Cyber Security after Hacking Team

14 ottobre 2015 - MixArt

Giuseppe Augiero

Augiero.it

Sicurezza Informatica

- Cosa intendiamo per sicurezza informatica?

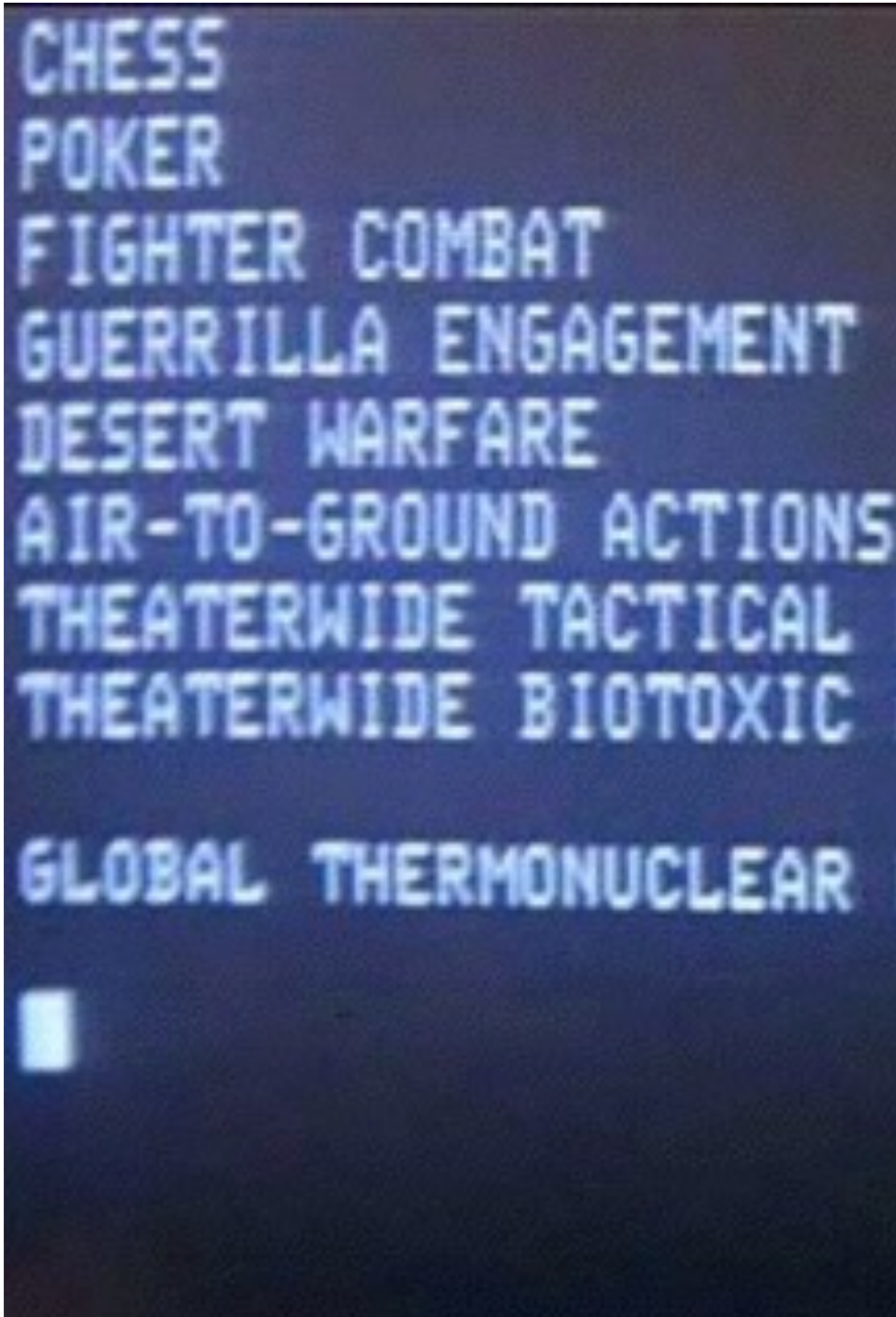
  - Disponibilità.
  - Integrità dell'informazione.
  - Riservatezza.
  - *Autenticità.*
  - *Non ripudio.*

