Guida all'autodifesa digitale #1

SOMMARIO

Illustrazioni di Pinza666

ELETTRICITÀ, CAMPI MAGNETICI, RUMORE E ONDE RADIO

Dopo questo rapido tour all'interno dei suoi componenti, occorre prendere atto di diverse cose, per quanto riguarda la riservatezza delle informazioni che transitano dentro a un computer.

Prima di tutto, che la parte essenziale delle informazioni circola sotto forma di corrente elettrica. Quindi niente impedisce di poter mettere l'equivalente di un banale voltmetro per misurare la corrente che passa, e ricostruire poi i dati manipolati dal computer in una forma o nell'altra.

Inoltre, tutta la corrente che circola ha la tendenza a creare un campo magnetico. Questi campi magnetici possono irradiarsi per qualche metro (1). Quindi, chi ne ha i mezzi, potrebbe ricostruire il contenuto di una schermata o di ciò che è stato scritto su una tastiera, e potrebbe farlo da dietro un muro, in strada o

dall'appartamento accanto. Con questo metodo, dei ricercatori sono riusciti a registrare da una distanza di 20 metri ciò che era stato digitato su una normale tastiera via cavo, partendo dalle emissioni elettromagnetiche che essa emanava (2).
Lo stesso tipo di operazione è possibile partendo dall'osservazione dei leggeri disturbi che genera il computer all'interno della rete elettrica a cui è attaccato (3).

Altre esperienze, che consistono nell'ascoltare con un microfono il rumore dei componenti elettronici del computer o quello della sua alimentazione elettrica, hanno permesso in certe condizioni di decifrare le chiavi di cifratura contenute sul computer target (4). In seguito a questo fatto sono state pubblicate delle correzioni ai software coinvolti, in modo da rendere più difficile questo tipo di attacco.

Infine, alcune periferiche (la tastiera, il mouse, le casse audio..) funzionano senza fili. Per farlo, comunicano con il computer attraverso le onde radio captabili e eventualmente decodificabili impunemente da chiunque stia intorno.

Per riassumere brevemente, anche se un computer non è connesso a una rete, e indipendentemente dai software che ci girano sopra, resta comunque possibile per delle persone ben equipaggiate “ascoltare” ciò che ci transita dentro.

Note:
1) Berke Durak, attraverso l’utilizzo di un semplice walkman capace di ricevere la radio, nel 1995 è riuscito a captare le onde elettromagnetiche emesse dalla maggior parte dei componenti del proprio computer. - http://nbl.gs/qgt

2) Martin Vuagnoux e Sylvain Pasini hanno realizzato degli spaventosi video per illustrare il loro studio Compromising Electromagnetic Emanations of Wired and Wireless Keyboards pubblicato nel 2009. - http://nbl.gs/qgu

3) Paul Kocher, Joshua Jaffe et Benjamin Jun hanno pubblicato nel 1998 un rapporto che spiegava le differenti tecniche di analisi del consumo elettrico.

4) Clément Bohic, 2013, “Crittografia: basterà ascoltare il processore per decifrare le chiavi” – http://nbl.gs/qgv

SOFTWARE

Dopo la lista dei componenti fisici che costituiscono un computer, occorre soffermarsi sull'elemento meno palpabile: il software.

All’epoca dei primissimi computer, ogni volta che si voleva eseguire una diversa operazione, si doveva intervenire fisicamente per cambiare la disposizione dei cavi e dei componenti. Adesso le cose sono molto cambiate: le operazioni da compiere per eseguire i diversi compiti sono divenute dei dati come gli altri. Questi dati, che vengono chiamati “programmi”, sono a loro volta caricati, modificati e manipolati da altri programmi ancora.
Questi ultimi generalmente sono scritti per riuscire a fare una sola cosa, e farla bene, in modo da restare comprensibili agli esseri umani che li progettano. E’ solo attraverso l’interazione di decine di migliaia di questi programmi, che si riesce a realizzare i compiti complessi per i quali vengono generalmente utilizzati i computer ai giorni nostri.

L'effetto prodotto dal nostro cliccare su un'icona, è quindi il lancio di una catena di eventi, una somma impressionante di calcoli, che causano degli impulsi elettrici che alla fine vanno a modificare un oggetto fisico (come quando masterizziamo un DVD, o come nel caso di un monitor che cambia i propri LED per mostrare una nuova pagina, o un hard-disk che attiva o disattiva dei micro-interruttori per creare la sequenza di numeri binari che costituirà un file).

IL SISTEMA OPERATIVO

Lo scopo di un sistema operativo è prima di tutto quello di permettere ai programmi di condividere l'accesso ai componenti materiali del computer. Il suo ruolo è anche quello di far comunicare i vari programmi tra di loro. Un sistema operativo viene generalmente fornito con un software, sufficiente almeno a consentire l'avvio di altri programmi.

La parte più fondamentale di un sistema operativo è il suo nucleo (il kernel), che si occupa

di coordinare l'utilizzo delle risorse fisiche da parte dei programmi.

Per ciascun componente fisico del computer che vogliamo utilizzare, il kernel attiva un programma che si chiama driver. Esistono dei driver per le periferiche di ingresso (come la tastiera e il mouse), per quelle d'uscita (il monitor, la stampante etc.) e per quelle di archiviazione (DVD, penne USB, etc.).

