BOTNET: Information Warfare

Theory and Practices from "the Scene"

27 Marzo 2008
Black Sun Factory Research Team

Definizione di Virus

- Nell'ambito dell'informatica un virus è un frammento di software, appartenente alla categoria dei malware, che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, generalmente senza farsi rilevare dall'utente. I virus possono essere o non essere direttamente dannosi per il sistema operativo che li ospita, ma anche nel caso migliore comportano un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso. Come regola generale si assume che un virus possa danneggiare direttamente solo il software della macchina che lo ospita, anche se esso può indirettamente provocare danni anche all'hardware, ad esempio causando il surriscaldamento della CPU mediante overclocking, oppure fermando la ventola di raffreddamento.

- Nell'uso comune il termine virus viene frequentemente usato come sinonimo di malware, indicando quindi di volta in volta anche categorie di "infestanti" diverse, come ad esempio worm, trojan o dialer.

Tratto da Wikipedia: **http://it.wikipedia.org/wiki/Virus_(informatica)**

Definizione di Worm

- Un worm è una particolare categoria di malware in grado di autoreplicarsi.
- È simile ad un virus, ma a differenza di questo non necessita di legarsi ad altri eseguibili per diffondersi.
- Tipicamente un worm modifica il computer che infetta, in modo da venire eseguito ogni volta che si avvia la macchina e rimanere attivo finché non si spegne il computer o non si arresta il processo corrispondente.
- Il mezzo più comune impiegato dai worm per diffondersi è la posta elettronica: il programma maligno ricerca indirizzi e-mail memorizzati nel computer ospite ed invia una copia di sé stesso come file allegato (attachment) a tutti o parte degli indirizzi che è riuscito a raccogliere.
- Questi eseguibili maligni possono anche sfruttare i circuiti del file sharing per diffondersi. In questo caso si copiano tra i file condivisi dall'utente vittima, spacciandosi per programmi ambiti o per crack di programmi molto costosi o ricercati, in modo da indurre altri utenti a scaricarlo ed eseguirlo.
- La tipologia forse più subdola di worm sfrutta dei bug di alcuni software o sistemi operativi, in modo da diffondersi automaticamente a tutti i computer vulnerabili connessi in rete.

Definizione di Trojan

- Un trojan o trojan horse (dall'inglese per Cavallo di Troia), è un tipo di malware. Deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice trojan nascosto.

- In genere col termine Trojan ci si riferisce ai trojan ad accesso remoto (detti anche RAT dall'inglese Remote Administration Tool), composti generalmente da 2 file: il file server, che viene installato nella macchina vittima, ed un file client, usato dal pirata per inviare istruzioni che il server esegue. In questo modo, come con il mitico stratagemma adottato da Ulisse, la vittima è indotta a far entrare il programma nella città, ossia, fuor di metafora, ad eseguire il programma. Esistono anche alcuni software legali con funzionalità simili ai trojan, ma che non sono dei cavalli di Troia poiché l'utente è consapevole della situazione.

Trojan: diffusione e funzionalità

- I trojan non si diffondono autonomamente come i virus o i worm, quindi richiedono un intervento diretto dell'aggressore per far giungere l'eseguibile maligno alla vittima. Spesso è la vittima stessa a ricercare e scaricare un trojan sul proprio computer, dato che i cracker amano inserire queste "trappole" ad esempio nei videogiochi piratati, che in genere sono molto richiesti.
- Un trojan può contenere qualsiasi tipo di istruzione maligna. Spesso i trojan sono usati come veicolo alternativo ai worm e ai virus per installare delle backdoor o dei keylogger sui sistemi bersaglio.
- All'incirca negli anni successivi al 2001 o 2002 i trojan incomiciarono ad essere utilizzati sistematicamente per operazioni criminose; in particolare per inviare messaggi di spam e per rubare informazioni personali quali numeri di carte di credito e di altri documenti o anche solo indirizzi email.
- I Trojan di nuova generazione hanno molteplici funzionalità, quali connessioni tramite IRC bot, formando appunto Botnet, e opzioni per nascondersi meglio nel sistema operativo, utilizzando tecniche di Rootkit.

Componenti di un Malware

- I Malware più semplici sono composti da due parti essenziali, sufficienti ad assicurarne la replicazione:
  - una routine di ricerca, che si occupa di ricercare dei file adatti ad essere infettati;
  - una routine di infezione, con il compito di copiare il codice del Malware all'interno di ogni file selezionato dalla routine di ricerca.
- Molti Malware sono progettati per eseguire del codice estraneo alle finalità di replicazione e contengono dunque altri due elementi:
  - la routine di attivazione;
  - il payload.
- I virus possono essere criptati e magari cambiare algoritmo e/o chiave ogni volta che vengono eseguiti, quindi possono contenere altri tre elementi:
  - una routine di decifratura;
  - una routine di cifratura;
  - una routine di mutazione, che si occupa di modificare le routine di cifratura e decifratura per ogni nuova copia del virus.

Gli AV e le strategie di analisi

- Gli antivirus per identificare un contenuto malevolo poggiano sulle cosiddette **“firme”** o **“signatures”**, ovvero sull'azione di confronto tra un contenuto analizzato ed i vari contenuti malevoli possibili, se in questo senso il contenuto malevolo non è censito nelle firme l'Antivirus non lo può identificare come malware.
- **Scansione euristica**: questa tecnica tenta di rilevare forme note e nuove di software dannoso cercandone le caratteristiche generali. Il vantaggio principale di questa tecnica è che non si basa sui file delle firme per identificare e contrastare il software dannoso. Lo svantaggio è la lentezza e il rischio di Falsi positivi.

Non puoi fermare quanto non è visto come una minaccia!...

- **Un antivirus, al pari di un HIPS, non può impedire che un codice non individuato dalle signatures o da analisi euristiche venga installato. A volte chiede conferma all'utente, ma anche questo non basta. Non si può confidare sull'informazione e le conoscenze dell'utente in merito alla bontà di un codice non identificato (effetto Zone-Alarm).**

- I modelli di difesa sono di tipo reattivo non proactive.
- Il modello per Signature a volte viene reso inefficace dalle varianti dei virus e dei Bot-worm
- Le nuove varianti appaiono prima che le signature siano create
- Alcuni Bot-worm hanno la capacità di aggiornarsi o di installare plug-in per inibire i controlli
- Il modello entra in crisi anche nel caso di attacchi zero-day
- Quando si introducono difese proattive si cade fatalmente nel rischio dei falsi positivi

Tecniche di offuscamento

- Nel passato alcuni crackers sono riusciti ad aggirare i programmi antivirus utilizzando dei payload crittografati con cui veicolare i loro attacchi. Ad esempio utilizzando UPX (The Ultimate Packer for eXecutables) e Morphine, un programma per crittare i dati. Ma abbiamo payload diffusi anche attraverso file GDI+ e JPEG che permettono di nascondere ulteriormente i Trojan horse compattati via UPX e crittografati via Morphine in modo da poter superare facilmente le prime difese impostate dagli utenti attraverso i filtri di contenuto o gli antivirus.

Definizione di BotNet

- Botnet è un termine usato per definire un'insieme di software robots, o "bots", che lavorano in modo autonomo e automatico. Questi software bot vengono solitamente controllati da remoto.
- In genere quindi la parola Botnet viene usata per definire un'insieme di computer compromessi (chiamati anche zombies o drones) che vengono controllati da remoto attraverso programmi di tipo worm, trojan o backdoor da una infrastruttura di gestione comune.
- Un botnet operator (anche definito "bot herder") può controllare remotamente il gruppo di zombie attraverso canali di raccolta dei sistemi compromessi quali IRC, dei server web o degli altri programmi di messaggistica online.

Definizione di Botnet

- Tradizionalmente il centro di “comando e controllo” (C&C) è posto all’interno di canali IRC privati (protetti da password) sui quali i sistemi zombies si loggano a seguito della compromissione. Un bot software lavora in modalità nascosta al sistema e al suo leggittimo proprietario ed è conforme all’RFC 1459 (IRC) standard.
- La compromissione può essere legata a vulnerabilità sistemistiche (exploit, buffer overflow, ecc…) o all’esecuzione già in prima istanza di trojan horse
- La prima operazione compiuta da un nuovo bot compromesso è l’ingresso nel canale di controllo a cui segue solitamente una fase automatica di scansione del segmento di rete locale del sistema compromesso per cercare nuove possibili vittime per allargare la compromissione ad altri PC.

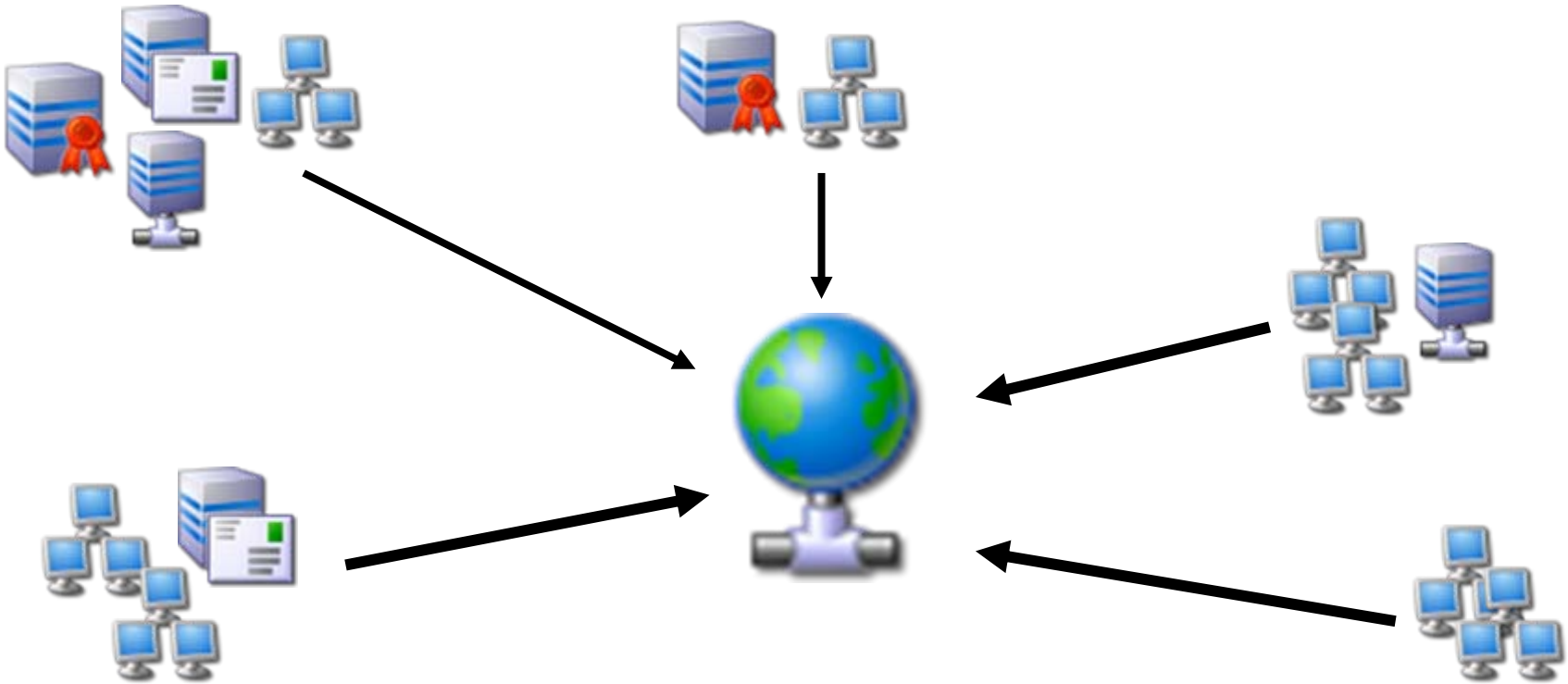
… Ma quanto sono pericolose queste Botnet?

"I bei vecchi tempi"...





