Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Dipartimento di Informatica – Scienza e Ingegneria

Corso di Laurea in Informatica per il Management

Analisi interdisciplinare del Flipper Zero, strumento di Cybersecurity

Relatore:
Dr. Andrea Melis

Presentata da:
ARIANNA ARRUZZOLI

Correlatore:
Dr. Gori Giacomo

III
a.a. 2022 - 2023

Abstract

Il Flipper Zero è uno strumento portatile multiuso, sviluppato per interagire con i sistemi informatici. La sua principale funzionalità è quella di salvare ed emulare i segnali, tramite i suoi svariati sensori, rivelandosi un comodo strumento per i pentester, ma anche uno strumento per effettuare attacchi Replay.

La rapida popolarità del dispositivo ha permesso la creazione di una numerosa community, all'interno della quale è possibile trovare repository che consentono di installare gratuitamente versioni personalizzarte del firmware del Flipper Zero. Alcune di queste repository sono raccolte e spiegate all'interno di questa tesi al fine di dimostrare come questo strumento possa essere utilizzato per perpetrare svariate tipologie di attacchi informatici.

Il dispositivo si presenta come "uno strumento da hacker nel corpo di un giocattolo", nel corso dell'elaborato vengono analizzate le tecniche di design e marketing, quali Nostalgia Marketing e Gamification, che permettono di visualizzare lo strumento come tale.

La sua dualità tra l'essere uno strumento per pentester e anche un'arma per gli attacchi informatici, accostata alla continua narrazione del Flipper Zero come giocattolo, fa sì che sorgano determinati dubbi relativamente alla sua vera natura.

L'analisi delle strategie di marketing utilizzate per la promozione dell'oggetto, permettono di definire questioni relativamente alla sicurezza data dalla condivisione delle informazioni, analizzando anche come questi dispositivi possano essere percepiti a livello giuridico.

Indice

Capitolo 1

Introduzione

Il Flipper Zero è uno strumento portatile multiuso, sviluppato per interagire con i sistemi informatici.

Si tratta di un dispositivo hardware composto da un ricetrasmettitore che permette l'interazione con vari sistemi di controllo degli accessi, tra cui Radio Frequency IDentification (RFID)[1], protocolli radio e, tramite i General-Purpose Input/Output (GPIO) pins, può essere utilizzato anche per effettuare hardware debugging. Il suo principale utilizzo consiste nella clonazione delle chiavi digitali e dei segnali inviati, i quali una volta memorizzati all'interno del Flipper Zero possono essere poi riutilizzati in qualsiasi momento.

L'idea dietro la creazione del Flipper Zero è infatti quella di combinare vari sensori e dispositivi, per permettere al consumatore di avere tutti gli strumenti necessari per un Penetration Test o per l'esplorazione hardware, all'interno di un unico oggetto facilmente trasportabile. Si propone come mezzo per attirare interesse verso il mondo dell'hacking, semplificando le procedure per i pentesters[2]; allo stesso tempo, se utilizzato con intenzioni malevoli, risulta altamente pericoloso.

[1]RFID-Radio Frequency IDentification, sistema che utilizza i campi elettromagnetici per identificare e tracciare autimaticamente i tag associati ad un oggetto.

[2]Persone che effettuano Penetration Test

Il Flipper Zero è caratterizzato da un design molto particolare, piccolo e colorato, che viene presentato al pubblico come uno strumento per hacker nel corpo di un giocattolo.[32] Lo stile utilizzato nella sponsorizzazione e progettazione riprende le grafiche degli arcade anni '80, scatenando un'immediata associazione con l'idea di video game.

Figura 1.1: Flipper Zero

A fare da mascotte a questo dispositivo troviamo un delfino, un cyber dolphin [13], che accompagna l'interazione con il Flipper Zero, definendone la personalità. Il delfino interagisce continuamente con il consumatore, tramite delle animazioni che ne raccontano lo stato d'animo. Rappresenta le sensazioni dell'oggetto: se il Flipper Zero è utilizzato spesso, allora il delfino sarà felice; se il Flipper Zero viene lasciato inutilizzato per un determinato intervallo di tempo, il delfino diventerà triste; se il Flipper Zero è scarico, il delfino si arrabbierà e trasmetterà queste necessità tramite dei fumetti. L'intero design è impostato per far diventare un gioco l'utilizzo del Flipper Zero, proponendo una narrativa del prodotto che vuole introdurre un lato educativo dell'oggetto.

Il Flipper Zero appare per la prima volta il 20 luglio 2020 su Kickstarter [32], alla ricerca di finanziamenti. Sviluppato da un team di ragazzi russi, il Flipper Zero riesce rapidamente a raggiungere il main goal, entrando quindi

in produzione, grazie anche alla politica dei rewards di Kickstarter che permette di ricevere un Flipper Zero per ogni donazione di 129$. I finanziamenti totali sono dieci volte tanto il main goal necessario per la produzione, permettendo l'aggiunta di features prima non comprese nel Flipper Zero, come il Bluetooth e l'aggiunta del sensore di Near-field communication (NFC).

La caratteristica più interessante del Flipper Zero, oltre alla convergenza di più strumenti e al design altamente portatile, è la possibilità di avere un firmware open source. Questo permette la creazione di una comunità di persone che operano attivamente sul Flipper Zero, dando libero accesso a varie migliorie del dispositivo e generando un engagement nel pubblico.

La libertà come in tante occasioni, in particolare nel mondo dell'hacking, porta con sé anche dei rischi. Il firmware open source indica l'eventualità dell'esistenza di un firmware che elimini tutte le limitazioni imposte dal firmware di base che permettono di far rientrare l'uso del Flipper Zero all'interno dei confini legali.

Il Flipper Zero è di per sé uno strumento dal grande potenziale, che se utilizzato con intenzioni malevoli, può trasformarsi in un'arma per la cybersecurity. L'accostamento ludico ad un oggetto con potenziali pericolosi, invece di avvicinare nuove persone al mondo dell'hacking, rischia di rendere divertenti i crimini informatici.

1.1 Penetration Test

Il Penetration Test è una metodologia di ricerca delle vulnerabilità di un sistema. Viene effettuato tramite l'impersonificazione dell'attaccante, al fine di verificare quanto in profondità sia possibile infiltrarsi nel sistema. In questo modo è possibile identificare gli effettivi punti deboli della struttura e di conseguenza quanto essa possa essere definita sicura.

Le vulnerabilità del sistema sono infatti delle debolezze dei sistemi informatici, che possono essere sfruttate da agenti malevoli per accedere ad informazioni o controlli che dovrebbero rimanere riservati.

I Penetration Test sono quindi degli attacchi simulati, condotti da esperti di sicurezza informatica o da team specializzati, che cercano di simulare gli stessi metodi e tecniche utilizzate dagli attaccanti per identificare eventuali falle nella sicurezza del sistema.

L'obiettivo principale dei Penetration Test è fornire alle organizzazioni una valutazione accurata e realistica della sicurezza dei loro sistemi, consentendo loro di identificare e correggere eventuali vulnerabilità prima che possano essere sfruttate da attacchi reali.

1.1.1 Fasi operative

Al fine di prevenire al meglio gli attacchi cyber, è importante verificare tutte le possibili vulnerabilità che possono essere sfruttate da agenti malevoli. Il miglior modo per individuarle è quindi quello di seguire le stesse tecniche e gli stessi step che vengono comunemente seguiti ed utilizzati in caso di attacco. Vi sono di norma 5 fasi principali durante l'esecuzione di un Penetration Test[54]:

1. Reconnaisance
2. Scanning
3. Gaining Access
4. Manteining Access
5. Cleaning Tracks

La prima fase (Reconnaisance) consiste in una ricognizione per la comprensione generale dell'ambiente che si vuole difendere o attaccare.

La seconda fase (Scanning) prevede l'individuazione di informazioni tecniche su eventuali punti d'accesso da provare a violare, consultando anche database di vulnerabilità note, che sono di dominio pubblico, come il CERT Vulnerability Notes Database, oppure il CVE (Common Vulnerabilities and Exposures List).
La terza fase (Gaining Access) prevede di entrare nel sistema, ad esempio identificando le credenziali di accesso. L'individuazione delle credenziali può essere perpetrata in varie modalità:

- *Precomputed attack*: effettuato tramite degli elenchi di possibili combinazioni compilate in precedenza, di possibili password e le loro rispettive trasformazioni in hash.

- *Brute force attack*: attacco informatico che prevede di individuare una chiave provando tutte le possibili combinazioni.

- *Dictionary attack*: elenchi di possibili password già esistenti, spesso costituite tramite data breach, che vengono utilizzati dall'algoritmo di brute force per provare esclusivamente le parole del dizionario. Questa tipologia di attacchi risulta funzionale poichè noi esseri umani tendiamo ad utilizzare sempre le stesse password.

- *Masks attack*: attacco che prevede di indovinare una password provando tutte le possibili combinazioni di chiave secondo schemi prefissati. Anche in questo caso gli esseri umani sono inefficienti nella creazione delle password poiché tendono a ripetere gli stessi schemi (ad esempio numeri alla fine della parola, oppure le iniziali delle parole in maiuscolo).

- *Rules attack*: anche in questo caso vengono utilizzati dei pattern su un attacco di Brute Force, ma la struttura della password dipende dai requisiti del sistema anziché dalle preferenze umane.

Ovviamente queste varie tipologie possono essere combinate insieme, al fine di individuare la modalità di attacco più efficiente.

La quarta fase (Manteining Access) si verifica quando l'attaccante (o il pentester) è riuscito ad entrare nel sistema e, per mantenere il controllo della macchina, crea una backdoor che gli permetta di rientrare al bisogno. In questa fase vengono quindi testati i meccanismi di sicurezza interni al sistema. Infine, la quinta fase (Cleaning Tracks) consiste nella cancellazione dei log e delle tracce dal sistema. I pentester la sfruttano per verificare il livello di difficoltà nella cancellazione delle eventuali tracce lasicate nel sistema durante le operazioni.

1.1.2 Tipologie di hacker

I Penetration Test possono essere eseguiti da collaboratori interni oppure da organizzazioni esterne. Queste possono essere costituite da: aziende di cybersecurity, i cui operatori sono anche definiti *White Hat* e sono vincolati da contratto di lavoro; oppure da hacker non autorizzati che ricercano dei bug per conto di terzi, operando con intento benevolo e non criminoso nei confronti dell'organizzazione, detti *Grey Hat*; oppure da *Black Hat*, attaccanti malevoli che hanno come obbiettivo l'esposizione delle vulnerabilità e la disabilitazione del servizio [16].

I tre agenti operano in modalità simili ma con obbiettivi differenti.

I White Hat operano a seguito di un consenso scritto, possono essere vincolati rispetto alla profondità che possono raggiungere nel sistema e devono rispettare clausole di riservatezza. Essi cercano di prevenire possibili attacchi tramite delle misure di sicurezza passive, come firewall, software antivirus e la costituzione di permessi per la limitazione degli accessi [40]. Sono quindi incaricati di analizzare le vulnerabilità per costruire attorno ad esse delle misure di sicurezza adeguate. Generalmente le vulnerabilità scoperte, vengono segnalate ai proprietari del sistema e, solo una volta risolte, vengono rese pubbliche.

