Ordine degli Ingegneri della provincia di Forlì-Cesena

RELATORE: Ing. Giorgio Sbaraglia

07 APRILE 2017

Giorgio Sbaraglia ©–2017

La presente documentazione è sottoposta alla licenza sul diritto d'autore **Creative Common CC BY-NC-ND**.

È permessa la ridistribuzione solo in forma intera ed invariata, citando espressamente l'autore.

Non può essere modificata o distribuita commercialmente.

Qualsiasi utilizzo diverso dalla succitata licenza potrà essere fatto solo previa richiesta all'autore Giorgio Sbaraglia (*giorgio@giorgiosbaraglia.it*).

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Corollario (informatico…) alla Legge di Murphy

Non importa chi sei

Non importa cosa fai

Non importa con cosa lo fai

Ti attaccheranno

(cit. Alessio Pennasilico - CLUSIT)

TUTTO CIÒ CHE PUÒ ESSERE ATTACCATO LO SARÀ

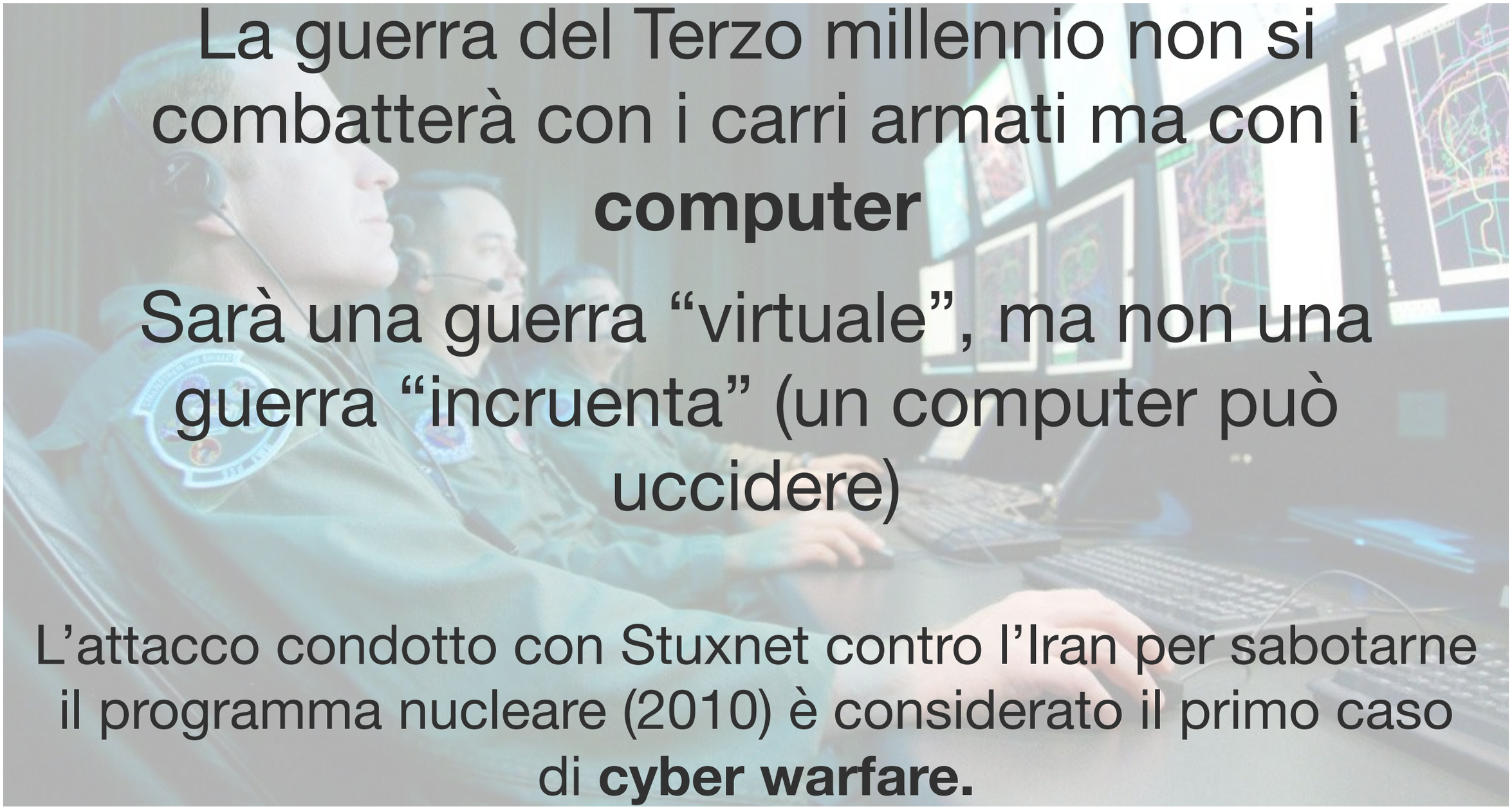
Giorgio Sbaraglia ©–2017

Agenda

1. Come si è evoluto il Cybercrime
2. Il Rapporto CLUSIT 2017
3. DeepWeb, Dark Web, rete TOR e Bitcoin
4. Le principali tecniche di attacco
5. I Ransomware
6. Il Social Engineering
7. I Malware su devices mobili
8. Come possiamo difenderci

Giorgio Sbaraglia ©–2017

CYBERWARFARE:
la guerra cibernetica



La guerra del Terzo millennio non si combatterà con i carri armati ma con i **computer**

Sarà una guerra “virtuale”, ma non una guerra “incruenta” (un computer può uccidere)

L’attacco condotto con Stuxnet contro l’Iran per sabotarne il programma nucleare (2010) è considerato il primo caso di **cyber warfare.**

Giorgio Sbaraglia ©–2017

Dicembre 2015: gli hacker "spengono" l'Ucraina

23 dicembre 2015 ore 15:35: la Ukrainian Kyivoblenergo, un distributore regionale di elettricità, subisce un attacco hacker.

Sette sottostazioni a 110 kV e ventitré a 35 kV vengono disconnesse per oltre tre ore.

L'attacco, proveniente da un paese straniero, prende il controllo da remoto dei sistemi SCADA delle centrali. Per ripristinare il servizio, i gestori sono dovuti passare al controllo manuale degli impianti.

225.000 persone rimangono senza energia elettrica.

Nel dicembre 2016 l'attacco si ripete, ma in forma più leggera (forse un test degli hacker per future azioni?)

Giorgio Sbaraglia ©–2017

Il FATTURATO del CYBERCRIME ha superato quello del traffico di DROGA

Giorgio Sbaraglia ©–2017

Agenda

1. Come si è evoluto il Cybercrime
2. **Il Rapporto CLUSIT 2017**
3. DeepWeb, Dark Web, rete TOR e Bitcoin
4. Le principali tecniche di attacco
5. I Ransomware
6. Il Social Engineering
7. I Malware su devices mobili
8. Come possiamo difenderci

BY NC ND Giorgio Sbaraglia ©–2017

Rapporto Clusit 2017, l'Italia preda degli hacker

Attacchi compiuti con tecniche di Phishing e Social Engineering:

+1.166%

Giorgio Sbaraglia ©–2017

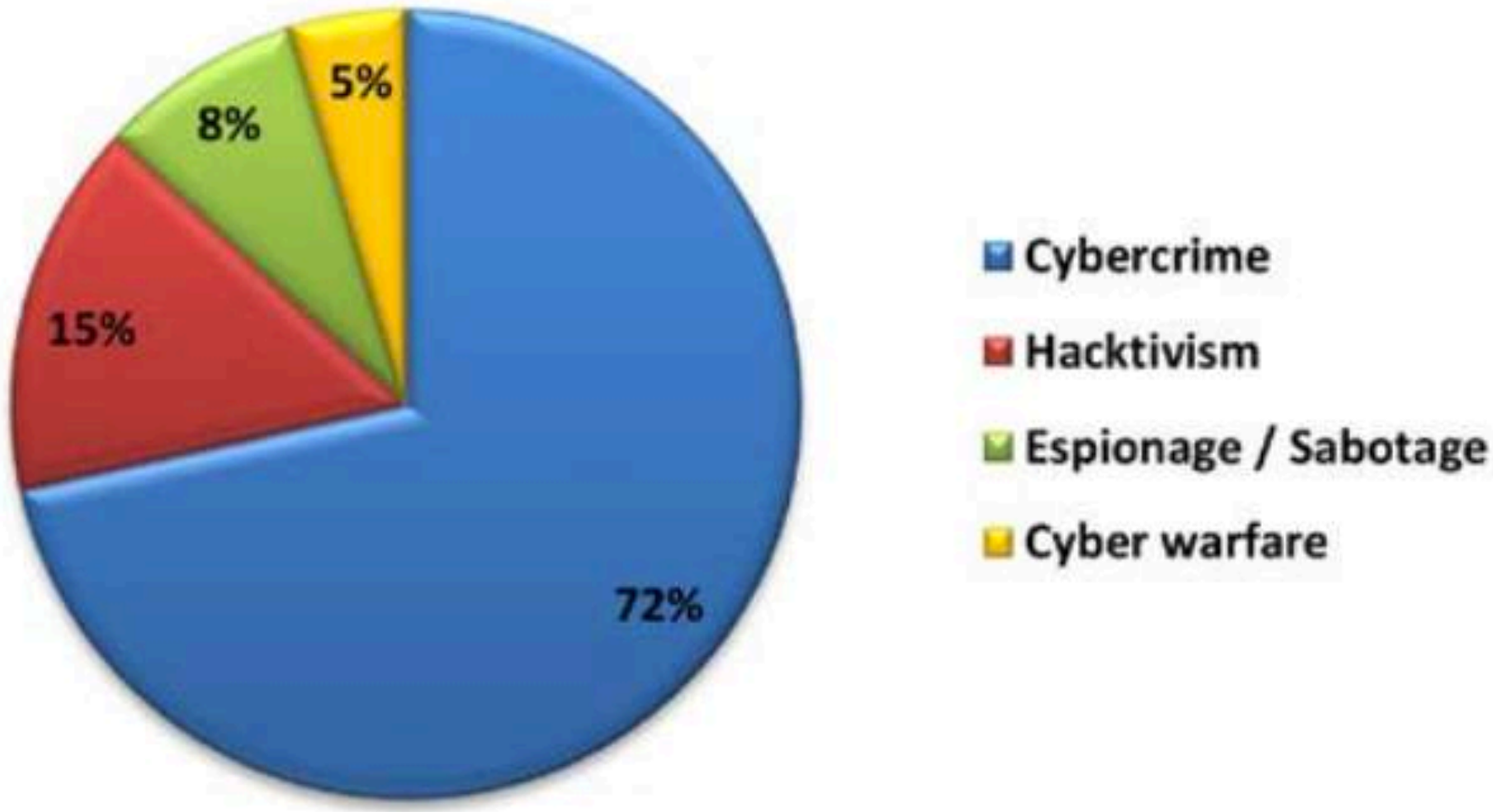
Rapporto 2017

Il 2016 è stato l'**anno peggiore di sempre** in termini di evoluzione delle minacce "cyber" e dei relativi impatti.

