# Cyber Security

Andrea Fumagalli
29 Gennaio 2024

SICUREZZA INFORMATICA Scuola "A. Limonta"

# Agenda

- Obiettivi di questo laboratorio
- Come difendersi
- I Pericoli del web
- Malware
- Attacchi informatici
- Tipologia di attacchi
- Attacchi famosi

# Obiettivi

# Mantra


Cyber Security
is everyone's
responsibility...
Protect your information
at home and at work!

# Perché questo laboratorio?

Tre semplici domande:

Che rischi corro su Internet?

Come faccio a difendermi da alcune minacce di Internet se non le conosco nemmeno?

Chi sono i cattivi con cui ho a che fare?

**Se avete le risposte potete andare a casa**

**altrimenti…….vi suggerisco di restare**

# Termini Tecnici (Glossario)

## INFORMATICA

**PC =** Personal Computer
**Hardware (HW) =** circuiti elettronici (il PC)
**Macchina =** computer = pc
**Software (SW) =** programma
**Programma =** insieme di istruzioni che esegue un particolare compito
**Byte =** elemento base trattato dal computer (lettera, numero, pixel di una foto, …)
**File =** insieme di dati (byte) salvati sul disco
**Attachment =** allegato
**Web =** Internet = "La Rete"
**URL =** Indirizzo di un sito
**Credenziali =** coppia utente/password
**Crash =** rottura di un programma
**Login =** collegamento iniziale verso un servizio/sistema
**Server =** fornitore di un servizio
**Client =** utilizzatore di un servizio

## SICUREZZA INFORMATICA

**Cyber Security =** Sicurezza Informatica
**Attacco =** avere accesso ad un sistema o dati in maniera illegale
**Attaccante =** colui che esegue un attacco
**Vittima =** colui che subisce un attacco
**Cyber Threats =** minacce informatiche
**Cyber Attacks =** attacchi informatici
**Hacker =** pirata informatico
**Disservizio =** disturbo/fermo di un servizio
**Cyber Warfare =** guerra cibernetica, preparazione e conduzione delle operazioni militari sulla base delle informazioni disponibili, oggi trattate tramite computer

**Cifrare =** nascondere il contenuto di un file usando un'opportuna regola
**Decifrare =** scoprire il contenuto di un file cifrato usando un'opportuna regola opposta a quella usata per cifrarlo



# Come difendersi

(…iniziamo dalla fine ☺ )

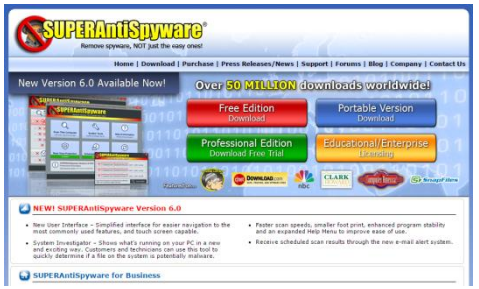
# L'AntiVirus

- Adottare un **ANTI-VIRUS** e tenerlo **AGGIORNATO (FONDAMENTALE!)**

✓ Intercetta tipicamente Virus, Trojan e Worm ma non altri malwa

✓Tanti sono gratis (AVG, Bitdefender, Avira,…)

- Adottare anche un **ANTI-SPYWARE e tenerlo AGGIORNATO**
- SuperAntiSpyWare - http://www.superantispyware.com/



# Password

Non usare la stessa password su più siti

- ✓ Non usare il vostro nome o cognome o data di nascita
- ✓ Inserite qualche numero o carattere speciale ($, %, ?, -, …)
- ✓ Usate almeno 8 caratteri, con varie Maiuscole

**Non scrivete la password sui foglietti !!!**

Programmi specifici per salvare le password

- ✓ KeePass - http://keepass.info
- ✓ Password Safe - https://www.pwsafe.net



# Incredibile…

# Social Media

Esempio: Facebook, Instagram e You Tube

Difendete sempre la vostra identità online.

Proteggete i vostri dati personali (nome, indirizzo, numero di telefono, …)

Diffidate di chi vi contatta o chiede informazioni troppo personali

*Siate sospettosi e guardinghi. Se rilevate qualcosa di strano avvisate subito i vostri Genitori che sapranno sempre come aiutarvi*


I pericoli del Web

# Il contesto

Internet: rete di tanti computer, tutti collegati fra loro

Popolo del web:

- ✓ Persone per bene
- ✓ Malintenzionati, farabutti ed adescatori
- ✓ Cyberterroristi
- ✓ Cyber Warfare (Guerre e Spionaggio)
- ✓ Governi (Nazioni) -> Lotte di potere

Persone brave…ma anche…persone cattive



# Perché gli attacchi informatici

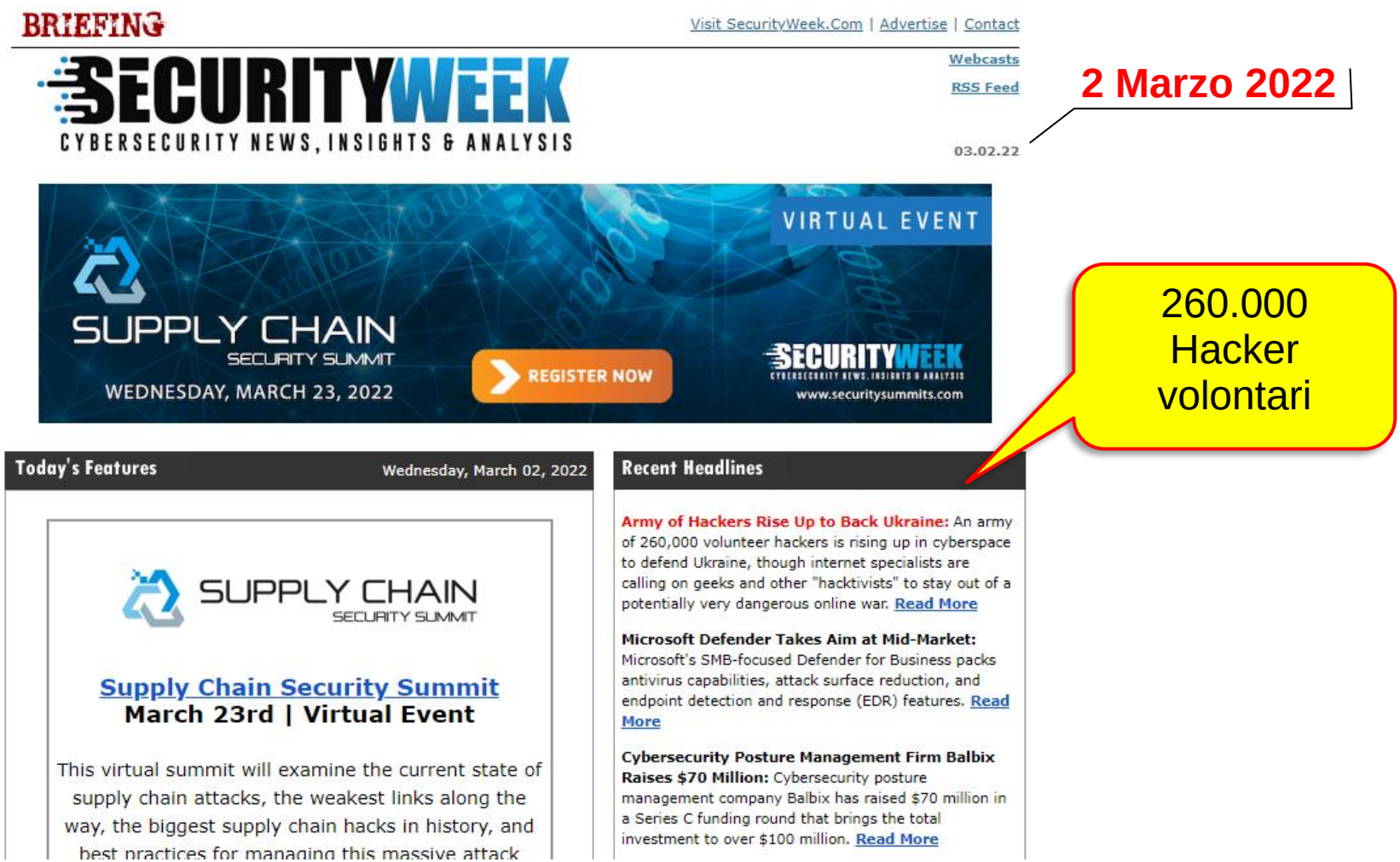
- ✓ Interessi economici e politici
  - Ricchezza, Potere, Territori, Predominio, …
- ✓ Guerre
- ✓ Lotte Idealiste e Attivismo
  - Hackers: il gruppo “Anonymous”


singoli utenti o intere comunità online che agiscono anonimamente – insieme o individualmente – per perseguire un obiettivo concordato, anche approssimativamente.