I Black Hat rappresentano coloro che arrecano un'offesa a danni di terzi, ricercando le vulnerabilità per sfruttarle nel perpetrare attacchi di vario ge-

nere. Il giorno nel quale, le vulnerabilità identificate dai Black Hat vengono rese pubbliche, in particolare vengono rese note allo sviluppatore o proprietario del sistema, viene definito lo *zero-day*, in tale giorno viene esposta la falla di sicurezza del sistema a seguito di un attacco.

Gli zero-day sono altamente temuti da parte dei proprietari dei sistemi, poichè nel momento in cui si verificano, non vi è modo di fermare l'attacco fino alla sua conclusione; questo perchè l'attaccante disabilita il sistema effettuando un *Denial of Service*[3], assicurandosi che la propria operazione possa avvenire indisturbata. Parimente gli hacker possono sfruttare le vulnerabilità zero-day per intrufolarsi nei sistemi o danneggiare le reti senza che gli sviluppatori di software ne siano a conoscenza. Questo rende le minacce degli zero-day molto pericolose e difficili da difendere.

Il consenso è il confine principale tra un Pentetration Test e un attacco informatico. Se l'autorizzazione non viene concessa preventivamente, si ricade nell'illecito.

La figura dei Grey Hat, confonde e sfuma il confine. Spesso infatti questa categoria di hacker opera tramite modalità illecite nella ricerca delle vulnerabilità, per poi venderle a terze parti. Queste terze parti possono essere l'azienda stessa, alla quale viene segnalata una vulnerabilità, oppure finanziatori esterni che ricercano degli *exploit*[4] relativamente ad alcune tecnologie o situazioni. I Grey Hat possono rappresentare i mercenari del mondo cyber. Nel caso in cui i mecenati siano istituzioni governative, si configura una situazione 'macchiavellica', poichè le istituzioni sono considerate legittimate a tale acquisto [40].

Generalmente i Grey Hat fanno riferimento ai principi presentati da Levy

[3]Il Denial of Service (DoS) è una tipologia di attacco informatico che ha come obbiettivo l'esaurimento delle risorse di sistema, al fine di impedire agli utilizzatori del servizio l'interoperabilità con esso. Mina il principio della *Availability*.

[4]Gli exploit sono delle sequenze di comandi che sfruttano una vulnerabilità, per generare un comportamento inatteso all'interno del sistema.

nel 1984 [33]. Questi principi di etica hacker fanno riferimento alla libertà di accesso alle informazioni, favorendo la trasparenza rispetto alla Security by Obscurity[5], professando un utilizzo delle abilità dell'individuo per il dissotterramento delle informazioni presenti in internet, senza alcuna tipologia di barriere, definendo il World Wide Web uno spazio libero.

Questi principi liberali tendono a sfociare in anarchia nel momento in cui ci si trova davanti a leggi per la regolamentazione delle informazioni online. Oggi grandi gruppi come WikiLeaks e Anonymus si appellano a questi principi per giustificare le proprie azioni [36].

Nel corso del tempo sono stati introdotti nuovi principi che hanno tentato di modificare la visione dei ruoli interpretati dai vari hacker. In particolare negli anni '90, Mizrach ha introdotto dieci principali valori, primo fra tutti "*above else, do not harm*"[36].

Questi principi etici si sono evoluti nel corso del tempo e adattati alle nuove regolamentazioni dello spazio cibernetico, variegando ed ampliando lo spettro all'interno del quale vengono identificati i Grey Hat.

1.2 Attacchi di Replay

Gli attacchi informatici di Replay sono una specifica categoria di attacchi basati sulla riproduzione della password di accesso.

Sono una tipologia di attacco molto semplice da eseguire ma molto intricato da difendere, non dipendono infatti dalla complessità dell'algoritmo di cifratura, ma bensì dalla capacità di Autenticazione del sistema.

Gli attacchi di Replay più facili da eseguire sono quelli effettuati sulle trasmissioni radio; poiché le informazioni viaggiano liberamente nell'etere, sono potenzialmente visibili a chiunque. Data questa caratteristica delle

[5]La *Security by Obscurity* è un principio che si basa sull'assunto di sicurezza data dalla segretezza delle informazioni; mantenendo nascosto il funzionamento interno di un sistema o di un componente, questo è protetto da eventuali attaccanti esterni.

trasmissioni radio, le conversazioni utilizzano dei meccanismi di cifratura, per garantire la confidenzialità delle informazioni. Così facendo, nell'eventualità di *eavesdropping*[6], l'attaccante non sarà in grado di comprendere o estrapolare i plaintext[7] della conversazione.

Le trasmissioni radio sono molto diffuse in oggetti di vita quotidiana e ve ne sono di varie tipologie: dai telecomandi, alle reti wireless, agli RFID contenuti ad esempio all'interno dei badge universitari.

L'attacco di Replay consiste nell'ascoltare la comunicazione tra due parti, il richiedente l'accesso e il sistema, al fine di identificare l'invio della chiave da parte del richiedente. Una volta identificata, viene copiato il messaggio nel suo intero, per poi essere rispedito successivamente, impersonificando il precedente richiedente.

L'attaccante non ha quindi bisogno di perdere tempo a decifrare la password inviata o a comprendere quale algorimto sia stato utilizzato, poichè rispedisce il messaggio già cifrato, eludendo la sicurezza messa in atto.

Se il sistema non prevede una Challenge and Response, è altamente probabile che permetta l'accesso.

La *Challenge and Response* è uno dei pochi baluardi esistenti, implementati per proteggere la confidenzialità della comunicazione da attacchi di Replay. Per garantire l'identità del richiedente accesso, il sistema deve essere in grado di dialogare con esso; sono quindi necessari due ricetrasmittenti a sostituzione del semplice trasmittente e ricevitore. La comunicazione mantiene la stessa prassi: il richiedente richiede l'accesso e il sistema lo concede una volta confermate le credenziali; nel mezzo, però, vengono inserite delle domande per il richiedente l'accesso, al fine di verificarne l'identità e di conseguenza l'autorizzazione.

Il sistema, una volta ricevuta la richiesta d'accesso, risponde tramite l'invio di un codice e ne richiede la versione cifrata tramite un algoritmo ed una

[6]Eavesdropping, tipologia di attacco che ascolta conversazioni e comunicazioni private tra due parti. Mina il principio della *Confidentiality*.

[7]Plaintext, messaggio in chiaro prima della cifratura.

chiave conosciuti solo a colui che ha il permesso di accedere. Il richiedente l'accesso cifra il codice e lo rispedisce al sistema, se il cyphertext[8] corrisponde a quello atteso dal sistema, allora viene permesso l'accesso. Questa metodologia preserva da vari attacchi di Replay poichè i codici inviati in chiaro sono univoci, per cui è impossibile che il sistema accetti un messaggio cifrato relativo ad un codice già trasmesso.

Un'ulteriore forma di difesa dagli attacchi di Replay, più diffusa e più semplice rispetto alla Challange and Response, è costituita dal Rolling Code.

Il *Rolling Code* prevede l'utilizzo di una sequenza di codici pseudo-random, condivisa tra il richiedente l'accesso e il sistema. Nel momento in cui il sistema riceve una richiesta di accesso, seleziona un codice all'interno della sequenza e lo invia, attendendo come risposta il codice successivo nella sequenza. Se il codice ricevuto è corretto, allora viene permesso l'accesso.

La sicurezza è garantita dall'unicità della sequenza, la quale contiene codici che non vengono ripetuti. Inoltre il sistema è provvisto di un contatore, che permette la selezione di un codice nuovo ad ogni richiesta.[9]

Poiché possono esserci problemi dovuti alla sincronizzazione, solitamente il sistema ha una finestra di codici ai quali è permesso l'accesso.

In caso di presenza di un eavesdropper, che veda la trasmissione del codice di accesso da parte del richiedente, al momento della trasmissione del codice precedente il sistema non garantirà l'accesso per un codice già utilizzato.

[8] Messaggio risultante dall'algoritmo di cifratura, ovvero il testo cifrato.

[9] Definito One Time Pad, ovvero chiavi utilizzabili solo una volta.

1.3 Il Flipper Zero come tool di Cybersecurity

Il Flipper Zero si propone al mercato come un oggetto che racchiude tutti i possibili strumenti hardware necessari per un Penetration Test.

> *"The main idea behind the Flipper Zero is to combine all the research and penetration hardware tools that you could need on the go in a single case."* (Flipper Devices Inc[13])

La sua molteplicità di sensori permette di leggere, memorizzare ed emulare svariate tipologie di segnali, facilitando il lavoro dei pentesters, ma semplificando anche la possibilità di attachi Replay.

1.3.1 Sensori del Flipper Zero

Sub-GHZ

I Sub-GHZ sono delle frequenze radio inferiori a 1GHz. All'interno del Flipper Zero è possibile infatti riceve e trasmettere le frequenze da 300 a 928 MHz. Queste frequenze vengono utilizzate per trasmettere comandi utilizzati nell'interazione con cancelli, serrature radio, interruttori a distanza, campanelli senza fili, smart lights e altro ancora.

Il Flipper Zero permette di leggere i segnali, salvarli al suo interno, per poi riprodurli. Consente inoltre di configurare una precisa frequenza, di definire la presenza di Hopping[10], di selezionare la tipologia di Modulazione, di riprodurre le frequenze come dei suoni e di impostare la ricezione in background.

Per permettere all'utente di selezionare le corrette impostazioni d'uso, il Flipper Zero mette a disposizione anche un *Frequency Analyzer*, che analizza

[10]L'Hopping è un misura di sicurezza che alterna periodicamente la frequenza sulla quale viene trasmesso il messaggio, serve ad impedire eventuali attacchi di *Denial of Service* all'interno delle comunicazioni radio. Nel caso in cui fosse presente e conosciuta all'attaccante, la comunicazione risulterebbe egualmente esposta a rischi di attacco.

il segnale di uno specifico trasmettitore descrivendone frequenza e potenza di segnale.

L'utilità e l'alta capacità di adattamento degli strumenti proposti dal Flipper Zero, permette agli utilizzatori di essere pronti in ogni evenienza. La possibilità di ascoltare ed identificare una qualsiasi tipologia di segnale radio può diventare pericoloso nel caso in cui si decida con intenti malevoli di ascoltare segnali radio che dovrebbero rimanere non pubblici.[11]

Le frequenze Sub-GHz sono utilizzate in specifiche bande in base allo stato in cui ci si trova. Infatti vi son frequenze che sono permesse al pubblico, mentre altre frequenze non possono essere utilizzate dai civili e variano in base alla posizione geografica.

Poichè il Flipper Zero è pensato come un oggetto utilizzato a livello globale, ha un range molto ampio, tale da permettere l'utilizzo di qualsiasi frequenza. Nel momento in cui il firmware del Flipper Zero viene aggiornato, egli memorizza la localizzazione del dispositivo che permette l'aggiornamento, affinchè nel momento in cui si provasse a trasmettere o ascoltare su frequenze non permesse ai civili, il Flipper Zero mandi una schermata di '*Trasmissione bloccata*'[12].

