Trompado (phishing)

MILAN KOLKA, 1-A OKTOBRO 2014

Kio estas „phishing“?

Elparolu „fiŝing”

Derivita el la angla vorto “fishing” = fiŝkaptado

Speco de trompado

Celo: akiri personajn datumojn por misusi ilin

Trompado per telefono

Trompado per telefono

Trompado per telefono

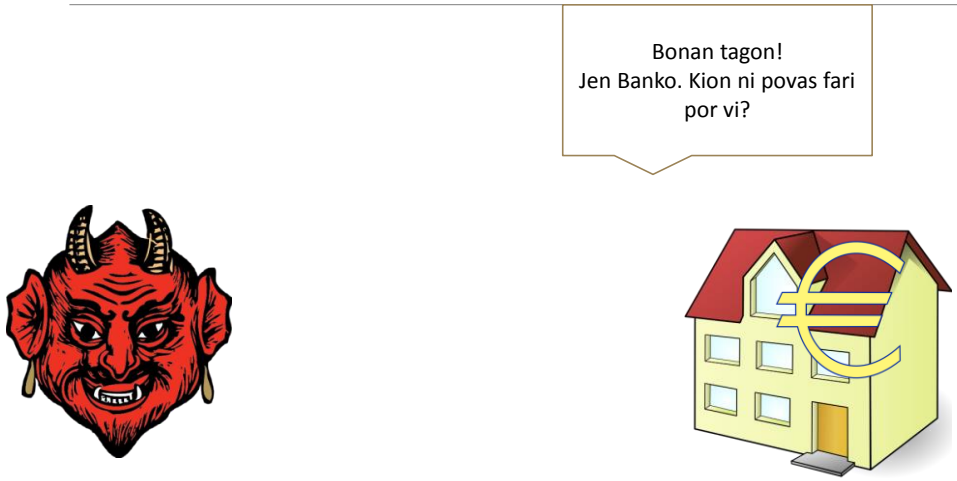
Trompado per telefono

Trompado per telefono

Trompado per telefono

Trompado per telefono

Kio okazos sekve?



Kio okazos sekve?

Bonan tagon,
Mi volas transdoni monojn.

Kio okazos sekve?

Kompreneble. Kia estas via bankklienta numero kaj pavorto?

Kio okazos sekve?

Kio okazos sekve?

Kio okazos sekve?

Al konto 48785499/5848, simbolo 488785, dudek mil kronojn.

Kio okazos sekve?

Via pagordono eniris.
Ni dankas, ke vi uzas servojn de Banko.
Ĝis revido.

Kio okazos sekve?

Dankon. Ĝis revido.

Defendo

Neniu banko kaj neniu administranto de iu sistemo bezonas koni vian pasvorton por vidi vian konton aŭ viajn datumojn.

Se vokas al vi iu el nekonata numero, vi ne scias, ĉu li estas vere tiu, kiu li diras, ke li estas.

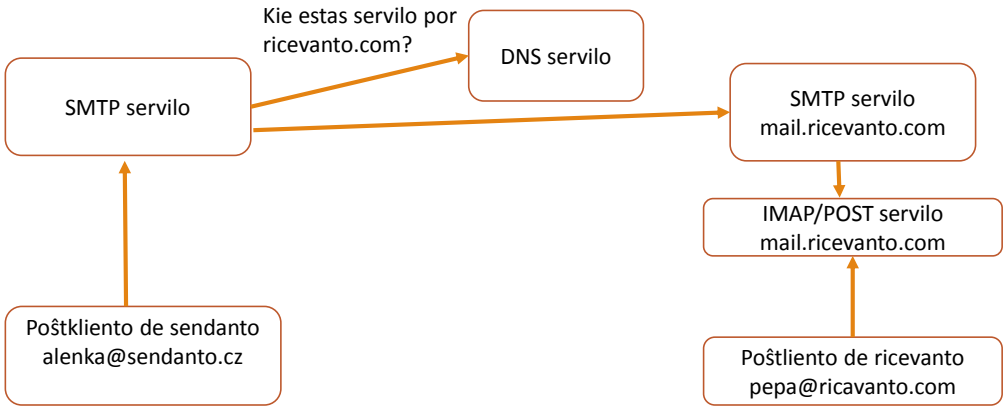
Trompado per retpoŝto

Ofte retpoŝtaj mesaĝoj, kiuj:

Proponas al vi multe da mono,

timigas vin, ke al vi minacas iu danĝero aŭ damaĝo.

