FermoLUG News

La Newsletter del FermoLUG Agosto 2017 - Numero 21

Indice

Guida essenziale ai neofiti

Per chi si avvicina la prima volta al sistema operativo libero d'eccellenza GNU/Linux non è così semplice afferrarne subito la sua potenza e semplicità; l'articolo propone le 3 cose basilari da conoscere per chi proviene dal sistema proprietario Microsoft Windows.

Pagina 2

Scopriamo #BadTunnel

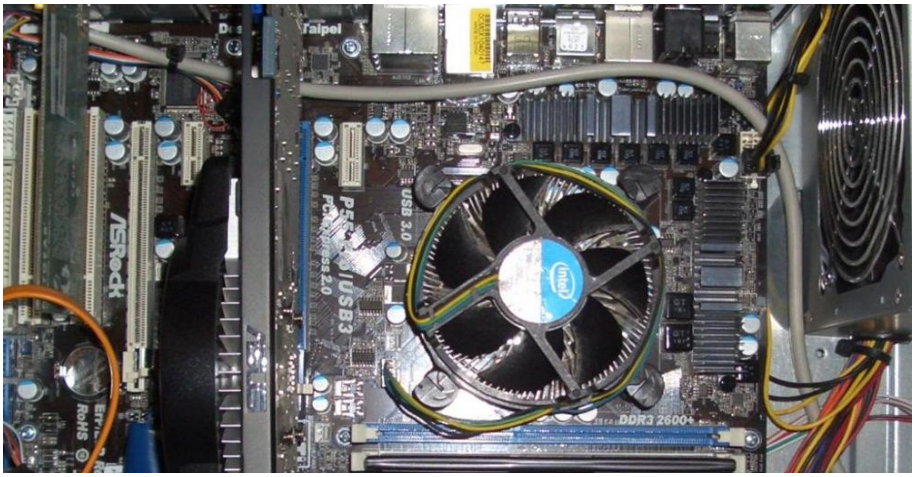
La vulnerabilità #BadTunnel è una tecnica che permette di avere accesso al traffico che passa sul network di un sistema operativo Microsoft Windows oltrepassando Firewall e NAT di rete.

Pagina 3

Autori cercasi!

Se ti piace scrivere articoli e recensioni, FermoLUG News ti sta cercando! Invia il tuo materiale a:

info@linuxfm.org



Il virus è stato inventato da un gruppo di ricercatori dell'università israeliana Ben Gurion: riesce a spiare anche dispositivi completamente isolati

Il malware che ruba i dati dal computer ascoltando le ventole

Un gruppo di ricercatori dell'università israeliana Ben Gurion (la stessa università in cui è stato scoperto il bug per scaricare i film con Chrome (http://www.lastampa.it/2016/06/25/tecnologia/news/un-bug-di-chrome-consente-di-scaricare-i-film-da-netflix-soDmVmtS5cBfpoIR00moUJ/pagina.html)) ha sviluppato un malware in grado di sottrarre dati anche a computer completamente isolati da internet, ascoltando il rumore prodotto dalle ventole e dalla CPU. Il malware, battezzato Fansmitter, è stato presentato in una ricerca appena pubblicata (https://arxiv.org/ftp/arxiv/papers/1606/1606.05915.pdf).

A differenza di altri virus simili, in grado di rubare dati a computer ascoltando le onde sonore emesse dagli amplificatori, Fansmitter può colpire anche dispositivi non solo «air-gapped» (non connessi a internet e isolati dagli altri), ma privi di speaker, webcam o qualunque altro hardware.

Una volta che il malware è stato installato, per esempio attraverso una chiavetta USB, è sufficiente sistemare uno smartphone, o un altro dispositivo dotato di microfono, nei dintorni del computer per poterlo spiare. I ricercatori sono riusciti a sottrarre dati a un computer posizionato a otto metri di distanza, trasferendoli a 900 bit/ora. Una velocità troppo bassa per trasportare file di medie dimensioni, ma sufficiente per sottrarre password o altri codici criptati.

