Le tecniche informatiche per la sottrazione di dati riservati

Cosimo Anglano
Dipartimento di Informatica
&
Centro Studi Interdipartimentale sulla Criminalitá Informatica

Universitá del Piemonte Orientale
Alessandria

Computer e dati riservati

- Dati riservati di diverso tipo che transitano mediante un computer
  - Credenziali di accesso a sistemi bancari
  - Numeri di carte di credito e codici di autorizzazione
  - Credenziali di accesso a servizi informatizzati quali web mail, social network, ecc.
  - Dati personali (codice fiscale, data nascita, ecc.)

Hanno un valore economico?

Tipo di credenziali	Prezzo di vendita
Data set “CVV2”: numero di carta di credito, codice di validazione, data di scadenza, indirizzo di fatturazione e nome del titolare	$1.5 – $3
Social Security Number (SSN), Data di nascita (DOB), Mothers Maid Name (MMN)	MMN: $5-$6 SSN: $1-$3 DOB: $1-$3
“Dump” dei dati memorizzati nelle bande magnetiche delle carte di credito	$15-$20 (standard) $20-$80 (gold/platinum)
Credenziali per home banking	$50-$1000 (in base al tipo di conto ed al saldo)
“Fulls”: insieme completo di tutti i dettagli sopra elencati	$5-$20

Dati tratti dal bollettino “RSA Online Fraud Report” del mese di Agosto 2010

Hanno un valore economico?

Selling cvv With Dob,ssn,mmn And Dbest Cvv Bank Login Dumps Fullz Mailer...

Categories > News

Page **1**

zingzingcc
rookie - member 10 posts

sell CVV fresh and good!!!!!
hello ! i'm a seller cvv cheap and good
I will be glad to serve you.
please contact me : zing.zingcc@yahoo.com
Y!M : zing.zingcc
I sell to are:CVV U.S., UK, CA, Ge, AU, Italian, Japan, France, ...
----- PRICE -----
CCV US
- US MASTER CARD = $2 per 1
- US VISA CARD = $2 per 1
- US AMEX CARD = $4 per 1
- US DISCOVER CARD = $4 per 1
- US CARD WITH DOB = $14 per 1
- US FULLZ INFO = $30 per 1
CCV UK
- UK CARD NORMAL = $4 per 1
- UK MASTER CARD = $5 per 1
- UK VISA CARD = $5 per 1

Hanno un valore economico?

- UK AMEX CARD = $6 per 1
- UK CARD WITH DOB = $15 per 1
- UK WITH BIN = $10 per 1
- UK WITH BIN WITH DOB = $25 per 1
- UK FULLZ INFO = $40 per 1

CCV AU
- AU MASTER CARD = $14 per 1
- AU VISA CARD = $14 per 1
- AU AMEX CARD = $15 per 1
- AU DISCOVER CARD = $15per 1

CCV CA
- CA MASTER CARD = $6 per 1
- CA VISA CARD = $6 per 1
- CA VISA BUSINESS = $14 per 1
- CA VISA GOLD = $14 per 1

CCV EU
- EU MASTER CARD = $15 - $20 per 1
- EU VISA CARD = $15 - $20 per 1
- EU AMEX CARD = $17 - $22 per 1
- EU DISCOVER CARD = $17 - $22 per 1

CCV GER
- GER MASTER CARD = $17 per 1
- GER VISA CARD = $16 per 1
- GER AMEX CARD = $18 per 1
- GER DISCOVER CARD = $20 per 1

CCV ITL
- ITL MASTER CARD = $18 per 1
- ITL VISA CARD = $17 per 1
- ITL AMEX CARD = $19 per 1
- ITL DISCOVER CARD = $20 per 1

.....

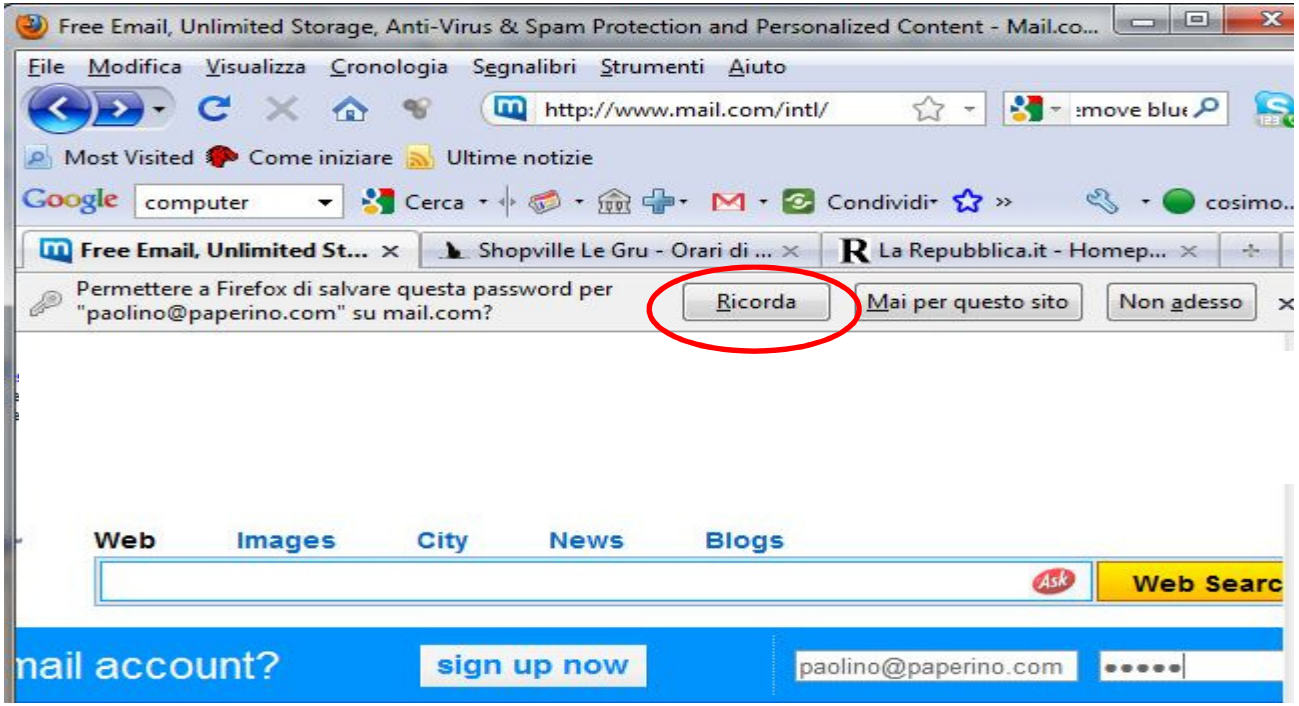
the conditions of sale:

1. Please Dont ask CC FREE, CC TEST. I do not have the time free to CC CC TEST.
2. If u want test please buy one and then if the cvv is good u can buy more from me
You Send money => I send good cvv
3. Cvv will be sent to you after receiving payment. Orders will be sent via e-mail or when you want.
4. I have a replacement policy for bad Cvv. All my cvv are inspected before sale
5. I only accept LR or WU

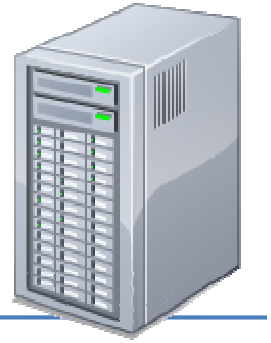
I'm looking for people who can work together
I am very happy to serve you in a long time, thank you!
zing.zingcc@yahoo.com
Y!m: zing.zingcc

20 May 2010 04:39 PM quote

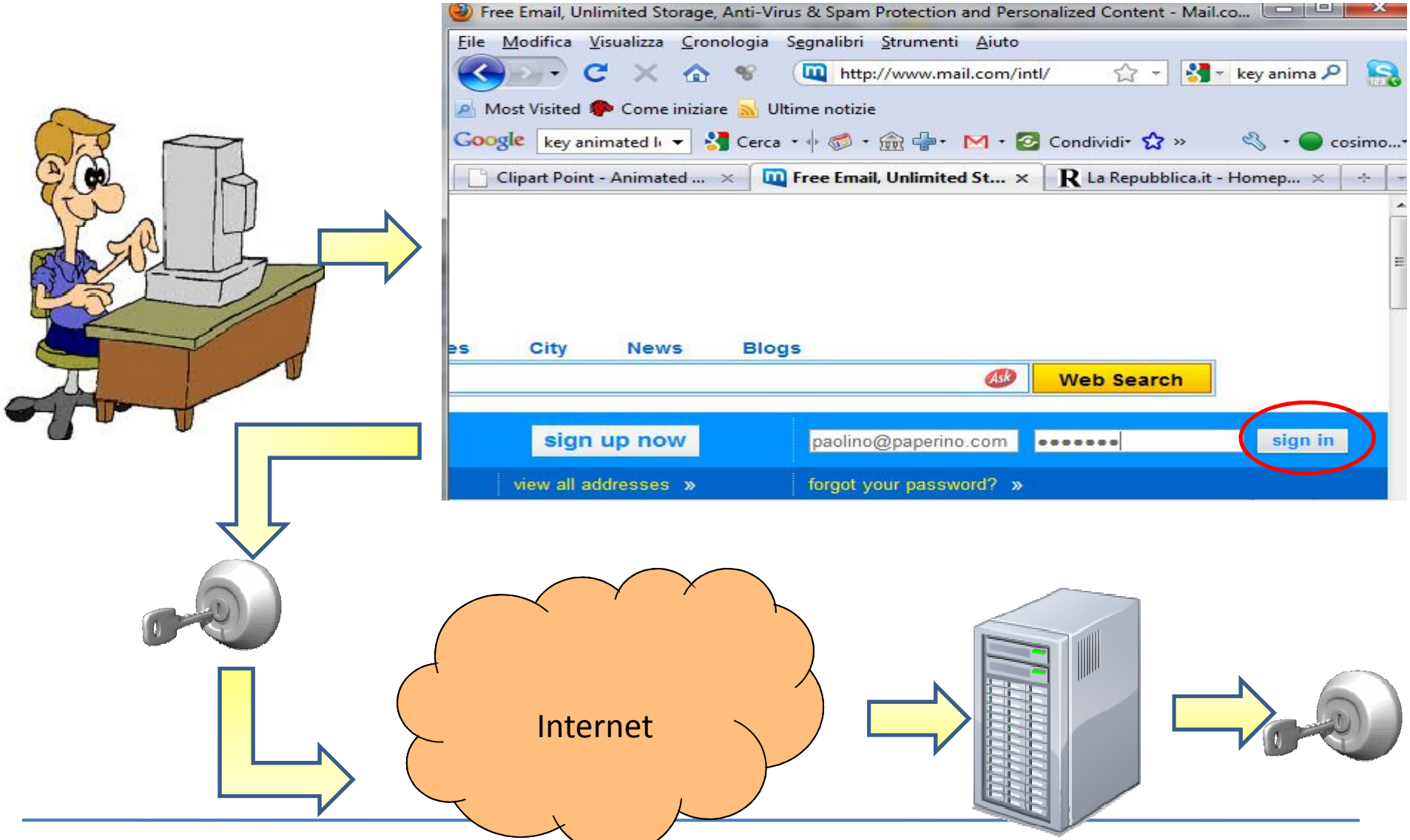
Dove sono memorizzati?



Internet

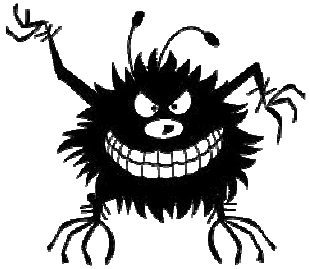


Dove sono memorizzati?



Come si possono sottrarre?

- Mediante appositi software (*malware*) installati sul computer all'insaputa dell'utente per mezzo di un *veicolo d'infezione*

