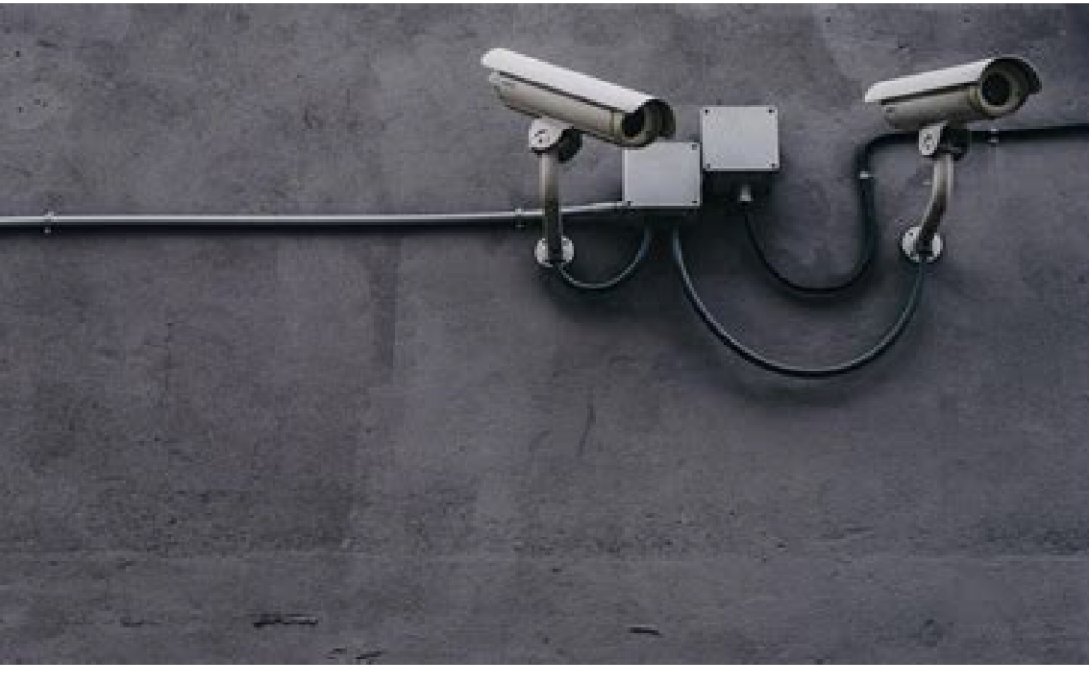
HackBack!
Chiacchiere con Phineas Fisher



L'hacking come Azione Diretta contro lo Stato della Sorveglianza

Abbiamo parlato con l'hacker di fama mondiale e auto-proclamatx anarchicx rivoluzionarix Phineas Fisher riguardo alla politica alla base dei loro attacchi all'industria della sorveglianza, al partito al potere in Turchia e alla polizia catalana. Qui di seguito una retrospettiva sulle imprese di Phineas Fisher accompagnata dalle loro considerazioni per noi.

Testo ed intervista di BlackBird

Hackerare viene spesso visto come qualcosa di tecnico, un semplice fatto di attacco e difesa. Tuttavia le motivazioni sono fondamentali. La stessa tecnologia che costruisce strumenti oppressivi può essere utilizzata come un'arma per l'emancipazione. L'hacking, nella sua forma più pura, non riguarda l'ingegneria tecnologica: si tratta di fare leva sulle dinamiche di potere mandando in cortocircuito la tecnologia. È un'azione diretta verso il nuovo mondo digitale nel quale tuttx viviamo.

Nella penombra dell'impero tecnologico, il mondo hacker è diventato un obiettivo di assimilazioni e infiltrazioni. Ma la base sotterranea non può essere sradicata: di tanto in tanto una nuova azione affiora in superficie. Alcunx delle/degli hacker che ammiriamo sono scrittori di codici che forniscono strumenti per la privacy online e l'anonimato. Altri gruppi creano e distribuiscono media alternativi. E poi ci sono quellx che fanno contro-hacking.