Kiel funkcias retpoŝto?



Kiel aspektas retmesaĝo?

Return-path: <Tracy@bossesemail.info>
Received: from mail.bossesemail.info ([195.162.69.25])
id 1XSR3F-0006F3-Ur
for milan@milankolka.cz; Fri, 12 Sep 2014 15:38:13 +0200
Received: by mail.bossesemail.info id h2brfa0001gn for <milan@milankolka.cz>; Fri, 12 Sep 2014 09:36:52 -0400 (envelope-from <Tracy@bossesemail.info>)
From: Tracy <Tracy@bossesemail.info>
To: milan@milankolka.cz
Subject: =?utf-8?B?T2RlIERuZcWha2EgVsOhcyBVxb4gVnlwYWTDoXbDoW7DrSBWbGFzxa8gTmVidWRlIFRyw6FwaXQh?=
Content-Type:multipart/alternative; boundary="335f89e7a191a7870aca7d5c99311b96";
Message-ID: <335f89e7a191a7870aca7d5c99311b96@bossesemail.info>

...

--335f89e7a191a7870aca7d5c99311b96

Content-Type:text/plain; charset=utf-8

100% přírodní léčba zastavuje vypadávání vlasů a revitalizuje jejich kořínky pomocí komplexu dosud nevyužitých bohatých živin, který spouští proces uzdravení pokožky hlavy.

Přečtěte si, jak si můžete regenerovat vlasy v rekordním čase >>

>> http://www.bossesemail.info

Konsekvencoj

Iu ajn povas vidi la mesaĝon (kutimaj mesaĝoj ne estas ĉifritaj)

Iu ajn povas ŝanĝi la mesaĝojn (ne kredu al adreso de sendanto)

Iu ajn povas skribi falsan mesaĝon (http://anonymizer.in/fake-mailer)

Demando pro datumoj

Retpoŝtadreso -------

Salutnomo: -------

Pasvorto:------

Sendu al administrator@gmail.com

Atentu!

Neniu adminstranto bezonas vian pasvorton.

Kio poste okazos?

La atakanto malbonuzas vian konton por sendi spamojn de via nomo.

Falsaj retpaĝoj

…

Bonvolu ensaluti ĉe

www.banko.**utocnik**.cz

Por ke vi savu vian konton…

Rigardu la adreson: ne estas domajno www.banko.cz, sed subdomajno de fremda domajno utocnik.cz!

Falsaj paĝoj 2

…

Bonvolu ensaluti ĉe

www.banko.cz

Por ke vi savu vian konton…

Rigardu: en la teksto estas ĝusta adreso de banko, sed la ligilo montras al alia retpaĝaro

www.banko.**utocnik**.cz)

Falsaj paĝoj 3

Bonvolu ensaluti ĉe

www.bank0.cz

Por ke vi savu vian konton…

Rigradu:

Anstataŭ litero “o” estas numero 0 (aŭ rusa o).

Defendo

Ĉiam uzu retadresojn de via banko, retpoŝto aŭ alia servo el viaj legosignoj aŭ skribu permane en adresa linio.

Neniam alklaku al ligiloj en strangaj retmesaĝoj

Oferto de multe pagita laboro

Dobrý den!

V rámci rozšíření naší společnosti, provádíme nábor nezávislých pracovníku.

Mé jméno je Ignacio Molina, jsem HR manažer velké evropské společnosti.
Nabízíme následující pozici - Regionální zástupce.

V počáteční fázi, budete potřebovat 2-3 hodiny denně.
Větší část práce, můžete vykonávat doma.

