Ordine dei Dottori Commercialisti e degli Esperti Contabili di Roma

Studio Sciarra

Sicurezza *Informatica*

10 Cose Da Non Fare Mai

Gli errori da evitare per mantenere i dati al sicuro

AGENDA

1. Usare password banali
2. Usare una sola password per tutto e a lungo
3. Scrivere la password, rivelarla o metterla in un file
4. Fidarsi ciecamente delle email
5. Scaricare e installare software e app senza autorizzazione
6. Rimandare gli aggiornamenti
7. Navigare pericolosamente
8. Collegare chiavette USB o dischi esterni
9. Collegarsi a reti Wi-fi “libere”
10. Perdere di vista smartphone/tablet/laptop

10 COSE DA NON FARE MAI ·CAPITOLO 1

USARE

PASSWORD

BANALI

Prima o poi, in ufficio capita di dover inserire una nuova password in uno dei servizi dei quali abbiamo un accesso. E di solito capita all'improvviso, magari perché il responsabile IT ha deciso che la password della posta va cambiata… oggi!

E così, colti alla sprovvista, nella maggior parte dei casi inseriamo il primo termine che ci viene in mente.
Se abbiamo fortuna, il software ci inviterà a usare una password più lunga, o con maiuscole e minuscole, o contenente anche dei numeri o dei caratteri speciali; ma molti servizi non ci faranno questo favore, e ci lasceranno usare una password facile da indovinare.
Gli esperti calcolano che le **mille password più comuni** (esistono sul Web liste delle password "hackerate") siano usate da circa **il 90% degli utenti** Internet.

LE CONSEGUENZE

Ma qual è il problema se qualcuno scopre la vostra password?
Beh, dipende ovviamente da quale servizio, e quali dati, la password dovrebbe proteggere. Le conseguenze possono andare da semplici fastidi a veri e propri disastri aziendali.

Ma cosa succede se un dipendente infedele usa la nostra password per creare danni all'azienda usando il nostro PC, per esempio cancellando file importanti, o alterando documenti fiscali, o ancora trafugando progetti per venderli alla concorrenza?

Beh, queste operazioni risulteranno eseguite da voi, e la responsabilità (anche legale) sarà vostra, perché è vostro dovere custodire le vostre password.

Se poi la password scoperta è quella della posta elettronica, si apre tutto un universo di azioni dannose delle quali potrete essere incolpati: l'intruso potrebbe mandare email offensive ai vostri superiori, o usare il vostro indirizzo per inviare malware a vostro nome, o compiere azioni penalmente rilevanti – per esempio inviare materiale pedopornografico Individuare a posteriori il vero responsabile delle operazioni criminose è molto difficile, anche perché non è necessario che sia una persona che può accedere fisicamente al vostro computer: un cracker che conosce il vostro indirizzo email può provare a indovinare la password ovunque egli si trovi.

A proposito, non crediate che un cracker si metta a digitare a manina ogni singola password cercando di trovare quella giusta: di solito si usano appositi programmi capaci di provare automaticamente anche 1000 password al secondo.

E ovviamente, le prime 1000 saranno quelle dell'elenco cui si accenava prima.
Seguite da tutte le loro variazioni (con maiuscole e minuscole, con lettere sostituite da numeri…).

Quindi se usate una password comune, e un cracker decide di scoprirla, non avete difesa.

Nel migliore dei casi, se dovesse ricorrere a un cosiddetto "attacco a forza bruta", ovvero un generatore che prova in sequenza ogni password possibile e ogni permutazione, potrebbe comunque arrivare alla soluzione nel giro di pochi giorni. E se è bravo, l'uso di tecniche sofisticate gli permetterà di abbreviare di parecchio questi tempi.

LE 25 PASSWORD PIÙ USATE NEGLI USA - anno 2015

1. 123456	1. 123456789	11. welcome	16. dragon	21. princess
2. password	7. football	12. 1234567890	17. master	22. qwertyuiop
3. 12345678	8. 1234	13. abc123	18. monkey	23. solo
4. qwerty	9. 1234567	14. 111111	19. letmein	24. passw0rd
5. 12345	10. baseball	15. 1qaz2wsx	20. login	25. starwars

COSA FARE

Come difendersi dunque?

La cosa più importante è assicurarsi che la password che scegliete sia così inusuale da non essere mai entrata in un dizionario. Ovviamente, non c'è sostituzione che tenga: scrivere F1do o Fid0 al posto di Fido non vi salverà. Usare una parola molto lunga nemmeno. Fuori discussione usare nomi propri (del coniuge o dei figli), titoli di film, artisti famosi, squadre di calcio. Bisogna cercare approcci diversi. Il più efficace è ricorrere a un generatore automatico di password, che crea sequenze di caratteri assolutamente uniche in quanto casuali.

Poiché invariabilmente sono difficili da ricordare, di solito il generatore dispone anche di un sistema di memorizzazione per le varie password generate. A voi rimarrà il compito di sceglierne (e ricordarne) una sola: quella che attiva il generatore, appunto.

Per la scelta di quest'ultima, consigliamo un paio di possibili approcci. Il primo è di usare una serie di 4/5 parole italiane unite insieme. Non devono essere frasi o battute famose, perché potrebbero essere state inserite nei dizionari dei cracker. Devono essere termini scelti a caso, per esempio generando 4 numeri interi sul sito random.org, e poi prendendo la prima parola presente nel dizionario alle pagine indicate dai numeri casuali.

Per ricordare la password potete immaginare una scenetta che coinvolga i quattro termini.

Per esempio, se usate velivolo, montagna, ananas, bufalo, pensate a un aereo che sorvola un monte e lancia ananas che arrivati a terra vengono mangiati da un bufalo.

Il secondo approccio (meno sicuro) è di scegliere un verso da una poesia o una canzone e comporre la password usando solo alcune lettere di ogni parola (per esempio le prime tre, o l'ultima).

Al momento, gli attacchi con dizionario coprono battute e versi celebri, ma non risulta comprendano ancora sequenze di caratteri presi da versi di poesie e canzoni. Ancora meglio se si tratta di poesie o canzoni italiane, magari dialettali.

È possibile, ovviamente, utilizzare due o più tecniche in combinazione fra loro.

10 COSE DA NON FARE MAI ·CAPITOLO 2

USARE

UNA SOLA

PASSWORD

PER TUTTO

E A LUNGO

Dunque, supponiamo che voi abbiate creato una password formidabile.

Difficilissima da attaccare. E che l'abbiate custodita con ogni cura.

Eppure, un giorno, vi chiama la banca e vi chiede conferma dell'ordine che avete appena fatto sul sito di Home Banking, di svuotare il vostro conto trasferendo i soldi su una banca nigeriana.

Voi cadete dalle nuvole, poi emettete un urlo che il funzionario di banca capisce essere un "**fermate tutto**" e,

dopo aver ripreso fiato, vi chiedete: come è potuto succedere?

Cosa ho fatto di sbagliato?

COSA È SUCCESSO?

Pensateci un attimo: La vostra password inattaccabile l'avete usata solo per l'accesso all'Home Banking? O per caso avete usato quella stessa password per due servizi di email, l'account dell'App Store, quello di Google Play, per l'accesso a LinkedIn, l'abbonamento a Badoo o ad Ashley Madison, all'Adobe Creative Cloud e a Tumblr? Bene, se questo è il caso, quello che probabilmente è successo è che un cracker è riuscito a penetrare nel database degli utenti di un noto servizio online, ha rubato credenziali e password, e adesso sta provando a entrare (con le stesse credenziali) in servizi più "appetitosi".