- ✓ Criminali
  - Interessi personali, su commissione



# CyberWar



BRIEFING

Visit SecurityWeek.Com | Advertise | Contact

SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

Webcasts
RSS Feed

03.02.22

2 Marzo 2022

VIRTUAL EVENT
SUPPLY CHAIN SECURITY SUMMIT
WEDNESDAY, MARCH 23, 2022
REGISTER NOW
SECURITYWEEK
www.securitysummits.com

260.000 Hacker volontari

Today's Features — Wednesday, March 02, 2022

SUPPLY CHAIN SECURITY SUMMIT

Supply Chain Security Summit
March 23rd | Virtual Event

This virtual summit will examine the current state of supply chain attacks, the weakest links along the way, the biggest supply chain hacks in history, and best practices for managing this massive attack

Recent Headlines

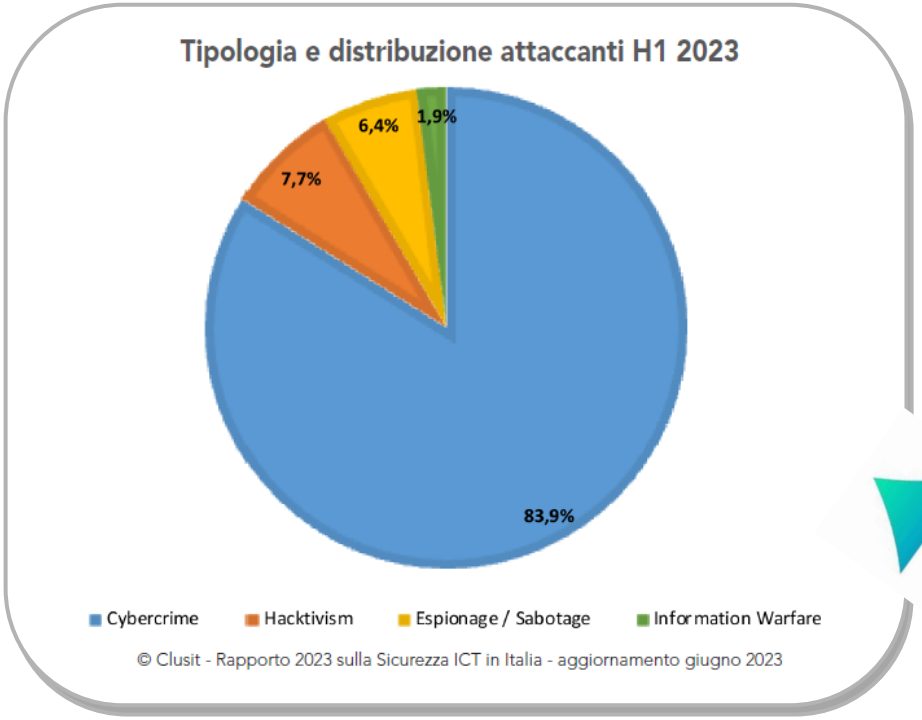
**Army of Hackers Rise Up to Back Ukraine:** An army of 260,000 volunteer hackers is rising up in cyberspace to defend Ukraine, though internet specialists are calling on geeks and other "hacktivists" to stay out of a potentially very dangerous online war. Read More

**Microsoft Defender Takes Aim at Mid-Market:** Microsoft's SMB-focused Defender for Business packs antivirus capabilities, attack surface reduction, and endpoint detection and response (EDR) features. Read More

**Cybersecurity Posture Management Firm Balbix Raises $70 Million:** Cybersecurity posture management company Balbix has raised $70 million in a Series C funding round that brings the total investment to over $100 million. Read More

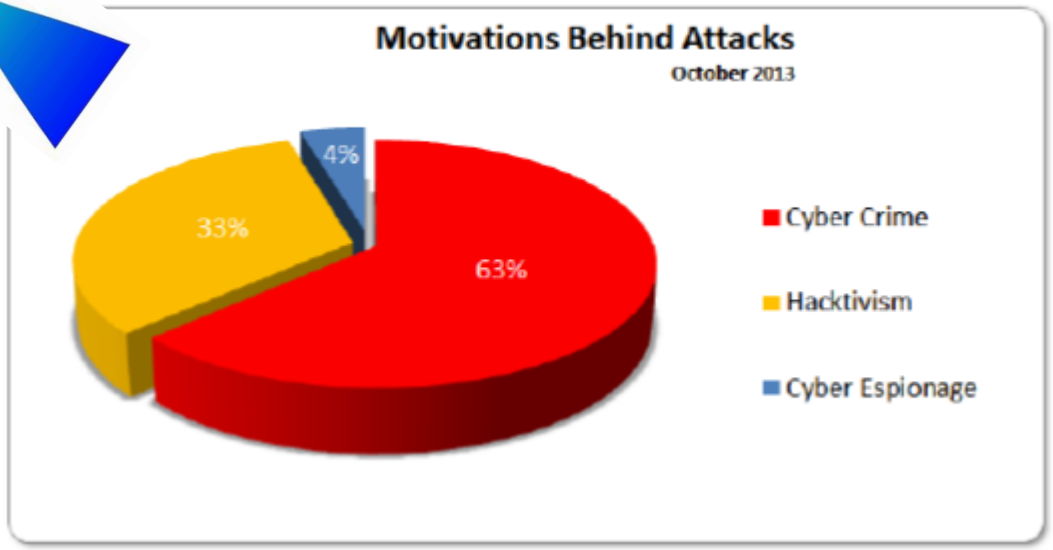
Fonte: https://www.securityweek.com/army-cyber-hackers-rise-back-ukraine