Tuttavia, sono state sviluppate svariate estensioni del firmware che permettono di modificare il blocco delle frequenze, annullandolo.

[11] Definire una frequenza radio privata è concettualmente sbagliato, poichè le onde viaggiano nell'etere; chiunque sia in possesso di un'antenna ha il potenziale di ascoltare le comunicazioni su determinate frequenze. La sicurezza di tali comunicazioni può essere data, in parte e mai completamente, dal fatto che la frequenza di trasmissione sia conosciuta da pochi e non sia quindi di dominio pubblico.

[12] Questa restrizione è stata aggiunta successivamente rispetto all'iniziale firmaware del Flipper Zero; l'accorgimento è arrivato a seguito di continue restituzioni da parte della dogana israeliana. Il Flipper Zero permetteva la trasmissione su frequenze utilizzate dalle forze di difesa israeliane (IDF) e poichè è illegale trasmettere o ascoltare per i civili [42], anche il Flipper Zero risultava illegale.

125 kHz RFID

Gli RFID, sono dei sistemi che utilizzano i campi elettromagnetici per identificare e tracciare automaticamente i tag associati ad un oggetto. Possono essere trovati in svariate forme come tessere di plastica, portachiavi, etichette, braccialetti e microchip per animali.

I tag RFID sono costituiti da un circuito integrato (IC), un'antenna e un substrato. La parte di un tag RFID che codifica le informazioni identificative è chiamata RFID inlay. Esistono due tipi principali di tag RFID: attivo e passivo. Un tag RFID attivo ha una propria fonte di alimentazione, spesso una batteria. Un tag RFID passivo riceve l'alimentazione dall'antenna di lettura, la cui onda elettromagnetica induce una corrente nell'antenna del tag RFID.

Il Flipper Zero ha un modulo RFID a bassa frequenza in grado di leggere, salvare, emulare e scrivere carte RFID.

NFC

NFC è una sigla che sta per Near-Field Comunication, il sensore permette infatti la comunicazione tra due dispositivi elettronici che si trovano a breve distanza, massimo 10 cm. È un'evoluzione dei sensori RFID e sviluppa, a differenza loro, una comunicazione bidirezionale. Quando due apparecchi NFC raggiungono una distanza inferiore ai 4 cm, viene instaurata una connessione peer-to-peer che permette di creare un dialogo per lo scambio di informazioni. La tecnologia NFC viene infatti utilizzata all'interno di carte di credito, passaporti e carte di identità elettroniche, che tramite il Challenge and Response permettono di avere un'autenticazione sicura.

Una scheda NFC è un transponder che opera a 13,56 MHz e dispone di un numero univoco (UID) e di una parte di memoria riscrivibile per l'archiviazione dei dati. A seconda del tipo di scheda, la memoria può essere segmentata in settori, pagine, applicazioni e altro. Quando sono vicine a un lettore, le carte NFC trasmettono i dati richiesti.

Quando il Flipper Zero scannerizza un NFC, memorizza le informazioni riguardanti UID, ATQUA e SAK; questi ultimi sono valori che indicano il produttore e la tipologia di tag utilizzato e servono ad identificare quale sia la tipologia di NFC appena scannerizzata.

Nel caso in cui il lettore fosse protetto da password, il Flipper Zero permette di leggere la richiesta del lettore, per poi inserire manualmente la password richiesta. Esiste però anche la possibilità di generare delle password per gli Amiibo[13] e per i Xiaomi Air Purifier.

Anche per questa tipologia di sensore il Flipper Zero è in grado di clonare le informazioni dell'NFC all'interno di una Magic Card. Le NFC magic cards sono particolari carte NFC sulle quali è possibile trascrivere l'UID, assegnandogli quindi quello appena copiato.

Infrared

Gli infrarossi, anche indicati come IR, sono una frequenza dello spettro elettromagnetico compresa tra le onde radio e la luce visibile. È una tipologia di segnale che viene utilizzata per varie tipologie di telecomandi, in particolare per televisori, sistemi di aria condizionata e sistemi audio.

Con il suo modulo a infrarossi integrato, Flipper Zero può ascoltare e salvare i comandi a infrarossi, trasformandosi in un sostituto del telecomando per i comandi imparati. Altrimenti è possibile utilizzare i telecomandi universali già presenti all'interno del Flipper per controllare altri dispositivi. I telecomandi universali consistono in realtà in un *attacco di Brute Force* che viene eseguito tramite un *attacco a dizionario*; all'interno del firmware sono infatti preimpostati dei dizionari di segnali che vengono iterati per ogni comando inviato.

Per quanto i telecomandi universali possano sembrare una soluzione rapida rispetto alla singola memorizzazione di tutti i possibili comandi di un

[13] Amiibo è una piattaforma di 'giocattoli in vita' di Nintendo, lanciata nel novembre 2014. Consiste in un protocollo di comunicazione e archiviazione wireless per collegare le figurine alle console per videogiochi.

telecomando, rappresentano in realtà un campanello d'allarme. Sono infatti un'innocua dimostrazione del fatto che il Flipper Zero abbia in realtà il potenziale di riprodurre comandi universali e generare attacchi di *Denial of Service*, rientrando all'interno dei confini legali esclusivamente per volontà di marketing e vendita del prodotto verso un più vasto pubblico.

GPIO pinout

Il GPIO, acronimo per General Purpose Input/Output, è un'interfaccia elettronica hardware disponibile su alcuni dispositivi elettronici. Possono agire come input, per leggere i segnali digitali provenienti da un circuito aggiunto, oppure come output, per controllare o segnalare agli altri dispositivi. Permettono l'estensione dell'hardware di base, proponendo delle nuove interfacce che comunicano tramite i pin. Ogni Input/Output pin ha uno specifico valore di riferimento.

Il Flipper Zero ha 18 pin sul lato, che permettono di aggiungere schede per nuove interfacce. In particolare sono prodotte delle schede che permettono al Flipper Zero di interagire con il Wi-Fi; tramite il modulo ESP32-S2.

Poichè la rete wireless si basa sulla comunicazione radio, è possibile intercettare i pacchetti che vengono inviati, oppure inviarne alcuni. In particolare è possibile inviare i pacchetti di disconnessione, facendo sì che tutti i dispositivi connessi al router vengano disconnessi simultaneamente, un esempio pratico è discusso nel capitolo 1.3.2.

iButton

I dispositivi iButton sono piccoli moduli forniti di indirizzi digitali univoci a livello globale. Un dispositivo iButton utilizza una piccola lastra di acciaio inossidabile come interfaccia di comunicazione elettronica. Sfruttando il protocollo di comunicazione 1-Wire, i dispositivi iButton offrono la possibilità di fornire o registrare dati. Data la loro univocità, vengono utilizzati per l'autenticazione all'interno dei sistemi di controllo degli accessi oppure per le transazioni di contante elettronico.

Il Flipper Zero permette di leggere e salvare le informazioni e i dati contenuti all'interno dell'iButton.

Bad USB

Le BadUSB sono utilizzate per effettuare attacchi alla sicurezza del computer tramite dispositivi USB programmati con software dannosi. Il Flipper Zero può fungere da dispositivo BadUSB; vi possono essere inseriti dei codici che una volta eseguiti, sono riconosciuti dai computer come Human Interface Device (HID), ovvero come device utilizzati per prendere input da persone fisiche.

Un dispositivo BadUSB può modificare le impostazioni di sistema, aprire backdoor, recuperare dati, avviare shell o eseguire qualsiasi operazione possibile con l'accesso fisico. Tutto ciò è possibile eseguendo una serie di comandi scritti nel linguaggio di scripting Rubber Ducky, noto anche come DuckyScript, che permette di simulare gli input esterni.

Semplicemente tramite il collegamento con un computer, il Flipper Zero può avviare un malware di qualsiasi genere, al fine di disabilitare il computer stesso.

Gli attacchi di questo tipo utilizzano la Code execution per effettuare una Priviledge Escalation all'interno del sistema, arrivando a controllare interamente la macchina. Una volta raggiunto il controllo totale è possibile eseguire un servizio di Reverse Shell[14], che permette ad agenti malevoli remoti di accedere al sistema. Inoltre, con il controllo della macchina, è possibile accedere ai dati, per un'eventuale esfiltrazione. Tra i malware che possono essere trasmessi tramite BadUSB è inoltre possibile installare un *ransomware*, ovvero un malware designato alla cifratura dei dati di un computer impedendone l'accesso al proprietario.

[14]La macchina vittima di attacco viene connessa ad un computer remoto, creando per quest'ultimo una backdoor per l'accesso e controllo remoto della macchina attaccata.

1.3.2 Uso malevolo del Flipper

Dalla presentazione fatta del Flipper Zero sembrerebbe essere un oggetto dalle meravigliose caratteristiche, ma nella realtà ha un elevato potenziale illecito.

Il firmware di base prodotto e diffuso dalla Flipper Devices, applica una serie di restrizioni ai vari sensori per permettere l'utilizzo del Flipper Zero all'interno dei confini legali.

Nonostante queste riduzioni del firmware è comunque possibile perpetrare attacchi di Replay, i quali, se effettuati senza il consenso del proprietario dell'oggetto che viene clonato, secondo il Codice Penale italiano ricadono del reato di *Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici* (Art. 615-quater).

Esiste una vasta community di utenti che hanno messo a disposizione online dei codici o algoritmi che permettono di utilizzare il firmware legale per scopi illeciti. I codici gratuiti sono facilmente scaricabili ed inseribili all'interno del Flipper Zero, permettendo a chiunque possieda tale apparecchio di sfruttarne i sensori per perpetrare attacchi di Brute Force, aprendo cassaforti elettroniche e cancelli elettrici.

Il firmware di base mette a disposizione un *Frequency Analizer*, che permette di identificare la frequenza utilizzata per lo scambio dei dati ascoltati in quell'istante. Questo strumento potrebbe essere utilizzato per identificare la frequenza sulla quale si svolge la comunicazione verso un determinato sistema, per poi inviare un attacco di Brute Force oppure Denial of Service su di essa.

Una delle estensioni più diffuse del firmware del Flipper Zero risulta essere il codice per l'apertura di sistemi utilizzati per la limitazione degli accessi. Queste estensioni si ispirano a delle funzionalità già presenti all'interno del firmware di base. Questo continene la possibilità di utilizzare dei telecomandi

universali per televisori, proiettori, condizionatori e sistemi audio. Tramite il sensore di infrarossi il Flipper Zero effettua un attacco a dizionario sui protocolli utilizzati per la trasmissione infrarossi [12]; nel momento in cui viene identificato il protocollo corretto, allora il Flipper Zero mostra una schermata tramite la quale è possibile visualizzare i pulsanti del telecomando e di conseguenza eseguire i comandi corrispondenti.