TeleComunicazioni

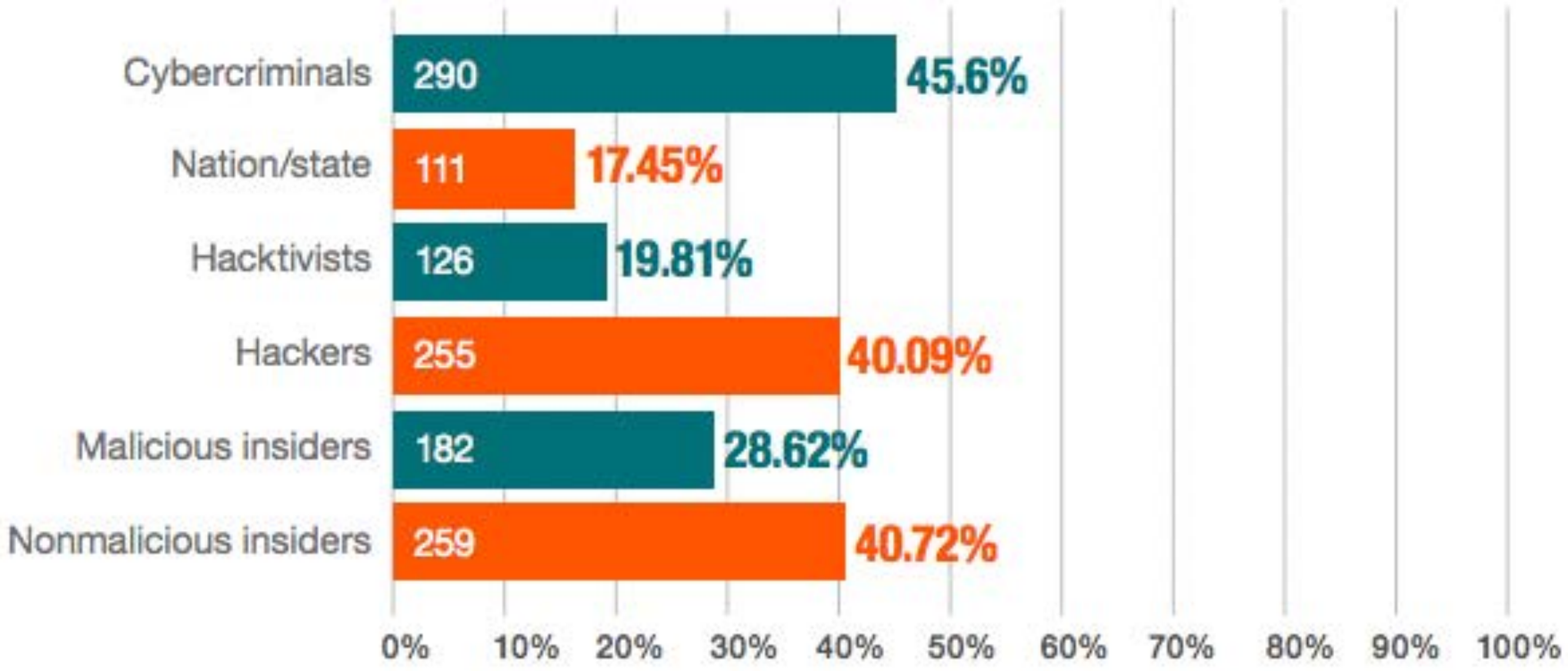
- Buona parte delle comunicazioni sono digitali.
- Attraverso Internet vengono scambiati miliardi di informazioni a diverso titolo.
- Siamo al sicuro?
- I nostri dati sono protetti?
- Di cosa dobbiamo preoccuparci?

La Guerra digitale

- Stiamo combattendo una guerra contro il crimine informatico.
- Quest'ultimo rappresenta una grande piaga.
- E' un problema globale e apparentemente invisibile.
- La terza guerra mondiale sarà "digitale".
- Il costo del cybercrime non è trascurabile.