Il kernel gestisce anche l'esecuzione dei programmi fornendogli delle porzioni di memoria e ripartendo i tempi di calcolo del processore tra i diversi programmi che si vogliono far lavorare.

Oltre al kernel, i sistemi operativi odierni come Windows, Mac OS X o GNU/Linux (con Debian, Ubuntu, Fedora, per esempio) includono anche molti strumenti e ambienti grafici che permettono di utilizzare il computer cliccando semplicemente su delle icone.

Il sistema operativo è in genere installato sull'hard-disk. E' possibile però utilizzare invece un sistema operativo installato su una penna USB o masterizzato su un DVD. In quest'ultimo caso si parla di sistema live (visto che sul DVD non si potrà compiere nessuna modifica).

LE APPLICAZIONI

Vengono chiamate "applicazioni" quei programmi che permettono di fare davvero ciò che stiamo chiedendo a un computer. Come esempi possiamo citare Mozilla Firefox come web browser, LibreOffice per le faccende d'ufficio o VLC per la musica e i video.

Ciascun sistema operativo definisce un metodo ben preciso con il quale le applicazioni possono accedere all'hardware, ai dati, alla rete e alle altre risorse. Le applicazioni che vogliamo utilizzare devono quindi essere pensate per girare sul sistema operativo del computer sul quale vogliamo farle andare.

LE LIBRERIE

Invece che riscrivere per ogni applicazione pezzi di programma incaricati di fare le stesse cose, i software li condividono tra loro in librerie.

Esistono librerie per la visualizzazione grafica (che assicurano una coerenza in quello che viene mostrato sullo schermo), per la lettura e la scrittura dei formati dei file, per interrogare certi servizi di rete, etc.

Se non siamo programmatori, raramente abbiamo bisogno di toccare le librerie. Può tuttavia essere interessante conoscere la loro esistenza, anche solo perché un problema (ad esempio un errore di programmazione) in una libreria può ripercuotersi su tutti i programmi che la utilizzano.

LA MEMORIZZAZIONE DEI DATI

Abbiamo visto come un hard disk (o una penna USB) consentano di conservare alcuni dati nel lasso di tempo tra un'accensione e l'altra del computer.
Ma per poterli ritrovare i dati devono essere disposti in un certo modo: uno scaffale dove si accumulano semplicemente i fogli non sarebbe una delle forme di archiviazione delle più efficaci..

LE PARTIZIONI

Come dentro a un armadio, in cui si possono mettere vari ripiani, così è possibile "scomporre" un hard-disk in più partizioni.

Ciascun ripiano può avere un'altezza o una classificazione diverse a seconda che ci si voglia mettere libri o classificatori, in ordine alfabetico o in ordine di lettura.
Allo stesso modo, in un hard-disk ciascuna

partizione potrà essere di grandezza diversa e contenere un differente modo di organizzare le cose: questo è ciò che viene chiamato file system.

I FILE SYSTEM

Un file system serve prima di tutto a ritrovare le informazioni all'interno della nostra immensa mole di dati, nella stessa maniera in cui l'indice di un libro di cucina permette di andare direttamente alla pagina giusta per leggere la ricetta per una cena.

Attenzione però che eliminare un file è come tirare una riga sopra uno degli argomenti dell'indice. Sfogliando tutte le pagine del libro di può ancora ritrovare la nostra ricetta finché la pagina non viene sovrascritta. Ma di questo parleremo meglio più in là.

Si possono inventare migliaia di formati diversi per organizzare i dati, e di conseguenza esistono

molti tipi diversi di file system. Quando si parla di formattazione ci si riferisce alla creazione di un file system su un supporto.

Dato che è il sistema operativo a fornire l'accesso ai dati, il file system è spesso legato strettamente a un particolare sistema operativo.

Per citarne qualcuno: NTFS e FAT32 sono quelli in genere usati per i sistemi operativi Windows; gli ext (ext3, ext4) sono spesso utilizzati sotto GNU/Linux; gli HFS, HFS+ e HFSX sono usati da Mac OS X.

È però anche possibile leggere un sistema operativo "estraneo" al sistema che si sta utilizzando, tramite un software adeguato. Windows per esempio è capace di leggere una partizione ext3, se si installa un software appropriato.
Una delle conseguenze di questa cosa è che su un computer possono esistere degli spazi di

archiviazione non riconosciuti dal sistema operativo, ai quali non si può dunque accedere facilmente.

I FORMATI DEI FILE

I dati che manipoliamo sono generalmente raggruppati sotto forma di file. Un file ha un contenuto e anche un nome, una posizione (la cartella in cui si trova), una dimensione e altri dettagli a seconda del tipo di file system utilizzato.

Ma all'interno di ciascun file, i dati sono a loro volta organizzati diversamente a seconda della loro natura e del software usato per modificarli. Per differenziarli si parla di formati dei file.
In genere si mette alla fine del nome di un file codice, che chiamiamo talvolta estensione, che permette di indicare il formato del file. Si può scegliere un'estensione o un'altra, modificarla, ma questo è più che altro a titolo indicativo, e non significa che cambiandola si cambi anche il formato del file.

Facciamo qualche esempio di estensione: per la musica, si usano spesso i formati mp3 o ogg, per i documenti di testo di LibreOffice si usa OpenDocumentText (ODT), per le immagini si può scegliere tra JPEG, ONG o altri, etc.