I Circoli Hacker Perduti

Non è un mistero, per chiunque presti attenzione, che per un lungo periodo il mondo hacker underground prendesse anche parte nella guerra in corso. Tuttavia l'effervescenza che caratterizzava la scena underground DIY degli scorsi decenni si è spenta, o comunque è retrocessa in angoli più remoti.

I pessimisti hanno pianto la morte delle comunità hacker con un proliferare di diserzioni individuali.
Vero è che il complesso tecno-militare è riuscito a ingrandire le fila dei mercenari: c'è un prezzo con il quale una certa mentalità può essere comprata, che sia con il denaro, il successo, la sensazione di potere o l'eccitazione nel giocare con formidabili giochini mentre si dà la caccia a quello che la propaganda di stato etichetta come "il nemico".

L'underground ha cercato di incrementare le zone di oscurità e resistenza, mentre la percezione pubblica si è spostata verso la normalizzazione del rapporto fra la mentalità hacker e la tecnologia.

L'Hacker non è più visto come l'adolescente ribelle che crea caos in un gioco casuale (come rappresentato dai film degli anni ottanta/novanta come War Games o Hacker) ma come un'unità altamente specializzata delle forze di occupazione militare, o come la loro scellerata controparte ispirata ai fumetti. Nella sua versione più depoliticizzata il termine "hacker" viene inteso solo come un nome qualsiasi dell'imprenditore capitalista, un simbolo che si può trovare negli "spazi hacker" di qualsiasi città gentrificata.

L'industria della sorveglianza è così orgogliosa dei suoi affari che non si preoccupa neanche di celarli. Rappresentanti delle forze armate e fornitori di programmi di spionaggio si mostrano regolarmente agli eventi della comunità hacker, reclutando apertamente talenti. I video commerciali che promuovono tattiche di "sicurezza offensiva" circolano tranquillamente, vendendo prodotti alle agenzie di spionaggio, alle aziende e ai governi.

È una storia vecchia: gli stati si guadagnano legittimità agli occhi dell'opinione pubblica mostrando come combattono quei crimini che pochi osano discutere (pedo-pornografia, traffico di esseri umani, terrorismo internazionale). Ma non appena hanno le armi della sorveglianza nel loro arsenale le puntano verso l'intera popolazione.

Nel mezzo di questa continua assimilazione del mondo hacker, il complesso della sorveglianza ha subito un colpo notevole seppur invisibile. Una persona, o forse un gruppo, ha reagito hackerando le compagnie di spionaggio informatico e pubblicando i contenuti dei loro archivi segreti. Quando stai combattendo contro un'industria che dipende dalla segretezza, rivelare pubblicamente le loro comunicazioni e strumenti interni può essere una strategia molto efficace.

L'hackeraggio del GammaGroup

Nell'agosto del 2014, è avvenuto un hacking contro "GammaGroup", un fornitore anglo-tedesco di programmi per lo spionaggio. A cui ha fatto seguito una fuga di informazioni di 40 Gb. Dopo questo attacco non c'erano più segreti riguardo GammaGroup: tutto era stato reso pubblico, inclusi i loro clienti, il catalogo dei prodotti, la lista dei prezzi e i programmi stessi, con tanto di manuali di formazione.

Il prodotto di punta della compagnia, un programma chiamato "FinFischer", era stato venduto a più di trenta agenzie governative e forze di polizia per spiare giornalistx, attivistx e dissidenti. L'azienda aveva infettato i/le dissidenti in Bahrain e in Egitto durante la Primavera Araba. Usando l'ingegneria sociale per indurre i loro obiettivi ad installare lo spyware.

i/le dissidenti presx di mira avrebbero cliccato su un documento allegato ad una mail o aperto un link che avrebbe poi installato il programma spia. Da lì in poi i clienti (aziende, governi etc) che compravano il programma dall'agenzia avrebbero avuto il controllo sui dispositivi infettati, sorvegliando i microfoni, le chiamate vocali o Skype, i messaggi, le mail, per non parlare del continuo tracciamento della posizione.