Il malware può spiare qualunque dispositivo, analizzando la rotazione e la potenza del rumore prodotto da ventole di diverso tipo e dimensioni e convertendole in onde sonore che vengono decifrate dal dispositivo di ascolto. Ci sono alcune contromisure possibili, si spiega nella ricerca: software in grado di rilevare i virus in azione sui dispositivi o ventole estremamente silenziose. Nessuna delle soluzioni presentata si è dimostrata efficace al 100 per cento, ma intanto cominciano già a diffondersi computer senza ventole. - Andrea Signorelli - Fonte: http://www.lastampa.it/2016/06/27/tecnologia/idee/il-malware-che-ruba-i-dati-dal-computer-ascoltando-le-ventole-7pLh1iRy2pINnw2b0JmJkM/pagina.html

3 cose su Linux che l'utente Windows dovrebbe sapere

La stragrande maggioranza di utilizzatori di personal computer ha avuto davanti sempre e solo sistemi operativi Microsoft (DOS prima, Windows poi). L'utente medio è quindi generalmente portato a pensare che esista un unico modo di usare un computer e un unico modo di fare le cose, e che un computer possa fare tutto e solo quello che il proprio sistema fa e se non lo fa è perché non si può fare.

Davanti a una dimostrazione delle funzionalità di uno dei tanti sistemi (liberi) basati su Linux, generalmente l'utente in questione resta sempre abbastanza spiazzato. I commenti più frequenti sono: "non lo sapevo!", insieme a: "credevo che fosse difficile da usare!", chiari sintomi di ignoranza (il primo) e pregiudizio o disinformazione (il secondo). Cercheremo dunque di predisporre qui una mini-terapia d'urto in tre pillole per affrontare la fase acuta della malattia. Per un trattamento più accurato si rimanda alla sterminata documentazione sull'argomento reperibile in rete, in libreria o presso i gruppi (LUG, Linux User Group) locali sparsi per tutto lo stivale.

Distribuzione, non un semplice sistema operativo

Di solito compriamo un computer già pronto all'uso, "chiavi in mano". Windows è quasi sempre preinstallato in fabbrica (tra l'altro con una licenza di tipo "OEM", cioè legata all'hardware e quindi non trasferibile ad un altro computer nel caso si voglia cambiare macchina). Spesso chiediamo al venditore di installarci (più o meno legalmente a seconda dell'onestà delle parti) tutto quello che ci serve, per cui non sempre sappiamo esattamente cosa abbiamo comprato, quali strumenti facciano parte della dotazione di Windows e quali siano stati aggiunti successivamente. In realtà Windows, da solo, è dotato di pochissimi strumenti preinstallati, per cui appena aperta la scatola si potrà al massimo navigare in internet, ascoltare musica o vedere delle foto. Windows è quindi "solo" poco più che un sistema operativo (https://it.wikipedia.org/wiki/Sistema_operativo). Tutte le applicazioni che vi servono devono essere installate successivamente, una per una, scaricando i file di installazione dai relativi siti o inserendo di volta in volta CD o DVD.

I sistemi basati su Linux, invece, sono ben più che semplici sistemi operativi. Essi sono disponibili sotto forma di distribuzioni (https://it.wikipedia.org/wiki/Distribuzione_%28software%29), cioè raccolte di software comprendenti un'abbondante (e variabile a seconda di chi l'ha realizzata e degli scopi per cui è stata creata) selezione di applicativi per la produttività personale, la manipolazione di file multimediali (audio, video, foto), per l'intrattenimento, la didattica, lo sviluppo software, la gestione del sistema e quant'altro, da installare **insieme** al sistema operativo. Inoltre quello che eventualmente dovesse mancare può essere cercato, trovato, scaricato e installato da un'apposita applicazione, attingendo agli archivi (repository) propri della distribuzione, contenenti per lo più software libero, ma non solo. Il concetto "installa l'app dallo store" è ormai familiare agli utilizzatori di smartphone, ma in realtà nasce ben prima di questi (https://it.wikipedia.org/wiki/Advanced_Packaging_Tool), proprio nel mondo delle distribuzioni Linux. Per fare un esempio: l'installazione di Ubuntu (http://www.ubuntu-it.org/) (la distribuzione Linux forse più nota) comprende anche la suite LibreOffice per la produttività individuale, programmi per la navigazione web e la posta elettronica, e Ubuntu Software Center (https://it.wikipedia.org/wiki/Ubuntu_Software_Center), lo "store" da cui poter scegliere tra migliaia di programmi da scaricare con un click. Significa ad esempio che un istante dopo l'installazione potete rimettere mano alla tesi di laurea che stavate scrivendo con LibreOffice (che è già installato), o configurare il vostro account di posta su Thunderbird (che è già installato) per riavere a disposizione tutte le vostre mail e magari aprire quel file PDF allegato con un visualizzatore (che è già installato).

