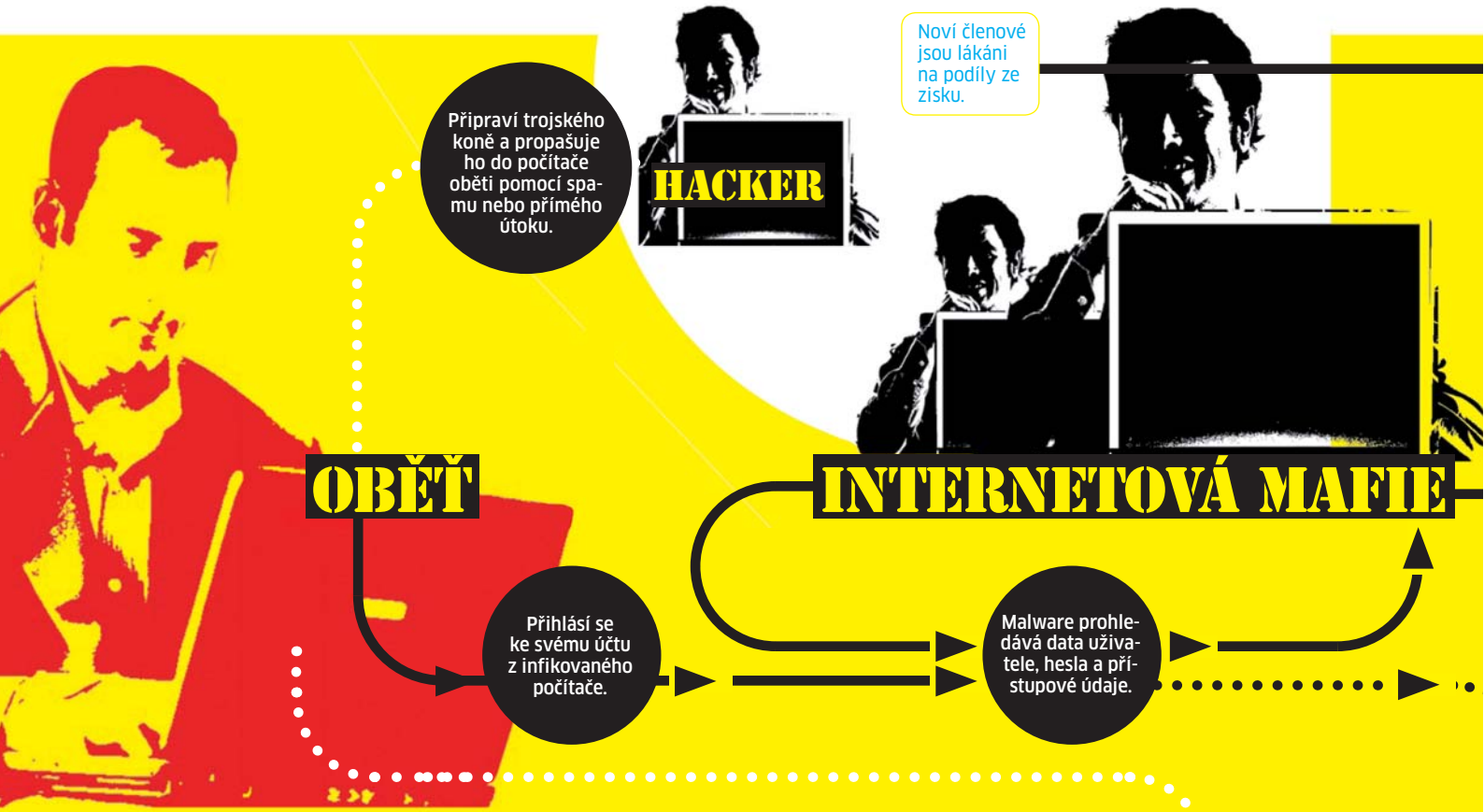


Bankovní loupež přes internet

Techniky phishingových podvodníků jsou den ze dne sofistikovanější. Dávno pryč jsou časy, kdy se používaly amatérské maily se zkomoleným textem – dnes jsou „hitem“ trojské koně, které vám **VYBÍLÍ ÚČET**, aniž byste o tom věděli…

ANDREAS HENTSCHEL

Když se řekne phishing, většina zkušenějších uživatelů se jen ušklíbne a představí si anglické či kostrbaté české dopisy amatérských podvodníků. Internetoví zločinci však nesedí s rukama v klíně, ale „pilně“ pracují na vylepšení svých technik. My vám nabídneme příběh zákazníka německé banky, kterého zjištění této skutečnosti stálo několik desítek tisíc korun.