- **Cybercrime** (Ransomware, ecc.): **72% del totale, +9,8%**
- **Cyber warfare +117%**
- **Hacktivism -23%**
- **Health (sanità) è il settore con la crescita maggiore (+102%)**
- **230.000 malware creati ogni giorno**

Giorgio Sbaraglia ©–2017

Tipologia e distribuzione degli attaccanti - 2016



© Clusit - Rapporto 2017 sulla Sicurezza ICT in Italia

EURISPES

Dal 1982
l'Istituto di Ricerca
degli italiani

RI2017
29°
RAPPORTO ITALIA

Rapporto Italia 2017 Eurispes

Il cybercrime costa alle aziende italiane

9 miliardi di euro l'anno.

Le piccole e medie imprese temono:

- furto dati dei clienti (20%),
- reputazione aziendale (17%),
- furti di denaro (11,5%),
- furti di identità (7,5%),
- furto di dati dei dipendenti (6,5%).

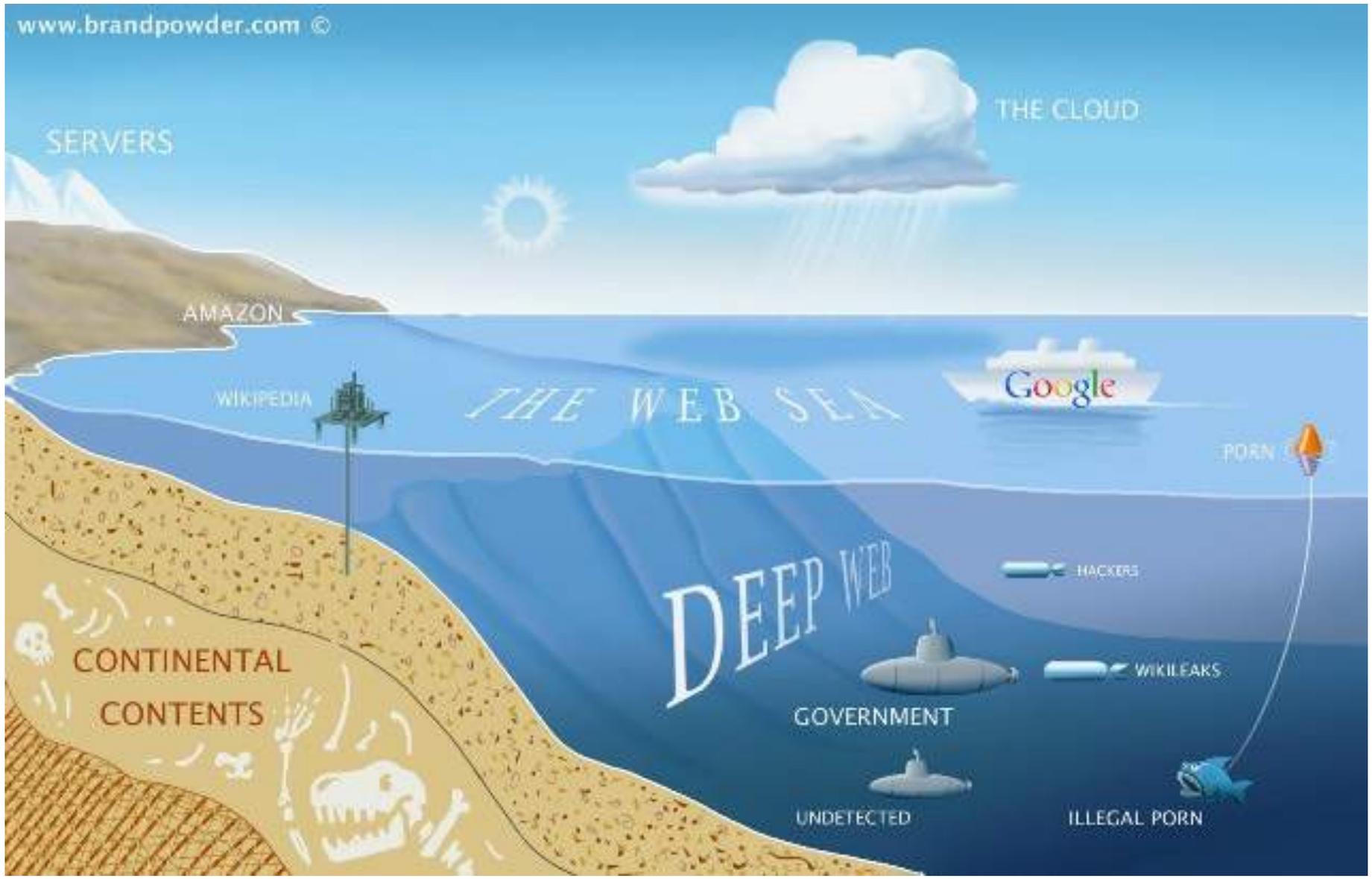
Giorgio Sbaraglia ©–2017

Agenda

1. Come si è evoluto il Cybercrime
2. Il Rapporto CLUSIT 2017
3. **DeepWeb, Dark Web, rete TOR e Bitcoin**
4. Le principali tecniche di attacco
5. I Ransomware
6. Il Social Engineering
7. I Malware su devices mobili
8. Come possiamo difenderci

Giorgio Sbaraglia ©–2017

Deep Web e Dark Web



Deep Web (aka **Hidden Web)**: indica l'insieme dei contenuti presenti sul web e **non indicizzati** dai comuni motori di ricerca (ad es. Google, Bing);

Dark Web invece indica l'insieme di contenuti accessibili pubblicamente che sono ospitati in siti web il cui indirizzo IP è nascosto, ma ai quali chiunque può accedere purché ne conosca l'indirizzo. (*cit. Rapporto CLUSIT 2016)*

Giorgio Sbaraglia ©–2017

Deep Web e Dark Web

L'opposto del **Deep Web** si chiama **SurfaceWeb** (o Visible Web o Indexed Web).

Il **Dark Web** è quella parte del Deep Web che sfrutta le **Darknet.** Per accedervi sono necessarie particolari configurazioni ed autorizzazioni.

Le principali Darknet sono: Freenet, I2P e **TOR** (**The Onion Router**).

TOR è stato creato negli anni '90 nei laboratori della Marina Militare USA. Nel 2006 è stato rilasciato come SW di pubblico dominio.

Quanto è grande il Deep Web?

Impossibile saperlo, ma si ritiene che sia **400-500 volte più grande del Surface Web.**

Le pagine indicizzate da Google sono 30,000,000,000,000 (30.000 Miliardi), dato ricavato da www.statisticbrain.com (anno 2014) per un totale di dati indicizzati di oltre 100.000.000 GB.

Moltiplichiamo quindi questi numeri per 400-500 volte.

Giorgio Sbaraglia ©–2017

Hackers, Cybercrime e Dark Web

Nel Dark Web esistono i **Black Market:** un mercato nero di vulnerabilità ed exploit.

Si sta sviluppando il modello di vendita noto come **criminal-as-a-service (CaaS)**, in cui gruppi di **hacker** offrono i propri servizi al **crimine ordinario** (che si sta spostando nel cybercrime).

Azienda	Luogo	Restrizioni/Caratteristiche	Prezzi
Vupen	Francia	Non vende a liste nere USA, Nato, UE. Tra i clienti la NSA	100mila dollari di sottoscrizione al suo bollettino. Più i costi di singole vulnerabilità
Zerodium	USA	Fa brokeraggio. Non vende a liste nere USA, Nato. Riporta le vulnerabilità ad aziende di	Fino a 1 milione di dollari per exploit
Exodus Intelligence	USA	cybersicurezza e governi, basata in gran parte su ricerca interna.	
Endgame	USA	Dice di vendere solo ai governi	
Netragard	USA	Solo clienti Usa (ma vedi articolo). Chiuso da poco il programma	Tra i 25 e i 160mila dollari a exploit
ReVuln (Luigi Auriemma, Donato Ferrante)	Malta	Specializzati in sistemi industriali (SCADA)	
Arc4dia	Quebec	Vende solo ad agenzie governative	
The Grugq	Bangkok	Lavora solo con governi USA e UE	Prende il 15 per cento di commissione (fonte Forbes)
Immunity	USA	Basata a Miami, fornisce un feed aggiornato di vulnerabilità ed exploit (anche non 0-day)	
Absolute Zero Day (Kevin Mitnick)	USA	Lanciato nel 2014, fa da broker tra compratori e venditori, segue restrizioni commerciali legge Usa.	
VBI (Dustin Trammel)	USA		Exploit intorno ai 100mila dollari
Security Brokers (Raoul Chiesa)	Italia		Dai 30 ai 50mila dollari a exploit a salire

Giorgio Sbaraglia ©–2017

Vulnerabilità, Exploit, Zero-day

Vulnerabilità	Una falla nella sicurezza di un programma, che può essere sfruttata per portare un attacco
Exploit **Exploit kit**	**Exploit** è un codice che sfrutta una vulnerabilità per portare un attacco. **Exploit kit** è un tool software che consente di automatizzare lo sfruttamento di vulnerabilità software ed eseguire un codice malevolo. La relativa facilità d'uso lo rende utilizzabile anche da hacker non particolarmente esperti. I più famosi: ANGLER, NEUTRINO, NUCLEAR.
Zero-Day	Una vulnerabilità nota solo agli attaccanti, non agli sviluppatori del software, che quindi hanno avuto zero giorni per ripararla. Gli exploit Zero-Day sfruttano queste falle.