Vi sembra difficile? Eppure, negli ultimi anni i cracker hanno rubato i dati di accesso di 160 milioni di account LinkedIn, di 150 milioni di utenti Adobe, di ben 350 milioni di account MySpace e, recentemente, di 800 milioni di account Yahoo, per citare solo alcuni dei casi più conosciuti.

Solo negli ultimi 5 anni, oltre 1,4 miliardi di account sono stati rubati dai database di decine di famosi servizi on line.

Tra l'altro, sebbene molti di questi furti di credenziali siano avvenuti già da qualche anno (tipicamente fra il 2012 e il 2014), essi sono stati scoperti solo recentemente perché i cracker hanno messo pubblicamente in vendita sul dark web le credenziali rubate, cosa che avviene di solito solo dopo che esse sono state già sfruttate dall'organizzazione criminale che ne ha estratto le informazioni più economicamente vantaggiose. Ci sono siti internet che vi consentono di verificare se i vostri dati fanno parte di quelli rubati in episodi noti di hackering.

Un esempio è www.haveibeenpwned.com: se avete il sospetto che qualcuno possa aver rubato la vostra password e siete iscritti a qualche servizio online, potrebbe essere il caso di andare sul sito e dare una controllata.

L'autenticazione a due fattori usa due controlli diversi per dare accesso a un servizio. Per esempio, un server che riceve la nostra richiesta d'ingresso può inviarci sul cellulare un codice da digitare sul PC, per garantirsi che alla tastiera ci siamo proprio noi.

Se invece la password del vostro Home Banking era usata solo per quel sito, forse un cracker vi ha presi di mira. Potrebbe aver iniziato con un attacco da dizionario, provando le due o tremila password più comuni; poi potrebbe aver fatto partire sul suo computer un attacco a forza bruta, cercando di individuare la combinazione di numeri e lettere casuali che avete usato.

Se un cracker è motivato (ovvero, ritiene di poter guadagnare parecchio accedendo al vostro account), può investire parecchio tempo e risorse di calcolo alla ricerca della vostra password.

Può per esempio mettere al lavoro una rete di computer "zombie", ovvero una cosiddetta "botnet", in cui centinaia o migliaia di macchine, messe sotto il suo controllo grazie a un malware, generano incessantemente nuove password fino a trovare quella giusta.

Con migliaia di macchine al lavoro, le password più brevi (8/10 caratteri) possono essere decifrate in pochi mesi.

COSA FARE

Di fatto, una password funziona un po' come una porta blindata: serve a dissuadere il ladro e a rallentare il suo lavoro, ma non può fermarlo per sempre.

Ma se cambiamo la password regolarmente, sarà come presentare al ladro una porta blindata nuova ogni volta che costui sarà quasi riuscito ad abbattere la precedente. Il problema è determinare la frequenza del cambio.

Cambi troppo diradati danno al cracker il tempo di decodificare la password, cambi troppo ravvicinati espongono al rischio di… dimenticarla; così si finisce per scriversela da qualche parte vanificando lo scopo (vedi prossimo capitolo).

La maggior parte delle aziende tende a proporre il cambio password in media ogni tre mesi; più frequente se il sistema informativo aziendale contiene dati particolarmente appetibili al crimine (segreti industriali, progetti, chiavi di accesso a conti bancari eccetera), meno frequente se si tratta di semplici dati contabili, gestionali, magazzino e simili.

Oltre al cambio frequente, è importante diversificare le password per i vari servizi.

Assolutamente indispensabile, poi, non utilizzare in azienda le stesse password che si usano per i propri account "personali".

Un'altra contromisura molto valida è ricorrere, dove possibile, alla "**two factor authentication**", o autenticazione a doppio livello.

Questa opzione è offerta da molti siti e servizi on line, e consiste nell'utilizzare più informazioni per determinare la vostra identità.

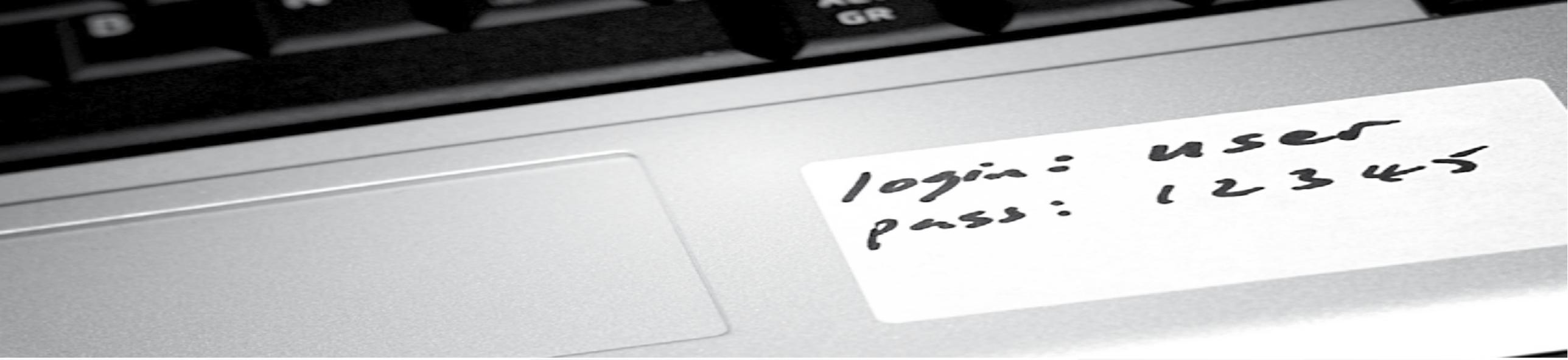
La più usata consiste nell'inviare al vostro cellulare un SMS contenente un codice, non appena chiedete di accedere a un servizio tramite login e password.

L'accesso potrà avvenire solo dopo che avrete inserito il codice appena ricevuto. In questo modo, il servizio on line saprà che siete proprio voi, a meno che il cracker non vi abbia rubato, oltre la password, anche il cellulare.

Oggi la maggior parte dei servizi on line offre l'autenticazione a due fattori come opzione, ma la maggior parte degli utenti non la usa, per disinformazione o pigrizia.

10 COSE DA NON FARE MAI · CAPITOLO 3

SCRIVERE LA PASSWORD, RIVELARLA O METTERLA IN UN FILE



Ai consulenti capita spesso di dover mettere le mani su computer aziendali e raramente hanno bisogno che l'utente del computer inserisca la password di accesso: nel 50% dei casi, è scritta su un post-it appiccicato sotto la tastiera. Altre volte il post-it con la password è nel primo cassetto della cassettiera.

E qualche volta (orrore!) è appiccicato in bella vista al bordo del monitor.

Quale sia l'utilità di una password che può essere vista da chiunque entri in un ufficio è chiaro a tutti.