Fatto non secondario, anche l'aggiornamento dei programmi è centralizzato e avviene esattamente come qualsiasi altro pacchetto del sistema operativo: la presenza di nuove versioni dei programmi viene periodicamente controllata e notificata (l'aggiornamento è sempre una scelta libera e consapevole dell'utente. Ci siamo capiti… (http://www.techeconomy.it/2016/05/27/windows-10-col-trucco-linganno/)), esattamente come (oggi) siamo abituati a fare con i nostri smartphone. Considerando che Debian (https://it.wikipedia.org/wiki/Debian) (distribuzione da cui deriva Ubuntu ed altre decine di "sorelle") e il suo sistema di gestione dei pacchetti nasce nel 1993, possiamo anche dire che nei sistemi operativi Linux praticamente **è sempre stato così**.

Un altro dettaglio a cui probabilmente nemmeno gli utenti Linux fanno più caso, ma se lo ricordano subito quando assistono ad un aggiornamento su Windows: durante l'aggiornamento di qualunque applicazione in uso – kernel compreso – non è mai (!) necessario chiudere nessuna applicazione, che continua a funzionare regolarmente; in alcuni casi viene suggerito – mai imposto – il riavvio dell'applicazione; solo nel caso del kernel viene suggerito il reboot, che è l'unico modo per caricare la nuova versione. Ancora per poco (http://www.zdnet.com/article/no-reboot-patching-comes-to-linux-4-0/), forse.

Antivirus chi?

Il primo programma che si installa solitamente dopo Windows è un antivirus, per ovvi motivi. Ovvi per gli utenti di Windows, ma non per gli utenti di Linux: io lo sono da 16 anni (Mandrake Linux 7.1 (https://it.wikipedia.org/wiki/Mandriva_Linux), la mia prima distribuzione, risale al 2000), e non ho mai installato un antivirus. I virus per Linux sono talmente pochi e talmente rari che gli antivirus sono considerati un inutile spreco di risorse. Quelli che esistono sono installati soprattutto su computer dove girano server di posta elettronica, e sono usati per proteggere i

sistemi Windows da eventuali malware diffusi via e-mail.
Ciò non significa che Linux, i programmi per Linux o il software open source in genere siano esenti da vulnerabilità. Come detto altrove (http://www.techeconomy.it/2016/05/27/windows-10-col-trucco-linganno/), "il software libero è libero, non perfetto: se no si chiamerebbe software perfetto". Le vulnerabilità si trovano e si correggono esattamente come per il software proprietario (anzi, meglio, perché il codice sorgente è di pubblico dominio, sotto gli occhi di tutti e il processo avviene alla luce del sole, generalmente a velocità superiore che nel software proprietario). Ma i virus, quelli proprio non li ho mai visti, e anche in questo caso possiamo dire che nei sistemi operativi Linux praticamente **è sempre stato così**.

Live, ovvero il sistema sempre con te (altro che cloud)

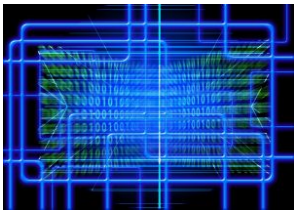
Diciamolo subito: non è sempre stato così. In passato l'installazione di un sistema operativo Linux era complicata, più di quella non semplice dei sistemi Windows coevi. Gli utenti Windows non ne hanno contezza dato che, come già detto, generalmente se lo trovano già installato nel PC, mentre gli utenti Linux generalmente se lo installano da sé e sicuramente lo installavano da sé nel passato di cui stiamo parlando. Anche per questa ragione col tempo gli sviluppatori hanno cercato di semplificare il processo di installazione, tanto che oggi è tutto molto semplice e amichevole: basta avviare il computer con il CD (o DVD, a seconda delle dimensioni della distribuzione, che dipendono essenzialmente da quanto software preinstallato è stato messo dentro) e seguire la guida passo-passo. Come Windows, ma con alcune differenze che non sono dettagli da poco:

- se state cercando di installare Ubuntu (per esempio. Vale per tutte le distribuzioni) in un computer dove è già installato Windows, Ubuntu se ne accorge e vi chiede gentilmente se volete davvero cancellare tutto o se invece volete installare Ubuntu accanto a Windows, decidendo poi all'avvio del PC di volta in volta quale sistema scegliere da una lista che vi comparirà sul monitor. In questo secondo caso pensa a tutto lui (oppure potete scegliere di farvi lasciare i comandi e guidare voi l'installazione, ammesso che sappiate cosa fare), ritagliandosi spazio nell'hard disk e sistemando per bene il sistema. Per inciso, non vale il viceversa: installare Windows su un pc con un sistema Linux equivale a concedere a Windows l'autorizzazione a cancellare tutto, formattare l'hard disk e occupare tutto lo spazio a disposizione. Windows si comporta come Ubuntu solo se trova altre versioni di Windows, ma non se trova altri sistemi operativi. Gentile, vi pare?
- probabilmente quello che avete inserito nel lettore è un **Live CD** (https://it.wikipedia.org/wiki/Live_CD) (o DVD). Quasi tutte le distribuzioni di Linux nell'ultimo decennio si presentano ormai sotto questa forma. Vuol dire che anziché installare il sistema sull'hard disk potete scegliere di avviarlo come se fosse già installato. Nulla verrà toccato nell'hard disk, ma dopo qualche istante avremo a disposizione un sistema pienamente funzionante, cosa utile per familiarizzare con l'interfaccia e per verificare che tutto l'hardware sia ben supportato e funzionante prima di procedere a un'installazione vera e propria. Unica differenza sarà nelle prestazioni, a causa della minor velocità di accesso ai dati da un supporto ottico (CD e DVD) rispetto a uno magnetico (hard disk), e nella impossibilità di salvare configurazioni e nuovi programmi eventualmente installati. Quest'ultimo problema si può risolvere (https://wiki.ubuntu.-com/LiveUsbPendrivePersistent) usando una **Live USB** (https://it.wikipedia.org/wiki/Live_USB), ovvero una distribuzione avviabile da chiavetta USB anziché da CD o DVD. Stesso principio, con il vantaggio di poter riservare spazio (a proposito, utente Windows: lo sapevi che puoi creare partizioni su una chiavetta USB?) per file e configurazioni personali del sistema live. Senza contare il fatto che una chiavetta USB occupa meno spazio di un disco. Davvero hai bisogno del cloud quando il tuo programma puoi tenerlo in tasca e farlo girare su qualsiasi computer?

È' altamente probabile, quindi, che un utente Linux giri sempre con una o più chiavette USB in tasca con una qualche distribuzione live installata sopra: per avere sempre un sistema "familiare" a disposizione, magari da infilare nel primo pc a disposizione, ma anche come strumento di disaster recovery (https://it.wikipedia.org/wiki/Disaster_recovery), anche (soprattutto?) di sistemi Windows, magari fuori uso e non avviabili per colpa di virus o malware. Infatti in questi casi si può avviare il pc con un sistema Linux Live (non può essere contagiato dagli eventuali virus, ricordate?) e mettere in salvo i dati copiandoli su un supporto esterno prima di procedere a formattazione e reinstallazione del sistema operativo. E dell'antivirus, e delle applicazioni, una ad una…

Adesso non potrete più dire che non lo sapevate! - Marco Alici - Fonte: http://www.techeconomy.it/2016/06/24/3-cose-linux-lutente-windows-sapere/

Scoperta grave vulnerabilità su Windows presente da 20 anni



È' stata scoperta solo pochi giorni fa una vulnerabilità che affligge tutti i sistemi operativi Windows denominata #BadTunnel. A fare questa sensazionale scoperta è stato un ricercatore di sicurezza cinese di nome **Yang Yu**, direttore del Xuanwu Lab of Tencent a Beijing, che ha individuato la falla presente ormai da 20 anni in tutte le versioni del sistema operativo di casa Microsoft, da **Windows 95 a Windows 10**.

Grazie al Bug Bounty, per questa scoperta Yang Yu ha guadagnato il massimo premio che Microsoft concede in questi casi, circa 50 mila dollari.

La scoperta verrà presentata ufficialmente da Yang al Black Hat Summit 2016 (https://www.blackhat.com/us-16/briefings/schedule/#badtunnel-how-do-i-get-big-brother-power-3915) che si terrà come di consueto a Las Vegas dal 30 luglio al 4 agosto. Per chi non conoscesse il Black Hat, è un evento molto noto nella comunità hacker e molto seguito in tutto il mondo, dove ricercatori e esperti di sicurezza presentano le loro scoperte.

"Questa vulnerabilità ha un impatto di sicurezza molto alto, probabilmente il più ampio mai registrato nella storia di Windows" – afferma Yang Yu.

Ma in cosa consiste #BadTunnel?