Giorgio Sbaraglia ©–2017

La quotazione del BITCOIN

Quotazione: ***1.141 USD/BTC*** *pari a:* ***1.067 €/BTC*** *(al 03/04/2017 ore 18:00)*

https://bitcoinity.org/markets

Giorgio Sbaraglia ©–2017

“Ransomware as a Service” (RaaS)

Oggigiorno nel **Dark Web** attraverso la rete **TOR (*The Onion Router*)** vengono offerti software Ransomware come **SATAN** che chiunque può “acquistare”, personalizzare e diffondere per infettare vittime, criptare i loro documenti e chiedere un riscatto in bitcoin.

Gli sviluppatori di Satan trattengono il 30% dei riscatti (può essere ridotta, se gli “incassi” sono alti!), il resto va al “cliente”.

Il rischio del **Ransomware-as-a-Service** è che questo tipo di minacce diventino fin troppo facili da sfruttare per chiunque.

Giorgio Sbaraglia ©–2017

Agenda

1. Come si è evoluto il Cybercrime
2. Il Rapporto CLUSIT 2017
3. DeepWeb, Dark Web, rete TOR e Bitcoin
4. **Le principali tecniche di attacco**
5. I Ransomware
6. Il Social Engineering
7. I Malware su devices mobili
8. Come possiamo difenderci

Giorgio Sbaraglia ©–2017

Le principali tecniche di cyber attacco

- Gli attacchi DDoS e le Botnet (e IoT…!)
- SQL Injection.
- APT (Advanced Persistent Threat).
- Attacchi "man-in-the-middle" e il protocollo HTTPS.
- I Keylogger.
- La vulnerabilità dei siti web: i rischi di WordPress e dei CMS open source.

Giorgio Sbaraglia ©–2017

IoT: l'Internet delle Cose

Le tecnologie **IoT**, includono dispositivi dotati di un sistema operativo che permette di connettersi e di scambiare informazioni e dati con altri oggetti per abilitare funzionalità di **monitoraggio** e di **controllo** (che permette agli oggetti di essere comandati a distanza).

Gli oggetti dell'Internet delle Cose:

- Domotica
- Veicoli e Trasporti
- Energia e Utility
- Smartphones
- Industry 4.0
- ecc.

Giorgio Sbaraglia ©–2017

L’attacco DDoS che ha spento mezza Internet in USA

21 ottobre 2016: almeno due attacchi DDoS sono stati sferrati contro **Dyn**, azienda del New Hampshire che fornisce la gestione dei Dns, utilizzando una botnet (*Mirai*) di oltre **500.000 dispositivi di IoT** (webcam, termostati, lampadine, ecc.), con una potenza di circa **1.200 Gbps**.

Molti siti web sono stati resi inaccessibili: Twitter, eBay, New York Times, Financial Times, Spotify, Github, alcuni circuiti Visa, Netflix, Reddit e molti altri.

Qualche settimana prima, un altro attacco DDoS era stato fatto contro il sito “**Krebs on Security**” (con circa **665 Gbps)**.

Giorgio Sbaraglia ©–2017

Un errore troppo frequente

"Ma cosa ci guadagnano ad attaccare proprio il mio computer? Non c'è nulla che possa interessare…"

Sbagliato!

Pensare di non essere un bersaglio appetibile significa non pensare alla sicurezza dei propri sistemi informatici e quindi diventare di fatto un bersaglio facile.

Giorgio Sbaraglia ©–2017

Un errore troppo frequente

Un computer od un server poco protetto può facilmente venire infettato e diventare parte di una botnet oppure essere utilizzato da un booter come "base di lancio" di un attacco DDoS (Distributed denial of service).

Ecco dunque spiegato "cosa ci guadagnano ad attaccare me".

Giorgio Sbaraglia ©–2017

SQL Injection (SQLI)

È un tipo di attacco “antico” che esiste da molto tempo (primi articoli nel 1998).
Sfrutta falle di sicurezza nelle tecniche di sviluppo di **applicativi web**: vengono inserite delle stringhe di codice SQL malevole all'interno di campi di input.
In altre parole: consiste molto semplicemente nell’inserire valori all’interno di campi web che alterino l’interpretazione da parte del database generando quindi query non sicure.

A differenza di un attacco DDoS, **un attacco SQLI può essere facilmente evitato con tecniche di programmazione attente.**

BY NC ND Giorgio Sbaraglia ©–2017

APT: Advanced Persistent Threat

Le minacce APT sono attacchi sofisticati ma anche **estremamente mirati**, che iniziano con l'intrusione dei cybercriminali all'interno della rete aziendale presa di mira.

Sono tra le minacce che oggi preoccupano di più le aziende che gestiscono dati sensibili o a rischio di spionaggio industriale.

- ☑ **AVANZATE:** usano tecniche di hacking avanzate, con più vettori di attacco.
- ☑ **PERSISTENTI:** l'attacco è continuo nel tempo, anche per mesi, si cerca di rimanere nel sistema per un lungo tempo.
- ☑ **MINACCIOSE:** cercano di rubare dati, di spiare e di non essere scoperte.

Giorgio Sbaraglia ©–2017

APT: Advanced Persistent Threat

Non è un classico attacco, dove gli hacker “sparano nel mucchio” con spam e phishing.

Non è come un normale malware o una vulnerabilità, non esiste una “firma” univoca che identifica l’azione di una APT e fa scattare un allarme in qualche software di sicurezza. Vengono usate tecniche di hackeraggio diversificate.

Il particolare livello di sofisticazione che caratterizza gli attacchi APT li rende DIFFICILI DA RILEVARE: possono passare diversi mesi tra il momento dell’attacco iniziale e la sua scoperta e neutralizzazione.

Il tempo medio di scoperta è di circa 220 giorni.

Giorgio Sbaraglia ©–2017

APT: Advanced Persistent Threat

Si sviluppano in SETTE fasi:

1. **Ricognizione:** per studiare l'obbettivo;
2. **Intrusione nella rete:** in genere con tecniche di spear phishing, social engineering;
3. **Furto di identità:** accesso a credenziali utente valide;
4. **Installazione di malware:** RAT (Remote Administration Tool) per controllare il sistema;
5. **Creazione di una backdoor;**
6. **Esfiltrazione dei dati:** per rubare i dati;
7. **Persistenza:** gli hacker cercano di rimanere nel sistema il più a lungo possibile.

Giorgio Sbaraglia ©–2017

I Keylogger

Si tratta di un programma che registra tutto ciò che viene digitato sulla tastiera, permettendo all'hacker di rubare una notevole quantità di dati confidenziali agli utenti (password, ecc.).

Il keylogger (software) più comune è un Trojan.

I keylogger basati su hardware sono meno comuni: richiedono accesso diretto sul computer della vittima.

Giorgio Sbaraglia ©–2017

L'importanza del protocollo HTTPS

IMPORTANTE: I siti sicuri (quelli da usare per dati riservati o pagamenti on-line) devono operare con il protocollo **HTTPS** invece di HTTP.

HTTPS è un protocollo che integra il protocollo standard HTTP con un meccanismo di crittografia di tipo Transport Layer Security (SSL/TLS). Questa tecnica aumenta il livello di protezione contro attacchi tipo "**man in the middle (MITM)**".

Digitate username e password solo se state utilizzando una connessione sicura

Giorgio Sbaraglia ©–2017

Un minaccia: reti Wi-Fi “free”

Pineapple Mark V

Pineapple Mark V è un dispositivo prodotto da Hak5, acquistabile per 99,99 $. Dotato di due schede di rete Wifi e semplici tools: Kali Linux e Wireshark (per catturare i pacchetti di dati), permette all’hacker di creare un **fake access point** (“free” e malevolo!). Si possono eseguire attacchi tipo **Man In the Middle** (MITM) in modalità Wifi ed eseguire phishing e furto di credenziali.

Le vittime sono gli utenti che si collegano alla rete Wifi creata da Pineapple ed i cui dati vengono “sniffati”.

Giorgio Sbaraglia ©–2017

Un minaccia: reti Wi-Fi “free”