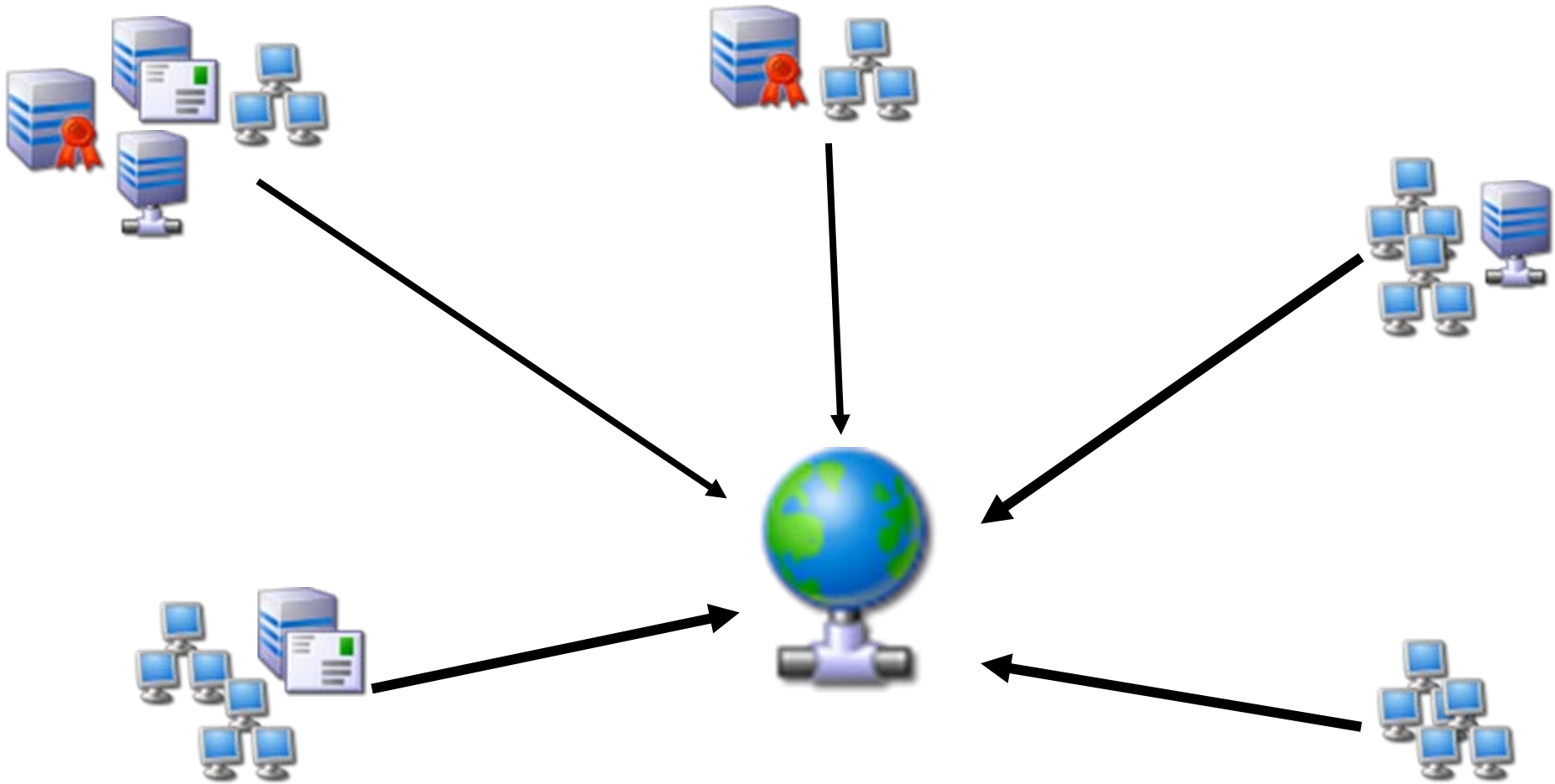

"I bei vecchi tempi"...



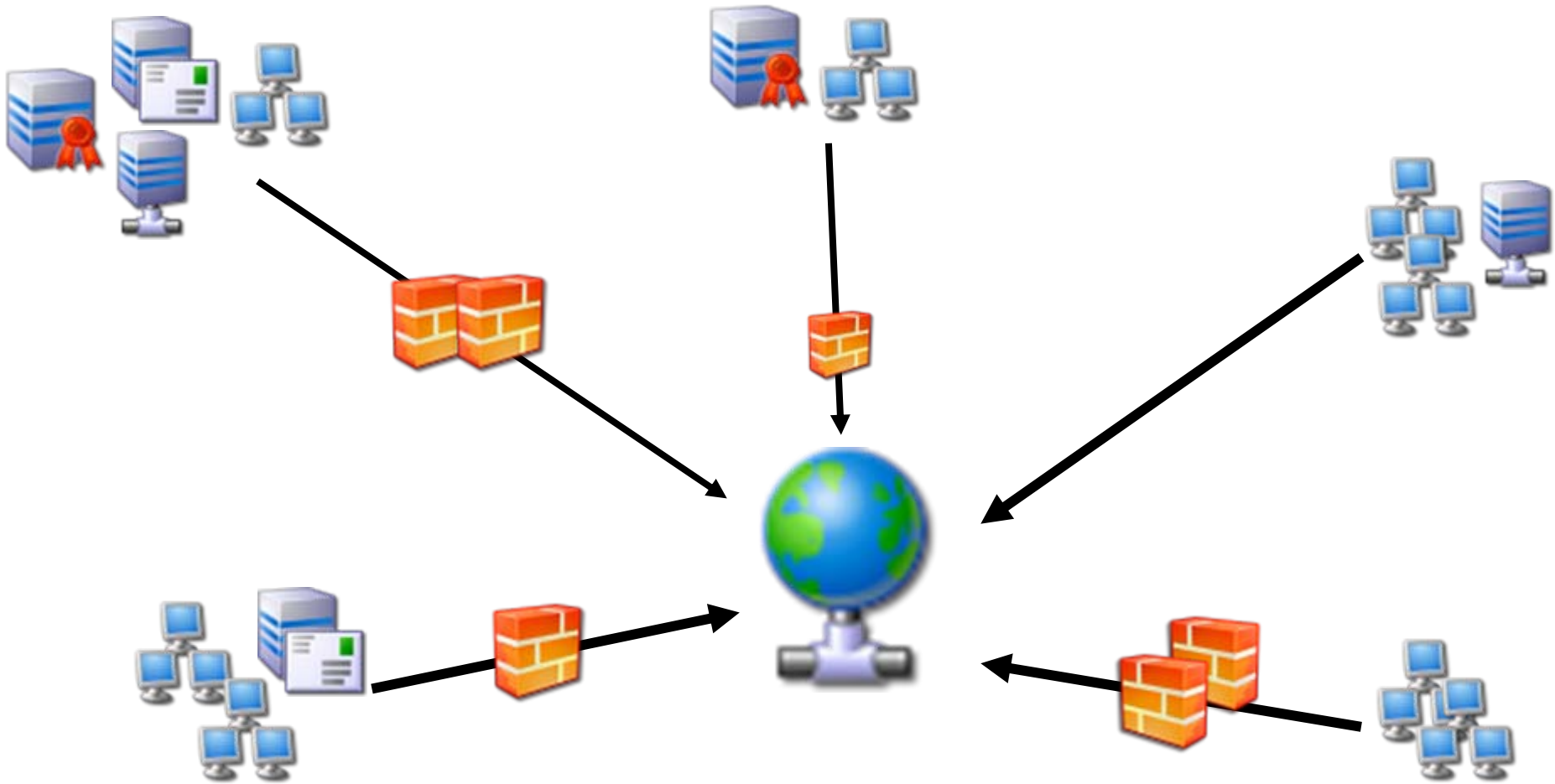
"I bei vecchi tempi"...

- Gli attacchi erano svolti su singoli bersagli
- I trojan erano sviluppati per controllare singole macchine o piccoli gruppi
- Le infezioni si diffondevano lentamente
- I vettori erano i classici:
  - software (Malware),
  - eMail attachment,
  - Exploit diretto di vulnerabilità
  - Programmi di Chat

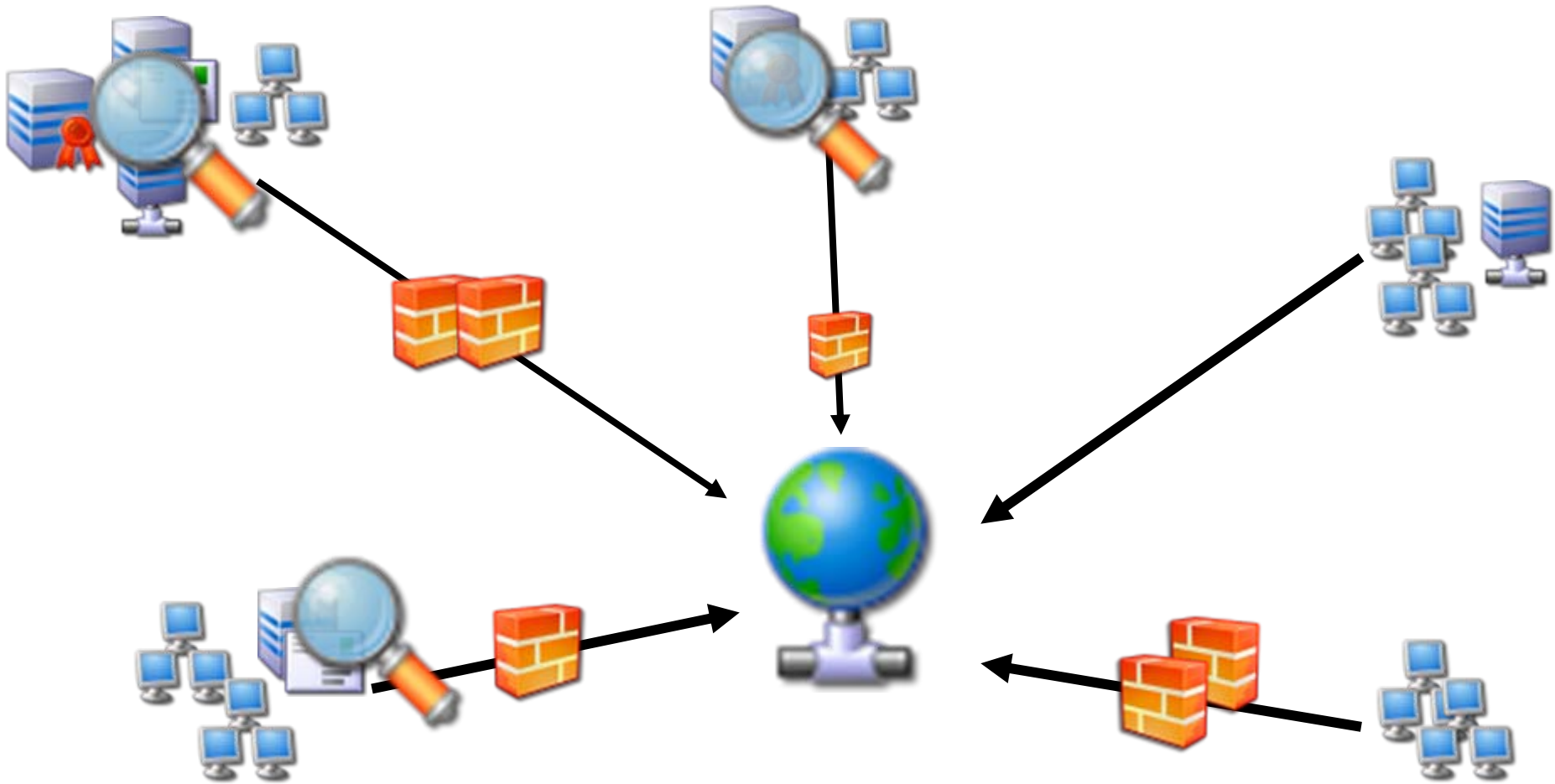
Internet oggi...



Internet oggi...



Internet oggi...



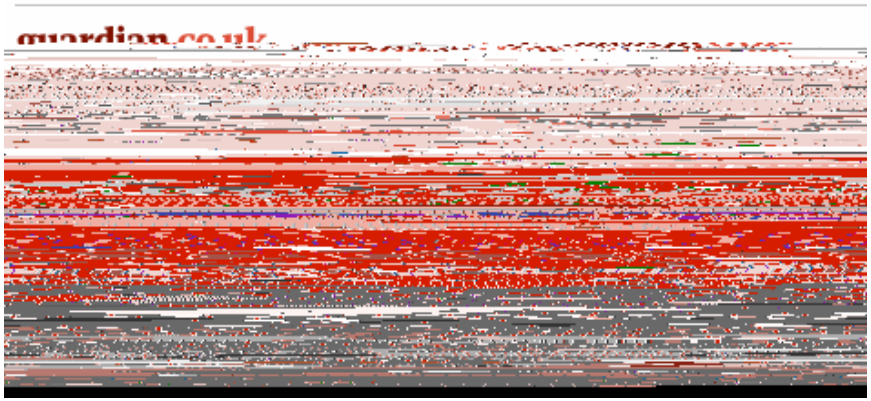
Antivirus, Firewalls, and more…

- L'attuale scenario mostra l'introduzione di alcune specifiche tecnologie utili nella lotta contro i tradizionali malware e il loro metodi di diffusione.
- Alcuni problemi sono quindi risolti, ma nonostante questo assistiamo ancora alla crescita della minaccia prodotta dalle Botnet.
- Le ragioni sono collegate a:
  - Cattive abitudini degli utenti Internet
  - Ignoranza
  - Mancanza di applicazione dei pure più basilari meccanismi di protezione

Per molti ma non per tutti…

- Cosa possiamo dire della situazione delle nazioni in via di sviluppo?
  - Dobbiamo vedere la IT Security in nuovi contesti.
  - Dobbiamo analizzare e valutare la spesa per la IT Security in queste nazioni
  - Dobbiamo abbandonare la percezione che Firewal e antivirus siano la panacea di ogni male
  - Le leggi contro Spam, Virus e violazioni informatiche non è allineata tra le varie nazioni

BotNet: Facts!