Subito dopo l'attacco hacker, qualcunx ha iniziato a pubblicare messaggi su Twitter spacciandosi per il PR di GammaGroup. La fuga di informazioni non era abbastanza: unx hacker che si fa chiamare PhineasFisher ha fatto uscire un file di testo vecchia-scuola contenente un manuale con i dettagli dell'attacco

alla Gamma:

"Non scrivo questo per vantarmi di quanto io sia un 31337 h4x0r (NdT come nell'originale) e di quali folli abilità abbia usato per mettere fuori gioco Gamma. Scrivo questo per demistificare l'hacking, per mostrare quanto sia semplice, con la speranza di informarvi e inspirarvi ad uscire e hackerare qualsiasi cosa... Volevo mostrare che l'attacco a Gamma Group in realtà non è niente di incredibile, e che voi avete l'abilità di uscire e fare azioni simili."

Il nome di quel file era "HackBack-A DIY Guide for those without the patience to wait for whistblowers" (HackBack-Una guida FaiDaTe per chi non ha la pazienza di aspettare informatori). Per una comunità hacker così pesantemente ferita, in cui la solidarietà iniziale, la libertà e il libero scambio di informazioni stava perdendo terreno contro la mercificazione della conoscenza da parte del mercato e dell'impero, questa azione è stata un respiro di aria fresca. E forse l'inizio di un movimento.

HackedTeam

"Vuoi di più. Devi hackerare il tuo obiettivo. Devi superare la criptazione e catturare i dati importanti, stando nascostx [sic] e irrintracciabile. Esattamente quello che facciamo noi."

Puoi sentire queste parole nella pubblicità di un prodotto chiamato "Da Vinci", un "sistema di controllo remoto" che è stato venduto in tutto il mondo da un'azienda italiana chiamata "Hacking Team".

Una società che si fa chiamare così spudoratamente "Hacking Team" e' quello che si crea quando un dipartimento di polizia locale approccia due hacker dalla mentalità mercenaria con una richiesta di collaborazione.
L'unità di criminalità informatica della polizia di Milano ha deciso che monitorare passivamente non era abbastanza per i loro scopi; per colmare i loro bisogni offensivi hanno chiesto a Alor e Naga, due famosx hacker italianx, un aiuto per modificare un noto strumento di hacking creato originariamente da loro.

Chi fossero i loro clienti e come riuscivano ad infettare e spiare le loro vittime è rimasto un segreto fino al 5 luglio 2015. Quel giorno l'account twitter della società ha annunciato: "Dato che non abbiamo niente da nascondere , pubblichiamo tutte le nostre e-mail, file e codici sorgente", fornendo i link a più di 400 Gb di dati. Come al solito inizialmente la società ha sostenuto che la fuga di notizie era fatta di informazioni false, ma falsificare una tale quantità di dati sarebbe stata un impresa quasi impossibile.

Chi sospettava che l'attacco avesse una firma familiare non aveva torto: il nome sarcastico di Phineas Fisher era di nuovo dietro questa pubblicazione.

Pubblicando tutte le informazioni interne (e successivamente un'altra guida riguardante dettagli tecnici e le motivazioni politiche) Phineas Fisher ha offerto al mondo una prova innegabile riguardo alle operazioni dei settanta clienti di Hacking Team. Molti di loro erano militari, forze di polizia e governi federali e provinciali; le entrate totali superavano i 40 milioni di euro.

