CENTER FOR SECURITY RESEARCH
DEPARTMENT FOR LAW ENFORCEMENT RESEARCH

НЕОВЛАСТЕНО НАВЛЕГУВАЊЕ ВО КОМПЈУТЕРСКИ СИСТЕМ - АСПЕКТИ НА МЕЃУНАРОДНА СОРАБОТКА ВО ОБЕЗБЕДУВАЊЕТО НА ЕЛЕКТРОНСКИ ДОКАЗ

м-р Оливер Ристески

Компјутерскиот криминал денес претставува феномен со глобални димензии, кој што не познава национални граници. Неговите извршители имаат мултинационален пристап во извршувањето на компјутерските кривични дела. Во најголем дел од случаите на неовластено навлегување во компјутерски систем, извршителите го извршуваат кривичното дело од една држава, а жртвата односно штетета настанува во друга држава. Меѓународната полициска соработка е од клучно значење за криминалистичката истрага за КД од областа на компјутерски криминалитет бидејќи во голем дел од извршените кривични дела сторителите, односно оштетените можат да бидат надвор од Р. Македонија. Во овие случаи најчесто станува збор за спроведување на заедничка криминалистичка истрага бидејќи во најголем дел податоците – електронските докази што се предмет на истрагата се наоѓаат на сервери кои се наоѓаат во странство и секое одлагање или одолговлекување на истрагата може да доведе до нивна промена или бришење со што сторителите вешто би ја избегнале правдата и нивното откривање и докажување би било многу тешко. Со дигиталната форензика се обезбедуваат електронски докази во една легална постапка кои што претставуваат причинско – последична врска помеѓу жртвата и извршителот, но оваа врска е посредна, односно индиректна преку интернет сервис провајдерот, кој што вообичаено се наоѓа надвор од Р. Македонија. Ова значи дека од обезбедените електронски докази криминалистичката истрага потребно е да се прошири и притоа кривично да се процесуираат извршителите согласно меѓународното кривично право и меѓународната легислатива во делот за компјутерски криминал (националното законодавство – Законот за меѓународна соработка во кривичната материја , Конвенцијата за компјутерски криминал , Европска конвенција за меѓусебна правна помош во кривичната материја , Европска спогодба за пренос на барањата за правна помош).

Меѓународната полициска соработка подразбира размена на информации од безбедносен карактер, но овие информации не претставуваат доказ во доказните постапки, согласно меѓународното кривично право.

Меѓународната правна помош претставува легален механизам при процесуирањето на извршителите на компјутерските кривични дела, особено во делот на кривично процесната материја. Форензички обезбедените електронски докази кај жртвата, потребно е во легална постапка да бидат процесуирани до матичната држава каде се наоѓа осомничениот и доколку е потребно криминалистичката истрага да се прошири во делот на обезбедување на други електронски и материјални докази кои ќе се искористат во законита постапка за докажување на извршителите на овие кривични дела пред суд.

Вообичаено кај кривичното дело „Оштетување и неовластено навлегување во компјутерски

систем“ во случај кога електронските докази укажуваат на фактот дека сторителот го извршил кривичното дело надвор од Р. Македонија, на пример со форензичката анализа на електронски податоци од оштетениот се добива IP адреса од интернет сервис провајдер (ISP) кој се наоѓа надвор од Р. Македонија, тогаш потребно е да побараме од провајдерот во една легална постапка согласно меѓународното кривично процесно право да бидат „замрзнати“ податоците, а потоа и доставување на информациите за IP адресата/ите, логови, време и др. информации од осомниченият. Без разлика од било каде во светот да е извршено кривичното дело, сепак неовластениот упад во компјутрескиот систем од оштетениот остава некаква дигитална трага која што е линк со осомниченият направен директно или индиректно преку интернет сервис провајдерот (ISP). Од информациите кои ги поседува провајдерот се добива идентитетот на осмниченият. Во целата оваа постапка на меѓународна соработка неопходно е обезбедувањето на електронските и материјалните докази да биде согласно законската легислатива со цел докажување на кривичното дело и неговите сторители пред надлежните судови. Во случај кога е потребно неодложно постапување согласно членот 35 од Конвенцијата за компјутерски криминал сите земји потписнички се должни „да назначат лица за контакт кои ќе бидат на располагање дваесет и четири часа на ден, седум дена неделно“ . Ова е потребно за да се обезбеди давање на неодложна помош заради криминалистичка истрага или кривични постапки во врска со кривични дела поврзани со компјутерски системи и податоци, односно обезбедување и складирање на електронски докази. Секоја земја потписничка на Конвенцијата е обврзана да спроведи повеќе мерки и активности, доколку тоа е допуштено со нивното домашно законодавство и практика, и тоа :

