CYBER BLUFF

EXTRA

In questi extra trovate delle brevi note al libro *Cyber Bluff*, divise per capitoletti. Sono da intendersi appunto come note, suggestioni e consigli per approfondire. Sono una selezione secondo il nostro gusto personale, sicuramente non esauriscono gli argomenti, ma sono come tutto il libro un invito a ricercare autonomamente quello che più vi ha interessato o colpito. Non coprono esattamente tutti i capitoli, in alcuni non avevamo molto da aggiungere e per altri il materiale a disposizione è veramente tanto e variegato, si è scelto quindi di segnalare le risorse a nostro parere più di nicchia, ma valide, o in altri casi quelle più riassuntive, da cui trarre ulteriori spunti. Non è improbabile, ma non datelo per sicuro, che se emergeranno curiosità, dimenticanze clamorose o filoni di indagine particolarmente interessanti durante le presentazioni del libro o nelle chiaccherate con qualche lettore questa sezione degli extra venga aggiornata.

Introduzione

Origine militare e storia di Internet

Sull'origine militare di Internet nel periodo della guerra in Vietnam consiglio la lettura di Yasha Livine, *Survelliance Valley*: https://surveillancevalley.com/

Alcuni degli episodi riportati in questo capitolo sono ripresi proprio da questo libro.

Ci sono diversi articoli accademici che trattano la storia di Internet. Uno dei più noti:

https://arxiv.org/html/cs/9901011

In generale è difficile tracciare un percorso unico, ogni ammennicolo elettronico, protocollo, programma apre un potenzialmente diverso filone di indagine.

Hacking

La storia della scena hacker è piuttosto complessa da tracciare. Per quanto riguarda gli Stati Uniti consiglio la lettura di

- *Hackers. Gli eroi della rivoluzione informatica* di Steven Levy
- *Giro di vite contro gli hacker. Legge e disordine sulla frontiera elettronica* di Bruce Sterling
- *Crypto* di Steven Levy

In verità si tratta di racconti e narrazioni molto parziali, la documentazione più diretta, in mancanza di fonti orali, sono forse le fanzine, pubblicazioni di solito solo digitali, dove venivano ospitati interventi tecnici accanto a riflessioni di senso, sfoghi, invettive ecc. A volte sgrammaticate, a volte piccole gemme, rappresentano la voglia di condividere le conoscenze, di accrescere le capacità del gruppo, di contribuire a una comunità diffusa e deteritorializzata.

CYBER BLUFF

EXTRA

Sulla scena italiana qualcosa si trova qui

https://www.autistici.org/hacking_e-zines/

La prima fanzine citata, ma non presente nel sito (*Butchered from inside*) si può recuperare da

http://www.s0ftpj.org/it/site.html

Se si preferisce il cartaceo c'è qualche libro, pochi in verità, tutti sanamente parziali, ovvero si racconta quello che si sa e si è vissuto, quindi sono una piccola parte del tutto.

Per un quadro molto parziale si dovrebbe leggere

- *+ kaos, 10 anni di hacking e mediattivismo*

https://www.agenziax.it/index.php/kaos

https://networkcultures.org/blog/publication/kaos-ten-years-of-hacking-and-media-activism/

- *Spaghetti hacker*, Stefano Chiccarelli e Andrea Monti, Apogeo, 1997

Parte della scena italiana: la parte più esplicitamente politicizzata, sicuramente non tutta, converge intorno a un incontro annuale. Per approfondire

https://www.hackmeeting.org

Esistono anche dei ritrovi "fissi" e più "territoriali" partoriti dall'esperienza di Hackmeeting, gli hacklab.

Questa pubblicazione è senza dubbio figlia di questa comunità e delle discussioni che negli anni l'hanno animata.

Per la scena internazionale consigliamo di buttare un occhio almeno a

- Phrack https://www.phrack.org
- Poc||Gtfo https://www.alchemistowl.org/pocorgtfo/

Più o meno ogni nazione ha avuto una propria scena hacker, sarebbe interessante indagare cosa è stato prodotto nell'Est del mondo per esempio, ma il problema della lingua risulta per me difficile da superare.