Questa fuga di informazioni ha confermato che c'erano molte buone ragioni per la richiesta mondiale di privacy e anonimato. Insieme alle rivelazioni di Snowden, la possibilità di sbirciare negli sporchi segreti di HakingTeam ci diede un'idea sulla grandezza della campagna di sorveglianza mirata portata avanti da governi e grandi aziende. Ad oggi sappiamo che ci sono molte altre organizzazioni senza scrupoli che traggono vantaggio dalle operazioni di spionaggio illegali; un esempio è il gruppo israeliano NSO Group, recentemente coinvolto nell'infezione mirata dei dispositivi dei giornalisti che indagano sul massacro di Iguala in Messico, usando semplici trucchi per spingere le vittime a compromettere i loro stessi dispositivi.

Questo smascheramento anonimo di HackingTeam è stata un'operazione brillante con ripercussioni in tutto il mondo.

Un Negozio di Segreti

Un'attività come Hackning Team dipende dalla segretezza. In molti casi per infettare gli obiettivi viene usato il cosiddetto "zero day[1] ". Uno zero day è una vulnerabilità in un programma per computer che non è ancora stata diffusa pubblicamente, che può essere sfruttata da chiunque la conosca per attaccare i programmi, i dati o le reti, in molti casi offrendo il controllo remoto completo su essi. Di recente il capitalismo della sorveglianza ha creato una rete di compagnie che agiscono da intermediatori finanziari, comprando queste vulnerabilità nei mercati neri e grigi. Il prezzo di un singolo zero day può variare da 10.000$ a 300.000$ e arrivare a un milione di dollari.

Le aziende di spionaggio informatico come Hacking Team "armano" queste vulnerabilità, incollandone molte insieme e vendendo le licenze alle forze di repressione così che loro possano semplicemente "cliccare e spiare", con la possibile aggiunta di servizi personalizzati per penetrare i sistemi che appartengono alle vittime scelte.

La finestra di opportunità per sfruttare questi zero day si accorcia col tempo. Più si sfrutta la conoscenza di una vulnerabilità non nota, più è alta la possibilità che qualcunx si accorga dell'attacco e inizi ad indagare sulle falle che lo hanno permesso, così come la possibilità che altri gruppi trovino le stesse falle. L'opportunità di usare le vulnerabilità finisce quando il programma nel dispositivo dell'utente viene corretto per riparare gli errori: per questo è così importante tenere i propri dispositivi aggiornati. Ci sono comunque dei casi in cui i produttori dei dispositivi rendono la

procedura di aggiornamento difficile o addirittura impossibile.

I trafficanti di vulnerabilità e i venditori di programmi di spionaggio permettono a persone tecnicamente incompetenti di infettare, spiare ed estrarre dati dai loro obiettivi solo compilando moduli e cliccando su un'applicazione internet. Questo e' quello che abbiamo visto quando abbiamo potuto analizzare programmi come "Xkeyscore" o il pacchetto "Galileo" di Hacking Team.

L'ironia sta nel fatto che vendere strumenti a prova di idiota alla polizia può dare una falso senso di sicurezza. Phineas ha scoperto che i sistemi compromessi usavano password assolutamente penose come "P4ssword", "wolverine" o "universo". Nessunx è liberx dalle regole base della sicurezza operativa!

[1] Per saperne di più riguardo alle vulnerabilità software e la guerra digitale del governo, guarda il documentario Zero Days sul caso "Stuxnet"

Hackera il Pianeta! Erdogan e Rojava

Un altro vantaggio del cyberspazio sta nel poter attaccare un bersaglio dall'altra parte del mondo senza dover viaggiare. Non serve neanche alzarsi dal letto, anche se spesso sarebbe meglio farlo per mantenere una mente equilibrata.

"Ho hackerato l'APK" annunciò Phineas nel 2016 dopo aver fatto breccia nei server del partito Turco al potere. Un archivio di più di 100GB di file ed e-mail dell'APK è stato consegnato alle forze rivoluzionarie in Kurdistan. Phineas ha dovuto fare in fretta perché prima che scaricasse tutti i dati Wikileaks aveva già pubblicato l'informazione.