Così come i software, anche i formati possono essere proprietari. I formati aperti sono definiti pubblicamente per impedire, tra le altre cose, che il loro utilizzo sia ristretto a un solo programma.

Certi formati proprietari vengono analizzati con la lente d'ingrandimento per poter essere utilizzati da altri programmi, ma la loro comprensione resta spesso imperfetta. È il tipico caso del vecchio formato di Microsoft Word (DOC) o quello di Adobe Photoshop (PSD).

Normalmente, tutti i dati ai quali il processore deve accedere, e quindi tutti i programmi e i documenti aperti, dovrebbero trovarsi dentro alla memoria volatile.

LA MEMORIA VIRTUALE (SWAP)

Ma per riuscire ad aprire un sacco di programmi e di documenti contemporaneamente, i sistemi operativi moderni hanno un trucco: quando è necessario scambiano dei pezzi di RAM con uno spazio all'interno dell'hard-disk dedicato a questo scopo. Si parla in questo caso di "memoria virtuale" o di swap.

Il sistema operativo arrangia insomma le cose in modo che il processore abbia sempre nella memoria viva i dati ai quali vuole realmente accedere. La swap è anche esempio di spazio di archiviazione al quale in genere non si pensa, memorizzato sull'hard-disk sia sotto forma di un grosso file attiguo (sotto Microsoft Windows e talvolta anche sotto Linux) sia in una partizione a parte (con Linux).

Torneremo in seguito sui problemi che pongono queste richieste di formato e spazio in termini riservatezza dei dati.

TRACCE DA TUTTE LE PARTI

Il normale funzionamento di un computer lascia numerose tracce di tutte quelle operazioni che ci facciamo sopra. A volte, queste tracce sono informazioni necessarie al suo funzionamento, altre volte vengono raccolte per permettere ai software di essere “più pratici”.

NELLA RAM

Abbiamo visto come il primo luogo di archiviazione delle informazioni su un computer sia la RAM.

Quando il computer è sotto tensione elettrica, la RAM contiene tutte le informazioni di cui si ha bisogno. Conserva dunque necessariamente le numerose tracce: ciò che viene digitato sulla tastiera (comprese anche le password), le schede aperte, i diversi avvenimenti che hanno ritmato la fase di avvio del computer. Prendendo in mano un computer acceso, non è molto difficile tirarne fuori l’insieme delle informazioni contenute dentro la RAM, salvandole per esempio in una

chiave USB o inviandole a un altro computer attraverso la rete. E impadronirsi di un computer può essere talmente semplice che può venire fatto anche collegandocisi attraverso un iPod mentre siamo girati di spalle (di questo caso se ne parla qui: Maximillian Dornseif, 2004, 0wned by an iPod. Bruce Schneier, 2006, Hacking Computers Over USB - http://nbl.gs/qhH). Una volta recuperate, le numerose informazioni che contiene la RAM possono essere sfruttate ad esempio per conoscere ancora meglio le persone che usano quel computer.

Quando si spegne l'alimentazione questi dati diventano illeggibili. Ma ci vuole un po' di tempo, il che potrebbe bastare per una persona mal intenzionata a recuperarne il contenuto. Questa operazione è chiamata "cold boot attack": l'idea è quella di copiare il contenuto della RAM prima che abbia il tempo di cancellarsi, in modo da sfruttarlo in seguito. È anche tecnicamente possibile portare la memoria di un computer appena spento a una temperatura molto bassa –

nel qual caso se ne riesce a conservare il suo contenuto per ore o persino giorni (Per approfondire: J. Alex Halderman et Al., 2008, Least We Remember: Cold Boot Attacks on Encryption Keys - http://nbl.gs/qhI).

Questo attacco deve essere eseguito però subito dopo lo spegnimento. Inoltre, se utilizziamo alcuni software di grandi dimensioni (ad esempio ritoccando un'immagine enorme con Adobe Photoshop o GIMP) prima di spegnere il computer, è probabile che le tracce che erano state precedentemente lasciate nella RAM vengano scoperte. E' importante sapere che esistono dei software appositamente progettati per sovrascrivere il contenuto della RAM con dati casuali.

NELLA MEMORIA VIRTUALE

Il sistema operativo utilizza, in alcuni casi, una parte del disco rigido per aiutare la RAM. Ciò accade sopratutto se il computer è molto utilizzato, ad esempio quando si lavora su

immagini di grandi dimensioni, ma anche in molti altri casi, in maniera imprevedibile.
La conseguenza più imbarazzante di questo sistema, seppur molto pratico, è che il computer scrive sul disco rigido le informazioni contenute nella RAM… informazioni potenzialmente sensibili, quindi, che rimarranno leggibili anche dopo aver spento il computer.
Con un computer configurato in modo standard, è quindi illusorio credere che un documento letto da una chiave USB, aperta anche con un software portatile non lasci mai tracce sul disco rigido.
Per impedire a chiunque di accedere a questi dati, è possibile utilizzare un sistema operativo configurato per cifrare la memoria virtuale. Ne parleremo prossimamente.

STANDBY E IBERNAZIONE

La maggior parte dei sistemi operativi consente di "mettere in pausa" un computer. Viene utilizzato principalmente con i computer portatili, ma è

ugualmente valido anche per i computer fissi.