BadTunnel è una tecnica per NetBIOS-spoofing tra network. La tecnica permetterebbe all'attaccante di avere accesso al traffico che passa sul network della vittima oltrepassando eventuali Firewall e NAT di rete.
Secondo Yang, la vulnerabilità è causata nello specifico da una serie di implementazioni apparentemente corrette ma che impattano sul layer di trasporto e quello applicativo e ad una serie di protocolli applicativi usati dal sistema operativo.

Ipotesi di attacco

Un attaccante potrebbe tramite una mail di phishing o tecniche di social engineering indurre la vittima a cliccare su un determinato link con il browser IE o Edge e a farla accedere ad una pagina malevola.
La pagina malevola dell'attaccante appare come un **File Server** o un **Local Print Server** e tramite una serie di altre vulnerabilità che includono:
- come Windows risolve i nomi di rete e accetta le risposte
- come IE e Edge Browser supportano le pagine con codice embeddato
- come Windows gestisce le path di rete via l'indirizzo IP
- come il NetBIOS Name Service NB e NBSTAT interroga e gestisce le transazioni
- come Windows gestisce le richieste sulla porta UDP 137

BadTunnel prende vita.

Simulazione di uno scenario di attacco prese dal paper tecnico di Yang

1. Alice e Bob sono su reti differenti e hanno tra loro firewall e NAT. Bob ha la porta 137/UDP e raggiungibile da Alice
2. Bob chiude le porte 139 e la 445 lasciando aperta solo la 137/UDP
3. Alice è convinta di accedere a file URI o UNC path che puntano a Bob tramite un altro hostname URI come http://WPAD/x.jpg o http://FileServer/x.jpg
4. Alice invia una query NBNS NBSTAT verso Bob e verso l'indirizzo LAN di brodacast
5. Se Bob blocca l'accesso alle porte 139 e 445 con una regola Firewall, Alice invierà una query di NBNS NBSTAT dopo circa 22 secondi. Se Bob invece chiude le porte 139 e 445 disabilitando il servizio Server Windows o il NetBIOS sul protocollo TCP/IP, Alice non ha bisogno di aspettare la connessione che scade prima di inviare la query.
6. Quando Bob riceve la query NBNS NBSTAT inviata da Alice, Bob risponde forgiando un NBNS NB response prevedendo il transaction id e lo invia ad Alice. Se un pacchetto heartbeat viene inviato ogni pochi secondi, la maggior parte dei firewall e dispositivi NAT tengono aperta la connessione sulla porta 137/UDP
7. Alice ora può aggiungere la risoluzione dell'indirizzo inviata da Bob all NBT cache. Il valore di default della TTL per la cache NBT è di 600 secondi.
8. Bob può ora dirottare il traffico di Alice attraverso l'utilizzo del WPAD (Web Proxy Auto-Discovery Protocol) o tramite ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) server.

(La tecnica di attacco con WPAD venne presentata al BlackHat nel 2007. Inoltre il worm FLAME impiegò una tecnica simile.)
Fortunatamente **Microsoft** è corsa ai ripari e ha rilasciato il bollettino di sicurezza **MS16-077** che mette al sicuro da attacchi di questo genere.
Se invece non è possibile installare la patch, per mitigare questo attacco è bene bloccare all'interno del proprio network la porta 137/UDP. Per utenti individuali invece si consiglia di disabilitare NetBIOS TCP/IP. - Fabio Natalucci - Fonte: http://www.techeconomy.it/2016/06/22/scoperta-grave-vulnerabilita-windows-presente-20-anni/

Associazione Culturale
Fermo Linux Users Group
Gruppo Utenti Linux di Fermo
C.F.90037220440
www.linuxfm.org
info@linuxfm.org

Gruppo Telegram:
bit.ly/fermolug
Mailinglist pubblica:
http://liste.linuxfm.org/mailman/listinfo/discussioni

Il FermoLUG nasce nel 2003 da un gruppo di amici con la voglia di condividere le proprie scoperte in ambito informatico.

Lo scopo principale dell'Associazione è quello di promuovere e diffondere il Software Libero facendo corsi di formazione, eventi aperti a tutti e tenendo attiva e legata la propria comunità di soci e simpatizzanti.

Se hai voglia di condividere idee, trucchi e soluzioni nell'uso quotidiano di GNU/Linux, inserisciti nella Mailing List: è un sistema facile e veloce per entrare direttamente in contatto con i membri del LUG!

Se desideri aiutarci attivamente nella nostra missione, iscrivendoti ufficialmente alla nostra associazione, clicca su "Diventa Socio" dal nostro sito web www.linuxfm.org.
Il costo dell'iscrizione è di 10€.