HERMES SoftLab
a ComTrade company

//Ekonomija kibernetskega kriminala na primeru e-bančnih zlorab/

Tadej Vodopivec, CISSP, CISA, CBCP

//Tehnični načrt napada/

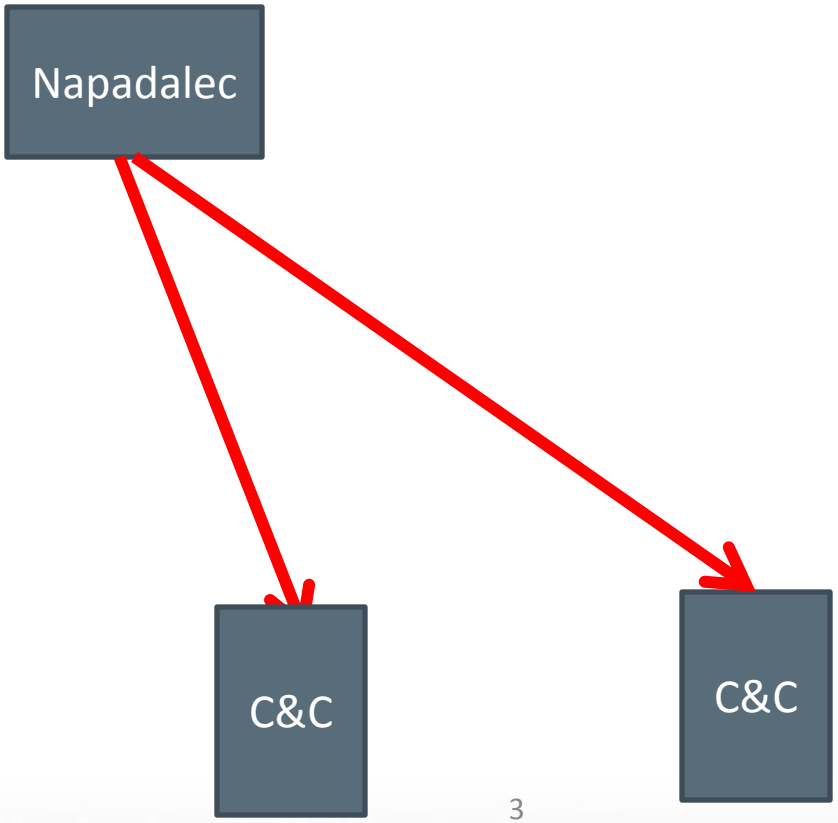
- Gradnja/najem/nakup botnet omrežja,
- izbira žrtev,
  - ciljano ali po kriterijih,
- izvedba napada,
  - nepooblaščen prenos denarja na račun kurirja – mule,
  - dvig in predaja gotovine.