◦ **Standby** - Lo standby spenge i componenti principali del computer mantenendo il computer acceso in modo da poterlo riaccendere rapidamente. Come minimo, la RAM continuerà ad essere alimentata per conservare tutti i dati su cui stavamo lavorando, tra cui password e chiavi di cifratura. In breve, un computer in standby protegge l'accesso ai dati tanto quanto un computer acceso.

◦ **Ibernazione** - L'ibernazione o sospensione consiste nel salvaguardare l'integralità della RAM sul disco rigido per poi spegnere completamente il computer. Al successivo avvio, il sistema operativo rileverà la sospensione, ricopierà il backup nella RAM e inizierà a lavorare di nuovo partendo da lì.

Nei sistemi GNU/Linux, la memoria viene solitamente copiata nella swap. Su altri sistemi in un file di grandi dimensioni, spesso nascosto.

Dal momento che è il contenuto della RAM ad

essere scritto sul disco rigido, questo significa che tutti i programmi e documenti aperti, le password, le chiavi di cifratura e altro, possono essere trovati da chiunque accederà al disco rigido. Questo, finché non ci si riscriverà sopra.
Tuttavia, nel caso di cifratura dell'hard-disk questo rischio è limitato: per accedere al backup della RAM verrà chiesta una password.

I LOG

I sistemi operativi hanno una forte tendenza a scrivere nel loro "diario di bordo" una storia dettagliata di ciò che producono.
I log sono proprio questo: dati utili per il funzionamento del sistema operativo, che possono essere utilizzati per correggere problemi di configurazione o altri bug.
Tuttavia, la loro esistenza a volte può essere problematica. Gli scenari esistenti sono moltissimi, ma gli esempi che seguono dovrebbero essere sufficienti a dare un'idea del rischio:

- Con GNU/Linux, ogni volta che viene acceso un computer, il sistema mantiene la data, l'ora e il nome dell'utente che accede;
- Con GNU/Linux, sono di solito conservati la marca e il modello di ciascun supporto rimovibile (disco esterno, chiavetta USB ...) che è stato collegato;
- Con Mac OS X, si conservano le date in cui si è stampato e il numero di pagine;
- Con Windows, il registro di sistema si salva il nome del software, la data e l'ora di installazione o disinstallazione di un'applicazione.

SALVATAGGIO AUTOMATICO E ALTRE ATTIVITÀ PIANIFICATE

Oltre ai log, è possibile che altre tracce di file, anche cancellate, rimangano sul computer. Anche se i file e il loro contenuto sono stati rimossi, parte del sistema operativo o un altro programma potrebbero averne conservata una copia deliberatamente. Ecco alcuni esempi:

- Utilizzando Windows, Microsoft Office può mantenere nel menu “documenti recenti” il riferimento al nome del file già cancellato e talvolta anche mantenere file temporanei con il contenuto del file in questione;
- Con GNU/Linux, un file vecchio può contenere al suo interno il riferimento al nome di un file precedentemente cancellato. E LibreOffice può conservare tutte le tracce di un file cancellato allo stesso modo di Microsoft Office. In pratica, ci sono dozzine di programmi che funzionano in questo modo;
- Quando si utilizza una stampante, il sistema operativo copia spesso il file in sospeso nella “coda di stampa”. Il contenuto di questo file, una volta completata la fase di stampa, non sarà scomparso dall’hard-disk;
- Con Windows, quando si collega un’unità rimovibile (chiave USB, disco rigido esterno, CD o DVD), il sistema inizia spesso esplorandone il contenuto per poi poter fornire un software adattato alla sua lettura: questa esplorazione

automatica lascia in memoria l'elenco di tutti i file presenti sul supporto utilizzato, anche se nessuno dei file è stato consultato.

È difficile trovare una soluzione adeguata a questo problema. Un file, anche se perfettamente cancellato, probabilmente continuerà a esistere sul computer per un po' di tempo anche in una forma diversa. Una ricerca sui dati grezzi del disco consentirebbe di vedere se esistono copie di questi dati o meno … a meno che non siano stati solo linkati o memorizzati in una forma diversa, compressi per esempio.
Solo la sovrascrittura dell'intero disco e l'installazione di un nuovo sistema operativo possono garantire che le tracce di un file vengano eliminate. E da un'altra prospettiva, l'uso di un sistema live in cui il team di sviluppo abbia prestato molta attenzione a questo problema, assicura che queste tracce non vengano lasciate altrove tranne che nella RAM. Torneremo prossimamente sull'argomento.

Oltre alle informazioni contenute in un file, vi sono informazioni che lo accompagnano di cui possiamo non accorgerci a prima vista: data di creazione, nome del software, computer, ecc. Questi “dati riguardo ai dati” sono comunemente chiamati “metadati”.

Una parte dei metadati viene salvata nel file system: il nome del file, la data e l’ora di creazione e modifica e spesso molte altre cose. Queste tracce sono lasciate sul computer - e questo di per sé potrebbe già essere un problema - ma generalmente non vengono salvate nel file.

D’altra parte, molti formati di file memorizzano anche i metadati all’interno del file stesso. Saranno quindi trasmessi durante un’eventuale copia su una chiave USB o quando si invia una e-mail o nella pubblicazione online. Queste informazioni possono essere note a chiunque abbia accesso al file.