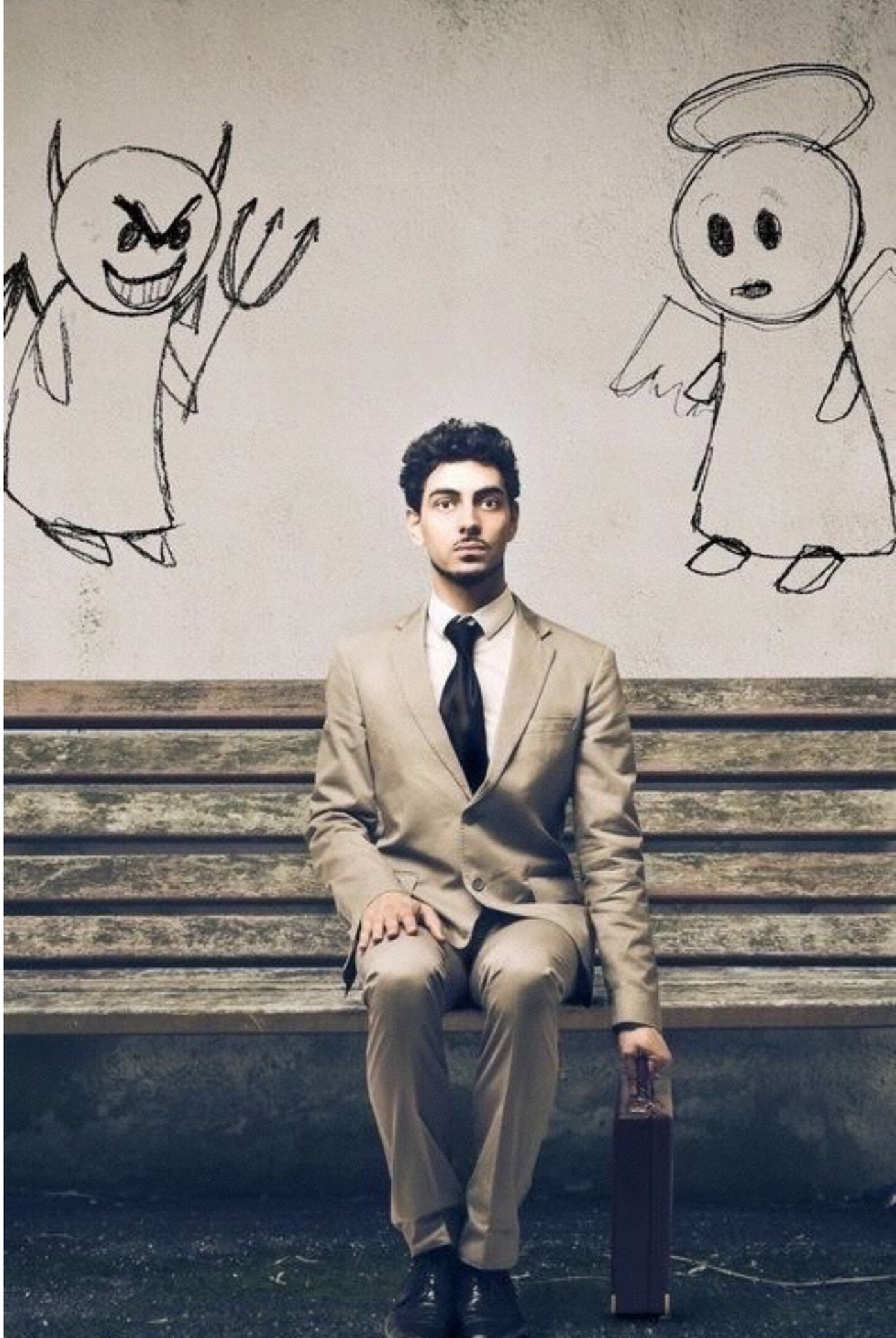


Chi ci attacca?