//BOTNETI/

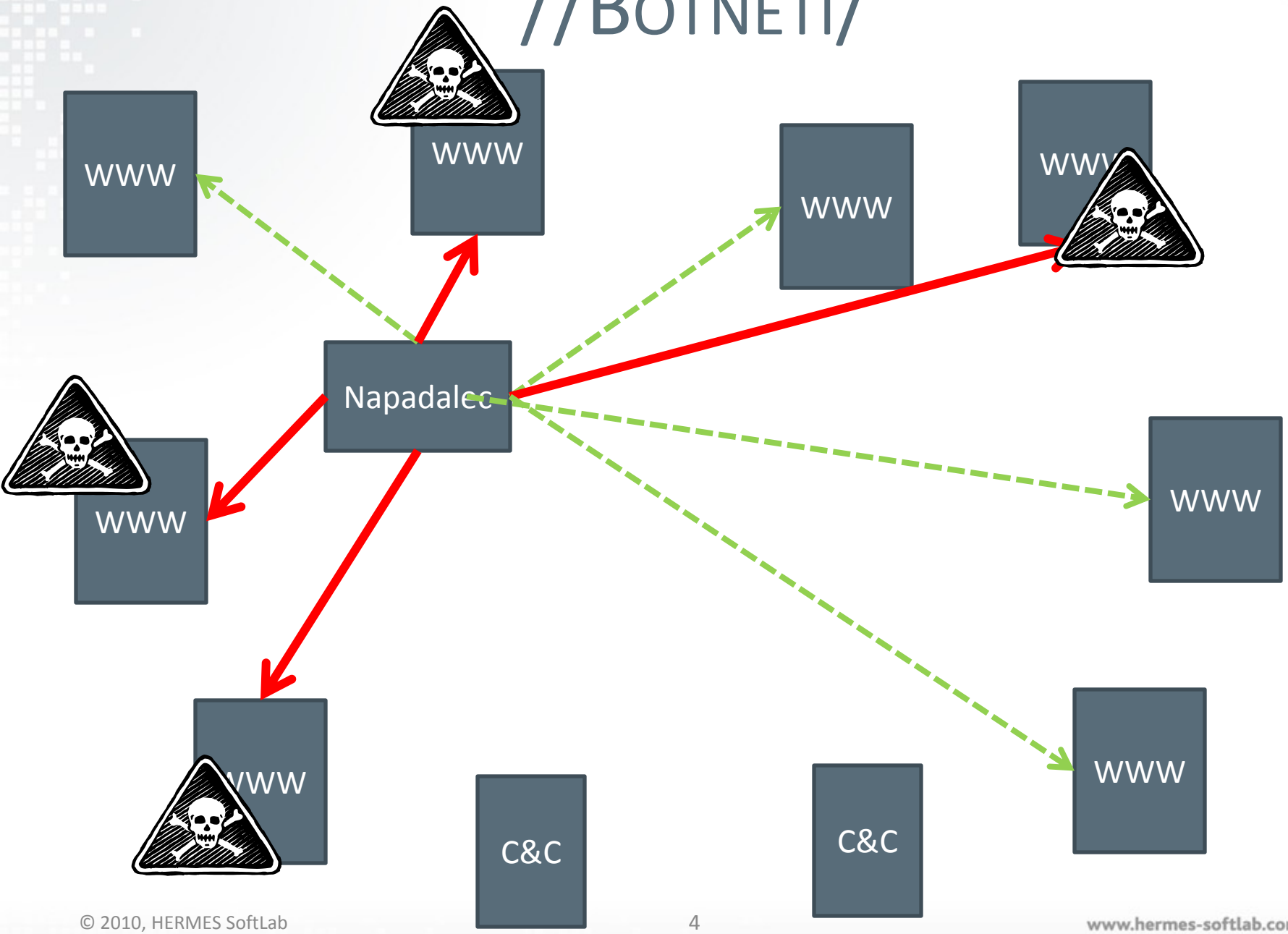
botnet *(angl. botnet, robot network)*

1. preko spleta v mrežo povezani boti (roboti) ali avtomatizirani programi npr IRC boti
2. prikrito omrežje računalnikov, okuženih z zlonamerno kodo, ki ga lahko upravljamo z oddaljene lokacije, največkrat za ilegalno početje

