

La Cultura della Sicurezza Informatica

Una Necessità ?

Dai Problemi alle Buone Abitudini



Luca Sacchi Ricciardi

Milano - 20/10/2017

Benvenuti



Luca Sacchi Ricciardi



Umano | Informatico | Geek

Salve a tutti e benvenuti a questa V edizione di DigitalMeet !

Mi chiamo Luca e sono qui a condividere con Voi la conoscenza di quanto ho appreso in 19 anni di consulenza nel mondo dell'informatica.

L' Agenda di Oggi

Benvenuti!

Poche parole per ringraziarvi



Chi Sono

Umano (?), Informatico, Geek

"2016/17 Eventi"

Panoramica sulla Sicurezza
Informatica



La Difesa

Buone Abitudini per difendere i
nostri dati



50% + 50%

Presentazione + Q&A



Rischiare ?

Cattive Abitudini



Tenere al sicuro l'OS

Tecniche e consigli

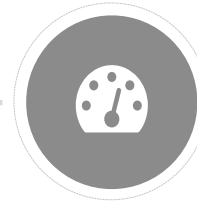
Step #1 - Connessione

VPN+DNS+Firewall



Step #2 Browser

DNT+Anonymous Browsing+Web
Filtering



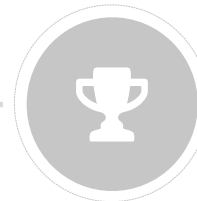
Step #3 Divide Et Impera

Account Lavoro VS Personale
Personal Firewall & Antivirus



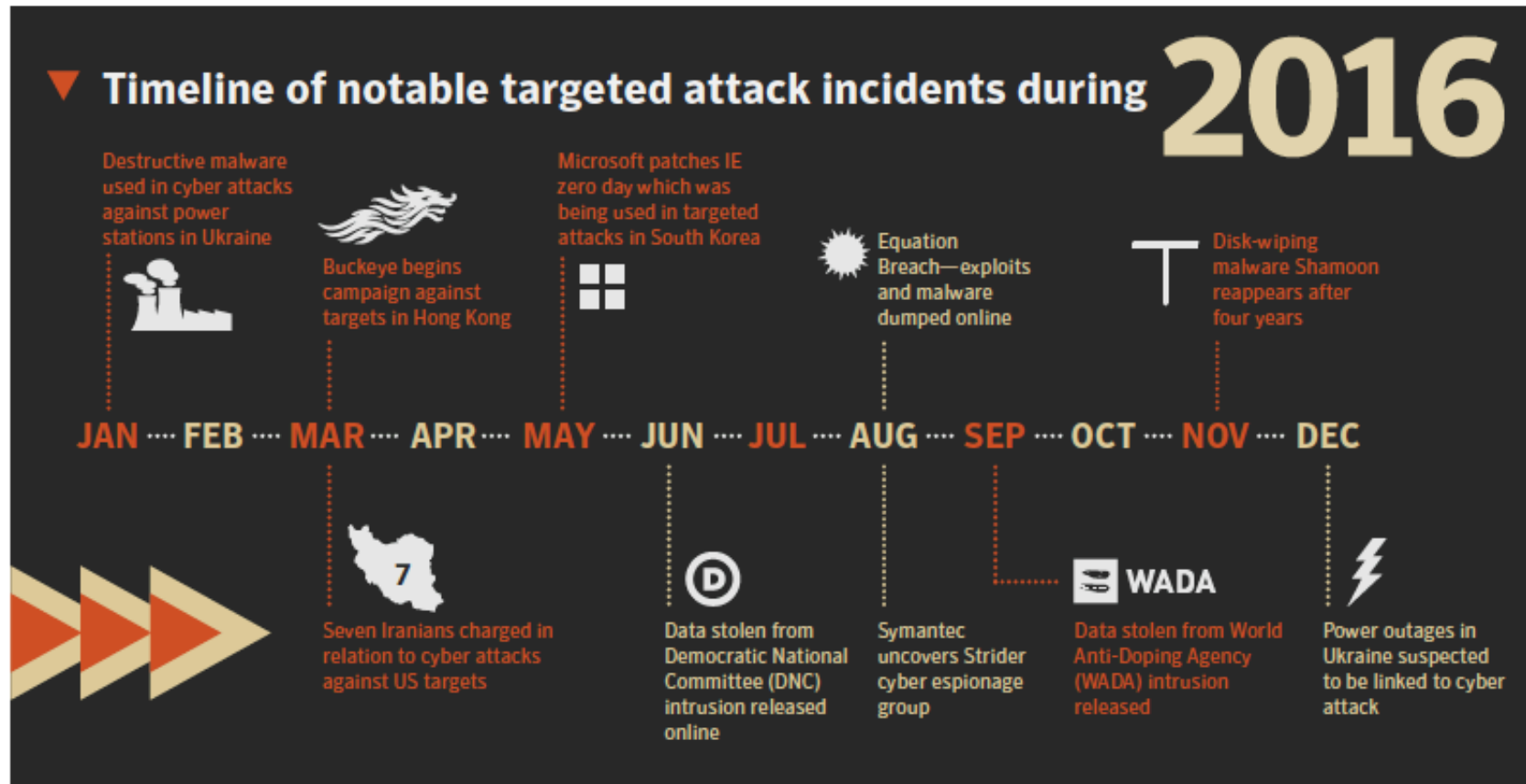
Conclusioni

Ricapitoliamo





"2016 Eventi"



Fonte:  Symantec

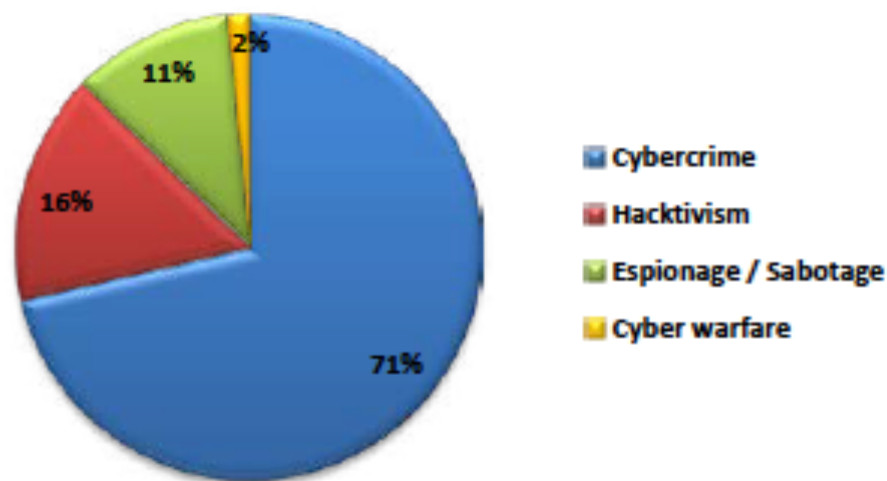
"2016 Eventi"

Cosa è accaduto ?

