment/ Systems",* јесте стандард заштите по питању зрачења ЕМЕ, који подразумева да заинтересовано лице (нападач) може са удаљености од 100 m (укључујући и умањење квалитета сигнала због зидова просторија) да региструје податке са циљаног рачунара,
– стандард *NATO SDIP-29 (formerly AMSG 719G) - "Installation of Electrical Equipment for the Processing of Classified Information",* јесте стандард који подразумева захтеве по питању инсталација, у односу на удаљеност нападача,

TEMPEST Standards Comparison

Descriptive	Full	Intermediate	Tactical
SDIP-27 *'New' NATO Standards*	Level A	Level B	Level C
NATO Laboratory Standards	AMSG-720B	AMSG-788A	AMSG-784
NATO Zoning Standards	ZONE 0	ZONE 1	ZONE 2
USA NSTISSAM /1-92 standard equivalence	LEVEL I	LEVEL II	LEVEL III
Previous SST product nomenclature	BT	AT	ET
New SST product nomenclature	TF	TI	TT

Слика 7 – ТЕМПЕСТ стандарди

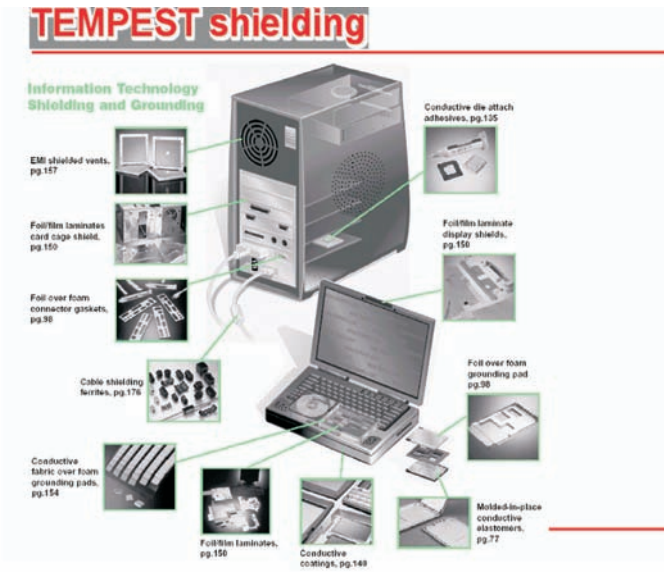
– стандард AMSG 799B - *"NATO Zoning Procedures"* је стандард који дефинише безбедоносне захтеве у односу на ниво заштите рачунара.

NATO SDIP-27 Standards	Former NATO AMSG Standards	USA NSTISSAM 1-92 Standards	NATO Tempest Zoning Standards
Level A	AMSG 720B	Level I	Zone 0
Level B	AMSG 788A	Level II	Zone 1
Level C	AMSG 784	Level III	Zone 2

SECAN Doctrine and Information Publication
SDIP- 27 Level A, B, C

Слика 8 – ТЕМПЕСТ стандарди (друга форма приказа)

Заштита и спречавање могућности отицања података и информација, на описани начин, подразумева употребу алуминијумских облога за мониторе и кућишта за хардвер рачунара, тастуру и каблове или рад и стављање безбедоносно осетљивих рачунара у исто тако заштићене просторије. Ако је потребно, одређена зграда се штити на тај начин што се у њој праве изоловане просторије које су херметизоване са свих страна и имају само врата, а опремљене су таблом за цртање и писање, са обавезом читања, забраном говора и употребом електронских средстава.



Слика 9 – Рачунари који испуњавају ТЕМПЕСТ стандарде

Ради заштите информација на претходно описани начин, развијени су тзв. ТЕМПЕСТ рачунари, чији су сви саставни делови обложени алуминијумским заштитним слојем (слике 9 и 10). Европска унија је, такође, усвојила своје стандарде из ове области и има своју развијену номенклатуру (слика 11).

Слика 10 – Рачунари САД према ТЕМПЕСТ стандардима

Слика 11 – Рачунари ЕУ према ТЕМПЕСТ стандардима (холандска верзија)

Рачунари који имају одређени ниво заштите означавају се према усвојеној стандардној номенклатури (слика 12).

Слика 12 – Одређивање номенклатуре рачунара са ТЕМПЕСТ стандардом

У складу са стандардом *73-2A NSA* (Агенције за националну безбедност САД), минимални ниво заштите, који ТЕМПЕСТ рачунар треба да обезбеди, јесте 50 децибела *(Db)*. За ниво од *100 Db* заштита око рачунара је потпуно хомогена.

Са америчког становишта, по питању издавања безбедоносне лиценце за одржавање, приступ ТЕМПЕСТ рачунарима и пратећој опреми, поред Американаца имају и лица из Аустралије, Новог Зеланда и земаља чланица НАТО, изабрана према строго дефинисаним безбедоносним критеријумима.

