Digeat N.4 - 19 Dicembre 2024

Da Tototruffa a Mitnick passando per Leonardo: l'hacker tra digitale e analogico

Di Stefano Gigante

Abstract

Il caso dell'"Hacker del Ministero della Giustizia", apparso sulla stampa come esempio cardine di una serie di violazioni normative e tecniche, rimette in discussione le nostre certezze su questa misteriosa figura. Tutto quello che sappiamo sugli Hacker è sbagliato. Prima del Condor, c'era il Cavaliere Ufficiale Trevi. Il pericolo non viene quindi da un mondo virtuale accessibile da una buia stanza illuminata dalla fioca luce di un monitor, ma da astuzie e *malpractice* del mondo fisico.

Indice

- Introduzione
- Il Principe della risata: hacker ante litteram?
- Da Totòtruffa al Condor
- "Essere hackerati", oggi
- L'hacker, dal punto di vista del diritto
- L'hacker, secondo sé stesso

Introduzione

Nel mentre questo articolo in è in elaborazione, è passato un mese dal c.d. "attacco hacker" al Ministero della Giustizia. Quando sarà pubblicato sarà passato probabilmente un altro mese. Un tempo più che sufficiente nell'immaginario collettivo per elaborare un momento che per molti si tingerà di sci-fi, ma non sempre nel modo sbagliato.

La notizia è nota: un 23enne è entrato nei server di diverse Procure, ottenendo le password di 23 PM e ponendo un grave problema di sicurezza. Storia attinta da quel genere di mistero che solletica chi ama una visione romantica dell'hacker: secondo la stampa, il giovane cercava un vero e proprio *Tesoro del Deep Web*.

Spesso quello che sappiamo nasconde l'attenzione da quello che dovremmo sapere: non ci sono gli schermi bui di una stanza in stile *Matrix* o la Night City descritta da *Cyberpunk 2020* (il secondo capitolo della saga da cui è ispirato il videoludico *2077*) dalla quale accedere ad un mondo di tesori, ma un piccolo furbo mondo di navi di marina ormeggiate con computer accesi e non protetti da password, computer inutilizzati, ma ancora connessi alla rete da cui creare nuovi account e mail di *phishing.*

Possiamo quindi imparare una lezione: **qual è il vero volto dell'hacker.**

Il Principe della risata: *hacker ante litteram?*

La cosa più simile ad un hacker che abbiamo mai visto in un film italiano appare in un film del 1961, *Tototruffa 62*, in cui, sia pur nella simpatica goffaggine tipica della "commedia all'italiana", il principe Antonio De Curtis detto Totò interpreta un prototipo dell'hacker.

Un *ingegnere sociale*, anticipatore del concetto immortalato qualche anno dopo dal decano degli hacker "*Condor"* Kevin Mitnick, dedito a guadagnarsi l'accesso a luoghi inaccessibili con strategie assai moderne.

Travestito da "Ambasciatore del Katonga", lo si vede entrare in ambasciata per farne scenario di una truffa, introducendo così il concetto di *phishing* e *scamming*, il primo espresso nell'ormai celeberrimo sketch in cui l'*ingegneria sociale* lo rende *Ingegner Trevi*, "discendente del proprietario dell'omonima fontana" pronto a venderla, assieme al suo vitalizio in monetine, allo sprovveduto turista *Decio Cavallo.*

Phishing è l'arte con cui l'hacker ottiene credenziali, dati finanziari e codici di accesso usando una fittizia identità digitale superiore per credibilità e fama alla sua identità reale, nonché *scamming* l'evoluzione finale del raggiro che rende quell'identità spendibile. L'anello più debole della catena è sempre e sempre sarà il PEBCAC ("problem exists between chair and computer", "*quel problema tra la sedia e il computer*"), l'essere umano.

Nella nostra storia italiana moderna è un PEBCAC che ha lasciato un computer alla mercé del nostro hacker. Ma è un PEBCAC scarica Ransomware ed altri Malware leggendo in intestazione loghi di Agenzia Cybersicurezza Nazionale e Polizia di Stato.