Vediamo assieme alcuni dati tratti dall'ultimo rapporto di



Tipologia e distribuzione degli attaccanti - 1H 2016



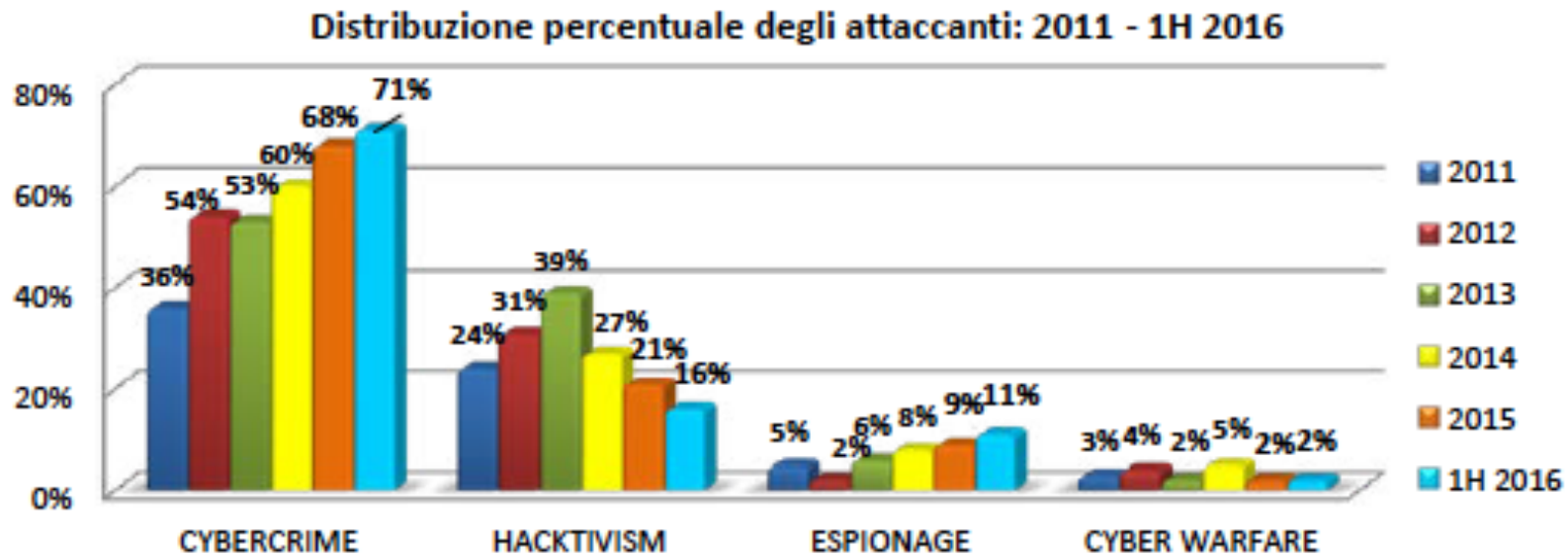
© Clusit - Rapporto 2016 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2016

<https://clusit.it/pubblicazioni/>

"2016 Eventi"

Cosa è accaduto ?

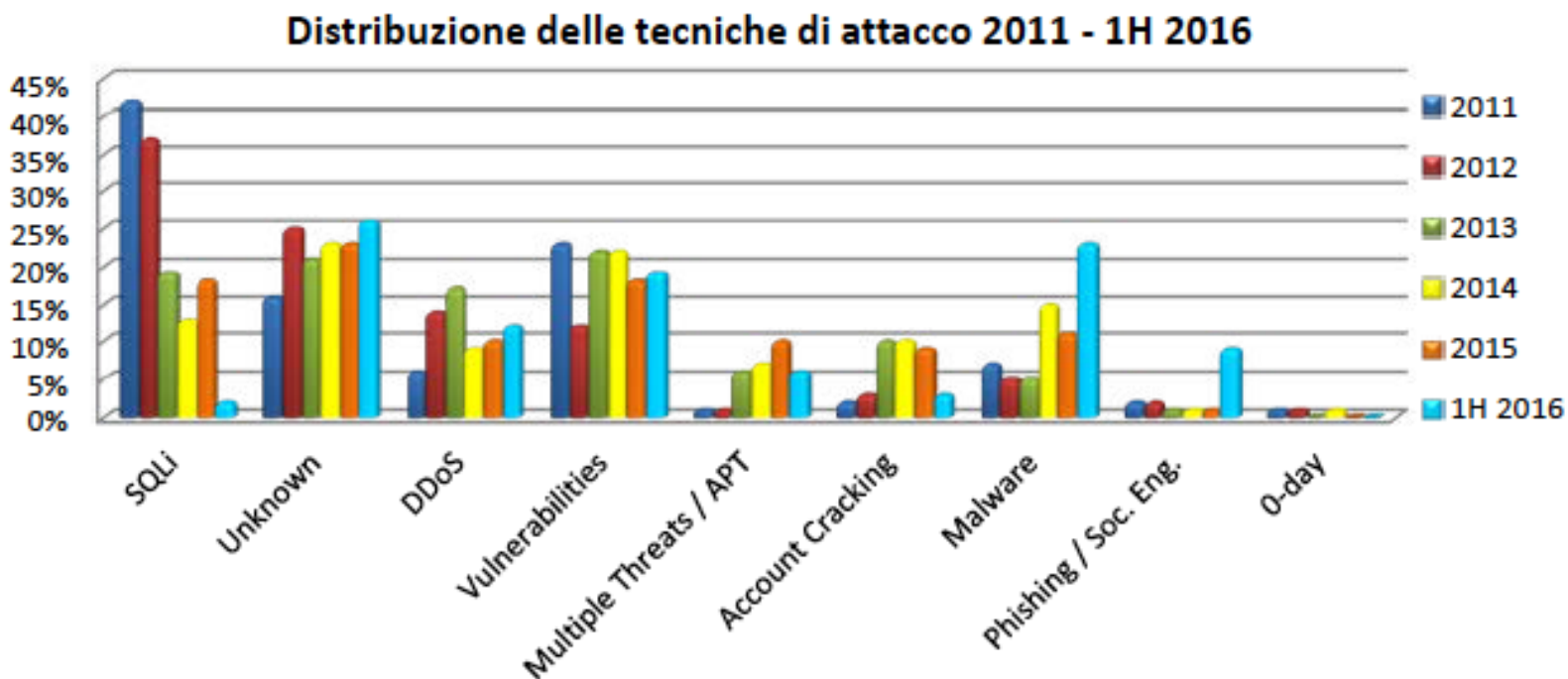
Vediamo assieme alcuni dati tratti dall'ultimo rapporto di