Papírový šok: Začalo to nenápadně

19. května 2007 se Dominik Kroll z vesnice nedaleko Mnichova probíral svými bankovními výpisy, které si předchozí den vyzvedl z banky. Mladík si letmo prohlédl účetní transakce, zkontroloval pár záznamů a ještě několikrát obrátil stránky tam a zpět – stejně jako by si svůj bankovní výpis prohlížel kdokoliv jiný.

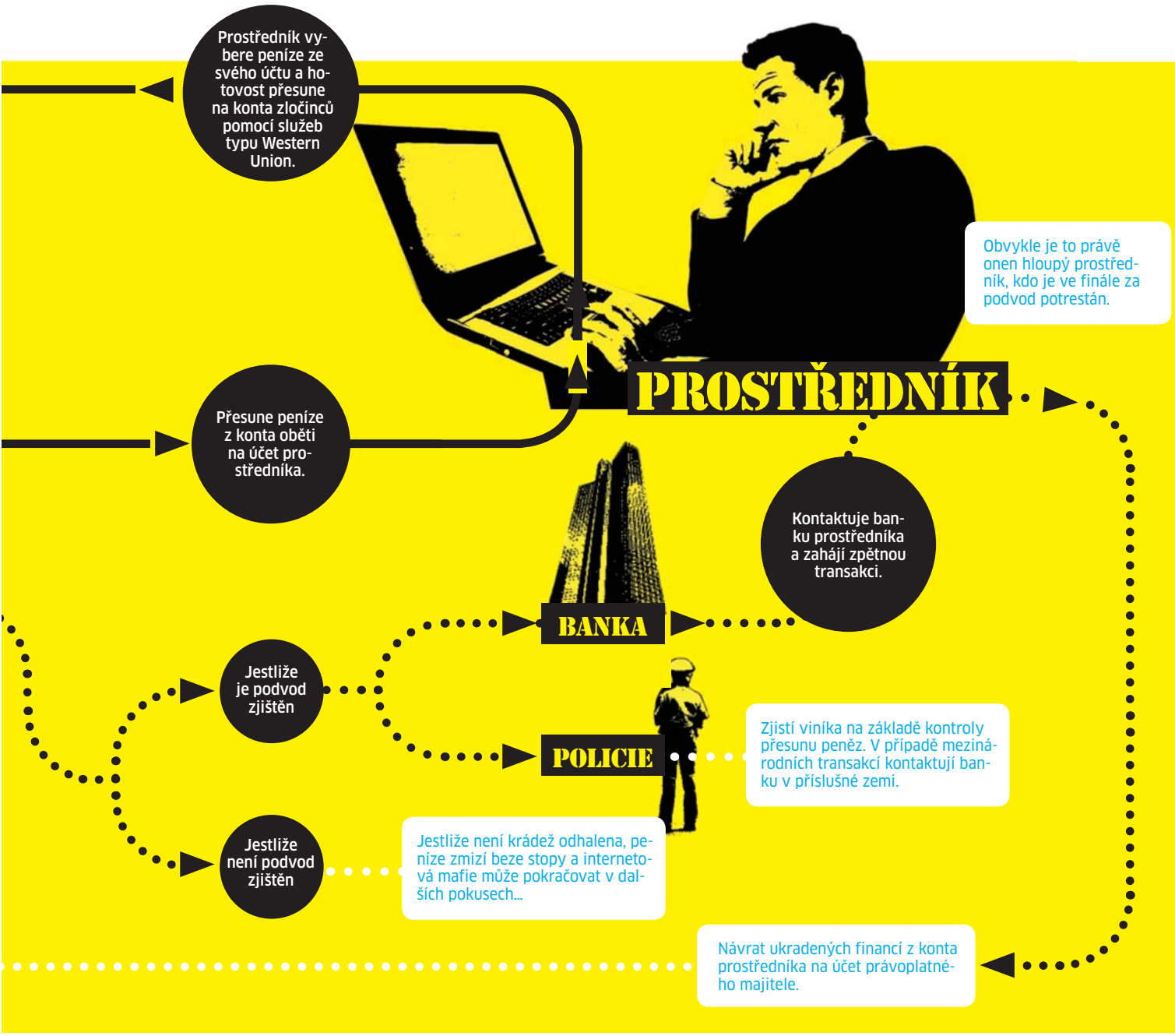
Až po chvilce upoutal jeho pozornost bankovní převod s částkou 2 117,50 eura. Příjemce: Maxim B., účet s IBAN číslem (mezinárodní číslo účtu).