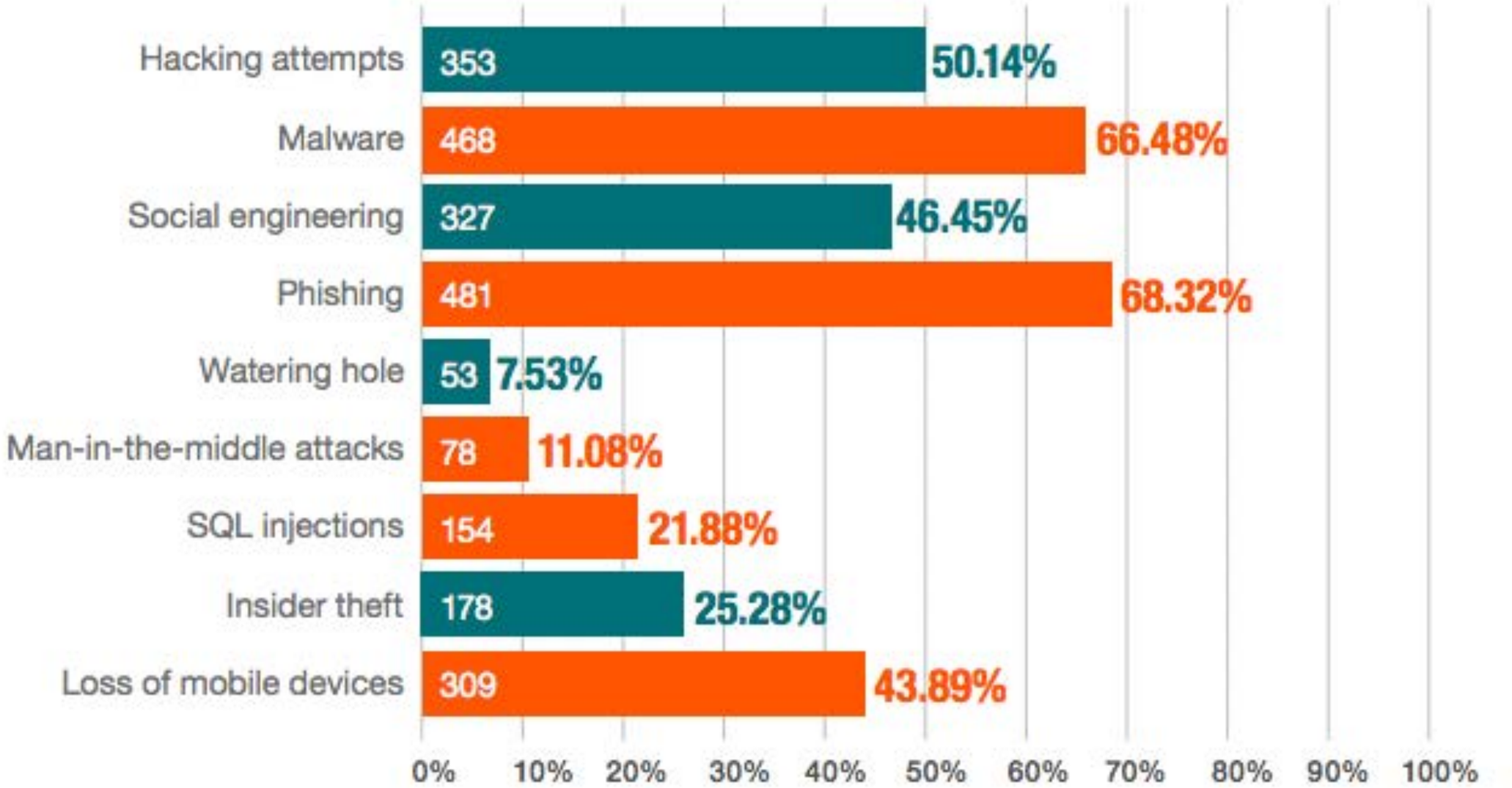
La domanda corretta dovrebbe essere:

Chi sono i buoni e chi i cattivi?



14 ottobre 2015 - Giuseppe Augiero

Tipologia di attacchi



Due situazioni:

- C’è chi è consapevole di essere stato attaccato.
- C’è chi lo ignora.