InfoWorld Log-in | Register

HOME | NEWS | TEST CENTER | TECHNOLOGIES | BLOGS | AUDIO/VIDEO | EVENTS | AWARDS | NEWSLETTERS | C

Estonia recovers from massive denial-of-service attack

Postings on Web sites indicate Russian hackers may be involved in the attacks

By Jeremy Kirk, IDG News Service
May 17, 2007

Talkback E-mail Printer Friendly Reprints Text Size A A

A spree of denial-of-service (DOS) attacks against Web sites in Estonia appears to be subsiding, as the government calls for greater response mechanisms to cyber attacks within the European Union.

Usi di una BotNet

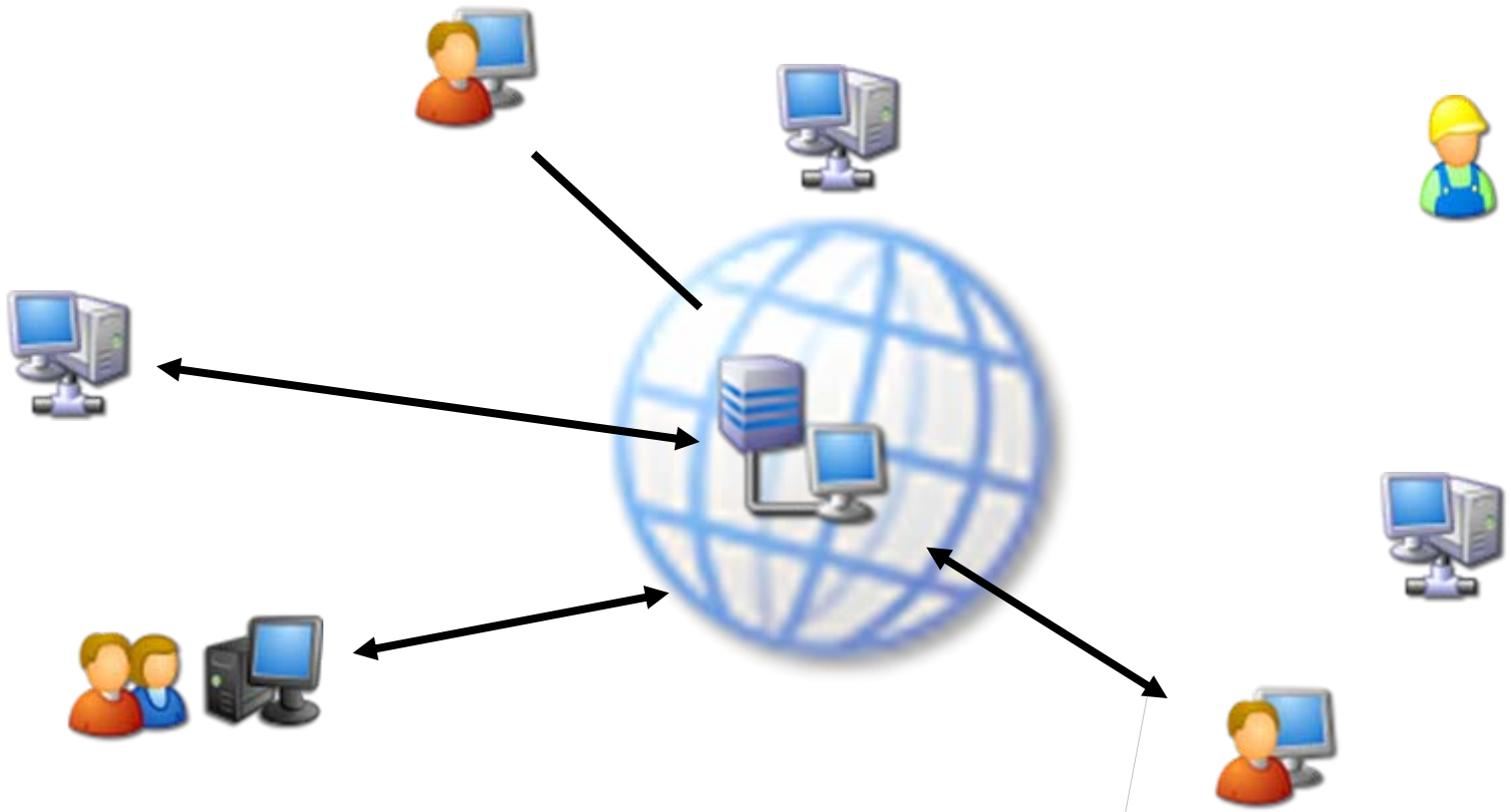
La flessibilità delle botnets è mostrata dalle tante possibili applicazioni malevole che si possono realizzare con esse:

- Distributed Denial-of-Service attacks
- Spamming
- Spreading malware
- Traffic sniffing
- Keylogging
- Identity theft

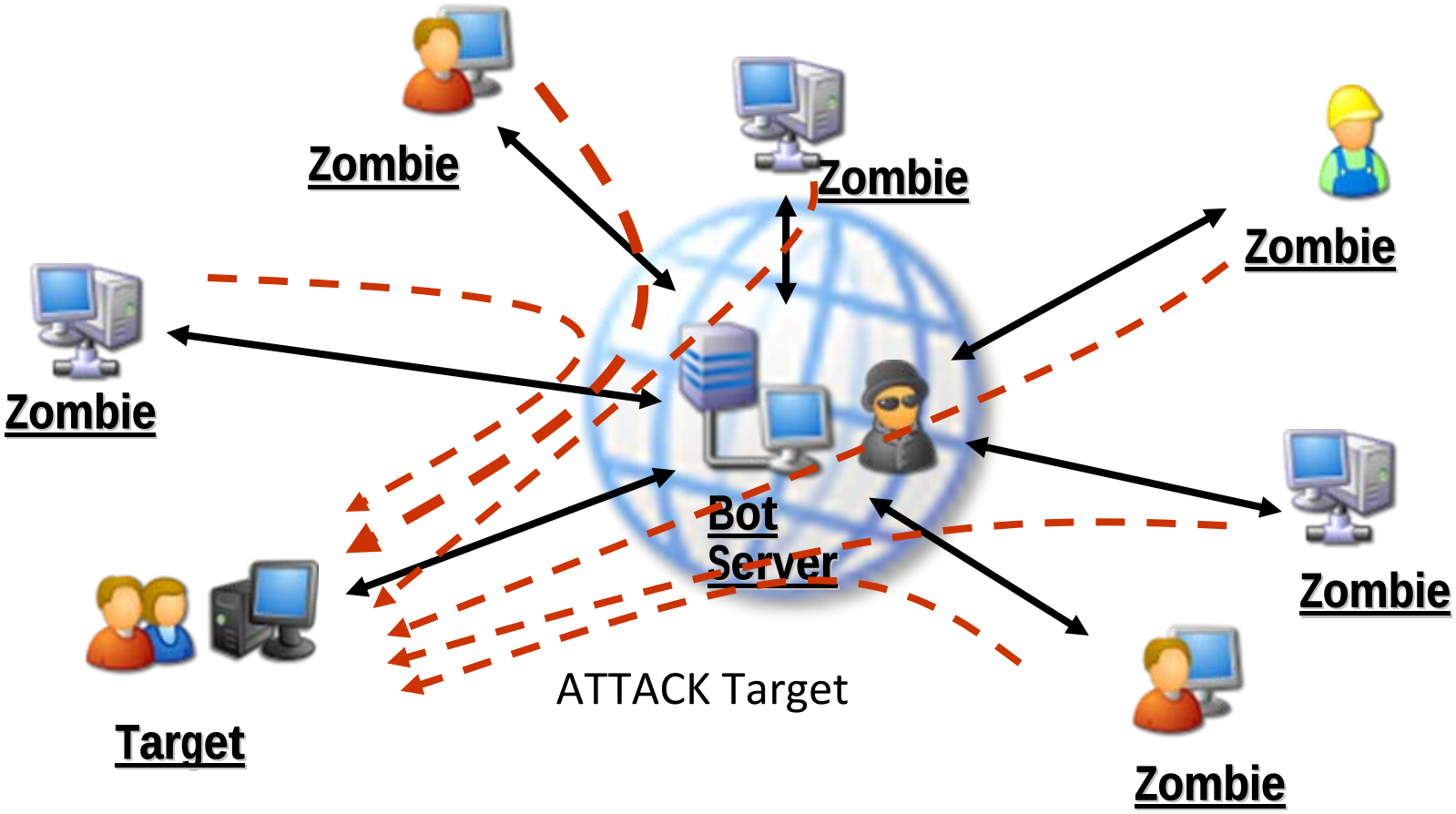
DDoS Attacks

- Un Denial-of-Service (DoS) è un attacco portato ad un host con l'obiettivo di disabilitarne uno o più servizi o funzionalità.
- Il DoS si perpetra sovraccaricando il servizio bersaglio. Questo sovraccarico (Flood) può essere generato dall'azione congiunta di varie macchine attaccanti. In questo caso si parla di Distributed Denial-of-Service (DDoS).
- Una botnet è la più efficace forma di controllo e di coordinamento per attuare attacchi DDoS