Dominik Kroll neznal žádného Maxima B, výše uvedenou částku nikomu nepřevedl, a už vůbec ne do zahraničí. „Nesmysl,“ to bylo jediné, co ho v té chvíli napadlo. Dokonce i dnes, o více než jeden a půl roku později, je slovo „nesmysl“ vše, co se mu vybaví o okamžiku zjištění. Kroll ihned tušil, že jde o phishing – o tomto „problému“ slýchal poměrně často.

„Každý den jsem ve své schránce našel minimálně 20 otravných mailů,“ říká. „Samozřejmě jsem nikdy na tyto maily neodpovídal.“

Trojské koně místo mailů: Nové triky phishingových podvodníků

V sousedním Německu zaznamenal Spolkový kriminální úřad v roce 2007 přibližně



4 200 případů phishingových podvodů. Na základě této informace propočítala organizace Bitkom, že během jediného roku z účtů zmizelo přibližně 19 milionů eur, průměrně tedy přes 4 500 eur na případ. Protože údaje za minulý rok ještě k dispozici nejsou, je prozatím rok 2007 rokem rekordním. V roce 2006 bylo zaznamenáno 3 500 případů s celkovou odcizenou částkou přes 13 milionů eur. Nicméně – to jsou jen oficiální čísla – celkové množství peněz, které bylo odcizeno z bankovních kont, bude pravděpodobně mnohem vyšší. (Podobné údaje pro ČR bohužel nejsou k dispozici.)

Jasná je také další informace: Phishingoví podvodníci se přizpůsobují bezpečnostním mechanismům bank. „Doba, kdy byli neviní uživatelé lákáni pomocí mailů na podvržené stránky, které měly odhalit jejich přístupové údaje k on-line bankovnictví, jsou už dávno pryč," říká detektiv ze Spolkového kriminálního úřadu. Tuto informaci potvrdila také speciální studijní skupina z Bochumi „Ochrana identity na internetu" (BKA), která dlouhodobě zdokumentovává informace o organizovaných internetových podvodech v Německu. V roce 2007 zjistila mnohem menší počet phishingových mailů než v roce předešlém. K jejich poklesu téměř na nulu došlo až v roce 2008, poslední pokus o získání přístupu k účtu přes e-mail byl zaznamenán v únoru.

Zánik těchto primitivních žádostí o přístupové údaje není žádným překvapením. Na začátku roku 2008 přešla většina finančních institucí na modernější způsoby zabezpečení, čímž zasadily podvodným e-mailům „ránu z milosti". Jednoduché phishingové metody už na nové způsoby zabezpečení nestačily.

V současnosti se využívá především zabezpečení pomocí specifických transakčních čísel – v Německu jde o tzv. iTANy (seznamy čísel pro transakce), u nás je obvyklé vygenerování čísla bankou při transakci a zaslání ve formě SMS na mobilní telefon. Tyto novinky jsou znát i ve statistice trestných činů: až do konce října 2008 zaznamenala instituce BKA pokles phishingových útoků zhruba o 50 procent.

Avšak ani lepší zabezpečení neznamená konec phishingu. Pachatelé se k datům dostávají jinými prostředky – kouzelné slovo zní „malware". Škůdci se dostanou do vašeho počítače přes e-maily, stažené programy nebo napadením prohlížeče. Od toho momentu je už škůdce přítomen u všech on-line aktivit oběti a není pro něj problém ani přesně identifikovat uživatele. Ve většině případů si uživatel infekce ani ne-

INFO

Pět tipů, jak se bránit phishingu

DENNÍ KONTROLA ÚČTU

Své finance kontrolujte co možná nejčastěji – ideálně denně. Díky tomu můžete banku okamžitě informovat o podezřelé transakci a zahájit kroky k zablokování transakce nebo k žádosti o vrácení peněz. Čím později nelegální transakci zjistíte, tím menší je pravděpodobnost, že své peníze ještě uvidíte.