# Evoluzione attacchi 2013-23



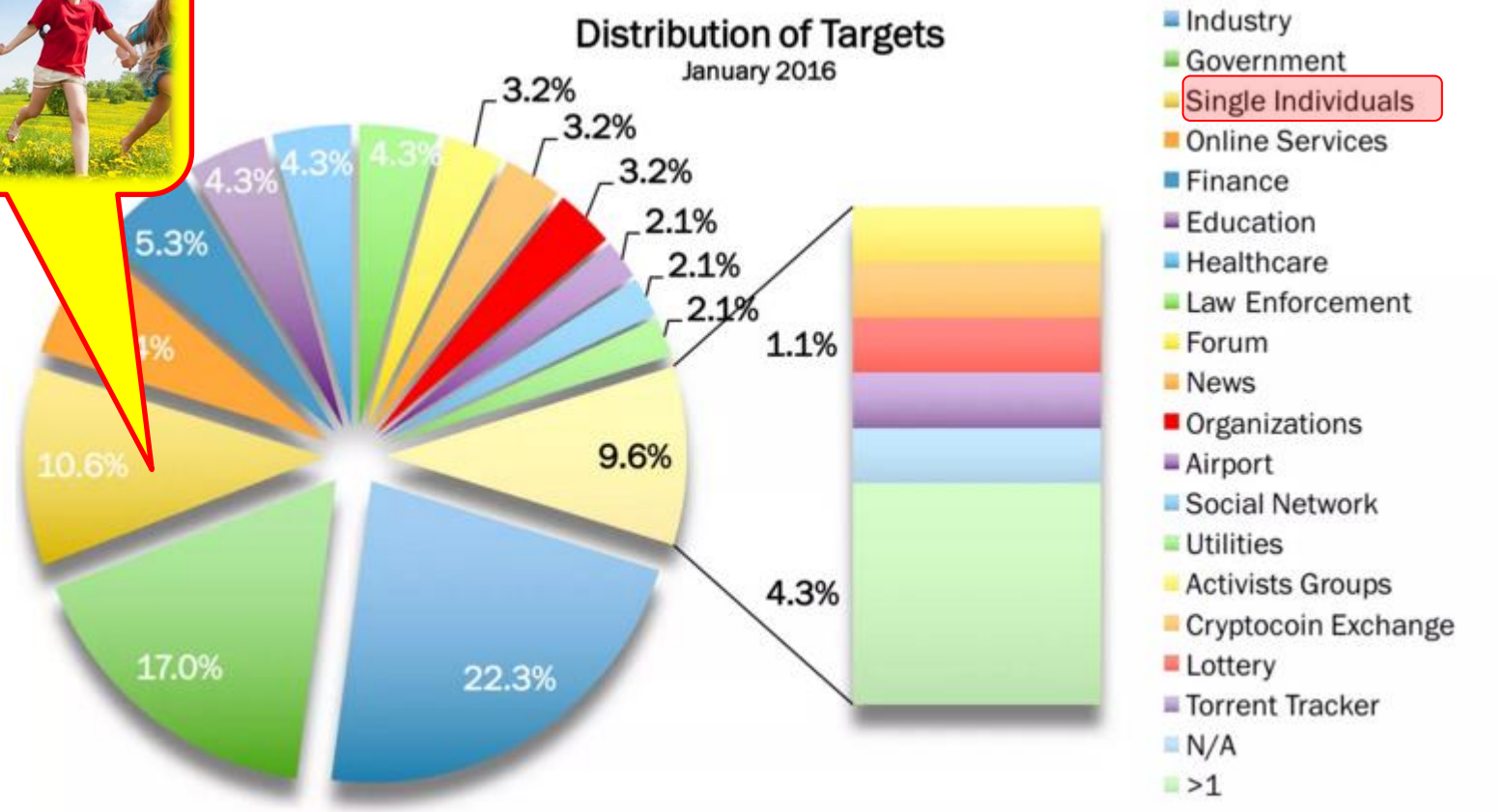

**Fonte:**
https://clusit.it/rapporto-clusit/

Cybercrime: guerra cybernetica (Governi)



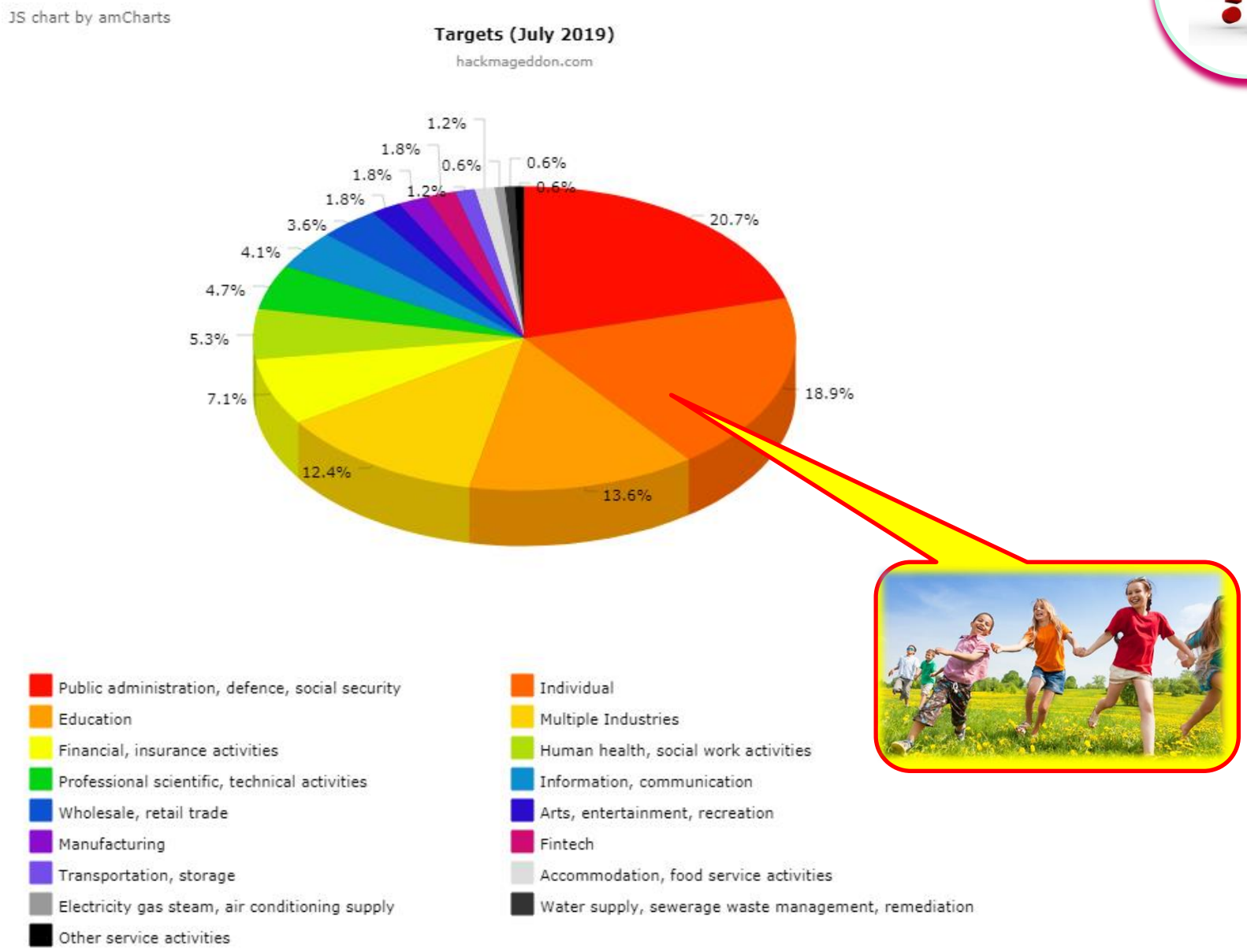

**Fonte:**
http://www.hackmageddon.com/

# Vittime degli attacchi 2016




**Fonte:** http://www.hackmageddon.com/

# Vittime degli attacchi 2019



# Chi siamo in Rete?

**Noi siamo…**

**DATI**

1.86 metri
85 Kg
Scarpa: 45
Tel 347.8044555
Carta credito: 3752…876
Indirizzo: Via ….
Targa auto: EP 753 XH

1.52 metri
44 Kg
Scarpa: 39
Anni: 10





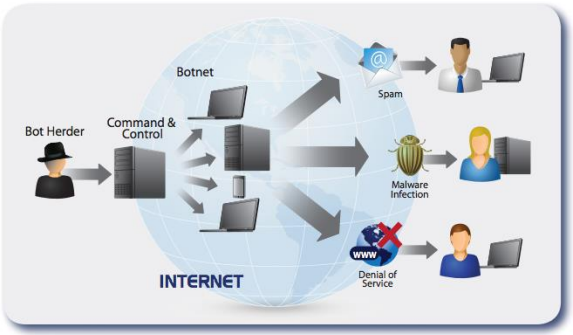
# Scopo Sicurezza Informatica

## Difendersi da Malware

- ricatto e reputazione
- furto di informazioni/dati
- danneggiamento dei dati

## Difendersi da Attacchi Informatici

- attività contro la legge
- pericolo e crimine
- reputazione





Malware

# Malware

**Software (programma) creato con lo scopo di danneggiare un computer, una rete o un sistema informatico.**

Malware = **Mal**icious soft**ware** (programma maligno)