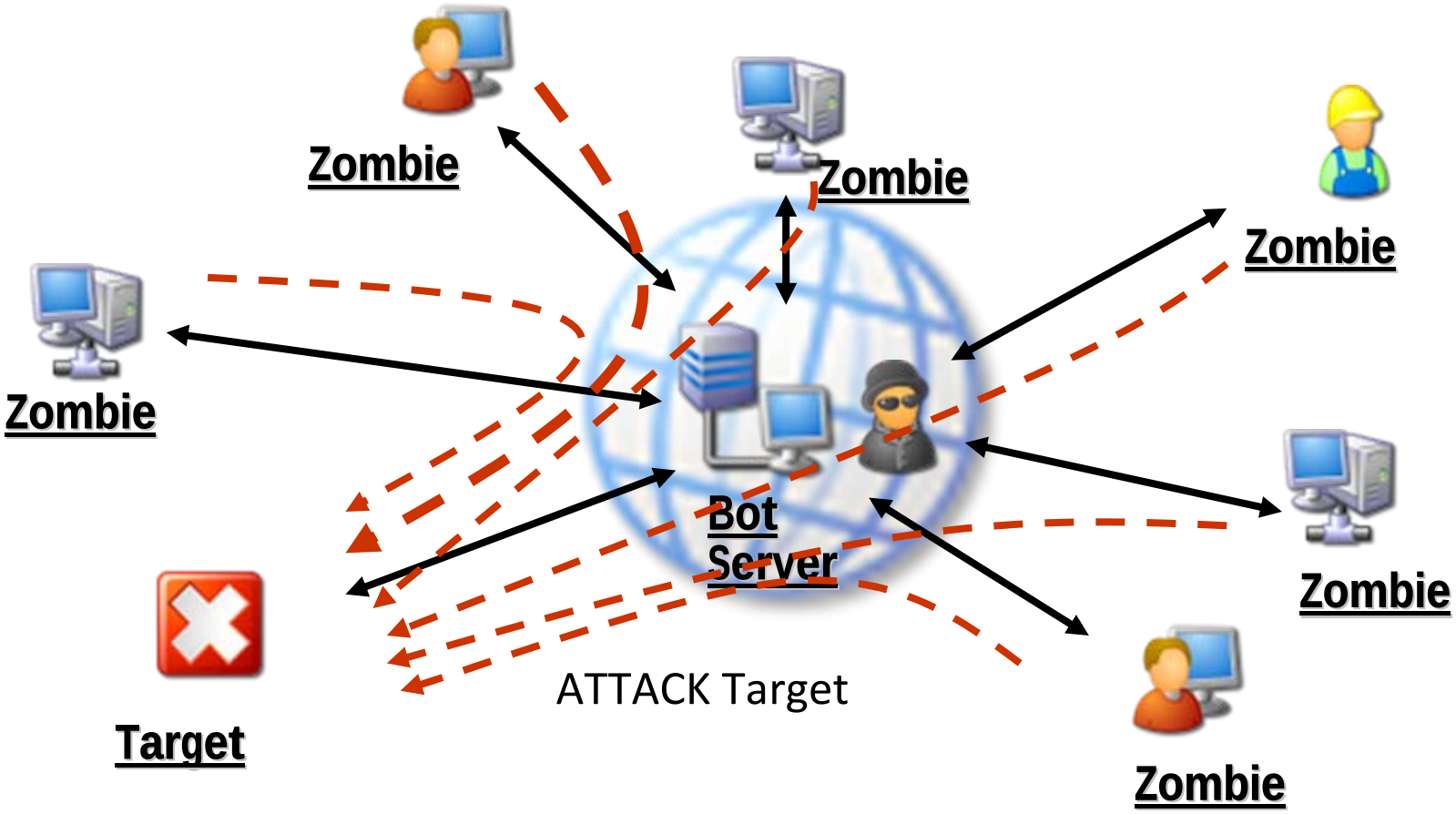
DDoS Attacks



DDoS Attacks



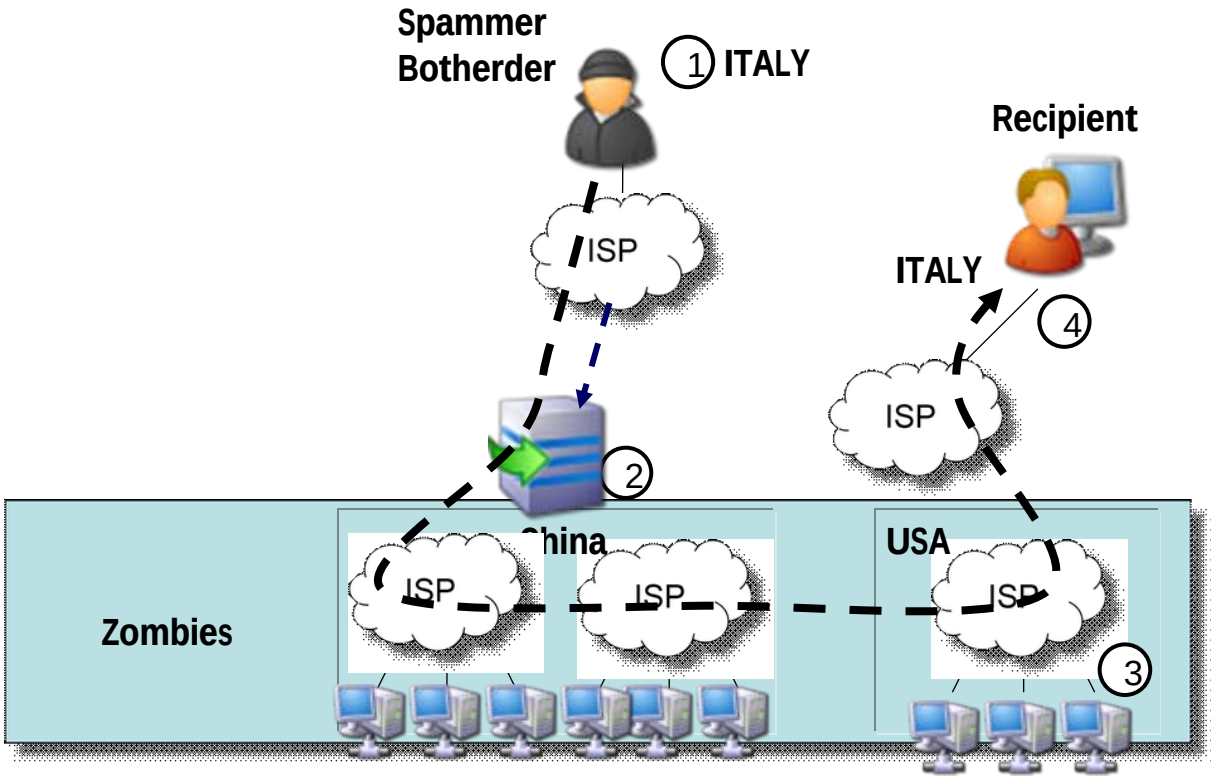
DDoS Attacks



Spam Distribution

- Un'altra comune forma di applicazione delle botnets è la distribuzione di spam. Questo metodo è efficace per i cyber criminali per creare guadagni attraverso l'infrastruttura botnet da loro creata e gestita.
- Una botnet può essere affittata ad aziende senza scrupoli che possono diffondere con essa advertisements pubblicitari in grandi volumi e in maniera molto efficiente evitando inoltre che i loro messaggi di spam possano venire filtrati da sistemi di protezione di tipo Antispam.
- Da dati raccolti e diffusi da aziende come SecureWorks la maggior parte dello spam mondiale è inviato attraverso sistemi clients con Windows XP a bordo.

Spam method of distribution

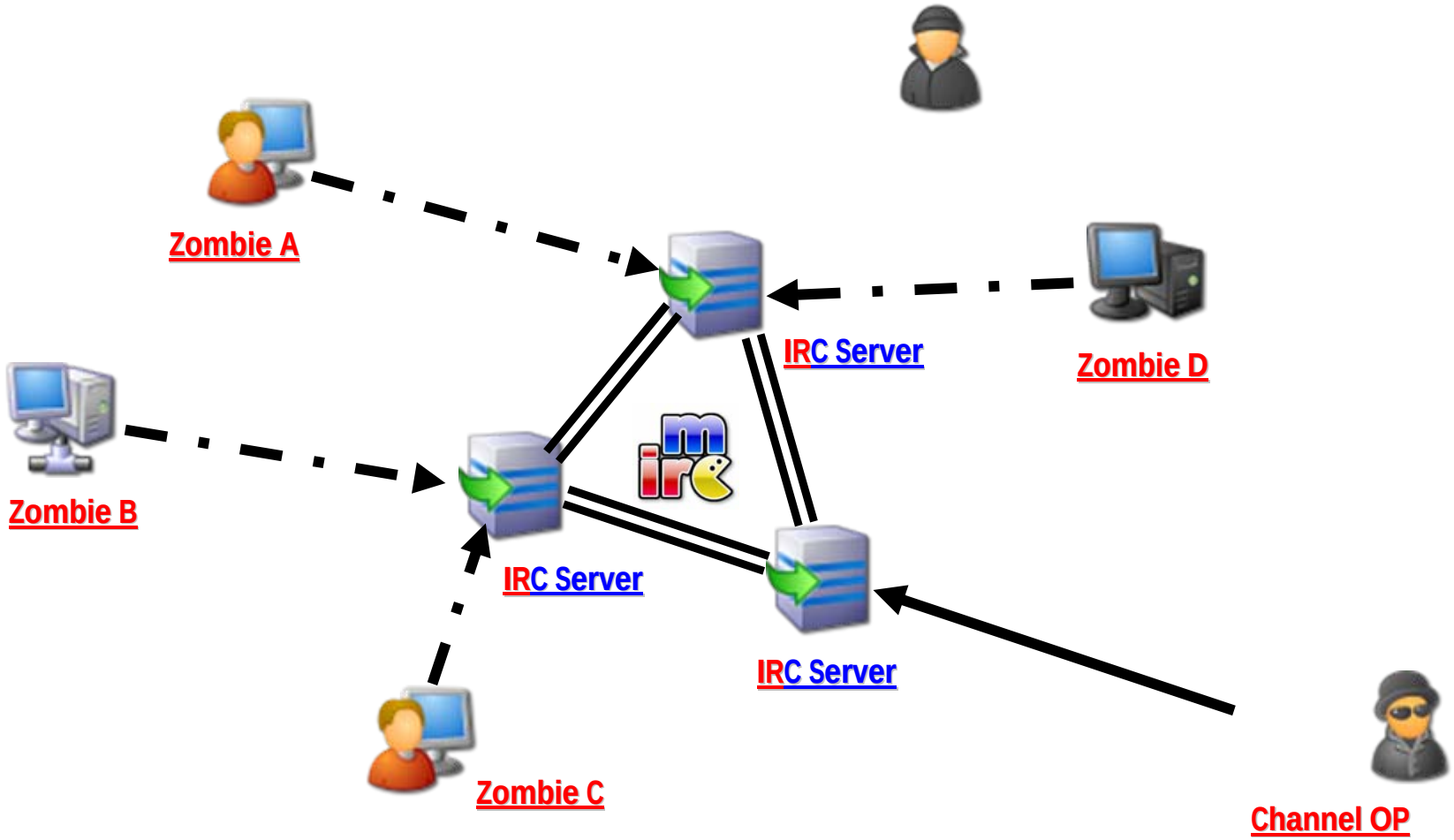


Malware distribution

- Un bot herder può usare la sua botnet per diffondere malware.
- Bots istruiti a compiere queste operazioni possono scaricare automaticamente adware o dialer.
- Questo permette altre forme di introito per i botnet herder, soprattutto laddove l'herder viene pagato per i classici hosts click o per la diffusione di advertisements.
- Per favorire il flusso economico il bot herder necessita a volte di conoscere l'esatta ubicazione dei propri zombie host in modo da garantire la rispondenza degli specifici adware installati con il mercato locale di riferimento.