"2016 Eventi"

Cosa è accaduto ?

Vediamo assieme alcuni dati tratti dall'ultimo rapporto di



Rapporto 2016 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2016

<https://clusit.it/pubblicazioni/>

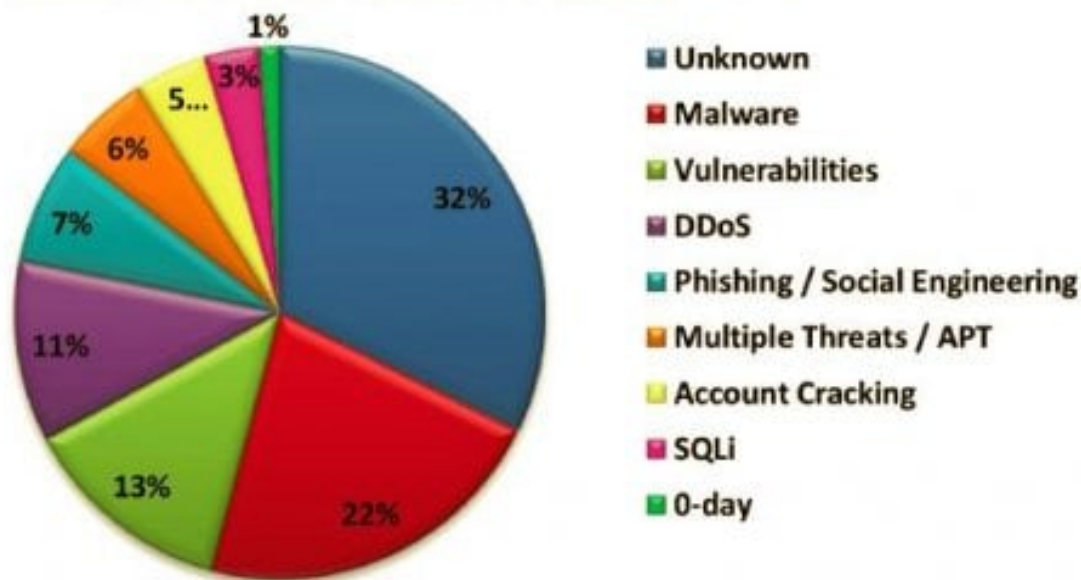
"2016 Eventi"

Cosa è accaduto ?