Questa metodologia è stata ampliata a tutti gli altri sensori presenti nel Flipper Zero per perpetrare una moltitudine di attacchi.

Il sensore Sub-GHz viene utilizzato perl'apertura dei cancelli elettrici; l'algoritmo prevede un attacco di Brute Force per identificare la frequenza corretta tramite la quale aprire il cancello 1.2. Determinati algoritmi permettono la selezione di alcuni protocolli specifici (sottointendendo una conoscenza minima del terreno su cui ci si muove)[22]. Altri algoritmi permettono invece di inviare un singolo comando che testa su tutte le frequenze e su tutti i possibili protocolli, senza necessità di conoscenze pregresse.[25]

Tramite medesime modalità è possibile utilizzare il sensore per gli iButton e per gli RFID [21]. L'algoritmo permette di eludere i sistemi che regolano gli accessi attraverso l'uso di porte apribili tramite badge oppure oggetti specifici dedicati, applicando degli attacchi a dizionario. Questo attacco può essere utilizzato per accedere all'interno delle camere d'albergo oppure per accedere ad aree confinate disponibili solo per alcuni.

Le GPIO pins possono essere utilizzate per collegare il Flipper Zero ad una cassafote elettronica, in particolare è possibile sfruttate le vulnerabilità note di alcune cassaforti, come la Sentry Safe e la Master Lock [24], per inviare un segnale specifico che funge da passpartout e permette di aprirle senza necessità di conoscere il codice di accesso [46].

Data l'ampiezza e varietà di codici prodotti dall'estesa community del

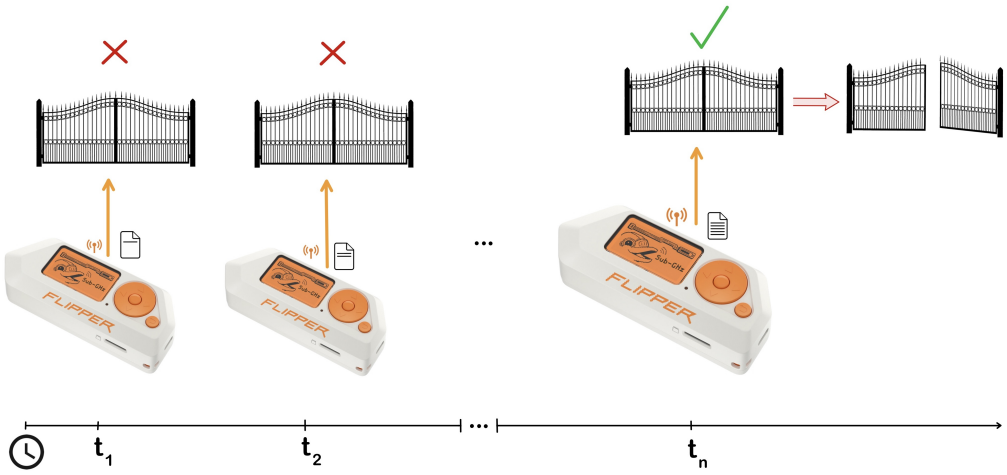

Figura 1.2: Flipper Zero che esegue un attacco a dizionario per l'apertura di un cancello elettrico. Vengono effettuati vari tentativi nel tempo, iterando le combinazioni contenute nel dizionario, fino ad incontrare la combinazione corretta che permette l'apertura del cancello.

Flipper Zero, esiste anche una versione del firmware che racchiude tutti i plugin generati, all'interno di un'unica versione del firmware 'illimitata' del Flipper Zero.

Il codice creato da Rogue Master è disponibile al pubblico su GitHub [47] e permette di estendere le possibilità del Flipper Zero. Installando quest'estensione gratuita è possibile avere di default, oltre al codice per gli esempi già forniti, anche i codici di apertura e chiusura di alcuni telecomandi delle automobili, in particolare di macchine marca Tesla e di casa Honda, permettendo a chiunque di poter eventualmente aprire automobili altrui.

Lo stesso autore ha pubblicato nella repository svariati codici per BadUSB che installano automaticamente vari programmi legati al Flipper Zero, oppure effettuano una donazione tramite Patreon a Rogue Master.

I codici messi a disposizione sfruttano ogni caratteristica del Flipper Zero, grazie anche al nuovo modulo ESP32-S2 che è possibile aggiungere tramite GPIO pins.

Grazie a questa scheda è possibile utilizzare i plugin del codice di Rogue Master per inviare pacchetti che effettuano la disconnessione di tutti i dispositivi dal router WiFi, risultando in attacchi di Denial of Service [19].

I plugin messi a disposizione permettono inoltre di visualizzare la lista dei vari Access Point presenti nelle vicinanze e di effettuare uno *spoofing*[15] della comunicazione [19]. Il Flipper Zero salverà poi all'interno della propria memoria SD tutti i file `.pcap` prodotti, ovvero file che contengono dati dei pacchetti trasmessi sulla una rete appena esaminata, per permettere la loro analisi da computer.

Un'altra peculiarità della nuova estensione è la possibilità di simulare un Access Point, ovvero di emulare l'accesso ad una rete Wi-Fi. Se un utente richiede l'accesso al finto Access Point, il Flipper Zero risponde con un pagina di login, personalizzabile secondo le esigenze del proprietario del Flipper Zero, dove l'utente inserirà le proprie credenziali di accesso che verrano inviate in chiaro sullo schermo del Flipper Zero 1.3 [4, 20] .

Questo rientra perfettamente nella definizione di *phishing*, il quale ricade nel reato di *Frode informatica*, regolamentato dagli Art. 640 e 640-ter del Codice Penale.

Un ulteriore modalità di uso del Flipper Zero, sempre fornita dalla repository di Rogue Master è la Bad Keyboard (BadKB).

La BadKB permette di combinare più sensori del Flipper Zero per eseguire script BadUSB da remoto. Attivando la funzionalità, il Flipper Zero

[15]Il termine *spoofing* indica un attacco compiuto tramite l'impersonificazione dell'autorizzato all'accesso. In questo esempio viene impersonificato un dispositivo autorizzato all'accesso alla rete. Il dispositivo impersonificato è autorizzato anche all'invio di pacchetti e potrebbe quindi disconnettere altri dispositivi, oppure, sfruttando il protocollo TCP, ricercare il momento di handshake tra un server e un client per identificare e rubare le credenziali.

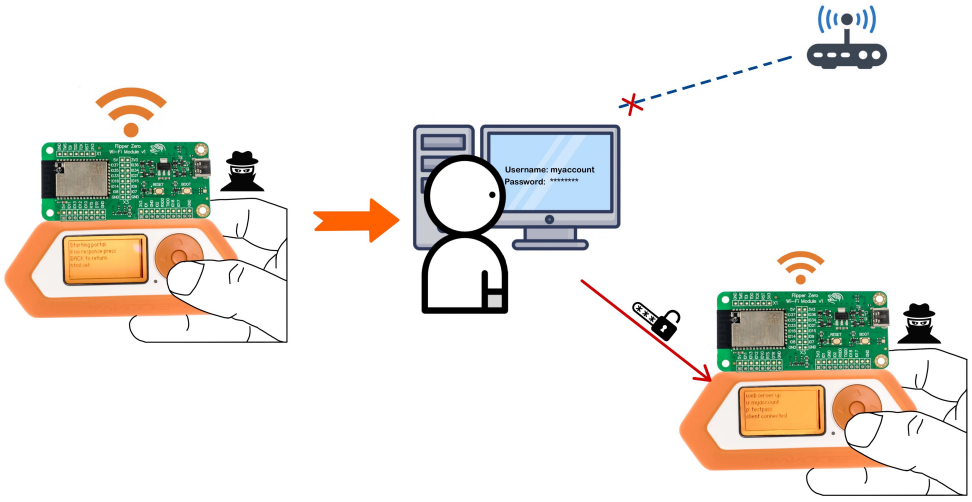

Figura 1.3: Furto di credenziali tramite Rogue Access Point. L'utente crede di inserire le proprie credenziali nella pagina di accesso del router; in realtà sta inserendo i propri dati nella pagina simulata dal Flipper Zero, che invece di permettere il collegamento ad internet invia le credenziali d'accesso in chiaro sullo schermo del Flipper Zero.

viene esposto come un dispositivo Bluetooth, con un nome personalizzabile (permettendo quindi delle dinamiche simili al Rogue Access Point).

Il computer visualizza la connessione come una tastiera, eludendo i sistemi di antivirus che bloccano l'esecuzione automatica degli script.

Una volta che un utente è collegato al dispositivo via Bluetooth è possibile eseguire dei codici BadUSB che prendono il controllo della macchina ed eseguono determinate azioni. Tramite questi script è possibile effettuare degli attacchi senza la necessità di essere collegati fisicamente con il dispositivo obbiettivo.

Grazie all'identificazione di una vulnerabilità all'interno della sequenza di accoppiamento via Bluetooth Low Energy (BLE), è possibile perpetrare questa tipologia di attacco anche per disturbare e disabilitare tutti i dispositivi di casa Apple, i quali mantengono il Bluetooth costantemente attivo per permettere determinate e diffuse funzionalità che lavorano tramite BLE [39].

Il Flipper Zero può quindi utilizzare la funzionalità del BLE per inviare infiniti segnali di notifica a tutti i dispositivi, rendendoli inutilizzabili per gli utenti, risultando in un rapido ed efficiente Denial of Service [26].

Una delle tipologie di attacchi che sembra essere stata ancora non sviluppata tramite il Flipper Zero, riguarda la clonazione delle carte di credito. Attraverso la possibilità di lettura ed emulazione via sensore NFC, si era diffuso online il mito di poter clonare le carte di credito o debito, generando grande preoccupazione.

In realtà le carte di credito contengono al loro interno un protocollo che impedisce gli attacchi Replay, tramite una comunicazione a chiave asimmetrica effettuata con la banca utilizzando identificatori univoci per ogni transazione. All'interno dei pagamenti contactless viene utilizzato il campo elettromagnetico prodotto dal sensore NFC e dal dispositivo di accoppiamento ravvicinato, che tramite pulsazioni effettua una comunicazione criptata [31], basata su chiavi private intrinseche della carta che non vengono lette dal Flipper Zero nel momento di analisi, rendendendo quasi impossibile la clonazione.

Capitolo 2

Lato marketing

Il Flipper Zero è uno strumento dalle molteplici potenzialità, che ha suscitato fin da subito l'interesse delle persone.

Il progetto su Kickstarter è riuscito a raggiungere rapidamente il proprio obbiettivo e a decuplicarlo. Più di quattro mila Flipper Zero sono stati prodotti ed inviati dopo 18 mesi di attesa. Una volta consegnati, il Flipper Zero è diventato un trend virale su varie piattaforme social, che hanno permesso di mostrare le sue possibili applicazioni.

I video con più visualizzazioni e condivisioni rimangono, ad oggi, delle dimostrazioni su come il Flipper Zero possa essere utilizzato per piccole irregolarità, come lo spegnimento e accensione di schermi in luogo pubblico, oppure come lo spegnimento di lavagne elettroniche nei licei.