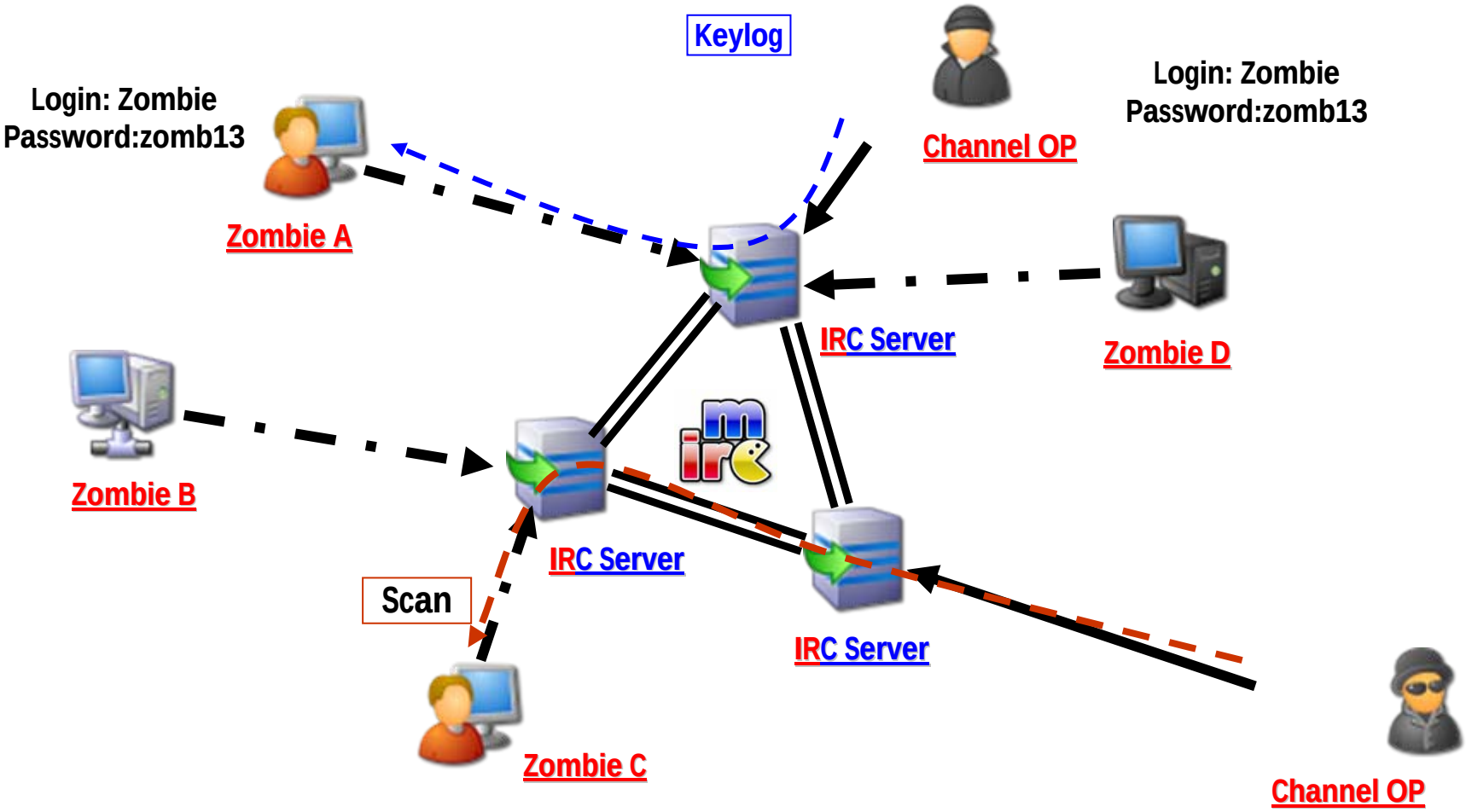
Sniffing, Keylogging & ID Theft

- Bot Channel operations include…



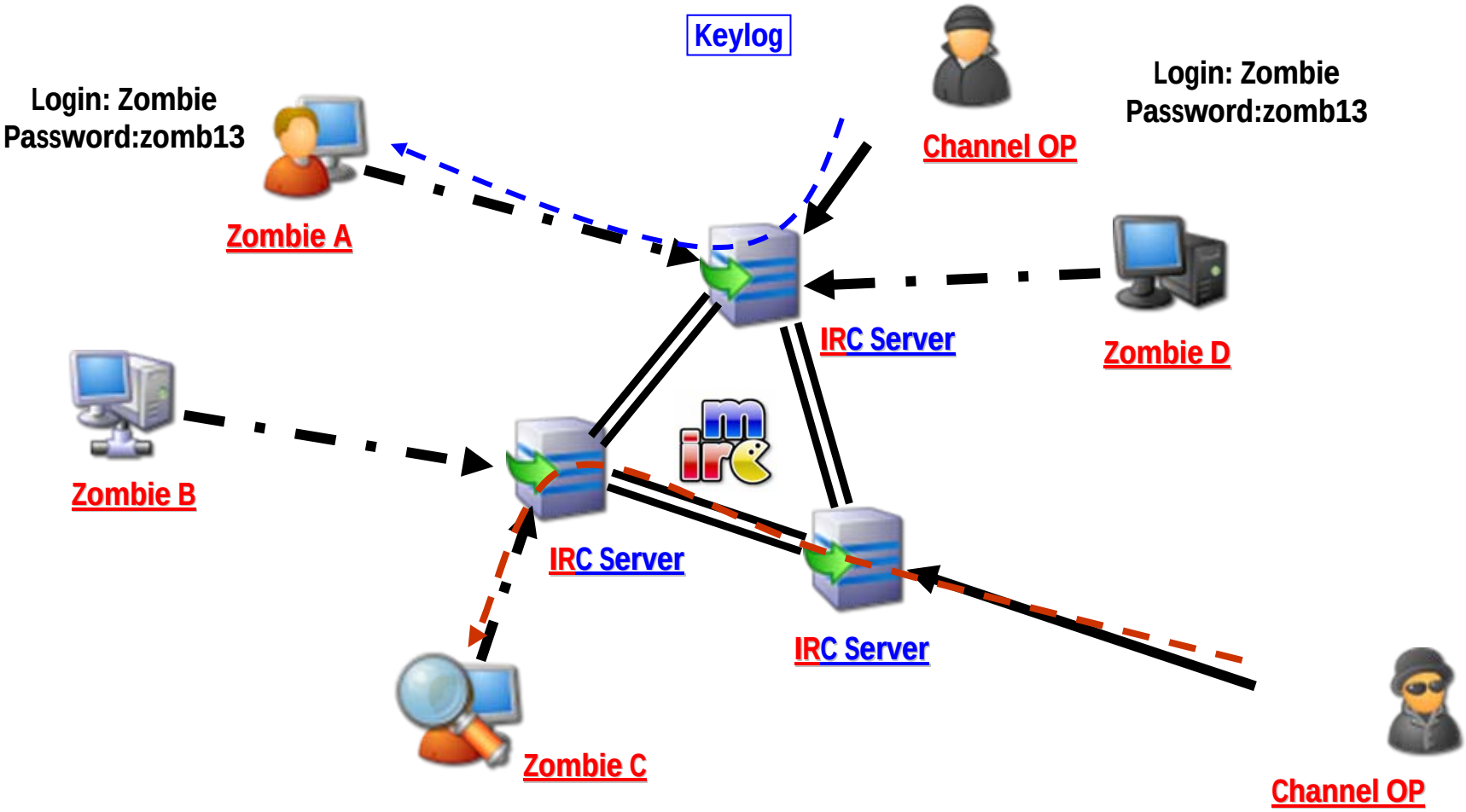
Sniffing, Keylogging & ID Theft

- Bot Channel operations include…



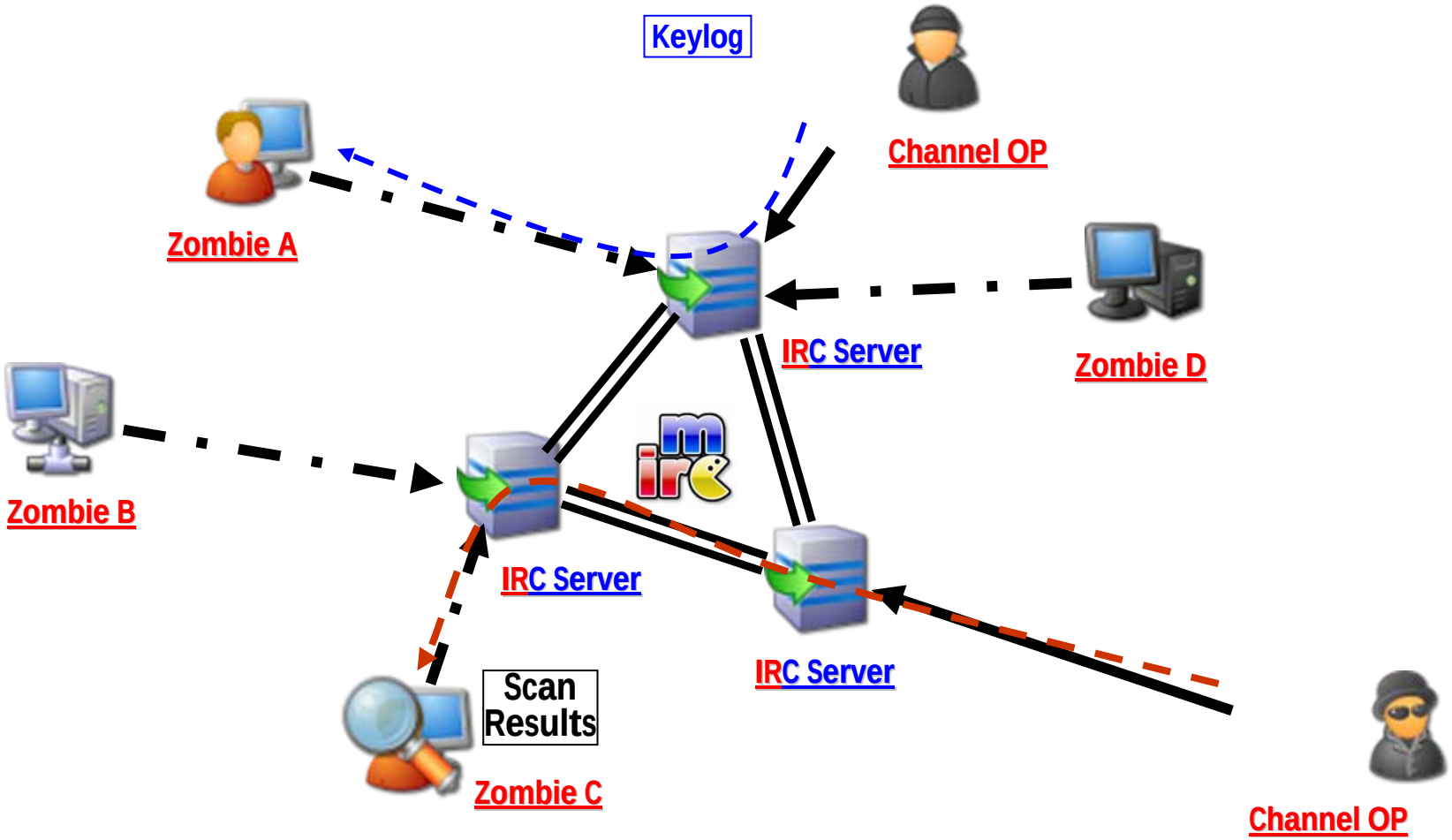
Sniffing, Keylogging & ID Theft

- Bot Channel operations include…



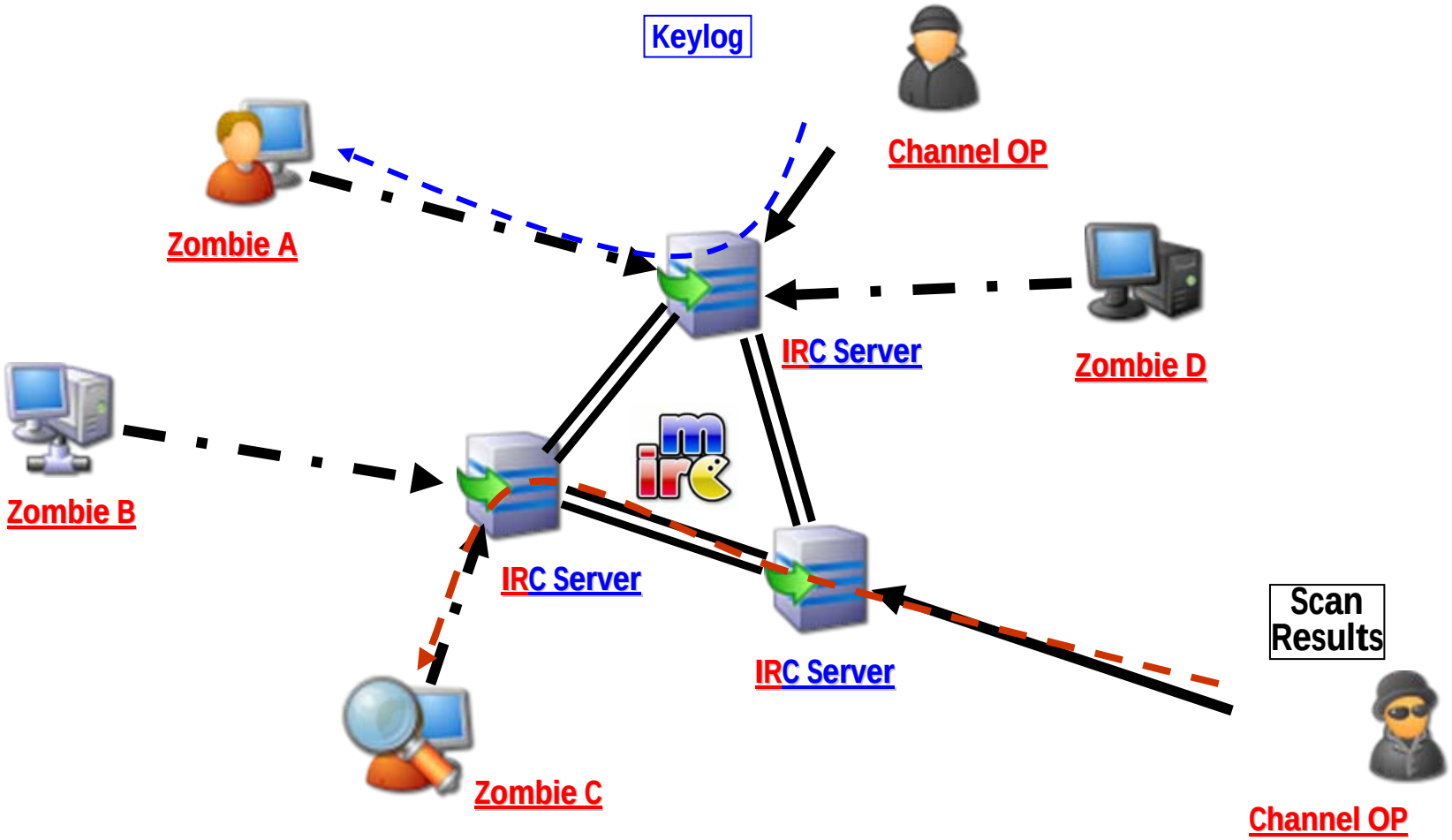
Sniffing, Keylogging & ID Theft

- Bot Channel operations include…



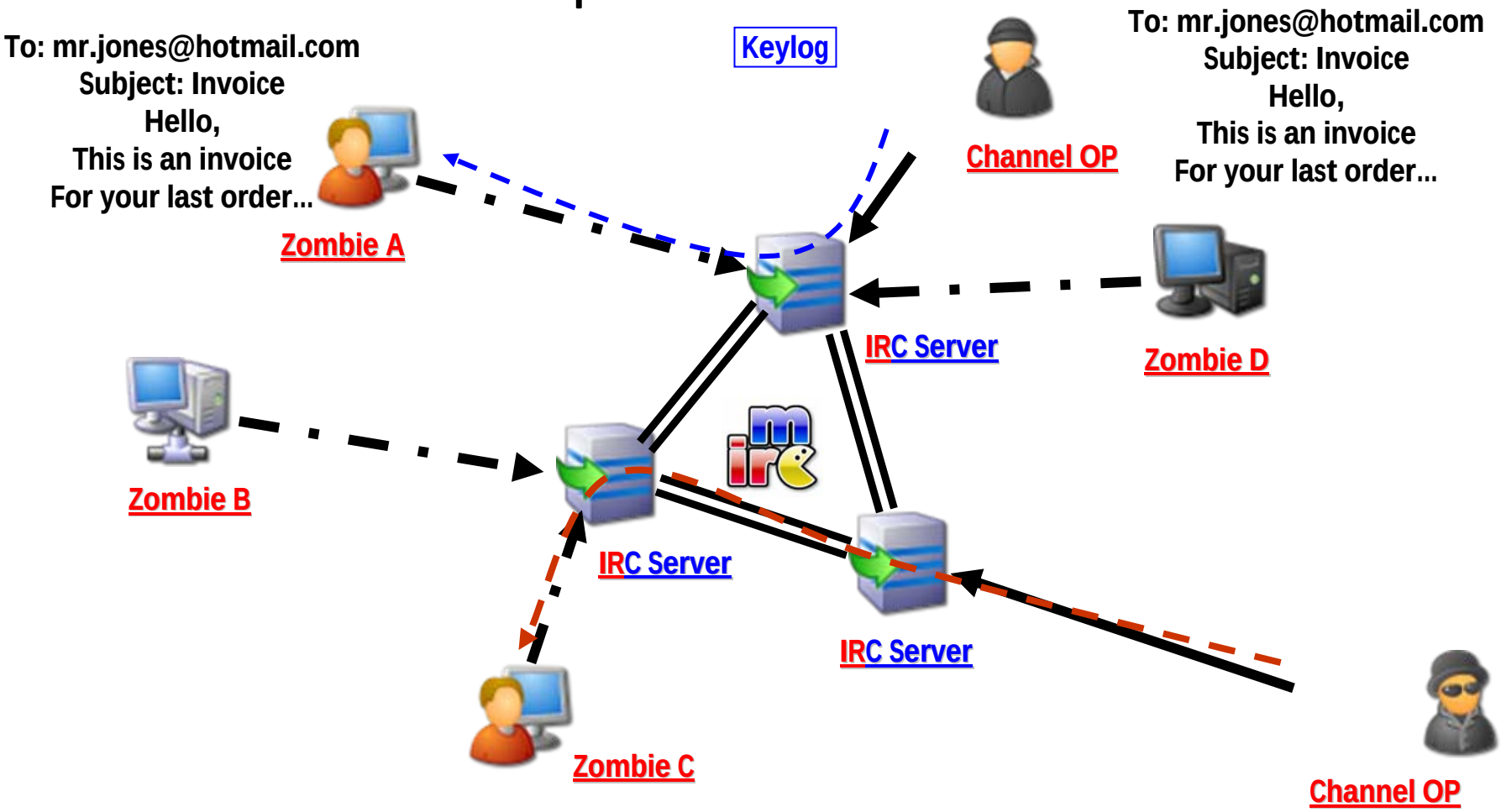