Resilienza

- Capacità di un sistema di adattarsi alle condizioni d'uso e di resistere all'attacco in modo da garantire la disponibilità dei servizi erogati.

Fattore H

- L’errore umano…

Cyber Defense

- Politiche di sicurezza cibernetica.
- Rilevante al fine di tutelare la difesa e gli interessi di sicurezza nazionale.
- Individuazione, difesa, risposta ed eventuale ripristino.

Strumenti di investigazione

- Le tecniche di investigazione, ovviamente, cambiano…

Intercettazioni

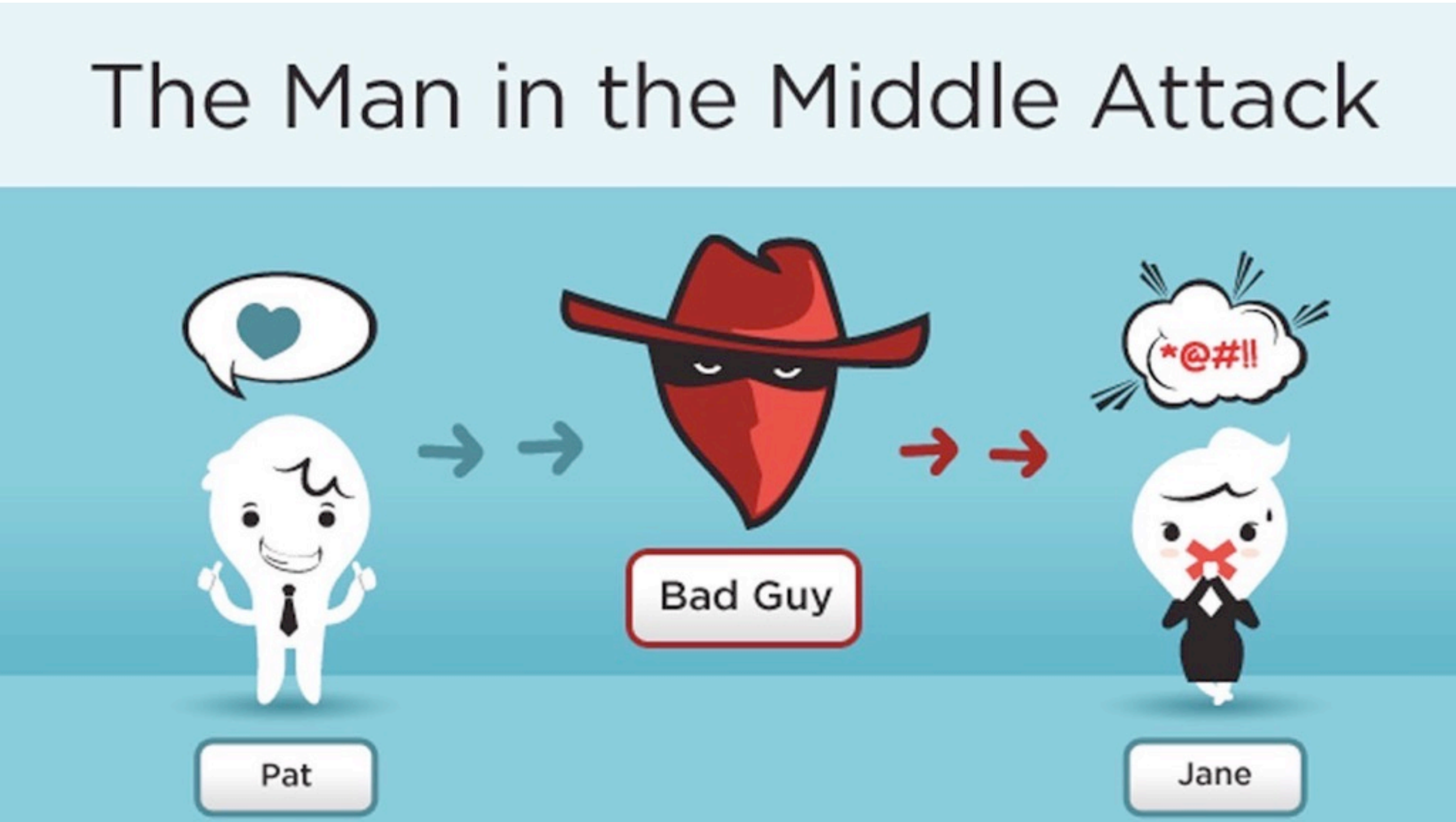
- Soluzioni sempre più sofisticate.