Per un'analisi giornalistica, ma non banale di alcune vicende e episodi del mondo dell'hacking internazionale, con il taglio da spy story, consigliano di leggere le produzioni di Carola Frediani:

- *Guerre di rete*, Laterza 2018
- *#Cybercrime. Attacchi globali, conseguenze locali*, Hoepli, 2019
- *Dentro Anonymous. Viaggio nelle legioni dei cyberattivisti*, 2012
- *Deep web. La rete oltre Google. Personaggi, storie e luoghi dell'internet profonda*, 2014

Segnaliamo infine la newsletter https://guerredirete.substack.com/ curata dall'autrice.

CYBER BLUFF

EXTRA

Home computing ‘80

Etichettato oggi con il termine retro computing. In rete potete trovare praticamente ogni tipo di risorsa su questo argomento, dagli emulatori di vecchie piattaforme, alle riviste e libri dell’epoca, anche il software abbonda.

Un paio di link per tutti, per le due piattaforme più note. Software e libri.

ZX Spectrum

https://archive.org/details/softwarelibrary_zx_spectrum

https://archive.org/search.php?query=Sinclair%20ZX%20Spectrum

Commodore 64

https://archive.org/details/softwarelibrary_c64

https://archive.org/details/books?and%5B%5D=commodore+64&sin=

Un universo piuttosto interessante da esplorare in questo ambito sono le scene demo sviluppatesi attorno a queste piattaforme. Le demo sono degli esercizi di stile: immagini, suoni e scritte che scorrono sullo schermo, cercando di spremere le scarse risorse della macchina al massimo. Nascono all’interno della scena del software pirata, in particolare dei giochi. Le diverse crew di cracker (persone che sproteggono i software per poterli copiare) usavano far precedere il programma copiato con una sorta di intro, con effetti grafici e il nome del gruppo. L’approccio era simile ai writer che dipingevano i treni, perché la loro tag, i propri messaggi uscissero dal quartiere e viaggiassero per la città. Ai tempi il software era diffuso con i mezzi più svariati: all’inizio i modem erano lenti, e non ci si deve immaginare persone che comunicano unicamente attraverso la rete. Il software copiato veniva spedito per posta, spesso acquistato sottobanco nei negozi di computer, o scambiato a mano con amici e parenti. In alcuni paesi venivano organizzati degli incontri più o meno clandestini, detti “copy party”, in cui ci si scambiava i software piratati, si discuteva di tecniche di cracking e i diversi gruppi si sfidavano in “demo contest”, con tanto di giuria.

A un certo punto la scena delle demo diviene però autonoma: il gioco perde di importanza, anche il cracking, e l’attenzione si sposta sulla scrittura di demo tecnicamente elaborate, con una propria autonomia narrativa.

Nasce così quella scena che sopravvive fino ad oggi tra persone appassionate di retro computing, grafica, musica e programmazione. Le crew “contemporanee” sono di solito composte da elementi piuttosto specializzati: chi si occupa della musica, chi della grafica, chi dei testi, chi programma. La struttura organizzativa ricalca in piccolo, quella di un team di sviluppo di un videogame.

Alcune crew inseriscono elementi di critica politica o sociale nelle proprie demo, si veda per esempio

- Booze design, Uncensored, https://www.youtube.com/watch?v=9LFD4SzW3e0

Per avventurarsi nel mondo delle demo per c64 si può visitare

- https://csdb.dk/

CYBER BLUFF

EXTRA

Retro computing in genere

Se vi interessa il tema, non potete assolutamente non visitare.

- https://museo.freaknet.org/it/

Anche curatori di

- https://binart.eu/

una mostra che mischia sperimentazione artistica e retro computing.