Solitamente:

- si installano in maniera “silenziosa”
- fanno attività non voluta dall’utente, talvolta sottraendo informazioni riservate (dati)
- possono permettere di prendere il controllo da remoto

Per eseguire **Attacchi Informatici**



# Dove si nascondono i malware?

# Cosa fanno

Non danneggiano il computer (hardware) o la rete o le stampanti

Producono comportamenti fastidiosi (pubblicità, sondaggi, etc)

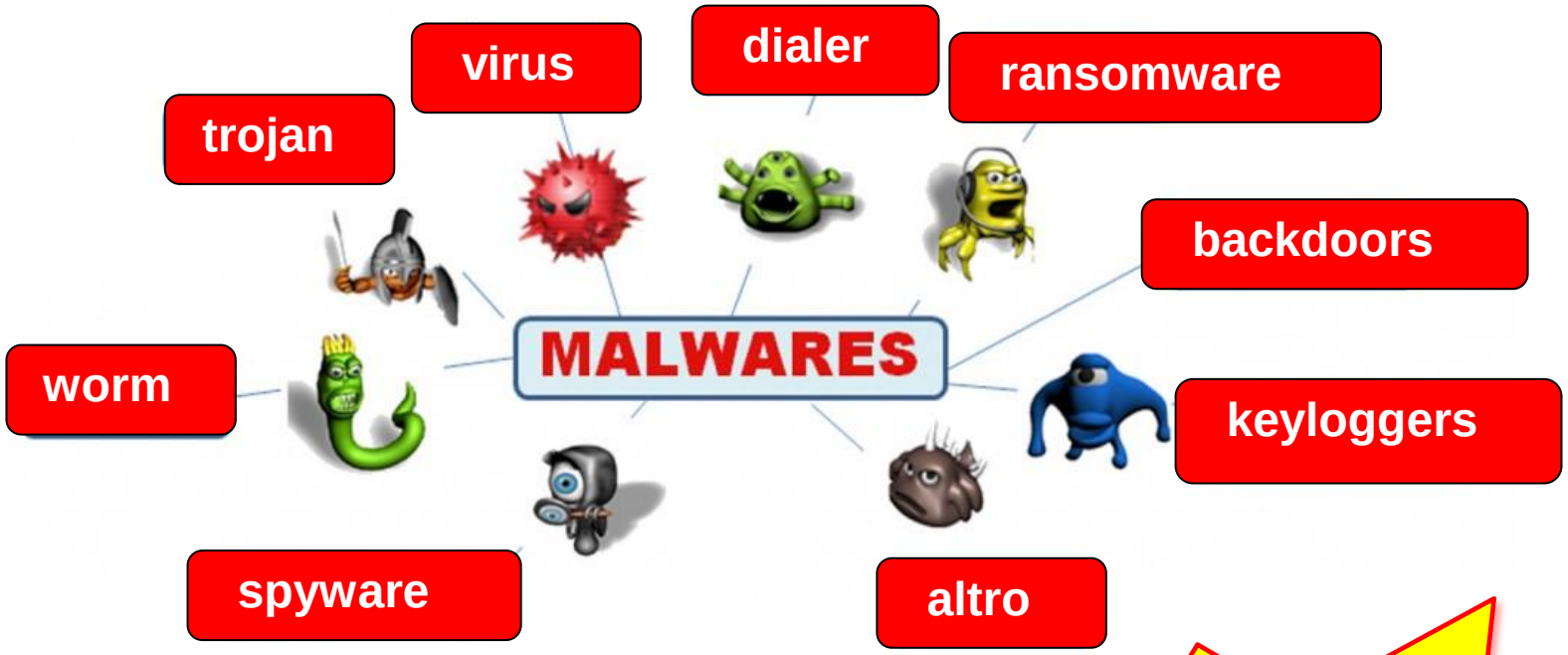
**Danneggiano o cancellano** dati

**Rubano** dati: password, numeri di telefono, foto, etc

Si contraggono in vari modi in base al tipo di malware



# Tipi di Malware




Si differenziano per quel che fanno e come si propagano

# Virus

Si “attaccano ad altri programmi”

Non si propagano da soli, ma solo insieme al programma a cui sono attaccati, quando questo viene trasferito tramite chiavette USB, email, DVD, etc

*Ogni volta che si riceve un programma da qualcuno, **scansionarlo** con l’antivirus…se risulta **INFETTO** non aprirlo !*



# Worm

Malware che si replica da solo: non necessita di legarsi ad altri programmi per propagarsi.

Modifica il computer che infetta, in modo essere attivo ogni volta che si accende il pc.

Per replicarsi, tipicamente sfruttano il collegamento ad internet e l'email



# Worm

Sul vostro pc ricercano indirizzi email dei vostri amici e scrivono loro delle false email a nome vostro o con un mittente falso (inventato) con agganciato sè stesso (il worm) camuffato per un programma lecito.

Molto spesso sfruttano il **social engineering**

I Worm vengono intercettati dagli antivirus

***Non dare*** *le proprie informazioni personali a sconosciuti.*
***Non fidarsi*** *delle mail "strane" che arrivano, verificarle!*
***Non cliccare*** *su link sconosciuti.*
*Prima di aprire un file ricevuto,* ***scansionarlo*** *con l'Antivirus*

# Worm

Foto compleanno

nestore.peppozzi

Foto compleanno

*Ciao Nestore,*

*ti allego alcune tue foto di quando sei venuto alla mia festa di compleanno qualche anno fa.*

*Dimmi se ti piacciono*

*Ciao*

http://www.spaccotutto.it/foto/compleanno_marietto

foto_compleanno.zip (1K)

Sans Serif

Send

Saved



# Spyware

Malware che ispeziona ed invia all'esterno l'attività in rete dell'utente: acquisti fatti, siti visitati, prodotti di interesse,…

Si installano tramite un'azione dell'utente (click)

Vengono sfruttati per attacchi di spamming o phishing o per inviare pubblicità mirata

***Non visitare*** *siti sospetti.* ***Diffidare*** *dalle vincite milionarie.* ***Non installare*** *programmi "strani o regalati".* ***Utilizzare un anti-spyware*** *tenendolo aggiornato.*



# Trojan horse

Programma maligno che ha funzionalità nascoste all'interno di un programma apparentemente utile.

L'utente stesso quindi installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice *Trojan* nascosto.

Dal 2001 i Trojan sono usati 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.



# Come si diffondono i Trojan

E’ la vittima che spesso non prestando attenzione ai siti che visita, scarica e installa il Trojan inavvertitamente: tipicamente vengono nascosti in programmi molto richiesti, es videogame o film piratati.