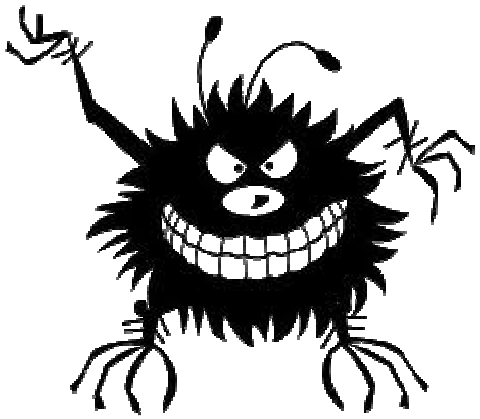


Veicoli di infezione: drive-by download

- Scaricamento (piú o meno) inconsapevole di software

Veicoli di infezione: trojan horse

- Programmi legittimi che peró al loro interno contengono il malware

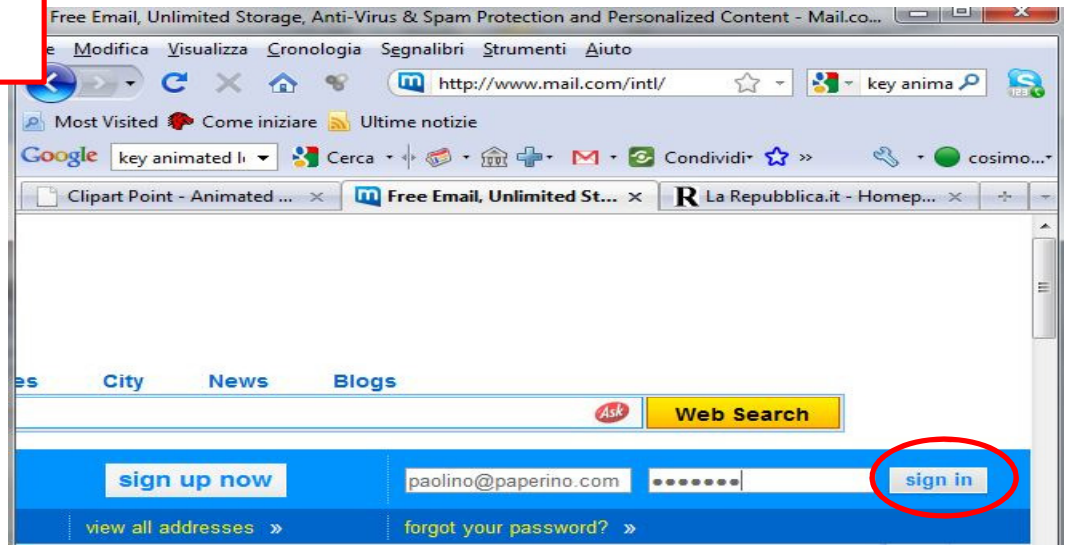


Veicoli di infezione: worm

- Malware che cerca attivamente di propagarsi ad altri computer raggiungibili via rete sfruttando vulnerabilitá di questi o tecniche di social engineering (es. messaggi di email)

Dove agisce il malware?

Keylogger
Screen logger



Dirottamento della connessione
Web page injection

Disk scanning & scavenging

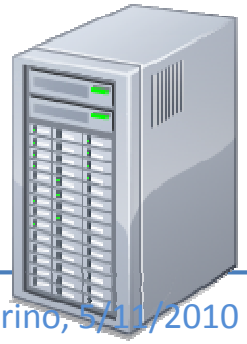
I “keylogger”

- Intercettazione dei caratteri digitati sulla tastiera

Server “legittimo”

Sddhfd mario sdsfd pass aasf3@@

Sddhfd mario sdsfd pass aasf3@@

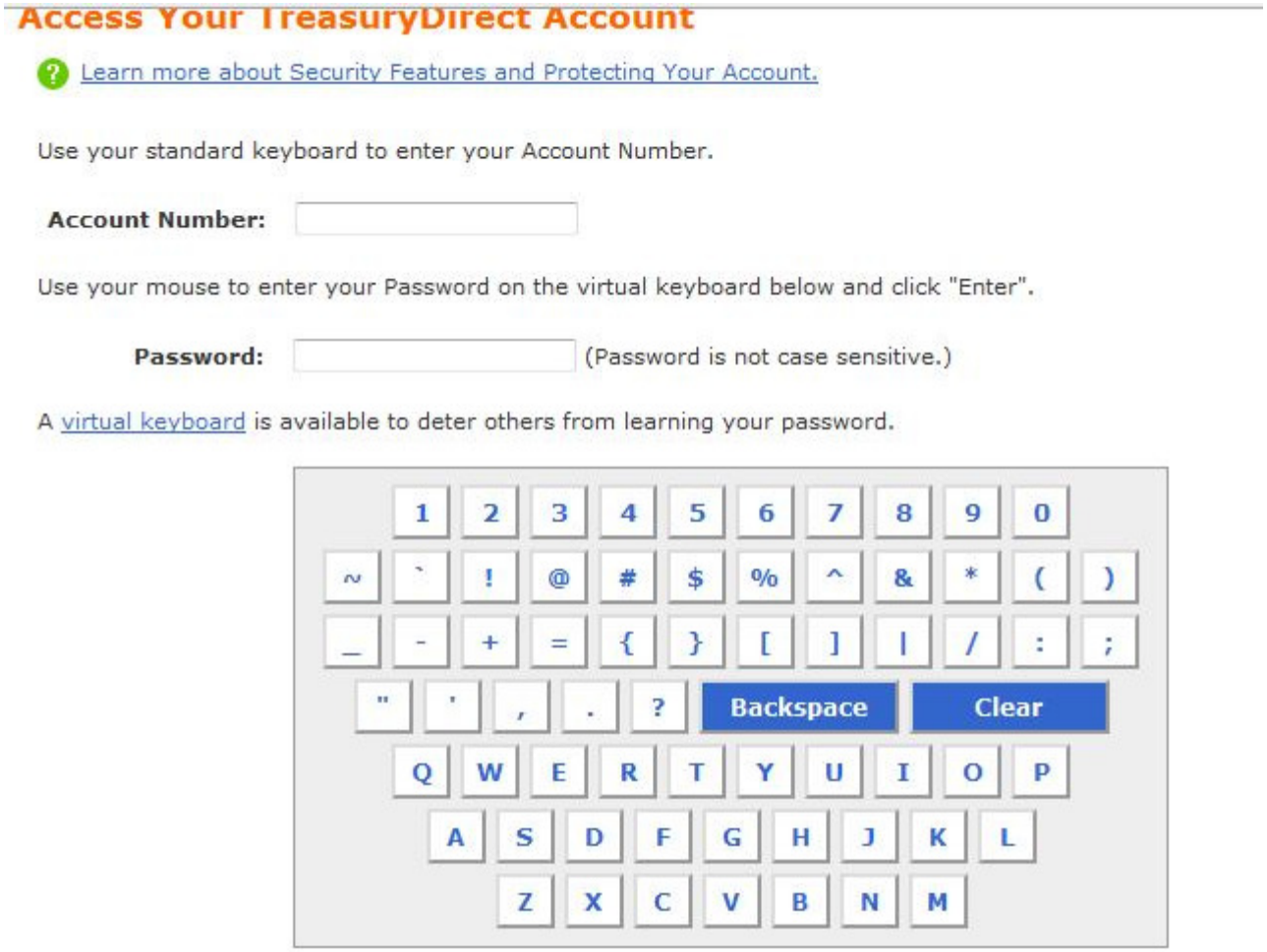


“drop” server

I “keylogger”: problemi

- Presentano alcuni problemi:
  - Troppi dati generati, pochi realmente interessanti
    - Elaborazione in loco: l’utente puó notare rallentamenti del proprio computer
    - Invio via rete: l’utente puó notare un’insolita attivitá di rete
  - Difficoltá ad individuare i dati interessanti a causa dell’assenza di contesto
    - credenziali spesso inserite per mezzo di pagine web
  - Utilizzo di “tastiere virtuali” sui siti bancari