Giorgio Sbaraglia ©–2017

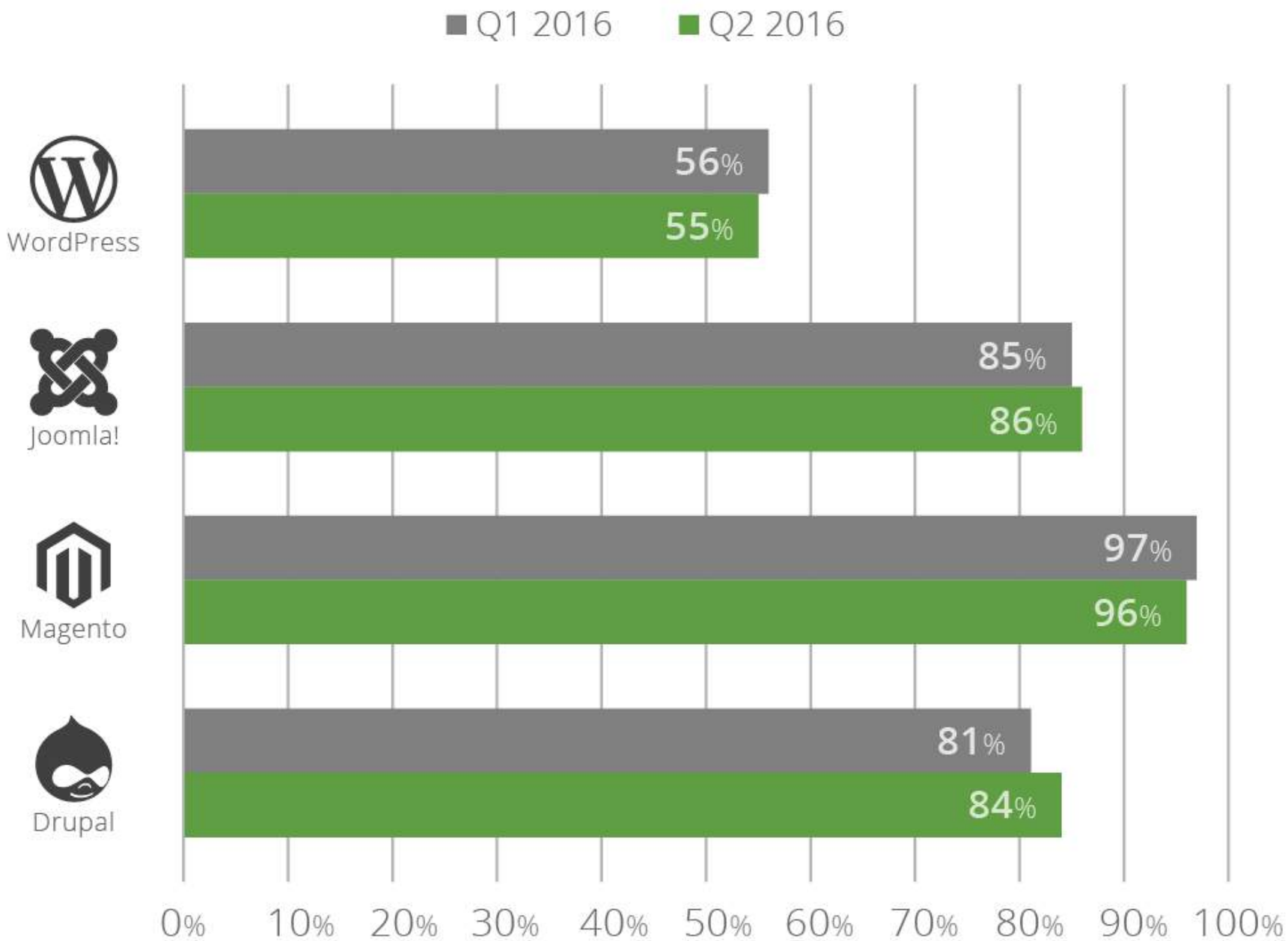
La vulnerabilità dei siti web: i rischi dei CMS

Hacked Website Report for 2016/Q2 di SUCURI

ha analizzato circa 21.821 siti web di cui: WordPress (78%), Joomla! (14%), Magento (5%), e Drupal (2%).

I risultati della ricerca hanno riscontrato che **circa il 55% delle installazioni WordPress erano non aggiornate**, ancora più alta per siti basati su altri CMS quali Joomla! (86%), Drupal (84%), e Magento (96%).

Hacked Website Report for 2016/Q2 di SUCURI



Giorgio Sbaraglia ©–2017

Hacked Website Report for 2016/Q2 di SUCURI

WordPress continua a guidare la graduatoria dei siti web infetti (al 74%), e i primi tre **plug-in** sfruttati dagli hacker continuano ad essere GravityForms, TimThumb, e RevSlider.

Sucuri hanno riscontrato su circa tre siti compromessi su quatto la presenza di una backdoor utilizzata dagli attaccanti per mantenere il controllo del sito.

MANTENERE SEMPRE I PLUG-IN AGGIORNATI

Giorgio Sbaraglia ©–2017

Agenda

1. Come si è evoluto il Cybercrime
2. Il Rapporto CLUSIT 2017
3. DeepWeb, Dark Web, rete TOR e Bitcoin
4. Le principali tecniche di attacco
5. **I Ransomware**
6. Il Social Engineering
7. I Malware su devices mobili
8. Come possiamo difenderci

Giorgio Sbaraglia ©–2017

I RANSOMWARE

- Categoria: **Trojan horse crittografico.**
- Scopo: **ESTORSIONE.**
- 85% delle vittime di ransomware risiede in Europa o negli Stati Uniti (fonte McAfee).
- **L'Italia è protagonista: subisce circa il 7% degli attacchi effettuati nel mondo** con aumento nel 2016 del 120% rispetto al 2015.
- **L'Italia è il secondo paese** più colpito nel mondo (dopo USA).
- Nel 2016, su 62 famiglie di crypto ransomware scoperte, 47 sono state sviluppate da cybercriminali russi (pari al 75%).
- I più recenti oltre a criptare i file, **fanno Upload** (per rivenderli).

Giorgio Sbaraglia ©–2017

I RANSOMWARE

- Le campagne di spam per la diffusione di Ransomware riescono ad aggirare i sistemi antispam con una efficacia di circa il 20%.
- Il 93% di chi subisce attacchi ha accusato downtime e/o perdita di dati.
- Il numero di utenti che effettivamente cade vittima del ransomware è di circa il 3% del totale.
- Riscatto richiesto: da poche centinaia di euro, fino a diverse migliaia.
- Nell'81% dei casi il riscatto non supera i 1.000 €.
- Riscatto in Bitcoin (o altra criptovaluta).
- Meno di un incidente su 4 viene denunciato alle autorità.

Giorgio Sbaraglia ©–2017

RANSOMWARE: un po’ di storia

- **Cryptolocker**: 2013.
- **CryptoWall**: inizio 2014.
- **CTB-Locker**: metà 2014. Ha migliaia di varianti.
- **TorrentLocker**: febbraio 2014 (Turkcell).
- **Ransom32**: fine dicembre 2015.
- **TeslaCrypt**: febbraio 2015. A maggio 2016 gli autori hanno rilasciato la chiave Master Key ed hanno chiuso il progetto.
- **Locky**: febbraio 2016 (via macro in file Word).
- **CryptXXX**: inizio 2016 (attraverso **pagine Web** compromesse)
- **Petya**: marzo 2016.
- **Cerber**: marzo 2016.
- **PokemonGo**: agosto 2016.
- **Popcorn**: fine 2016 (dilemma: pagare o diffonderlo?).
- **DMA-Locker, CryptoShade, CrySis, PCLock,**…..?

Giorgio Sbaraglia ©–2017

RANSOMWARE: i vettori d'infezione

I vettori d'infezione utilizzati dai ransomware sono sostanzialmente i medesimi usati per gli altri tipi di attacchi malware:

1. **Email di phishing**: il più diffuso, oltre il 75% degli attacchi è portato con messaggi di posta elettronica.
2. Navigazione su siti compromessi: il cosiddetto "**drive-by download**" da siti nei quali sono stati introdotti exploit kit che sfruttano vulnerabilità dei browser, di Flash Player o altri.
3. All'interno (in bundle) di **altri software** che vengono scaricati: per esempio programmi gratuiti che ci promettono di "crackare" software costosi per utilizzarli senza pagare.
4. Attacchi attraverso **desktop remoto (RDP)**: attacchi con furto di credenziali per accedere ai server e prenderne il controllo. Sono i più gravi (es. LOKMANN.KEY993).

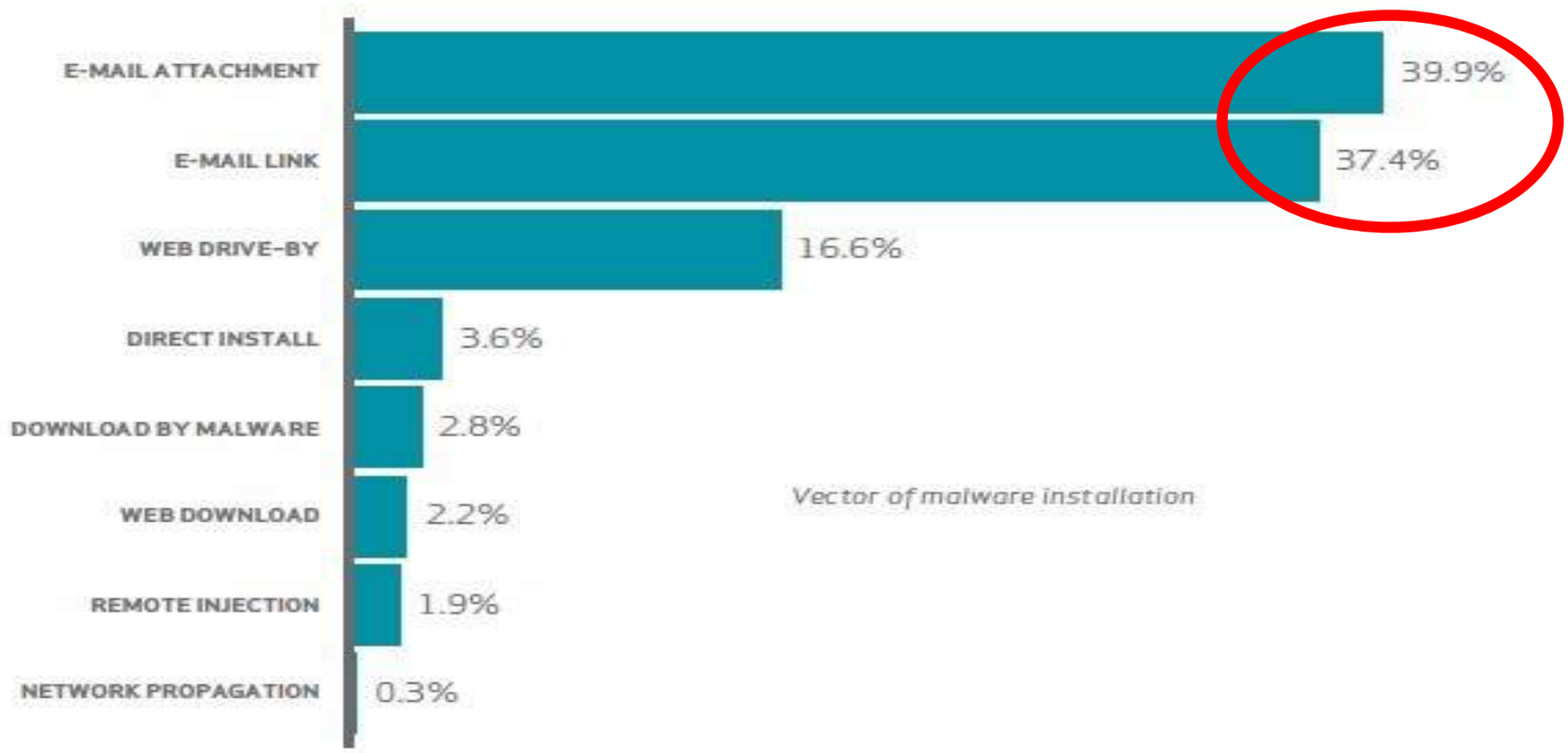
Giorgio Sbaraglia ©–2017

RANSOMWARE: i vettori d'infezione

La gran parte delle vittime sono aziende manifatturiere, pubbliche o attività professionali. Oltre il 75% dei vettori di attacco è legato ai **messaggi di posta elettronica**.