La vicenda Karl Kock

Sulla vicenda di Karl Kock, tragica e piuttosto emblematica di quel periodo storico esistono diverse produzioni tutte piuttosto di nicchia:

- *23 : la storia dell'hacker Karl Kock* di Hans-Christian Schmid, Michael Gutmann, Schmid, Hans-Christian Gutmann, Michael, Shake, 2001
- Un film, di cui è possibile reperire i sottotitoli in italiano: 23 – *Nichts ist so wie es scheint* ("Nothing is what it seems"), 1998
- Una graphic novel realizzata da Andrea Ferraresso nel 2006, http://www.olografix.org/uccidere-un-hacker/
- La vicenda dal punto di vista del sistemista americano che svelò l'intrusione: *The kgb, the computer and me*, 1990 (una sorta di docu fiction)

La vicenda Hacking Team

Piuttosto che leggere articoli di giornale spesso piuttosto confusi date un'occhiata direttamente all'archivio di e-mail sottratte e disponibile su

- https://wikileaks.org/hackingteam/emails/

La storia fornirebbe mille filoni da indagare, dai rapporti di Hacking Team con le istituzioni alla vendita a paesi sotto embargo per violazione dei diritti umani. C'è poi l'aspetto tecnico, la possibilità di studiare da vicino il software che vendevano, che probabilmente è simile a tutta la famiglia di suite di programmi trattati nel mercato della sorveglianza internazionale.

Già prima dell'intrusione Hacking Team era stata indicata come un'azienda dalle frequentazioni quantomeno ambigue, si veda a questo proposito i numerosi articoli apparsi su sito di Citizen Lab, aggregati in

- https://citizenlab.ca/tag/hacking-team/

In particolare

- https://citizenlab.ca/2017/01/new-york-times-article-features-citizen-lab-research-hacking-team/
- https://citizenlab.ca/2015/08/hacking-team-leak-highlights-citizen-lab-research/

CYBER BLUFF

EXTRA

Si potrebbe anche cercare di approfondire la vicenda dal punto di vista del gruppo o singolo che ha rivendicato la parternità dell'attacco. Si trovano con semplici ricerche in rete documenti a firma Phineas Fisher, in particolare sulla vicenda Hacking Team si cerchi "how he took down HackingTeam".

Si troveranno diverse traduzioni, mirror, ecc. Ad esempio uno dei primi risultati per me è stato

- https://gist.github.com/jaredsburrows/9e121d2e5f1147ab12a696cf548b90b0

da cui potete leggere il documento integrale, per altro ricco di link tecnici e considerazioni interessanti per chi sia motivato a approfondire anche l'aspetto tecnico della vicenda.

Si può anche dare un occhio a

- https://twitter.com/hashtag/phineasfisher
- una ricerca con le parole tipo "phineas fisher" "pastebin" può risultare utile per recuperare altri documenti prodotti

La vicenda Stuxnet

Citata molto spesso, a parte il documentario già segnalato tra i consigli per approfondire alla fine del libro dal titolo Zero Days, tenete presente anche il libro

- *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital*, Kim Zetter, 2015

La vicenda Telecom/Sismi

Non ha trovato posto nel libro per problemi di spazio, ma si tratta di una storia veramente interessante e emblematica, dove ricorrono stilemi e paradigmi comportamentali e ideologici tipici del rapporto tra Stato, industria/finanza e IT.

Per una narrazione parziale dal punto di vista di uno dei tecnici coinvolti si legga

- *Le tigri di Telecom*, Andrea Pompili, Stampa Alternativa, 2009

La storia si dipana in mille rivoli, si intreccia con l'espansione e contrazione dei possedimenti Telecom in Italia e in Brasile, con la riforma dei servizi segreti che porta alla scomparsa del Sisde e del Sismi, ecc. Per orientarsi e approfondire il complesso intreccio processuale si può partire dalla pagine di wikipedia italia, che non è fatta malissimo e aiuta a dare un ordine alla storia.