I “keylogger”: tastiere virtuali



Gli “screen logger”

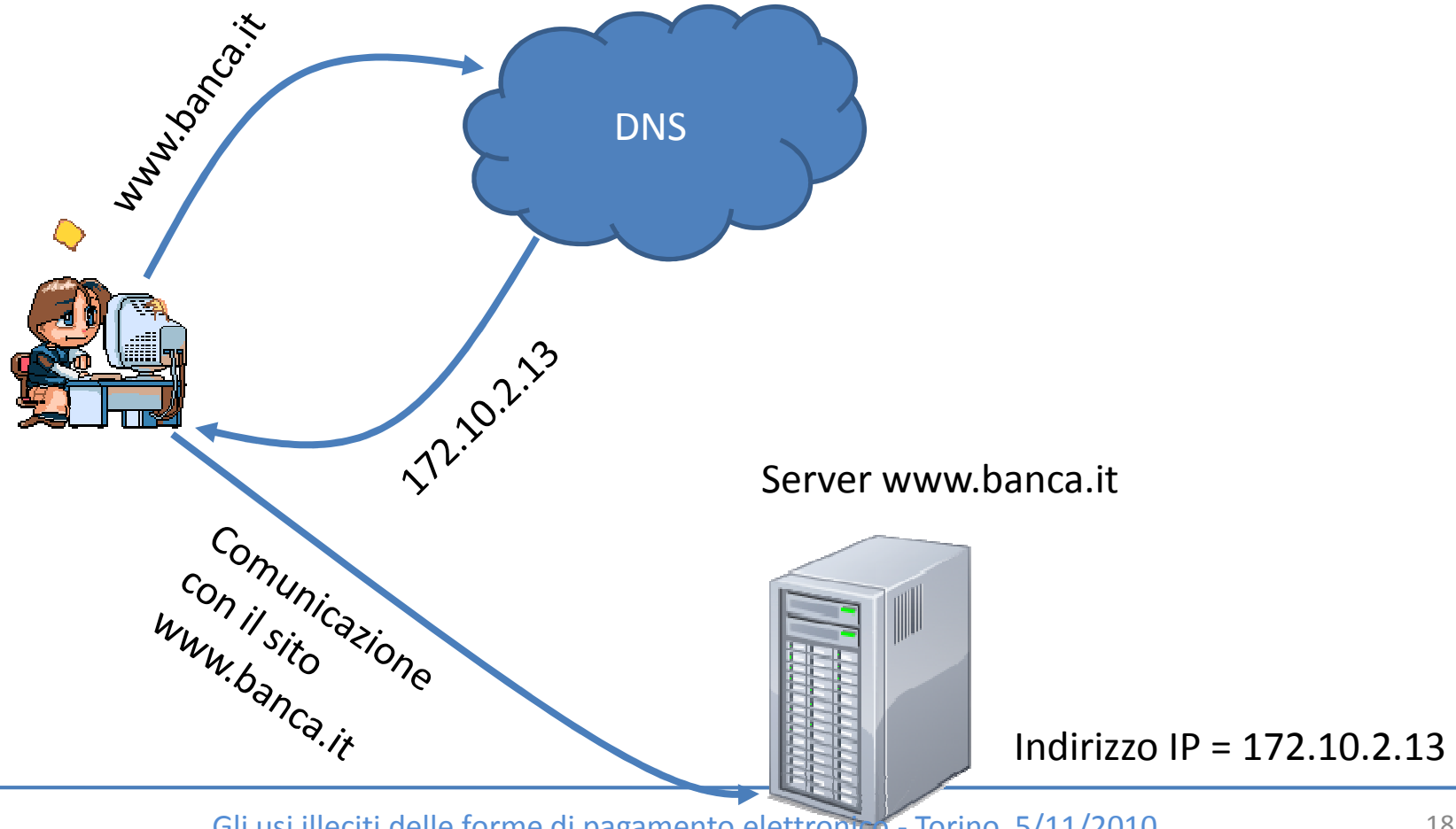
- Catturano tutto ció che é visualizzato sullo schermo, quindi anche la sequenza di tasti premuti su una tastiera virtuale
- Inviano queste informazioni ad un drop server
- Alcuni screen logger sono in grado di catturare anche le comunicazioni audio (skype e simili)
- Generano un traffico di rete potenzialmente alto, e quindi rilevabile

Dirottamento della connessione

- Consiste nel dirottare una connessione richiesta ad un sito web verso un altro sito, controllato dai malintenzionati
- Puó essere utilizzato per:
  - Phishing in tempo reale
  - Impedire l'accesso a siti specifici, quali ad esempio quelli che si occupano di sicurezza informatica