I metadati registrati dipendono dai formati e dal

software utilizzati. La maggior parte dei file audio consente di registrare il titolo del brano ed eseguire la canzone. I programmi di scrittura o i PDF registreranno il nome dell'autore, la data e l'ora della creazione e talvolta persino la cronologia completa delle ultime modifiche e quindi, potenzialmente, le informazioni che si pensava fossero state eliminate. (Per approfondire: Deblock Fabrice, 2006, Quando i documenti Word tradiscono la fiducia. - http://nbl.gs/qhJ)

Formati immagine come TIFF o JPEG, file fotografici creati da una fotocamera digitale o da un telefono cellulare, contengono metadati EXIF. Questi possono contenere la marca, il modello e il numero di serie del dispositivo utilizzato, ma anche la data, l'ora e talvolta le coordinate geografiche dello scatto, per non parlare di una versione in miniatura dell'immagine. Sono questi metadati che metteranno fine alla latitanza di John McAfee, fondatore ed ex capo della società di sicurezza informatica con lo stesso nome. (Per

approfondimenti: Big Browser, 2012, vizio di forma – la bufala che ha portato all'arresto di John McAfee - http://nbl.gs/qhK). Tutte queste informazioni tendono a rimanere dopo aver utilizzato un software di foto ritocco. Il caso dell'anteprima in miniatura è particolarmente interessante: molte foto disponibili su Internet contengono ancora l'intera foto da cui è stato fatto il ritaglio … e con le facce dietro sfocate. (Maximillian Dornseif et Steven J. Murdoch, 2004, Hidden Data in Internet Published Documents - http://nbl.gs/qhL).

Per la maggior parte dei formati di file aperti, tuttavia, esiste un software per esaminare ed eventualmente eliminare i metadati. Ne parleremo nei prossimi capitoli della Guida.

SOFTWARE MALEVOLI, INTRUSI E ALTRI SPIONI

Oltre alle tracce che l'intero sistema operativo lascia mentre sta girando, sui nostri computer possono esserci anche svariati intrusi. A volte installati a nostra insaputa (e che permettono per esempio di deviare i log altrove), a volte inclusi invece nel software che abbiamo installato.

Questi informatori possono far parte di tecniche di sorveglianza, dalla "lotta alla pirateria" dei software proprietari, alla schedatura mirata di un individuo, passando per la raccolta dati per fare spam o altre truffe.

La portata di questi dispositivi aumenta fortemente quando il computer è collegato a Internet. La loro installazione in questo caso è enormemente più facile se non si fa niente per proteggersi, e il recupero dei dati collezionati può essere fatto a distanza.
Coloro che raccolgono queste informazioni però non sono pericolosi tutti alla stessa maniera:

dipende dai casi, dalle motivazioni e dai mezzi. Gli autori di violenze domestiche (1), i siti Internet in cerca di consumatori, le multinazionali come Microsoft, la polizia di Saint-Tropez, o la National Security Agency… così come tante altre persone e strutture spesso in concorrenza tra loro e che non formano certo una totalità coerente.

Per introdursi nel nostro computer non hanno acceso agli stessi passe-partout e non sono tutti in grado di usare il piede di porco così bene: per esempio, lo spionaggio industriale è una delle cause più importanti della sorveglianza più o meno legale e malgrado le apparenze (2), non dobbiamo credere che Microsoft ceda tutti i propri trucchi alla polizia francese.

Note
(1) Catherine Armitage, 2014, “Spyware’s role in domestic violence” parla dell’utilizzo di malware e altri strumenti tecnologici da parte di autori di violenze domestiche – http://nbl.gs/qgw

(2) Microsoft, in partnership con l'Interpol, ha costruito una suite di strumenti chiamata COFEE (Computer Online Forensic Evidence Extractor) messa a disposizione delle polizie di una quindicina di paesi.
Korben, 2009, Cofee – La clé sécurité de Microsoft vient d'apparaitre sur la toile. – http://nbl.gs/qgx

CONTESTO LEGALE

In ogni caso, gli sbirri e i servizi di sicurezza francesi dispongono al momento dei mezzi per mettere in atto sorveglianza informatica molto completa in piena legalità, appoggiandosi ai diversi "informatori" che presentiamo qui di seguito.
[NDT: La situazione italiana da questo punto di vista presenta analogie e differenze rispetto all'attualità francese qui raccontata. Il che meriterebbe un discorso ben più approfondito di quello che possiamo fare in poche righe. Per farvi

un'idea di come siamo messi in Italia al momento riguardo malware e dintorni, potete ascoltare questa puntata di Le dita nella presa, andata in onda su Radio Onda Rossa. – http://nbl.gs/qgy]

La legge "di rinforzo alla lotta contro il crimine organizzato, il terrorismo e il loro finanziamento, e per migliorare l'efficacia e la garanzia della procedura penale" del 2016 include delle disposizioni di legge per consentire di installare dei captatori (1) che registrino e comunichino ciò che appare sullo schermo o ciò che le diverse periferiche (tastiera, webcam, scanner, telefono…) trasmettono al computer. L'installazione di questi captatori viene autorizzata ad essere effettuata da remoto o penetrando nel domicilio della persona sorvegliata per piazzare i software necessari. Queste misure non si applicano soltanto ai reati rilevanti di "terrorismo", (come ad esempio quello di "proliferazione di armi di distruzione di massa"), ma anche a certi reati commessi da più persone (i

reati “associativi”). Si può andare dal concorso nella “circolazione e soggiorno irregolare di uno straniero in Francia” passando per la “distruzione, degradazione e deterioramento di un bene”, ma anche in caso di semplice richiesta da parte del Procuratore della Repubblica per “urgenza risultante da un rischio imminente di contaminazione delle prove o di grave attentato persone o beni”.