- https://it.wikipedia.org/wiki/Scandalo_Telecom-Sismi

La vicenda Snowden

Questa storia è rimbalzata ovunque sui media non pensiamo di dover aggiungere molto, se non un invito a approfondirne gli aspetti tecnici, cercando laddove sia fattibile di consultare autonomamente i documenti rilasciati sono ormai raccolti e indicizzati in diversi archivi, in particolare si veda

- https://cryptohome.org (per questi e molti altri documenti riferibili all'intelligence internazionale)
- si veda anche questo archivio curato da giornalisti canadesi, https://www.cjfe.org/snowden

La vicenda Valut 7 e 8

Wikileaks pubblica due serie di leak abbastanza simili al materiale rilasciato da Snowden relativo al Nsa, ma riferibili alla Cia. Il materiale tecnicamente è quasi più interessante del precedente, perché descrive meglio i tool sviluppati e le loro finalità.

- https://wikileaks.org//vault7/
- https://wikileaks.org/vault8/

La vicenda Echelon

Prima delle rivelazioni di Snowden intorno al 2000 un'altra fuori uscita di notizie aveva anticipato i tentativi di utilizzare le grossi dorsali di telecomunicazione come meccanismo di sorveglianza. Il progetto nasce negli anni '70 come una collaborazione tra Usa, Australia, Canada, Nuova Zelanda e Inghilterra, anche noto ai tempi della guerra fredda come *Five eyes* (cinque occhi, come i paesi aderenti). Per un quadro generale si veda

- https://en.wikipedia.org/wiki/ECHELON

Risorse e manuali utili

L'elenco potrebbe essere lunghissimo, come regola generale iniziate a leggere qualcosa e approfondite i termini, i software o le tecniche che più vi interessano cercando sui motori di ricerca, l'importante è partire da qualche parte.

- https://contrabbandiera.it/product/guida-autodifesa-digitale/, traduzione italiana di http://guide.boum.org/
- Un sito nato dopo la vicenda Snowden con alcuni consigli per cercare di evitare il controllo di massa: https://prism-break.org/it/

Servizi autogestiti

Il modello autogestionario sarebbe un buon modello di sviluppo decentrato di Internet. L'idea che piccole o medie strutture gestiscano risorse come posta elettronica, piattaforme varie e eventuali, non è qualcosa di tecnicamente impossibile o particolarmente utopistico. Da un certo punto di vista è molto più terra terra che non i tracotanti sogni di gloria dei colossi del web, e della strana religione dei Big Data. Non di meno non è la strada che le cose stanno prendendo. Esistono però una serie di servizi che ci sentiamo di consigliare, se non altro perché ne conosciate l'esistenza e perché di fatto rappresentano un modello di concreto di come si potrebbero decentralizzare le strutture, disarticolando i centri di potere.

CYBER BLUFF

EXTRA

Qui di seguito vi proponiamo una raccolta non esaustiva di strumenti utili, non commerciali, autogestiti e rispettosi della vostra intimità. Non tutti i servizi sono ancora attivi, ma in tutti vengono indicate nel caso delle alternative.

Scambio file

https://zerbino.esiliati.org/

Per scambiare velocemente file temporanei. I dati vengono cancellati dopo **un mese**, la dimensione massima è **256MB. Carica il tuo file**, **condividi il link con chi devi.**

https://upload.disroot.org/

Idem, sempre per file temporanei.

https://framapic.org

Condivisione immagini, solo immagini. Non occorre registrarsi, si sceglie dopo quanto tempo i file verranno cancellati.

https://cloud.disroot.org

Occorre registrarsi. Cloud basato su Nextcloud. Oltre al cloud, hai a disposizione calendario e contatti, gallerie, task, appunti, pad collaborativi, aggregatore di feed rss, segnalibri, audio/video conferenze e altro.

Scrittura collettiva, **appunti e gestione progetti**

https://we.riseup.net/

Occorre registrarsi. Ogni utente può creare un numero illimitato di progetti. Ogni progetto ha a disposizione wiki, condivisione file, gallery di immagini, elenchi di task, sondaggi, discussioni di gruppo. Le pagine dei wiki possono essere rese pubbliche o visibili soltanto ai membri del progetto.

https://pad.riseup.net/

Non occorre registrazione. Scrittura collettiva di appunti. Quando si crea un nuovo pad se ne sceglie nome e durata (1 giorno, 2 mesi, 1 anno). Condividi il link con chi devi, chiunque ha il link può liberamente scrivere sul pad.

https://pad.cisti.org

Stessa cosa di sopra.

https://pad.disroot.org/

Stessa cosa di sopra.

https://framapad.org/it/

Idem.