1. Давање на технички совети;

2. Зачувување на податоци во согласност со членовите 29 и 30 од Конвенцијата;

3. Прибирање докази, обезбедување на правни информации и лоцирање на осомничени лица.

Ова претставува многу важен дел од легален аспект овозможувајќи делотворно и ефикасно работење при истраги кои се однесуваат на компјутерски кривични дела кои содржат елемент на електронски докази во повеќе јурисдикции.

Барање за меѓународна правна помош, согласно Законот за меѓународна соработка во кривичната материја може да побара Јавниот обвинител и Судијата на претходна постапка, преку Министерството за правда доправно лице кое се занимава со информатички услуги со седиште во странство - интернет сервис провајдер. При поднесувањето на барањето за доставување на компјутерски податоци, Јавниот обвинител не може директно да му се обрати на интернет сервис провајдер со седиште во странство, бидејќи потребно е постапката да се спроведе преку Секторот за компјутерски криминал и дигитална форензика при Министерството за внатрешни работи. Барањата треба да се поднесат согласно процедурата за меѓународна правна помош. Јавниот обвинител потребно е да изготви барање за меѓународна правна помош до странскиот интернет провајдер од кој се бараат податоците и да издаде и наредба до Секторот за компјутерски криминал и дигитална форензика. Со барањето за

доставување на компјутерски податоци од интернет сервис провајдерот со седиште надвор од Р. Македонија може да се побараат да се достават следните видови на информации:

- Логови и IP адреси од осомничениот, податоците кои се бараат потребно е да содржат точен час, датум, како и временска зона;

- Податоци за претплатникот – информации за идентификација на корисникот на одредена IP адреса, која с екористи од страна на осомничениот;

- Податоци за интернет сообраќај - датотеки со логови каде се евидентирани активности на оперативниот систем на одреден компјутерски систем или на друг софтвер или на комуникации помеѓу компјутери, особено на изворот и дестинацијата на пораките;

- Податоци за содржина – тука спаѓаат пораки, слики, филмови, музика, документи и сл.

Постапката за барање и обезбедување на компјутерски податоците од странски интернет сервис провајдери (ISP), во зависност од провајдерот е регулирана во нивните безбедносни протоколи за соработка со институциите. Во САД, како земја со најмногу развиена информатичка технологија, Интернет сервис провајдерите согласно сегашната законска регулатива имаат надлежност директно да соработуваат со претставници на институциите од други држави, вклучувајќи ја и Р. Македонија и истовремено и да ги обезбедат компјутерските податоци побарани по сите точки од барањето за нивните корисници. Оваа соработка во САД според федералните закони не е облигаторна, односно соработката меѓу ISP и институциите е на доброволна основа. Вообичаено се добиваат позитивни одговори за оние барања за кои нивните експертски правни тимови сметаат дека треба да бидат обезбедени податоци. За останатите земји во светот истотака се применува механизмот за меѓусебна правна помош, а во зависност од националното законодавство и безбедносните протоколи од ISP и приложените докази кон барањето за меѓународна правна помош, повратно се добиваат и потребните компјутерски информации. Поголемите интернет провајдери од кои најчесто се обезбедуваат компјутерски информации имаат свои безбедносни протоколи за соработка со Law enforcement кои ги објавуваат на официјалните веб страни. Во зависност од безбедносните политики (Facebook, Google, Microsoft и Yahoo), можат да бидат побарани од нашите надлежни органи (МВР, ЈО, Судија на претходна постапка и МНР) да бидат електронски податоци и истите по целосно комплетирање на барањето да бидат доставени до наште органи со цел обезбедување на несоборливи електронски докази, а со тоа и процесуирање на сторителите на овие кривични дела.