Questi brevi video hanno permesso di far conoscere il Flipper Zero ad un vasto pubblico, generando interesse nei confronti del nuovo oggetto.

La dialettica dell'essere "prodotto da hacker russi" porta avanti reminescenze dei film di spionaggio ambientati nel periodo della guerra fredda, mentre il ruolo che gli hacker sono arrivati a rappresentare, di tipologie specifiche di spie, a seguito delle varie operazioni di data leaks portati avanti da WikiLeaks e Anonymus, hanno fornito un sottotono perfetto per la creazione

di svariato materiale virale.

Il trend ha avuto come risultato, la creazione di una documentazione approfondita, per permettere ad esperti, e non, di comprendere il dispositivo e il suo funzionamento.

Parallelamente, sono stati sviluppati codici open source che hanno permesso di ricercare sempre nuove metodologie per l'uso del Flipper Zero come strumento per attacchi informatici.

Il design del Flipper Zero suggerisce una progettazione dell'oggetto più complessa, rispetto alla semplice idea di dispositivo pensato per avvicinare al mondo della cybersecurity anche le persone più lontane o giovani. È il Product Branding dell'oggetto che indirettamente sottolinea la dualità del dispositivo e che stimola l'interesse nei suoi confronti, rappresentando al meglio la definizione di "strumento da hacker nel corpo di un giocattolo".

2.1 Analisi dei concorrenti

Il successo mediatico del Flipper Zero ha permesso di attirare una nuova luce sugli strumenti utilizzati dagli esperti del settore. È necessario sottolineare però, come il Flipper Zero non sia un'invenzione, ma bensì un'innovazione di tecnologie già presenti nel mercato.

È possibile trovare i sensori presenti nel Flipper Zero come singolarmente reperibili a basso costo online, oppure in un negozio di elettronica. È possibile comprare il raspberry e trovare online tutorial per utilizzarlo in svariate modalità. È possibile trovare anche delle applicazioni che sfruttano i sensori dello smartphone per inviare attacchi a dizionario, spacciandosi per telecomandi universali [9, 35, 50], vendendo online anche chiavette che fungono da estensioni del telefono per trasmettere via infrarossi [7, 10].

Inoltre è possibile trovare anche il vero precursore del Flipper Zero, ovvero il pwaunagotchi 2.1 .

Figura 2.1: Pwaunagotchi

Il progetto del pwaunagotchi nasce nel 2019 su GitHub [8], completamente open source, e similmente al Flipper Zero presenta un personaggio all'interno del dispositivo, che ne definisce la personalità. Il design è completamente ispirato al Tamagotchi, un giocattolo molto diffuso a fine anni '90 e inizio degli anni 2000, che permetteva di prendersi cura di un animaletto virtuale. Il pwaunagotchi riprende l'idea dell'animaletto virtuale, aggiungendo la possibilità di operare sulle reti Wi-Fi.

Al suo interno è presente un Raspberry Pi 0 W, che permette di eseguire un continuo sniffing delle reti circostanti. Il pwaunagotchi ascolta le reti e ricerca un 4-way handshake , ovvero il momento nel quale un client si connette tramite password ad un server, all'interno una rete Wi-Fi Protected Access (WPA). Se non si verificano handshake nel breve termine, il pwaunagotchi applica due strategie principali [23]: invia pacchetti per la disconnessione dei client, oppure effettua una disabilitazione del servizio, tramite un attacco di Denial of Service. Così facendo i client sono obbligati a ricollegarsi ed effettuare un handshake con il server.

Il pwaunagotchi produce poi dei file `.pcap` che riportano il traffico di rete ascoltato. Questi file, mediante appropriati hardware e software, possono essere utilizzati per trovare le password di accesso.

Peculiarità di questo piccolo oggetto è data dall'algoritmo di Artificial Intelligence (AI) che lo costituisce. L'algoritmo gestisce in autonomia lo sniffing delle reti e cerca di accumulare più dati possibili relativamente all'ambiente circorstante.

Anch'esso è opensource e ha una community attiva di utenti. A differenza del Flipper Zero, dispone di tutorial su come costruire il proprio pwaunagotchi, sottolineando così la sua natura open source. Inoltre è esplicitamente un oggetto che permette di effettuare eavesdropping.

Il Flipper Zero è ispirato al pwaunagotchi [32], tanto da potersi considerare una sua evoluzione resa prodotto.

Sia il pwaunagotchi, che gli altri componenti elettronici, sono completamente personalizzabili e richiedono impegno da parte di coloro che desiderano utilizzare lo strumento. Il consumatore deve infatti essere attento nel reperire le tecnologie adatte e a programmarle correttamente per ottenere il risultato desiderato.

Il Flipper Zero è il primo prodotto commercializzato che risulta essere completo. Non sono necessarie conoscenze intriseche di informatica o elettronica per utilizzarlo. Questa caratteristica consente di vedere il Flipper Zero come uno strumento che permette anche alle persone meno esperte di interagire con il mondo della cybersecurity.

L'interazione di persone non competenti con sistemi di sicurezza, può risultare nel paradosso degli Script Kiddies (Skiddies), ovvero persone giovani, e quindi teoricamente inesperte, le quali, non comprendendo pienamente il funzionamento di una tecnologia o di un sistema di sicurezza, utilizzano degli strumenti creati da altri per effettuare determinate operazioni [51]. Comprendendo solo parzialmente il funzionamento degli strumenti, incorrono spesso in malware e virus informatici, che vengono diffusi all'interno del sistema, arrecando danni o effettuando illeciti in modo ignaro.

2.2 Nostalgia Marketing

Fondamentale all'interno del processo di creazione di un prodotto è la fase di Product Branding, ovvero quel processo di scelta e definizione dei tratti distintivi dell'oggetto.

La delineazione dell'identità del prodotto, fa sì che questo venga ricordato e riconosciuto dai consumatori nel tempo. Il Product Branding fa sì che il prodotto sia distinguibile dai suoi concorrenti di settore.

L'obbiettivo iniziale di ogni campagna pubblicitaria è catturare l'attenzione del consumatore [48]. In particolare, tramite le proprietà intrinseche dell'oggetto come forma, dimensioni, colori e luminosità, si ricerca l'attenzione automatica del consumatore. Queste caratteristiche catturano l'attenzione rapidamente e permettono un riconoscimento del prodotto, anche nel lungo periodo.

Nella propria identità, il Flipper Zero inserisce molti elementi vintage, ripresi dalle console di Videogioco Arcade degli anni '70 e dai Game Boy di inizio anni '90.

Questa correlazione con gli elementi del passato crea una relazione tra il marchio e la spinta del consumatore nell'acquistare il prodotto e a fidarsi del brand [38].

> *"Cognition is perhaps the first important consumer behavior reaction to occur as nostalgic cues will stimulate the retrieval/generation of thoughts through the consumer's memory/thought process. Memory and thought retrieval have their roots in psychology, and many marketers have adapted the theories related to memory to explain the cognitive outcomes in terms of marketing"*
> (Marchegiani, Phau [37])

La *Nostalgia Marketing* è una strategia di marketing che prevede l'inserimento, all'interno del prodotto, di caratteristiche che stimolino un sentimento di nostalgia, al fine di ottenere un maggior successo nel mercato [6].

La nostalgia influenza le preferenze dei consumatori relativamente a marchi, servizi e prodotti, tramite dei trigger emozionali che risultano essere decisivi nella selezione del prodotto [6]. In particolare, nel momento di selezione dell'articolo, un consumatore esclude la fase di comparazione con altri prodotti, data la fiducia che ripone nell'oggetto che genera in lui nostalgia.

La nostalgia fa riferimento alle memorie del passato, sia di quelle vissute direttamente, sia delle memorie acquisite tramite risorse esterne, quali filmografia e libri [52]. Nonostante il sentimento di nostalgia sia più forte nei soggetti in età adulta o avanzata, la nostalgia indiretta riesce a comprendere anche le fasce di età più basse [6].

In particolare nel caso del Flipper Zero, le sue caratteristiche provocano un sentimento di nostalgia per tutti coloro che hanno vissuto l'esperienza degli arcade e dei Game Boy, ma soprattuto anche di coloro che ne hanno avuta esperienza indiretta. Questo senso di nostalgia collettiva, stimola nei consumatori una preferenza nei confronti dei prodotti più popolari [11], incitando l'acquisto di oggetti che ricordano di un periodo passato, al fine di non sentire l'esclusione dal gruppo [11].

Per effettuare Nostalgia Marketing è importante che il prodotto abbia caratteristiche retrò, definte come Retro Martketing. Il Retro Marketing comprende: retro product, retro communication, retro branding, brand revitalization, retro style, and retro packaging [6].

In particolare il Flipper Zero, sfrutta ampiamente le sue caratteristiche retrò, sia come prodotto (relativamente ad aspetto e grafiche) sia a livello di comunicazione.

Il prodotto retrò (retro product), è un prodotto o un servizio che evoca ricordi e stimola un sentimento di nostalgia nel consumatore.[2]

La comunicazione retrò (retro communication) è una strategia di comunicazione che prevede l'utilizzo di campagne pubblicitarie ad hoc che inducono sentimenti nostalgici, creando una connessione tangibile con il passato [5]. Sottolineano così il valore intangibile del prodotto, tramite un senso di

sicurezza e tranquillità [6] portate dalla familiarità con lo stile proposto.

2.3 Gamification

Una delle caratteristiche peculiari del Flipper Zero è la sua immagine ludica. Questa caratteristica rinforza sia l'idea del Flipper Zero come strumento didattico, sia l'engagement nei confronti del prodotto, dal punto di vista del marketing.

Il gioco è una metodologia sempre più diffusa all'interno della pedagogia, poichè permette di insegnare passivamente a soggetti attivi e concentrati [49].

Questa concentrazione data dal carattere ludico, risulta utile nei contesti di vendita del prodotto, generando interesse da parte dei consumatori.

Il termine *Gamification* ha varie definizioni, in particolare vi si è spesso riferiti come l'adozione di elementi di design e di dinamiche appartenenti ai giochi, all'interno di contesti non di gioco, che risulta motivante per gli utenti [53].

Nel momento in cui gli oggetti con caratteristiche di gioco, sono servizi offerti al pubblico, come nel caso del Flipper Zero, la definizione più corretta risulta essere:

> *"Gamification refers to a process of enhancing a service with affordances for gameful experiences in order to support users' overall value creation."* (Kai Huotari, Juho Hamari [30])

Questa definizione permette di sottolineare come la Gamification si basi sull'esperienza di gioco. In questo caso il valore dell'oggetto viene dato esclusivamente dal rapporto, in particolare dall'engagement, che gli utenti hanno con esso. Questo rapporto edonistico con l'oggetto fa sì che l'utente lo riutilizzi più volte [34].

Tale caratteristica è determinante per il successo di un piccolo prodotto che si sta sviluppando sul mercato. Il Flipper Zero, nella propria pagina di

presentazione, elenca indirettamente tutti gli elementi che lo fanno rientrare all'interno della Gamification.