CYBER BLUFF

EXTRA

Fogli di calcolo

https://calc.disroot.org/

Fogli di calcolo collaborativi (e condivisibili). Non occorre registrazione.

https://accueil.framacalc.org/it/

Stessa cosa di sopra. Non occorre registrazione.

Alternative a pastebin

https://bin.disroot.org/

Alternativa a pastebin. Non occorre registrazione.

Gestione progetti

https://framemo.org/

Lavagna di appunti collettivi. Non occorre registrazione. [Sito in lingua francese]

https://framaestro.org/

Permette di scegliere vari strumenti da riunire in una schermata (condivisibile con altri). Adatto per riunioni e progetti collettivi. [Sito in lingua francese]

Caselle di posta

Autistici/Inventati

Disroot.org

Chiacchiere e discussioni

https://forum.disroot.org/

A dispetto del nome vintage, puo'essere utilizzato come mailing-list, chat permanente, messaggistica istantanea. Occorre registrarsi.

https://webchat.disroot.org/

Chat online. Occorre avere un utente xmpp (autistici, disroot o altro)

Pianificazione appuntamenti e sondaggi

https://poll.disroot.org/

Pianificare un appuntamento o prendere una decisione collettivamente. Non occorre registrazione.

https://framadate.org/

Stessa cosa di sopra. Appuntamenti e decisioni.

CYBER BLUFF

EXTRA

Videoconferenze

https://framatalk.org/accueil/it/

Audio/Video chat

https://vc.autistici.org

Audio/Video chat

https://calls.disroot.org/

Audio/Video chat

https://farma.cisti.org/

Audio chat

Motori di ricerca

https://search.disroot.org/

Accorciatori di link

http://vado.li/

https://frama.link/

CYBER BLUFF

EXTRA

Numeretti strambi, la crittografia

La crittografia è un argomento troppo ampio, quindi ci limiteremo a dare qualche riferimento secondo noi utile per approcciarsi in qualche maniera alla questione.

Un libro serio

Per chi volesse un libro da cui partire per capire le basi matematiche e applicative:

- *Serious cryptography, A Practical Introduction to Modern Encryption*, Jean-Philippe Aumasson, 2017, No starch
- *Crypto Dictionary*, Jean-Philippe Aumasson, 2021, No starch

Paccioccare con gli strumenti senza troppa fatica

Per sperimentare invece con gli strumenti a disposizione vi consigliamo di provare Tails, una distribuzione Linux concepita per sfruttare i diversi strumenti citati velocissimamente anche nel libro. Partite dalla documentazione

- https://tails.boum.org/doc/index.it.html

Anche se poi non le userete in questa forma, vale la pena passare un po' di tempo a paccioccare con queste cose, magari un giorno vi tornerà utile.

Cypherpunk

Se volete capire un po' meglio quello strano fenomeno culturale detto cypherpunk la pagina inglese di Wikipedia contiene un bignami non pessimo: https://en.wikipedia.org/wiki/Cypherpunk

Segnaliamo inoltre un libro che sul finire degli anni '90 fotografò un intreccio interessante tra pensiero radicale e movimentista italiano e un certo approccio maturato all'interno della comunità cypherpunk. Il testo è stato pubblicato da Nautilus e si intitola Kriptonite.

Potete scaricarlo da

http://www.nautilus-autoproduzioni.org/wp-content/uploads/2015/01/KRIPTO.pdf

L'escamotage narrativo e l'introduzione meritano sicuramente una lettura.

La responsabilità dei crittografi

Per sondare una nicchia interessante del dibattito accademico interno al mondo della crittografia vi consigliamo di leggere l'articolo di Phillip Rogaway *The Moral Character of Cryptographic Work*. Integralmente in inglese o nella sintesi apparsa su una rivistina autoprodotta da un piccolo manipolo di persone con la passione per la letteratura immaginifica.