COSA PUO' SUCCEDERE

In linea teorica, un ufficio dovrebbe essere frequentato solo da persone autorizzate.
Ma, soprattutto nelle grandi organizzazioni, anche queste persone possono creare dei problemi. Ricordiamoci sempre che la responsabilità delle operazioni eseguite dal vostro computer aziendale, o con il vostro account aziendale, è personale, e che una volta inserita la password il sistema informativo vi riconosce e vi attribuisce le operazioni che verranno compiute: in pratica, se un collega scontento crea danni alla società usando il vostro account, risulterà che il danno lo avete operato voi. Anche nel caso riusciste a dimostrare che non siete stati voi, dovrete rispondere della "mancata custodia", ovvero di non avere fatto tutto il possibile per evitare che qualcuno usasse il vostro account al vostro posto, e questa è già una motivazione sufficiente per non lasciare le password in bella vista o in luoghi facilmente intuibili.
Inoltre, in ufficio può sempre capitare qualche estraneo. E se in azienda avete dati particolarmente importanti, non è detto che qualcuno non provi a entrare con qualche scusa proprio per rubare le password di accesso. Un corriere, un fattorino, sedicenti tecnici del fornitore telefonico o dell'aria condizionata, addetti alle pulizie… un hacker motivato applica facilmente tecniche di questo tipo (vanno sotto il nome di "social engineering") per arrivare ad adocchiare i dati di accesso.
Naturalmente, in alcuni casi gli account e le password sono gestite in modo stretto dal reparto IT, che per esempio ne permette l'uso solo a partire da specifici computer o indirizzi IP, ma in molti casi questo non succede: un esempio tipico sono gli indirizzi email che devono essere consultabili da remoto, quindi da qualsiasi dispositivo o IP, per consentirne l'uso ai dipendenti in trasferta di lavoro.

Negli anni scorsi, hanno avuto una certa popolarità dei simpatici quadernetti, organizzati alfabeticamente come rubriche telefoniche, dove i dipendenti con memoria corta potevano trascrivere ordinatamente tutte le password di accesso ai vari servizi. Vi lasciamo immaginare le conseguenze del loro uso sulla sicurezza in azienda.

Altre tecniche di social engineering usate dagli hacker mirano a farvi rivelare le password tramite telefonate o false mail. Le telefonate funzionano più facilmente in grandi organizzazioni, dove una telefonata da uno sconosciuto che vi dice di essere il nuovo tecnico dell'IT, o il contabile di una banca che deve fare un controllo, potrebbe non sollevare immediatamente sospetti. Le mail sono più trasversali, e in molti casi non sollevano dubbi nemmeno in uffici e organizzazioni di piccole dimensioni.
Un'ultima cosa: se per ricordare le varie password le memorizzate in un file, non è che otteniate una sicurezza migliore di quella che avreste scrivendole sul post-it da attaccare sotto la tastiera. Questo perché l'accesso ai vostri file da parte di estranei non è poi un evento così improbabile. Se vi allontanate dal PC per qualche minuto, qualcuno potrebbe per esempio copiare la vostra cartella "Documenti" in una chiavetta USB e cercare poi con calma ciò che gli serve.

COSA FARE

Ribadiamo per la terza volta il consiglio già dato nei capitoli 1 e 2: l'uso di un password manager è la soluzione di gestione password più adatta a minimizzare i rischi, perché lascia un solo punto di attacco a chi volesse impadronirsi delle vostre credenziali.

Le singole password generate automaticamente dal programma sono molto robuste, e scegliendo bene la singola password di attivazione del programma, per esempio con uno dei metodi illustrati nel capitolo 1, il livello di protezione è decisamente elevato.

Da notare che nel caso di password manager integrati nel sistema, la password iniziale coincide in genere con quella di login. Al contrario, soluzioni "**fai da te**" - dai post-it ai file di password più o meno "mascherati", vanno assolutamente banditi.

E sarà meglio anche fare in modo che nessuno possa utilizzare il nostro computer in nostra assenza: niente login senza password, prima di tutto; e per i momenti in cui vi allontanate dalla scrivania, per una riunione o un caffè, ricordatevi di attivare un salvaschermo che, all'uscita, chieda nuovamente l'inserimento della password di login.

Infine, imparate a diffidare di chiunque vi chieda di rivelare le vostre password, sia che telefonino dichiarandosi tecnici neoassunti o verificatori bancari, sia che inviino mail o si presentino di persona.

Chiunque vi chieda la vostra password vi deve far squillare un campanello di allarme in testa, perché l'IT aziendale, le banche, i fornitori, conoscono già le password che servono loro per rapportarsi con voi, e non hanno bisogno che voi gliele riveliate.

Anche un tecnico che debba fare assistenza sul PC in vostra presenza non vi chiederà "mi detti la sua password", ma piuttosto "venga qui e inserisca la sua password".

A meno, ovviamente, che non l'abbia già letta sul post-it sotto la tastiera.

PROTEGGERE Usando un password manager come Key, custodire la "master password", quella che dà accesso al programma e quindi a tutte le password memorizzate, è fondamentale. Per questo Key usa un algoritmo formidabile. La chiave di criptaggio infatti viene derivata dalla master password, prima sottoponendola a una complessa funzione matematica, poi aggiungendole un codice di autenticazione basato su hash (HMAC) a 256 bit, infine inserendo dei dati pseudo-casuali (Salting) … e ripetendo il processo 20.000 volte

FIDARSI

CIECAMENTE

DELLE EMAIL

Qual è il primo programma che apriamo ogni mattina?
Per molti di noi è l'email.

Nonostante l'avanzare massiccio dei software di messaggistica, di chat e di social networking, l'email rimane fra i principali strumenti di comunicazione per chi lavora, al pari del telefono.

Ogni giorno, i circa 4,3 miliardi di titolari di caselle email inviano circa 200 miliardi di email.

La maggior parte delle quali (si calcola oltre l'80%) è spam, ovvero mail spazzatura: messaggi pubblicitari o contenenti malware.

La maggior parte di essi viene filtrata dagli Internet Service Provider,
ma sono davvero troppi e ogni tanto qualcuno riesce ad arrivare sui nostri PC.

COSA PUO' SUCCEDERE

E così succede per esempio di trovarsi in casella un'email di un noto corriere che ci dice che non ha potuto consegnarci un pacchetto, e di cliccare sul PDF allegato per i dettagli.

Noi clicchiamo sul PDF, e mentre riflettiamo sul fatto che non aspettavamo nessun pacchetto da nessun corriere… sentiamo il disco fisso che si mette in movimento.

Pochi secondi dopo, una schermata ci avvisa che i nostri file sono stati criptati, e che per leggerli di nuovo dobbiamo pagare un riscatto.

E mentre cerchiamo il numero del tecnico, il "Ransomware" (letteralmente "software ricattatore") che abbiamo sul PC entra nella rete aziendale, si propaga al server, inizia a criptare lo storage centrale e i NAS, si installa e agisce sui PC dei colleghi.

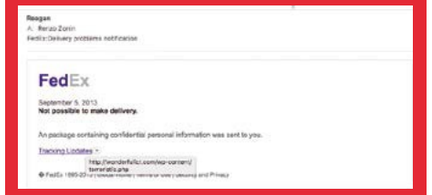
Dopo pochi minuti, l'azienda è completamente bloccata. Questo è, naturalmente, lo scenario peggiore; purtroppo, sta succedendo sempre più di frequente, perché sono ormai in circolazione diversi software di questo tipo.

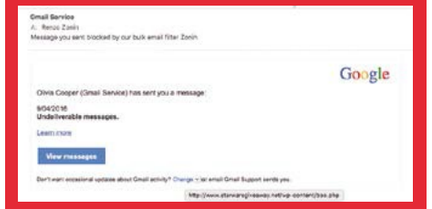
Oltretutto, stanno diventando sempre più sofisticati, e soprattutto abili a propagarsi in una rete aziendale, riducendo le probabilità che qualche unità disco passi inosservata.

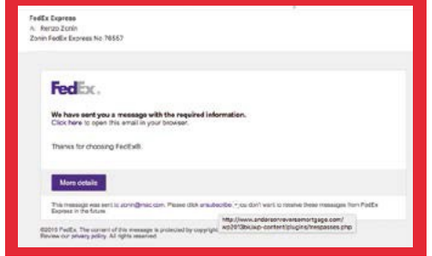
Ma anche se il messaggio di spam non contiene un ransomware, può comunque provocare problemi e inconvenienti vari, o perlomeno perdite di tempo mai gradite. I messaggi possono per esempio veicolare virus e trojan horse di vario tipo, come per esempio i keylogger (programmi che registrano cosa battete sulla tastiera e inviano i dati a chi li ha creati) grazie ai quali gli hacker possono entrare in possesso di account e password che usate dal PC; in altri casi, la mail non contiene allegati, ma un link a un sito malevolo.