La legge sull’informazione in Francia del 2015 dà più o meno gli stessi poteri ai “servizi informativi specializzati” per la “ricerca, la raccolta, lo sviluppo e la messa a disposizione del Governo di informazioni relative a problemi geopolitici e strategici oltre che a minacce e a rischi suscettibili di minacciare la vita della Nazione”.

Note:
(1) Usiamo qui il termine “captatore” come viene usato nell’ambito legale, istituzionale e giornalistico in Italia, spesso in modo generico e

poco chiaro: per captatore si intende uno strumento informatico pensato per facilitare l'investigazione e l'accumulo di prove digitali nell'ambito di un'indagine. Potremmo semplificare chiamandolo "malware" o "virus", visto che tecnicamente non esiste una vera e propria differenza con questo tipo di oggetto. Ma certamente il termine "virus" è ammantato di un'aura malefica e teppista, mentre "captatore" ha un che di decisamente più rassicurante e burocratico. - NDT

I SOFTWARE MALEVOLI

I software malevoli (1) (spesso chiamati malware) sono dei programmi sviluppati con l'intento di nuocere: raccolta di informazioni, possesso di informazioni illegali, inoltro di spam, etc. I virus, i worm, i trojan, gli spyware, i rootkit (software che consentono di prendere il controllo di un computer) e i keylogger fanno parte di questa famiglia. Alcuni di questi programmi

possono appartenere a più di queste categorie contemporaneamente.

Per riuscire a installarsi su un computer, alcuni software malevoli sfruttano delle vulnerabilità del sistema operativo (2) o delle applicazioni. Si appoggiano su degli errori di progettazione o di programmazione per ribaltare il funzionamento dei programmi a proprio vantaggio. Purtroppo sono state trovate molte di queste “falle di sicurezza” in molti software, e nuove ne vengono costantemente trovate, sia da chi cerca di correggerle, sia da chi vuole sfruttarle.

Un altro metodo corrente è quello di invogliare le persone che utilizzano un computer a lanciare il software malevolo nascondendolo all’interno di un programma apparentemente inoffensivo. È così che un semplice link a un video postato su un social network legato alla rivoluzione siriana ha portato di fatto gli utenti a scaricarsi un virus contenente un keylogger (3). In questo caso

l'attaccante non è obbligato a trovare delle vulnerabilità gravi nei software odierni. È particolarmente difficile assicurarsi che dei computer condivisi da diverse persone oppure dei computer che si trovano in luoghi pubblici come una biblioteca o un Internet point, non siano stati compromessi: è sufficiente che una sola persona un po' meno attenta si sia fatta fregare..

Inoltre, la maggior parte dei software malevoli "seri" non lascia tracce immediatamente visibili della propria presenza, e possono essere difficili da scoprire. Il caso senza dubbio più complicato è quello delle vulnerabilità non ancora note, chiamate "zero day", e che i software di antivirus non sono grado di riconoscere, perché non ancora inventariate. È proprio una di queste vulnerabilità "zero day" che l'azienda VUPEN ha venduto alla NSA nel 2012 (4).
Nel 2006, Joanna Rutkowska ha presentato nel corso della conferenza Black Bar il malware

“Blue Pill”. Questa presentazione dimostrava che era possibile scrivere un rootkit che sfruttasse le tecnologie di virtualizzazione per ingannare il sistema operativo e rendere in questo modo veramente difficile identificare la presenza del malware, una volta scaricato.

Questi software possono rubare le password, leggere documenti salvati sul computer (anche i documenti cifrati, se sono stati decifrati sul momento), neutralizzare i dispositivi di anonimato su Internet, catturare degli screenshot e nascondersi dagli altri programmi. Ma possono anche utilizzare il microfono, la webcam o altre periferiche del computer. Esiste un vero e proprio mercato specializzato dove si possono comprare questo tipo di programmi, personalizzati per differenti obiettivi.

Questi software permettono di effettuare numerose operazioni: ottenere numeri di conti bancari, password degli account Paypal, di

inviare spam, di partecipare all'attacco di un server saturandolo di richieste, etc. Ma sono anche molto efficaci per spiare organizzazioni o individui specifici.

Per fare un esempio dagli Emirati Arabi, un attivista per i diritti umani Ahmed Mansour, è stato vittima di un attacco condotto sul proprio smartphone. Gli è stato inviato un sms che conteneva un link a un virus. Questo virus permetteva alla persona che lo controllava di utilizzare in ogni istante la videocamera, il microfono e di sorvegliare le attività del telefono della vittima. L'attacco è stato scoperto e neutralizzato grazie a Citizen Lab. (5)

I servizi investigativi e gli sbirri francesi hanno il diritto di utilizzare questo tipo di software, il che vuol dire che quasi sicuramente ne dispongono. Una suite di software di spionaggio, attribuita ai servizi, è stata trovata per esempio soprattutto in Iran (6).