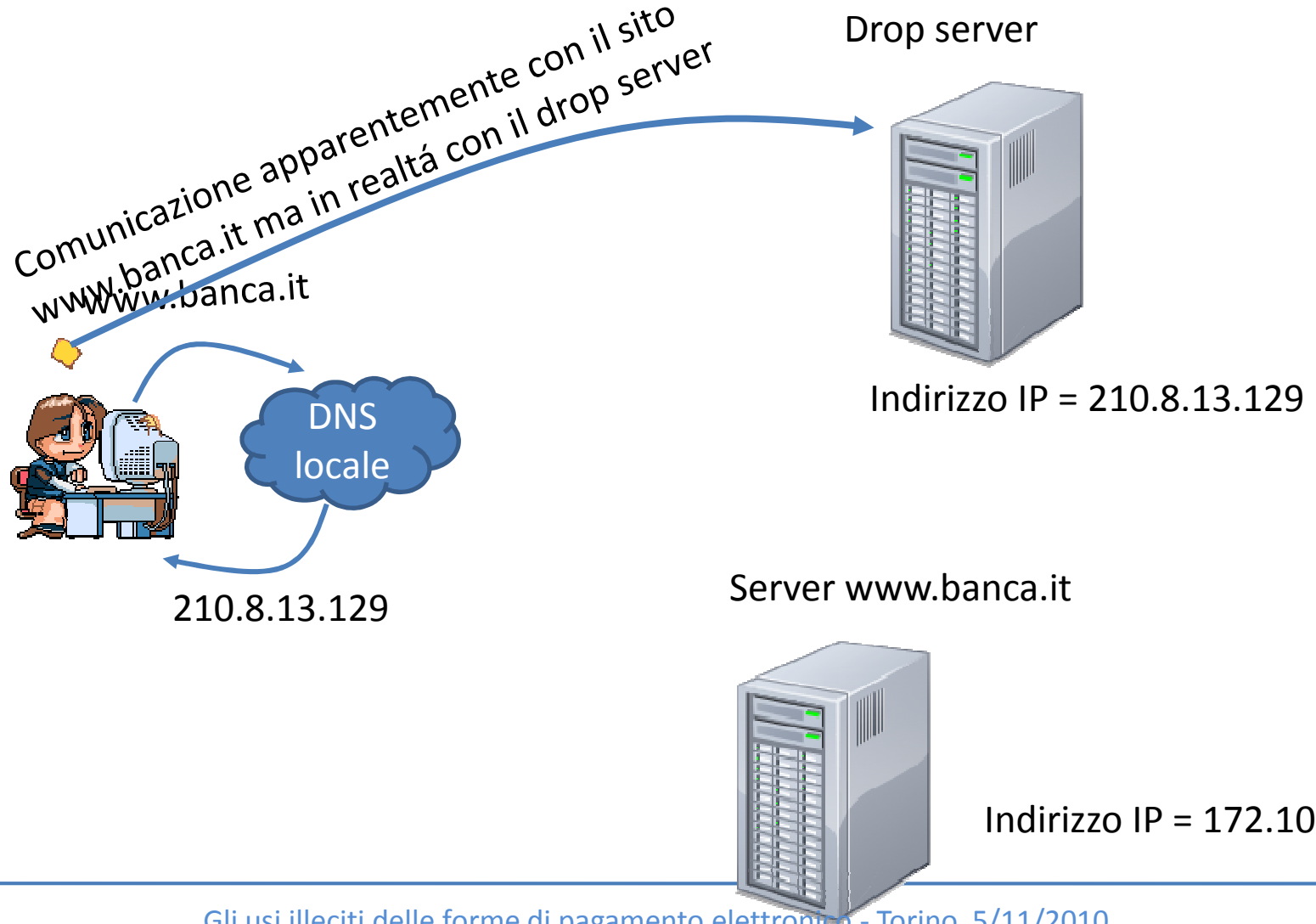
Dirottamento della connessione

- Funzionamento normale



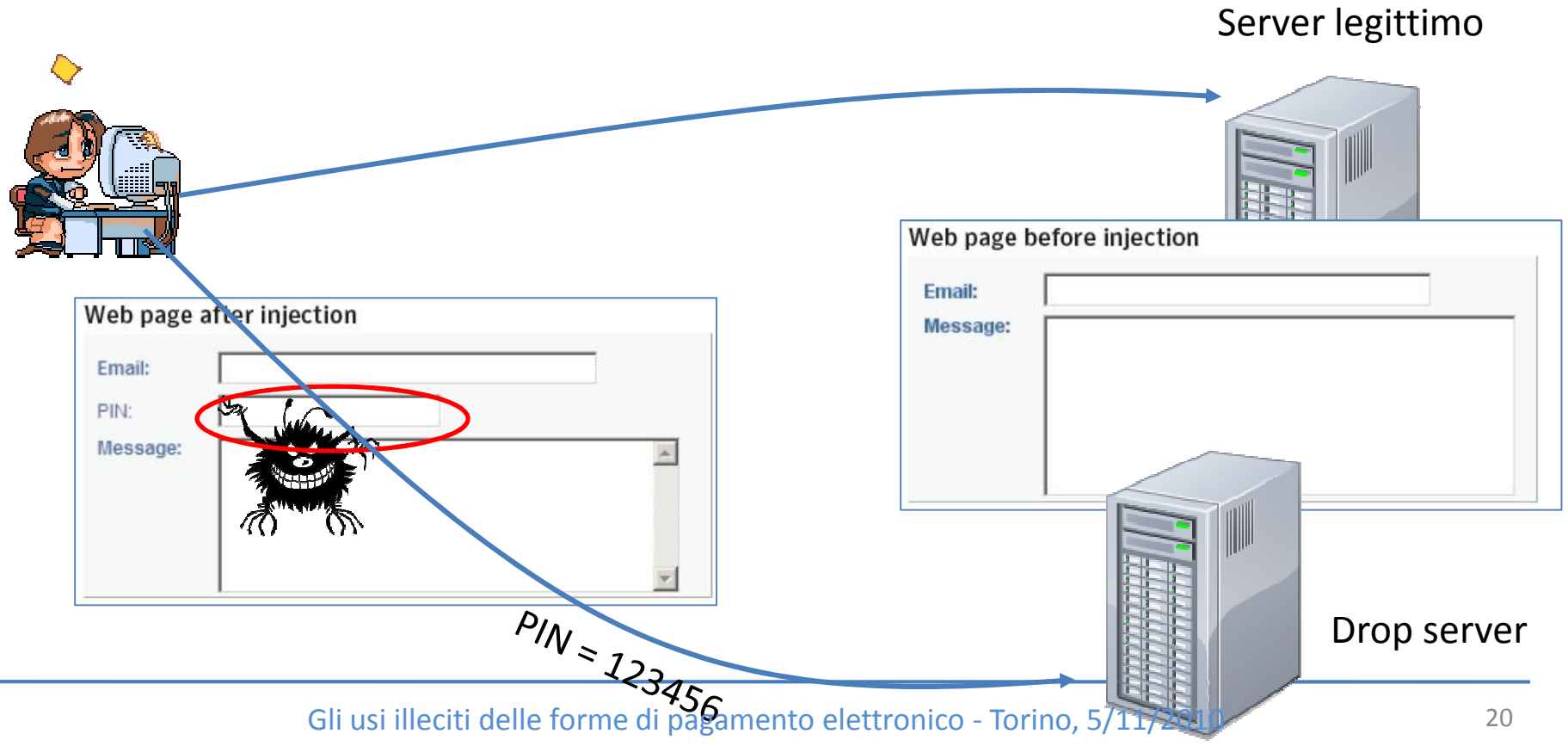
Dirottamento della connessione

- Connessione dirottata



Web page injection

- Reperimento della pagina web richiesta, sua modifica in tempo reale, ed invio delle informazioni immesse ad un drop server (*man-in-the-browser*)