Ottenere credenziali, accesso a dati, PEC o bloccare i dati di qualcuno diventa facile come una metamorfosi nell'*Ambasciatore del Katonga o nell'Ingegner Trevi.*

Da Totòtruffa al Condor

Eravamo nel 1961: due anni dopo, nel 1963 sarebbe nato Kevin Mitnick, nel pieno della grande generazione dei *Phreaker*, i *"Phone Hackers"* parte di un pantheon dell'hacking moderno. Il debutto ufficiale del Condor nel mondo dell'hacking ***non vede scenari da telefilm.***

Vede l'allora dodicenne Mitnick, figlio di madre single con troppo tempo e poca supervisione decidere di voler viaggiare per Los Angeles, ma di famiglia monoreddito degli anni '70, avere pochi soldi da dedicarvi. Decise così di praticare un investimento che combinò il suo primo atto da *ingegnere sociale* col suo primo "hacking", inteso nel senso di *persona ,(Internet's User Glossary, RFC 1392)****[1]*** passando al *cracking* quando tale conoscenza diventa un peccaminoso "frutto del bene e del male" da usarsi a suo vantaggio. Nel primo passaggio il giovane Kevin si procura la conoscenza, fingendosi uno scolaro intento in una ricerca su biglietti e obliteratrici e si fa istruire allo scopo da un controllore gentile. Nel secondo passaggio **Kevin acquista un'obliteratrice usata** col medesimo pretesto per poi **rubare dai cassonetti** mazzetti di biglietti in parte ancora utilizzabili.

Mitnick imparò due lezioni in una: la **conoscenza del sistema tecnico** gli aveva fornito chiavi di accesso (i biglietti "auto-obliterati" da esibire) e **l'ingegneria sociale** che gli aveva aperto tali porte.

Concettualmente **fu la stessa operazione che nel 1979 lo consacrò come hacker:** nel pieno della *cultura hacker*, desideroso di impressionare un gruppo di hacker alla Los Angeles Unified School District, decise di "bucare i server" dell'Arca, il sistema informatico usato da DEC per lo sviluppo del sistema operativo RSTS/E. Anche qui, l'hacker passo dal PEBCAC: un giro di telefonate dopo, Mitnick aveva convinto l'amministratore di sistema di essere uno sviluppatore particolarmente distratto e di voler iniziare, in tempi precedenti la 2FA, una procedura di recupero. Tornò così dai suoi nuovi "amici" (che usati i dati ottenuti lo "scaricarono" dandogli una nuova lezione sul fattore umano) vantandosi di essere non solo entrato nell'Arca, ma di averlo fatto da amministratore di sistema, in grado di erogare nuove password.

> **Questo ricorderà al lettore quanto descritto sull'hacking al Ministero.** E se il debutto del *Condor* non solletica la similitudine, lo faranno le parole che un *Condor* ormai adulto userà per riassumere la sua esperienza ormai decennale dinanzi al Congresso USA: *"Ho ottenuto accesso non autorizzato ai sistemi informatici di alcune delle più grandi aziende del pianeta e sono penetrato con successo alcuni dei sistemi informatici più resilienti mai sviluppati. Ho usato sia mezzi tecnici che non tecnici per ottenere il codice sorgente di vari sistemi operativi e dispositivi di telecomunicazione per studiare le loro vulnerabilità e il loro funzionamento interno"*

Enfasi sia data a mezzi tecnici e non tecnici: conoscendo il segreto, diventerà più facile difendersi e, assai probabilmente, **se si ricordasse di associare la figura dell'hacker al *Condor* ed all'*Ingegner Trevi* anziché figure come il *Mr. Robot* televisivo o i personaggi di *Matrix* e *Cyberpunk***, si riuscirebbe a migliorare la postura social di enti ed amministrazioni *in primis*, ma anche dei privati: si confida alcuni dei quali stiano leggendo queste parole.

"Essere hackerati", oggi

Ancora oggi, nel 2024, secondo il Threat Report periodico di Crowdstrike tra le minacce principali vi sono le intrusioni dirette con **accesso fisico (hands-on-keyboard)** e l'esfiltrazione dati da account legittimi.