I Trojan vengono intercettati dagli antivirus



# Trojan RAT

Una categoria speciale di Trojan sono i RAT (Remote Administration Tool), composti da 2 parti:

- Modulo server, installato sulla macchina vittima
- Modulo client, installato sulla macchina dell'attaccante (a casa sua) usato dall'attaccante per inviare istruzioni che il server esegue

Il modulo server si comporta come una backdoor, fornendo un accesso illecito alla macchina della vittima

***Aggiornare*** *costantemente l'antivirus e farlo* ***girare*** *regolarmente !*
***Scansionare*** *qualsiasi programma scaricato da web o ricevuto (email USB, etc)*



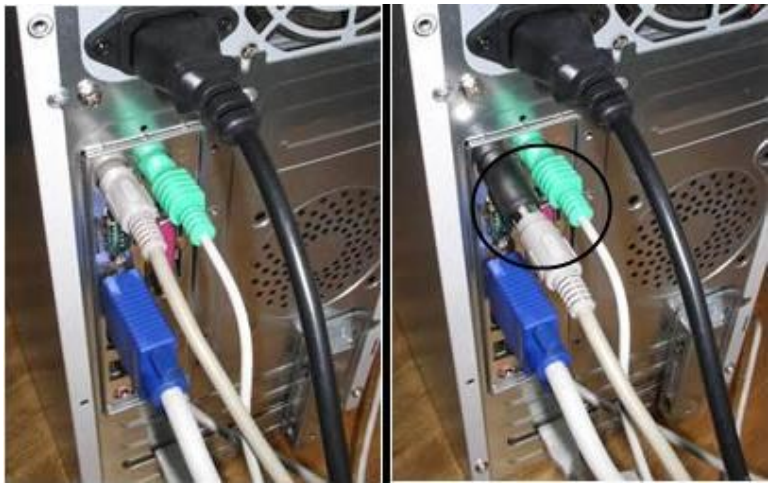
# Trojan RAT

# Keylogger

Strumento per intercettare tutto ciò che un utente scrive sulla tastiera (Key=tasto, logger=tracciatore)

Può essere hardware (dispositivo fisico) o software (programma portato da trojan o worm)





*Keylogger HW: **controllare** i collegamenti*
*Keylogger SW: Far **girare** l'Antivirus (**aggiornato!!!**)*

# Ransomware

Colpiscono sistemi Windows, apparsi a Settembre 2013 (Cryptolocker) e Maggio 2017 (Wannacry).

Si propagano tramite Trojan o email con attachment maligno travestito da PDF

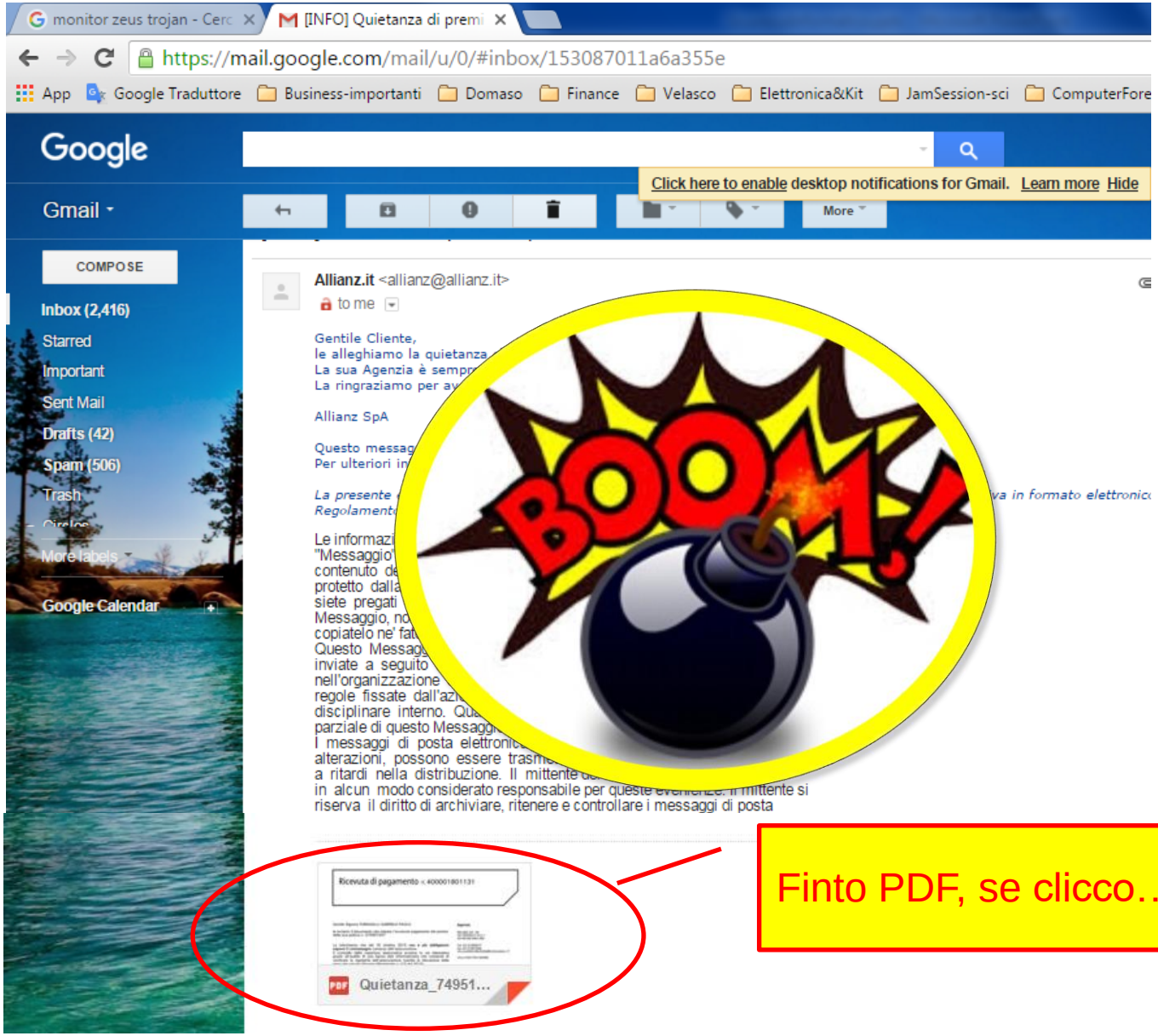
Crittografano i file di lavoro (.xls, .doc, .pdf, foto …) e poi chiedono di pagare un riscatto per decrittografarli.

Anche rimuovendo il Trojan, i file restano cifrati

Si stanno **propagando molto** in questi ultimi 5 anni



# CryptoLocker



# CryptoLocker


*Molti Antivirus **non** lo intercettano. **Controllare** bene le email. **Non lanciare** allegati di dubbia provenienza*

# Ransomware: come comportarsi

Non pagare il riscatto – talvolta la chiave di cifratura/decifratura non è nota agli attaccanti

Ripartire da una copia di backup

Strategia: eseguire backup regolari

Recente evoluzione: prima di crittografare i file, li rubano (esfiltrandoli) per poi vendere i ns dati nel dark web (ulteriore minaccia)



# Annunci tranello

Email che vi coinvolgono emotivamente: vincita, complimenti, vecchi amici, persone ammalate, etc

Arrivano da indirizzi “strani” o con contenuti “strani”: 1000 visitatore del sito, etc

Vogliono arrivare alle **vostre password/dati/foto** o addirittura a **voi stessi** ⇨ state attentissimi, non date i vostri dati

**MAI ACCETTARE APPUNTAMENTI**

***Rifiutate ogni proposta e Avvisate subito** i vostri Genitori che sapranno sempre come aiutarvi*




Attacchi Informatici

# Cyber Attacks

Prendere possesso di una rete informativa e dei relativi sistemi per compiere azioni illecite ed averne un beneficio spesso illegale.

Effettuati all'insaputa dei legittimi proprietari di reti o computer.