Меѓународната полициска соработка и меѓународната правна помош се клучни во сузбивањето на компјутерскиот криминалитет бидејќи е мултинационален криминал за кој не постојат национални граници и само со градење на безбедносни капацитети од мултинационален карактер може сериозно да се одговори на меѓународниот компјутерски криминал.

ЕЛЕКТРОНСКИ (ДИГИТАЛЕН) ДОКАЗ

Традиционално и историски гледано доказната постапка и докажувањето се темели на докази, доказите се во физички облик, тие можат да бидат документи, фотографии, предмети, итн. Доказите што се користат во судските постапки, а кои произлегуваат од електронските уреди како што се компјутерите и нивните периферни уреди, компјутерски мрежи, мобилни телефони, дигитални камери и друга преносна опрема вклучувајќи ги и уредите за чување податоци (USB меморија, SD картици и сл.) како и од интернет, се форми на електронски докази. Всушност електронскиот доказ претставува збир на податоци што се наоѓа или пренесува во електронска (дигитална) форма и како таква може да се користи во судска постапка.

Дефиницијата согласно Упатството за електронски докази на Советот на Европа гласи:

„Секоја информација генерирана, меморирана или пренесена во дигитална форма која подоцна може да биде потребна за докажување или недокажување на факти кои се оспоруваат во правна постапка претставува електронски доказ.“

Обезбедувањето, обработката и употребата на електронските докази во Р. Македонија согласно Законот за кривична постапка е регулирано во чл. 250- Докажување со снимка, од Законот за кривична постапка.

(1) Фотографии, филмови или други аудио или визуелни снимки добиени со

технички средства може да служат како доказ во кривичната постапка.

(2) Во однос на снимката се постапува како и со другите предмети кои можат да се употребат како доказ, водејќи сметка да не се оштети или уништи и да се сочува нејзината содржина во неизменет облик. По потреба ќе се преземат потребни мерки за да се зачува снимката во неизменет облик или да се изработи нејзина копија.

(3) Доколку поинаку не е пропишано со овојзакон, содржината на снимката се утврдува со нејзино репродуцирање. Снимката ја репродуцираат стручни лица.

и во Член 251 „Електронскидоказ “ .

За прибавување на електронски доказ се применуваат одредбите од членовите 198 и 199 на овој закон, доколку поинаку не е определено со овој закон .

Одредбите од членот 198 се однесуваат на „Привремено одземање на компјутерски податоци“, а во случај на жива форензика се применуваат и одредбите од членот 184 „Пребарување на компјутерски систем и компјутерски податоци“ .

Карактеристики на електронските докази се:

- Лесно можат да се манипулираат (променат или избришат);
- Можат да се променат автоматизирано после одземањето;

- Не секогаш се наоѓаат на местото на извршување на кривичното дело „Оштетување и неовластено навлегување во компјутерски систем“;

- Потребни се посебни начини и процедури за обезбедување, одземање, обработка и складирање на електронските докази;

- Потребно е навремено, соодветно и легално постапување со електронските докази;

Извори на електронски докази можат да бидат електронските уреди и опремата која може да се поврзе со електронски информации, како што се електронски уреди, опрема, софтвер, хардвер, или друга ИТ технологија која може да функционира независно, заедно или поврзана со традиционалните компјутерски системи. Електронските уреди кои се користат за да се подобри пристапот на корисникот и да се зголеми функционалноста на компјутерскиот систем, значи дека бројот и видот на ИТ уредите кои може да содржат електронски докази секојдневно се зголемува. Тука спаѓаат: надворешно куќиште на печатена плоча, микропроцесори, хард дискови, меморија и конектори за други уреди, монитор или друг уред за прикажување, тастатура, глушец, надворешно поврзани единици, периферни уреди, софтвер, печатари, скенери, рутери, надворешни хард дискови и други уреди за зачувување, таблети, мобилни телефони, дигитални фото апарати, камери за видео надзор и др.

