Електронен подпис и четец ви пазят от хакери

След ударите през лятото кредитните институции започнаха да ги въвеждат

Така изглеждат картите с чип и четците, които пазят сертификата от хакери. Четците с клавиатура спасяват и ПИН-а на човек. СНИМКА: АГНЕС АСЕНОВА

ГАНЕТА СТОЯНОВА

Най-добрата защита срещу източване на данни от персоналния компютър е ползването на електронен подпис или на сертификат с хардуерна защита, обясниха специалисти. Точно това препоръчват и от ГДБОП на банките и повечето от тях вече въвеждат този начин на работа. Досега

банките масово издаваха сертификати, които са във вид на ключов файл,

защитен с ПИН, който трябва да се инсталира в компютъра.

Хакерите обаче ползват вируси от типа "Троянски кон", с които влизат в РС-то на човек и само чакат нужната информация да се появи - в случая потребителско име, парола, ПИН и самия ключов файл със сертификата за електронно банкиране. Щом вирусът докопа тази информация, я предава на мошеника и той може да си нарежда преводи в своя полза, защото откраднатата информация го идентифицира онлайн пред банката.

Банките не пропускаха да предупредят клиентите си да се пазят от "троянци", като не отварят имейли от непознат адрес, да не влизат в сайтове, които нямат знак за сигурност, да не запаметяват потребителски имена и пароли в браузъра си, да актуализират антивирусните си програми и др. Но дори човек стриктно да спазва тези мерки,

няма гаранция, че „Троянският кон“ няма да се промъкне

"Дори да обновяваш антивирусната си програма ежедневно, няма гаранция. Програмата може да е писана за конкретния удар. Може и да е нова и SYMANTEX (водеща антивирусна компания) да не знае още за нея", обясни водещ специалист по компютрите. Според него дори сертификатът да е на диск или на USB и да се пуска само при работа с банката той пак влиза в РС-то и вирусът го прехваща.

Ето защо най-сигурното разрешение е поверителната информация да не влиза в компютъра. Това се постига с ползването на универсален електронен подпис, който се издава върху смарт карта и може да се използва за други публични услуги - на НАП, НОИ и др. Сигурност се постига и чрез сертификат, издаден от банка, но отново на карта с чип.

Сертификатът работи с два ключа - частен и публичен, генерирани в смарт картата. Частният ключ обаче никога не излиза от него! Той служи за създаване на електронния подпис в картата, достъпът до която е със специални карточетци. Така

крадците няма как да стигнат до чипа,

а без тази информация нищо не могат да направят.

Четците пък са с клавиатури и без. Едните струват към 90 лв., другите около 20. При по-модерните крадците няма да ви вземат ПИН-а. Но дори това да стане, все пак сте защитени, защото картата е у вас! Мошениците не могат да ви източат парите, тъй като само ПИН без частен ключ не върши работа - трябва да ви откраднат и смарт картата.

Троянски кон...

(Продължение от 13-а стр.)

Според Колев, след като троянският кон вече е проникнал и заразил компютъра и бандитите са се сдобили с личните данни, потребителското име и цифровия сертификат, необходим за оторизация при интернет банкирането, могат да се извършват неправомерни транзакции от сметките на клиентите на банките.

След това предимно чрез интернет се набират хора, които се използват за "мулета", "финансови агенти" или човешки "проксита". Те са зарибявани да изкарват лесни пари

чрез обяви в различни интернет сайтове за работа

Част от посредниците се намират и в сайтове за запознанства - най-вече руските www.mamba. ru. и www. rambler.ru. На жадните за лесна печалба хора, които обикновено са със затруднено материално положение, им се предлагат онлайн договори за извършване на дейност като "финансови агенти".

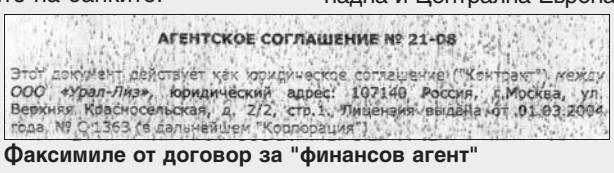
Задълженията им включват откриване на банкова сметка на тяхно име в някои от финансовите институции у нас. Според договора, който сключват, те трябва да получават пари в сметката си, след което да ги превеждат чрез офиси на фирми за парични преводи - Western Union и Money Gram.

Антимафиотите са установили, че всички отмъкнати пари от банкови сметки на българи са били изпратени до офисите на двете компании на територията на Русия, а получателите са хора с руски имена. За финансовия агент остава комисиона, която обикновено е 10% от изпратените пари.