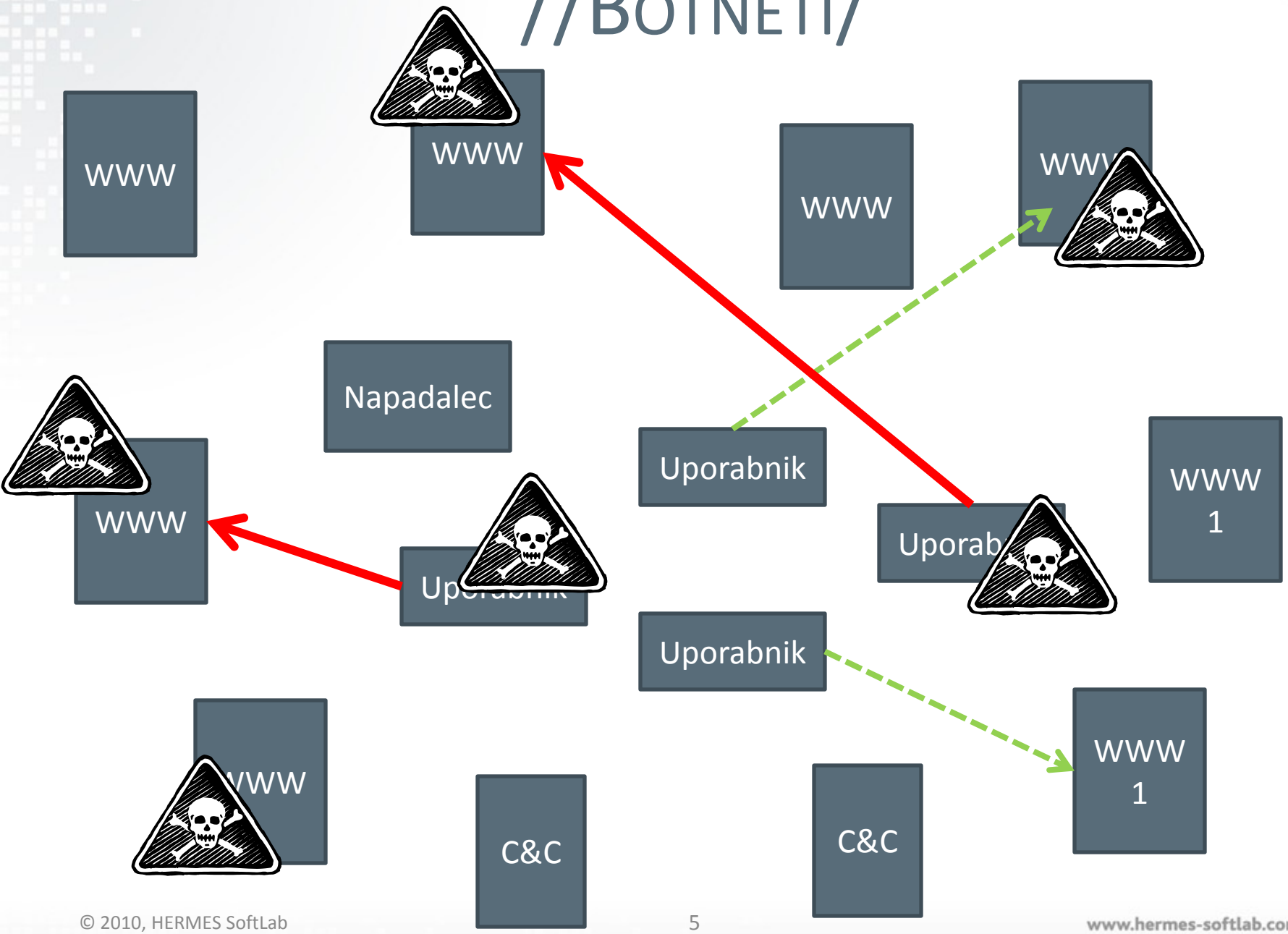
vir: www.islovar.org



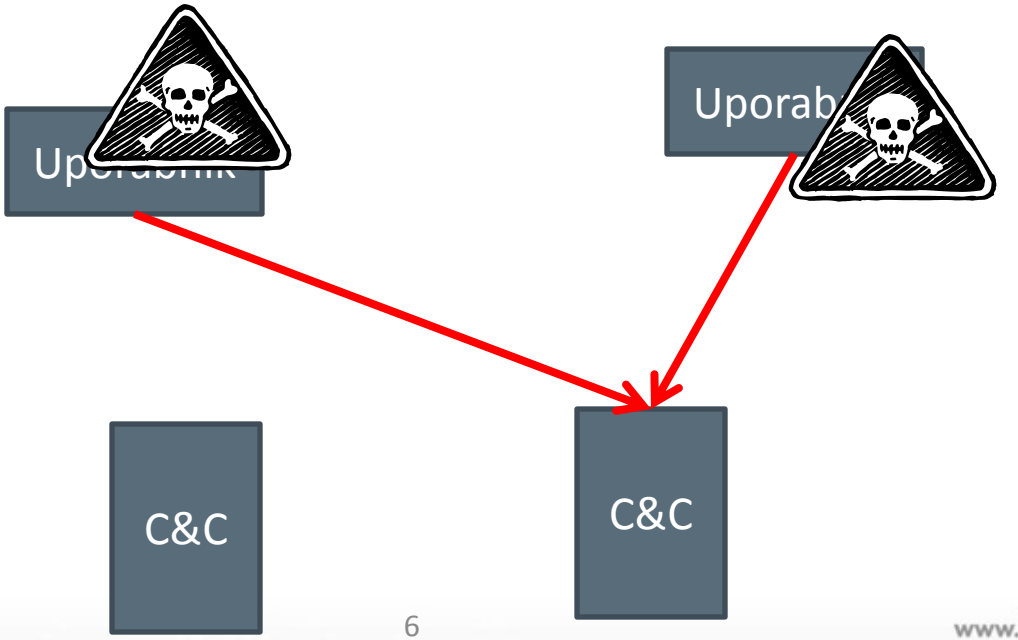
//BOTNETI/



//BOTNETI/


WWW
WWW
WWW
WWW
Napadalec
WWW
Uporabnik
WWW
1
Uporabnik
Uporabnik
WWW
1
WWW
C&C
C&C