A livello di design il Flipper Zero ricorda una console di gioco portatile, instaurando passivamente l'idea che l'oggetto possa essere utilizzato per le medesime attività.

La mascotte del Flipper Zero, il cyber dolphin, ha come proprietà dei punti esperienza cumulabili che vengono raccolti ad ogni utilizzo del Flipper Zero, permettendo al delfino di raggiungere livelli superiori. Al raggiungimento del nuovo livello viene sbloccata una nuova grafica del delfino, come premio per il risultato ottenuto.

La presenza di livelli all'interno del Flipper Zero innesca un indiretto meccanismo di competizione e confronto tra i vari consumatori. Si crea un ideale di status di esperti, basandosi sul livello del cyber dolphin.

Queste caratteristiche spingono il consumatore ad utilizzare l'oggetto spesso, ricercando la soddisfazione nel ricevere il premio del superamento del livello.

I premi e la competizione sono, infatti, due fattori chiave all'interno della Gamification [29].

Inoltre la personalità del delfino che varia in base alla frequenza d'uso del Flipper Zero, costituisce una sorta di reminder per l'utente. L'interattività influenza l'attitudine dell'utente verso ciò che è percepito come divertente e giocoso [55].

La Gamification è uno strumento molto potente, che può essere applicata ad una moltitudine di oggetti, rivolgendosi verso la maggior parte delle fasce di età.

Nel contesto di un dispositivo, moralmente dubbio, come il Flipper Zero, rischia di diventare pericolosa. Forzare l'engagement dell'utente, nei confronti di un oggetto che può essere facilmente utilizzato per costituire degli

illeciti, necessita di regolamentazioni molto strette e controlli da parte delle istituzioni.

Capitolo 3

Benessere Sociale

La tipologia di attacchi informatici descritti precedentemente, è sempre stata di comune percezione, una nicchia di crimini relegata a coloro che sono esperti dell'ambito informatico.

L'informatica è una materia di studio molto recente, derivante da grandi teoremi matematici e solo da 40 anni alla portata di tutti.

Nonostante sia una tecnologia utilizzata nel quotidiano dalla quasi totalità della popolazione, la maggior parte degli utenti ne fa un uso ad alto livello[1], ignorando il funzionamento proprio della macchina.

Il Flipper Zero permette di utilizzare strumenti di basso livello tramite delle componenti di alto livello, progettate per un'interazione con l'utente altamente semplifcata, rendendo questi strumenti accessibili anche a coloro che ignorano la composizione degli stessi.

Questa caratteristica permette al prodotto di vendersi come un mezzo di diffusione della conoscenza, ma rimane una facile via di accesso a strumenti

[1] *Alto livello* è un termine utilizzato per indicare le componenti che permettono l'interazione tra macchina ed utente, tramite le quali è possibile comprendere ed utilizzare i dispositivi. Un esempio di componente di alto livello è l'interfaccia grafica. Il suo opposto è il *basso livello*, termine che indica le componenti meno astratte e più vicine al codice macchina.

utilizzati per aggirare agevolmente algoritmi matematici creati a difesa delle proprietà private o intelletive.

Viene fornito in mano un oggetto con il potenziale di un'arma anche a dei minori, ingannati dalla sembianze di un giocattolo.

Sicuramente le tecniche di marketing utilizzate mirano a raggiungere anche un pubblico giovane, rischiando però di far passare un messaggio erroneo, rendendo il crimine un gioco.

Scambiare per ludico, un crimine informatico, potrebbe indurre persone anche molto giovani a compiere crimini minori tramite il Flipper Zero.

Impedire la presenza di questa tipologia di dispositivi all'interno del mercato, al fine di evitare la diffusione di conoscenze relative all'aggiramento dei sistemi di sicurezza, non porterebbe come conseguenza all'impedimento dell'avvento di deteminati crimini.

Allo stesso modo sarebbe errato nascondere l'esistenza di armi che consentono questa tipologia di azioni, poichè non permetterebbe di sviluppare delle difese appropriate.

All'interno del mondo militare, vige il concetto di Security by Obscurity, ovvero dell'ideale di sicurezza dato dalla segretezza delle informazioni.

All'interno della cybersecurity, al contrario, vi è la concezione di sicurezza derivante dalla conoscenza delle informazioni.

In particolare, all'interno del mondo della cybersecurity, la sicurezza è data dall'inattaccabilità di un determinato algoritmo. Come accennato nel capitolo 1.1, gli algoritmi di cifratura e decifratura, utilizzati per l'occultamento delle informazioni, hanno una procedura chiara e conosciuta da tutti.

La sicurezza non è data dal funzionamento di un algoritmo tenuto nascosto, bensì dall'efficacia dell'algoritmo stesso di resistere ad attacchi informatici.

Il confronto tra il mondo militare e il mondo della cybersecurity è necessario, in quanto entrambe le realtà esistono come difesa da agenti nocivi; poichè il Flipper Zero può essere considerato un'arma, vanno discusse le sue implicazioni in quanto tale.

Il Flipper Zero non è un'arma offensiva che provoca danni fisici, ma è possibile utilizzarlo in una serie di circostanze che permettono il furto di proprietà e informazioni. Data l'importanza che le informazioni stanno rapidamente acquisendo all'interno della vita di tutti i giorni, è necessario salvaguardarle.

Conoscere il funzionamento delle nuove tecnologie e il loro potenziale, permette di aggiornare ed integrare le misure di sicurezza esistenti. Inoltre, essere a conoscenza di determinati punti deboli che potrebbero essere sfruttati, permette di prevenire determinati attacchi e rinforzare le difese.

Se le informazioni fossero tenute nascoste, rispettando la dottrina militare, si verrebbe a conoscenza di determinati punti deboli esclusivamente a posteriori di un attacco (zero-day), subendo maggiori danni, come illustrato nel capitolo 1.1.2.

Un lato positivo delle community è anche la possibilità di avere un gran numero di persone dedite allo stesso progetto e al suo sviluppo, con numero di partecipanti tale che non sarebbe possibile ottenere all'interno di un team di sviluppo legato via contratto.

"*Given enough eyeballs, all bugs are shallow*" [41] è una citazione tratta da Raymond che sottolinea come l'open source sia in realtà una modalità di miglioramento del codice che tramite partecipanti attivi identifica le falle di sicurezza e permette di operare al fine di eliminarle.

È quindi importante essere a conoscenza di determinati strumenti e del loro funzionamento interno, la possibilità di codici open source diffusi nelle varie piattaforme permette di conoscere le modalità di attacco dell'oggetto e iniziare a progettare delle misure di difesa adeguate, per delle tipologie di

attacchi che grazie a questo dispositivo tenderanno a diventare più frequenti.

3.1 Dilemma Morale

La produzione di oggetti della portata del Flipper Zero, porta indirettamente a porsi davanti questioni etiche e morali, sopratutto a seguito del contrasto tra gli ideali di sicurezza militare e gli ideali di sicurezza del mondo della cibersicurezza.

La questione se la Flipper Devices Inc. (casa produttrice del Flipper Zero) abbia introdotto un prodotto moralmente etico, oppure moralmente dubbio, può essere discussa considerando la Dottrina del Doppio Effetto.

La Dottrina del Doppio Effetto è basata sulla distinzione tra ciò che un uomo prevede come risultato della sua volontaria e cosa invece, intende in senso stretto [15]. Più chiaramente: le nostre azioni non hanno soltanto conseguenze buone, da noi espressamente volute e desiderate, e quindi intenzionali, ma possono avere anche conseguenze cattive non intenzionali, che prevediamo accompagneranno quelle volute. [17]

La dottrina quindi serve a stabilire non a quali condizioni un atto diventa lecito, ma solo fino a che punto sia possibile compiere un atto lecito quando si è a conoscenza che esso abbia conseguenze sia buone che cattive[17].

È possibile quindi ipotizzare che la produzione del Flipper Zero sia spinta da ideali di diffusione della conoscenza e volontà di avvicinamento al mondo della cybersecurity per più persone, dalla volontà di offrire un servizio a coloro che lavorano come pentester semplificando le operazioni; e che gli effetti collaterali quali la scelta di utilizzare questo determinato prodotto come arma o come mezzo per commettere dei reati, sia una presa di responsabilità che non riguarda la Flipper Devices Inc., ma sia una scelta propria degli

utenti utilizzatori del Flipper Zero.

Dal punto di vista giuridico, la responsabilità è difatti di coloro che utilizzano il Flipper Zero come arma, ma rimane difficile intendere una totale ingenuità da parte di coloro che producono il Flipper Zero su come questo possa essere utilizzato anche come arma per perpetrare attacchi informatici.

Secondo gli ideali di open source, è corretta la diffusione della conoscenza di uno sturmento che possa essere utilizzato anche come arma, andando ad allargare la possibilità di formazione conseguibile tramite questo oggetto.

Riprendendo l'ideale Platonico che vede il male come un errore di valutazione dovuto ad un'educazione insufficiente[2], è possibile giustificare gli ideali di diffusione della conoscenza dichiarati dalla Flipper Devices Inc., imputando le scelte di utilizzo dello strumento come arma esclusivamente ai suoi utilizzatori.

Non va comunque esclusa l'ipotesi che questa giustificazione sia in realtà un tentativo di ridicolizzare e sviare l'attenzione da un fenomeno sempre più presente, ovvero la produzione e diffusione di armi per attacchi informatici.

3.2 Atti legislativi

Il Flipper Zero è uno strumento diventato virale grazie ad una moltitudine di esempi che ne mostrano l'utilizzo nel commettere illeciti. Le narrative proposte sia dai Social Media, che dalle repository presenti su GitHub mostrano come il Flipper Zero sia in realtà un oggetto utilizzato principalmente per effettuare crimini informatici.

[2] "*E quasi tutto quello che si chiama intemperanza nei piaceri e sì rimprovera, come se gli uomini fossero malvagi volontariamente, non si biasima a ragione. Perché malvagio nessuno è di sua volontà, ma il malvagio diviene malvagio per qualche prava disposizione del corpo e per un allevamento senza educazione, e queste cose sono odiose a ciascuno e gli capitano contro sua voglia*" Platone, Timeo, 86 d-e

All'interno del termine *crimini informatici* sono compresi tutti quei crimini commessi tramite l'utilizzo di una specifica tecnologia [36].

I crimini informatici, in Italia, sono regolamentati dal Codice Penale. L'applicabilità del Codice Penale è limitata dal Principio di Legalità, espresso dall'articolo 1 - *Reati e pene: disposizione espressa di legge* [45].

Il Principio di Legalità comprende il Divieto di Analogia[3] e di conseguenza permette di definire reato esclusivamente ciò che è espresso all'interno del Codice Penale.

Relativamente alle tecnologie e alla loro rapida evoluzione, questo crea un vuoto legislativo.

All'interno del Codice Penale esistono articoli che definiscono reati informatici, come il reato di *Accesso abusivo ad un sistema informatico o telematico* (Art. 615-ter), ma non sono presenti all'interno del sistema legislativo generale regolamentazioni applicabili ad oggetti come il Flipper Zero.