Електронските докази според видот на податоците кои што ги содржат можат да бидат :

- Статистички податоци
- Живи податоци (меморија и сервери)
- Интернет податоци

Барањата од безбедносните институции секоја софтверска компанија ги зачувува во делот на извештајот за транспарентност.

Legal Process 129

Emergency Requests 0

Total Requests 129

Users/Accounts Requested 159

% of Requests Where Some Data Produced 51.0%

Request Types Emergency Requests 0 0.0%

Legal Process 129

100.0%

% of Requests Where Some Data Produced

Emergency Requests

0%

Legal Process

51.0%

Превземено од Transparency report from facebook

Исто така постои и можност во случај на итност (Emergency request), кога е неопходно брзо и експедитивно постапување да се побара „замрзнати“ - зачувување на податоците кои што можат да послужат какоелектронски доказ во кривична постапка. Во зависност од сервисот барањата за итно постапување се испраќаат од страна на службеник од Law enforcement најчесто полициски службеник од Секторот за компјутерски криминал и дигитална форензика до ISP, детално се дава опис на кривично правниот настан и што се бара да биде зачувано, а потоа се комплетира постапката за меѓународна правна помош и се пушта официјално барањето за добивање компјутерски информации преку Министерство за правда.

МЕЃУНАРОДНА ПОЛИЦИСКА СОРАБОТКА - ИНТЕРПОЛ

Интерпол е меѓународна полициска организација со седиште во Лион, Франција, чија што основна цел е меѓународна полициска соработка во делот на превенција и борба против меѓународниот и националниот криминал. Компјутерскиот криминал не познава национални граници и има мултинационален карактер од аспект на извршување на кривичното дело од една држава, а настанување на последиците и штетата во друга држава. Интерпол овозможува меѓународна полициска соработка меѓу полициските службеници кои работат на спроведување на законот да можат преку интерпол безбедно да комуницираат, да споделат и добијат клучни полициски информации секогаш кога е потребно, обезбедувајќи ја безбедноста на граѓаните во светот. Визија на интерпол е „Поврзување на полициите за побезбеден свет“, а неговата мисија е „Превенција и борба против криминалот, преку зајакната соработка и иновација во полициските и безбедносните работи“

Соработката помеѓу криминалистичките служби во светот е од круцијално значење, бидејќи со напредокот на информатичкото општество и интернетот целиот свет комуницира како една мала единка за која не постојат национални граници, посебно за кривичните дела од областа на компјутерски криминалитет. Затоа е потребна современа меѓународна стратегија во превенцијата и репресијата против меѓународниот компјутерски криминалитет. При неовластеното навлегување во компјутерски систем, покрај меѓународната правна помош, претходно е потребно размена на безбедносно разузнавачки информации меѓу криминалистичките полиции, со цел сузбивање на организиран компјутерски криминал каде што интернет сервис провајдерите се во една земја, оштетените во друга, а извршителите се наоѓаат во трета. Меѓународната полициска соработка опфаќа безбедна комуникација, директен пристап до полициските евиденции, навремено ажурирање на информатичките

бази со податоци со криминалистички информации и градење на капацитети од областа на безбедноста. Секоја земја членка на Интерпол има свои национални централни бироа (НЦБ) преку кои се одвива комуникацијата со останатите НЦБ од земјите членки на Интерпол и со генералниот секретаријат на Интерпол. Во состав на НЦБ Интерпол – Скопје функционира и отсекот за компјутерски криминал, кој се занимава со меѓународна полициска соработка од областа на комјутерски криминал и дигитална форензика.Компјутерскиот криминал на светско нивое брзорастечки криминалкој што се развива пропорционално со развојот на информатичката технологија. Криминалците вешто ја користат брзината, удобноста и анонимноста на интернетот за да извршат разновидни криминални активности кои не знаат за национални границите, физички или виртуелни, притоа предизвикувајќи сериозна штета и претставуваат реална закана засите кои ја користат информатичката технологија и интернетот. Улогата на ИНТЕРПОЛ во делот на меѓународната полициска соработка од областа на компјутерски криминал се состои од :