Страх од детекције ЕМЕ са рачунара временом је постао све већи са развојем модерних средстава за регистровање ЕМЕ високе осетљивости (*state-of-the-art equipment*), без обзира на све већу употребу оптичког кабла као преносног медија (слабо зрачење ЕМЕ), као и вишеструке модулације и мултиплексере, за потребе заштите информације. Зато је неопходно да се у раду са осетљивим информацијама на рачунарима примењују следеће превентивне мере:

– спречавати физичко присуство неовлашћених лица близу рачунара који су у раду и зраче ЕМЕ,
– обезбедити за рад рачунаре који су заштићени у складу са ТЕМПЕСТ стандардом на посебно осетљивим местима, ради смањења или елиминисања отицања службених података,
– смањити ниво снаге која се користи у раду појединих рачунарских компоненти.

При томе, треба водити рачуна да се цена опреме за пријем сигнала путем емитоване ЕМЕ креће у распону од 5.000 до 250.000 долара (зависно од јачине сигнала и удаљености са које треба да буде детектована). С друге стране, цена опреме за заштиту рачунарских компоненти према ТЕМПЕСТ стандарду такође је различита (зависи од процене са које дистанце се очекује неовлашћено праћење рада рачунара), али је вишеструко мања и корисна, јер се могу избећи нежељене последице.

Један од начина да се заштити приступ рачунарима јесте непрекидна употреба квалитетних и ажурних антивирусних програма (АВП). Антивирусни програм или антивирус је рачунарски програм који се користи за заштиту, идентификацију и уклањање рачунарских вируса, као и сваког другог софтвера који може да оштети или нанесе штету оперативном систему рачунара. За разлику од првобитних антивируса који су били базирани искључиво на тре-

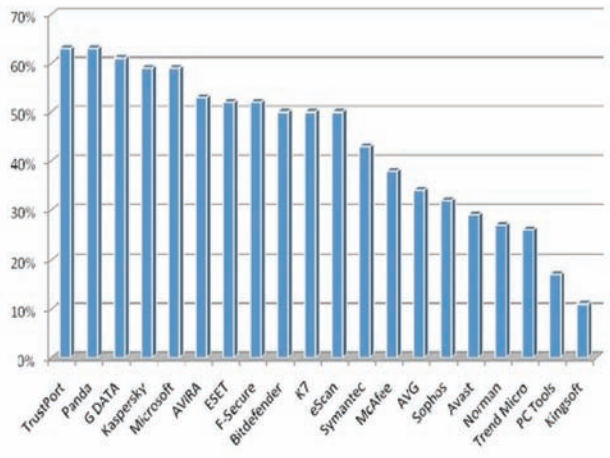
тирању рачунарских вируса, модерни антивирусни програми израђују се тако да систем штити од што већег броја различитих могућих малвера, као што су црви, фишинг напади, бекдор, руткит и тројанци.[18]

Почеци заштите рачунара били су у спречавању тада познатих вируса. Радили су по принципу проналаска и брисања фајлова из одређене датотеке (фолдера), наводећи корисника рачунара на редослед команди које треба да уради ради његовог брисања. Међутим, касније су вируси почели да мењају начин смештања на рачунару и постали су савршенији, тако да је њихово проналажење веома тешко. Зато се у антивирусе уграђује алгоритам, који по понашању одређеног фајла процењује да је то вирус и пријављује га кориснику, нудећи му опције брисања, смештања у карантин (изолације), ради његовог детаљнијег испитивања, јер постоје вируси који се активирају када се покуша њихово брисање.

Постоји велики број АВП програма (слика 13), који се могу снимити са неких од понуђених сајтова и платити електронским путем (што може да буде осетљиво због укуцавања и достављања података електронским путем) или се могу купити у некој од специјализованих наменских продавница које се баве продајом комерцијалних АВП програма.

Постоје и заштитни или спајвер програми, који чувају важне корисникове податке од неовлашћеног приступа других, спречавају улазак у компјутер и приступ одређеним интернет страницама, као и

[18] Прво уклањање једног рачунарског вируса извршено је 1987. године софтвером Бернт Фикс, а радило се о једном од првих вируса - Виена.



Слика 13 – Преглед најчешће коришћених комерцијалних АВП програма .

покретање разних апликација. Многи од тих система данас су интегрисани у *windows* и друге оперативне системе.

Закључак

Све што је наведено о техникама и активним или пасивним средствима за извиђање рачунара, само су основне информације приказане о овој делатности. У циљу стицања детаљног сазнања, а због могућег утицаја сајбер активности на безбедност информационо-комуникационих система појединих важних институција и самим тим националну безбедност државе, овој области потребно је посветити више пажње.

Литература:

[1] Интернет сајт: *Sajber Komanda SAD*, октобар 2010.

[2] Интернет сајт: *Microsoft – један од кривaца за хакерски напад на Google,* 15. јануар 2010.

[3] Интернет сајт: *TEMPEST*, октобар, 2010. [4] Интернет сајт: Malicious program and viruses,фебруар 2010.

[5] Markus G. Kuhn, Ross J. Anderson*: Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations?,* септембар 2001.

[6] Markus G. Kuhn: *Electromagnetic Eavesdropping Risks of Flat-Panel Displays*, допуна рада из 2008. године.

[7] Wim van Eck: *Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?,* Холандија, септембар 2010.