Visto che molti programmi di gestione email permettono di visualizzare automaticamente codice HTML (comportandosi, in pratica, come un browser Internet), basta fare clic e visualizzare il sito relativo al link per mandare in esecuzione qualsiasi codice malevolo inserito nella pagina.

ESEMPI DI EMAIL CON MALWARE







COSA FARE

La prima contromisura da adottare è dotarsi di un buon sistema antispam. Molti provider di posta elettronica lo offrono come servizio incluso nel costo della casella, ma offrono anche un livello "premium" con un supplemento di prezzo.

Se il server della posta è in azienda, sarà il responsabile IT a occuparsi della messa in sicurezza. Infine, vanno attivati e tenuti aggiornati i filtri antispam presenti sul proprio programma di email.

Fatto tutto questo, bisogna comunque stare in allerta. Arriva una mail da una banca che vi chiede di confermare le vostre credenziali di accesso?

È sicuramente falsa, la banca sa benissimo quali sono le vostre credenziali, e se le deve controllare vi chiede di andare di persona. Un corriere ha problemi nel consegnare un pacco?
Quando succede, al limite vi chiama al cellulare, o se davvero manda una mail allora indica il mittente del pacco, il codice di tracciamento, l'ora e l'indirizzo della mancata consegna; se la mail è un generico "c'è un problema, clicca qui" è falsa.

Se ancora avete dei dubbi, un trucco utile è passare con il mouse (senza cliccare) sopra il mittente: scoprirete che quello che appariva come FamosoCorriere@Americano diventa improvvisamente un misterioso individuo russo o nigeriano o cinese.

Allo stesso modo, passando sopra il link sul quale la mail invita a cliccare quello che appariva essere il sito del FamosoCorriere diventa un oscuro indirizzo totalmente sconosciuto.

O, nelle truffe più sofisticate, un indirizzo che a prima vista può somigliare a quello del famosoCorriere, ma leggendolo con attenzione si vede che è solo "imitato".

Più subdole sono le mail di spam che paiono arrivare da un vostro contatto, spesso generiche del tipo "Guarda questa foto allegata". Fortunatamente, la maggior parte di queste comunicazioni ormai passano via social, quindi vederle per mail vi dovrebbe insospettire immediatamente. Vale sempre l'idea di passare con il mouse sul mittente per vedere se davvero è chi dice di essere.

Non prendiamo proprio in considerazione, infine, le sgrammaticate email che dicono più o meno "Buongiorno, sono alto funzionario di Banca Nigeriana e cerco persona fidata che si presenti come erede di defunto generale golpista per dargli accesso a conto da 5 milioni di dollari che poi ci dividiamo".

Eppure, se le mandano ancora, vuol dire che qualcuno ci casca.

10 COSE DA NON FARE MAI · CAPITOLO 5

SCARICARE

ED INSTALLARE

APP SENZA

PERMESSO

Causa riduzione dei budget, hanno chiesto a voi di "sistemare" le foto scattate dai colleghi alla festa aziendale, per metterle sulla pagina Facebook della ditta.

Certo, non lo si può fare con Paint o con PowerPoint… ma che problema c'è, conoscete un sito pirata da dove scaricare Photoshop e con la banda che c'è in ufficio è un attimo.

Poco dopo, la versione illegalmente piratata del programma Adobe è installata sul vostro PC.

Doppio click sul "Keygen", il programma scaricato insieme a Photoshop che vi fornisce un falso numero di serie, e ottenete… il seriale?

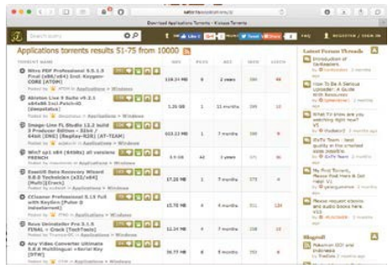
No, ottenete di trovarvi il PC infettato da un virus

COSA PUO' SUCCEDERE

Installare software pirata è un reato, e questo in teoria dovrebbe bastare a scoraggiare questa operazione.

Invece, l'Italia figura ai primi posti nel mondo per utilizzo di software illegale. È evidente che la possibilità di subire una denuncia non funziona come deterrente. Vediamo se funziona questo: la maggior parte del software pirata contenuto nei circuiti del P2P (gli storici torrent ed eMule), o nei più recenti circuiti di condivisione file (gli eredi di RapidShare), sono in realtà file infetti. Generalmente, il malware si nasconde non nel software vero e proprio, ma nel programmino (il "Keygen") che, scaricato insieme al file principale, dovrebbe generare il numero di serie fasullo per usare il programma. Al lancio, il Keygen chiede all'utente il permesso di fare modifiche al sistema… e una volta autorizzato può fare quello che vuole. L'installazione di trojan e keylogger è l'evento più comune, ma si sono verificati anche incidenti più gravi (Ransomware).

Detto questo, non è che installare software legale metta sempre al riparo da ogni rischio. Sulla piattaforma Android, per esempio, migliaia di applicazioni presenti sul Play Store ufficiale di Google non sono quello che sembrano. Voi pensate di aver scaricato un gioco gratuito

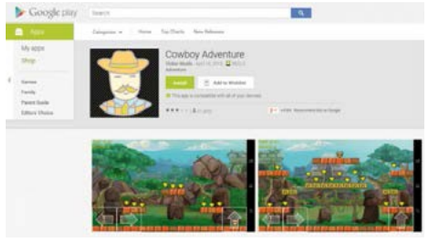


e invece avete installato (e magari dato autorizzazioni d'accesso pressoché illimitate) un programma che si occuperà di controllare la vostra navigazione Internet, di rastrellare le email e i numeri di telefono dei vostri contatti, di catturare i dati della vostra carta di credito, di abbonarvi di nascosto a costosi servizi aggiuntivi, mostrarvi continuamente pubblicità e via di questo passo. Difficile capire quali sono le applicazioni truffaldine, anche se in alcune categorie sono più frequenti: per esempio, i "cloni" di app e giochi famosi, soprattutto se le versioni ufficiali non sono ancora presenti sulla piattaforma. Un esempio? Prisma, un'app iOS che è arrivata su Android solo dopo che una dozzina di suoi "cloni" erano già spuntati nel Play Store. Questi cloni sono stati scaricati da 1,5 milioni di utenti, molti dei quali sono stati infettati da trojan. Questo fenomeno è al momento meno pronunciato sul desktop, ma non è detto che, con la diffusione anche sui PC da tavolo dell'approccio tipico del mobile (con le app distribuite dagli app store "ufficiali") non si vada verso un aumento del numero di casi. I primi segnali ci sono già: per esempio il rapido aumento della diffusione di programmi "made in china" che risultano essere imitazioni gratuite di programmi più noti.

COSA FARE

Premesso che per nessun motivo si dovrebbe installare software pirata nel proprio PC aziendale, e tanto meno usare in ufficio programmi per il P2P, è in ogni caso sconsigliabile installare autonomamente qualsiasi software su un computer “di produzione”, senza prima essere autorizzati da un responsabile.

C’è sempre la possibilità che il software installato autonomamente possa andare in conflitto con programmi fondamentali per il lavoro, in particolare su piattaforme come Windows dove fra registro di sistema e framework vari ci sono parecchie probabilità di incorrere in incompatibilità.