E oltre il 90% di tutte le email di phishing sono finalizzate al **RANSOMWARE.**

(fonte: Verizon Data Breach Report 2015)



Giorgio Sbaraglia ©–2017

E-mail “maligne”

Giorgio Sbaraglia il pacchetto non consegnata per voi
SDA Express Courier per: Giorgio Sbaraglia 25/06/2015 22.12

Giorgio Sbaraglia

Il vostro pacchetto con il codice di spedizione **73255793** è arrivato al **24 giugno 2015**. Corriere non ha espresso un pacco per te. Stampare l'etichetta di spedizione e mostrarlo in ufficio postale più vicino per ottenere il pacchetto.

Scarica etichetta di spedizione

Se il pacco non viene ricevuto entro 30 giorni lavorativi Sda Express ha il diritto di chiedere un risarcimento da voi per esso sta tenendo nella quantità di 7,45 EUR per ogni giorno di conservazione. È possibile trovare le informazioni sulla procedura e le condizioni di pacchi tenendo l'ufficio più vicino.

Tutela della Privacy

Decreto Legislativo 30 giugno 2003, n. 196 Art. 7 (Diritto di accesso ai dati personali ed altri diritti) 1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile. 2. L'interessato ha diritto di ottenere l'indicazione: a) dell'origine dei dati personali; b) delle finalità e modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2; e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati. 3. L'interessato ha diritto di ottenere: a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato. .Clicca qui per cancellarti.

Enel
L'ENERGIA CHE TI ASCOLTA.

ENEL SERVIZIO ELETTRICO - Servizio di Maggior Tutela
DATI CLIENTE
Numero cliente: 15 966 436
Codice Fiscale: ABXZJ4193XW

Giorgio Sbaraglia

BOLLETTA PER LA FORNITURA DI **ENERGIA ELETTRICA**
N. fattura 13354714 del 1/02/2016 Bimestre dicembre - gennaio 2015-2016
Totale da pagare entro il 28/02/2016: euro **463,99**

Come da lei richiesto, sar`a addebitato nel giorno esatto della scadenza su conto corrente presso: 50271448072
Clicca qui per scaricare

DATI FORNITURA | RIEPILOGO IMPORTI FATTURATID

Politica sulla privacy

Enel adotta un sistema di corporate governance ispirato ai pi`u elevati standard di trasparenza e correttezza nella gestione dell'impresa. Tale sistema di governo societario `e conforme a quanto previsto dalla legge e dalla normativa CONSOB di riferimento risulta altres`i allineato tanto alle raccomandazioni del Codice di Autodisciplina delle societ`a quotate - cui Enel SpA ha aderito sin dal 2000 - quanto alle best practice internazionali. Il sistema di governo societario adottato da Enel, oltre a costituire uno strumento essenziale per assicurare l'efficace gestione e il valido controllo delle attivit`a in ambito aziendale, `e orientato: alla creazione di valore per gli azionisti; alla qualit`a del servizio ai clienti; al controllo dei rischi d'impresa; alla trasparenza nei confronti del mercato; al contemperamento degli interessi di tutte le componenti dell'azionariato, con particolare attenzione ai piccoli azionisti; alla consapevolezza della rilevanza sociale dell'attivit`a in cui Enel `e impegnata e della conseguente necessit`a di considerare adeguatamente, nel relativo svolgimento, tutti gli interessi coinvolti. Le strutture di governance preposte al perseguimento di tali obiettivi sono principalmente l'assemblea degli azionisti, il consiglio di amministrazione ed i comitati con funzioni consultive o propositive costituiti al suo interno, il presidente e l'amministratore delegato, il collegio sindacale di Enel S.p.A.

clicca qui per cancellare l'iscrizione (ususcribe)

Giorgio Sbaraglia ©–2017

RISULTATO → CRYPTOLOCKER !

I tuoi dati personali sono criptati da CTB-Locker.

I tuoi documenti, foto, dati e altri file importanti sono stati criptati con la crittografia forte e chiave univoca, generati per questo computer.

Chiave privata di decodifica e' memorizzata su un server segreto e nessuno puo' decifrare i file fino a quando si paga per ottenere la chiave privata.

Se viene visualizzata la finestra principale di Loker, segui le istruzioni sul loker. Se non visualizzate nulla, sembra che voi o il vostro antivirus abbiate eliminato il programma loker. Ora avete l'ultima possibilita' di decifrare i file.

Apri http://w7yue5dc5amppggs.onion.cab o http://w7yue5dc5amppggs.tor2web.org nel tuo browser. Sono porte pubbli[illegible]

Se hai problemi con porte, utilizza la connessione diretta:

1. Scaricare Tor Browser dalla http://torproject.org/

2. Nel Browser To[illegible] http://w7yue5dc5amppggs.onion/.
Si noti che questo server e' disponibile solo tramite Tor Browser. Riprova tra 1 ora se il sito non è raggiungibile.

Scrivi nella seguente ch[illegible] di stampa.

6TUDYDU-DR7GXGQ-J2FQ6HT-E27RRKQ-ER3X2ZL-24DOZDT-PYS5T43-GU4HAHN
2EW2CR6-CRHN6Y5-5EWSD5K-QJNQAF2-7VHJ6BE-HHF42VK-7LZJXBN-PAMMHDW
YW5PVJX-UOPOYVC-DV2SUYC-H3OOXL4-3GQUKAE-T3SLFI3-H3RMGEF-RJSKNED

Segui le istruzioni sul server.

Queste istruzioni sono anche salvate in file con nome DecryptAllFiles.txt nella cartella Documenti. E' possibile aprire e utilizzare copia-incolla per l'indirizzo e la chiave.

CryptoLocker

non è un malware,

è un DISASTRO

Giorgio Sbaraglia ©–2017

POPCORN:
pagare o infettare qualcun altro?

Warning Message!!

We are sorry to say that your computer and **your files have been encrypted**,
but wait, don't worry. There is a way that you can restore your computer and all of your files

0 years, 6 days, 00 hours, 45 min and 58 sec

Time remain when your files will lost forever!

Your personal unique ID: **0e72bfe849c71dec4a867fe60c78ffa5**

Please send at least **1.0 Bitcoin** to address **1LEiPgvh6S9VEXWV2dZTytSRd7e9B1bWt3**

Click to check your Balance

Restoring your files - The fast and easy way

To get your files fast, please transfer **1.0 Bitcoin** to our wallet address **1LEiPgvh6S9VEXWV2dZTytSRd7e9B1bWt3**. When we will get the money, we will immediately give you your private decryption key. Payment should be confirmed in about 2 hours after payment made.

Restoring your files - The nasty way

Send the link below to other people, if two or more people will install this file and pay, we will decrypt your files for free.

https://3hnuhydu4pd247qb.onion.to/r/0e72bfe849c71dec4a867fe60c78ffa5

What we did?

We had encrypted all of your important images, documents, videos and all other files on your computer. We used a very strong encryption algorithm that used by all governments all over the world (Encryption -Wikipedia). We store your personal decryption code to your files on our servers and we are the only ones that can decrypt your files. Please don't try to be smart, anything other than payment will cause damage to your files and the files will be lost forever!!!

If you will not pay for the next 7 days, the decryption key will be deleted and your files will be lost forever.

Why we do that?

We are a group of computer science students from Syria, as you probably know Syria is having bad time for the last 5 years. Since 2011 we have more the half million people died and over 5 million refugees. Each part of our team has lost a dear member from his family. **I personally have lost both my parents and my little sister in 2015.** The sad part of this war is that all the parts keep fighting but eventually we the poor and simple people suffer and watching our family and friends die each day. The world remained silent and no one helping us so we decided to take an action. (Syria War in Wikipedia)

Be perfectly sure that all the money that we get goes to food, medicine, shelter to our people. We are extremely sorry that we forcing you to pay but that's the only way that we can keep living.

CC BY NC ND Giorgio Sbaraglia ©–2017

RANSOMWARE: come attacca

L'utente riceve email (Phishing) con un allegato o un link

Antispam non la blocca

Allegato contiene un file eseguibile (exe, com, scr, js, vbs) o un file (.doc, .xls, ecc.) contenente una macro

Utente clicca su link o allegato ed attiva il TROJAN

Antivirus NON blocca l'eseguibile

L'agent trojan ("dropper") si collega ad un server C&C, invia info, poi scarica il malware e la chiave pubblica di criptazione

Il malware agisce:

- chiude i processi di sistema importanti
- elimina tutti i punti di ripristino del sistema
- cancella le "shadow copies" di Windows
- cripta i file Office, pdf, cad, db, img, audio, video
- fa questo sull'HD e sui dischi collegati in rete

Compare un messaggio con la RICHIESTA DI RISCATTO in Bitcoin (BTC) e le istruzioni per pagarlo

Giorgio Sbaraglia ©–2017

RANSOMWARE: come difendersi

1) Non aprire mai gli **allegati** di email di dubbia provenienza.
2) Fare attenzione alle email provenienti **anche da indirizzi noti** (potrebbero essere stati **hackerati**!).
3) Abilitare l'opzione "**Mostra estensioni nomi file**" nelle impostazioni di Windows.
4) Disabilitare la **riproduzione automatica ("autorun")** di chiavette USB, CD/DVD e altri supporti esterni.
5) Disabilitare **l'esecuzione di macro** da parte di componenti Office (Word, Excel, PowerPoint ecc…).
6) Non aprire link provenienti da WhatsApp o Facebook, se non si è certi del mittente (vedi "Social Engineering").
7) Attenzione a cliccare su **banner** in **siti non sicuri**.
8) **Backup frequente** dei dati (vedere "Backup strategy").
9) Programmi **Antimalware** (antivirus) sempre aggiornati.
10) Utilizzare **password** univoche e complesse.