Odměna se pohybuje v rozmezí 500 - 2500 eur plus bonusy.
Pracovní plán projednává se individuálně s každým zaměstnancem.

Kio estos via laboro?

Gajnu monon per ŝtelita kreditkarto.

Transferi monon el rompita konto al alian

Uzi sian konton por transferi ŝtelitan monon.

Vi iĝos “blanka ĉevalo”.

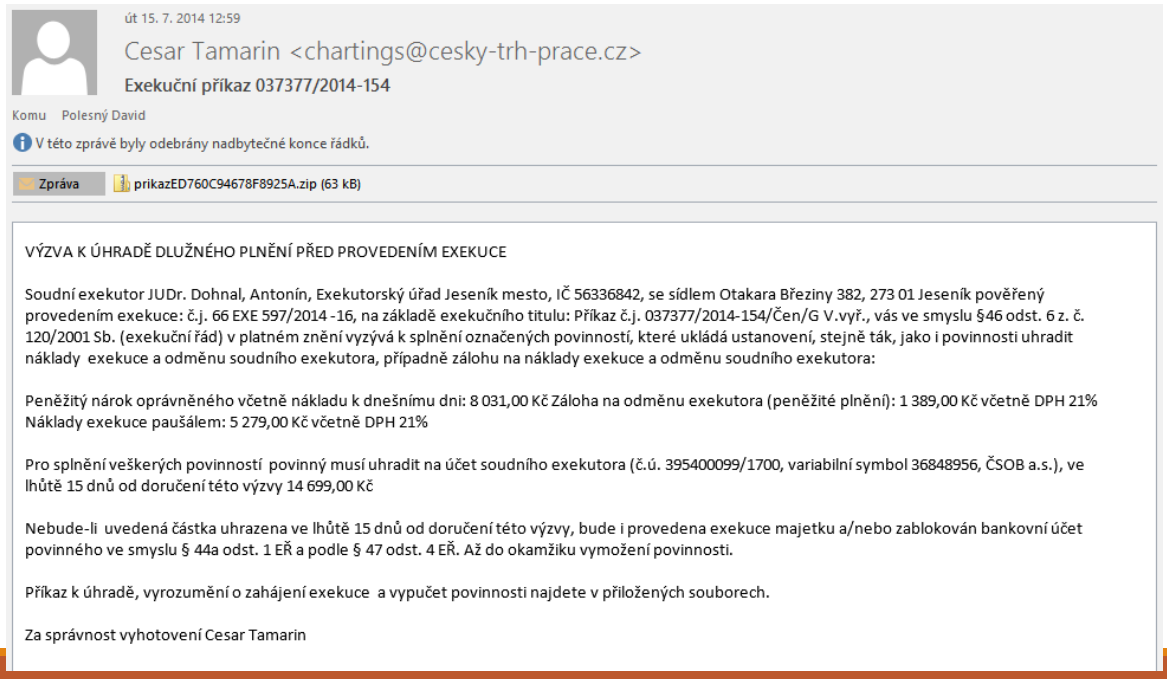
Defendo

Forigu la retmesaĝon.

Neniam respondu.

Trompado per virusoj

“ekzekucia komando”



út 15. 7. 2014 12:59

Cesar Tamarin <chartings@cesky-trh-prace.cz>

Exekuční příkaz 037377/2014-154

Komu Polesný David

V této zprávě byly odebrány nadbytečné konce řádků.

Zpráva prikazED760C94678F8925A.zip (63 kB)

VÝZVA K ÚHRADĚ DLUŽNÉHO PLNĚNÍ PŘED PROVEDENÍM EXEKUCE

Soudní exekutor JUDr. Dohnal, Antonín, Exekutorský úřad Jeseník mesto, IČ 56336842, se sídlem Otakara Březiny 382, 273 01 Jeseník pověřený provedením exekuce: č.j. 66 EXE 597/2014 -16, na základě exekučního titulu: Příkaz č.j. 037377/2014-154/Čen/G V.vyř., vás ve smyslu §46 odst. 6 z. č. 120/2001 Sb. (exekuční řád) v platném znění vyzývá k splnění označených povinností, které ukládá ustanovení, stejně ták, jako i povinnosti uhradit náklady exekuce a odměnu soudního exekutora, případně zálohu na náklady exekuce a odměnu soudního exekutora:

Peněžitý nárok oprávněného včetně nákladu k dnešnímu dni: 8 031,00 Kč Záloha na odměnu exekutora (peněžité plnění): 1 389,00 Kč včetně DPH 21% Náklady exekuce paušálem: 5 279,00 Kč včetně DPH 21%

Pro splnění veškerých povinností povinný musí uhradit na účet soudního exekutora (č.ú. 395400099/1700, variabilní symbol 36848956, ČSOB a.s.), ve lhůtě 15 dnů od doručení této výzvy 14 699,00 Kč

Nebude-li uvedená částka uhrazena ve lhůtě 15 dnů od doručení této výzvy, bude i provedena exekuce majetku a/nebo zablokován bankovní účet povinného ve smyslu § 44a odst. 1 EŘ a podle § 47 odst. 4 EŘ. Až do okamžiku vymožení povinnosti.

Příkaz k úhradě, vyrozumění o zahájení exekuce a vypučet povinnosti najdete v přiložených souborech.

Za správnost vyhotovení Cesar Tamarin

Kiel funkcias la viruso?

1. Uzanto malfermas la mesaĝon kaj estas terurita

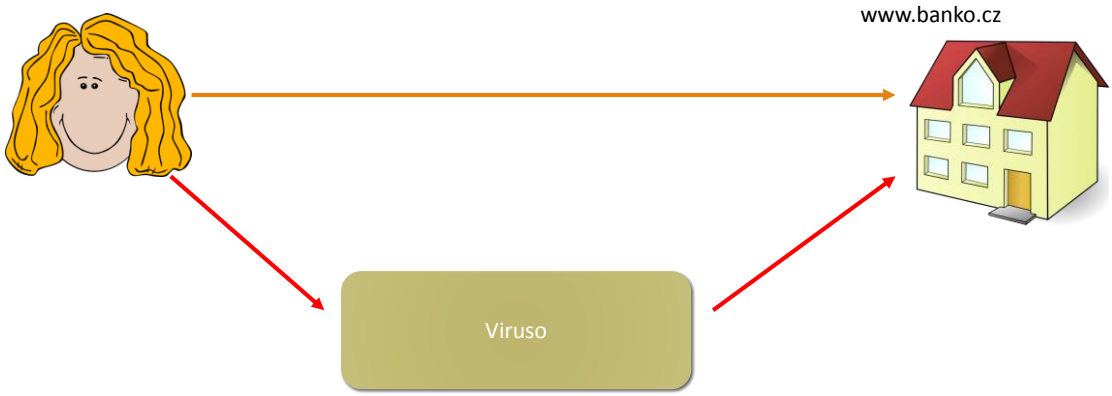
2. Uzanto malfermas kunsendaĵon. Ĝi estas sendanĝera arĥivo de tipo zip

3. La arĥivo enhavas dosieron kun nomo “ekzekuciao komando” aŭ simila. Uzanto alklakos ĉe ĝi.

4. Sed la dosiero ne estas dokumento, sed programo (viruso)

5. La programo estas instalita en komputilon de uzanto.

La viruso “redaktas” retpaĝojn de banko.



Kio okazos...

La ŝanĝita paĝo:

sendos salutnomon kaj pasvorton de uzanto al atakanto.

Proponos al uzanto instali “sekuran” aplikaĵon en lian plurfunkcian telefonon .

La “sekura aplikaĵo” transsendos sms mesaĝojn de banko al la atakanto.

Konsekvenco

La atakanto komandas komputilon kaj plurfunkcian telefonon

La atakanto konas ĉiujn datumojn necesajn por komandi vian bankkonton.

La atakanto transferas monon el via konto al konto de sia kunlaboranto (blanka ĉevalo)