Il ragionamento vale a maggior ragione per i dispositivi mobili forniti dall’azienda, come smartphone o tablet.

In questi apparecchi, soprattutto nel mondo Android (ma anche iOS ha subito qualche attacco ultimamente), è molto facile installare malware senza rendersene conto, perché i controlli dello store ufficiale sono poco approfonditi e spesso Google agisce solo a posteriori, rimuovendo un’app malevola solo dopo che gli utenti hanno fatto da cavie subendone le conseguenze.

10 COSE DA NON FARE MAI · CAPITOLO 6

RIMANDARE

GLI

AGGIORNAMENTI

Siamo arrivati in ufficio in largo anticipo…
perché non fare una capatina su Facebook prima di iniziare il lavoro?
Ma guarda, c'è un post consigliato con un bellissimo filmato di teneri gattini… andiamo subito a vederlo!
Ma cos'è questo messaggio di Adobe?
"È disponibile una nuova versione di Flash Player – aggiorna subito il tuo PC".
Ma figuriamoci, dobbiamo vedere i gattini… aggiorneremo domani.
Un clic su "Cancella" e facciamo partire il video.
Finito il video, il nostro PC è infettato da un trojan entrato grazie a una vulnerabilità del Flash Player.
Proprio quella che l'aggiornamento che abbiamo saltato avrebbe risolto.

COSA PUO' SUCCEDERE

Scrivere software è, ancora oggi, più un'arte che una scienza esatta. Sarà forse per questo che la maggior parte dei sistemi operativi e dei programmi contengono decine, se non centinaia, di "punti critici" per la sicurezza.

Ovvero difetti (o veri e propri errori di programmazione) che se adeguatamente sfruttati permettono a programmi nocivi di installarsi nel PC e venire eseguiti, quasi sempre senza che l'utente si accorga di nulla… almeno fino a che non si produce il danno.

E a quel punto è tardi per rimediare. La guerra fra i "cracker" (ovvero coloro che cercano questi difetti per sfruttarli a proprio vantaggio, di solito per fini illegali) da una parte e gli hacker (quelle persone che cercano i difetti nei programmi allo scopo di perfezionarli, correggendo gli errori o informando i produttori della loro esistenza) e i programmatori dall'altra è in corso da decenni ed è senza esclusione di colpi.

L'obiettivo di ogni cracker è scoprire una falla cosiddetta "zero day", ovvero della quale i programmatori non sono informati e per la quale non c'è rimedio, e approntare un cosiddetto "exploit", cioè il codice per sfruttare quella falla.

Una volta messo a punto l'exploit che consente di entrare nel PC e di scalare i privilegi di accesso, diventando di fatto amministratore del sistema,

L'obiettivo di ogni cracker è scoprire una falla cosiddetta "zero day", ovvero della quale i programmatori non sono informati e per la quale non c'è rimedio.

Il cracker può procedere come meglio crede, aggiungendo all'exploit stesso il "payload" che preferisce – in pratica, codice malevolo specifico per eseguire determinate operazioni: leggere i dati sul PC, modificare o cancellare file, criptarli con un ransomware, rubare credenziali di accesso, o installare keylogger che registrano tutto quello che battete sulla tastiera e lo inviano al cracker.

Insomma, la gamma delle conseguenze di un exploit è davvero ampia.

Di solito, dopo che le prime infezioni vengono segnalate si procede a scoprire qual era la vulnerabilità, a correggerla e a inviare agli utenti l'avviso di eseguire l'aggiornamento del software.

Ma a questo punto l'exploit potrebbe essere già in circolazione da parecchio, e quindi non c'è tempo da perdere: bisogna procedere il più rapidamente possibile all'aggiornamento del software, per non correre il rischio di essere presi di mira.

COSA FARE

Dobbiamo però distinguere due grandi categorie di aggiornamenti del software: gli aggiornamenti di versione (o "major update"), che servono di solito a introdurre nuove funzionalità o a migliorare le prestazioni, e le patch di correzione (spesso definite "minor update") che servono a correggere errori, bug o vulnerabilità. Le patch di correzione urgenti vengono emesse senza preavviso non appena sono pronte, e vanno in genere installate immediatamente. Le patch di correzione per vulnerabilità lievi o poco frequenti invece vengono spesso raggruppate in blocchi e inviate agli utenti a cadenza settimanale o mensile. Le macchine Windows spesso vengono configurate per gestire i relativi aggiornamenti di sistema operativo in automatico, mentre per quanto riguarda il software applicativo di solito si viene avvisati della disponibilità di patch dall'applicativo stesso (eventualmente via centro notifiche).
Come abbiamo visto nell'esempio di Flash, che fra l'altro è uno dei programmi che più frequentemente richiede patch di sicurezza, è meglio procedere rapidamente agli aggiornamenti di questo tipo. Gli aggiornamenti di versione invece sono di solito preannunciati per tempo, e generalmente hanno cadenze regolari (semestrali o annuali). Si riconoscono a prima vista perché il numero di versione del software viene incrementato di una unità (come nel passaggio da Windows 7 a Windows 8) quando ci sono notevoli cambiamenti rispetto alla versione precedente, o di un decimale (come da Windows 8 a Windows 8.1) per cambiamenti più limitati, miglioramenti di efficienza, eccetera.

Gli aggiornamenti di sicurezza in genere incrementano il secondo decimale (come l'aggiornamento di iOS 9.3.5 rilasciato da Apple lo scorso agosto, per correggere tre falle zero day usate da cracker dei servizi segreti di un paese mediorientale per monitorare l'attività di dissidenti politici).

In ambito aziendale, però, una "major update" di un sistema operativo o di un software applicativo potrebbe creare problemi di compatibilità all'interno del sistema informativo: per esempio, un nuovo sistema operativo potrebbe necessitare di computer con più memoria o processore più potente, e una nuova release di un applicativo potrebbe non supportare più un vecchio formato di file che però viene ancora usato in qualche reparto.

Quindi, nel caso di aggiornamenti di versione, la cosa migliore è aspettare che il reparto IT aziendale faccia le sue verifiche, ed aggiornare solo dopo il nulla osta. E cosa succede se la nuova versione contiene anche delle patch di sicurezza urgenti?

Nessun problema: i produttori di software distribuiscono infatti le stesse patch incluse nella nuova versione anche sotto forma di aggiornamento di sicurezza per la versione precedente del software.

Le patch di sicurezza vanno installate al più presto. Le nuove versioni del software devono prima essere autorizzate dall'IT aziendale.

NAVIGARE

PERICOLOSAMENTE

Una pausa pranzo passata alla scrivania ingoiando un panino può essere davvero noiosa. Perché non rallegrarla facendo un giretto sul Web?
Per esempio, cercando qualche interessante sito di prodotti gastronomici etnici, giusto per tirarci su il morale… detto fatto, da Google arriviamo a una pagina appetitosa.
Il sito si apre e mentre ci riempiamo gli occhi con quelle specialità, all'improvviso appare una finestra pop-up: "È stato rilevato un pericoloso virus sul tuo PC", dice.
E prosegue "vuoi scaricare l'antivirus per eliminarlo?".

Rispondiamo sì e… pochi secondi dopo il nostro PC, che in realtà era assolutamente "pulito", si ritrova infettato da malware.