> Il punto debole dell'organizzazione diventa l'organizzazione stessa, e qualora non sia possibile per limiti dimensionali piantare una "talpa" in loco (quale il caso citato di un tecnico IT pronto ad abusare delle credenziali ottenute), l'oggetto delle piccole organizzazioni è il PEBCAC, e l'incremento dei mezzi tecnici consente di farlo in remoto, ancora più remoto.

Si pensi alla cosa più innocente del mondo: il test *"scopri quale Principessa Disney potresti essere"* o *"scopri il tuo nome da Supereroe dove la prima parola è il tuo mese di nascita e la seconda il tuo giorno di nascita".*

Nessun problema, si potrebbe pensare: è solo un gioco. Ma non lo è. Tra le password più comuni usate dall'utente medio, fonte WEF, compare infatti la sequenza 12345678, immortalata dal celebre film *Spaceballs* come "la combinazione che un idiota userebbe per la sua valigia", ma anche ogni possibile combinazione dataria, dalle date di nascita proprie agli anniversari fino alla data di nascita del proprio figlio. Tutti amano i bambini, vero? E tutti amano scoprire che il proprio nome da supereroe potrebbe essere qualcosa di "epico" come *Red Riot*. Nome che casualmente consentirà al gestore del test (che se è stato così furbo da metterlo su un sito esterno che chiede una email valida per spedire "la licenza da eroe" otterrà un indirizzo su cui collaudare quanto ottenuto) di provare come password o pin 050683, laddove 05 e 06 risultano associati a "Red" e "Riot" e la data di nascita era lì in chiaro in fondo al *nickname* usato per generare la mail o nel profilo social del futuro hackerando.

O un attacco *clickjacking*: un'interfaccia costruita in modo che il prezioso click diventi consenso e accesso a qualsiasi altra cosa, ben nascosta nell'equivalente virtuale di una ricevuta da firmare con un bel foglio di carta copiativa e un diverso documento sul fondo, o uno qualsiasi dei molteplici mezzi con cui **un essere umano prende il controllo dei sistemi informatici di un altro essere umano usando astuzie tipicamente umane.**

Scopo di questa esposizione non è negare che tra le forme di accesso abusivo vi siano quelle che passano per **vulnerabilità del sistema**, ma anche qui è più probabile che **l'hacker passi dall'intervento umano omissivo o commissivo,** servendosi di *botnet* (reti di computer "zombificati" da malware che sfruttano vulnerabilità coperte da aggiornamenti che l'utente non ha mai fatto temendo il complottistico fantasma dell'"aggiornamento che rallenta il computer").

> Bensì ricordare quanto lo *specimen* che *l'hacking* al Ministero della Giustizia ci ha ricordato è lontano anni luce dai *quickhack* del mondo di *Cyberpunk*, accesso istantaneo ad un immateriale dai contorni dell'irreale, o dai serial televisivi con figure dall'aspetto trasandato e inquietante con le rapide dita su una tastiera in un improbabile rito tecnomagico che culminerà invariabilmente con la scoperta di una parola chiave simile ad un *cheat code* per la realtà, ma affine a profondi conoscitori dello strumento informatico e della natura umana.

L'hacker, dal punto di vista del diritto

Dal punto di vista legale, bisogna ricordare con l'Epistola ai Romani, versetto 6:23 il valore del *frutto del peccato*. Se hacker è chi conosce approfonditamente i meccanismi che regolano sia lo strumento ICT che la mano che lo impugna, l'abuso non è privo di conseguenza.

> L'art. 615 ter c.p. ad esempio, l'accesso abusivo ad un sistema telematico o informatico, aggravato non a caso dalla forte componente umana dell'abuso del potere o di qualifiche personali (investigatori privati, operatori di sistema infedeli), o il quater, che sanziona *chi abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.*

La formulazione vi ricorderà qualcosa: non è un caso che l'art. 617 sexies c.p. e il 640 ter c.p. tornino di prepotenza nel *phishing*, di cui possono costituire concorso, e sostanziato proprio modificando le comunicazioni tra enti e persone, con mezzi sempre più evoluti dalla "mail dalla banca" con loghi artefatti al *deepfake* dove chiamate e videochiamate vengono "ricostruite" con l'Intelligenza Artificiale chiudendo (per ora) quel cerchio partito da un *Totò* in *blackface* vestito da ambasciatore e passato per un allampanato ragazzino al telefono pronto a giurare di essere programmatore della DEC.