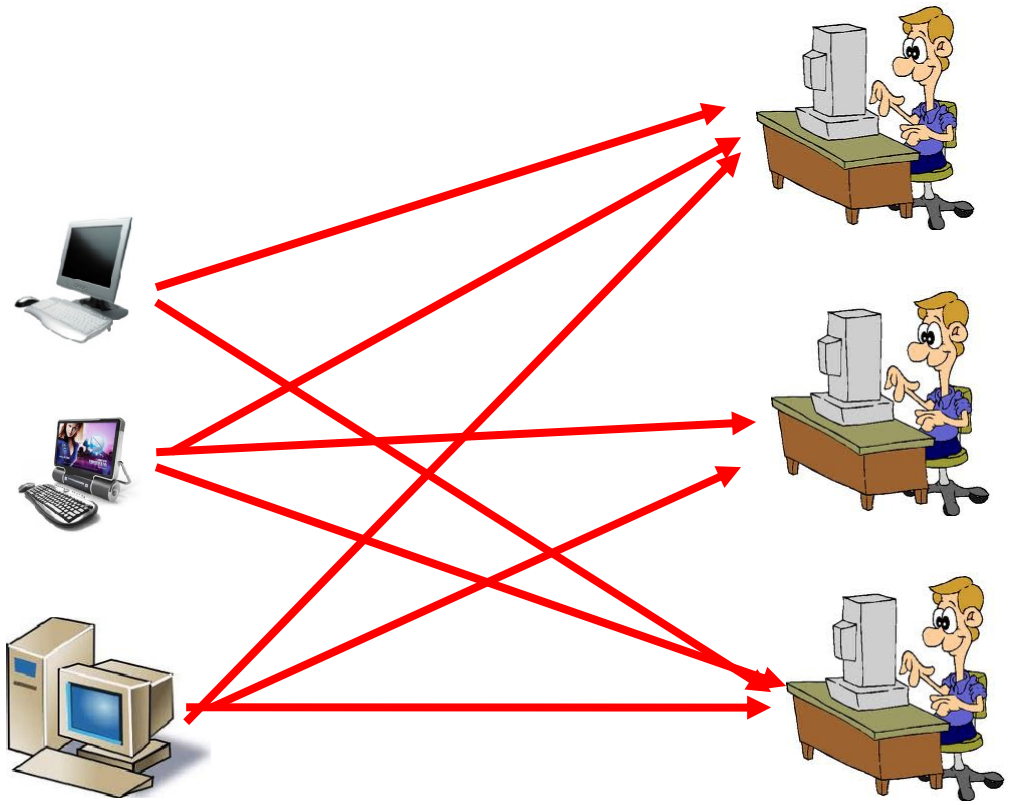


Le Botnet: di tutto, di piú

- Malware che permette ad un controllore remoto di assumere il controllo del computer
  - sul computer infettato viene eseguito un agente software (detto '*bot*')
- Il computer diventa uno "*zombie*": resta in attesa di comandi provenienti da un centro di Controllo e Comando (C&C)
- *Botnet* = rete di bot
- *Bot herder* = gestore della botnet

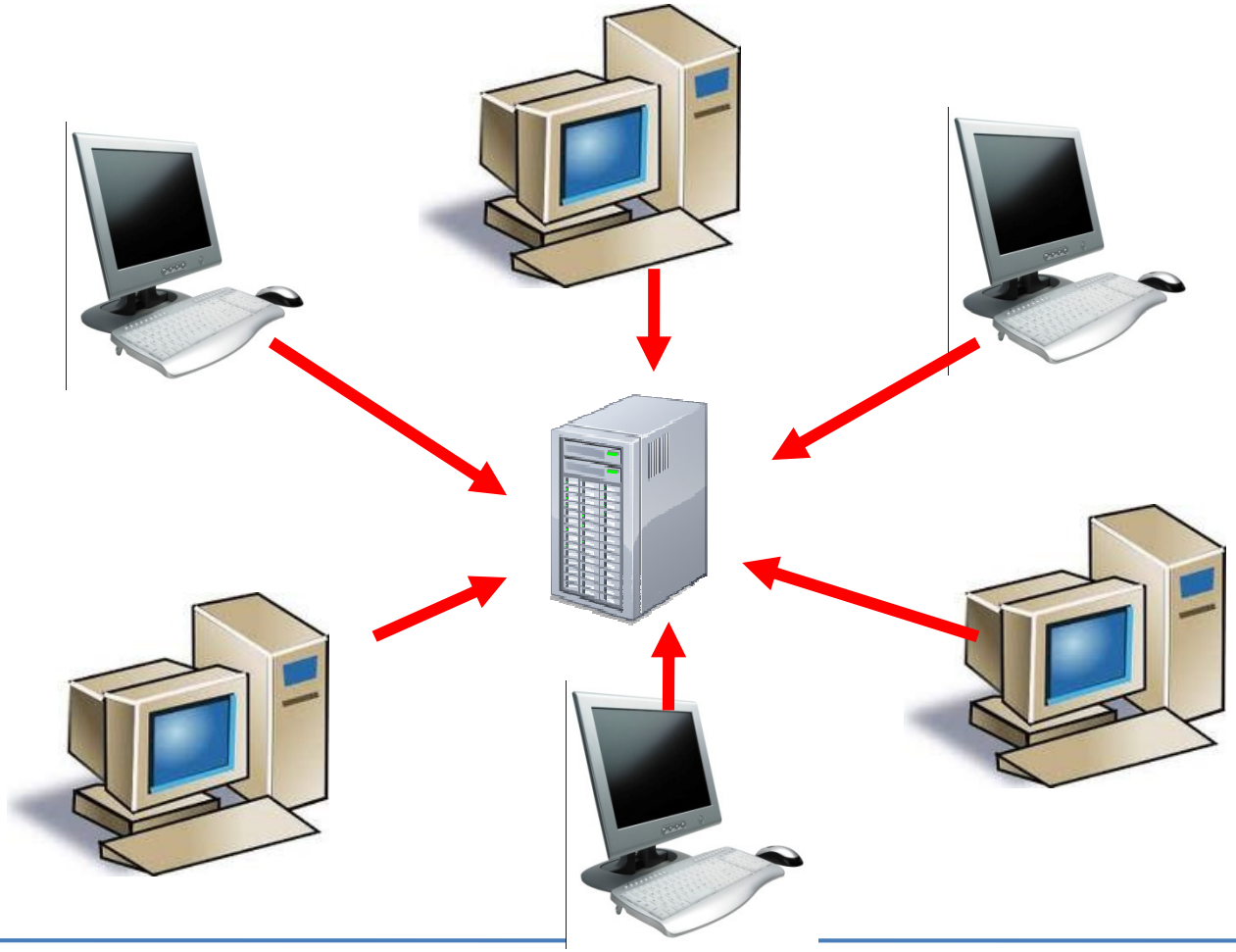
Botnet: usi tipici

- Invio di messaggi di spam senza che il vero autore sia rintracciabile



Botnet: usi tipici

- Attacchi “distributed denial of service”