COSA PUO' SUCCEDERE

Ebbene sì, è assolutamente possibile essere colpiti da malware semplicemente visitando un sito Web.
E non è detto che i più pericolosi siano quelli che tutti pensano: siti porno a pagamento e siti di gioco d'azzardo, per esempio, hanno una "reputazione" da difendere con la loro clientela, e quindi sono molto vigili nell'evitare problemi di malware.
Le statistiche invece ci dicono che, in Europa, la maggior parte dei brutti incontri si ha visitando siti dei settori agricoltura, gastronomia e bevande, assicurazioni, produzione industriale e giornali. Negli USA invece la classifica vede al primo posto le aviolinee.
,Ma nella classifica mondiale combinata degli attacchi la spuntano i siti delle industrie farmaceutiche e chimiche.
Cos'hanno in comune questi siti? Il fatto di essere ad alto traffico. Perché ovviamente non è il proprietario del sito che inserisce il malware: sono i cracker che scelgono in quali siti inserire di nascosto i loro malware, e ovviamente prediligono pagine ad alto traffico e… insospettabili.
Tipicamente, il codice malevolo inserito nelle pagine Web va ad attaccare le vulnerabilità note dei browser (soprattutto Explorer), oppure dei loro plug-in, in particolare Flash player, il plug-in Silverlight di Microsoft o Adobe Reader.
Spesso i cracker fanno ricorso a Javascript per scaricare, installare e lanciare i loro malware. In altri casi, si ricorre al trucco di far scaricare il codice dell'infezione facendolo passare per un codec video, senza il quale non si può vedere un determinato filmato.

lMa anche siti che non sono stati hackerati, e che quindi dovrebbero essere puliti, possono contenere malware. In molti casi, per esempio, il codice malevolo è stato trovato all'interno dei banner pubblicitari presenti sulla pagina, ovviamente all'insaputa del proprietario del sito.
Infine, ci sono siti creati appositamente con l'intento di scaricare malware sui PC degli utenti, vere e proprie trappole dove si viene fatti arrivare, in genere, per vie traverse: per esempio con messaggi su Twitter o Facebook che invitano a visitare una pagina Web, ma usando un indirizzo abbreviato (Tinyurl, Bit.ly) che non permette di capire dove si sta realmente andando… fino a che è ormai troppo tardi.

Una volta che il cracker è riuscito a far scaricare e a mettere in esecuzione dalla pagina Web il suo malware, la gamma di cose che può fare dipende come al solito dal tipo di "payload" che l'exploit provvede a installare sul PC. Si va dal monitoraggio della tastiera al furto del file dei contatti, dall'installazione di toolbar aggiuntive sul browser al temuto criptaggio dei file con richiesta di riscatto.

Iniziare a pensare che su Internet è pieno di gente che vuole derubarci è già un buon punto di partenza per evitare di cadere vittime di truffatori online.

COSA FARE

Anche se può sembrare un atteggiamento paranoico, mettersi in testa che su Internet è pieno di gente che vuole derubarvi è un buon approccio iniziale.

Lo è perché ci obbliga a prestare attenzione a quello che facciamo, avendo la consapevolezza che si può incappare facilmente in qualche losco individuo.

Poi ci sono cose più concrete che possiamo fare per difenderci: mantenere aggiornati il browser e tutti i plug-in critici, per esempio, aiuta perché riduce il numero di vulnerabilità del sistema. Ancora meglio è

spegnere i plug-in, o metterli nella modalità che richieda l'autorizzazione dell'utente prima di farli funzionare. Un'altra buona idea è di installare un Adblocker (software che blocca i banner pubblicitari) e uno Scriptblocker (software che blocca l'esecuzione di programmi Javascript, altro strumento spesso usato dai cracker per inserire il malware sui PC degli utenti).

Questi due tipi di programmi evitano che il browser visualizzi contenuti potenzialmente a rischio, e che li metta in esecuzione. Per i siti di cui abbiamo assoluta fiducia possiamo escludere il blocco, compilando una cosiddetta "whitelist", una lista di siti sicuri che viene gestita dai programmi di blocco.

10 COSE DA NON FARE MAI · CAPITOLO 8

COLLEGARE CHIAVETTE O DISCHI ESTERNI

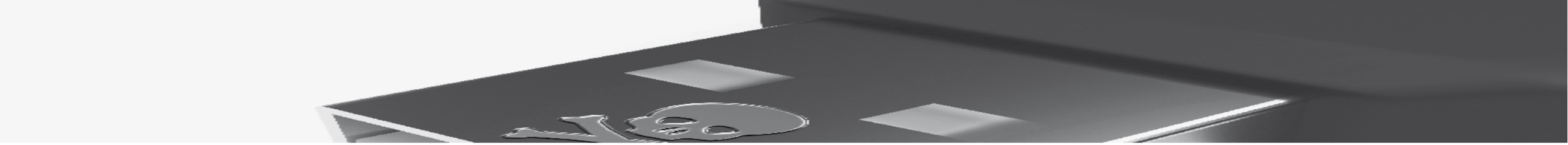
“Papà, quando vai in ufficio mi stampi la tesina d’esame?

Sono solo una ventina di pagine… tieni, è in questa chiavetta USB”.

E così, incuranti dei regolamenti di sicurezza informatica, durante la pausa pranzo inserite la chiavetta del pupo nel PC…

e qualche secondo dopo il vostro computer è infettato da un virus.

E adesso?



COSA PUO' SUCCEDERE

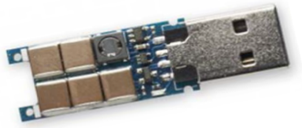
Prima che Internet diventasse pervasiva, la maggior parte delle infezioni da virus informatico si prendevano scambiandosi floppy disk infetti.

Col tempo, i floppy sono diventati un ricordo del passato, ma le chiavette USB li hanno validamente sostituiti per spostare rapidamente dati da un computer a un altro, soprattutto quando si tratta di macchine non in rete.

Purtroppo, anche la chiavetta USB è facilmente soggetta a infezioni, proprio come il suo antenato magnetico.

Il principale colpevole di queste infezioni è, in genere, Autorun.inf, un file che Microsoft introdusse anni fa per semplificare l'installazione di software da parte dei non esperti. In pratica, quando si inserisce un disco esterno (che sia un CD o una chiavetta) Windows controlla se esso contiene un file Autorun.inf, e se lo trova lo esegue.

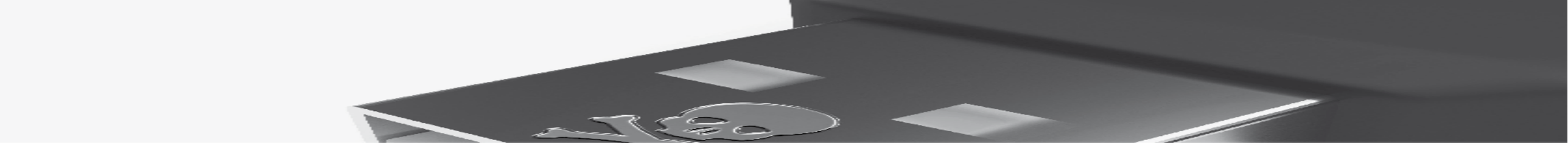
Ovviamente, un cracker può mettere in autorun ciò che vuole, anche perché se con i floppy disk c'erano ovvi problemi di spazio (la capacità massima era di 1,4 Megabyte), con le chiavette USB si hanno a disposizione anche diversi Gigabyte.



Sembra una normale chiavetta USB, ma aprendola rivela un circuito ad alta tensione capace di mettere fuori uso l'hardware di un PC appena collegata.

Chiaramente, nessun cracker che si rispetti trascurerà di inserire nel suo malware un sistema di replicazione, per cui il computer infettato provvederà in seguito a infettare a sua volta ogni chiavetta USB che gli verrà collegata.