"24 часа" разполага с един такъв договор за финансов агент, предлаган по интернет от фалшивата компания Ural Liz с офис в Москва на ул. "Верхняя Красноселская".

В точка 2 от "споразумението за наемане на агент" се казва, че " независимо от резултата от посредническите услуги, оказвани на корпорацията, агентът участва само в законна дейност, която се състои в получаване на депозити по открити в България банкови сметки и последващи транзакции на сумите към корпорацията чрез "Уестърн Юнион", като удържа част от сумата като комисиона".

"До момента ГДБОП е установила шест фалшиви руски компании, които наемат наши "мулета" за изпращане на крадени пари в Русия. Освен Ural Liz това са още Local Solutionsq FFK Stone, E-Trans, при нея е използвано името на съществуваща руска компания за дърводобив, Clobal Chariti и Premium Finance Company. Тези компании са публикували обявите си за работа в интернет освен у нас и в много страни от Западна и Централна Европа.



АГЕНТСКОЕ СОГЛАШЕНИЕ № 21-08

Этот документ действует как юридическое соглашение("Контракт") между ООО «Урал-Лиз», юридический адрес: 107140 Россия, г.Москва, ул. Верхняя Красносельская, д. 2/2, стр.1. Лицензия выдана от 01.03.2004 года. № С-1363 (в дальнейшем "Корпорация")

Факсимиле от договор за "финансов агент"

Така кръгът на измамата се затваря. Парите, изтеглени от банковите сметки на неподозиращи нищо клиенти, отиват в сметката на "мулето", а оттам в Русия.

Антимафиотите засичат още, че IP адресите на компютрите, от които са извършвани неправомерните транзакции, са от адресното пространство на български интернет доставчици.

Използваните компютри са "пробити", като са превърнати в т.нар. зомбирани компютри. Хората, клиентите на доставчиците на интернет, нямат представа, че компютрите им се използват за неправомерни банкови транзакции. Според жаргона в мрежата "зомбиран" компютър е машина, инфектирана от програма, която разпраща спам

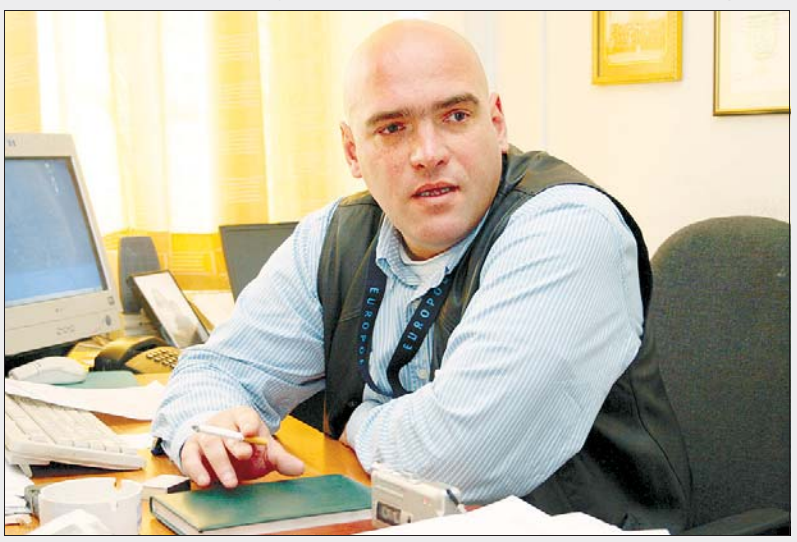
без знанието на собственика на компютъра

Нашите "мулета" всъщност са бушони, които се използват веднъж или най-много два пъти. И да бъдат заловени, веригата към измамниците се къса, коментират антимафиоти.

"Благодарение на усилията на банките и ГДБОП успяхме да възстановим над 50% от откраднатите суми. Освен това пресякохме много опити за източване на пари. Пикът на тези измами бе през юни-юли т.г. След активно съдействие от банките измамите с електронно банкиране са спрени. Надявам се след публикациите в медиите т.нар. "мулета" да не пристъпват към такива сделки, защото те са съучастници в престъпления и ще носят наказателна отговорност.

Досега сме стигнали до всички тях и който се е хванал, винаги е бил задържан", заяви Явор Колев.

За борба с измамите ГДБОП търси съдействие от руските служби и Интерпол. Ако хората се съмняват за финансови измами в интернет, могат да сигнализират на новия сайт **www. cybercrime.bg**.



Шефът на отдел "Компютърни престъпления" в ГДБОП Явор Колев предупреждава българите да не се подлъгват от бърза печалба от интернет измамниците.

СНИМКА: "24 ЧАСА"