//BOTNETI/



//PRIMERI UPORABE BOTNETOV/

- DDoS napadi – onemogočanje storitev
  - po naročilu,
- kraja podatkov:
  - na zalogo,
  - po naročilu – ciljano npr. iz določenega podjetja,
- zlorabe e-bančništva:
  - “kraja identitete”,
  - t.i. man-in-the-browser napadi,
- Fraud-as-a-service.

//ZEUS/

- Trojanski konj: kit komplet + storitev podpore za okrog 500 €,
- zanimivost: End User License Agreement
- prestrezanje tipkovnice & prikaza v realnem času
- potvarjanje prikaza v realnem času
- uporaba Jabber IM za posredovanje podatkov
- uspešni napadi na enkratna gesla

- http://www.rsa.com/blog/blog_entry.aspx?id=1515
- https://zeustracker.abuse.ch/

//ZEUS EULA/

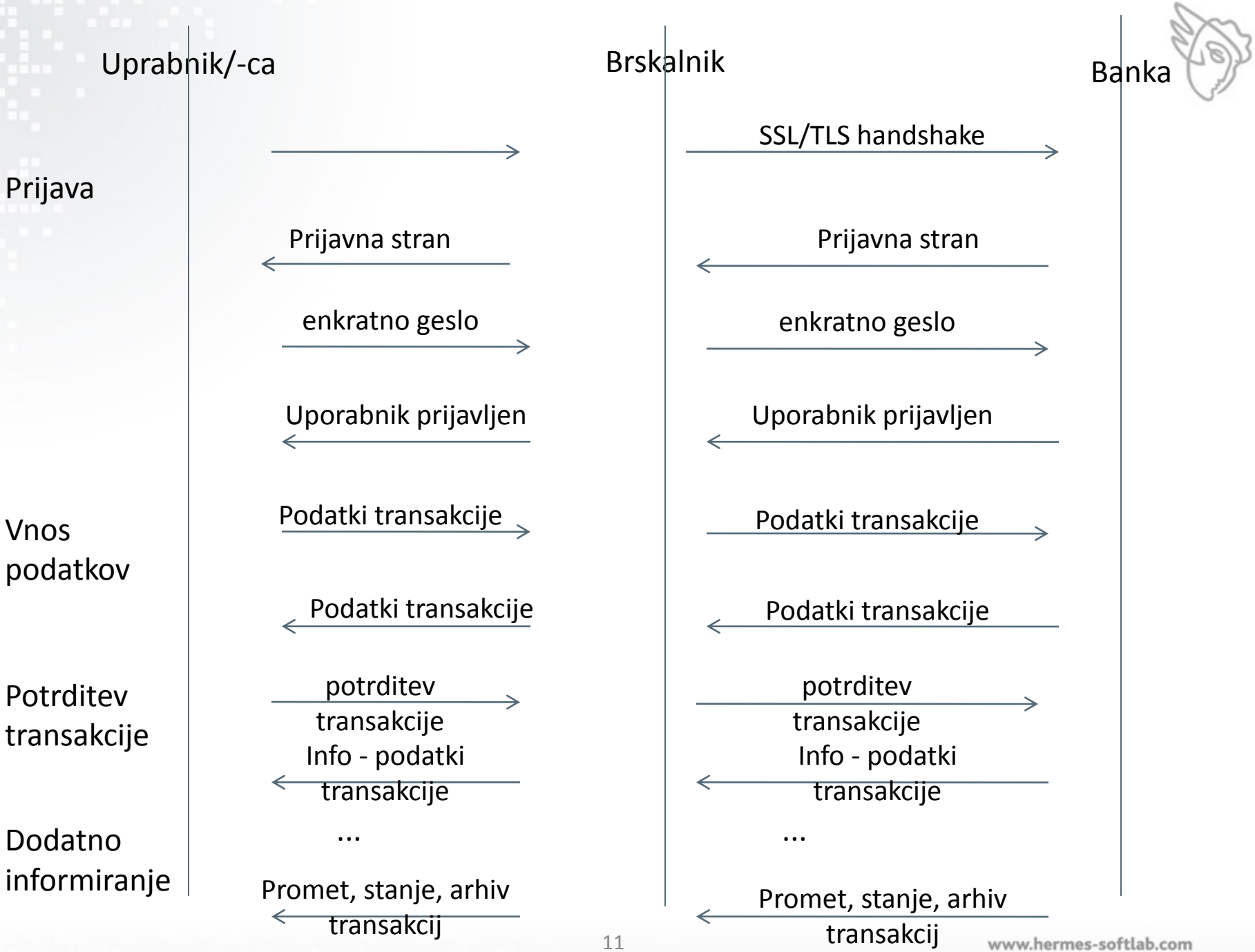
- Does not have the right to distribute the product in any business or commercial purposes not connected with this sale.
- May not disassemble / study the binary code of the bot builder.
- Has no right to use the control panel as a means to control other bot nets or use it for any other purpose.
- Does not have the right to deliberately send any portion of the product to anti-virus companies and other such institutions.
- Commits to give the seller a fee for any update to the product that is not connected with errors in the work, as well as for adding additional functionality.