AKTUALIZACE SOFTWARU

Obvyklá a „nudná", přesto důležitá poznámka: Základem bezpečného počítače je pravidelná aktualizace softwaru a signatur bezpečnostních nástrojů. Nezapomínejte ani na svůj prohlížeč, který vám při on-line bankovnictví dělá prostředníka...

VĚNUJTE POZORNOST CHYBOVÝM HLÁŠENÍM

Při práci s internetovým bankovnictvím věnujte mimořádnou pozornost všem chybovým hlášením, která se na obrazovce objeví. Hlášení o chybně zadaném hesle může být prvním náznakem, že se děje něco neobvyklého.

NIKDY NEUKLÁDEJTE HESLA

Celá řada programů, a dokonce i některé prohlížeče vám nabízí ukládání hesel. Je to sice pohodlné, ale nikoliv bezpečné. Nikdy si takto neukládejte hesla ke svému internetovému bankovnictví ani k jiným důležitým účtům (Pay Pal, eBay...). V případě nakažení malwarem je jejich zneužití jen otázkou času.

KOMBINUJTE BEZPEČNOSTNÍ METODY

I když jednoduché a snadno napadnutelné zabezpečení přístupu a ovládání účtu pomocí samotného jména a hesla už nenabízí žádná banka, ne vždy je v základní nabídce to nejlepší zabezpečení. Pokud si nejste jisti zabezpečením svého počítače, raději si objednejte příplatkové bezpečnostní prvky. Lepší je investovat o pár korun měsíčně více, než se pak snažit získat zpět své ukradené peníze.

všimne, a tudíž neví, že svému počítači – ani jím zobrazovaným informacím – již nemůže „důvěřovat".

Perfektní načasování: Krádeže hotovosti před dlouhým víkendem

Dominik Kroll doopravdy ve svém počítači našel trojského koně. Antivir ho našel v systémové složce, maskovaného jako DLL soubor, a protokol virového skeneru ho označil jako „Spy.Banker.CKW". Ano, Spy.Banker je starý známý a podle virové databáze firmy Kaspersky pochází z Ruska. V databázi firmy F-Secure ho lze vysledovat už v roce 2005, kdy se poprvé objevil na Dálném východě, kde vykonával „špionáž" proti zákazníkům japonských bank. Očividně se stal natolik úspěšným, že na něj bylo brzy možné narazit v modifikované formě i v Evropě.

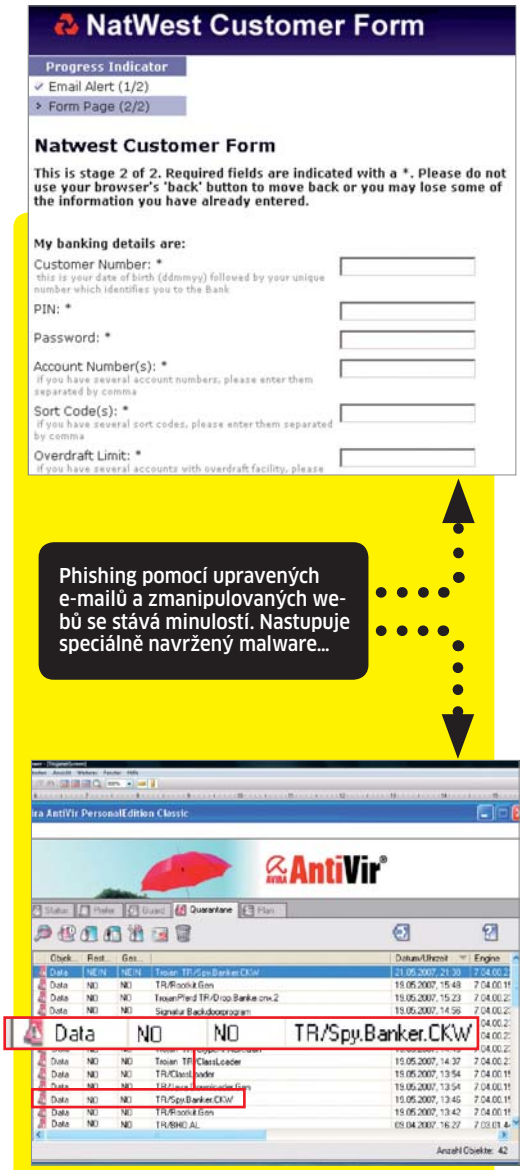
Mirko Manske z BKA považuje Spy.Banker za typický phishingový nástroj současnosti. „Pachatelé stále více spoléhají na efektivní malware, který dokáže úspěšně atakovat on-line bankovní transakce iTANu prostřednictvím manipulací v reálném čase, jako jsou útoky Man-in-the-Middle a Man-in-the-Browser."