- Оперативна и криминалистичко - истражна поддршка
- Сајбер разузнавање и анализа
- Дигитална форензика
- Иновации и истражување
- Градење на капацитети
- Национални сајбер критики

Глобалниот комплекс за иновации на Интерпол претставува глобално координативно тело за откривање и спречување на дигитални злосторства. Глобалниот комплекс за иновации е најсовремен истражувачки и развојен центар, кој е отворен во 2014 година, со цел да ја унапреди превенцијата и борбата против комјутерскиот криминалитет, преку научно истражување, дигитално форензички експертизи и развој на нови иновативни полициски алатки.

ПОЛИЦИСКА СОРАБОТКА ВО ЕВРОПСКИТЕ ЗЕМЈИ - Европол

Европол е меѓународна полициска агенција со седиште во Хаг, Холандија во состав на Европската унија чија што основна цел е сузбивање на меѓународниот сериозен и организиран криминал и тероризам.Европол има надлежност во делот на откривање и обезбедување на докази за сериозни кривични дела и лоцирање на нивните извршители кои што имаат мултинационален карактер, во делот на меѓусебна соработка притоа користејќи современ информатички систем за размена на криминалистичко разузнавачки информации со цел подобрување на соработката на безбедносните служби на земјите членки на ЕУ. Основни задачи на Европол се:

- Собирање, чување, обработка, анализа и размена на податоци и разузнавачки информации;

- Известувања до надлежните органи на земјите-членки за информациите што ги засегаат и за сите откриени врски меѓу кривичните дела;

- Помош за истраги во земјите-членки, особено преку доставување на сите релевантни информации до националните единици;

- Повикувања до надлежните органи на засегнатите земји – членки да започнат, водат или координираат истраги и предлози за основање заеднички истражни тимови во посебни случаи;

- Обезбедување разузнавачка и аналитичка поддршка на земјите-членки во врска со големи меѓународни случаи;

- Подготовка на проценки на закани, стратешки анализи и извештаи за општи ситуации поврзани со неговата цел, вклучено проценки на закани од организиран криминал.

Според најновата проценка на закани од интернет-Organised Crime Threat Assessment (IOCTA) , компјутерскиот криминал станува поагресивен и економски исплатлив. Ова може да се види во најновите појавни облици на различни форми на компјутерски криминал, вклучувајќи и оштетување и неовластено навлегување во компјутерски систем.Компјутерскиот криминал претставува поголем проблем како криминолшки феномен во земјите на ЕУ, бидејќи имаат современо информатичко општество со добро развиена интернет – инфраструктура, во кое административните, дипломатските, безбедносните, одбранбените, банкарските и останати социо – економски услуги граѓаните ги извршуваат преку интернет online системите. Овие електронски комуникации вклучуваат лични податоци, банкарски информации и доверливи владини класифицирани информации кои се често мета на неовластено навлегување во компјутерски систем. Поголем безбедносен пропуст ЕУ доживува моментално затоа што хакери со години имале пристап до комуникацијата на дипломатите на ЕУ.