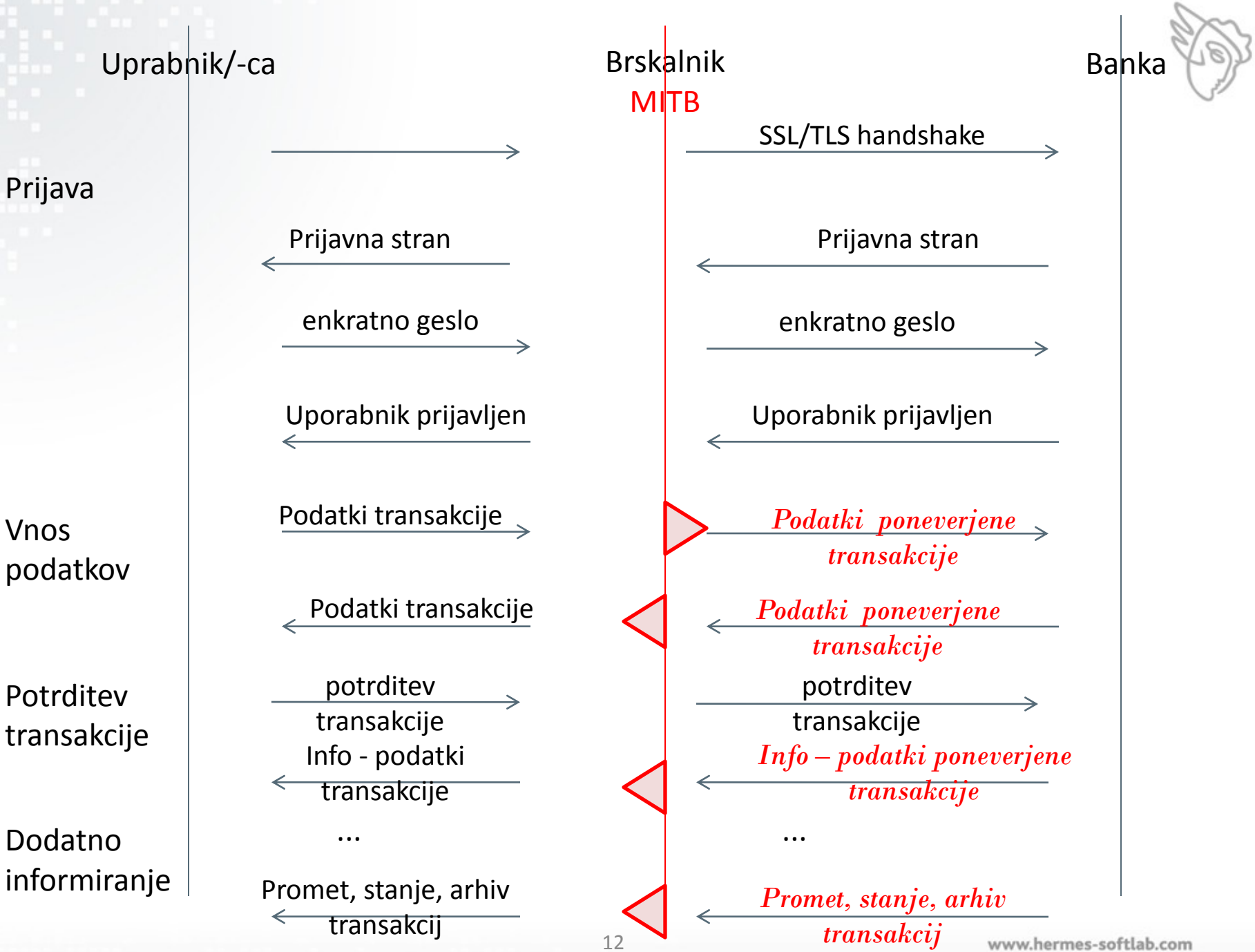
"In cases of violations of the agreement and being detected, the client loses any technical support. Moreover, the binary code of your bot will be immediately sent to anti-virus companies."