Tempi duri per hacker e truffatori, titolava il numero del 24 Febbraio di *sistema società* introducendo le *Norme in materia di misure per il contrasto ai fenomeni di criminalità informatica,* (G.U. n. 45 del 23.02.2012), implicitamente introducendo in un testo tecnico e ragionato quel filo che oggi ispira questo testo, che va dall'*Ingegner Trevi* ai *netrunner* della sci-fi passando per gli hacker, esaminando però l'hacker nel profilo della condotta perseguibile ma non dal punto di vista etico e sociologico.

L'hacker, secondo sé stesso

Non si potrà che chiudere provando a definire il protagonista di questa rubrica. Eroe, *villain*, cacciatore di tesori o conoscenza forse: utente evoluto in ogni caso.

> Tradizionalmente ogni buon *hacker* si qualificherà come *white hat*, dal linguaggio grafico dei *Western*, "eroe" ambientato da curiosità e ricerca o un *black hat* animato da scopi sfacciatamente illeciti. Ma a meno che si tratti di test preconcordati, un *white hat* ricade spesso nella categoria del *gray hat*, la cui unica garanzia è un codice etico e morale solido, ma non giustiziabile.

La mente non potrà che correre ad un precedente scritto apparso proprio su queste pagine virtuali: come tracciare, dall'esterno, il confine tra l'*hacktivism*, l'atto dell'hacker che sprotegge programmi regolarmente acquistati esponendosi però alle conseguenze legali allo scopo di ribadire la signoria sul proprio sistema informatico ad esempio ma anche per difendere importanti cause etiche e morali, la sete di conoscenza e l'edonismo dello *script kiddie*, *wannabe* armato di conoscenze di seconda mano

e desideroso di provarsi al mondo?

> Chi deciderà se non a posteriori chi ha agito per vendetta, calcolo, curiosità o amore per la tecnologia? Non chi vi scrive, non chi ci legge forse. Ognuno ha diversi ruoli nella storia di un altro: anche un *netrunner*, anche un *Ambasciatore in Blackface*, anche il *Condor*, anche il cacciatore del *Tesoro del Berlusconi Market* sul *Deep Web.*

Ma anche chi legge ora queste righe potrà ben esserlo: un *trickster* non ha confini, e se mantenere il discorso sospeso tra diritto, statistica e immaginario collettivo bisogna, si potrà fare un ultimo salto dal (*Neuromante*, traduzione di T. Pincio per Mondadori)[2] della sci-fi di *William Gibson* e *Mike Pondsmith* al distopico mondo di *Cory Doctorow.* il probabile/improbabile eroe, *Marcus Yallow*, comincia il cammino che in *Little Brother* e *Homeland* lo renderà l'*hacker, hacktivist e terrorista* più temuto di America usando per studio un portatile da lui costruito con parti da lui conosciute e approvate e "sperimentando" coi tag *RFID* dei libri della biblioteca.

A tutti gli esempi di *hacker* apparsi in queste righe, si potrà aggiungere il *minimo comun denominatore*: **l'utente consapevole della tecnologia** che sua al punto da volerla rendere propria portandola oltre ogni limite e diventando da utente creatore.

NOTE

[1] Si fa riferimento all'edizione inglese dell'Internet User's Glossary, RFC 1392, che alla voce "Hacker" riporta "A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The term is often misused in a pejorative context,where "cracker" would be the correct term. See also: cracker.".

[2] Durante la stesura di questo articolo è stata annunciata un'edizione rinnovata del romanzo citato, con la traduzione di Tommaso Pincio che descrive in quel modo l'incipit, ed una mostra, la "No Curves" che descrive come "colorato al neon" e "neon runners" il mondo del primo immaginario cyberpunk. Sono stati quindi inseriti il link all'originale inglese dell'incipit per correttezza verso l'autore originale Gibson e la mostra. In aggiunta, si segnala l'incipit della versione tradotta direttamente, reperibile qui.