Sniffing, Keylogging & ID Theft

- Bot Channel operations include…



Sniffing, Keylogging & ID Theft

- Bot Channel operations include…



BotNet Architecture

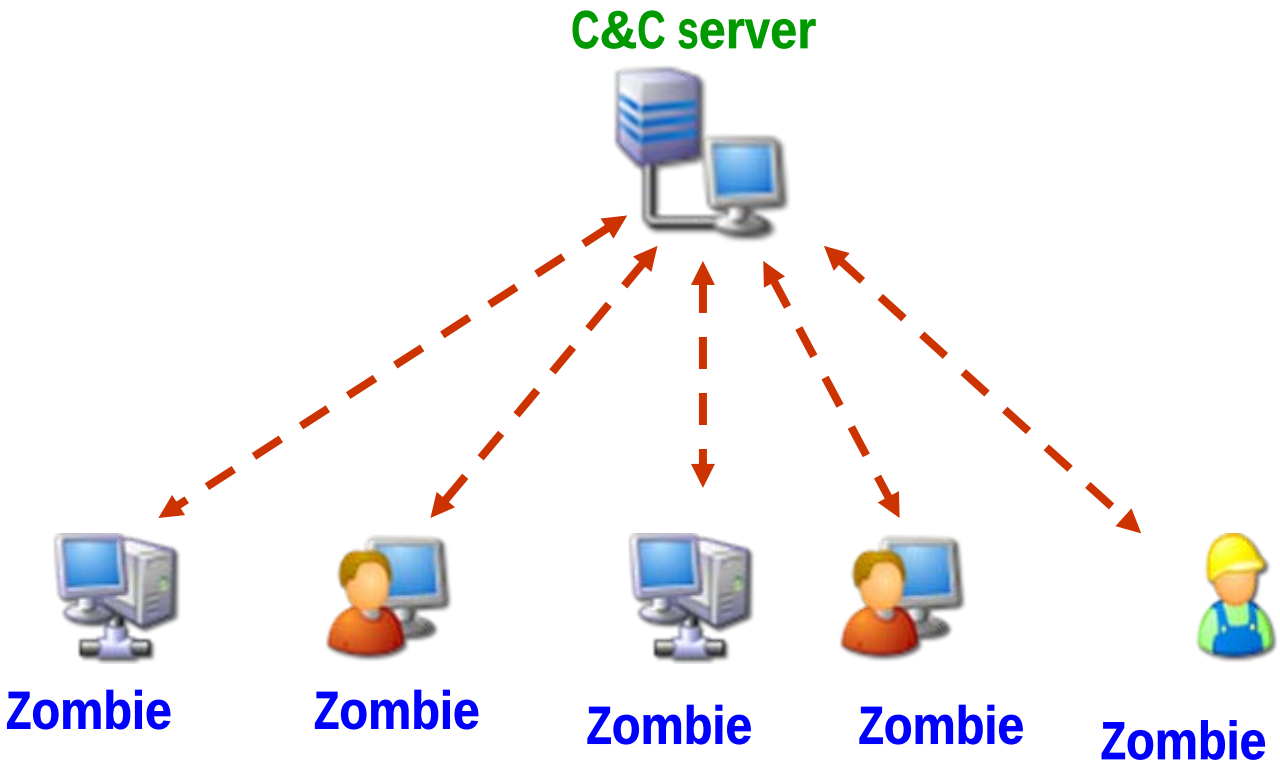
Le comunicazioni in una botnet richiedono tre coponenti:

- un sender,
- un channel,
- un receiver,

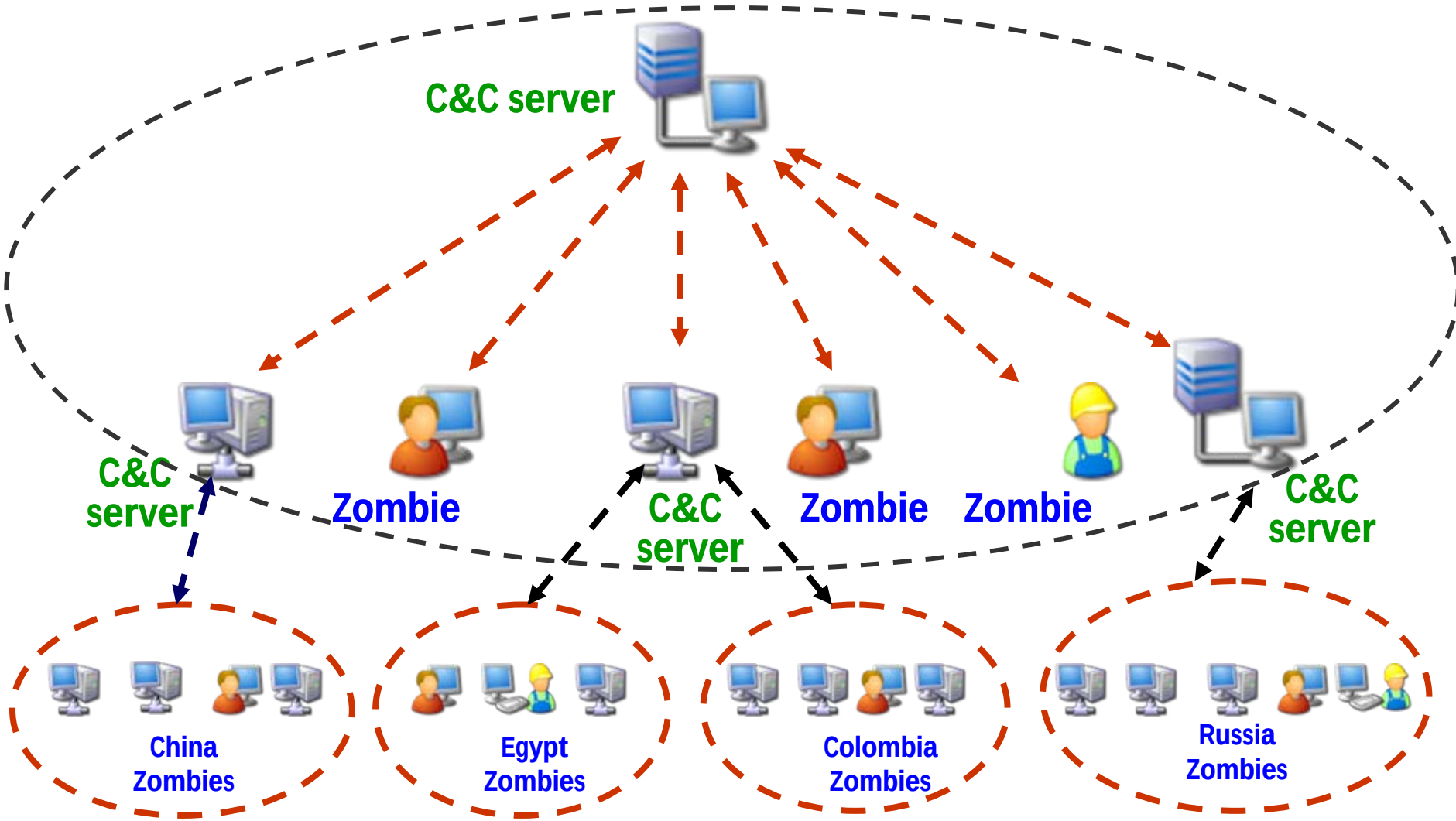
Ci sono inoltre vari modelli di comunicazione e controllo di una Botnet, al solito ognuno ha i suoi vantaggi e i suoi svantaggi.

Mostriamo ora tre di questi modelli.