I dati non furono l'unica cosa che arrivò in Kurdistan grazie alle azioni di hacking: Phineas sfruttò anche una vulnerabilità nei sistemi di sicurezza di una banca non conosciuta e spedì 10.000 € in bitcoin al Rojava Plan, un gruppo che coordina la solidarietà internazionale con la regione autonoma del Rojava.

Mossos e Capri Espiatori

Nel maggio 2016, dopo aver guardato il documentario "Ciutat Morta", Phineas pensò di provare un semplice attacco alle forze di polizia catalane. Ciutat Morta è un film riguardo al caso 4F, una famosa vicenda nella storia dello stato spagnolo in cui le forze repressive hanno torturato e imprigionato diversx giovani sudamericanx come vendetta dopo che un poliziotto venne mandato in coma dal lancio di una pietra a seguito di una carica della polizia nel centro di Barcellona.

Come risultato di questa nuova azione di hacking, usando una vulnerabilità ben nota, Phineas coprì il sito del sindacato di polizia catalana con un manifesto ironico che dichiarava che l'organizzazione "è stata rifondata come un sindacato a favore dei diritti umani". Seguì una fuga di dati con dettagli personali di circa 5000 account di polizia, insieme a un tutorial di 40 minuti sulle tecniche usate nell'attacco hacker.

Poco dopo la polizia fece irruzione in diversi centri sociali e hacklab di Barcellona, sostenendo poi di aver catturato l'hacker. Solo ore dopo i/le giornalistx segnalarono che la stessa persona li aveva contattati per dire che era viva e vegeta e che la polizia aveva imprigionato solo un capro espiatorio che per caso aveva ritwittato le informazioni sfuggite all'azienda.

Ma chi è questx Phineas Fisher in realtà?

Una delle conseguenze più interessanti delle azioni di Phineas Fisher sta nello sguardo dex compagnx hacker quando parli dell'argomento con loro. Chi viene dal Cile ti dirà che Phineas è sicuramente di origini latine. Negli squat di Barcellona giurano che il suo tono è familiare. In Italia fanno lo stesso. Negli Stati Uniti pensano che parli come uno di loro. C'e' poi l'ipotesi secondo cui, come qualsiasi hacker molto capace, Phineas debba venire dalla Russia, una di quelle persone Russe che parla sorprendentemente bene lo spagnolo.

C'è davvero qualcosa di familiare nelle azioni di questo fantasma: un profondo senso di giustizia e internazionalismo, e la sensazione che le sue azioni rimarranno sotto il radar perché, come in passato, non si può credere che una persona che vive una vita altrimenti ordinaria possa essere la mente dietro tali imprese.

La verità è che non interessa a nessunx tranne che alla polizia che sta avendo difficoltà ad identificare questa persona malgrado tutto il loro armamentario di modelli conflittuali e strumenti di analisi stilistica. Non ci interessa l'identità della persona che fa queste cose. Non è importante in fin dei conti: quando questa identità sarà scoperta, ne apparirà una nuova. Quando si abbandona il culto della persona, si guadagna improvvisamente un sacco di libertà.

Quello che ci importa è che, chiunque sia, è con noi e le sue azioni ci aiutano a capire il nostro valore.

Queste azioni dirette mostrano che, anche se a volte servono un sacco di sforzo e dedizione per sviluppare un set di abilità specifiche, di solito non è necessario niente di straordinario. Forse non sei particolarmente capace a livello tecnico, ma magari sei capace di interagire con le persone: spesso questa è l'unica cosa che serve per realizzare un hacking fantastico. Oppure non hai un bagaglio di esperienze tecniche ma con una perseveranza determinata e giocosa puoi raggiungere di più che con un corso formale se si tratta di fare breccia nel reame di burocrati da cubicolo che si occupano solo di far rispettare la prassi.