Nessuno è in grado di sapere quanti computer sono al momento infettati da software malevoli, ma alcuni ritengono si tratti di una cifra che va dal 40 al 90% delle installazioni di Windows. Quindi è altamente probabile trovarne uno sul primo Windows che incroceremo. Fino ad oggi, usare un sistema operativo minoritario (come Gnu/Linux) diminuisce significativamente i rischi di infezione poiché, essendo meno richiesti, lo sviluppo di malware specifici risulta meno vendibile.

Possiamo intanto suggerire qualche metodo per limitare i rischi:
non installare (o non utilizzare) software di provenienza sconosciuta: non dare fiducia al primo sito web che si incontra (7); prendere sul serio, ovvero considerare un minimo, gli avvisi dei sistemi operativi recenti che tentano di mettere in guardia l'utente quando utilizza un software poco sicuro, o quando dicono che è necessario un aggiornamento di sicurezza;

infine, limitare le possibilità di installazione di nuovo software: riducendo l'uso dell'utente "amministratore" e le varie persone che ne hanno accesso.

Note:
(1) Tutta questa parte è fortemente ispirata dal passaggio dedicato alla questione nella Surveillance Self-Defense Guide de l'Electronic Frontier Foundation. – http://nbl.gs/qgz
(2) Secondo l'Internet Storm Center, nel 2016, un'installazione di Microsoft Windows dove non erano stati fatti gli aggiornamenti di sicurezza era in grado di resistere alla compromissione circa sette ore da quando veniva connessa direttamente a Internet. – http://nbl.gs/qh0
(3) Eva Galperin et Al., 2014, Quantum of Surveillance: Familiar Actors and Possible False Flags in Syrian Malware Campaigns – http://nbl.gs/qh2 (pdf)
(4) Grégoire Fleurot, 2013, Espionnage: Vupen, l'entreprise française qui bosse pour la NSA. –

http://nbl.gs/qh3

(5) Andréa Fradin, 2016, « Pegasus », l'arme d'une firme israélienne fantôme qui fait trembler Apple. – http://nbl.gs/qh4

(6) Martin Untersinger, 2015, Dino, le nouveau programme-espion développé par des francophones, Le Monde.fr. – http://nbl.gs/qh5

(7) Questo consiglio vale anche per le persone che utilizzano Gnu/Linux. Nel dicembre 2009, il sito gnome.look.org ha diffuso un malware presentato come uno screensaver . Il software era scaricabile sotto forma di pacchetto Debian in mezzo a mille altri scrensaver e sfondi. – http://nbl.gs/qh6

HARDWARE PER LO SPIONAGGIO

Gli attaccanti che vogliono mettere le mani sui segreti contenuti all'interno dei nostri computer, come abbiamo visto, possono utilizzare dei software malevoli, ma possono anche usare dell'hardware che non ha niente da invidiare al

buon vecchio James Bond.
Esiste tutta una gamma di strumenti più o meno facilmente disponibili che permette l'intrusione o l'esfiltrazione di informazioni a praticamente tutti i livelli di un computer. In seguito alla pubblicazione da parte di Edward Snowden di documenti confidenziali della NSA, è stato pubblicato un vero e proprio catalogo di spionaggio informatico sul quotidiano tedesco Der Spiegel (1).

Senza poterli elencare in modo esaustivo, all'interno di questo catalogo scopriamo un po' a caso falsi connettori USB che permettono di ritrasmettere sotto forma di onde radio quello che transita tramite loro, minuscole cimici installate nei cavi che collegano il monitor o la tastiera al computer, in modo da poter intercettare a distanza ciò che scriviamo o vediamo. E poi una valanga di materiale da spionaggio installato sul computer, sull'hard disk, sul bios etc.

Il quadro non è molto incoraggiante e una seria revisione del proprio computer comporterebbe smontarlo da cima a fondo, con poche possibilità di essere in grado poi di riuscire a farlo funzionare di nuovo. Detto ciò, questi strumenti non sono a disposizione di ogni tipo di avversario. Inoltre non c'è niente che ci induca a pensare che l'uso di tali strumenti sia diventato abituale, vuoi per ragioni di costo, di installazione o altro.

In ogni caso ci addentreremo lo stesso un po' sul caso dei keylogger, che rientrano sia nella categoria degli strumenti di spionaggio, che in quella dei software malevoli.

1) Spiegel, 2013, Interactive Graphic: The NSA's Spy Catalog- http://nbl.gs/qh7

I KEYLOGGER

I keylogger, che possono essere sia hardware che software, hanno lo scopo di salvare di

nascosto tutto quello che viene digitato sulla tastiera di un computer per poi poterlo ritrasmettere all'agente o alla persona che li ha installati.

Una volta piazzati, la loro capacità di salvare, tasto dopo tasto, tutto quello che viene digitato sulla tastiera gli permette di aggirare ogni dispositivo di cifratura e di accedere direttamente a password, passphrase e altri dati sensibili.

I keylogger hardware sono dei dispositivi collegati alla tastiera o al computer. Possono assomigliare a degli adattatori, a delle schede d'estensione all'interno del computer (PCI o mini-PCI) o integrarsi dentro la tastiera (tanto per farsi un'idea, molti modelli sono in libera vendita a una somma che va dai 40 ai 100 dollari). Quindi, se non li si cerca specificatamente, sono difficili da scovare.
Nel caso di una tastiera wi-fi, per ricostruire quali tasti sono stati premuti non c'è neanche bisogno

di un keylogger: si intercettano le onde radio emesse dalla tastiera per comunicare con il ricevitore e poi si rompe la chiave di cifratura utilizzata, che nella maggior parte dei casi è abbastanza debole. Da una distanza minore è anche possibile registrare e decodificare le onde elettromagnetiche emesse dalle tastiere via cavo, compreso quelle integrate nel portatile..