Ma l'ingresso di malware tramite chiavetta non è l'unico problema di sicurezza che può riguardare una porta USB. C'è un altro problema, che riguarda principalmente le porte USB degli smartphone e tablet: lo spyware. Da qualche anno, si stanno moltiplicando nei locali pubblici, nei terminal degli aeroporti e negli hotel le prese USB dedicate alla ricarica dei cellulari. In teoria dovrebbero essere semplicemente collegate a un trasformatore di alimentazione, ma sono stati segnalati casi di porte di ricarica che in realtà celavano un controller USB e una scheda digitale, in grado di connettersi al dispositivo che si sta ricaricando e di rubare i dati in esso contenuti.
Apparecchi di questo tipo possono essere installati solo da gruppi ben organizzati di cracker, e infatti i rari casi registrati pare riguardino operazioni di servizi segreti o di spionaggio industriale in grande stile.
Tuttavia, se sul proprio smartphone si tengono dati estremamente riservati e importanti, sarà meglio tener conto di questa possibilità e quindi evitare di collegare il cellulare alla prima USB che si trova.



COSA FARE

Per prima cosa, sarebbe meglio essere prudenti nel collegare al proprio computer aziendale chiavette USB di dubbia provenienza.

In particolare, le statistiche ci dicono che la maggior parte delle chiavette infette arriva dall'ambito scolastico/universitario e dalle copisterie.
Disabilitare l'Autorun sul proprio computer Windows è un'operazione che richiede solo un paio di minuti, ma bisogna saper maneggiare il malefico Registro.
Nel caso, si può chiedere l'intervento del personale IT aziendale, sempre che non abbiano già provveduto.

È importante poi che l'antivirus che gira localmente sul PC sia programmato in modo da effettuare una scansione di ogni nuovo disco che viene collegato alla macchina, prima di darne accesso al resto del sistema.

È sempre consigliabile disabilitare l'Autorun sul proprio computer. L'operazione è semplice ma richiede di manipolare il Registro, quindi meglio farla fare a un esperto.

10 COSE DA NON FARE MAI · CAPITOLO 9

COLLEGARSI

A RETI

WI-FI LIBERE

È proprio vero, qualsiasi piano tariffario si scelga per il nostro smartphone/tablet, i Giga non bastano mai.

Per fortuna che ogni tanto abbiamo la fortuna di scovare qualche rete Wi-fi non protetta,
come questa qui.

Approfittiamone per spedire in ufficio la documentazione riservata del nuovo cliente…
e già che ci siamo diamo anche un'occhiata all'estratto conto della banca.

Il giorno dopo, scoprite che il vostro conto corrente è stato svuotato: secondo la banca, avete fatto un **bonifico per l'intero importo verso un conto nell'Europa dell'Est**.

Ma come?

Una rete Wi-fi è come una normale rete locale: chi ha competenze adeguate può sapere tutto delle altre macchine collegate.

COSA PUO' SUCCEDERE

Le reti Wi-fi libere, ovvero alle quali è possibile accedere senza autenticarsi, sono uno dei terreni di caccia preferiti dai cracker, perché ci si entra facilmente e non si corre il rischio di essere identificati.

Quello di cui non ci rendiamo conto, purtroppo, è che una rete Wi-fi funziona appunto come una normale rete di Pc, e quindi chi è nella stessa rete e dispone di adeguate competenze tecniche può sapere esattamente cosa state facendo, vedere i vostri file, e trarre vantaggio da questo.

In realtà, i cracker possono interagire con una rete Wi-fi libera in vari modi. Il più semplice è appunto collegarsi come utente e controllare cosa fanno gli altri dispositivi connessi. Trovato un "soggetto" interessante, possono eseguire un attacco cosiddetto MitM,

"Man in the middle": in pratica, voi pensate di essere collegati all'hotspot Wi-fi, ma in realtà il vostro flusso dati passa dal computer del cracker il quale a sua volta lo passa all'hotspot, ma solo dopo averlo controllato, registrato e, se necessario, alterato.

Così un cracker MitM può, per esempio, cambiare al volo l'Iban di un vostro bonifico dirottando i soldi su un conto a lui intestato. O cambiare un commento che state inserendo su Facebook.

Un'altra possibilità è che all'hotspot libero si colleghino computer infettati da malware, che tenteranno a loro volta di trasmettere il software malevolo a tutte le altre macchine connesse alla rete.

Il caso peggiore è forse incappare in un hotspot che è sotto il controllo di un cracker, o perché quest'ultimo è riuscito a prendere il controllo del router, o perché la rete stessa è stata approntata da un cracker con l'intento di attaccare i malcapitati che si dovessero collegare. Una rete di questo tipo, una vera e propria trappola, viene chiamata in gergo "honeypot", vaso di miele.

Quando ci si collega a una rete di questo tipo, tutto il proprio traffico è monitorato e, nel caso, registrato, reindirizzato, modificato dal cracker. A complicare ancora di più la vita di chi cerca una rete Wi-fi cui collegarsi, esistono apparecchi hardware (Pineapple per esempio) capaci di intercettare

i dispositivi che cercano di collegarsi a reti già conosciute, e rispondere al tentativo di connessione fingendo di essere la rete cercata.

Una volta stabilita la connessione, questi apparecchi sono in grado di localizzare ogni vulnerabilità del dispositivo connesso e possono quindi eseguire attacchi di vario tipo, dal MitM a installazione di malware e via discorrendo.

COSA FARE

Visto che non c'è modo per capire se la rete Wi-fi cui ci si sta connettendo è "sicura" o in qualche modo infetta, bisogna agire all'insegna della prudenza.

Per esempio evitando proprio di eseguire operazioni che trasferiscano dati sensibili, informazioni di accesso a servizi eccetera.

A parte questo, l'uso di un sistema VPN, per cominciare, può dare una ragionevole sicurezza che i dati che scambiate, essendo criptati, non possano essere sfruttati da eventuali cracker in ascolto.

La VPN va usata anche per i collegamenti web Https, perché questi ultimi possono essere facilmente intercettati e decodificati con attacchi MitM.

Altri accorgimenti utili sono il disabilitare la condivisione dei file dal pannello di controllo di Windows, o meglio ancora stabilire la connessione tramite il profilo di rete "Pubblica", invece che Casa o Aziendale.

Dovresti preferire una VPN anche se non sei su una rete pubblica per proteggere te stesso da elementi di tracciamento onnipresenti come i perma-cookie.

Questo dispositivo intercetta le richieste di connessione dei dispositivi mobili, e risponde fingendo di essere la rete da essi cercata.

Questo fa capire a Windows che si sta muovendo in ambiente potenzialmente ostile, e regola alcune impostazioni in modo da garantire più privacy.

Infine, è utile disabilitare la connessione automatica a reti Wi-fi aperte che tipicamente è impostata come attiva su smartphone e tablet.

10 COSE DA NON FARE MAI · CAPITOLO 1

PERDERE

DI VISTA

SMARTPHONE

TABLET

O NOTEBOOK

L'ennesimo viaggio di lavoro in treno. Ormai abbiamo il posto fisso, come Hemingway all'Harry's Bar.
Come sempre, saliamo trascinandoci dietro il pesante trolley e la ventiquattrore con notebook e documenti.
Arriviamo arrancando al posto, e come al solito poggiamo la valigetta sul sedile e issiamo il trolley sulla rastrelliera.

Ci giriamo e… la valigetta dov'è finita?

Ecco: sono bastati 5 secondi di distrazione a un ladro (o due, spesso agiscono in coppia)
per mandare all'aria tutto il programma del viaggio.
Già, perché ovviamente era tutto lì dentro…

Bilanci, ricorsi, pareri, documenti … e adesso?