Come citato in precedenza, il Flipper Zero non costituisce un'invenzione, poichè i suoi componenti presi singolarmente hanno le stesse potenzialità criminose, ma non sono considerati una minaccia, in quanto vengono utilizzati quotidianamente all'interno di altre tecnologie innocue.

Esistono svariati dispositivi utilizzati come hacking tools che vengono commercializzati, ma nonostante siano meno virali del Flipper Zero, sono comunque legali.

La legislazione non dovrebbe quindi essere mirata alla limitazione dell'uso delle componenti intrinseche del Flipper Zero, bensì a regolamentarne l'utilizzo.

Esattamente come il Garante della Privacy ha limitato le modalità di utilizzo di ChatGPT[18], così sarebbe necessario l'intervento del legislatore per

[3]Divieto di Analogia: è vietato per l'interprete, l'attività di applicare una norma ad un caso non completamente ricoperto o descritto da essa.

regolamentare l'uso del Flipper Zero.

Il prodotto mostra delle autodichiarazioni che garantasticono la conformità delle tecnologie utilizzate a livello globale, ma all'interno di queste l'oggetto viene dichiarato come "*Portable handheld electronic device featuring virtual pet, designed for education, development and prototyping of electronics and software*" [14].

Questa dichiarazione svicola dal reale utilizzo del Flipper Zero, poichè vengono omesse le reali funzionalità dell'oggetto, alcune delle quali sono illustrate nel capitolo 1.3.2 , che senza necessità di alcune espansioni, è utilizzabile come clonatore di dispositivi di accesso.

Ad oggi, nel mondo, le legislature hanno limitato l'utilizzo del Flipper Zero in Brasile e la reperibilità dello stesso negli Stati Uniti d'America.

3.2.1 Brasile

All'interno del Brasile, le telecomunicazioni vengono regolamentate dall'Agenzia Nazionale delle Telecomunicazioni (Anatel), la quale è stata fondata nel 1997 a seguito del Decreto 2338 del 07/10/1997. L'Anatel è legata al Ministero delle Comunicazioni, con la funzione di organismo di regolamentazione delle telecomunicazioni [27] .

L'Anatel è stata la prima a livello mondiale, ad effettuare delle regolamentazioni relativamente al Flipper Zero, in particolare ha dichiarato a Marzo 2023, che *"l'apparecchiatura è un'emittente di radiofrequenze e richiede la certificazione dell'Agenzia per essere utilizzata"*[1].

La dichiarazione spiega come Anatel, appellandosi all'articolo 2 della Ley General de Telecomunicaciones (LGT) [28], richiami l'obbligo di certificazione come condizione necessaria per l'uso del Flipper Zero all'interno del Brasile.

I requisiti per l'ottenimento della certificazione, non sono però soddisfatti dalla costituzione stessa del Flipper Zero; l'utilizzo dello spettro radioelettrico per la clonazione dei segnali rappresenta un rischio troppo elevato per la diffusione del dispositivo sul mercato brasiliano.

La limitazione d'uso del dispositivo si applica esclusivamente all'uso personale del Flipper Zero, il quale può comunque essere utilizzato dagli agenti pubblici e dagli enti di sicurezza, previa omologazione. [1]

3.2.2 Stati Uniti - Amazon

Amazon è una delle principali aziende per il commercio al dettaglio. Negli Stati Uniti, Amazon ha fatto rientrare il Flipper Zero all'interno della categoria *Lock Picking and Theft Devices* [3], in particolare sotto la voce 'Dispositivi designati per la duplicazione delle chiavi'.

Questa definizione risulta assolutamente corretta relativamente all'uso del Flipper Zero, ma la peculiarità di questa restrizione è la sua provenienza.

Il Flipper Zero è libero di circolare nel mercato statunitense, viene distribuito tramite i grandi rivenditori, come ad esempio Walmart, un'altra catena di department store. Ma Amazon si è trovato costretto a bloccare la vendita del Flipper Zero sulla propria piattaforma per via delle leggi federali relative al servizio di posta. [3]

Il Codice delle Leggi degli Stati Uniti d'America, specifica all'interno della sezione *Nonmailable locksmithing devices and motor vehicle master keys*, 18 U.S.C. §1716A [43] e della sezione *Nonmailability of locksmithing devices*, 39 U.S.C. §3002a [44] come il commercio di dispositivi che sono designati all'apertura non autorizzata o alla duplicazione delle chiavi, sia espressamente vietata. La pena ricade sia sul mittente dell'oggetto, sia sul servizio utilizzato per la spedizione.

In questo modo Amazon si tutela nei riguardi di dispositivi non regolamentati dalla legge.

In questo caso la legislazione non regolamenta l'utilizzo degli oggetti in modo diretto, ma cerca di prevenirne la diffusione regolamentando il servizio di posta.

Capitolo 4

Conclusione

La crescente diffusione del Flipper Zero solleva ulteriori riflessioni sulla direzione in cui si sta sviluppando il panorama della cybersecurity.

L'evoluzione degli attacchi informatici mostra una tendenza verso tipologie di attacco sempre più sofisticate ed insidiose. Parallelamente, a contrario di questa complessità crescente, si assiste alla produzione di strumenti che semplificano le modalità di perpetrare tali attacchi.

Questi strumenti sviluppano un'interfaccia altamente user friendly, permettendo anche a coloro che non sono esperti della materia di utilizzarli senza alcuna difficoltà.

Il paradosso dello Skiddie, precendemente relegato alla semplice riproduzione di codice senza una completa comprensione dello stesso, si sta ampliando anche verso strumenti più sofisticati.

L'utilizzo di un marketing con scopo ludico o pedagogico è fuorviante rispetto alla reale importanza dell'accaduto. Semplificando le modalità di accesso ad armi per attacchi informatici, si aumenta anche la probabilità che questi possano verificarsi.

Il Flipper Zero raggiunge il suo obbiettivo da educatore nell'evidenziare l'attuale mancanza di conoscenza generale nei confronti della cybersecurity, mascherando da giocattolo uno strumento che permette di perpetrare pesanti attacchi informatici.

L'applicazione di strategie di marketing mirate ad aumentare e prolungare nel tempo l'interazione con l'oggetto, accostate ad una promozione dello stesso prima come giocattolo e poi come strumento per la cybersecurity, risultano in una riduzione dell'importanza dell'oggetto stesso, che viene quindi percepito come innocuo.

Tramite il camuffamento da giocattolo fa si di sottolineare il livello di semplicità di diffusione che hanno raggiunto questa tipologia di strumenti, ma sopratutto la facilità con la quale questi possano essere utilizzati, senza necessità di conoscenza o abilità specifiche da parte dei consumatori.

Il quesito se sia moralmente corretta la produzione e vendita di dispositivi con questi potenziali, non ha una risposta definitiva e conclusiva. I principi del codice open source permettono di vedere questa aperta produzione come un'opportunità per accrescere la consapevolezza relativamente a questi dispositivi e di movimentare la ricerca per sistemi di difesa più completi.

La comprensione e l'importanza della cybersecurity è un tema sempre più attuale in un mondo che sta digitalizzando molto rapidamente.

Ci si sta mobilitando a livello normativo per gestire e regolamentare le possibili nuove realtà che si stanno creando, basti pensare alla direttiva NIS 2 entrata in vigore recentemente.

Ciò che rimane ancora statica è la conoscenza delle persone verso questa tipologia di pericoli e attacchi. È importante introdurre una formazione adatta, per permettere che la comprensione dei possibili pericoli arrivi ad essere cultura generale; e contemporaneamente movimentare la ricerca verso nuovi sistemi di difesa.

Bibliografia

[1] Agência Nacional de Telecomunicações - Anatel: *Anatel presenta chiarimenti su Flipper Zero*. 2023. – URL https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-apresenta-esclarecimentos-sobre-o-flipper-zero

[2] Amatulli, Cesare ; Pino, Giovanni ; Deangelis, Matteo ; Cascio, Robert: Understanding purchase determinants of luxury vintage products. In: *Psychology & Marketing* 35 (2018), 05. – URL https://doi.org/10.1002/mar.21110

[3] Amazon: *Amazon Seller Central - Lock Picking & Theft Devices*. – URL https://sellercentral.amazon.com/help/hub/reference/external/G200164850#mnd_2jc_jcb__SECTION_754452FAC8644E8A94FA0D97229FDB96

[4] bigbrodude6119: *Video dimostrativo per la feature di Rogue Access Point*. – URL https://www.youtube.com/watch?v=Y8aBjpd3XI4

[5] Brown, Stephen ; Kozinets, Robert ; Sherry, John: Sell Me the Old, Old Story: Retromarketing Management and the Art of Brand Revival. In: *Journal of Customer Behaviour* 2 (2003), 06, S. 133–147

[6] Crespo-Pereira, Veronica ; Membiela-Pollán, Matías ; Sánchez-Amboage, Eva: Nostalgia, Retro-Marketing, and Neuromarketing: An Exploratory Review. 7 (2022), 01, S. 127. – URL https://doi.org/10.56140/JOCIS-v7-5

[7] DERCLIVE: *DERCLIVE - Telecomando IR per smartphone con telecomando a infrarossi.* – URL https://www.amazon.it/DERCLIVE-Telecomando-smartphone-telecomando-infrarossi/dp/B09CKTJYV7/ref=asc_df_B09CKTJYV7/?tag=googshopit-21&linkCode=df0&hvadid=610945603150&hvpos=&hvnetw=g&hvrand=17419704917991206596&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=1008141&hvtargid=pla-1678830342603&th=1

[8] EVILSOCKET: *Pwaunagotchi - repository.* – URL https://github.com/evilsocket/pwnagotchi

[9] EVOLLY.APP: *App Store - TV Remote Universal Control.* – URL https://apps.apple.com/it/app/tv-remote-universal-control/id1539090879

[10] EVOLLY.APP: *MatrixWielder™.* – URL https://apps.apple.com/it/app/tv-remote-universal-control/id1539090879

[11] FAN, Yafeng ; JIANG, Jing ; HU, Zuohao: Abandoning distinctiveness: The influence of nostalgia on consumer choice. In: *Psychology & Marketing* 37 (2020), 10

[12] FLIPPER DEVICES INC.: *Documentazione del flipper.* – URL https://docs.flipper.net

[13] FLIPPER DEVICES INC.: *Flipper Zero - Sito web ufficiale.* – URL https://flipperzero.one

[14] FLIPPER DEVICES INC.: *EU Declaration of Conformity.* 2022. – URL https://cdn.flipperzero.one/RED-DOC.pdf?_gl=1*147ct8w*_ga*MjA0MTEyODQ1Mi4xNjk5MjY4NjAw*_ga_GM78S6JK0K*MTY5OTI2ODYwMC4xLjAuMTY5OTI2ODYwMC42MC4wLjA.