Во состав на Европол во 2013 година е формиран Европскиот центар за сајбер криминал - European Cybercrime Centre (EC3), со цел зајакнување на информатичката безбедности откривање и докажување на новите форми на компјутерски криминал во ЕУ. Во составот на EC3 постојат три оддели и тоа, оддел за стратегија, оддел за дигатална форензика и оддел за операции. Според Проценката на закани од интернет (IOCTA), во којае образложено колку е широк и разновиден спектарот на компјутерски криминал и како EC3 е клучен дел од Европол во борбата против компјутерскиот криминал. Криминалните активности од областа на компјутерски криминал вклучуваат:

- Користејќи botnets—networks на уреди кои се заразени со малициозен софтвер без знаењена корисниците - да пренесуваат вируси кои добиваат недозволена далечинска контрола врз информациско комуникаските уреди, крадат лозинки и оневозможуваат антивирусна заштита;

- Создавајќи “back doors”на компромитираните уреди за да се дозволи кражба на пари и

лични податоци или далечински пристап до уредите за креирање на ботнет мрежи;

- Создавање онлајн форуми за трговија со хакирани податоци;
- Хостинг и создавање контра - антивирусни услуги;
- Перење традиционални и виртуелни валути;
- Online измама, како на пример преку системи за плаќање на интернет и социјално инженерство;
- Разни форми на online сексуална експлоатација на деца, вклучително и дистрибуција на online материјали за сексуална злоупотреба на деца и пренос на сексуална злоупотреба на деца во живо;
- Online хостирање на операции кои вклучуваат продажба на оружје, лажни пасоши, фалсификувани и клонирани кредитни картички, дроги и услуги за хакирање.
- Malware или малициозен софтвер, добива контрола над компјутерскиот систем или мобилен уред за кражба на вредни информации или оштетување на податоци. Постојат многу видови на малициозен софтвер и тие можат да се надополнуваат еден со друг при извршување на напад.
- Ботнет (или роботска мрежа) е составен од компјутери кои комуницираат едни со други преку интернет. Командниот и контролниот центар ги користи за испраќање спам, подигање на дистрибуирани напади на DdoS.
- Rootkit е збирка на програми кои овозможуваат пристап до администраторски пристап до компјутер или компјутерска мрежа, со што се овозможува на напаѓачот да добие root или привилегиран пристап до компјутерот и можеби други компјутерски уреди на истата мрежа.
- Worm се реплицира преку компјутерска мрежа и врши злонамерни акции без упатства.
- Тројанец претставува легитимна програма, или е вградена во неа, но е дизајнирана за злонамерни цели, како што се шпионирање, крадење податоци, бришење на датотеки, проширување на ботнет и изведување DDoS напади.
- Преносник на датотеки ги инфицира извршните датотеки (како .exe) преку нивно презапишување или внесување на инфициран код кој ги оневозможува.
- Backdoor/remote-access Trojan (RAT) пристап до компјутерски систем или мобилен уред од далечина. Може да се инсталира од страна на друго парче од малициозен софтвер. Таа им дава речиси целосна контрола на напаѓачот, кој може да изврши широк спектар на акции, вклучувајќи:

-мониторинг активности

-извршување на команди

-испраќајќи ги датотеките и документите назад кон напаѓачот

-најавување на тастатурата

-преземање снимки на екранот

- Ransomware ги спречува корисниците да пристапуваат до нивните уреди и бара од нив да платат откуп преку одредени методи на плаќање преку интернет за да го вратат пристапот.
- Scareware е лажен анти - вирусен софтвер кој претендира да скенира и да најде малициозни / безбедносни закани на кориснички уред, така што тие ќе платат за да го отстранат.
- Spyware е инсталиран на компјутер без знаење на сопственикот да ја следи нивната активност и да ги пренесува информациите на трети лица
- Adware прикажува рекламни банери или скокачки прозорци кои вклучуваат код за следење на однесувањето на корисникот на интернет

Меѓународната полициска соработка (Интерпол, Европол) и меѓународната правна помош се од круцијално значење за меѓународните криминалистички истраги во сузбивањето на компјутерскиот криминалитет кој по самата феноменологија има меѓународна компонента во најголем дел од неговите појавни облици. Затоа е потребен мултинационален пристап, односно користење на сите легални механизми во меѓународната полициска и правна помош и само со градење на безбедносни капацитети од мултинационален карактер може сериозно да се одговори на предизвиците од меѓународниот компјутерски криминалитет.