Nasce un problema…

Man in the Middle

- Gli attacchi di tipo Man in the Middle possono non andare a buon fine nel caso di:
  - Crittografia.
  - Uso di chiavi firmate.
  - Interlock.
- Tor (non in tutti i casi).

E se ci spostassimo sugli Endpoint?



Il trojan

- Una possibile soluzione è installare un trojan direttamente sul dispositivo della “vittima”.
- Il trojan permette di aprire una strada per il controllo del dispositivo.
- Permette di effettuare un numero quasi infinito di operazioni sul sistema dove è installato.

Come installarlo?

- Occorre una soluzione che permetta di bypassare eventuali:
  - Antivirus.
  - Firewall.
  - Ids/Ips.
  - Sistemi di deep inspection.

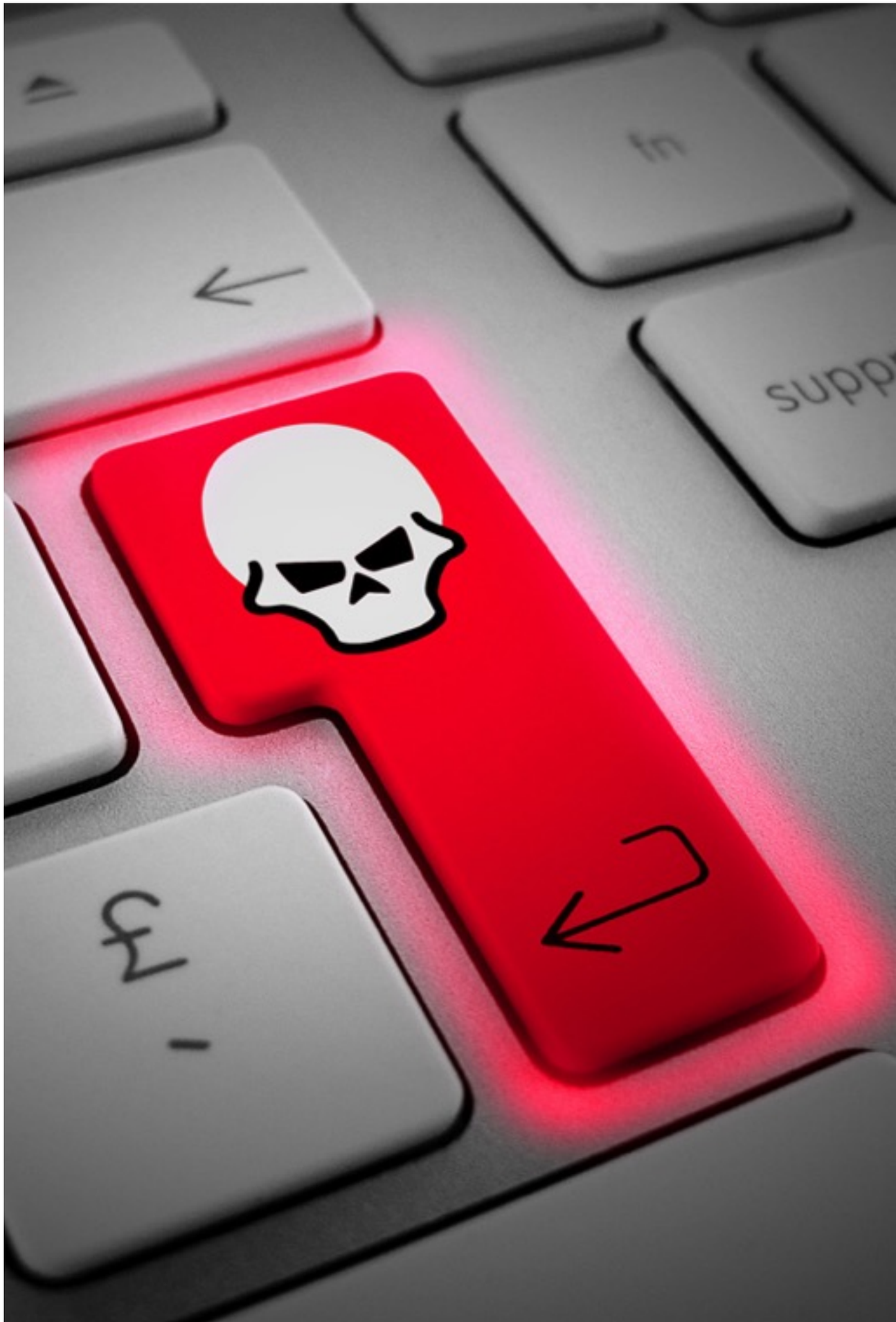
0 day

- Una buona soluzione è rappresentata dall'utilizzo di zero day.

- E' qualsiasi vulnerabilità non nota e indica un tipo di attacco che inizia nel "giorno zero", cioè nel momento in cui viene scoperta una falla di sicurezza in un sistema informatico.

- Questo tipo di attacco può mietere molte vittime proprio perché è lanciato quando ancora non è stata distribuita alcuna patch, e quindi i sistemi non sono ancora protetti.

- Esistono alcune aziende informatiche che vendono zero day.



Chi controlla il controllore?

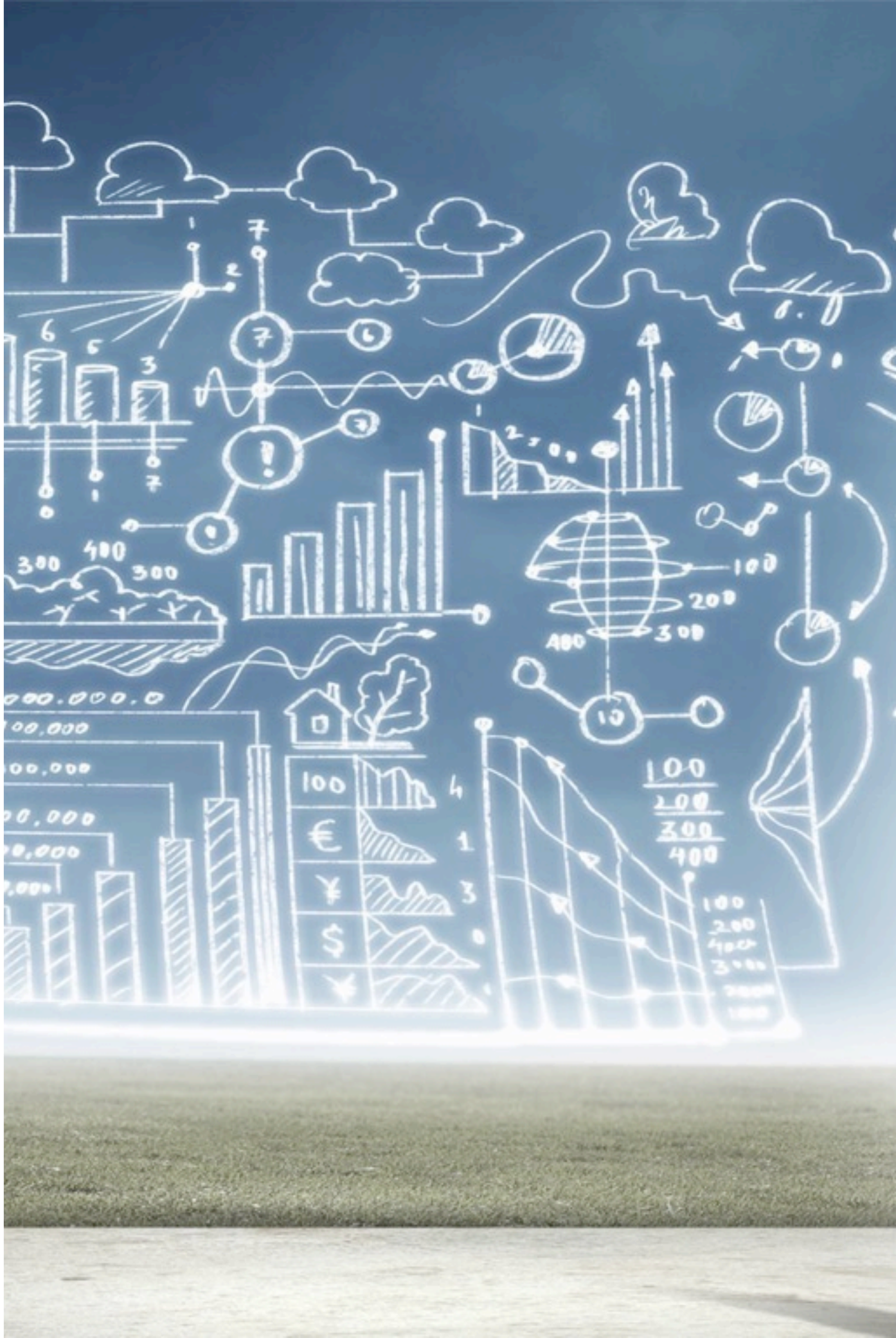
- Chi garantisce che chi controlla il dispositivo sia realmente autorizzato a farlo?