Giorgio Sbaraglia ©–2017

RANSOMWARE: come difendersi

11) Disabilitare Adobe Flash, Javascript (o comunque tenerli aggiornati, per evitare attacchi “drive-by download”).
12) Aggiornare sempre i browser (e anche le “estensioni”).
13) Evitare il **jailbreak** di dispositivi iOS e il **rooting** di quelli Android.

E PER LE AZIENDE:

14) Formare il personale, non sottovalutare fattore umano.
15) Utilizzare account senza diritti da amministratore, oppure usarli per lo stretto necessario.
16) Installare servizi **Antispam** efficaci ed evoluti.
17) Network Access Control (**NAC**): creare reti aziendali “**Guest**” per ospiti, visitatori.
18) Implementare soluzioni di tipo “**User Behavior Analytics**" (UBA) sulla rete aziendale *(analisi anomalie traffico web)*.
19) Implementare sistemi di **Sandboxing**.

BY NC ND Giorgio Sbaraglia ©–2017

Ho preso un Ransomware: cosa faccio ora?

Le opzioni sono quattro:

1. **Ripristinare i file da un backup** (la soluzione migliore).
2. **Cercare un "decryptor"** in rete per decriptare i file (funziona solo in alcuni casi).
3. **Non fare nulla** e perdere i propri dati.
4. **Pagare il Riscatto** ("Ransom").

CC BY NC ND Giorgio Sbaraglia ©–2017

1) Ripristinare i file da un backup

1. Individuare QUALE È la macchina colpita (il cosiddetto “paziente zero”).
2. Procedere ad una BONIFICA della macchina (o delle macchine) infettate.
3. **Ripristinare i file da un backup** (che sia disponibile, recente e funzionante).
4. In mancanza di un backup, si può tentare recupero dal Cloud o dalle Shadow Copies di Windows (se il malware non le ha cancellate).

Giorgio Sbaraglia ©–2017

2) Cercare un “decryptor” in rete

1. Individuare il tipo di ransomware che ha colpito: in genere l’attaccante ce lo comunica (assieme alla richiesta di riscatto).
2. Tentare una ricerca in rete per cercare il decryptor relativo al ransomware specifico.
3. Questa opzione ha **basse probabilità di successo** (praticamente nessuna se la cifratura è stata fatta con algoritmi di crittografia forte come AES 256, Salsa20 o altri), ma può valere comunque la pena di provare.

Giorgio Sbaraglia ©–2017

3) Non fare nulla e perdere i dati.

1. Togliere comunque dalla macchina il disco con i file compromessi e metterlo da parte: potrebbe succedere che in futuro qualcuno riesca a trovare il decryptor per decifrare quei nostri file, che potrebbero essere recuperati. Potrebbero passare mesi, ma potrebbe accadere…
2. Oppure (per lo stesso motivo) fare un backup dei file crittografati e poi bonificare comunque la macchina.

Giorgio Sbaraglia ©–2017

4) Pagare il Riscatto ("Ransom")

1. Leggere le istruzioni che ci sono state inviate con la richiesta di riscatto.
2. Individuare un sito che faccia "exchange" di Bitcoin, aprire un account ed acquistare i Bitcoin per il pagamento.
3. installare un browser TOR.
4. Con TOR accedere al sito indicato dagli hacker (nel Dark Web!).
5. Pagare il riscatto.
6. Aspettare e sperare…

Giorgio Sbaraglia ©–2017

Implicazione giuridiche per le vittime dei Ransomware

È lecito per la vittima pagare il riscatto?

Sì: in presenza di una condotta estorsiva il soggetto passivo si configura quale vittima.

Inoltre l'estorsione non pregiudica la vita o l'incolumità di una persona fisica, bensì di un proprio bene.

Unico caso in cui è perseguibile: sequestro di persona per scopo d'estorsione, ex art. 1, legge 15 marzo 1991 n. 82 in forza del quale può essere disposto il sequestro dei beni appartenenti al soggetto sequestrato e ai familiari.

Giorgio Sbaraglia ©–2017

Implicazione giuridiche per le vittime dei Ransomware

SE CHI PAGA È L'AZIENDA

D.Lgs. 231/2001 "Responsabilità amministrativa delle società e degli enti": qualora i reati siano commessi nell'interesse o a vantaggio di questi, ci sono altri aspetti da valutare:

- **Reati Societari** (se la cifra per il riscatto è stata accantonata tramite false comunicazioni sociali, impedito controllo, ostacolo all'esercizio delle funzioni delle autorità di vigilanza).
- **Autoriciclaggio** se il pagamento proviene da illecito illecito (es. reato di evasione fiscale).
- **Finanziamento della criminalità organizzata** (il riscatto va chiaramente a finanziare la criminalità organizzata).

Giorgio Sbaraglia ©–2017

Agenda

1. Come si è evoluto il Cybercrime
2. Il Rapporto CLUSIT 2017
3. DeepWeb, Dark Web, rete TOR e Bitcoin
4. Le principali tecniche di attacco
5. I Ransomware
6. **Il Social Engineering**
7. I Malware su devices mobili
8. Come possiamo difenderci

CC BY NC ND Giorgio Sbaraglia ©–2017

La vignetta di Peter Steiner (1993)

Nel 1993 il famoso disegnatore **Peter Steiner** pubblicò sulle pagine del **"New Yorker"** questa vignetta.

Inizialmente non ebbe molta attenzione, ma nel corso degli anni successivi è diventata popolarissima.

"Su Internet non tutto è quello che sembra"

... pensare che è stata realizzata nel 1993, quando il Web era appena nato.

Giorgio Sbaraglia ©–2017

Il SOCIAL ENGINEERING

Cos'è il social engineering? *(human hacking)*

Semplicemente *(cit. Paolo Attivissimo)*:

“FREGARE IL PROSSIMO CON LA PSICOLOGIA”

Scopo degli aggressori è indurre l'utente a fidarsi del *contenuto* del messaggio che mandano e quindi eseguirne i comandi.

Il social engineering è fatto apposta per aggirare Antivirus, Firewall, ecc.: quando il sistema non ha bugs da sfruttare, **si punta sulle debolezze e sulla curiosità delle persone.**

Per evitare truffe di questo tipo, che sono diffusissime: non fidarsi mai dei link contenuti all'interno dei messaggi, perché possono essere falsificati in mille modi.

Giorgio Sbaraglia ©–2017

Il SOCIAL ENGINEERING

Il social engineering fa leva sulle "vulnerabilità" umane:

- ☑ Autorevolezza
- ☑ Colpa
- ☑ Panico
- ☑ Ignoranza
- ☑ Desiderio
- ☑ Avidità
- ☑ Compassione e buoni sentimenti

Giorgio Sbaraglia ©–2017

Phishing, Spear Phishing e Watering Hole

PHISHING: *"pesca a strascico"* mediante email. Il 93% delle email contiene Ransomware e circa il 10% di queste riesce nell'intento di ingannare l'utente.

SPEAR PHISHING: l'oggetto dell'attacco viene accuratamente selezionato. Gli attaccanti acquisiscono una profonda conoscenza delle vittime e le email inviate sono preparate ad hoc per catturarne l'attenzione ed indurle in errore.

WATERING HOLE: *"l'abbeveratoio"*. I criminali infettano i siti più visitati dalle potenziali vittime. In questo caso muta lo scenario poiché è la vittima ad andare nel sito infetto e non l'attaccante a sollecitarne la visita attraverso una email. Sono gli attacchi (*drive-by download*) più subdoli e difficili da individuare.

Giorgio Sbaraglia ©–2017

La vera storia di “The Man in the Mail”

Nota anche come **BEC: Business Email Compromise**), è una delle truffe basate sul phishing più efficaci e paradossalmente più semplici. I delinquenti intercettano la posta elettronica di un'azienda e dirottano i bonifici sui propri conto correnti. Colpisce soprattutto aziende di import/export.

COME FUNZIONA?

1. Il ladro viola la casella di posta (quella del mittente oppure quella del destinatario) mediante: phishing, social engineering, furto delle credenziali o attacco “brute force”, keylogger.
2. Studia le comunicazioni dell’azienda, la carta intestata, le firme dei responsabili, lo stile della corrispondenza.
3. Poi si inserisce in conversazioni già in corso comunicando coordinate bancarie diverse (le sue!) su cui eseguire i pagamenti. Per fare questo usa lo “**spoofing**” (imbrogliare), usando un indirizzo email appena diverso, oppure accede direttamente all’email violata.

Giorgio Sbaraglia ©–2017

Proteggersi da “The Man in the Mail”

- Usare credenziali di accesso alle mail robuste e sicure.
- Impostare una corretta gestione delle password.
- Non utilizzare in azienda indirizzi email gratuiti basati su webmail.
- Controllare periodicamente se sul proprio account di posta sono impostate regole di inoltro della posta verso un altro indirizzo.
- Leggere le mail con attenzione, soprattutto quelle che si riferiscono a pagamenti. Nel dubbio fare verifiche con mezzi diversi (per es. il telefono, oppure un’altra email).
- Controllare bene il mittente delle email: un dettaglio (anche solo una lettera!) potrebbe fare la differenza.
- Usare un sistema di CIFRATURA ed AUTENTICAZIONE delle email (The GnuPG, Enigmail, GPGTools, Gpg4Win, iPGMail).
- E soprattutto: **Evitare di pensare "*figurati se una cosa del genere può succedere a me*”.**