Zde to však nekončí. Dominik Kroll je přesvědčen, že ho pachatelé sledovali již delší dobu a v taktice krádeže byl systém: přenos byl proveden ve středu 16. května 2007 a ve čtvrtek 17. května byl svátek – tedy začátek dlouhého víkendu. Tento mladý muž totiž nevěří na náhodný výběr týkající se doby výběru, a dokonce i částka, která byla ukradena, nijak nevybočuje z řady. Je zřejmé, že pachatelé znali běžný rozsah převodů na Dominikově kontě. Toto konto totiž používal ke kontrole financí hudební skupiny, ve které v té době hrál na kytaru. Účty za nástroje a vybavení, stejně jako poplatky a provize pro agentury – přes toto konto byly prováděny všechny operace. Neobvyklé tady nebyly ani částky v tisících eur. I z tohoto důvodu neupoutal záznam na bankovním výpisu o převodu 2 117,50 eura jeho pozornost hned napoprvé.

Nepřípustné: Banky jednají, jako kdyby phishing vůbec neexistoval

Okamžik, když si Dominik Kroll všiml, že jsou peníze pryč, se pro něj stal začátkem maratonu. Protože je pobočka jeho banky v sobotu zavřená, zavolal na infolinku. Tam mu poradili zablokovat své on-line konto mnohonásobným vložením falešného PIN, což neprodleně udělal. Pak poslal fax svému bankovnímu poradci.

„Abych ho co nejdříve na podvod upozornil a zahájil protiútok," říká Kroll. Byl také velice optimistický ve věci „vrácení svých peněz".



„Zloději spoléhají na efektivní malware..."

První zklamání přišlo, když zavolal na policii. Policista na lince ho vyzval, aby v pondělí ráno zašel do své banky, a řekl mu, že jediný, kdo pro něj může v praxi něco udělat, je pouze jeho banka. V pondělí ráno, hned po otevření banky, stál tedy Dominik Kroll u přepážky.

Druhé překvapení přišlo v bance: „Tvářili se, jako by se takovéhle věci nikdy nestávaly," říká Kroll. Poradce ze zákaznického servisu pro elektronické bankovnictví nebyl dostupný, proto Krolla znovu poslali na policii

U nás bezpečněji?

U našich západních sousedů hraje stále nemalou roli v zabezpečení transakcí internetového bankovnictví použití tzv. TAN kódů.

TAN kódy jsou číselné řetězce, které klient dostane v bance a které se používají pro ověření transakce. Nevýhodou této metody je ale malá odolnost vůči útoku Man-in-the-Middle.

U nás začíná v oblasti internetového bankovnictví převládat ověřování transakcí pomocí kódů zaslaných ve formě SMS na mobilní telefon (někdy se také označují jako mTAN), což je z hlediska zabezpečení lepší řešení. Přímo v SMS si totiž můžete ověřit, jakou transakci potvrzujete. Mezi další bezpečné metody, obvykle ale nabízené za příplatek, patří autentizační kalkulátor, zadávání údajů ze zašifrované SMS nebo použití certifikátu uloženého na bezpečném místě (čipová karta, USB klíč).

Za překonanou lze už dnes označit ochranu pomocí grafické klávesnice, protože moderní keyloggery už nemají problémy ani s touto taktikou (viz například **www.supremtec.com**).

V současné době už nabízí většina prohlížečů ochranu proti phishingu, která vás dokáže upozornit na nebezpečné a podezřelé WWW stránky.

s tím, že má podat žalobu. Po jejím podání se zase vrátil do banky, kde se mu začal věnovat specialista na on-line bankovnictví. Dozvěděl se, že získat peníze zpět z banky v Estonsku může trvat až 14 dní (tuto informaci získal 21. května). Když se dalších devět dní nic nedělo, volal Dominik 30. května do banky znovu, aby zjistil stav vyšetřování. Nečekaly na něj však žádné dobré zprávy. Bylo mu sděleno, že jeho peníze již zpět z Estonska nelze získat a že jeho případ byl předán pojišťovací společnosti.