Eseguiti da Hackers

**I legittimi proprietari dei computer colpiti appariranno come i colpevoli**.



# Tipi di Attacchi

Controllo del PC altrui

Furto di informazioni: banche, assicurazioni, …

Controllo di impianti: centrali energetiche, industrie,…

MITM: Man In The Middle  (impersonificazione)

Creazione di Botnet, per scopi malvagi

Tranelli, frodi, violazione legge



# Quanti? Dove? Mappe Cyber Threats

https://threatmap.bitdefender.com/

https://threatmap.checkpoint.com/

https://cybermap.kaspersky.com/

http://threatmap.fortiguard.com/

Sono mappe “live” descrivono attacchi che stanno avvenendo adesso

**Tante altre….quasi sempre aziende che si occupano di Cyber Security**



# Come si contrastano - Blue Team

Team di Informatici Difensori, all'interno di un'organizzazione (azienda, Governo, ecc)

Incaricati di intercettare le minacce, prevenire gli attacchi e risolvere eventuali incidenti

In Italia: CNAIPIC (Polizia Postale e delle Telecomunicazioni)

**C**entro **N**azionale **A**nticrimine **I**nformatico per la **P**rotezione delle **I**nfrastrutture **C**ritiche.

Sala Operativa 24/7 – Intelligence – Analisi

Gli agenti del CNAIPIC sono **FORTISSIMI, fra i migliori al Mondo**

Nelle aziende: Security Operations Centre (SOC)



# Come si contrastano

Attacchi /giorno = ca. 5*60*60*24=432.000 al giorno

Industria/Servizi: Dipartimenti opportuni (Security)

SOC: Security Operation Centre

Autorità e Polizia Postale (CNAIPIC)

Normative e Regolamenti

GDPR: normativa Europea protezione dati sensibili

Consapevolezza e Prevenzione



# La causa principale…quasi sempre

Anche negli attacchi più sofisticati….la Root Cause è quasi sempre collocata fra la sedia e la tastiera

…sfruttano **IGNORANZA** ed **IMPREPARAZIONE**

si evitano con **CONSAPEVOLEZZA** e **PREPARAZIONE**

# Dove “vivono” i cattivi ?

# Navigare nel Dark Web: TOR

The Onion Router - gratis

Browser per navigazione anonima (Firefox modificato)

**The Hidden Wiki:**

http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page

**Torch:**

http://torchdeedp3i2jigzjdmfpn5ttjhthh5wbmda2rr3jvqjg5p77c54dqd.onion/search?query=bitcoin

Tor Project Manifesto:

We believe everyone should be able to explore the **internet with privacy**. We are the Tor Project, a 501(c)3 US nonprofit. We **advance human rights and defend your privacy online** through free software and open networks.

# Tipologie di attacco

# Social Engineering

Ingegneria Sociale: studio del comportamento di una persona al fine di sottrargli informazioni

Sfrutta l'ingenuità della vittima (es. tecnici del gas, etc)

Tecnica usata anche da spie ed agenti segreti

Solitamente si nasconde la proprià identità, ***impersonando*** qualcun altro ⇨ **bravi Attori**

E' molto **sofisticato e difficile da riconoscere. Quando lo si riconosce solitamente il danno è già avvenuto.**



# Social Engineering

E’ un attacco pericolosissimo perché la vittima ripone **piena fiducia** nell’attaccante e risulta disposto a fare praticamente tutto quello che viene richiesto.

La vittima **NON** si accorge dell’attacco, se non quando è troppo tardi.

Si contrasta con la **CONSAPEVOLEZZA**,

lo **STUDIO** e la **PREPARAZIONE**



# Botnet

Nate nel 2001, insieme di computer collegati via Internet, comandati da un botmaster tramite una postazione chiamata Command & Control

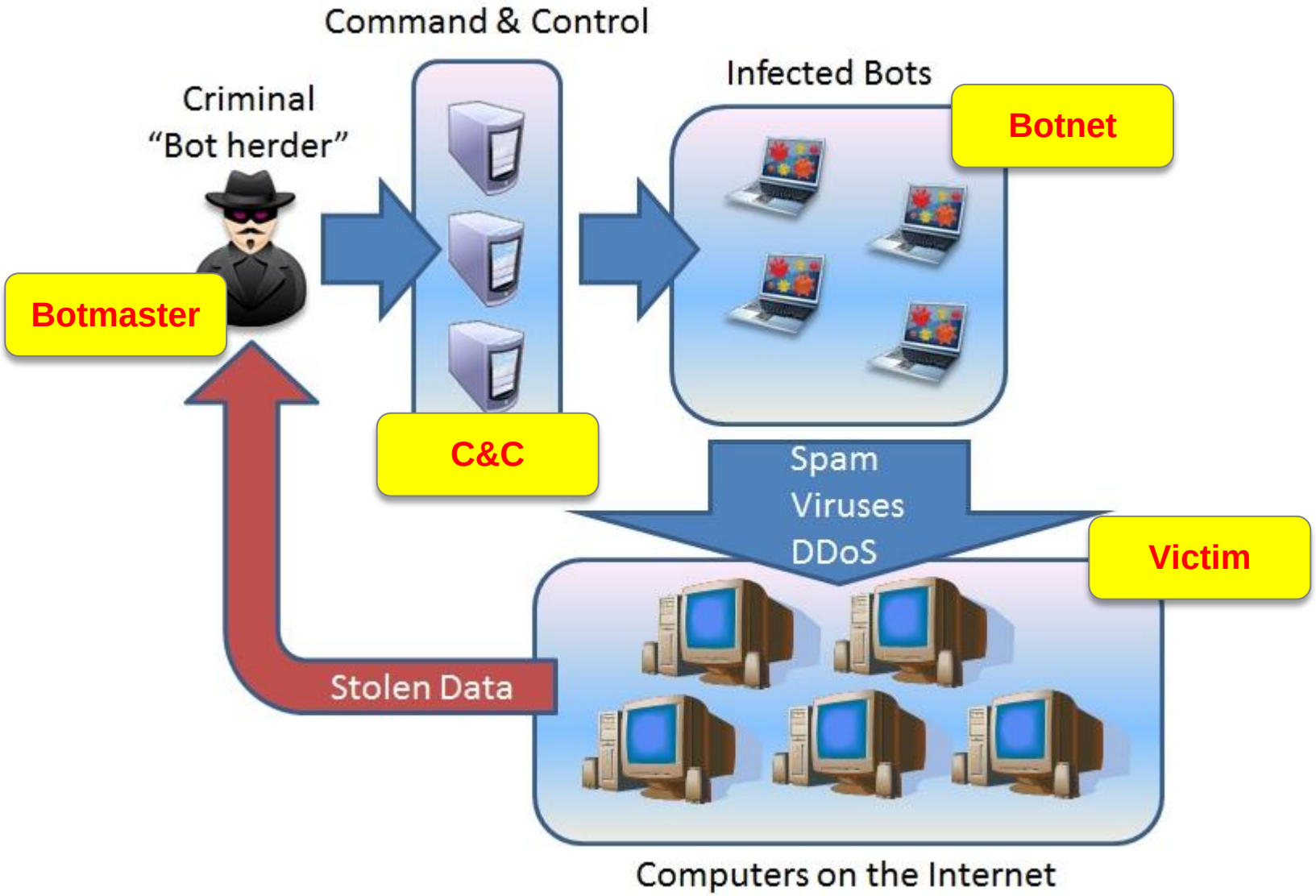
Botnet = ro**bot net**work (rete di robot)

Esercito di computer “Zombie”, ricevono i comandi tramite una chat (IRC), simile a skype o “whatsapp”

Usati per svolgere compiti ripetitivi e quasi sempre malvagi:



# Botnets


Command & Control
Criminal
"Bot herder"
Infected Bots
Botnet
Botmaster
C&C
Spam
Viruses
DDoS
Victim
Stolen Data
Computers on the Internet

# Quanto è difficile procurarsi una Botnet?

Si possono costruire:

- **How To Build A Botnet In 15 Minutes:**

**http://readwrite.com/2013/07/31/how-to-build-a-botnet-in-15-minutes**

**- tante guide disponibili su Web**

**- tanti tool disponibili su Web: es ICE IX**

("Ice IX is a nasty little piece of malware that injects a fake Facebook page")


O affittare: 200 $ al giorno

# DOS o DDOS

DOS= Denial of Service (1 pc attaccante)