Botnet: usi tipici

- Sottrazione di dati riservati
  - Banking/financial botnets
- Utilizzano una combinazione delle tecniche si sottrazione dati descritte in precedenza
- Utilizzano una combinazione di veicoli di infezione per diffondersi piú efficacemente

La botnet Zeus/Zbot

- Probabilmente la botnet bancaria piú nota grazie alla copertura sui media
  - non é peró l'unica, né quella piú aggressiva
- Combina una botnet (*Zbot*) con un malware in grado di sottrarre dati riservati (*Zeus*)
- Prima rilevazione nel 2007
  - sviluppata inzialmente in un paese di lingua russa
  - evoluzioni successive e continue ne hanno aumentato il potenziale offensivo

Funzionalitá di Zeus

- Acquisizioni di informazioni di sistema:
  - Nome e versione della bot
  - Versione e lingua del sistema operativo del computer infettato
  - Ora locale impostata sul computer infettato
  - Paese in cui si trova il computer infettato
  - Indirizzo IP del computer infettato

Funzionalitá di Zeus

- Furto di credenziali memorizzate su hard disk mediante tecniche di disk scanning
  - Password di account di posta elettronica POP 3 o IMAP
  - Password per servizi FTP
  - Credenziali e password salvata da Internet Explorer (dalla prossima versione anche da Firefox)

Funzionalitá di Zeus

- Furto di credenziali bancarie
  - Intercettazione di qualunque dato inviato ai siti web elencati in un file di configurazione o filtraggio di parole specifiche (username, password, ecc.)
  - Dirottamento delle connessioni
  - TANGrabber: aquisizione dei Transaction Authentication Number) utilizzati per le transazioni bancarie
  - Web page injection

Funzionalitá di Zeus

- Funzioni di controllo del computer infettato:
  - Spegnimento/riavvio del computer
  - Cancellazione dei file di sistema
  - Accesso remoto al computer ed esecuzione di comandi dallo stesso
  - Aggiornamento del file di configurazione
  - E molte altre

Zeus: veicoli di infezione

- Molteplici, principalmente drive-by downloads ottenuti mediante finti messaggi email

From: FDIC
Date: [Header Details Removed]
To: [Header Details Removed]
Subject: FDIC alert: check your Bank Deposit Insurance Coverage

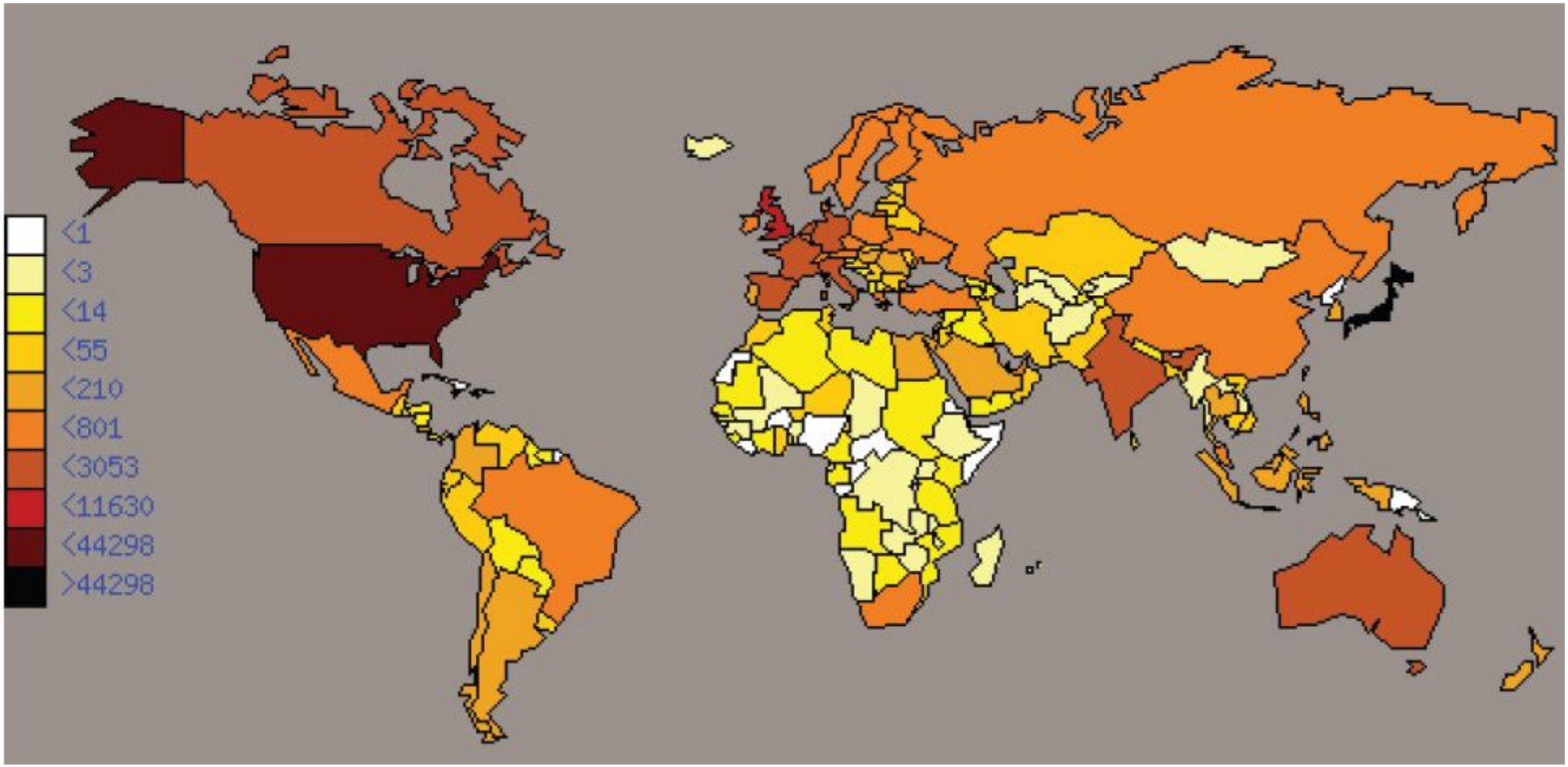
You have received this message because you are a holder of a FDIC-insured bank account.
Recently FDIC has officially named the bank you have opened your account with as a failed bank, thus, taking control of its assets.