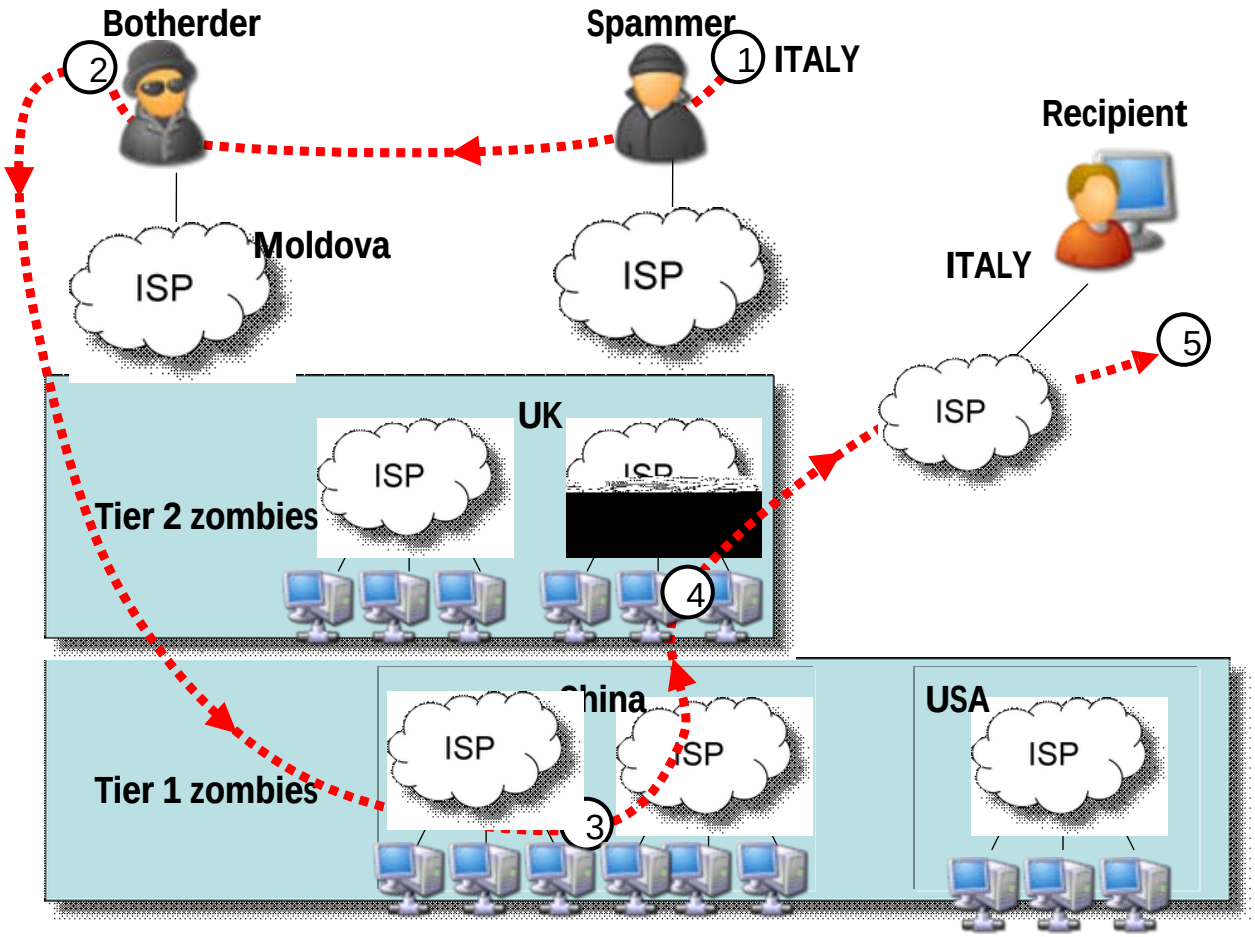
Many-to-one



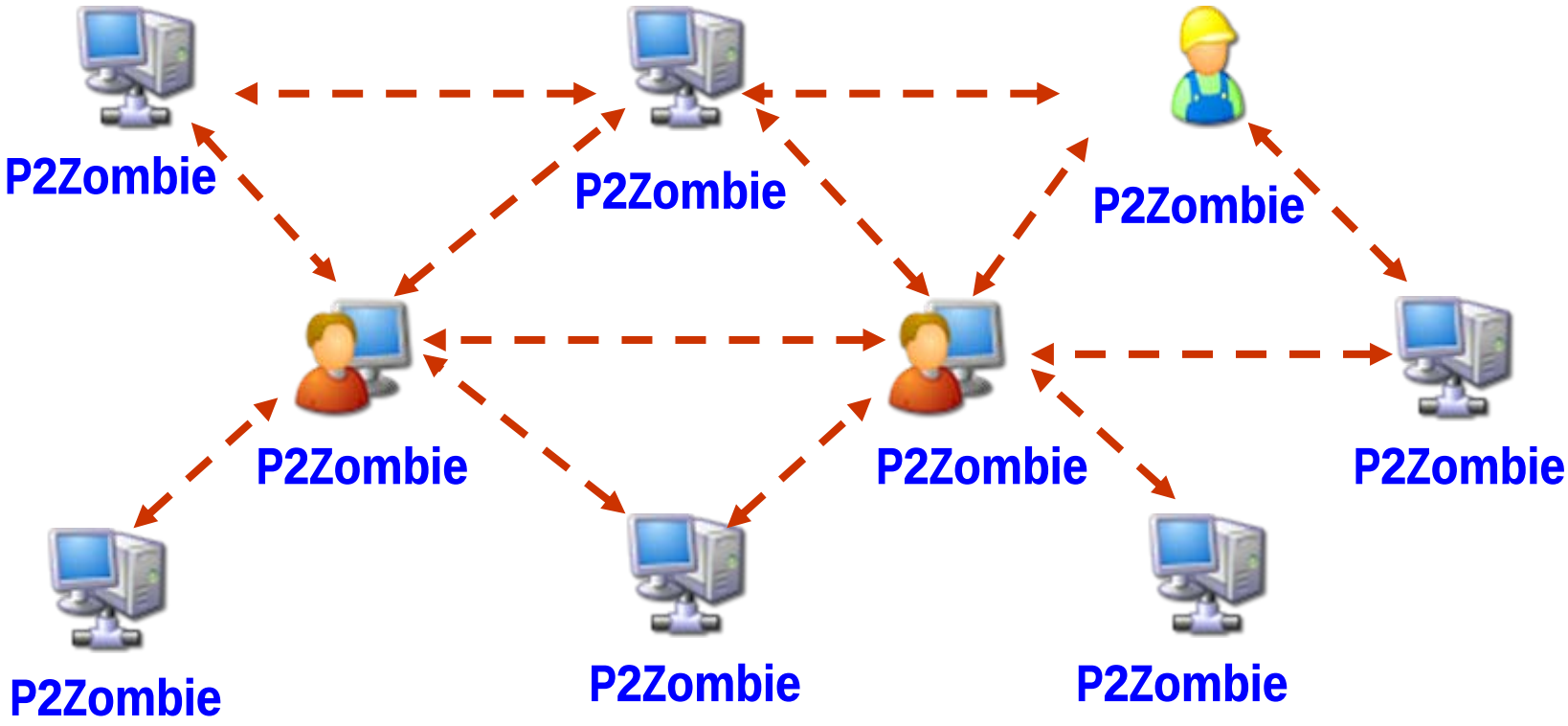
2-Tiers BotNet



Example: 2 Tiers Spam Distribution



Many-to-many


P2Zombie
P2Zombie
P2Zombie
P2Zombie
P2Zombie
P2Zombie
P2Zombie
P2Zombie
P2Zombie

How to create a BotNet?

- Due possono essere i metodi di creazione di una botnet:
  - Standard, script-kiddie way
  - Creative, 31337 way

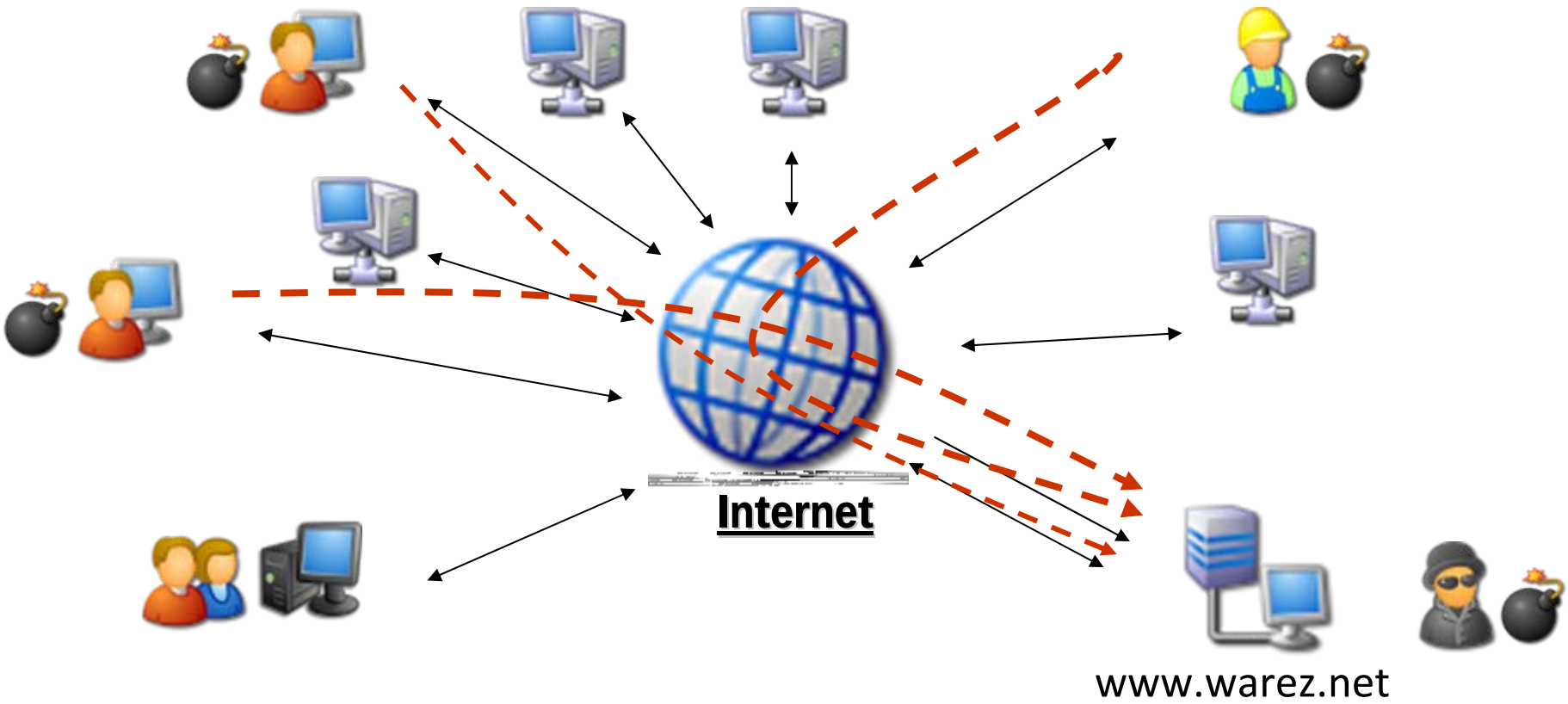
Botnet creation 4 dummies

- **All you need to do is:**
  - Individuare una buona Trojan Console (Agobot, Rbot, ecc…);
  - Definire il comportamento che assumerà il Trojan attraverso le opzioni della Gui;
  - Offusca la signature (automagically);
  - Compila il Trojan (meglio se Multistage)
  - Predisponi un canale su IRC o un Web site per la Bot gathering
  - Diffondi il Trojan attraverso i sistemi P2P o i Siti Warez
  - Enjoy