Vediamo assieme alcuni dati tratti dall'ultimo rapporto di



Tipologia e distribuzione delle tecniche d'attacco - 2016



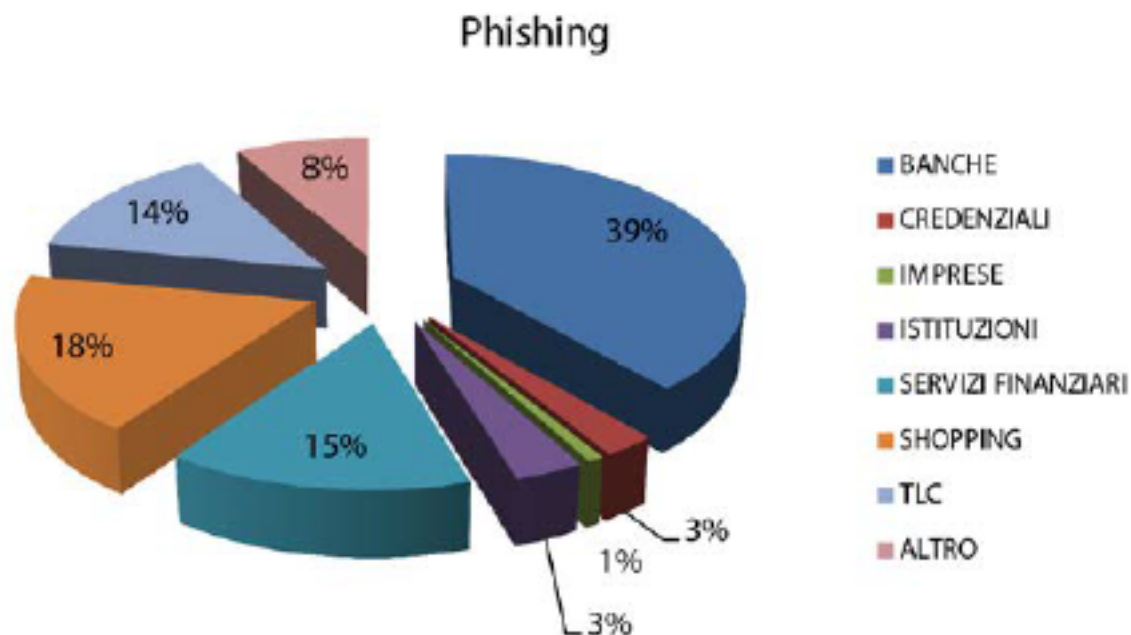
© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

<https://clusit.it/pubblicazioni/>

"2016 Eventi"

Cosa è accaduto ?