Versione integrale in inglese

https://cs.pomona.edu/~michael/courses/csci190f20/papers/moral_crypto.pdf

Riassuntino a pagina 46 del n.7 di Ruggine

https://collanediruggine.noblogs.org/files/2018/09/ruggine7WEB.pdf

CYBER BLUFF

EXTRA

La crittografia non va comunque presa troppo sul serio. Provate a ricordare il fitto dibattito nato intorno alla app Immuni, nel quale anche i media mainstream si inerpicavano in perifrasi nel tentativo di illustrare il funzionamento del modello decentralizzato Apple/Google o gli altri standard sviluppati per l'occasione. A aprile/maggio 2020 ferveva la discussione e sembrava che tutta Italia fosse chiamata a farsi un'opinione in merito, a settembre il giochino geek aveva già perso di interesse, a dicembre 2020 non ne parlava più nessuno. Quello che secondo l'allora commissario Arcuri doveva essere uno strumento fondamentale nella fase di gestione endemica della pandemia si era rivelato solo una buzz word. Non è che fosse pensato male tecnicamente, è solo che non serviva a niente. Dal punto di vista del protocollo era tutto funzionante, solo che per curare delle persone servono altre persone, e una app è poco utile, anche al contact tracing.

CYBER BLUFF

EXTRA

Malware maleficarum

Malware, virus, worm, vari e eventuali

Storielle

Virus e worm sono vecchie conoscenze dell'informatica, hanno degli antecedenti letterari ancor prima che realizzazioni pratiche.

Questa pagina di Wikipedia traccia una time line ricca di spunti

- https://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms

Il termine malware è di utilizzo più recente e connota tutto, qualsiasi programma che esegua attività non "gradite" su un computer, dove "gradite" è chiaramente una questione interpretativa.

Se siete interessanti agli aspetti narrativi e ai risvolti di cronaca legati all'utilizzo dei malware vi rimandiamo ai libri segnalati nelle note all'Introduzione, in particolare quelli di Carola Frediani.

Tecnicaglie

Per le persone più curiose consigliamo

- https://class.malware.re/

Si tratta di un corso universitario, anche solo scorrendo la pagina potete farvi un'idea di come si tratta, si analizza e si definisce un malware dal punto di vista tecnico. Se poi vi sentite particolarmente audaci potete provare a seguirlo, il materiale è a disposizione.

In rete troverete molto materiale simile, potete approcciare la questione anche dal punto di vista della reverse engineering. Un bellissimo corso in questo senso è

- https://guyinatuxedo.github.io/

L'approccio è molto pratico e basato sui CTF (Capture the flag). Quest'ultimi sono dei balocchi, alla stregua di problemi di scacchi o giochi di ingegno. C'è un programma o un sistema da analizzare e bisogna catturare una bandierina, nella forma di un codice, una frase o un'azione da compiere, celata da qualche parte o comunque ottenibile solo forzando il sistema a consegnarcela.

Sono quelle che potremmo definire delle palestre di hacking nell'accezione pop di film come War Games o serie come Mr Robot. Se vi interessa questo tipo di tecnicaglia i due link precedenti sono sicuramente un punto di partenza utile, su cui passare i prossimi 2 o 3 anni. Per non scoraggiarvi subito tenete presente che la curva di apprendimento è molto alta all'inizio, ma comunque l'idea è capire il metodo e apprezzare le malizie e le sfumature, se non riuscite a risolvere un giochino guardare e capire le soluzioni è comunque parte del processo di apprendimento.

L'analisi dei malware è molto in voga tra gli enti governativi, un sito interessante a riguardo che produce analisi tecniche di malware e le pubblica in italiano è

https://cert-agid.gov.it/category/malpedia/

Nelle note a "L'innocente confusione tra dati e istruzioni" troverete altro materiale utile sul tema, perché gli argomenti sono strettamente legati: i malware utilizzano

exploit noti o meno per arrivare a installarsi sul proprio bersaglio. Quando su un giornale leggete “Il malware sfrutta la vulnerabilità tal dei tali per installarsi sulla macchina” si intende questo tipo di processo.