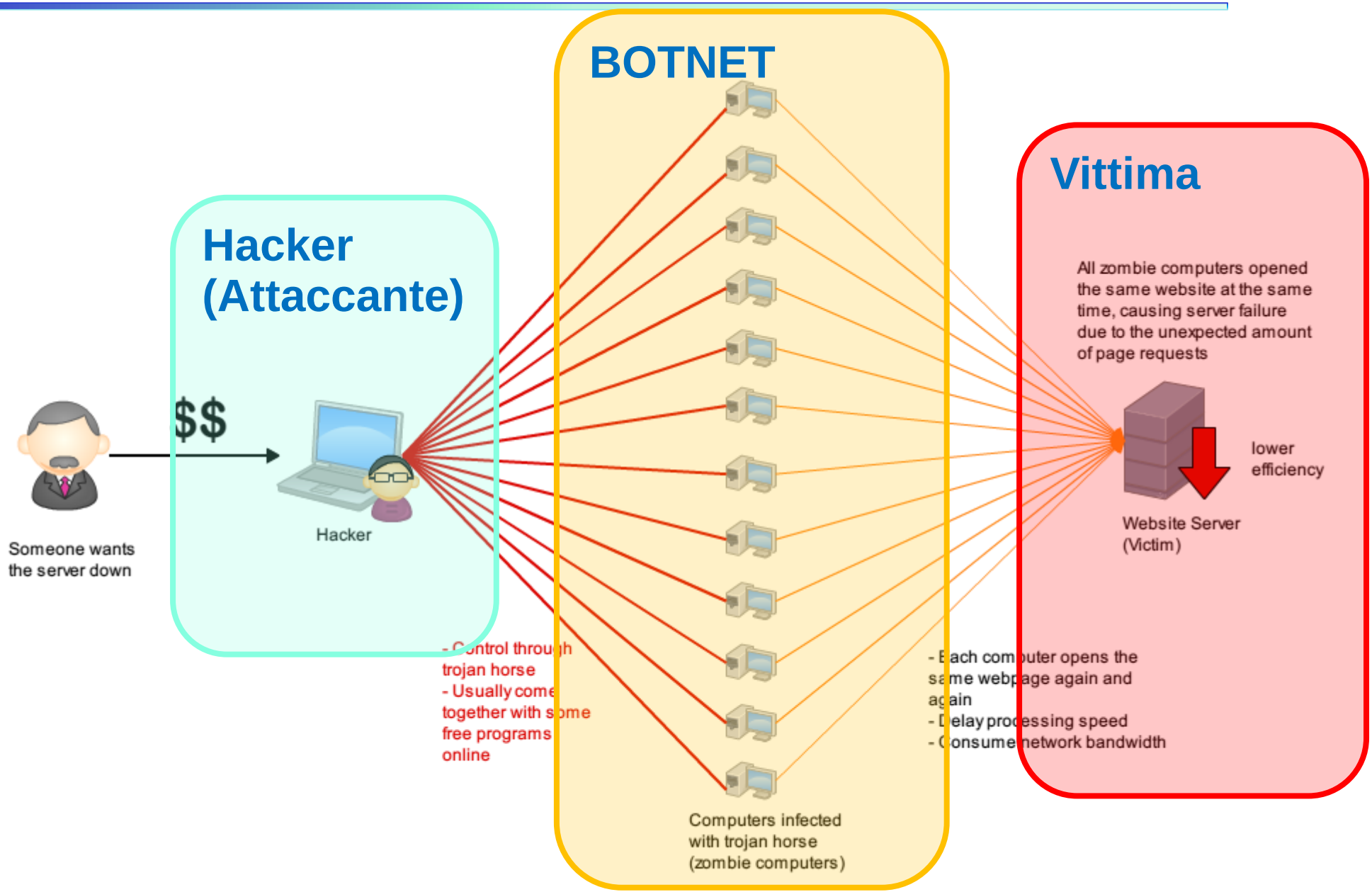
DDOS= Distributed Denial of Service (tanti pc attaccanti)

Un sito viene preso di mira rendendolo indisponibile agli altri utenti che cercando di collegarsi lo troveranno bloccato.

Si blocca il servizio per cui il sito è stato costruito: es. vendita biglietti concerto, online banking, prenotazioni, acquisto di qualche bene, etc



# DOS o DDOS


BOTNET
Hacker (Attaccante)
$$
Someone wants the server down
Hacker
- Control through trojan horse
- Usually come together with some free programs online
Computers infected with trojan horse (zombie computers)
Vittima
All zombie computers opened the same website at the same time, causing server failure due to the unexpected amount of page requests
lower efficiency
Website Server (Victim)
- Each computer opens the same webpage again and again
- Delay processing speed
- Consume network bandwidth

# Phishing

Truffa effettuata raggirando la vittima con tecniche di Social Engineering, convincendola a comunicare informazioni personali, bancarie o riservate.

Di solito si presentano come una email con un link che riconduce ad un sito malevolo simile ad uno vero

**Esempio:** https://mail.**gogle**.com/mail/u/0/#inbox


***Non cliccare** su link sospetti·**Ignorare email** da mittenti non noti· **Non comunicare mai i propri dati se non si è sicuri· Non credere alle facili vincite o assegnazione di premi o richieste di aiuto***



# Attacchi famosi

# Stuxnet


Malware scoperto nel Giugno 2010

Attacco alla **centrale nucleare** di Natanz (Iran)

- Sabotaggio alla centrifuga, aumentando la velocità di rotazione delle turbine per danneggiarle

- Colpiva computer industriali basati su Windows, sfruttando 4 errori di programmazione all'epoca ancora sconosciuti

- La diffusione iniziale avvenne tramite penna USB infetta per poi contaminare gli altri PC collegati alla rete

**Estremamente sofisticato !!!**

# Stuxnet - Identikit

Worm del 2006, apparso nel 2010 - cyberweapon

**TARGET:** Programma Nucleare Iraniano – Centrali

**SISTEMI COLPITI:** PLC con MS Windows+Siemens Step7 -> centrifughe delle centrali

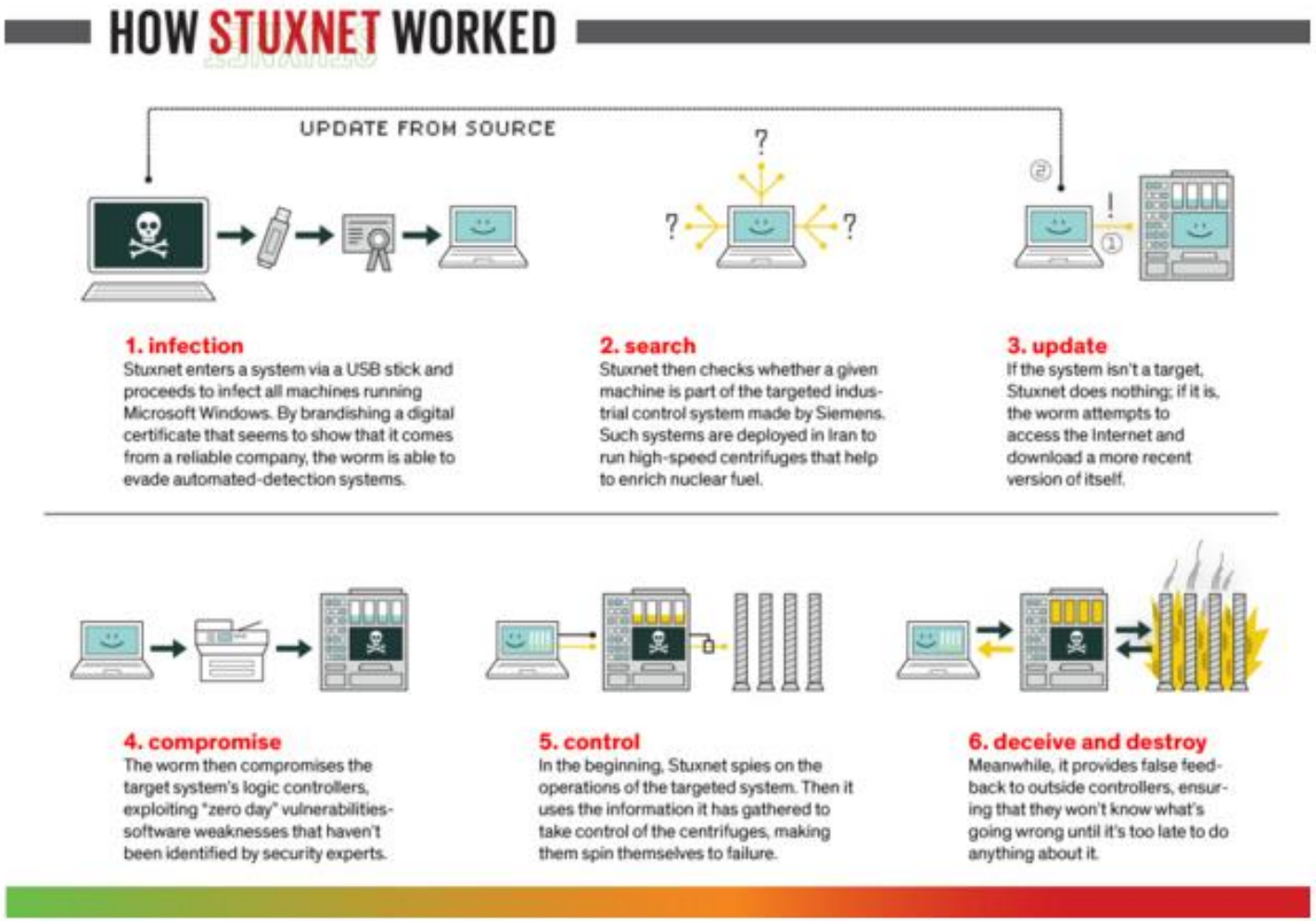
**METODOLOGIA:** 4 vulnerabilità (0-day) di Windows