I keylogger software sono molto più diffusi, perché possono essere installati a distanza (tramite un sito internet, attraverso un software malevolo, o altro) e generalmente per il recupero dei dati raccolti non richiedono un accesso fisico alla macchina (l'invio si può fare per esempio periodicamente via mail). La maggior parte di questi software registrano anche il nome dell'applicazione che sta girando, la data e l'ora in cui è stata eseguita e i tasti che sono stati digitati durante il suo uso.
Negli Stati Uniti, l'FBI utilizza da molti anni i keylogger software (1).

L'unico modo per individuare un keylogger hardware è quello di familiarizzare con questi dispositivi e di fare regolarmente una verifica visiva della propria macchina, all'interno e all'esterno. Anche se il catalogo della NSA pubblicato alla fine del 2013, ci fa rendere conto di quanto sia difficile essere in grado di accorgersi di un keylogger appena più grande di un'unghia. Nel caso dei keylogger software, le strade da battere sono le stesse degli altri software malevoli.

1) Nel 2000, l'utilizzo di un keylogger ha permesso alla FBI di ottenere la passphrase usata da un tramite della mafia di Filadelfia per cifrare i propri documenti – http://nbl.gs/qh8

PROBLEMI DI STAMPA?

Sembrerebbe quasi di aver fatto il giro di tutte le sorprese che i nostri computer possono riservarci.. ma invece ci si mettono anche le stampanti ad avere i loro piccoli segreti.

UN PO' DI STEGANOGRAFIA

Prima cosa da sapere: molte stampanti di fascia alta firmano il proprio lavoro (1). Questa firma steganografica, chiamata watermarking, si basa su dettagli di stampa molto leggeri, spesso invisibili ad occhio nudo, e vengono inseriti su ciascun documento. Permettono di identificare in modo certo la marca, il modello e in certi casi il numero di serie della macchina che ha stampato. Si capisce bene il motivo per cui questi dettagli stanno lì: per poter risalire alla macchina a partire dai documenti.

Tant'è vero che la persona che aveva diffuso nel giugno 2017 dei documenti top secret della NSA sull'inquinamento delle elezioni negli Stati Uniti del 2016 da parte di hacker russi, è stata beccata. C'erano ancora i marchi della stampante usata per stampare i documenti riservati quando li hanno pubblicati sul giornale The Intercept (2).

Inoltre, ci sono altre tracce lasciate sui documenti a causa dell'usura della macchina – e questo succede con tutte le stampanti. Con l'età le testine di stampa si spostano, appaiono leggeri errori, i pezzi si usurano e tutto questo va a formare una vera e propria firma della stampante. Proprio come la balistica permette di identificare un'arma a fuoco a partire da un proiettile, è possibile utilizzare questi difetti per identificare una stampante a partire dalle pagine che fa uscire.

Per proteggersi in parte da questa cosa, è interessante sapere che i dettagli di stampa non resistono a una fotocopia ripetuta: fotocopiare la pagina stampate, poi fotocopiare la fotocopia ottenuta, consente di far sparire questi marchi. Ma d'altra parte…. ne lasceremo sicuramente altri, le fotocopiatrici presentano dei difetti e talvolta dei marchi steganografici, simili a quelli delle stampanti. Insomma è un cane che si

morde la coda e il problema diventa più che altro scegliere quali tracce si vogliono lasciare..

Note:
1) L' Electronic Frontier Foundation cerca di mantenere una lista dei costruttori e dei modelli di queste stampanti indiscrete – http://nbl.gs/qh9
2) Robert Graham, 2017, How The Intercept Outed Reality Winner – http://nbl.gs/qhA

LA MEMORIA, ANCORA...

Alcune stampanti sono sufficientemente "evolute" da assomigliare più a un vero e proprio computer piuttosto che a un timbro.
Queste possono porre problemi anche a un altro livello, visto che sono dotate di memoria viva: questa memoria, proprio come quella di un PC, conserverà la traccia dei documenti che sono stati trattati per tutto il tempo in cui la macchina è attaccata alla corrente… o finché un altro documento non copre quella traccia.

La maggioranza delle stampanti laser dispongono di una memoria viva che può contenere una dozzina di pagine. I modelli più recenti o quelli che comprendono uno scanner integrato, possono invece contenere diverse migliaia di pagine di testo..

Ancora peggio: alcuni modelli, spesso utilizzati per le grosse tirature come quelle delle copisterie, hanno a volte degli hard disk interni ai quali l'utente non ha accesso e che conservano anch'essi delle tracce – e in questo caso, anche dopo essere staccati dalla corrente.

Nel prossimo numero:
Qualche illusione di sicurezza - Un metodo per proteggersi la crittografia...

Quello che avete tra le mani è il terzo numero della traduzione a puntate della Guide d'autodéfence numerique.
L'edizione originale integrale (in francese) è leggibile online e scaricabile liberamente qui:
http://guide.boum.org
Trovate invece le puntate precedenti della traduzione in italiano qui:
http://numerique.noblogs.org