Vediamo assieme alcuni dati tratti dall'ultimo rapporto di



Rapporto 2016 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2016

<https://clუსit.it/pubblicazioni/>

2016 Eventi

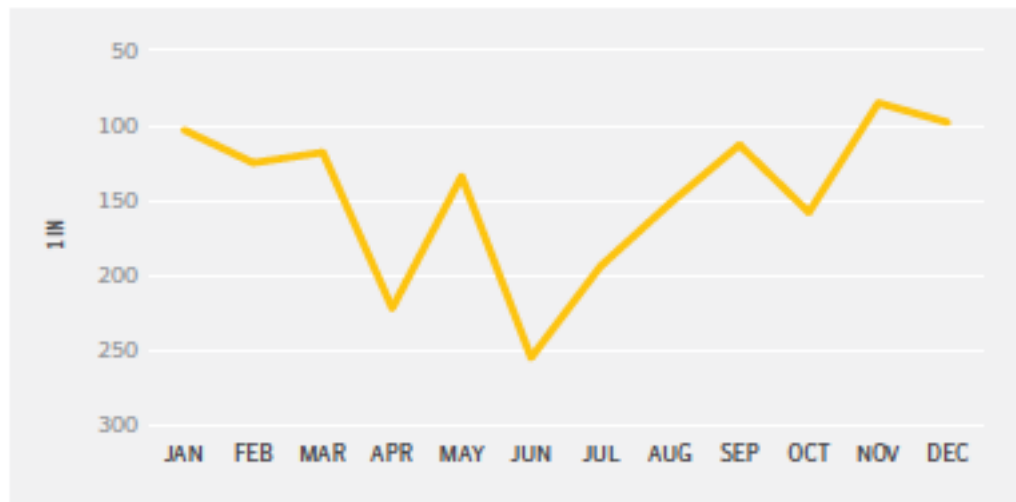
AUMENTO DEI MALWARES

Vediamo assieme alcuni dati tratti dall'ultimo rapporto di



Overall email malware rate

2014	2015	2016
1 in 244	1 in 220	1 in 131



2016 Eventi

CALO DEL PHISING

Vediamo assieme alcuni dati tratti dall'ultimo rapporto di  Symantec

Overall phishing rate

2014	2015	2016
1 in 965	1 in 1846	1 in 2596

2016 Eventi

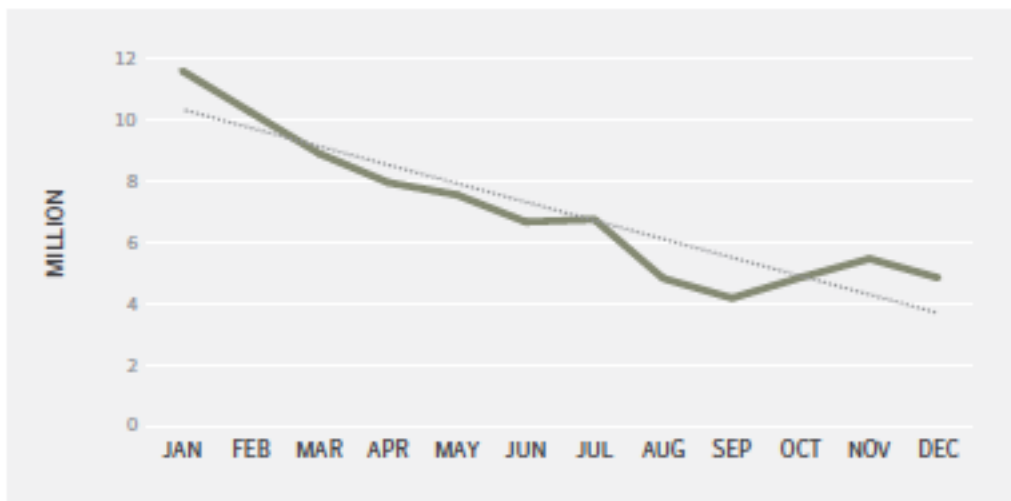
CALO ATTACCHI A SITI WEB

Vediamo assieme alcuni dati tratti dall'ultimo rapporto di



Web attacks blocked per month

The number of web attacks per unique system fell steadily throughout 2016.



2016 Eventi

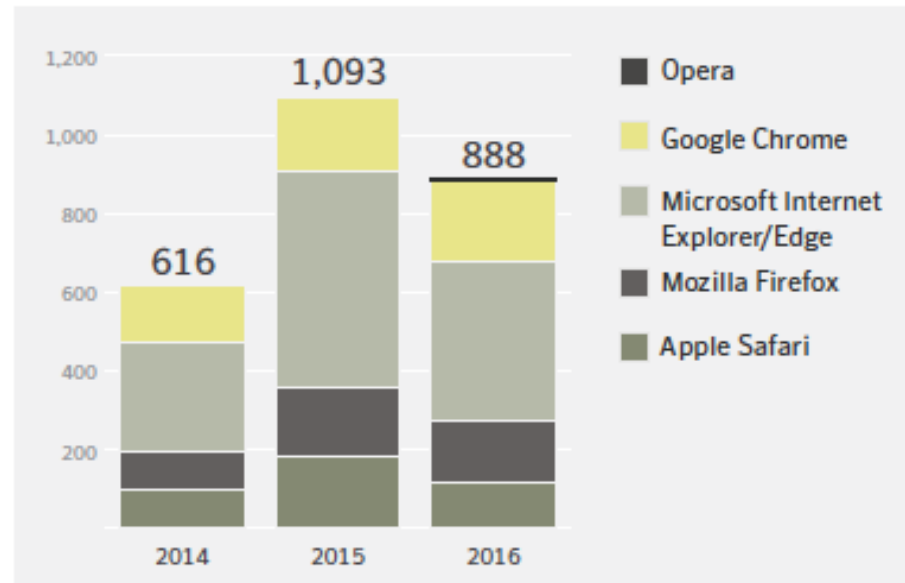
BROWSER PIU' SICURI

Vediamo assieme alcuni dati tratti dall'ultimo rapporto di



Browser vulnerabilities

The number of browser vulnerabilities discovered dropped from 1,093 in 2015 to 888 in 2016.



2016 Eventi

Vediamo assieme alcuni dati tratti dall'ultimo rapporto di  Symantec

- 01** Email received disguised as routine notification, most commonly an **INVOICE** or **RECEIPT**



- 02** Includes attachment, typically JavaScript (JS) file or Office file containing malicious macro



- 03** Opened attachment executes PowerShell script to download malware



- 04** Malware downloaded is typically ransomware

The final payload is typically ransomware but may also be an online banking threat such as Dridex



Rischiare ?