You need to visit the official FDIC website and perform the following steps to check your Deposit Insurance Coverage:

- Visit FDIC website:
  http://www.fdic.gov/bankinsured/failed/personalfile/holder.php?email=[redacted]&id=3697342892747411130595691046927301254126 52
- Download and open your personal FDIC Insurance File to check your Deposit Insurance Coverage

FDIC Federal Deposit Insurance Corporation

Diffusione di Zeus



Dati di ottobre 2009 – tratti da N. Falliere ed E. Chien, “Zeus: King of the Bots”

Zeus: prezzi di mercato

- Zeus viene venduto dal suo autore (sconosciuto) ed ha dei meccanismi di protezione dalla copia
- Prezzi attualmente rilevati:

– Zeus Kit: $3K - $4K	
– Backconnect	$1500
– Firefox form grabber	$2000
– Jabber (IM) chat plugin	$500
– VNC (Virtual Network Computing) private module	$10K
– Windows 7/ Vista Support	$2000

*Note: Unauthorized Zeus variant copies sold in the underground would go for ~$800

Dati tratti dal bollettino "RSA Online Fraud Report" del mese di Agosto 2010

Zeus: solo computer?

- *Zitmo – Zeus in the mobile*:
  - telefoni smartphone Blackberry o che utilizzano il sistema operativo Symbian
  - Rilevata nel Settembre 2010
  - Infezione mediante scaricamento di software in seguito alla ricezione di un SMS
  - informazioni su numero telefonico e marca/modello del telefono carpite mediante Zeus

Zeus: solo computer?

- Uso di one-time password via SMS per evitare attacchi tipo man-in-the-browser

Richiesta transazione

Immissione del codice one-time

Zeus: solo computer?

Invio tramite SMS di codice one-time per la convalida della transazione

Inoltro del codice one-time all'insaputa della vittima

Accesso mediante user name e password

Richiesta transazione

Immissione del codice one-time

Zeus, ma non solo …

- *Mariposa*: particolarmente efficace
  - Ha infettato circa 12,000,000 di computer
  - Autore arrestato in Slovenia all'inizio del 2010
- *SpyEye*: prevede anche un "Zeus killer" per soppiantare Zeus all'interno del computer che infetta

Zeus, ma non solo …

- *Bugat*: simile a Zeus, diffuso mediante Zbot
- *Carberp*
- *Feodo*: l'ultimo arrivato (in ordine di tempo)
  - Individuato a metá Ottobre 2010
  - Maggiori capacitá rispetto a Zeus

Diffusione del fenomeno

- Alcune statistiche sulla diffusione:
  - Zeus: si stimano 3.600.000 computer infettati solo negli USA
  - Mariposa: stimati 12.000.000 di computer infettati
- Puó un solo individuo/gruppo gestire un flusso cosí alto di informazioni?

Diffusione del fenomeno

- In realtá, l'uso di tecnologie botnet non é limitato ai soli esperti di informatica
  - Vendita di veri e propri kit che automatizzano la customizzazione del malware e la sua veicolazione
  - Sistemi semplificati di controllo e comando dei bot
- Potenziale di diffusione estremamente elevato nella comunitá criminale

Rilevamento di botnet

- Il malware puó essere individuato mediante antivirus
- Gli antivirus riconoscono un programma malware solo dopo che lo stesso é stato rilasciato
  - nel frattempo, i computer possono essere infettati

Rilevamento di botnet

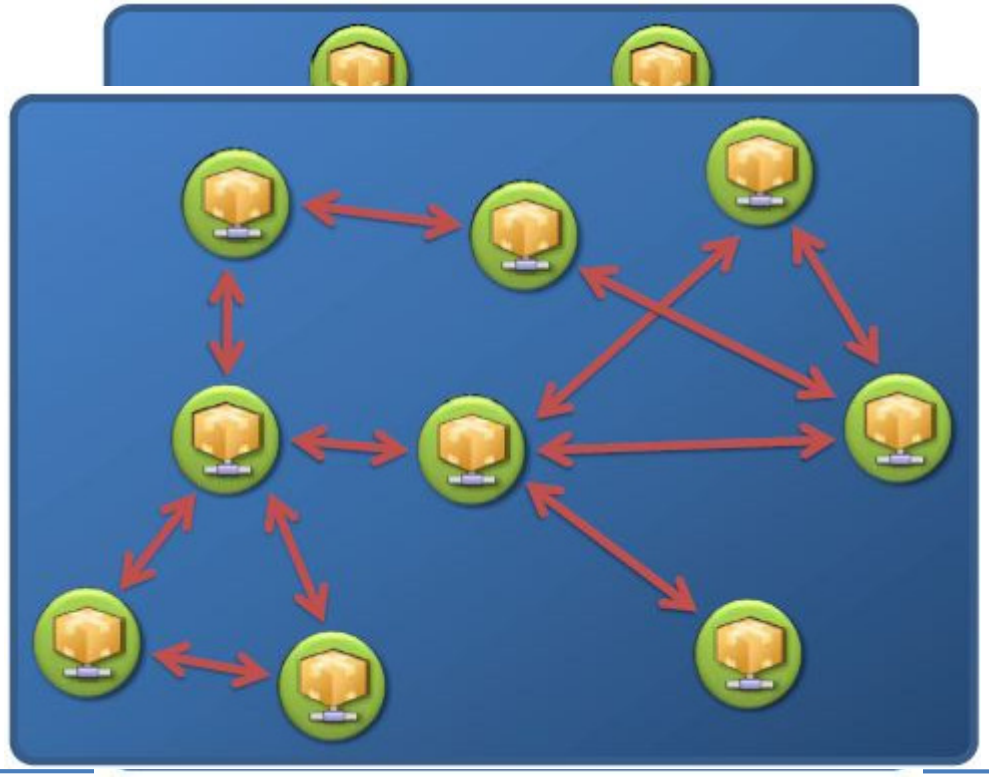
- Un software bot puó essere individuato cercando le sue comunicazioni al C&C
  - Spesso sono usate comunicazioni cifrate o offuscate: facili da individuare
- Le botnet di ultima generazione utilizzano canali di comunicazione standard, quali post su Twitter o su Facebook

Smantellamento di botnet

- Individuazione e neutralizzazione del centro C&C
- Le botnet di ultima generazione utilizzano tecniche sofisticate per rendere difficoltosa l'individuazione dei server C&C

Smantellamento di botnet

- Inoltre, sono utilizzate tecniche di ridondanza in cui i server C&C formano una rete



Concludendo….

- Gli strumenti tecnici per la sottrazione di dati riservati sono molto sofisticati
- Gli strumenti tecnici di contrasto sono relativamente efficaci dopo che il malware é stato esaminato

Concludendo….

- Per un contrasto efficace é fondamentale la collaborazione dell'utente, il quale deve essere "educato" ad un uso consapevole dei servizi di rete, che costituiscono il veicolo attraverso cui il malware si propaga