Nuovo problema…

- … le prove.

3 aziende

- Esistono 3 aziende che offrono “trojan per uso investigativo”:
  - Hacking Team (Italia)
  - Gamma Group (Inghilterra)
  - Uso (Israele)



]HackingTeam[

Rely on us.

Rcs Galileo

- Controllo dei target.
- Raccolta di prove in maniera invisibile da pc e smartphone.
- Multipiattaforma.
- Connessioni di controllo cifrate e non “rintracciabili”.

Dark Net

- L’idea era quella di creare una nuova soluzione che permettesse di violare e analizzare il traffico anonimo di tor.

Colpo di scena

- … qualcuno viola la HT e porta via tutto il materiale su cui può mettere le mani.

Chi?

- Chi veniva controllato?
- Chi controllava?

- Chi, dopo questa situazione, può controllare il target?

Versione casalinga

- A questo punto è possibile a tutti utilizzare una soluzione del genere?

- GitHub
- DeepWeb

LA DOMENICA DEL CORRIERE

Supplemento settimanale illustrato del nuovo CORRIERE DELLA SERA - Spedizione in abbonamento postale - Gruppo 2°

Anno 60 — N. 36 — 7 Settembre 1958 — L. 40.—

La donna ideale 1958. A Senigallia (Ancona) ha avuto luogo il 7° Concorso per l'elezione della donna che, per il complesso delle sue qualità, la più importante delle quali non è la bellezza, potesse essere considerata ideale. Ha vinto, e la sua vittoria non è stata facile, la graziosa maestrina del "Musichiere", Laura Lardori, nata a Sangemini (Terni) 22 anni fa. È una ragazza semplice, che ha il gusto della casa e ama i fornelli, che ha una buona cultura e pratica discretamente qualche sport. Il pittore Walter Molino raffigura la vincitrice mentre è in cucina per la prova più difficile.

Esiste qualcosa di più pericoloso?

- Certamente!!!
- Parliamo di alcuni RootKit e Rat che in questo periodo girano per la rete.

Open Source

- … non basta.

Identità

14 ottobre 2015 - Giuseppe Augiero

Dati distribuiti

- Dove sono i nostri dati?

Futuro

- … è nero .
- … e c’è grande crisi.

- Abusi.
- Mercato delle contromisure.

Cosa fare?

- Occorre necessariamente avere senso critico.
- Dobbiamo essere consapevoli di quello che facciamo.
- La paranoia non è una buona soluzione.

Consapevolezza

Cyber Security after Hacking Team

14 ottobre 2015 - MixArt

Giuseppe Augiero

Augiero.it