Le cattive abitudini

A mio avviso a mettere a rischio i nostri dati sono principalmente questi comportamenti :

- uso di software non originale (cracks spesso contengono malware)
- uso di documenti infetti (ebooks e docs)
- uso di siti di streaming online (che installano plugins di adware o mining Bitcoin)
- non installare ed aggiornare con regolarità antivirus/anti-malware e personal firewall
- non usare strumenti di limitazione alla navigazione (webfiltering)

La Difesa

Ottime Abitudini

Penso che siano ottime abitudini :

- usare solo software originale (io preferisco l'OpenSource) ed aggiornarlo.
- usare il proprio OS imparando a conoscerlo sia da utente che da admin
- effettuare su dispositivi esterni il backup dei dati
- usare antivirus anti-malware e sistemi di sandboxing.
- limitare la tipologia di siti visitabili (webfiltering)

Tenere al sicuro l'OS

Ottime Abitudini

Scegliete prima di tutto un sistema operativo attuale (es. Linux, Windows10, HighSierra)

- usate un utente non privilegiato per le attività giornaliere
- effettuate backup frequenti
- aggiornate regolarmente e spesso OS e tools antivirus/anti-malware
- tenete attivo il firewall del vostro computer
- effettuate con regolarità la manutenzione da admin o usate appositi tools.

Step #1 - Connessione

Ottime Abitudini

Ecco alcune cose che si possono fare per mettere in sicurezza la connessione:

- abilitare il firewall (packet inspection) sul router (e tenere aggiornato se possibile il suo firmware)
- usare connessioni WiFi crittografate (e se paranoici anche una vpn se ci si connette via WiFi)
- usare una VPN per mascherare al provider il proprio traffico
- usare un servizio DNS che permetta il webfiltering e protegga da malware
- usare (in ufficio) meccanismi di authentication/authorization/accounting.

Step #2 Browser

Ottime Abitudini

Ecco alcune cose che si possono fare per mettere in sicurezza la navigazione:

- usare account differenti se si usa lo stesso pc per lavoro e svago
- usare un browser di ultima generazione aggiornato regolarmente
- personalizzare le impostazioni per attivare meccanismi a protezione della privacy come il “Do Not Track (DNT)”
- usare la navigazione “anonima”
- navigare senza aver effettuato login al browser (Chrome)
- installare solo estensioni ‘affidabili’
- usare tools come Pi-Hole per filtrare le pubblicità
- sottoscrivere (gratis) un servizio per filtrare la navigazione per categorie

Step #3 Divide Et Impera

Ottime Abitudini

Ricorda che è sempre meglio dividere gli ambiti di utilizzo e tenere separati svago e lavoro.

Se come me utilizzi sempre lo stesso PC, usa due account differenti.

Conclusioni

...

Abbiamo visto quale sia la situazione della Sicurezza Informatica in Italia e preso atto del fatto che occorra un risveglio: occorre tenersi informati , adottare buone abitudini nell'uso della tecnologia e continuare sempre a formarsi.

La pigrizia e l'ignoranza saranno sempre fonte di preoccupazione e guai.

Riferimenti

Qui di seguito i link al materiale utilizzato per illustrare i concetti esposti ed altri che ho il piacere di segnalarVi quali fonti interessanti per approfondimenti

Fonti:

<https://www.symantec.com/content/dam/symantec/docs/reports/istr-healthcare-2017-en.pdf>

https://clusit.it/wp-content/uploads/download/Rapporto_Clusit%202016.pdf

Siti di informazione:

<http://www.ilsole24ore.com/tecnologie/sicurezza-e-privacy.shtml>

<http://www.fastweb.it/tag/?i=sicurezza%20informatica>

<https://clusit.it/pubblicazioni>

Video:

<https://www.youtube.com/watch?v=Yg1gWyY8fDw>

Q & A



Luca Sacchi Ricciardi

----->
Umano | Informatico | Geek



<https://www.facebook.com/illucasacchi/>



[@il_Luca_Sacchi](https://twitter.com/il_Luca_Sacchi)



<http://it.linkedin.com/in/lucasacchi>

Grazie per aver partecipato



Luca Sacchi Ricciardi

Umano | Informatico | Geek



<https://www.facebook.com/illucasacchi/>



[@il_Luca_Sacchi](https://twitter.com/il_Luca_Sacchi)



<http://it.linkedin.com/in/lucasacchi>