//URLZONE/

- Storilec dobi program URLZone Builder,
- z njim izdela konfiguracijsko datoteko, specifično za napadeno storitev,
- okužba z “drive-by” napadom prek različnih ranljivosti,
- uspešno okužen računalnik dobi “navodila” iz C&C centra (konfiguracijska datoteka),
- trojanski konj prestreza HTTPS promet skozi brskalnik,
- ko zazna transakcijo, zamenja znesek in nadomesti ciljni račun z mulinim računom,
- v vseh prikazih uporabniku (promet, stanje) svojo transakcijo nadomesti z originalno uporabnikovo,

- http://www.finjan.com/MCRCblog.aspx?EntryId=2345
- http://www.finjan.com/GetObject.aspx?ObjId=679


Uprabnik/-ca
Brskalnik
Banka
SSL/TLS handshake
Prijava
Prijavna stran
Prijavna stran
enkratno geslo
enkratno geslo
Uporabnik prijavljen
Uporabnik prijavljen
Vnos podatkov
Podatki transakcije
Podatki transakcije
Podatki transakcije
Podatki transakcije
Potrditev transakcije
potrditev transakcije
potrditev transakcije
Info - podatki transakcije
Info - podatki transakcije
Dodatno informiranje
...
...
Promet, stanje, arhiv transakcij
Promet, stanje, arhiv transakcij



//POSLOVNI NAČRT NAPADALCA/

- Kaj bomo delali:
  - Prevzeli bomo nadzor nad pomanjkljivo zaščitenimi računalniki uporabnikov e-bančnih storitev več bank v različnih državah,
  - poiskali račune z dovolj denarja in
  - si vzeli z njih nekaj denarja.

//Za koga?

- Seveda zase :-)
- Naše glavne »stranke« pa bodo:
  - komitenti tistih bank, ki imajo veliko število komitentov, ki uporablja enako tehnično rešitev za e-bančništvo – z »razbitjem« zaščite take banke pridobimo večjo ciljno publiko,
  - komitenti tistih bank, kjer znamo z razumnim vložkom zaobiti zaščito; prednost imajo banke s slabšo zaščito, vendar moramo upoštevati tudi prejšnjo alinejo,
  - fizične osebe, samostojni podjetniki in mala podjetja – v povprečju predpostavljamo, da so v tej skupini računalniki slabše zaščiteni kot v srednjih in velikih podjetjih,
  - uporabniki razširjenih računalniških platform, kjer lahko z uspešnim napadom na posamezno platformo pridobimo večjo ciljno publiko.

//PREDNOSTI PRED KONKURENCO/

- Klasični tatovi, gospodarski kriminalci:
  - Policija in kriminalisti so bolje organizirani in usposobljeni za boj proti klasičnim tatovom in gospodarskim kriminalcem, področje kibernetskega kriminala je zanje novo in nimajo enako razdelanih učinkovitih metod,
  - Za seboj puščamo malo otipljivih sledi, ker delamo na daljavo,
  - Ciljne »stranke« nas ne pričakujejo in pred nami niso ustrezno zaščitene,
- Druge kriminalne skupine s podobnimi cilji:
  - Uporaba tehnično naprednih metod za pridobivanje kontrole nad računalniki,
  - Uporaba varnostnih mehanizmov za preprečevanje prisluškovanja,
  - Uporaba mehanizmov za izogibanje poznanim sistemom zaznavanja prevar in zlorab na bankah,
  - »Trg« je relativno nezasičen.