**CONTAGIO:** chiavetta USB



# Stuxnet

Worm: pare creato dagli USA (operazione “Giochi Olimpici” iniziata nel 2006 contro l’Iran) in collaborazione con il governo Israeliano.



# Stuxnet

**MOVENTE:** Sabotaggio

**MANDANTI:** USA + Israele

**DIFFUSIONE:** incontrollata….

**VARIANTI:** Duqu, Flame (2012)

| Paese | Computer infettati |
|---|---|
| Iran | 62 867 |
| Indonesia | 13 336 |
| India | 6 552 |
| Stati Uniti | 2 913 |
| Australia | 2 436 |
| Regno Unito | 1 038 |
| Malaysia | 1 013 |
| Pakistan | 993 |
| Finlandia | 7[65] |
| Germania | 5 (settembre 2010)[66] |

# Mariposa

Nata: 2008 Smantellata: 2009 Arresti: 2010

**12 Milioni** di computer compromessi, usando un Trojan il cui costo è 800-1000 euro circa

**La più grande botnet mai costruita !**

Si diffondeva tramite chat, chiavette USB o scambio file

Scopo principale: rubare credenziali e file importanti

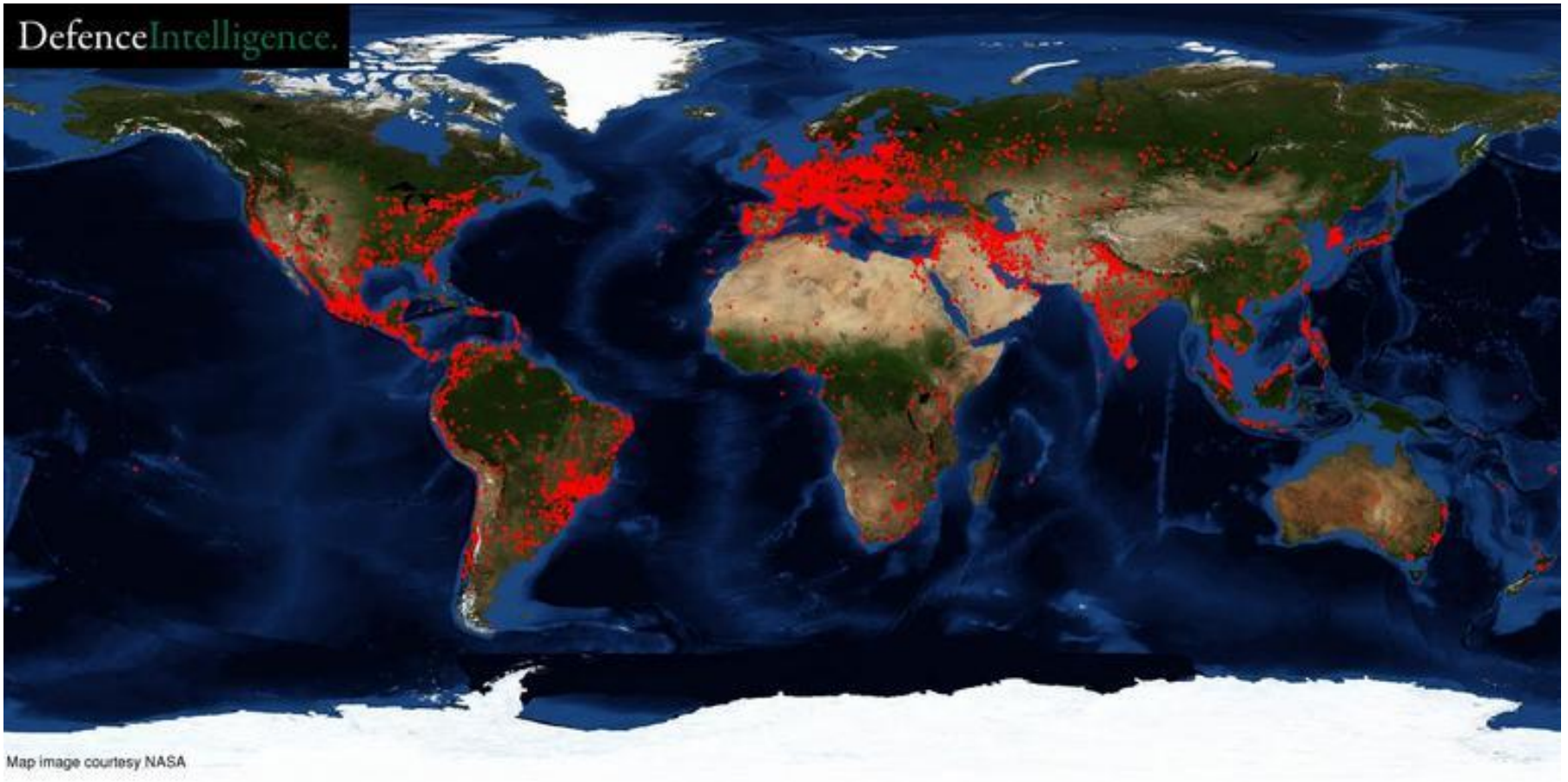
Scopo secondario: affittare la rete per altri attacchi (DDOS), a pagamento

Arrestati: 1 Sloveno (Trojan), 3 Spagnoli (Botnet)

**Intera storia:** http://defintel.com/docs/Mariposa_White_Paper.pdf



# Mariposa




**Come è stata scoperta?** Il capo della banda (Netkairo) si è collegato da casa sua (1 sola volta!), anziché da un Internet point anonimo.

# Zeus

Trojan diffuso tramite mail di phishing o download da siti maligni che colpisce sistemi Windows

Contiene un keylogger software (legge i tasti che schiacciamo)

Ruba informazioni bancarie, credenziali email e per accesso ai social network  e costruisce una botnet

Scoperto nel 2007, è **ancora in circolazione**

Vi sono molte varianti, difficilmente intercettate dagli antivirus

Talvolta viene usato per installare CriptoLocker



# Esempi recenti

John Brennan, Direttore CIA - Social Engineering - 2015

https://www.wired.com/2015/10/hacker-who-broke-into-cia-director-john-brennan-email-tells-how-he-did-it/

Hackers Stole $80 Million from Bangladesh Bank – RAT - 2016

http://thehackernews.com/2016/03/bank-hacking-malware.html

How Hacking Team got hacked – Intrusion - 2015

https://arstechnica.com/information-technology/2016/04/how-hacking-team-got-hacked-phineas-phisher/




Grazie, spero sia stato di Vostro interesse ☺
Andrea Fumagalli