COSA PUO' SUCCEDERE

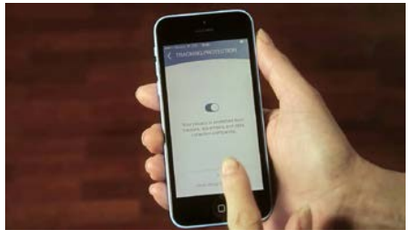
I furti, o per meglio dire i borseggi, non sono tutti uguali. Il ladro che si incontra più di frequente è quello che, appena messe le mani su un computer, un tablet o un cellulare, lo va a vendere per pochi euro a un ricettatore o in qualche mercatino dell'usato.

Fortunatamente, è il ladro che provoca meno danni: è vero, magari manda all'aria il viaggio, o gli appuntamenti della giornata, ma per rimettere le cose a posto basta comprare un dispositivo identico a quello sottratto e ricaricare i dati da un backup (**perché noi a abbiamo i backup aggiornati di tutto, VERO?**).

Qualche ora e si è nuovamente operativi, con un danno economico minimo, soprattutto se l'azienda ha stipulato un'assicurazione contro i furti.

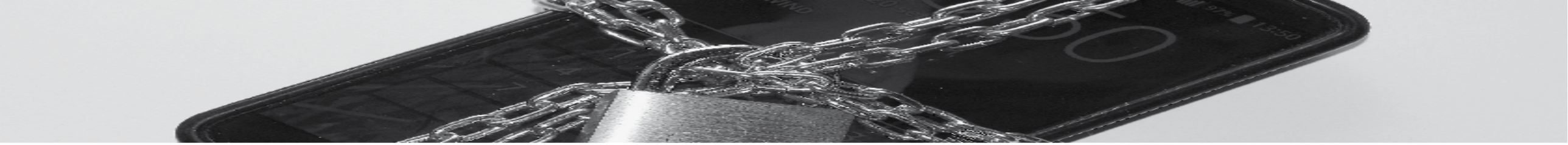
Il ladro più pericoloso è quello che non mira al computer, ma ai dati in esso contenuti.

I veri problemi, invece, sorgono se quello che ha rubato il vostro dispositivo non era a caccia di una preda qualsiasi, ma voleva rubare proprio il vostro computer. Quel ladro in effetti non mira alla macchina, ma ai dati in essa contenuti. I furti su commissione sono ora poco frequenti, visto che è possibile andare a sbirciare i file di un'azienda concorrente via Internet senza quasi lasciare tracce, a patto di assoldare un bravo cracker.



Ma ci sono aziende che hanno protetto i loro sistemi informativi con gli strumenti e le metodologie giuste, rendendoli pressoché inviolabili… e a questo punto, per un concorrente senza scrupoli l'opzione del furto diventa l'unica percorribile.

Esiste anche una terza possibilità: un borseggiatore ruba qualsiasi dispositivo trovi, ma invece di rivenderlo subito lo porta a un complice cracker che esamina il contenuto alla ricerca di informazioni preziose: accessi automatici a conti correnti, credenziali di accesso a servizi premium e sistemi di pagamento elettronico, chiavi di accesso al sistema informativo aziendale eccetera.



COSA FARE

Proteggere i dati da tentativi di accesso da parte di estranei è la prima cosa da fare. Sincerarsi quindi di avere inserito password robuste per l'accesso al sistema, e ricordarsi di tenere aggiornato il software della macchina per ridurre al minimo le vulnerabilità sfruttabili per i tentativi di intrusione.

Un'altra cosa molto utile è applicare la crittografia integrale del disco. Infatti, chi fosse interessato ai dati potrebbe aggirare le password semplicemente estraendo il disco dal computer e inserendolo in una macchina di sua proprietà.

Con la crittografia, questo non sarà possibile, perché senza la chiave di accesso i dati saranno illeggibili. Uno spiacevole effetto collaterale di questo accorgimento è che se vi si guasta il PC, non è possibile recuperare i dati inserendo il disco in un'altra macchina. Nemmeno ricorrendo ad aziende specializzate nel "data recovery".

Quindi, è assolutamente vitale che di tutti i dati abbiate un backup sicuro. Sul server aziendale, sul desktop dell'ufficio, sul cloud della ditta, ma il backup ci deve essere.

Usare un disco criptato evita che il ladro ne legga i dati semplicemente estraendolo dal nostro laptop e inserendolo nel suo computer.

E se volete essere assolutamente sicuri che il cracker non avrà il tempo di decrittare i vostri file, potete ricorrere a specifici software che provvedono a cancellare i dati in caso di furto o smarrimento del dispositivo.

Risolto il problema dati, torniamo per un attimo al dispositivo hardware: non c'è proprio modo di ritrovarlo?

Beh, a parte sperare nell'opera delle forze dell'ordine, le probabilità di ritrovare l'apparecchio salgono se si è provveduto a installare e attivare uno di quei software che trasmettono via mail la posizione del dispositivo e una foto di chi lo sta usando appena si accorgono di essere stati rubati.

Gli utenti Apple da tempo trovano preinstallata l'utility "Trova il mio iPhone" (o l'equivalente "Trova il mio Mac"). Utility simili ora sono disponibili anche per Windows e Android.

Per molte persone, Internet è un'entità virtuale, e virtuale è tutto ciò che su Internet viene fatto. In realtà, da molto tempo non è più così. Internet è strettamente legata alla vita reale della maggior parte di noi. Il conto corrente bancario che controlliamo dal PC non è virtuale, sono soldi veri, che abbiamo guadagnato. Se compriamo qualcosa on line, il denaro viene preso dalla nostra carta di credito e a casa ci arriva un prodotto.

Se conversiamo con gli amici su Facebook, paghiamo una bolletta, prenotiamo una vacanza, stiamo facendo cose reali, che fino a ieri erano magari più scomode, richiedevano code alla posta o telefonate intercontinentali. Internet non ha trasformato nulla in "virtuale": ha semplicemente fornito a tutti noi uno strumento unificato e molto versatile sul quale appoggiare parte della nostra vita reale, con indubbi vantaggi in fatto di comodità e costi.

Ma anche se Internet è vita reale, noi ci ostiniamo a usarla come se fosse un mondo a parte, assolutamente perfetto, e dal quale non possono derivare problemi. Usciremmo mai di casa senza chiudere a chiave la porta? Guideremmo in un quartiere malfamato con finestrino aperto, braccio fuori e Rolex d'oro al polso in bella vista? Seguiremmo da soli in un vicoletto buio uno sconosciuto che, dice lui, vuol proporci un affare? No, vero? E allora come mai ci ostiniamo a usare password elementari per i nostri account Internet, clicchiamo su banner pubblicitari equivoci, e ci colleghiamo alla prima rete Wi-fi non protetta che captiamo con lo smartphone?

Il fatto è che nella vita reale abbiamo assimilato da tempo quali comportamenti sono sicuri e quali no, anche perché ce li insegnano fin da piccoli. Sappiamo di dover stare attenti ai ladri e di non fidarci degli estranei, sappiamo che non si attraversa col rosso e non si dimentica il gas aperto. Ma i comportamenti sbagliati su Internet, quelli non ce li ha spiegati nessuno. Di solito, si apprendono con l'esperienza, ovvero dopo che il danno è stato fatto.

Bene: abbiamo pensato di risparmiarvi un po' di danni, compilando questo decalogo di cose da non fare mai su Internet. Per ogni operazione proibita spieghiamo cosa può comportare e come difendersi.

Speriamo vi possa essere utile per usare Internet in modo cosciente e sicuro.