La sicurezza non è una qualità assoluta; non ci sarà mai un potere assoluto nel cyberspazio. Citando Phineas: "*Questa è la bellezza e il paradosso dell'hacking: con* 100 *ore di lavoro una persona può disfare anni di lavoro di un'azienda multimilionaria. L'hacking dà agli oppressi una possibilità per combattere e vincere*".

Le azioni di unx hacker modestx ma motivatx possono andare oltre ai grandi ego gonfiati dell'industria della sicurezza informatica, o degli accademici che non osano agire al di fuori dagli schemi. Non sono sempre i grandi attacchi hacker che cambiano la realtà: chi impara a rimanere nell'anonimato, chi non ha paura e mantiene la disciplina necessaria a non far trapelare dettagli personali ha già un grande vantaggio. Anche non avere un ego da nutrire è fondamentale per mantenere la propria libertà personale.

Alla fine Phineas Fisher tacque. "*Ho chiuso gli account perché non avevo altro da dire*". E probabilmente era abbastanza. A volte una piccola azione e' tutto quello che serve per cambiare l'umore della collettività, per renderci consapevoli del nostro stesso potere.

Epilogo: Anni Silenziosi di Espropriazione a Venire

Phineas Fisher non esiste più. Era più di un nome: la punta di una rete sotterranea di pratiche e desideri. Non era una, ma una serie di azioni. Guerriglia cibernetica: colpisci e nasconditi.

Ad ogni modo, come chiunque scriva alla mail di hackback può testimoniare, Phineas gode ancora della libertà. Intrattenendo una conversazione affascinante, dimostrerà che lo stato non ha il controllo assoluto. Come ripete spesso: è ancora possibile attaccare il sistema e farla franca.

Phineas si è tenutx impegnatx. Si diverte a parlare dall'ombra delle sue nuove occupazioni.

Come ha detto a noi:
"L'esproprio ha alcune conseguenze materiali, ma in realtà è un'arma ideologica. Le regole di questo sistema non sono fatti immutabili, ma regole imposte da una minoranza, regole che noi possiamo mettere in discussione, cambiare e anche distruggere. Quando qualcunx rapina una banca, lo stato spende una grande quantità di risorse per indagare, non perché abbia qualche senso economico spendere 100.000 *indagando su un furto di* 3.000*, ma lo fanno ugualmente per proteggere l'illusione condivisa della proprietà privata. Provano a spazzare via lo spirito ribelle che gioca al di fuori delle loro regole."*

E aggiunge:
"Non servono studi di informatica per poter partecipare a quello cui l'ex capo dell'NSA Keith Alexander si riferisce come il responsabile del più grande trasferimento di ricchezza nella storia. In questo grande progetto la maggior

parte del lavoro non è fatto da hacker, ma da profani, quelli che sanno come trovare gli indirizzi a cui ricevere posta e pacchi, come usare un documento di identità falso in modo convincente e come usare un telefono anonimo. Queste sono tutte le capacità che servono per aprire un contratto di telefonia mobile, aprire conti bancari e chiedere prestiti, fare acquisti online e riceverli. Chiunque può imparare ad usare il TorBrowser e i bitcoin e partecipare al mercato del darknet. Le mafie e il crimine organizzato hanno capito questo cambiamento, ma anarchicx con l'abitudine all'illegalità e all'espropriazione non hanno ancora capito che non siamo più nell'era pre-internet e che ci sono strategie migliori che rapinare una banca con una pistola. Stiamo vivendo un momento unico nella storia, e abbiamo una grande opportunità."

Infatti è così. Lunga vita all'hacking, e a tutti gli espropri silenziosi a venire.

Testo originale da
CrimethInc.
HackBack! Talking with Phineas Fisher
Hacking as Direct Action agains the Surveillance State
5 giugno 2018

Tradotto e impaginato a Gennaio 2023
da Distrozione DIY Label
per info e contatti:
www.autistici.org/distrozione
distrozione@autoproduzioni.net