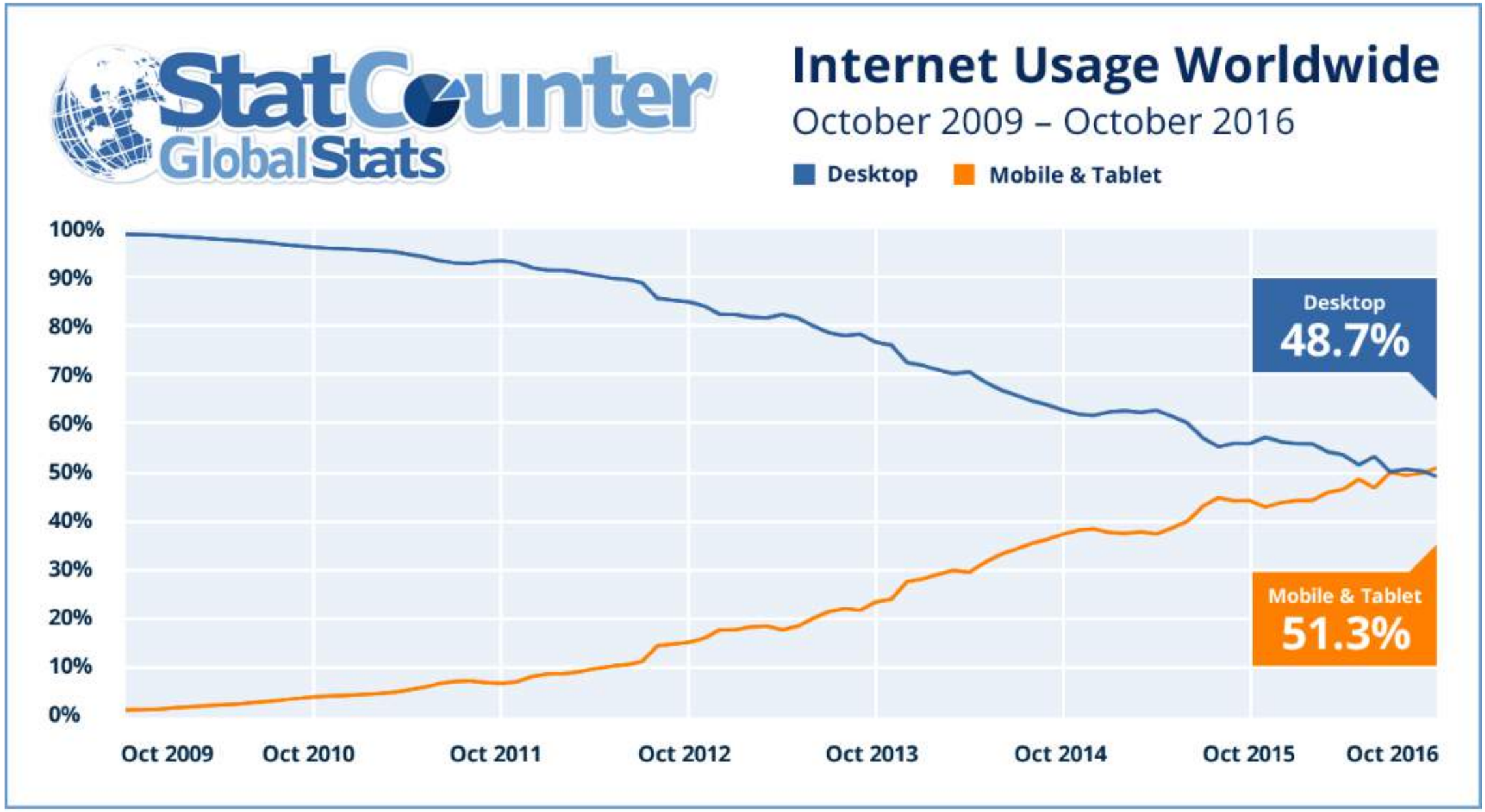
CC BY NC ND Giorgio Sbaraglia ©–2017

Agenda

1. Come si è evoluto il Cybercrime
2. Il Rapporto CLUSIT 2017
3. DeepWeb, Dark Web, rete TOR e Bitcoin
4. Le principali tecniche di attacco
5. I Ransomware
6. Il Social Engineering
7. **I Malware su devices mobili**
8. Come possiamo difenderci

Giorgio Sbaraglia ©–2017

2016: il sorpasso del Mobile sul fisso



Ad Ottobre 2016 il traffico Internet da **Mobile** ha superato - per la prima volta - quello da fisso. Questo è vero soprattutto nei paesi meno sviluppati, non lo è (ancora) in Europa ed in USA.

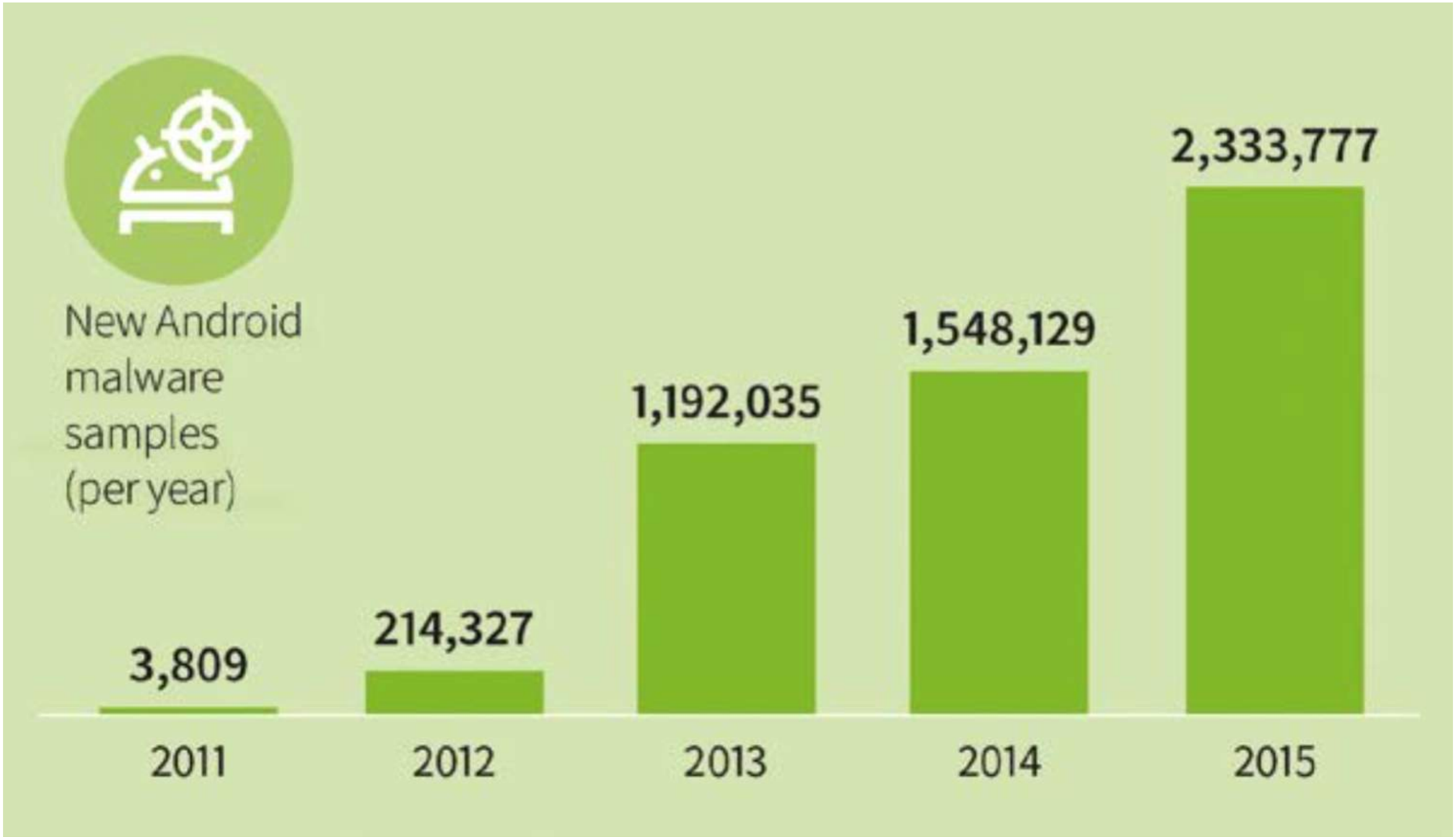
Giorgio Sbaraglia ©–2017

Principali Malware su devices mobili

Malware	Chi colpisce	Come attacca	Come difendersi
Stagefright	95% dei dispositivi **Android** sono vulnerabili	Invio messaggio multimediale (MMS) contenente un particolare set di istruzioni	Google ha rilasciato patch. Disattivare la ricezione di MMS (anche su APN)
DressCode	Presente in 3.000 apps **Android**	Il Trojan nelle app richiama server di c/c e usa il device come “bot” per infiltrarsi nelle reti aziendali	Scaricare app solo da siti sicuri. Aggiornare OS. Evitare il Rooting.
KeyRaider	**iOS** (solo jailbroken)	Attraverso Apps da repository cinesi di Cydia. Ruba AppleID	Non fare jailbreak
XcodeGhost	**iOS** (jailbroken e non-jailbroken)	Scaricando Apps infette con XcodeGost (da Cina)	Le Apps infette sono state rimosse da AppStore

Giorgio Sbaraglia ©–2017

Malware su devices Android



Fonte: G DATA Security Labs: numero di nuovi ceppi di malware registrati anno su anno.

Giorgio Sbaraglia ©–2017

Un malware che attacca WhatsApp e Telegram

Questa vulnerabilità è stata scoperta l'8 marzo 2017.

L'attacco viene fatto attraverso un'immagine o un filmato inviato via WhatsApp e Telegram.

Aprendo l'immagine si viene reindirizzati ad una pagina HTML contenente malware che accedono ai messaggi, alle foto, ecc. e che potrebbero inviare messaggi per conto dell'utente.

Il bug dovrebbe essere stato già risolto da WhatsApp e Telegram.

Occorre AGGIORNARE le App.

Giorgio Sbaraglia ©–2017

Gli SPYWARE su smartphone

Per il cybercrime è più utile spiare il dispositivo piuttosto che rubarlo.

SPYWARE: è un'applicazione di monitoraggio (spionaggio!) che viene installata su uno smartphone all'insaputa del proprietario.

Può essere installata:

1) con **accesso diretto al dispositivo.**

2) **da remoto:** le tecniche per riuscire ad installare l'app (con tutti i permessi necessari) passano ancora una volta attraverso il **phishing**, il **social engineering** e la **navigazione Web**. Spesso viene usato lo **spoofing** per scrivere a nome di un amico, collega, che consiglia l'utilizzo una "stupenda" app. Analogamente a come avviene per i Ransomware si spinge la vittima ad installare un'app.