CYBER BLUFF

EXTRA

L'innocente confusione tra dati e istruzioni

Il prezzo degli errori

Nel capitoletto del libro si è parlato di exploit da un punto di vista di senso, si è definito un po' di terminologia e altre cosette. Per farsi un'idea più precisa di quanto valga un exploit funzionante potete controllare da soli sul sito

- https://vuldb.com/

Cliccando anche un po' a caso noterete come ogni vulnerabilità sia "prezzata". Non è un listino ufficiale, si tratta di una stima, l'exploit vale sostanzialmente quanto chi lo compera è disposto a pagarlo. Sorge spontanea la domanda, ma chi lo compera? Dipende, nel mercato della sicurezza bianco e nero ci sono diversi acquirenti, aziende specializzate in sicurezza informatica, governi, criminalità organizzata, ragionate un po' come in una spy story e forse non andrete lontano dal vero.

Non tutte le vulnerabilità sono però oggetto di vendita, esiste una corrente di pensiero che spinge invece per il rilascio pubblico e la produzione di Proof of concept funzionanti e liberamente scaricabili. L'idea è di fornire gli strumenti per provare e verificare i problemi.

Gli approcci alla questione divergono insomma: c'è chi sviluppa exploit, li usa e se li tiene per sé, chi li vende e chi li rilascia pubblicamente, con sfumature diverse e intrecci tra le tre possibilità.

Esistono liste di discussione pubbliche sul mondo delle vulnerabilità informatiche e svariati database consultabili in rete. Riportiamo qualche link tra i più noti qui di seguito

- https://www.securityfocus.com/vulnerabilities
- https://www.exploit-db.com/
- https://www.cvedetails.com/

Se volete leggere qualche libro interessante e tecnico sul mestiere di ricercare bug sfruttabili per segnalarli o costruirci sopra degli exploit, attività anche nota come bug hunting, vi consiglio

- *A Bug Hunter's Diary, A Guided Tour Through the Wilds of Software Security*, Tobias Klein, 2011, Nostarch
- *Real-World Bug Hunting, A Field Guide to Web Hacking*, Peter Yaworski, 2019, Nostarch

Esistono anche piattaforme dedicate solo a questo, in cui le persone si registrano e ricevono una sorta di "licenza" per cercare bug su alcune infrastrutture, nel momento in cui trovano qualcosa e lo segnalano, ricevono in cambio del denaro e aumentano la propria reputazione. Con una migliore reputazione puoi entrare a far parte di progetti più remunerativi, su invito. Si tratta sostanzialmente di una versione geek e digitale del lavoro a "cottimo", con in più l'esigenza pressante di arrivare prima degli altri. Racchiude in sé praticamente tutto il peggio del mondo del lavoro, ma con l'illusione di stare partecipando a un giochino per hacker.

AlanTuring

Potete trovare tanto materiale autonomamente noi vi consigliamo un fumetto

- *Enigma. La strana vita di Alan Turing*, Tuono Pettinato e Francesca Riccioni, Rizzoli, 2012

Instant messaging / Social media aka social network

È forse l'argomento più battuto da giornalisti e ricercatori, per questo è forse anche quello su cui si sentiamo di non avere molto da dire. Sono tanti i libri, gli articoli su questi argomenti. Se volete leggerne uno solo vi consigliamo con qualche riserva e precisazione

- *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, 2019, Luiss University Press

La parte di ricerca nel libro è sicuramente completa, ben curata e interessante, il problema sta nelle conclusioni che non sono all'altezza della critica e si stanziano su posizioni da "capitalismo buono".

Potete leggere questa recensione del libro su Carmilla che mette in evidenza questo aspetto

- https://www.carmillaonline.com/2020/09/10/nemico-e-immaginario-surveillance-capitalism/

o se preferite immergervi in atmosfere esotiche e acarose quest'altra all'interno del numero 1 della fanzine *Choosy* (che, recensione a parte, vale almeno una visita veloce)

- https://ifdo.noblogs.org/files/2020/09/Choosy-N1.pdf