[15] FOOT, Philippa: The Problem of Abortion and the Doctrine of the Double Effect. In: *Oxford Review* 5 (1967), S. 5–15

[16] Formosa, Paul ; Wilson, Michael ; Richards, Deborah: A principlist framework for cybersecurity ethics. In: *Computers & Security* 109 (2021), S. 102382. – URL https://www.sciencedirect.com/science/article/pii/S0167404821002066. – ISSN 0167-4048

[17] Francesco Tito: *Corsi di Bioetica e di Etica della Medicina e della Biologia - a.a. 2014/2015.* – URL https://www.uniba.it/it/docenti/de-franco-raffaella/attivita-didattica/materiale-didattico-1

[18] Garante per la protezione dei dati personali: *Provvedimento dell'11 aprile 2023 [9874702].* – URL https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9874702

[19] GitHub, 0xchocolate: *Repository Flipper Zero Wifi Marauder.* – URL https://github.com/0xchocolate/flipperzero-wifi-marauder

[20] GitHub, bigbrodude6119: *Repository Git Hub per funzionalità Evil Portal, per effettuare il Rogue Access Point.* – URL https://github.com/bigbrodude6119/flipper-zero-evil-portal

[21] GitHub, Dark Flippers: *Multi Fuzzer Plugin.* – URL https://github.com/DarkFlippers/Multi_Fuzzer

[22] GitHub, Dark Flippers: *Sub-GHz Bruteforcer Application for Flipper Zero.* – URL https://github.com/DarkFlippers/flipperzero-subbrute

[23] Github, evilsocket: *Pwaunagotchi - documentazione ufficiale.* – URL https://pwnagotchi.ai/intro

[24] GitHub, H4ckd4ddy: *Repository Git Hub per sfruttamento delle vulnerabilità delle cassaforti di marca Sentry Safe e Master Lock.* – URL https://github.com/H4ckd4ddy/bypass-sentry-safe

[25] GitHub, Tobia Bocchi: *Plugin per Brute Force OOK tramite Flipper Zero.* – URL https://github.com/tobiabocchi/flipperzero-bruteforce

[26] Goodin, Dan: This tiny device is sending updated iPhones into a never-ending DoS loop. In: *arstechnica.* – URL https://arstechnica.com/security/2023/11/flipper-zero-gadget-that-doses-iphones-takes-once-esoteric-attacks-mainstream/

[27] Governo del Brasile: *DECRETO Nº 2.338, DE 7 DE OUTUBRO DE 1997. REGULAMENTO DA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES.* 1997. – URL https://www.planalto.gov.br/ccivil_03/decreto/d2338.htm

[28] Governo del Brasile: *LEI Nº 9.472, DE 16 DE JULHO DE 1997. LEY GENERAL DE TELECOMUNICAÇÕES.* 1997. – URL https://www.planalto.gov.br/ccivil_03/decreto/d2338.htm

[29] Hamari, Juho ; Koivisto, Jonna ; Sarsa, Harri: Does Gamification Work? – A Literature Review of Empirical Studies on Gamification. (2014), S. 3025–3034. – URL https://doi.org/10.1109/HICSS.2014.377

[30] Huotari, Kai ; Hamari, Juho: A definition for gamification: anchoring gamification in the service marketing literature. In: *Electronic markets* 27 (2017), S. 21–31. – URL https://doi.org/10.1007/s12525-022-00575-7

[31] ISO/IEC JTC 1: Cards and security devices for personal identification. Contactless proximity objects. Radio frequency power and signal interface / International Organization for Standardization. BSI, Juli 2020. – Standard. – ISBN 978 0 539 27502 5

[32] KICKSTARTER, Flipper Devices Inc.: *Flipper Zero — Multi-tool Device for Hackers.* – URL `https://www.kickstarter.com/projects/flipper-devices/flipper-zero-tamagochi-for-hackers`

[33] LEVY, Steven: *Hackers: Heroes of the Computer Revolution.* Penguin USA, 2001

[34] LIN, Kuan-Yu ; LU, Hsi-Peng: Predicting mobile social network acceptance based on mobile value and social influence. In: *Internet Research* 25 (2015), 02, S. 107–130. – URL `https://doi.org/10.1108/IntR-01-2014-0018`

[35] LTD, Beijing Xiaomi Mobile Software C.: *Mi Remote controller.* – URL `https://play.google.com/store/apps/details?id=com.duokan.phone.remotecontroller&hl=it&gl=US`

[36] MANJIKIAN, Mary: *Cybersecurity Ethics.* Routledge, 2018

[37] MARCHEGIANI, Christopher ; PHAU, Ian: Away from "Unified Nostalgia": Conceptual Differences of Personal and Historical Nostalgia Appeals in Advertising. In: *Journal of Promotion Management* 16 (2010), 03, S. 85. – URL `https://doi.org/10.1080/10496490903572991`

[38] MERCHANT, Altaf ; LATOUR, Kathryn ; FORD, John ; LATOUR, Michael: How Strong is the Pull of the Past? Measuring Personal Nostalgia Evoked by Advertising. In: *Journal of Advertising Research* 53 (2013), 06, S. 150–165. – URL `https://doi.org/10.2501/JAR-53-2-150-165`

[39] ORGANIZATION, Xtreme: *Xtreme-Firmware Bad Keyboard feature, repository su Git Hub.* – URL `https://github.com/Flipper-XFW/Xtreme-Firmware#bad-keyboard`

[40] PATTISON, James: From defence to offence: The ethics of private cybersecurity. In: *European Journal of International Security* 5 (2020), Nr. 2, S. 233–254

[41] Raymond, Eric S.: *The cathedral and the bazaar*. Springer Netherlands, 1999. – 23–49 S

[42] Reddit thatismyusername_: *Segnalazioni da parte dei consumatori dei limiti imposti dalla dogana israeliana.* 2022. – URL https://www.reddit.com/r/flipperzero/comments/wo204r/my_flipper_got_refused_by_government/

[43] Representatives, Office of the Law Revision Counsel of the United States House of: *Injurious Articles as Nonmailablity of locksmithing devices,18 U.S.C. 1716A*. 2009. – URL https://www.govinfo.gov/content/pkg/USCODE-2009-title18/html/USCODE-2009-title18-partI-chap83-sec1716A.htm

[44] Representatives, Office of the Law Revision Counsel of the United States House of: *Nonmailability of Locksmithing Devices, 39 U.S.C. 3002a.* 2011. – URL https://www.govinfo.gov/content/pkg/USCODE-2011-title39/html/USCODE-2011-title39-partIV-chap30-sec3002a.htm

[45] Repubblica Italiana: Art. 1 - Reati e pene: disposizione espressa di legge. In: *Codice Penale* (1930)

[46] Rogue Master: *Documentazione della Repository di Git Hub che spiega come utilizzare il plugin di apertura delle cassaforti.* – URL https://github.com/RogueMaster/flipperzero-firmware-wPlugins/blob/420/documentation/SentrySafe.md

[47] Rogue Master: *Repository del firmware principale di raccolta dei plugin del Flipper Zero.* – URL https://github.com/RogueMaster/flipperzero-firmware-wPlugins

[48] Rumen Pozharliev, Patrizia C.: *La mente del consumatore: Guida applicata al neuromarketing e alla consumer neuroscience*. LUISS University Press, 2020

[49] Saravanakumar, G: GAMIFICATION AND LEARNING: ENGAGING STUDENTS THROUGH PLAYING. In: *EDUCATION 5.0: REVOLUTIONIZING LEARNING FOR THE FUTURE* (2023), S. 176

[50] Services, Codematics: *App Store - Universal TV Remote Control.* – URL `https://apps.apple.com/it/app/telecomando-tv-universale/id1492122256`

[51] Sheenan, John: Computer Viruses and Younger Users - who are the script kiddies? (2023), 08

[52] Sierra, Jeremy ; Mcquitty, Shaun: Attitudes and Emotions as Determinants of Nostalgia Purchases: An Application of Social Identity Theory. In: *Journal of Marketing Theory and Practice* 15 (2007), 04, S. 99–112. – URL `https://doi.org/10.2753/MTP1069-6679150201`

[53] Spil, Ton ; Sunyaev, Ali ; Thiebes, Scott ; Baalen, Rolf: The Adoption of Wearables for a Healthy Lifestyle: Can Gamification Help? (2017), 01. – URL `https://doi.org/10.24251/HICSS.2017.437`

[54] Stiawan ; Idrisand ; Abdullah ; Aljaber ; Budiarto: Cyber-Attack Penetration Test and Vulnerability Analysis. In: *International Journal of Online and Biomedical Engineering (iJOE), 13(01)* (2017). – URL `https://online-journals.org/index.php/i-joe/article/view/6407`

[55] Zichermann, Gabe ; Cunningham, Christopher: *Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps.* 1st. O'Reilly Media, Inc., 2011. – ISBN 1449397670

Ringraziamenti

In primis vorrei ringraziare il mio correlatore, Giacomo, grazie per l'assistenza continua e per avermi sempre entusismato per il lavoro che stavo facendo.

Vorrei ringraziare i miei genitori, per il loro supporto costante, anche quando la mia ansia risultava difficile da gestire e comprendere. Vorrei ringraziarli per aver sempre creduto in me, ancora prima che ci credessi io. Grazie per avermi spronato contro ogni ostacolo. Sopratutto grazie papà per le ispirazioni e grazie mamma per le correzioni grammaticali.

Vorrei ringraziare le mie nonne, stendardo e ispirazione del fatto che non serve un costume per essere wonder woman. Un pensiero speciale a nonna Eugenia, che mi aveva promesso che sarebbe stata presente oggi con il suo abito migliore, e che sono sicura indossi mentre mi guarda dall'alto.

Un grazie a Dawid, senza di te questa tesi non esisterebbe, grazie per l'affetto e il supporto costante.

Un ringraziamento a tutti i miei amici, siete molti da nominare, ma grazie per ogni parola dolce che avete speso nei miei confronti anche non comprendendo la mia situazione o piano di studi. Un grazie speciale ad Alice, mia consulente giurista, senza la quale avrei un capitolo scritto con i piedi. Un grazie a Betta, Laura, Lara, Cov, Deno, Baldo e tutti gli amici di Ancona, per farmi sentire sempre accolta e a casa.

Un grazie ai poggesi, agli ngiunghiti, mi avete insegnato che se ti metti in testa di scalare un monte per costruirci un rifugio, nella vita puoi fare tutto, con un sorriso, qualche battuta e un pezzetto di cioccolata.

Un grazie alla mia cricca di Bolognesi, dalle mie stupende coinquiline, compagne di serate passate a fare discorsi profondi sul balcone; grazie ai moschettieri e alla mia balotta universitaria, specialmente a Greta, Simo e Tommi. Vi voglio bene, siete la conferma che i luoghi vengono resi belle dalle persone che incontriamo, avete reso Bologna un posto più che speciale.

Infine grazie a Bologna, per avermi accolta, nella sua rossa uggiosa pianura, dandomi la possibilità di incrociare la mia vita con quella di centinaia di persone diverse fra loro, che mi hanno fatta crescere e arricchita. Per avermi insegnato un sacco di vocaboli del dialetto bolognese che farò fatica a disimparare, soprattutto perché controvoglia.

Questa è la prima tappa di un viaggio, continuiamo a tutta dritta.