Giorgio Sbaraglia ©–2017

Gli SPYWARE su smartphone

Tramite la connettività lo spyware invia all'esterno una serie di informazioni:

- Rubrica telefonica e email
- SMS ricevuti
- Contenuto della casella di posta
- Storico delle chat (es. WhatsApp)
- Registrazioni audio
- Registrazioni video
- Immagini da fotocamera
- Tutto ciò che viene digitato
- Ogni file presente in memoria

Giorgio Sbaraglia ©–2017

Gli SPYWARE su smartphone

Inoltre lo spyware può prendere il controllo ed avviare funzioni (all'insaputa dell'utente) quali:

- telefonate
- SMS
- chat
- email

La violazione di uno smartphone oggi può essere potenzialmente più grave e pericolosa di quella di un PC

Giorgio Sbaraglia ©–2017

Agenda

1. Come si è evoluto il Cybercrime
2. Il Rapporto CLUSIT 2017
3. DeepWeb, Dark Web, rete TOR e Bitcoin
4. Le principali tecniche di attacco
5. I Ransomware
6. Il Social Engineering
7. I Malware su devices mobili
8. **Come possiamo difenderci**

Giorgio Sbaraglia ©–2017

Acquisire Consapevolezza

"La <u>piccola</u> azienda non ha bisogno di una <u>piccola</u> sicurezza, ma dello stesso livello di sicurezza della grande azienda"

(cit. Alessio Pennasilico, membro comitato direttivo CLUSIT)

Gli strumenti informatici e tecnologici per proteggersi adeguatamente ESISTONO. Quello che manca è:

- **la CONSAPEVOLEZZA dell'esistenza del problema,**
- **poi la capacità di scegliere correttamente le persone e gli strumenti per risolvere il problema.**

Giorgio Sbaraglia ©–2017

Ridurre i rischi di “Data Breach”

- ☑ Trasformare l’**utente** da anello debole a prima linea di difesa.
- ☑ Applicare il principio del **minimo privilegio** per quanto riguarda l’accesso ai dati.
- ☑ Adottare politiche di **patching** dei sistemi.
- ☑ Predisporre un corretto **Disaster Recovery Plan** (DRP)
- ☑ **Crittografare** i dati sensibili.
- ☑ Utilizzare **l’autenticazione a due fattori.**
- ☑ Attenzione anche alla sicurezza fisica: **outsourcing.**

“Principle of Least Privilege” (POLP)

Jerome Saltzer definiva così quello che in inglese viene chiamato “**Principle of Least Privilege**” (POLP):

“Ogni programma ed ogni utente del sistema dovrebbero operare utilizzando il **più basso livello di “diritti”** necessari a portare a termine il proprio compito”.

In altre parole:

- ☑ **Limitare i privilegi degli utenti.**
- ☑ **Limitare il numero e l’utilizzo di account privilegiati.**
- ☑ **Evitare di esporre credenziali privilegiate su sistemi meno privilegiati e potenzialmente compromessi.**

Giorgio Sbaraglia ©–2017

Verizon Data Breach Investigations Report 2016

- Le **password deboli** sono la causa del **63%** delle violazioni.
- Rispetto al 2015 crescono del 16% gli attacchi **ransomware**.
- **Email di phishing**: nel **30%** dei casi questi messaggi vengono aperti dagli utenti, in crescita rispetto all'anno precedente (23%).
- Nel **13% vengono cliccati anche gli allegati e i link** nella mail, permettendo così l'infiltrazione del malware.
- Nell'**89%** dei casi i motivi che spingono i cybercriminali sono di natura finanziaria e di spionaggio.
- L'**85%** degli attacchi sfrutta le dieci vulnerabilità più conosciute ma non ancora risolte, anche se esistono patch disponibili.

Giorgio Sbaraglia ©–2017

Giovedì … gnocchi

“Patch Tuesday, Exploit Wednesday”

Molti sfruttamenti delle falle nei vari sistemi avvengono poco dopo la pubblicazione di una patch.

Analizzando la patch medesima, gli Hackers possono capire con facilità come approfittare delle vulnerabilità evidenziate (con tecniche di “reverse engineering”) ed attaccare i sistemi che non sono stati ancora patchati.

SCARICARE SEMPRE - E SUBITO - GLI AGGIORNAMENTI DI SISTEMA

Giorgio Sbaraglia ©–2017

Security come “Gioco di Squadra”

La sicurezza informatica di un’azienda si costruisce con **molti componenti**, ciascuno in grado di dare il suo contributo:

1. Antivirus sugli endpoint (sempre aggiornati)
2. Antispam (Mail Gateway)
3. Firewall perimetrali
4. URL filtering
5. Gestione differenziata dei privilegi d’accesso
6. User Behavior Analytics (analisi comportamentale del traffico)
7. Sandboxing
8. Gestione degli aggiornamenti firmware e patching
9. Password Management
10. Backup dei dati

Nessuno di questi componenti è sufficiente - da solo - a garantirci la sicurezza, ma tutti sono necessari.

Giorgio Sbaraglia ©–2017

Le verifiche periodiche di sicurezza

Vulnerability Assessment (VA): valutazione della vulnerabilità di un sistema informatico. Si cercano di individuare le vulnerabilità del sistema, usando gli stessi strumenti degli hacker (si parla di "*ethical hacker*").

Penetration Test (Pen Test): possono essere fatti con diverse modalità:

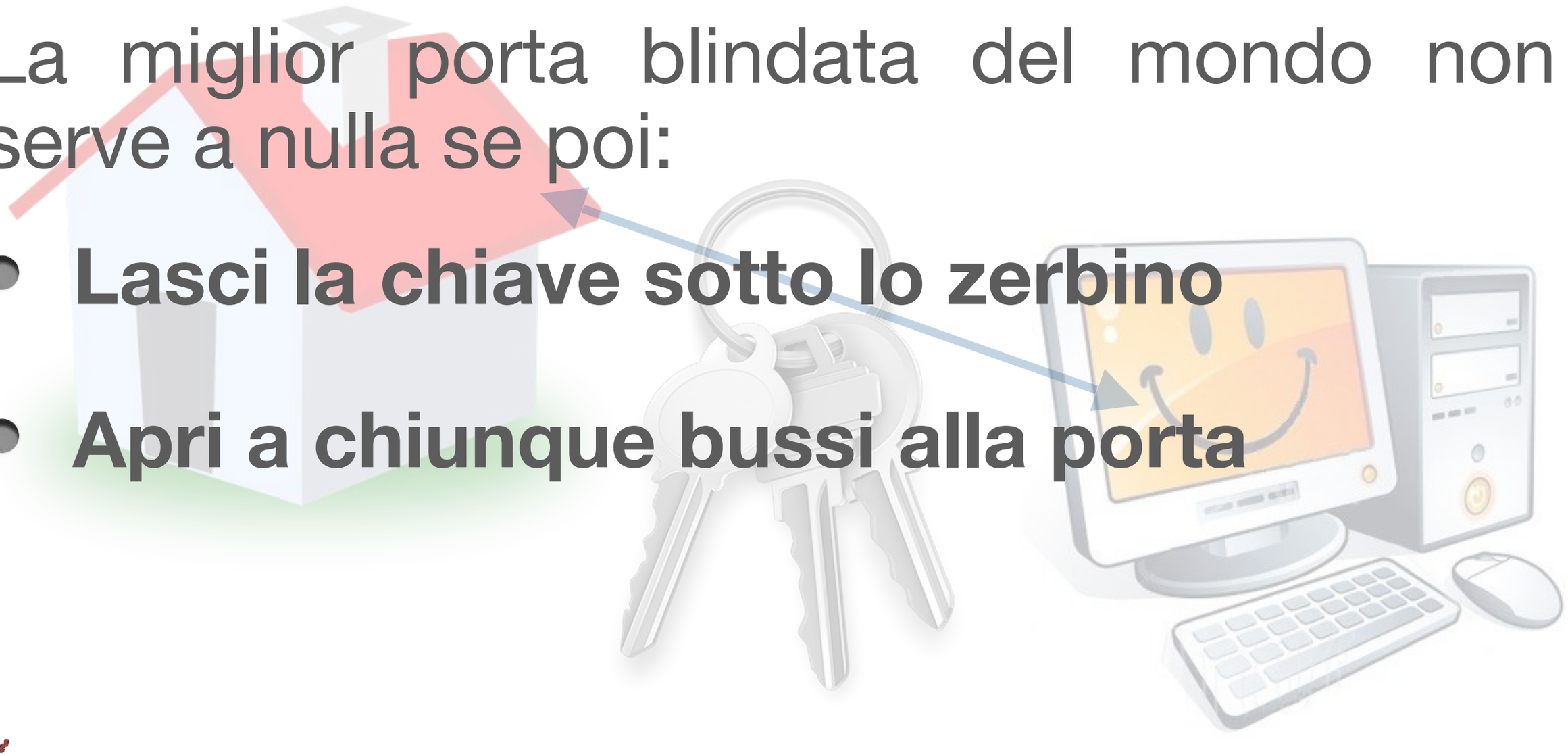
- **white box**: l'attaccante ha piena conoscenza dei sistemi (infrastruttura, account, indirizzi IP; è usata nel mondo bancario dove l'hacker può essere un utente registrato.
- **black box**: simulando un attaccante che non ha alcuna conoscenza dei sistemi.

CC BY NC ND Giorgio Sbaraglia ©–2017

In Sintesi:
Sicurezza Computer come sicurezza Casa

La miglior porta blindata del mondo non serve a nulla se poi:

- **Lasci la chiave sotto lo zerbino**
- **Apri a chiunque bussi alla porta**



Giorgio Sbaraglia ©–2017

Il succo del discorso…

In ogni cyber attacco c’è sempre almeno un ERRORE UMANO

PEBKAC: “Problem Exists Between Keybord And Chair”

Giorgio Sbaraglia ©–2017

Grazie per l'attenzione!

giorgio@giorgiosbaraglia.it

334 6712113

www.giorgiosbaraglia.it

Giorgio Sbaraglia ©–2017