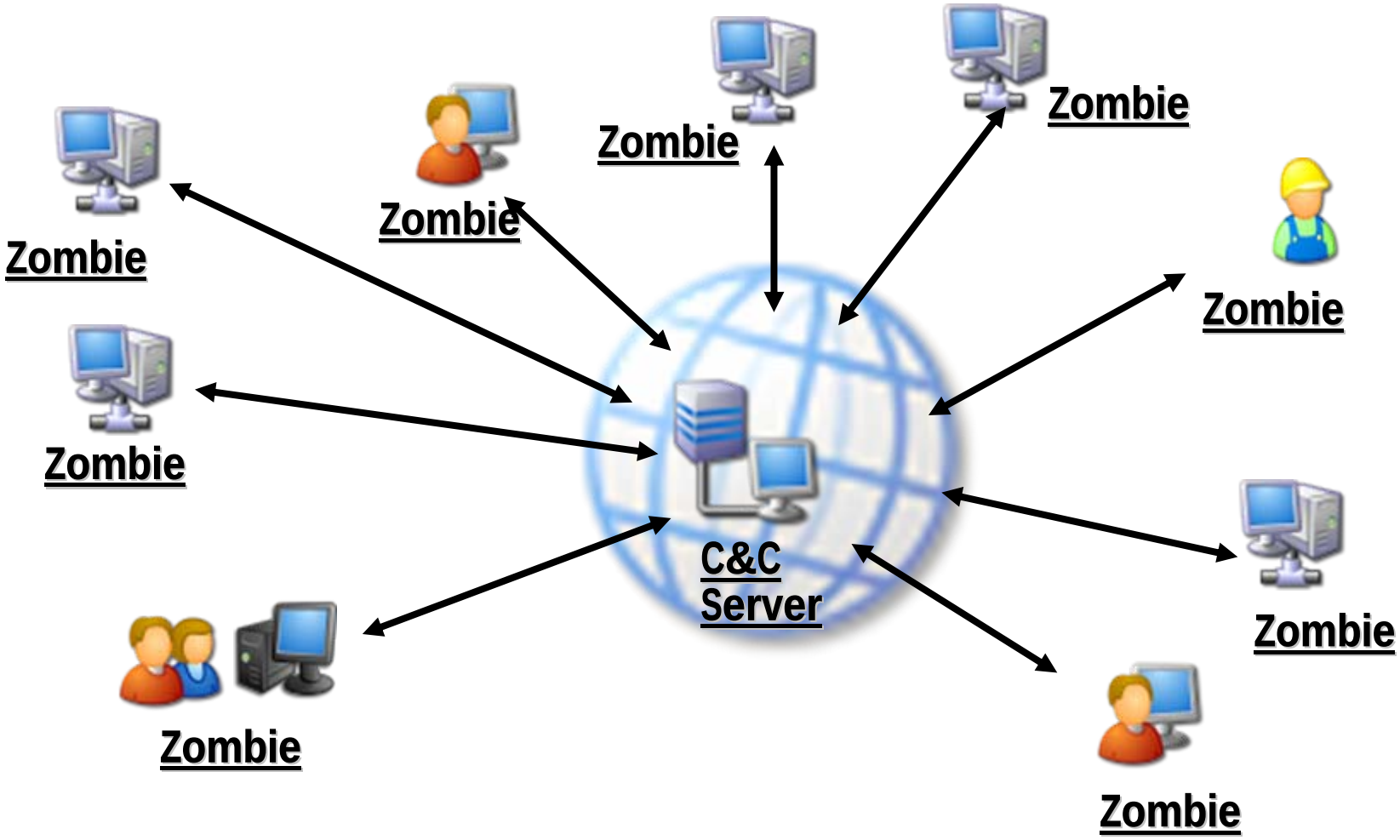
Botnet 31337

- An 31337 cr3w could do worst…
  - Individua o sviluppa un exploit 0-day
  - Integralo in un trojan multistage
  - Compila il tutto e codificalo con Morphine o UPX
  - Diffondilo in ambienti P2P, Warez, Chat, etc…
  - Organizza il Bot-gathering, meglio se multistage
  - Vendi la Botnet o noleggiala
  - Enjoy

Botnet diffusion



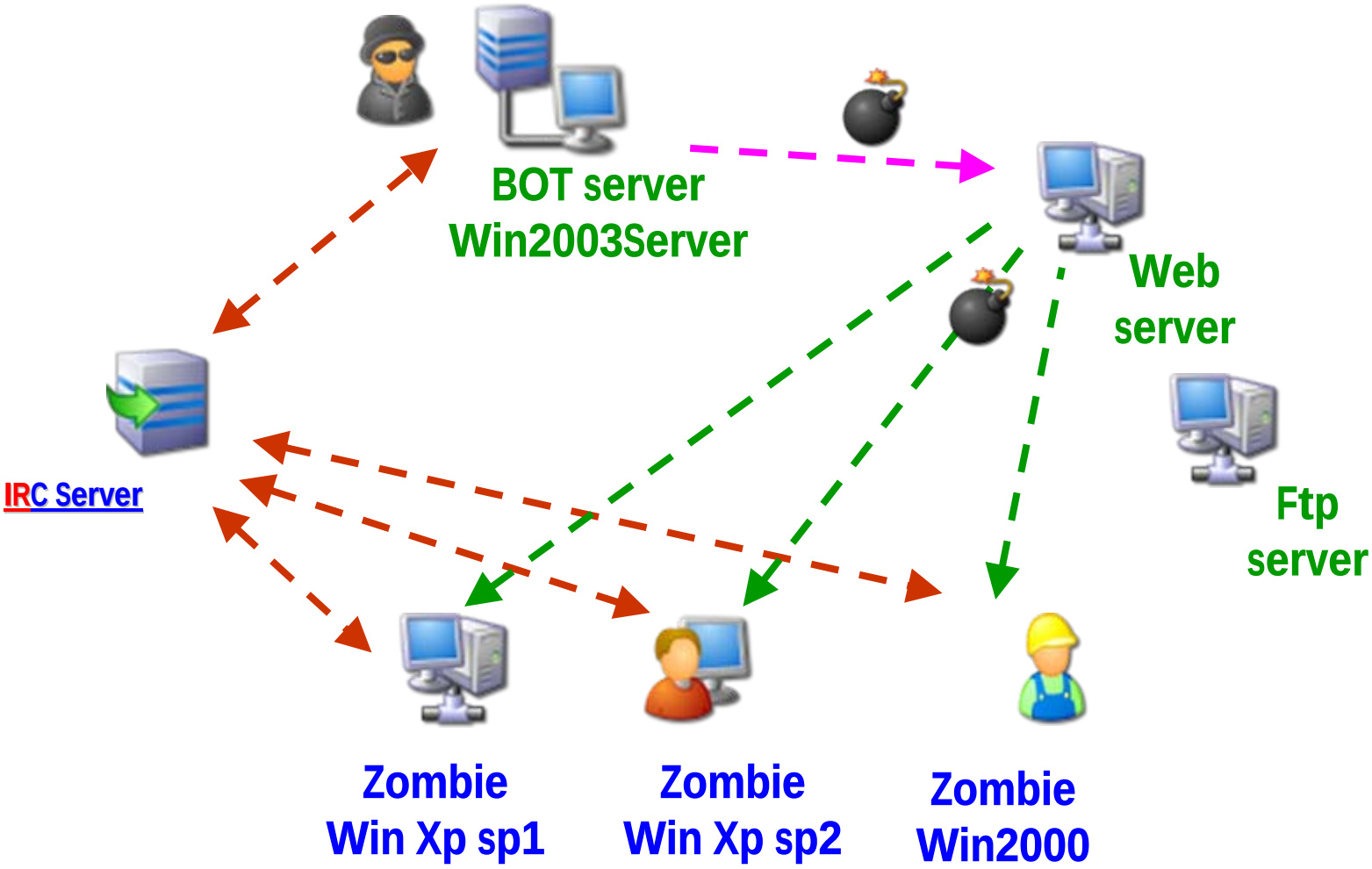
1-tier Botnet structure



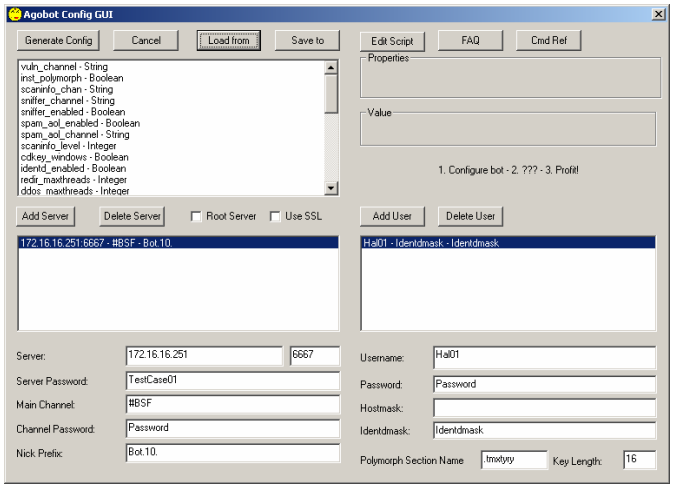
Let's Rock!

- Ora è venuto il momento di vedere qualcosa live…
- Ladies and Gentlemen, we are proud to introduce you: Agobot, the first and probably the most diffused and known Bot-worm…

Il laboratorio



Preparazione del Bot



Config Gui

Visual C++
gcc

Compilazione

BotNet.exe

Comandi 1 (funzionali)

1	commands.list	Lists all available commands
2	cvar.list	prints a list of all cvars
3	cvar.get	gets the content of a cvar
4	cvar.set	sets the content of a cvar
5	cvar.loadconfig	loads config from a file
6	cvar.saveconfig	saves config to a file
7	mac.logout	logs the user out
8	login	logs the user in

Comandi 2 (bot.)

9	bot.about	displays the info the author wants you to see
10	bot.die	terminates the bot
11	bot.dns	resolves ip / hostname by dns
12	**bot.execute**	makes the bot execute a .exe
13	bot.id	displays the id of the current code
14	bot.nick	changes the nickname of the bot
15	bot.open	opens a file (whatever)
16	**bot.remove**	removes the bot
17	bot.removeallbut	removes the bot if id does not match
18	bot.rndnick	makes the bot generate a new random nick
19	bot.status	gives status

Comandi 3 (bot.)

20	**bot.sysinfo**	displays the system info
21	bot.longuptime	If uptime > 7 days then bot will respond
22	bot.highspeed	If speed > 5000 then bot will respond
23	bot.quit	quits the bot
24	bot.flushdns	flushes the bots dns cache
25	bot.secure	delete shares
26	bot.unsecure	enable shares / disable dcom
27	**bot.command**	runs a command with system()

Comandi 4 (irc.)

28	irc.disconnect	disconnects the bot from irc
29	irc.action	lets the bot perform an action
30	irc.dccsend	sends a file over dcc
31	irc.getedu	prints netinfo when the bot is .edu
32	irc.gethost	prints netinfo when host matches
33	irc.join	makes the bot join a channel
34	irc.mode	lets the bot perform a mode change
35	irc.netinfo	prints netinfo
36	irc.part	makes the bot part a channel
37	irc.privmsg	sends a privmsg
38	irc.quit	quits the bot
39	irc.raw	sends a raw message to the irc server
40	irc.reconnect	reconnects to the server
41	irc.server	changes the server the bot connects to

Comandi 5 (http. & ftp.)

42	http.download	downloads a file from http
43	http.execute	updates the bot from a http url
44	http.visit	visits an url with a specified referrer
45	ftp.download	downloads a file from ftp
46	ftp.execute	updates the bot from a ftp url
47	ftp.update	executes a file from a ftp url
48	http.speedtest	Speed Test to see how fast the bot.

Comandi 6 (ddos.)

49	ddos.udpflood	starts a UDP flood
50	ddos.synflood	starts an SYN flood
51	ddos.httpflood	starts a HTTP flood
52	ddos.stop	stops all floods
53	ddos.phatsyn	starts syn flood
54	ddos.phaticmp	starts icmp flood
55	ddos.phatwonk	starts leet flood
56	ddos.targa3	start a targa3 flood

Comandi 7 (redirect.)

57	redirect.tcp	starts a tcp port redirect
58	redirect.gre	starts a gre redirect
59	redirect.http	starts a http proxy
60	redirect.https	starts a https proxy
61	redirect.socks	starts a socks4 proxy
62	redirect.socks5	starts a socks5 proxy
63	redirect.stop	stops all redirects running

Comandi 8 (*gestione processi*)

64	rsl.reboot	reboots the computer
65	rsl.shutdown	shuts the computer down
66	rsl.logoff	logs the user off
67	pctrl.list	lists all processes
68	pctrl.kill	kills a process
69	pctrl.listsvc	lists all services
70	pctrl.killsvc	deletes /stops service
71	pctrl.killpid	kills a pid

Comandi 9 (*gestione processi*)

72	inst.asadd	adds an autostart entry
73	inst.asdel	deletes an autostart entry
74	inst.svcadd	adds a service to scm
75	inst.svcdel	deletes a service from scm
76	harvest.cdkeys	makes the bot get a list of cdkeys
77	logic.ifuptime	exec command if uptime is bigger than specified
78	logic.ifspeed	exec command if speed(via speedtest) is bigger than specified

Comandi 10 (harvest.)

79	harvest.emails	makes the bot get a list of emails
80	harvest.emailshttp	makes the bot get a list of emails via http
81	harvest.aol	makes the bot get aol stuff
82	harvest.registry	makes the bot get registry info from exact registry path
83	harvest.windowskeys	makes the bot get windows registry info

Comandi 11 (shell. & plugin.)

84	plugin.load	loads a plugin
85	plugin.unload	unloads a plugin (not supported yet)
86	shell.handler	FallBack handler for shell
87	shell.enable	Enable shell handler
88	shell.disable	Disable shell handler

Comandi 12 (scan.)

89	scan.addnetrange	adds a netrange to the scanner
90	scan.delnetrange	deletes a netrange from the scanner
91	**scan.listnetranges**	lists all netranges registered with the scanner
92	scan.clearnetranges	clears all netranges registered with the scanner
93	scan.resetnetranges	resets netranges to the localhost
94	**scan.enable**	enables a scanner module
95	**scan.disable**	disables a scanner module
96	scan.startall	enable all Scanners and start scanning
97	scan.stopall	disable all Scanners and stop scanning
98	scan.start	signal start to child threads
99	scan.stop	signal stop to child threads
100	scan.stats	displays stats of the scanner

Grazie dell'attenzione

Black Sun Factory Research Team

Stefano Maccaglia
Raffaele Addesso
Alberto Passavanti

info@bsfactory.net