//TEMELJNE VREDNOTE/

- veliko število končnih računalnikov pod našim nadzorom,
- zaščita komunikacije z računalniki, ki jih imamo pod nadzorom, vključno s preprečevanjem infiltracije tujih računalnikov,
- dovolj kurirjev (mul), da ponavljajoča nakazila na isti račun ne zbujajo suma,
- vodenje operacij s fizičnega območja, kjer nas oblasti ne bodo preganjale.

STRENGTHS	WEAKNESSES
• Imamo varno zaledje v odmaknjeni državi • Dovolj denarja pridobimo že ob relativno nizkem uspehu zlorab • Banka in uporabnik morata braniti vse fronte, nam je dovolj ena vstopna »varnostna luknja« • Banke se morajo držati zakonov, mi ne	• Nimamo specialistov za izdelavo zlonamerne programske opreme
OPPORTUNITIES	**THREATS**
• Veliko število ranljivih računalnikov • Možnost »nakupa« zlonamernega paketa programske opreme od druge specializirane kriminalne organizacije	• Banke vpeljejo dodatne zaščite transakcij • Kurirji (mule) nas »izdajo« • Kriminalisti ali varnostni analitiki se infiltrirajo v naše omrežje računalnikov pod kontrolo (angl. botnet network) • Organi pregona uničijo Command & Control Centre omrežja računalnikov pod kontrolo.

//POSLOVNE ODLOČITVE/

- Zaradi odsotnosti lastnih specialistov za izdelavo zlonamerne programske opreme bomo uporabili ponudbo zunanjega izvajalca na črnem trgu.
- Uporabimo rešitev URLZone. Licenčnina znaša 4.000 USD za vsako obvladovano banko (hipotetičen podatek).
- Ponudnik nam za 40% soudeležbe pri dobičku ponuja tudi svoje omrežje mul, a se raje odločimo, da organiziramo svoje mule, ki bodo zadovoljne z 10% transakcije.

//Se nam splača napasti banko s 100.000 aktivnimi uporabniki?

- Licenca za program 4.000 USD/banko = cca. 3.000 €,
- 5% aktivnih uporabnikov (5.000) trči ob okuženo spletno stran,
  - ocena na podlagi podatkov Netcraft, Dasinet,
- 7,5% od teh (375) se okuži,
  - povzeto po Finjan-ovi analizi URLZone,
- 10% (37) ima več kot 1.000 € na računu,
- Povprečni izplen 2000 €/ komitentu,
  - mula dobi 10%, ostane 1.800 €,
- 37 x 1.800 = 66.600 €,
- 10.000 € strošek organiziranja mul,
- **Skupaj: 52.600 € čistega,**
  - pred obdavčitvijo ☺ ob vložku 13.000 €,
  - Tveganje, da nas organi pregona onemogočijo ali celo aretirajo, so ob predvidenih ukrepih samo-varovanja sprejemljiva.

//IZRAČUN ZA 10.000 UPORABNIKOV/

- 10.000 aktivnih uporabnikov,
- 3-4 “uporabne žrtve”:
  - okužene,
  - > 1.000 € na računu,
- 4 x 1.800 = 7.400 €,
- licenca 3.000 €,
- manj mul, nižji strošek – 4.000 €,
- ostane 400 € čistega ob vložku 7.000 €,
- glede na tveganja ni posebej privlačno,
- osredotočili se bomo torej na banke z veliko komitenti.

//KONEC/

- Botneti so nevarni!
- Pri oceni konkretnega tveganja se vživite v vlogo napadalca.
- Poskusite predstavljeni koncept razmišljanja pri ocenjevanju tveganj prenesti v svoje poslovne procese.

TADEJ.VODOPIVEC@HERMES.SI

HERMES SoftLab d.o.o.
Litijska 51
1000 Ljubljana