Když Dominik Kroll tuto zprávu obdržel, jeho případ už ležel na stole policejního inspektora v Mnichově, který má na starosti internet a počítačové zločiny. I on si je vědom poklesu počtu phishingových případů, protože zatímco v současnosti má na starosti maximálně jeden případ týdně, ještě před dvěma lety to bylo třikrát tolik. Případy si jsou vždy podobné jako vejce vejci: kradená částka se obvykle pohybuje mezi 500 až 7 000 eury, ve většině případů jde o krádež do 3 000 eur. Dalším identickým rysem je cílová destinace peněžní transakce: peníze téměř vždy přistanou ve východní Evropě.

Pro policejního důstojníka je nejdůležitějším vodítkem směr peněz: „Je téměř nemožné zjistit pachatele na základě identifikace škůdce na počítači." Jeho první otázka tedy zní: „Kam byly peníze převedeny a je možné je získat zpět?"

Obvykle je totiž možné podvody zvrátit, což by mělo být základní prioritou bank. „Avšak i my jako policie můžeme hrát určitou roli," míní inspektor, „například při vyžádání si právní asistence od policie či předložení tzv. soudních prostředků pro zahraniční úřady. Dokonce můžeme zmrazit peníze ve Western Union."

Poskytovatelé finančních služeb jsou klíčovým prvkem scénáře phishingu. Ve většině případů přistanou ukradené peníze na německém kontě, které patří finančnímu agentu či prostředníkovi. Tito lidé jsou obvykle neinformovaní prostředníci – pouze na konto obdrží určitou částku, tyto peníze vyberou v hotovosti a převedou je pomocí služeb typu „Western Union" pachatelům v cizině. Za jejich práci je jim zaplacen poplatek ve výši asi 10 procent.

Konflikt zákonů: Kdokoliv, kdo pomáhá

Zní to lukrativně, ale končí to obvykle u soudu i s horou dluhů. Jestliže oběť zjistí odcizení peněz, její banka kontaktuje banku prostředníka. Oběť může vyžadovat vrácení peněz, i když už byla částka prostředníkem vybrána a poslána „dál". Inspektor popisuje případ mladé ženy, která během několika dnů převedla do zámoří 35 tisíc eur. Radost z rychle vydělané provize ve výši 3,5 tisíce eur však neměla dlouhého trvání – nyní stále ještě dluží téměř 30 tisíc...

Banka ji také „udala" na policii a tato žena byla ve finále odsouzena k několika měsícům vězení za účast při praní peněz. Nevědomost neomlouvá – pokud jsou peníze převedeny více než jednou, je tato činnost považována soudci za účelné jednání. A to obvykle bývá první krok k odsouzení. Podobným postupem byl polapen podvodník, který vyloupil konto Dominika Krolla: v květnu 2008 informoval inspektor Krolla, že v Estonsku byl zadržen podvodník Maxim B. Otázkou tedy zůstává pouze to, zda byl Maxim B. opravdovým lupičem, nebo jen nastrčeným prostředníkem. Ukradenou částku vrátila banka na konto Dominika Krolla teprve v září loňského roku.

Jako perličku na závěr lze ocitovat text z oznámení, které banka Dominikovi poslala při vrácení peněz: Jde o projev dobré vůle, bez uznání jakéhokoliv právního závazku. „Užil jsem si spoustu problémů, než jsem peníze dostal zpět," říká Dominik Kroll. Byla to pro něj tak tvrdá lekce, že se dokonce rozhodl skoncovat s on-line bankingem.

My takovýto radikální krok nedoporučujeme, podle našeho názoru je internetové bankovnictví při správné volbě zabezpečení praktickým pomocníkem. Příběh by ale měl být varováním pro všechny, kdo provozují své internetové bankovnictví z potenciálně nebezpečných počítačů. Ovládat své bankovní konto z počítače s pirátskými Windows XP, s vypnutými aktualizacemi, cracknutým firewallem a ukradeným antivirem je počítačovou verzí ruské rulety...

AUTOR@CHIP.CZ